АКАДЕМИЯ НАУК
СОЮЗА СОВЕТСКИХ СОЦИАЛИСТИЧЕСКИХ РЕСПУБЛИК

ТРУДЫ МАТЕМАТИЧЕСКОГО ИНСТИТУТА ИМЕНИ В. А. СТЕКЛОВА

XI

ACADEMIE DES SCIENCES DE L'URSS
TRAVAUX DE L'INSTITUT MATHÉMATIQUE STEKLOFF

Б. Н. ДЕЛОНЕ и Д. К. ФАДДЕЕВ

ТЕОРИЯ ИРРАЦИОНАЛЬНОСТЕЙ ТРЕТЬЕЙ СТЕПЕНИ

ИЗДАТЕЛЬСТВО АКАДЕМИИ НАУК СССР
МОСКВА • 1940 • ЛЕНИНГРАД

Ответственный редактор
акад. *И. М. ВИНОГРАДОВ*

Редактор издательства *З. Н. Перля*

Технический редактор *О. Н. Персиянинова* Корректор *А. С. Шамбан*

Сдано в набор 5/VII 1939 г. Подписано к печати 11/V 1940 г. Формат 70 × 108/16. Объем 21 1/4 п. л. и 4 вкл. Учетно-издат. л. 34.1. В 1 п. л. 63 000 печ. зн. Тираж 1000 экз. Уполн. Главлита № А-24263. Рисо № 945. АНИ № 1247. Заказ № 3033.

1-я Образцовая типография Огиза РСФСР треста „Полиграфкнига". Москва, Валовая, 28.

ПРЕДИСЛОВИЕ

Большая часть современной теории алгебраических чисел рассматривает вопросы, простейший, но уже не тривиальный, пример которых мы находим в теории квадратичных иррациональностей, данной еще Гауссом в „Disquisitiones arithmeticae". Сюда относятся: теория единиц, теория идеалов, законы взаимности, а следовательно, отчасти, и теория поля классов.

Подробное изучение теории алгебраических иррациональностей третьей степени интересно не только потому, что оно дает следующий по сложности за квадратичным случаем пример на все эти задачи, для решения которых и в этом случае еще можно дать вполне удобные алгорифмы, а главным образом потому, что оно ставит некоторые дальнейшие вопросы, которые в квадратичном случае еще столь тривиальны, что при изучении его не стали перед исследователем. Сюда относятся, в первую очередь, вопросы классификации кубических иррациональностей, так называемая обратная задача теории Галуа для этих иррациональностей, и вопрос о приближении рациональными числами к иррациональностям высших степеней, в полной мере не решенный до сих пор и тесно связанный с вопросом о представлении чисел неполными (т. е. такими, у которых число переменных меньше их степени) разложимыми формами. Эти оба капитальных вопроса впервые в нетривиальной форме появляются в теории кубических иррациональностей, но дальше имеют место для иррациональностей любой степени.

До сих пор в математической литературе не существует монографии по теории кубических иррациональностей. Наша книга заполняет этот пробел.

Весьма естественно, что эта монография издается нашей Академией Наук, так как большое число исследований по теории иррациональностей третьей степени принадлежит математикам, так или иначе связанным с нашей Академией: Е. Золотареву, А. Маркову, Г. Вороному, мне, В. А. Тартаковскому, Д. К. Фаддееву, Б. А. Венкову и О. К. Житомирскому. Важнейшие исследования иностранных математиков, сюда относящиеся, принадлежат Эйзенштейну, Туэ, Морделлю, Нагелю, А. Вейлю и Зигелю, а также Дедекинду и Гассе. Исследования этих двух последних математиков мы не включили в монографию, так как они гетерогенны ей по методу и представляют собою скорее применение общей теории поля классов к частному случаю кубического поля.

Можно надеяться, что из соображений, подобных рассмотренным в I и III главах, удастся построить теорию, близкую к теории поля классов, которая даст возможность разрешать многие вопросы, разрешаемые при помощи теории поля классов, без применения аналитической теории чисел.

Мы с Д. К. Фаддеевым являемся равноправными соавторами этой книги, и примерно половина материала, в ней содержащегося, принадлежит Д. К. Фаддееву. Каждый параграф обсуждался обыкновенно сначала совместно, а затем каждый из нас просматривал параграфы, написанные другим. Параграфы 7, 8, 9, 12, 19, 22, 23, 24, 25, 34, 35, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 64, 70, 72, 73, 74, 79, 80, 81, 82 написаны Д. К. Фаддеевым, параграфы 1, 2, 3, 4, 5, 6, 10, 11, 13, 14, 15, 16,

17, 18, 20, 21, 26, 27, 28, 29, 30, 31, 32, 33, 36, 37, 38, 39, 40, 41, 60, 61, 62, 63, 65, 66, 67, 68, 71, 75, 76, 77, 78 написаны мною. За написание § 69 мы очень обязаны проф. В. А. Тартаковскому.

План и замысел книги в основном принадлежит мне, но благодаря неоценимому сотрудничеству Димитрия Константиновича, который отдавал все свое увлечение нашей работе, удалось осуществить значительно более обширный план, чем тот, который мы намечали сначала, когда начинали писать эту книгу совместно с Нагелем. Специально для этой книги мы с Д. К. Фаддеевым произвели многие исследования, которых нехватало среди имевшихся результатов по теории иррациональностей 3-й степени,— сюда относится многое помещенное в I и III главах, а также многое другое.

Перейду к краткому изложению содержания отдельных глав.

Глава I заключает в себе возможно более полное и последовательное геометрическое изложение теории алгебраических иррациональностей любых степеней, рассматриваемой, по моему предложению, как теория решеток в n-мерном комплексном пространстве K_n, повторяющихся умножением. Она является как бы введением ко всей книге. Такие решетки несколько общее, чем алгебраические поля, и связаны с их прямыми суммами, но они нам нужны в главе III для решения задачи, обратной задаче теории Галуа для полей 3-й и 4-й степени. Геометрический характер изложения в главе I принят потому, что он нам необходим в III и особенно в IV главе. В I главе сначала (§ 2) рассматривается предлагаемое мною доказательство теоремы о существовании бесконечного числа независимых неприводимых алгебраических иррациональностей данного измерения и сигнатуры. Идея рассмотреть при вычислении объема $Q^*(r)$ аффинное преобразование с коэффициентами растяжения $r, r^2, \ldots, r^n$ по осям принадлежит студенту МГУ Е. Вегеману. Далее (§ 3) дана геометрия теории Галуа, разрабатываемая мною [19]. [1] § 4 содержит чисто геометрическое изложение теорин единиц Дирихле, а в § 5 помещены исследования Минковского из „Diophantische Approximationen“ геометрии теории идеалов (это единственный параграф предлагаемой геометрической теорин алгебраических чисел, имевшийся до сих пор в литературе). Теорема 1 § 5 принадлежит Д. К. Фаддееву. § 6 посвящен изложению теории n-мерных побочных решеток, предложенных Клейном, являющейся некоторым углублением теории идеалов. Частный случай для $n=2$ рассмотрен Клейном [27] в его известных лекциях по теории чисел, а случай $n=3$ был предметом докторской диссертацин Фуртвенглера [63]. Как теория единиц, так и теория идеалов излагаются в I главе сразу для самой произвольной n-мерной максимальной решетки, хотя бы и приводимой. §§ 7, 8 и 9 содержат теорию различных форм, связанных с решетками в K_n. Мое предложение рассматривать обобщенные безутианы возникло в связи с нашей общей с И. Соминским и К. Биллевичем мыслью при табуляризацни полей 4-й степени [18] (см. § 40) проектировать поле параллельно подполю. Рассматривать решетку, взаимную с данной, и соответственно форму, полярную данной разложимой, предложил Д. К. Фаддеев [60]. Эта форма представляет собою также очень важное алгорифмическое подспорье, в чем можно убедиться в § 64.

Глава I может быть полезна для желающего изучать теорию алгебраических чисел, так как содержит довольно полное и последовательное изложение основных фактов теории.

Глава II заключает в себе элементы теории алгебраических полей 3-й степени. Она изложена, в противовес главе I, чисто алгебраически и может быть читаема независимо от прочтения главы I. В главе II мы даем везде самые удобные вычислительные алгорифмы, которые мы знаем, для фактического вы-

[1] Цифры, помещенные в прямоугольные скобки рядом с именем автора, относятся к списку литературы; если такой скобки нет, то это значит, что указываемое исследование появляется в этой книге впервые.

полнения вычислений, в ней рассматриваемых, и иногда даже сопровождаем их численными примерами. В § 11 я предлагаю одну формулу для непосредственного возвышения кубического числа в любую степень; способ извлечения корня предложен Фаддеевым, он удобен для проверки, основная ли данная единица или нет, а также используется в § 49 для решения задачи, обратной задаче Чирнгаузена, для двух уравнений 4-й степени. В § 13 дано мое [15] решение этой задачи для двух уравнений 3-й степени. § 15 содержит теорию, развитую Ф. Леви [28] и мною [15]. В § 16 изложен мой [15] способ решения задачи эквивалентности для двух кубических двойничных форм без теории приведения. § 17 содержит изложение известного способа Вороного [8] для вычисления базиса кубического поля; способа, бывшего главным результатом его магистерской диссертации, § 18 — алгорифм разложения простого числа на простые идеалы в поле n-го порядка по Золотареву [26] и, в частности, в кубическом поле.

Глава III. В §§ 26—30 и 37—41 дана непосредственная табуляризация решеток, повторяющихся умножением, а следовательно и полей 3-й и 4-й степеней всех сигнатур. Параграфы эти оканчиваются таблицами таких решеток. Табуляризация колец 3-й степени положительного дискриминанта была впервые произведена Арндтом [1—4] в 1852 г., по идее Эйзенштейна [21], как табуляризация классов двойничных кубических форм. Аналогичная табуляризация для отрицательного определителя была произведена Метьюсом (Mathews) и Бервиком [30, 31] и иначе мною [15]. Табуляризация колец 4-й степени с сигнатурой (числом пар комплексных корней) $\tau = 0$ была произведена мной, И. Соминским и К. Биллевичем [18], а для $\tau = 1$ таблица была вычислена Ч. Поплавским. §§ 32—35 содержат геометрию кубических двойничных форм; теория приведения была разработана Метьюсом [30, 31] и мною, рассмотрение кубических двойничных форм как норм принадлежит Фаддееву. Теорема § 36 была доказана Тартаковским еще в 1919 г. в связи с появившимся у нас с ним предположением, возникшим из рассмотрения обширной таблицы дискриминантов кубических единиц, вычисленной в 1918 г. для меня при помощи арифмометров студентами Киевского университета; эта теорема до сих пор осталась нигде не опубликованной.

Относительно классификации кубических областей по квадратичным и областей 4-й степени по кубическим должен сказать следующее. Эйзенштейн в 1841 г. [21] дал любопытную классификацию кубических двойничных форм по их квадратичным ковариантам, которая была затем усовершенствована в работах Арндта [1—4]. На моих семинарах в Ленинградском университете я не раз указывал, что эта теория Эйзенштейна может быть, во-первых, рассматриваема как классификация кубических колец по квадратичным областям, во-вторых, геометризирована и, в-третьих, обобщена на области высших порядков. Б. А. Венков впоследствии [6] переизложил классификацию Эйзенштейна на язык теории алгебраических чисел, а О. К. Житомирский [24] закончил ее геометризацию, а именно, указал как надо выбирать оси в пространстве проекции, и после этого мне удалось уже сообразить, в чем состоит обобщение этой теории на области 4-й степени. Подробно обобщение на области 4-й степени проделал Д. К. Фаддеев [59]. В настоящее время я и Фаддеев [62] строим эту теорию для полей любой степени. Если считать прямою задачею теории Галуа нахождение всех алгебраических свойств заданного поля в зависимости от его группы Галуа, а обратною — нахождение по данной группе всех полей, имеющих ее своей группой Галуа, то излагаемая в §§ 42—53 теория является полным решением обратной задачи теории Галуа для полей 3-й и 4-й степеней. Мы приводим здесь эту теорию (в весьма тщательной и подробной обработке Фаддеева) и для полей 4-й степени, так как их классификация основана на рассмотрении полей 3-й степени, и даже, что весьма любопытно, на рассмотрении общих трехмерных решеток, повторяющихся умножением (т. е. также и приводимых), и их побочных решеток.

Глава IV посвящена алгорифму Вороного для вычисления автоморфизмов умножения полей 3-й степени. Сначала мы думали дать все существующие для этой цели алгорифмы: Золотарева [25], Минковского [33], Шарва (Charve) [67]; Вороного [9], Бервика [5] и Успенского [55], однако затем предпочли изложить только алгорифм Вороиого, как являющийся самым глубоким. Случай $D>0$ обработан Д. К. Фаддеевым, а случай $D<0$ мною (см. также мою заметку [16]). В § 64 даиа (усовершенствованная Д. К. Фаддеевым) переработка алгорифма Вороного для $D<0$, предложенная мною на съезде в Харькове, такая, что приходится вычислять только с целыми рациональными числами. Должеи сказать, что Д. К. исключительно изящно усовершенствовал мои вычисления, заметив, что лучше всего преобразовывать параллельно данную тройничную кубическую разложимую форму и ей полярную. Он же ввел треугольный символ для тройничной кубической разложимой формы.

Глава V содержит изложение теоремы Туэ. Основные мысли изложения, данного в §§ 65, 66, 68, принадлежат В. А. Тартаковскому (см. [17]), ему же принадлежит термин: „заградительный ряд". § 69 и приводимый в ием результат принадлежат В. А. Тартаковскому; этот результат, существенно дополняющий результат Туэ, до сих пор не был опубликован.

В § 70 дан результат Зигеля [46], полученный им из соображеиий, близких к соображению Туэ, в оригинальиой переработке Фаддеева, носящей геометрический и значительно более элементарный характер (не используются гипергеометрические разложения и связанные с ними оценки). Более тщательное проведение оценок позволило дать несколько более сильный результат: 15 решений вместо 18. Этот результат является обобщением моей теоремы § 75 на случай положительного дискриминанта. Надо думать, что граница 18 по Зигелю или 15 по Фаддееву для числа решений — ие точная (моя граница 5 для случая отрицательного дискриминанта — точная).

Глава VI заключает в первой своей части, в §§ 71, 75, 76, мои исследования [11—14] о представлении чисел кубическими двойничными формами отрицательного определителя и (в конце § 75) добавление Нагеля [42] к моей работе [12], а в §§ 72, 73, 74 — продолжения моего исследования [11], даиные Д. К. Фаддеевым [57, 61]; теорема Нагеля [40] содержится в этих исследованиях как частиый случай. Во второй части главы VI помещеио доказательство основной теоремы Морделля, даиное А. Вейлем (André Weil) [7], и исследования Д. К. Фадлеева [58] об уравнении $x^3+y^3=Az^3$.

Термином „поле" мы обозначаем везде конечное алгебраическое расширение поля рациональных чисел. С точки зрения решеток, повторяющихся умножением, рассматриваемых в главе I, поле представляет собою совокупность одноименных координат всех точек некоторой неприводимой решетки, повторяющейся умножением, и этих же координат частных, получающихся от деления ее точек друг на друга. Аналогичную совокупность координат в том случае, если решетка, повторяющаяся умножением, может быть и приводима, мы называем „областью".

Б. Делоне

ЛИТЕРАТУРА

1. Arndt. Versuch einer Theorie der homogenen Functionen des dritten Grades mit zwei Variabeln. Archiv d. Math. und Phys., 17. 1851.
2. — Untersuchungen über die Anzahl der cubischen Klassen, welche zu einer determinierenden quadratischen Klasse gehören. Archiv d. Math. und Phys., 19, 1852.
3. — Tabellarische Berechnung der reducierten binären kubischen Formen und Klassification derselben. Archiv d. Math. und Phys., 31, 1858.
4. — Zur Theorie der binären kubischen Formen. Journ. f. Math., 53, 1857.
5. Berwick. An algorithm for finding units in cubic fields of negative discriminant. Proc. of the London Math. Soc., 1913.
6. Веников. Классификация кубических областей по квадратичным. Труды II Всесоюзного съезда математиков в Ленинграде в 1934 г.
7. Weil A. Sur un théorème de Mordell. Bull. Sci. Math., 2 Ser., t. 54, 1930.
8. Вороной. О целых алгебраических числах, зависящих от корня уравнения 3-ей степени. СПб. 1894.
9. — Об одном обобщении алгорифма непрерывных дробей. Варшава, 1896.
10. Dedekind. Ueber reine cubische Körper. Journ. f. Math., 121, 1900.
11. Делоне. Решение неопределенного уравнения $X^3q + Y^3 = 1$. Изв. Ак. Наук 1922.
12. — О числе представлений числа кубической двойничной формой отрицательного определителя. Изв. Ак. Наук 1922.
13. — Math. Z. Bd. 28 и 31, перевод работ 11 и 12.
14. — Ueber den Algorithmus der Erhöhung. Журн. Леи. М. О. 1927.
15. — Решение задачи эквивалентности и табуляризация кубических двойничных форм отрицательного определителя. Журн. Леи. М. О. 1926.
16. — Interprétation géometrique de la généralisation de l'algorithme des fractions continues donné par Voronoï. C. R. 1923.
17. — О неопределенных уравнениях. Труды Всеросс. съезда мат. в Москве в 1927 г.
18. — Таблица чисто вещественных областей 4-го порядка совместно с И. Соминским и К. Биллевичем. Изв. Ак. Наук 1935.
19. — К геометрии теории Галуа. Юбилейный сборник Граве 1939.
20. Eisenstein. Théorème sur les formes cubiques... Crelle 27, 1844.
21. — Untersuchungen über die cubischen Formen mit zwei Variabeln. Crelle, 27, 1844.
22. — Eigenschaft der Ausdrücke, welche bei der Auflösung cubischer Gleichungen erscheinen. Crelle 27, 1844.
23. — Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken. Crelle, 28, 1844.
24. Житомирский. Sur la classification des formes cubiques. Изв. Ак. Наук, 1935.
25. Золотарев. Об одном неопределенном уравнении 3-й степени. СПб. 1869.
26. — Теория целых комплексных чисел с приложением к интегральному исчислению. СПб. 1874.
27. Klein. Ausgewählte Kapiteln der Zahlentheorie. Литограф. лекц. Göttingen 1896.
28. Levi F. Kubische Zahlkörper und binäre kubische Formenklassen. Berichte der Sächsischen Ges. d. Wiss. Bd. 66, 1914.
29. Марков. Sur les nombres entiers dépendants d'une racine cubique d'un nombre entier ordinaire. Mém. de l'Acad. de St. Petersbourg VII ser. t. 38.
30. Mathews a. Berwick. On the reduction of arithmetical binary cubics which have a negative determinant. Proc. London. Math. Soc. 10, 1912.
31. — On the reduction and classification of binary cubics which have a negative determinant. Proc. London Math. Soc. 10, 1912.
32. Minkowski. Diophantische Approximationen. 1905.
33. — Zur Theorie der Kettenbrüche. Ges. Abh. u. Ann. de l'École Normale supérieure, 3 sér., t. XIII.
34. Mordell. Note on the integer solutions of the équation $Ey^2 = Ax^3 + Bx^2 + Cx + D$. Messenger of Math., vol. 51, 1922.
35. — On the integer solntions of the equation $ey^2 = ax^3 + bx^2 + cx + d$. Proc. London Math. Soc., vol. 21, 1922.

36. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Cambridge Philos. Soc., vol. 21, 1922.
37. — Indeterminate equations of the third degree. Science Progress London, 1923.
38. Nagell. Vollständige Lösung einiger unbestimmten Gleichungen dritten Grades. Skrifter Videnskapsselskapet, Cristiania, 1922.
39. — Ueber die Einheiten in reinen kubischen Zahlkörpern. Ibid. 1923.
40. — Solution complète de quelques équations cubiques à deux indéterminées. Journ. de Math., 9 ser., t. 4, 1925.
41. — Ueber einige kubische Gleichungen mit zwei Unbestimmten. Math. Z. 24, 1925.
42. — Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante. Math. Z. 28, 1928.
43. — Zur Theorie der kubischen Irrationalitäten. Acta Math. 55, 1930.
44. — L'analyse indéterminée de degré supérieur. Mémorial des Sciences Mathématiques, fasc. XXXIX, 1929.
45. Reid. Tafel der Klassenzahlen für kubische Zahlkörper. Diss. Göttingen, 1899.
46. Siegel. Ueber einige Anwendungen diophantischer Approximationen. Abh. der Preuss. Akad. der Wiss. 1929.
47. — Die Gleichung $ax^n - by^n = c$. Math. Ann. 114, 1937.
48. Тартаковский. Решение уравнения $x^4 - \rho y^4 = 1$. Изв. Ак. Наук 1926.
49. Thue. Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen. Cristiania Videnskabsselscabs Skrifter, 1908.
50. — Ueber rationale Annäherungswerte der réellen Wurzeln der ganzen Functionen dritten Grades $x^3 - ax - b$. Ibidem 1908.
51. — Om en general i store wele tal ulösbar ligning. Ibidem 1908.
52. — Ueber Annäherungswerte algebraischer Zahlen. Journ. für Math. 135.
53. — Eine Lösung der Gleichung $P(x) - Q(x) = (x - \rho)^n \cdot Pr(x)$ in ganzen Functionen P, Q und R für jede beliebige ganze Zahl, wenn ρ eine Wurzel einer beliebigen ganzen Function bedeutet. Vidensk. Skrifter, 1909.
54. — Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten alier Wurzeln gewisser ganzen Functionen. Journ. für Math. 138.
55. Успенский. A method of finding unites in cubic orders of a negative discriminant. Trans. Amer. Math. Soc. 33, 1931.
56. Фаддеев. Табуляризация областей и колец Галуа третьего порядка. Труды Физ.-Мат. инст. Ак. Наук СССР, т. V. 1934.
57. — Об уравнении $x^4 - Ay^4 = 1$ (ibidem).
58. — Об уравнении $x^3 + y^3 = Az^3$ (ibidem).
59. — Классификация алгебраических областей четвертого порядка по их кубическим резольвентам. Труды II Всес. съезда мат. в Ленинграде в 1934 г.
60. — Об одном свойстве группы классов идеалов областей третьей степени. Ibidem.
61. — Об одном классе неопределенных уравнений 3-й степени. Ibidem.
62. — Построение алгебраических областей, группой Галуа которых является группа кватернионов. Уч. зап. Л. Г. У. 1937.
63. Furtwängler. Kubische Zahlkörper und Zahlengitter. Diss. Göttingen.
64. Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Math. Z. 31, 1930.
65. Чеботарев. Основы теории Галуа I и II.
66. — Задача, обратная задаче Чирнгаузена. Вестн. чист. и прикл. знан. Одесса 1922.
67. Charve. De la réduction des formes quadratiques ternaires positives et de son application aux irrationnelles du 3-me degré (Ann. Sc. de l'Ecole Norm. Sup., supplément au t. 9 (2 série) 1880.

ОГЛАВЛЕНИЕ

Глава III

ГЕОМЕТРИЯ, ТАБУЛЯРИЗАЦИЯ И КЛАССИФИКАЦИЯ АЛГЕБРАИЧЕСКИХ ПОЛЕЙ 3-й И 4-й СТЕПЕНИ

Глава IV

АЛГОРИФМ ВОРОНОГО

Глава V

ТЕОРЕМА ТУЭ

Глава VI

О НЕОПРЕДЕЛЕННЫХ УРАВНЕНИЯХ 3-Й СТЕПЕНИ С ДВУМЯ НЕИЗВЕСТНЫМИ

ГЛАВА I

ТЕОРИЯ РЕШЕТОК, ПОВТОРЯЮЩИХСЯ УМНОЖЕНИЕМ

§ 1. Решетки в n-мерном комплексном пространстве, повторяющиеся умножением

Мы будем рассматривать n-мерное комплексное пространство K_n, т. е. будем считать точкой систему любых n комплексных чисел $x^{(1)}, x^{(2)}, \ldots, x^{(n)}$, которые будем называть координатами этой точки, причем номера координат мы везде будем обозначать верхними значками в скобочках. Самую же эту точку будем кратко обозначать той же буквой без верхних знаков. Пусть $\omega_1, \omega_2, \ldots, \omega_n$ представляют n точек K_n, комплексно некомпланарных с началом, т. е. определитель из их координат

$$\begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \ldots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \ldots & \omega_n^{(2)} \\ \ldots & \ldots & \ldots & \ldots \\ \omega_1^{(n)} & \omega_2^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix} . \tag{1}$$

не равен нулю. Условимся называть суммой, разностью, произведением и частным двух точек пространства K_n точку, каждая из координат которой есть сумма, разность, произведение или частное соответственных координат обеих рассматриваемых точек. Мы будем называть n-мерной решеткой в K_n, или просто решеткой в K_n, совокупность всех точек вида $u_1\omega_1 + u_2\omega_2 + \ldots + u_n\omega_n$, где $u_1, u_2, \ldots, u_n$ — все возможные системы n целых рациональных чисел, т. е. совокупность всех точек K_n, получающихся сложением и вычитанием из точек $\omega_1, \omega_2, \ldots, \omega_n$. Самую решетку эту мы будем обозначать $[\omega_1, \omega_2, \ldots, \omega_n]$ или $[\omega]$ и называть $\omega_1, \omega_2, \ldots, \omega_n$ ее базисом, или ее основным n-вектором. Бывают, оказывается, *решетки, которые повторяются умножением*, т. е. имеют то свойство, что произведение любых двух точек такой решетки есть опять точка этой же решетки. Целью настоящей главы является построение полной теории таких решеток.

Основными пунктами этой теории будут следующие. В настоящем параграфе мы покажем, что всякая такая решетка может быть дополнена до некоторой максимальной, т. е. такой решетки, которая дальше не может уже быть сгущена при условии сохранения свойства повторяться умножением; затем мы покажем, что всякая максимальная решетка либо сама *неприводима*, либо есть прямая сумма таких неприводимых решеток, каждая из которых уже не может быть дальше упрощена. В § 2 мы покажем, что для всякого числа измерений n и всякой *сигнатуры* τ существует бесконечно много различных неприводимых решеток. В § 3 мы построим теорию Галуа таких решеток. В § 4 рассмотрим теорию *автоморфизмов умножения* для произвольных решеток в K_n, т. е. существуют ли такие точки в K_n и каковы такие точки, после умножения на которые некоторой решетки в K_n решетка эта совмещается сама с собою. В §§ 5 и 6 мы построим теорию идеалов решеток, повторяющихся умножением, которая нам дальше понадобится в главе III в теории классификации полей

3-й и 4-й степени. В §§ 7, 8 и 9 мы рассмотрим разные формы, связанные с такими решетками.[1]

Точку пространства K_n, никакие две из координат которой не равны друг другу и у которой нет координат, равных нулю, мы будем называть точкой общего положения в K_n.

Лемма 1. *Во всякой решетке, построенной на n комплексно некомпланарных векторах K_n, существуют точки общего положения.*

Действительно, рассмотрим точку $\omega = u_1\omega_1 + u_2\omega_2 + \ldots + u_n\omega_n$, построенную из $\omega_1, \omega_2, \ldots, \omega_n$ лексикографически, т. е. так, что целые рациональные коэффициенты $u_1, u_2, \ldots, u_n$ весьма быстро растут, т. е. что всякий следующий коэффициент во много раз больше предыдущего. Рассмотрим, например, i-тую и k-тую координаты этой точки; они имеют вид:

$$\omega^i = u_1\omega_1^{(i)} + u_2\omega_2^{(i)} + \ldots + u_n\omega_n^{(i)}; \qquad \omega^k = u_1\omega_1^{(k)} + u_2\omega_2^{(k)} + \ldots + u_n\omega_n^{(k)}.$$

Предположим, что $\omega_n^{(k)} = \omega_n^{(i)}$; $\omega_{n-1}^{(k)} = \omega_{n-1}^{(i)}$; $\ldots$; $\omega_{l+1}^{(k)} = \omega_{l+1}^{(i)}$; но уже $\omega_l^{(k)} \neq \omega_l^{(i)}$. Все i-тые и k-тые координаты быть равны друг другу у всех n векторов не могут, так как тогда определитель (1) имел бы две одинаковые строки и был бы, против предположения, равен нулю. Мы видим, следовательно, что $\omega^{(k)} \neq \omega^{(i)}$, так как l-тые их слагаемые $u_l\omega_l^{(k)}$ и $u_l\omega_l^{(i)}$ у них не равны, все следующие за этими слагаемые у них равны нулю, а суммы им предшествующих во сколько угодно раз (если u_l достаточно быстро растут) меньше этих l-тых слагаемых. Равняться нулю какая-нибудь координата точки ω, например i-тая, тоже не может, так как, если $\omega_n^{(i)} = 0$, $\omega_{n-1}^{(i)} = 0$ $\ldots$, то будет наконец какая-нибудь $\omega_l^{(i)}$, не равная нулю, так как иначе определитель (1) имел бы строку, сплошь состоящую из нулей и должен был бы равняться нулю; но тогда все слагаемые $\omega^{(i)}$, следующие за $u_l\omega_l^{(i)}$, равны нулю, а сумма всех предыдущих во сколько угодно раз меньше этого l-того слагаемого, и, следовательно, координата $\omega^{(i)}$ не равна нулю.

Лемма 2. *Координаты точки ω решетки, повторяющейся умножением в K_n, суть все корни некоторого уравнения n-ой степени с целыми рациональными коэффициентами и старшим коэффициентом 1. Если ω — точка общего положения, то все уравнения, которым удовлетворяют координаты других точек рассматриваемой решетки, повторяющейся умножением, получаются из уравнения, которому удовлетворяет ω, при помощи рациональных преобразований Чирнгаузена (Tschirnhausen).*

В виду того, что решетка повторяется умножением, мы имеем для любой ее точки ω как общего, так и не общего положения,

$$\begin{aligned}
\omega_1\omega &= a_{11}\omega_1 + a_{12}\omega_2 + \ldots + a_{1n}\omega_n,\\
\omega_2\omega &= a_{21}\omega_1 + a_{22}\omega_2 + \ldots + a_{2n}\omega_n,\\
&\ldots\ldots\ldots\ldots\ldots\\
\omega_n\omega &= a_{n1}\omega_1 + a_{n2}\omega_2 + \ldots + a_{nn}\omega_n,
\end{aligned}$$

с целыми рациональными коэффициентами a_{ik}. (Здесь $\omega_1, \omega_2, \ldots, \omega_n$ суть точки базиса решетки.) Отсюда следует, что

$$F(\omega) = \begin{vmatrix} a_{11} - \omega, & a_{12}, & \ldots & a_{1n} \\ a_{21}, & a_{22} - \omega, & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1}, & a_{n2}, & \ldots & a_{nn} - \omega \end{vmatrix} = 0$$

[1] Перед чтением этой I главы надо просмотреть *приложение* в конце главы I, содержащее необходимые леммы из теории вещественных решеток.

Полином $F(\omega)$ имеет целые рациональные коэффициенты, и старший его коэффициент равен 1. Если ω есть точка общего положения, то все ее n координат различны, и, следовательно, они суть *все* корни уравнения n-ой степени $F(\omega)=0$. Первое утверждение леммы доказано для точек общего положения. Переходим к доказательству второго утверждения.

Пусть ω — точка общего положения. Тогда векторы $1, \omega, \omega^2, \ldots, \omega^{n-1}$ не компланарны, ибо определитель, составленный из их координат, есть определитель Вандермонда для координат точки ω, среди которых нет равных, и потому неравен нулю.

Все эти векторы, кроме вектора 1, принадлежат нашей решетке, вектор же 1 может решетке не принадлежать. Однако он является целой частью некоторого вектора, принадлежащего решетке, например вектора, все координаты которого равны свободному члену a_n уравнения

$$F(\omega)=\omega^n+a_1\omega^{n-1}+\ldots+a_n=0,$$

корнем которого является ω, ибо такой вектор есть линейная комбинация $-(\omega^n+a_1\omega^{n-1}+\ldots+a_{n-1}\omega)$ с целыми коэффициентами векторов $\omega, \omega^2, \ldots, \omega^n$, заведомо принадлежащих решетке. Любой вектор $\tilde{\omega}$ решетки есть, следовательно, некоторая линейная комбинация векторов $1, \omega, \ldots, \omega^{n-1}$ с рациональными коэффициентами, т. е. имеет вид

$$\tilde{\omega}=\varphi(\omega)=b_1\omega^{n-1}+\ldots+b_{n-1}\omega+b_n.$$

Координаты вектора $\tilde{\omega}$ суть, следовательно, корни уравнения $G(\tilde{\omega})=0$, получаемого из уравнения $F(\omega)=0$ преобразованием Чирнгаузена φ с рациональными коэффициентами, причем в с е корни преобразованного уравнения, и только они, образуют координаты точки $\tilde{\omega}$. Если $\tilde{\omega}$ — точка общего положения, то это уравнение не отличается от уравнения $\widetilde{F}(\tilde{\omega})=0$ (составленного для $\tilde{\omega}$ так же, как $F(\omega)$ для ω), так как оба уравнения имеют одинаковые корни. Каждую точку необщего положения можно рассматривать как предел последовательности точек общего положения и поэтому, из соображений непрерывности, уравнения $\widetilde{F}(\tilde{\omega})=0$ и $G(\tilde{\omega})=0$ также совпадают.

Лемма доказана полностью, ибо уравнение $\widetilde{F}(\tilde{\omega})$ имеет целые коэффициенты и старший коэффициент его равен 1.

Введем понятие о *сигнатурном пространстве*. Если уравнение $F(\omega)=0$ имеет σ вещественных корней и 2τ комплексно сопряженных, то и соответственные координаты любой точки $\tilde{\omega}$ рассматриваемой решетки вещественны и комплексно сопряженны. Таким образом, решетки, повторяющиеся в K_n умножением, бывают $\left[\frac{n}{2}\right]+1$ сигнатурных типов: без комплексных координат, с одной парой комплексно сопряженных координат, с двумя парами, и т. д. Все решетки данного сигнатурного типа, или данной сигнатуры, у которых вещественны именно данные координаты и комплексно сопряженны именно данные пары координат точек K_n, лежат в одном и том же „сечении“ пространства K_n, которое характеризуется вещественностью и комплексной сопряженностью соответствующих координат. Это „сечение“ мы будем называть с и г н а т у р н ы м с е ч е н и е м пространства K_n. Если нумерация осей K_n выбрана так, что в рассматриваемом сигнатурном сечении вещественны первые σ координат $\zeta^{(1)}, \zeta^{(2)} \ldots, \zeta^{(\sigma)}$ точки, а комплексно сопряженны соседние пары остальных ее $n-\sigma=2\tau$ координат

$$\xi^{(1)}+i\eta^{(1)}, \quad \xi^{(1)}-i\eta^{(1)}, \quad \xi^{(2)}+i\eta^{(2)}, \quad \xi^{(2)}-i\eta^{(2)},$$
$$\ldots, \quad \xi^{(\tau)}+i\eta^{(\tau)}, \quad \xi^{(\tau)}-i\eta^{(\tau)},$$

то всякой такой точке можно сопоставить в вещественном n-мерном пространстве $R_{n,\tau}$ точку, с вещественными координатами $\zeta^{(1)}$, $\zeta^{(2)}$, ..., $\zeta^{(\sigma)}$, $\xi^{(1)}$, $\eta^{(1)}$, $\xi^{(2)}$, $\eta^{(2)}$, ..., $\xi^{(\tau)}$, $\eta^{(\tau)}$. Вещественное пространство $R_{n,\tau}$, так сопоставленное рассматриваемому сигнатурному сечению пространства K_n, мы будем называть *соответствующим* ему сигнатурным пространством. Переход от сигнатурного сечения к соответствующему ему вещественному сигнатурному пространству $R_{n,\tau}$ состоит собственно в соответственном выборе осей в пространстве K_n. А именно для этого надо оси координат, соответствующие тем σ из координат точек сигнатурного подпространства, которые вещественны, оставить теми же, которые были в K_n, а каждую пару осей K_n, соответствующую комплексно сопряженным координатам $x^{(i)}x^{(k)}$, заменить другой парой так, чтобы эти координаты заменялись на $\frac{x^{(i)}+x^{(k)}}{2}$, $\frac{x^{(i)}-x^{(k)}}{2i}$. Сумма, разность, произведение и частное двух точек одного и того же сигнатурного сечения пространства K_n есть, как легко видеть, опять точка того же сигнатурного сечения. В соответственном вещественном пространстве $R_{n,\tau}$ сложение и вычитание точек производится, очевидно, по тому же правилу, как в K_n, а именно, просто складываются или вычитаются соответственные координаты, т. е. сумме или разности двух точек K_n, лежащих в этом сигнатурном сечении, будет в $R_{n,\tau}$ соответствовать точка, координаты которой в $R_{n,\tau}$ суть просто суммы или разности соответственных координат складываемых точек. Точке же K_n, являющейся произведением двух точек K_n с координатами в $R_{n,\tau}$

$$\zeta_1^{(1)},\ \zeta_1^{(2)},\ \ldots,\ \zeta_1^{(\tau)},\ \xi_1^{(1)},\ \eta_1^{(1)},\ \xi_1^{(2)},\ \eta_1^{(2)},\ \ldots,\ \xi_1^{(\tau)},\ \eta_1^{(\tau)},$$

и

$$\zeta_2^{(1)},\ \zeta_2^{(2)},\ \ldots,\ \zeta_2^{(\tau)},\ \xi_2^{(1)},\ \eta_2^{(1)},\ \zeta_2^{(2)},\ \eta_2^{(2)},\ \ldots,\ \xi_2^{(\tau)},\ \eta_2^{(\tau)} \tag{1}$$

соответствует в $R_{n,\tau}$ точка с координатами

$$\begin{aligned}&\zeta_1^{(1)}\zeta_2^{(1)},\ \zeta_1^{(2)}\zeta_2^{(2)},\ \ldots,\ \zeta_1^{(\sigma)}\zeta_2^{(\sigma)},\ \xi_1^{(1)}\xi_2^{(1)}-\eta_1^{(1)}\eta_2^{(1)},\ \xi_1^{(1)}\eta_2^{(1)}+\xi_2^{(1)}\eta_1^{(1)},\\ &\ldots,\ \xi_1^{(\tau)}\xi_2^{(\tau)}-\eta_1^{(\tau)}\eta_2^{(\tau)},\ \xi_1^{(\tau)}\eta_2^{(\tau)}+\xi_2^{(\tau)}\eta_1^{(\tau)}.\end{aligned} \tag{2}$$

Таким образом, в зависимости от сигнатуры τ способ умножения точек в $R_{n,\tau}$ меняется.

Норма точки пространства K_n — произведение ее комплексных координат $N(\omega)=\omega^{(1)}\cdot\omega^{(2)}\cdot\ldots\cdot\omega^{(n)}$ — есть, вообще говоря, комплексное число; для точки же сигнатурного сечения норма есть число вещественное, и оно выражается через вещественные координаты соответственной точки $R_{n,\tau}$ так:

$$N(\omega)=\zeta^{(1)}\cdot\zeta^{(2)}\ldots\zeta^{(\sigma)}\cdot(\xi^{(1)2}+\eta^{(1)2})\ (\xi^{(2)2}+\eta^{(2)2})\ldots(\xi^{(\tau)2}+\eta^{(\tau)2}). \tag{3}$$

Если n произвольных точек ω_1, ω_2, ..., ω_n в K_n лежат n-мерно с началом координат, т. е. комплексно линейно независимы, то неравный нулю определитель из их координат можно назвать комплексным объемом параллелепипеда, на них построенного, т. е. построенного на векторах, идущих из начала координат к этим точкам. Квадрат этого определителя называется дискриминантом системы точек $\omega_1, \omega_2, \ldots, \omega_n$ пространства K_n и обозначается $D[\omega_1, \omega_2, \ldots, \omega_n]$; это, вообще говоря, некоторое комплексное число. Если точки $\omega_1, \omega_2, \ldots, \omega_n$ лежат в одном и том же сигнатурном сечений, то мы имеем формулу (4) (стр. 17), и следовательно, если векторы, идущие в точки $\omega_1, \omega_2, \ldots, \omega_n$, в K_n комплексно некомпланарны, то и соответствующие им векторы в $R_{n,\tau}$ вещественно некомпланарны, и обратно. В частности система точек в соответствующем $R_{n,\tau}$, соответствующих точкам некоторой n-мерной решетки в K_n, повторяющейся умножением, есть, следовательно, n-мерная вещественная решетка в пространстве $R_{n,\tau}$.

$$\begin{vmatrix} \zeta_1^{(1)}, & \zeta_2^{(1)} & \dots\dots & \zeta_n^{(1)} \\ \zeta_1^{(2)}, & \zeta_2^{(2)} & \dots\dots & \zeta_n^{(2)} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \zeta_1^{(\sigma)}, & \zeta_2^{(\sigma)} & \dots\dots & \zeta_n^{(\sigma)} \\ \xi_1^{(1)}+i\eta_1^{(1)}, & \xi_2^{(1)}+i\eta_2^{(1)} & \dots\dots & \xi_n^{(1)}+i\eta_n^{(1)} \\ \xi_1^{(1)}-i\eta_1^{(1)}, & \xi_2^{(1)}-i\eta_2^{(1)} & \dots\dots & \xi_n^{(1)}-i\eta_n^{(1)} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \xi_1^{(\tau)}+i\eta_1^{(\tau)}, & \xi_2^{(\tau)}+i\eta_n^{(\tau)} & \dots\dots & \xi_n^{(\tau)}+i\eta_n^{(\tau)} \\ \xi_1^{(\tau)}-i\eta_1^{(\tau)}, & \xi_2^{(\tau)}-i\eta_2^{(\tau)} & \dots\dots & \xi_n^{(\tau)}-i\eta_n^{(\tau)} \end{vmatrix} = (2i)^\tau \begin{vmatrix} \zeta_1^{(1)}, & \zeta_n^{(1)} \dots\dots & \zeta_n^{(1)} \\ \zeta_1^{(2)}, & \zeta_2^{(2)} \dots\dots & \zeta_2^{(2)} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \zeta_1^{(\sigma)}, & \zeta_2^{(\sigma)} \dots\dots & \zeta_n^{(\sigma)} \\ \xi_1^{(1)}, & \xi_2^{(1)} \dots\dots & \xi_n^{(1)} \\ \eta_1^{(1)}, & \eta_2^{(1)} \dots\dots & \eta_n^{(1)} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \xi_1^{(\tau)}, & \xi_2^{(\tau)} \dots\dots & \xi_n^{(\tau)} \\ \eta_1^{(\tau)}, & \eta_2^{(\tau)} \dots\dots & \eta_n^{(\tau)} \end{vmatrix} \tag{4}$$

Из формулы (4) мы видим, что дискриминант системы n точек K_n, лежащих в одном и том же сигнатурном пространстве, есть вещественное число, а именно, мы имеем тогда

$$D[\omega_1, \omega_2, \dots, \omega_n] = (-1)^\tau \cdot 4^\tau \cdot V^2, \tag{5}$$

где V обыкновенный объем в вещественном пространстве $R_{n,\tau}$ параллелепипеда, построенного на векторах, идущих к соответственным точкам $R_{n,\tau}$. Если ω_1, $\omega_2, \dots, \omega_n$ точки K_n, принадлежащие одной и той же решетке, повторяющейся в K_n умножением, то дискриминаит

$$D_{(\omega_1, \omega_2, \dots, \omega_n)} = \begin{vmatrix} \omega_1^{(1)}\omega_2^{(1)} \dots \omega_n^{(1)} \\ \omega_1^{(2)}\omega_2^{(2)} \dots \omega_n^{(2)} \\ \dots\dots\dots\dots \\ \dots\dots\dots\dots \\ \omega_1^{(n)}\omega_2^{(n)} \dots \omega_n^{(n)} \end{vmatrix}^2, \tag{6}$$

как целая рациональная целочисленная функция от целых алгебраических чисел, есть целое алгебраическое число. Выражение же это, как легко видеть, есть рациональная симметрическая комбинация от корней того уравнения с целыми рациональными коэффициентами, которому удовлетворяет некоторая точка ω общего положения в рассматриваемой решетке, через которую выражаются рационально (по лемме 2) все точки $\omega_1, \omega_2, \dots, \omega_n$, следовательно, оно есть рациональное число. Таким образом дискриминант системы n некомпланарных с началом точек решетки, повторяющейся умножением, есть отличное от нуля целое рациональное число. Положительное — если τ, соответствующее этой решетке, четное, и отрицательное — если τ нечетное. Причем объем параллелепипеда, построенного на этих векторах, $V = \frac{\sqrt{|D|}}{2^\tau}$. Дискриминант основного параллелепипеда решетки называется дискриминантом решетки.

Лемма 3. *Все точки всех решеток, повторяющихся в K_n умножением данного сигнатурного типа, образуют в соответственном $R_{n,\tau}$ дискретную систему точек $W_{n,\tau}$.* Все точки всех таких решеток имеют координаты в K_n, удовлетворяющие уравнениям n-ой степени с целыми рациональными коэффициентами и старшим коэффициентом, равным 1 (лемма 2). Мы имеем, следовательно, для любой такой точки $x^{(1)} + x^{(2)} + \dots + x^{(n)} = -a_1; \dots; x^{(1)} \cdot x^{(2)} \dots x^{(n)} = \pm a_n$, где $a_1, a_2, \dots a_n$ — целые рациональные, или, если это написать через координаты

$$\zeta^{(1)}, \zeta^{(2)} \dots \zeta^{(\sigma)}, \xi^{(1)}, \eta^{(1)}, \xi^{(2)}, \eta^{(2)} \dots\dots \xi^{(\tau)}, \eta^{(\tau)}$$

этой же точки в $R_{n,\tau}$, мы получаем уравнения:

$$\begin{aligned}
&\zeta^{(1)}+\zeta^{(2)}+\ldots+\zeta^{(\sigma)}+2\xi^{(1)}+2\xi^{(2)}+\ldots+2\xi^{(\tau)}=-a_1,\\
&\zeta^{(1)}\zeta^{(2)}+\zeta^{(1)}\zeta^{(3)}+\ldots+\xi^{(\tau-1)}\xi^{(\tau)}-\eta^{(\tau-1)}\eta^{(\tau)}+\xi^{(\tau-1)}\eta^{(\tau)}+\xi^{(\tau)}\eta^{(\tau-1)}=a_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\qquad(7)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\zeta^{(1)}\cdot\zeta^{(2)}\ldots\zeta^{(\sigma)}\cdot(\xi^{(1)2}+\eta^{(1)2})(\xi^{(2)2}+\eta^{(2)2})\ldots(\xi^{(\tau)2}+\eta^{(\tau)2})=\pm a_n,
\end{aligned}$$

т. е. все эти точки лежат в $R_{n,\tau}$ в точках пересечения дискретных семейств поверхностей (7). Мы будем обозначать эту систему точек в $R_{n,\tau}$ через $W_{n,\tau}$.

Мы будем называть центрировкой решетки в K_n решетку в K_n, состоящую из всех точек центрируемой решетки плюс некоторые дальнейшие точки K_n, которые имеют *вещественные* координаты относительно основного n-векторника центрируемой решетки.

Мы будем называть решетку в K_n, повторяющуюся умножением, максимальной, если никакая ее центрировка уже не повторяется умножением.

Лемма 4. *Во всякой решетке, повторяющейся умножением, есть точка $(a, a, \ldots, a)$, все координаты которой суть одинаковые целые рациональные числа; если решетка максимальна, то в ней есть точка* $(1, 1, \ldots, 1)$. Действительно, пусть ω точка решетки общего положения и $\omega^n+a_1\omega^{n-1}+\ldots+a_{n-1}\omega+a_n=0$ то уравнение с целыми рациональными коэффициентами и старшим коэффициентом 1, которому удовлетворяют координаты этой точки (см. лемму 2). В таком случае точка $-(\omega^n+a_1\omega^{n-1}+\ldots+a_{n-1}\omega)$ имеет все свои координаты, равные a_n. Предположим теперь, что наша решетка максимальна, и пусть ω_0 какая-нибудь ее зафиксированная точка общего положения. Рассмотрим совокупность всех точек K_n, которые получаются, если соединять сложением и вычитанием все точки рассматриваемой решетки и точку $(1,1,\ldots,1)$ сами с собою и друг с другом. Получаемая совокупность $\omega+k$ вся состоит из точек той же сигнатуры, как и точки данной решетки, и если ее рассматривать в соответственном $R_{n,\tau}$, то она состоит из точек соответственной $W_{n,\tau}$. Но совокупность $\omega+k$, очевидно, n-мерна, так как уже совокупность ω n-мерна, и повторяется сложением и вычитанием, т. е. представляет собою в вещественном пространстве $R_{n,\tau}$ n-мерную решетку (см. лемму 1 „Приложения“), а следовательно, и в K_n также представляет n-мерную решетку. Но решетка эта повторяется умножением, так как точка

$$(\omega_1+k_1)(\omega_2+k_2)=\omega_1\omega_2+\omega_1k_2+\omega_2k_1+k_1k_2=\omega+k_1k_2$$

опять вида $\omega+k$. Таким образом, если рассматриваемая решетка максимальна, то она содержит точку $(1, 1, \ldots, 1)$.

Лемма 5. *Всякая решетка, повторяющаяся умножением в K_n, есть подрешетка некоторой и притом только одной максимальной решетки.*

Всякая решетка, повторяющаяся умножением в K_n, а следовательно, и всякая ее подрешетка, принадлежит к одному определенному из возможных $\left[\frac{n}{2}\right]+1$ сигнатурных типов, по числу пар комплексно сопряженных ее координат. Весь вопрос о том, максимальна ли данная решетка, повторяющаяся умножением в K_n, или нет, и каковы те максимальные решетки, в которых она содержится, и содержится ли она вообще в какой-либо максимальной решетке, может быть, следовательно, рассматриваем в соответственном вещественном пространстве $R_{n,\tau}$. Из леммы 3 следует, что всякая решетка, повторяющаяся умножением, лежит в некоторой максимальной решетке, так как если бы можно было без конца ее центрировать, сохраняя ее свойство повторяться умножением, то получились бы точки $R_{n,\tau}$, сколь угодно близкие к началу, а между тем в системе $W_{n,\tau}$ нет точек, отличных от начала внутри некоторого вполне определенного шара, описанного вокруг начала.

Остается доказать, что каждая решетка, повторяющаяся умножением, содержится только в одной максимальной решетке.

Допустим обратное, что некоторая решетка содержится в двух максимальных решетках A_1 и A_2. Обе эти решетки, по лемме 4, содержат точку 1 и базисы их будут рационально выражаться один через другой, ибо базис исходной решетки выражается целым рациональным образом через оба эти базиса. Обозначим через N общий знаменатель в выражении базиса решетки A_2 через базис A_1. Если все точки решетки A_1 поделить на N, то получится, очевидно, новая решетка, которую мы обозначим через $\frac{A_1}{N}$. Решетка A_2 содержится, как подрешетка, в $\frac{A_1}{N}$. Перемножим теперь решетки A_1 и A_2, т. е. перемножим всевозможными способами точки решетки A_1 на точки решетки A_2 и составим все суммы таких результатов умножения. Получим новую точечную совокупность, которую мы обозначим A_1A_2. Эта совокупность, очевидно, повторяется сложением и умножением и содержит решетки A_1 и A_2, ибо каждая из них содержит точку 1. Эта совокупность дискретна, ибо она содержится в результате умножения решетки A_1 на $\frac{A_1}{N}$. Но этот результат равен $\frac{A_1}{N}$, ибо решетка A_1 повторяется умножением, и, следовательно, произведение любой точки из $\frac{A_1}{N}$ на любую точку из A_1 принадлежит $\frac{A_1}{N}$. Итак A_1A_2 есть решетка, повторяющаяся умножением и содержащая в себе обе решетки A_1 и A_2. Следовательно, хотя бы одна из них не максимальна, что противоречит сделанному предположению. Лемма доказана полностью.

Мы будем называть **делителем нуля** всякую точку K_n, отличную от начала, т. е. такую, у которой не равны нулю все координаты одновременно, но среди координат которой есть координаты, равные нулю, так как для такой точки существуют в K_n точки, отличные от начала, такие, что от умножения этой точки на такую точку получается нуль, т. е. начало. Таким дополнительным до нуля множителем будет всякая точка K_n, у которой равны нулю все те координаты, которые у рассматриваемой точки не равны нулю, и не равна нулю хоть одна из координат, которые у рассматриваемой точки равны нулю. Между прочим, надо заметить, что из теоремы, которую мы сейчас докажем, следует, что если некоторая точка максимальной решетки есть делитель нуля, то дополнительные до нуля к ней множители есть и в самой этой решетке.

Решетку, повторяющуюся или не повторяющуюся умножением, не имеющую среди своих точек делителей нуля, мы будем называть **неприводимой** решеткой. Неприводимые максимальные решетки играют большую роль; они являются как бы простейшими решетками, из которых составлены все максимальные решетки. Дело в том, что имеет место следующая основная теорема.

Теорема. *Любая максимальная решетка либо сама неприводима, либо разлагается, и притом только одним способом, в прямую сумму неприводимых максимальных решеток низших измерений, построенных на отдельных комплексах координатных осей.*

Если в рассматриваемой максимальной решетке $[\omega]$ нет делителей нуля, то решетка неприводима.

Предположим теперь, что в рассматриваемой максимальной решетке есть некоторый делитель нуля ϕ, и пусть оси K_n перенумерованы так, что n_1 первых координат под ряд $\phi^{(1)}, \phi^{(2)}, \ldots, \phi^{(n_1)}$ не равны нулю, а $n_2 = n - n_1$ остальных $\phi^{(n_1+1)}, \ldots, \phi^{(n)}$ равны нулю. Пусть K_{n_1} есть n_1-мерное комплексное пространство, построенное на n_1 первых осях K_n, а K_{n_2} — n_2-мерное, построенное на n_2 остальных. Точка ϕ лежит в пространстве K_{n_1}. Координаты точки ϕ, как и всякой точки рассматриваемой максимальной решетки $[\omega]$, суть все корни некоторого уравнения n-ой степени с целыми рациональными коэффициентами и старшим

коэффициентом, равным 1, причем, так как n_2 из этих координат равны нулю, n_2 младших коэффициентов этого уравнения равны нулю, а (n_2+1)-й уже не равен нулю, т. е. n_1 первых координат точки ϕ: $\phi^{(1)},\phi^{(2)},\ldots,\phi^{(n_1)}$, неравные нулю, удовлетворяют уравнению $\phi^{n_1}+a_1\phi^{n_1-1}+\ldots+a_{n_1-1}\phi+a_{n_1}=0$ с целыми рациональными коэффициентами a_i, у которого $a_{n_1}\neq 0$, и, следовательно, точка $\theta=-\phi^{n_1}-a_1\phi^{n_1-1}-\ldots-a_{n_1-1}\phi$, очевидно, принадлежащая рассматриваемой решетке $[\omega]$, имеет координаты $(\overbrace{a,\ a,\ \ldots,a}^{n_1},\overbrace{0,\ 0,\ \ldots,0}^{n_2})$, где $a=a_{n_1}$ — целое рациональное число. Рассмотрим совокупность точек рассматриваемой максимальной решетки $[\omega]$ вида $\theta\cdot\omega$, где ω пробегает все точки этой решетки. Все эти точки лежат в пространстве K_{n_1}, причем все они, очевидно, лежат в одном и том же сигнатурном сечении K_{n_1}, так что их можно рассматривать в некотором одном R_{n_1,τ_1}, и уравнения, которым удовлетворяют координаты их в K_{n_1}, будут, так же как для ϕ, n-го порядка с целыми рациональными коэффициентами и старшим коэффициентом 1. Все эти точки $\theta\cdot\omega$, следовательно, лежат в W_{n_1,τ_1}. Но совокупность $\theta\cdot\omega$, очевидно, повторяется сложением и вычитанием и, следовательно (по лемме 1 „Приложения"), есть решетка в R_{n_1,τ_1}, а следовательно, и решетка в K_{n_1}.

Решетка эта n_1-мерна в K_{n_1}, так как, если точка ω — общего положения в K_n, то $\theta\cdot\omega$ — общего в K_{n_1} положения, и, следовательно, уже векторы $\theta\cdot\omega$, $(\theta\cdot\omega)^2,\ldots,(\theta\cdot\omega)^{n_1}$ лежат в K_{n_1} n_1-мерно, так как определитель из их координат не равен нулю. Обозначим через η точку пространства K_{n_1}, имеющую координаты $\overbrace{1,\ 1,\ \ldots,1}^{n_1},\overbrace{0,\ 0,\ \ldots,0}^{n_2}$. В виду того, что $\theta[\omega]$, как мы сейчас показали, n_1-мерная решетка в K_{n_1}, то очевидно, что и $\eta[\omega]$ — также n_1-мерная решетка точек в K_{n_1}, а именно, решетка $a^{-1}\cdot\theta[\omega]$, где a тут мы рассматриваем как число.

Решетка $\eta[\omega]$ повторяется в K_{n_1}, очевидно, умножением, так как $\eta\omega\cdot\eta\omega=\eta\eta\omega\omega=\eta\omega$. Будем обозначать точку $\eta\omega$ через $\tilde{\omega}$. Точка $\tilde{\omega}$ получается из соответственной точки ω, если оставить первые n_1 координат точки ω без изменения, а остальные n_2 положить равными нулю. Точка $\tilde{\omega}$ есть, следовательно, ортогональная проекция точки ω на координатное подпространство K_{n_1}. Мы получили таким образом, что совокупность ортогональных проекций всех точек ω заданной решетки на подпространство K_{n_1} есть n_1-мерная решетка $[\tilde{\omega}]$ в этом подпространстве. Проекции $\tilde{\omega}$ могут, вообще говоря, уже не быть точками решетки $[\omega]$. Покажем, однако, что если решетка $[\omega]$ максимальна, то эти проекции $\tilde{\omega}$ суть также ее точки. Действительно, рассмотрим совокупность всех сумм и разностей точек ω и $\tilde{\omega}$ самих с собою и друг с другом. Эта совокупность будет, очевидно, также решеткой в K_n, потому что, как все точки ω, так и все точки $\tilde{\omega}$ можно рассматривать лежащими в $R_{n,\tau}$, и они во всяком случае содержатся все в решетке $\left[\frac{\omega}{a}\right]$ (тут a в знаменателе надо рассматривать как число). Обозначим эту решетку $[\omega]^*$. Решетка эта повторяется умножением, так как

$$(\omega_1+\tilde{\omega}_2)(\omega_3+\tilde{\omega}_4)=\omega_1\omega_3+\omega_1\tilde{\omega}_4+\omega_3\tilde{\omega}_2+\tilde{\omega}_2\tilde{\omega}_4,$$
$$=\omega_1\omega_3+\tilde{\omega}_1\tilde{\omega}_4+\tilde{\omega}_3\tilde{\omega}_2+\tilde{\omega}_2\tilde{\omega}_4,$$

а решетки $[\omega]$ и $[\tilde{\omega}]$ повторяются умножением. Если, следовательно, $[\omega]$ максимальна, то она содержит $[\tilde{\omega}]$.

Будем обозначать через $\tilde{\tilde{\omega}}$ разность $\omega-\tilde{\omega}$, где ω любая точка решетки $[\omega]$, а $\tilde{\omega}$ ее ортогональная проекция на пространство K_{n_1}. Все точки $\tilde{\tilde{\omega}}$, очевидно, лежат в подпространстве K_{n_2} в одном и том же сигнатурном сечении, т. е. их можно рассматривать в соответственном вещественном пространстве R_{n_2,τ_2}. Но совокупность $\tilde{\tilde{\omega}}$ очевидно повторяется сложением и вычитанием и, следовательно, есть подрешетка решетки $[\omega]$, а именно n_2-мерная решетка, лежащая в K_n и состо-

ящая из всех тех точек $[\omega]$, у которых первые n_1 координат равны нулю. Очевидно, что всякая точка $[\omega]$ имеет вид $\tilde{\omega}_1 + \tilde{\omega}_2$, и обратно, т. е. что сама решетка $[\omega]$ есть прямая сумма $[\tilde{\omega}] \oplus [\tilde{\omega}]$ решеток $[\tilde{\omega}]$ и $[\tilde{\omega}]$, лежащих в пространствах K_{n_1} и K_n и повторяющихся в них умножением. Решетки эти максимальны в пространствах K_{n_1} и K_{n_2}, так как если бы одну из них, например $[\tilde{\omega}]$, можно было бы так центрировать, чтобы центрировка ее $[\tilde{\omega}]^*$ тоже повторялась в K_{n_1} умножением, то решетка $[\tilde{\omega}]^* \oplus [\tilde{\omega}]$ в K_n тоже повторялась бы умножением, так как $(\tilde{\omega}_1^* + \tilde{\omega})(\tilde{\omega}_3^* + \tilde{\omega}_4) = \tilde{\omega}_1^*\tilde{\omega}_3^* + \tilde{\omega}_1^*\tilde{\omega}_4 + \tilde{\omega}_2\tilde{\omega}_3^* + \tilde{\omega}_2\tilde{\omega}_4 = \tilde{\omega}_1^*\tilde{\omega}_3^* + \tilde{\omega}_{\ 2}\tilde{\omega}_4$, так как оба средние слагаемые равны нулю, а решетки $[\tilde{\omega}]^*$ и $[\tilde{\omega}]$ повторяются умножением, и, следовательно, $[\omega]$ не была бы максимальной.

Продолжая так же разлагать решетки $[\tilde{\omega}]$ и $[\tilde{\omega}]$, если они имеют в своих пространствах K_{n_1} и K_{n_2} делителей нуля, мы приходим к доказываемой теореме.

Это разложение в прямую сумму неприводимых решеток единственно, так как если бы было одно разложение, пространства неприводимых частей которого были бы $K_{n_1}K_{n_2}\ldots K_{n_k}$, то у любой точки $[\omega]$ все координаты, соответствующие каждому из этих пространств, либо одновременно не равны нулю (это будет, если в эту точку из соответственной неприводимой части входит слагаемое, отличное от начала), либо одновременно равны нулю (что будет, если в эту точку из рассматриваемой неприводимой части входит слагаемое нуль), так как точка неприводимой части, отличная от начала, не имеет ни одной координаты, равной нулю. Предположим, что было бы другое разложение на неприводимые части $K_{n_1}, K_{n_2} \ldots K_{n_l}$. Возьмем какую-нибудь точку, принадлежащую, например, i-той из этих неприводимых частей, и пусть одна из ее координат принадлежит j-той неприводимой части первого разложения; тогда все координаты j-той неприводимой части первого разложения у этой точки не равны нулю, т. е. они суть координаты рассматриваемой i-той неприводимой части второго разложения. Таким образом, если две неприводимые части обоих разложений имеют одну общую координату, то и все их координаты общие, т. е. сами разложения совпадают. Таким образом теорема доказана. Для немаксимальной решетки теорема может быть неверна.

Лемма 6. *Всякая точка ω, координаты которой суть корни уравнения n-й степени с целыми рациональными коэффициентами и старшим коэффициентом 1, принадлежит некоторой максимальной решетке.* Действительно, если уравнение неприводимо, то решетка $[1, \omega, \omega^2, \ldots, \omega^{n-1}]$ повторяется умножением; если приводимо, то прямая сумма таких решеток для неприводимых его множителей повторяется умножением.

§ 2. О существовании бесконечного числа различных неприводимых максимальных решеток любого данного измерения $n > 1$ и данной сигнатуры τ

Начнем с вывода одной важной асимптотической формулы.

В силу леммы 3, все точки всех решеток, повторяющихся в K_n умножением, данной сигнатуры τ образуют в соответственном $R_{n,\tau}$ дискретную (не решетку) систему точек $W_{n,\tau}$. Опишем в пространстве $R_{n,\tau}$ шар радиуса r с центром в начале и дадим асимптотическую формулу для числа $N_{r,n,\tau}$ точек $W_{n,\tau}$, лежащих внутри такого шара в зависимости от его радиуса r. А именно, мы докажем лемму.

Лемма. *Число $N_{r,n,\tau}$ выражается асимптотической формулой* $\nu_{n,\tau} \cdot r^{\frac{n(n+1)}{2}}$, где $\nu_{n,\tau}$ — *некоторая константа, зависящая только от n и τ, т. е.*

$$\lim_{r\to\infty} \frac{N_{r,n,\tau}}{\nu_{n,\tau} \cdot r^{\frac{n(n+1)}{2}}} = 1.$$

Действительно, будем называть пространство $R_{n,\tau}$ пространством корней алгебраических уравнений n-ой степени и сигнатуры τ; рассмотрим кроме того n-мерное вещественное пространство A_n коэффициентов всех алгебраических уравнений n-ой степени с вещественными коэффициентами и старшим коэффициентом, равным 1, т. е. такое пространство, в котором каждой точке сопоставляется такое уравнение, имеющее своими коэффициентами координаты этой точки, и обратно. Совокупность всех целочисленных (т. е. коэффициенты которых — целые рациональные числа и старшие коэффициенты которых равны единице) уравнений n-ой степени образует в пространстве A_n коэффициентов n-мерную решетку всех точек с целыми рациональными координатами, т. е. решетку, основной параллелепипед которой есть куб с ребром 1. Только часть этой решетки даёт уравнения данной сигнатуры τ. Будем называть в пространстве A_n областью сигнатуры τ ту область его, ограниченную известными неравеиствами Борхарда, в которой лежат точки, дающие уравнения данной сигнатуры, и будем обозначать эту область через $A^*_{n,\tau}$. Каждой точке пространства A_n соответствует одно уравнение n-ой степени, и, наоборот, каждому уравнению n-ой степени соответствует одна точка пространства A_n. Каждой точке пространства $R_{n,\tau}$ соответствует одно уравнение n-ой степени сигнатуры τ, но одному такому уравнению соответствует не одна, а $\sigma!\tau!2^\tau$ точек пространства $R_{n,\tau}$, так как, если условиться на осях $\zeta^{(1)}, \zeta^{(2)} \ldots \zeta^{(\tau)}$ откладывать вещественные корни, а на осях $\xi^{(1)}, \eta^{(1)}, \ldots, \xi^{(\tau)}, \eta^{(\tau)}$ откладывать соответственно вещественные части и коэффициенты при i в парах комплексно сопряженных корней $\xi + i\eta$, $\xi - i\eta$, то можно на осях ζ $\sigma!$ способами отложить σ вещественных корней, парам осей ξ, η $\tau!$ способами сопоставить пары комплексно сопряженных корней, и еще в каждой паре комплексно сопряженных корней выбирать тот или иной знак для η. Рассмотрим в пространстве $R_{n,\tau}$ основную область $R^*_{n,\tau}$ такую, что каждому уравнению n-ой степени сигнатуры τ соответствует в этой области уже одна и только одна точка. Для этого можно, например, условиться откладывать на оси $\zeta^{(1)}$ наибольший по численной величине корень, на $\zeta^{(2)}$ — следующий по численной величине, и т. д., аналогично сопоставлять $\xi^{(1)}$, $\eta^{(1)}$ комплексно сопряженную пару с наибольшим по численной величине $\xi^{(1)}$ и т. д. и, наконец, все η брать положительные. Очевидно, что формулы Виета

$$\left.\begin{aligned} -a_1 &= \rho^{(1)} + \rho^{(2)} + \ldots + \rho^{(n)}, \\ a_2 &= \rho^{(1)}\cdot\rho^{(2)} + \rho^{(1)}\cdot\rho^{(3)} + \ldots + \rho^{(n-1)}\cdot\rho^{(n)}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ \pm a_n &= \rho^{(1)}\cdot\rho^{(2)} \ldots \rho^{(n)}, \end{aligned}\right\}$$

где $\rho^{(1)}$ $\rho^{(2)} \ldots \rho^{(n)}$ — корни, преобразуют область $R^*_{n,\tau}$ пространства $R_{n,\tau}$ взаимно однозначно в области $A^*_{n,\tau}$ пространства A_n, кроме точек границ этих областей, которые, однако, для нас в дальнейшем не имеют существенного значения.

Рассмотрим в пространстве $R_{n,\tau}$ шар с радиусом 1 и центром в начале координат и назовем $P^*(1)$ тело, образующее общую часть этого шара и области $R^*_{n,\tau}$, и пусть оно преобразуется преобразованием Виета в некоторое тело $Q^*(1)$ пространства A_n. Обозначим через $v_{n,\tau}$ объем тела $Q^*(1)$. Увеличим радиус шара, описанного из начала в пространстве $R_{n,\tau}$, в r раз и обозначим через $P^*(r)$ тело, являющееся общей частью этого шара радиуса r и области $R^*_{n,\tau}$. В виду того, что область $R^*_{n,\tau}$, как легко видеть, есть конус с вершиной в начале, тело $P^*(r)$ получается из тела $P^*(1)$ гомотетией по отношению к началу с коэффициентом r. Но такую гомотетию можно рассматривать так же как совокупность равномерных растяжений по всем n осям $R_{n,\tau}$ с одним и тем же коэффициентом r для каждой оси. В силу вида преобразования Виета, таким

растяжениям по осям $R_{n,\tau}$ с одним и тем же коэффициентом r соответствуют растяжения по n осям A_n с коэффициентами r, r^2, r^3, ..., r^n, поэтому объем тела $Q^*(r)$, получаемого из $P^*(r)$ преобразованием Виета, равен $v_{n,\tau} r \cdot r^2 \ldots r^n = v_{n,\tau} r^{\frac{n(n+1)}{2}}$. При увеличении радиуса r число точек пространства A_n, соответствующих целочисленным уравнениям, лежащих в теле $Q^*(r)$, асимптотически равно объему этого тела, так как совокупность всех точек A_n, соответствующих целочисленным уравнениям, представляет собою просто решетку, основной параллелепипед которой есть куб с ребром 1.

Остаточный член этого асимптотического равенства не превосходит площади поверхности тела $Q^*(r)$ с некоторым множителем, не зависящим от r. Площадь поверхности тела $Q^*(r)$, в свою очередь, не превосходит площади поверхности тела $Q^*(1)$, умноженной на $r^{2+3+\cdots+n} = r^{\frac{n(n+1)}{2}-1}$. Действительно, если мы через dP обозначим дифференциал площади поверхности тела $Q^*(1)$, через dP_1, dP_2, ..., dP_n — его ортогональные проекции на плоскости координат и введем аналогичные обозначения dQ, dQ_1, ..., dQ_n для тела $Q^*(r)$, то будем иметь:

$$dP = \sqrt{dP_1^2 + \ldots + dP_n^2},$$

$$dQ = \sqrt{dQ_1^2 + \ldots + dQ_n^2}.$$

Очевидно, далее, что

$$|dQ_i| = \left|\frac{r r^2 \ldots r^n}{r^i} dP_i\right| \leqslant \frac{1}{r} \cdot r^{\frac{n(n+1)}{2}} dP_i,$$

откуда следует, что

$$dQ < r^{\frac{n(n+1)}{2}-1} \cdot dP,$$

и, следовательно,

$$Q < r^{\frac{n(n+1)}{2}-1} \cdot P.$$

Итак, остаточный член асимптотического равенства имеет порядок $r^{\frac{n(n+1)}{2}-1}$, т. е. во всяком случае порядок остаточного члена меньше порядка главного члена. Но число точек A_n внутри $Q^*(r)$ — то же самое, что и число всех точек, соответствующих целочисленным уравнениям, т. е. точек сетки $W_{n,\tau}$, лежащих в теле $P^*(r)$ пространства $R_{n,\tau}$, и, следовательно, это последнее число асимптотически равно $v_{n,\tau} r^{\frac{n(n+1)}{2}}$.

Но легко видеть, что число точек $W_{n,\tau}$ в шаре r просто в $\sigma!\,\tau!\,2^\tau$ раз больше, чем в теле $P^*(r)$, и, следовательно, если мы обозначим $v_{n,\tau}\sigma!\,\tau!\,2^\tau = \nu_{n,\tau}$, то число точек $W_{n,\tau}$ в шаре r асимптотически равно $\nu_{n,\tau} r^{\frac{n(n+1)}{2}}$, что и требовалось доказать.

Выведенная асимптотическая формула показывает, что система точек $W_{n,\tau}$ как бы сгущается при удалении от начала в том смысле, что число точек этой системы, лежащих в шаре, описанном из начала, растет не как объем шара, т. е. не пропорционально r^n, а скорее, именно пропорционально $r^{\frac{n(n+1)}{2}}$, и, следовательно, „густота“ точек $W_{n,\tau}$ в шаре, т. е. отношение этого числа к объему шара, не постоянна, а растет как $r^{\frac{n(n-1)}{2}}$.

Используя выведенную асимптотическую формулу, легко доказать следующую основную теорему теории решеток, повторяющихся умножением.

Теорема 1. *Существует бесконечно много различных неприводимых максимальных решеток любого данного числа измерений n и данной сигнатуры τ.*

Для доказательства рассмотрим систему $W_{n,\tau}$ и покажем, что если из нее выключить все точки, которые принадлежат хоть одной из приводимых максимальных решеток, входящих в ее состав, то останется система $W^*_{n,\tau}$, которая, так же как и система $W_{n,\tau}$, бесконечно сгущается с удалением от начала в том смысле, что число ее точек в шаре радиуса r с центром в начале растет скорее, чем объем этого шара. Если это будет показано, то дальше рассуждение следующее. Возьмем некоторую точку ω_1 из системы $W^*_{n,\tau}$; она (лемма 6) принадлежит некоторой максимальной решетке, входящей в $W_{n,\tau}$. Если отбросить в $W^*_{n,\tau}$ все точки, принадлежащие этой неприводимой максимальной решетке, то останется система точек $W^{*'}_{n,\tau}$, которая также бесконечно сгущается с удалением от начала, так как решетка не сгущается, а везде одинаково густа. Пусть ω_2 — какая-нибудь точка этой системы; тогда она принадлежит некоторой второй неприводимой максимальной решетке, входящей в $W_{n,\tau}$ и уже отличающейся от сейчас рассмотренной. Если отбросить в $W^*_{n,\tau}$ все точки, принадлежащие либо первой, либо второй из этих двух неприводимых решеток, то останется система $W^{*''}_{n,\tau}$, которая также бесконечно сгущается с удалением от начала, и т. д. Так получается бесконечно много различных неприводимых максимальных решеток, заключающихся в $W_{n,\tau}$, причем таким процессом они получаются все.

Остается, таким образом, показать, что система $W^*_{n,\tau}$ бесконечно сгущается при удалении от начала, и в этом все дело. Рассмотрим все те приводимые максимальные решетки, заключающиеся в $W_{n,\tau}$, которые имеют разбиение по данным двум координатным подпространствам K_{n_1} и K_{n_2}, прямая сумма которых равна K_n (т. е. $n_1+n_2=n$), причем нам безразлично, неприводимы или приводимы составные части такой решетки, лежащие в K_{n_1} и K_{n_2}. Все эти решетки входят в прямую сумму $W_{n_1,\tau_1}\bigoplus W_{n_2,\tau_2}$ систем W, лежащих в K_{n_1} и K_{n_2} и являющихся совокупностями точек системы $W_{n,\tau}$, лежащими в K_{n_1} и K_{n_2}. Число точек W_{n_1,τ_1}, лежащих в n_1-мерном шаре радиуса r (имеющем центр в начале и получающемся в сечении n-мерного шара в $R_{n,\tau}$ радиуса r, имеющего центр в начале, n_1-мерною плоскостью $R_{n,\tau}$, в которой лежит система W_{n_1,τ_1}), равно $N_{rn_1\tau_1}\approx\nu_{n_1\tau_1}r^{\frac{n_1(n_1+1)}{2}}$. Число же точек системы W_{n_2,τ_2}, лежащей в n_2-мерном шаре радиуса r, имеющем центр в начале и получающемся в сечении n-мерного шара n_2-мерною плоскостью R_{n,τ_2}, в которой лежит система $W_{n_2\tau_2}$, равно $N_{rn_2\tau_2}\approx\nu_{n_2\tau_2}r^{\frac{n_2(n_2+1)}{2}}$. „Произведение этих двух друг другу ортогональных шаров, n_1-мерного и n_2-мерного, радиусов r образует некоторое тело, заключающее в себе рассматриваемый n-мерный шар радиуса r (тут под „произведением“ понимается совокупность точек, являющихся концами сумм всех возможных векторов, проведенных из начала ко всевозможным точкам „умножаемых“ шаров). Число точек прямой суммы $W_{n_1\tau_1}\bigoplus W_{n_2\tau_2}$ в этом „произведении“ равно $N_{rn_1\tau_1}\cdot N_{rn_2\tau_2}\approx\nu_{n_1\tau_1}\nu_{n_2\tau_2}r^{\frac{n_1(n_1+1)+n_2(n_2+1)}{2}}$, и следовательно, если выбросить из n-мерного шара r все те точки $W_{n,\tau}$, которые входят в неприводимые максимальные решетки, отвечающие разложению $K_n=K_{n_1}\bigoplus K_{n_2}$, надо из $N_{rn,\tau}$ вычесть число меньшее, чем $N_{rn_1\tau_1}\cdot N_{rn_2\tau_2}$. Всех возможных представлений K_n в виде прямой суммы двух дополнительных координатных подпространств K_{n_1} и K_{n_2} — ограниченное число, причем тут придется брать только такие разбиения, которые совместимы с рассматриваемым сигнатурным сечением, так как координаты, соответствующие комплексно сопряженным корням, разъединять нельзя. Если мы вычтем из $N_{rn\tau}$ произведения $N_{rn_1\tau_1}\cdot N_{rn_2\tau_2}$, соответствующие всем этим разложениям, то разность будет даже меньше, чем число точек $W_{n,\tau}$, заключающихся в n-мерном шаре r, не принадлежащих никакой приводимой максимальной решетке, входящей в $W_{n,\tau}$. Посмотрим, какова эта разность.

Заметим, что если $n_1 + n_2 = n$, то

$$n_1(n_1+1) + n_2(n_2+1) < n(n+1);$$

действительно,

$$n_1^2 + n_1 + n_2^2 + n_2 < (n_1+n_2)(n_1+n_2+1) = n_1^2 + n_1 + n_2^2 + n_2 + 2n_1n_2$$

на $2n_1n_2$.

Рассматриваемая разность, следовательно, имеет вид

$$ar^{\frac{n(n+1)}{2}} - b_1r^{m_1} - b_2r^{m_2} - \ldots b_kr^{m_k},$$

где число k вычитаемых ограничено, коэффициенты $a, b_1, \ldots, b_k$ постоянны, и все показатели $m_1, m_2, \ldots$ меньше, чем $\frac{n(n+1)}{2}$ по крайней мере на $2(n-1)$, так как, если n_1 и n_2 — целые положительные числа и $n_1 + n_2 = n$, то n_1n_2 не меньше, чем $n-1$. Отношение этого числа к объему n-мерного шара $\Gamma_n r^n$, следовательно, при увеличении r бесконечно возрастает, т. е. система $W^*_{n,\tau}$ сгущается с удалением от начала, что и требовалось доказать.

Докажем дополнительную к теореме 1 теорему 2, принадлежащую Эрмиту.

Теорема 2. *Число решеток, повторяющихся умножением, объемы v основных параллелепипедов которых по абсолютной величине меньше заданной величины, ограничено.*

Так как всякая решетка, повторяющаяся умножением, есть подрешетка некоторой максимальной решетки, повторяющейся умножением, то достаточно доказать эту теорему только для максимальных решеток. Но всякая максимальная решетка есть прямая сумма неприводимых решеток, причем дискриминант ее, очевидно, равен произведению дискриминантов этих неприводимых решеток, так как за основной n-векторник рассматриваемой решетки можно взять n-векторник, составленный из совокупности n_1 векторов n_1-векторника первого слагаемого, n_2 векторов n_2-векторника второго слагаемого и т. д.; пространства же $K_{n_1}, K_{n_2}, \ldots, K_{n_k}$ взаимно ортогональны. Достаточно, следовательно, доказать теорему только для неприводимых решеток, повторяющихся умножением, данного сигнатурного типа. Рассмотрим параллелепипед, имеющий одну из вершин в точке пространства $R_{n,\tau}$, $n-1$ первых координат (в $R_{n,\tau}$), $y^{(1)}, y^{(2)}, \ldots, y^{(n-1)}$ которой положительны и меньше $\frac{1}{\sqrt{2}}$, а n-ая $y^{(n)}$ положительна и столь велика, что произведение $y^{(1)} \cdot y^{(2)} \ldots y^{(n-1)} \cdot y^{(n)}$ больше, чем заданная величина L, и такой, что грани его параллельны координатным плоскостям в $R_{n,\tau}$, а центр находится в начале. Тогда параллелепипед этот есть выпуклое тело с центром в начале, объем которого более чем в 2^n раз превосходит объем основного параллелепипеда любой решетки в $R_{n,\tau}$, имеющей одну из точек в начале и объем основного параллелепипеда которой не больше L. Всякая такая решетка, по лемме „Приложения“ к гл. I, имеет, следовательно, кроме начала, еще по крайней мере две точки (симметричные относительно начала) внутри этого параллелепипеда. Всякая неприводимая решетка, повторяющаяся умножением в K_n рассматриваемого типа, объем основного параллелепипеда которой не больше L, имеет, следовательно, по крайней мере одну точку, отличную от начала, лежащую в этом параллелепипеде. Но так как для этой точки произведение $\zeta^{(1)}\zeta^{(2)} \ldots \zeta^{(\sigma)} \cdot (\xi^{(1)^2} + \eta^{(1)^2}) \ldots (\xi^{(\tau)^2} + \eta^{(\tau)^2}) = \pm a_n$ есть целое рациональное число, отличающееся от нуля, т. е. больше или равно единице по абсолютной величине, то n-ая координата в $R_{n,\tau}$ уже наверно больше $\frac{1}{\sqrt{2}}$, и точка эта в K_n имеет все координаты по абсолютной величине меньшие 1 и одну (или две комплексно сопряженные, если n-я координата есть мнимая часть комплексной координаты) бо́льшую 1, т. е. точка эта — общего положения в K_n, так как координаты всякой точки неприводимой решетки распадаются на ν комплексов по δ

(где $\delta > 1$) одинаковых координат (где $n = \nu \cdot \delta$), что будет доказано в следующем параграфе. Но все точки всех решеток, повторяющихся в K_n умножением, рассматриваемого типа суть точки системы $W_{n,\tau}$, лежащей в соответственном $R_{n,\tau}$; система же эта дискретна и имеет, следовательно, лишь ограниченное число точек в рассматриваемом параллелепипеде. Если же две решетки, повторяющиеся умножением, имеют общую точку ω общего положения, то они имеют и общую n-мерную подрешетку, например построенную на векторах $\omega, \omega^2, \ldots, \omega^n$. Но всех вообще различных центрировок такой решетки, составленных из точек дискретной системы $W_{n,\tau}$, — ограниченное число.

§ 3. Геометрия теории Галуа

1. Максимальные подрешетки максимальной решетки

Разобьем все n осей K_n на ν комплексов, не имеющих между собою общих осей, так чтобы в каждом из этих комплексов было по одному и тому же числу δ осей, и приравняем для каждого из этих комплексов между собою координаты, соответствующие осям, заключающимся в этом комплексе. Так получается система уравнений, определяющая линейное ν-мерное подпространство пространства K_n, которое мы будем называть **ν-мерной биссектрисой** пространства K_n, или, скорее, выбранной системы осей пространства K_n. Если n — простое число, K_n имеет только одну одномерную биссектрису $x^{(1)} = x^{(2)} = \ldots = x^{(n)}$; если же n — не простое, то есть биссектрисы, измерения ν которых — любые делители n, причем если ν — делитель n, то биссектрис такого измерения ν столько, сколькими разными способами можно разбить n координат на ν комплексов по δ координат. Если для такого разбиения полагать координаты каждого одного из таких комплексов равными между собою, а координаты всех остальных комплексов этого разбиения равными нулю, то получится ν одномерных прямых в K_n, которые, как легко видеть, ортогональны друг другу. Мы будем называть эти прямые **осями** соответственной биссектрисы.

Если подрешетка O_1 измерения ν (низшего чем n) n-мерной максимальной решетки O в K_n *повторяется в K_n умножением* и не может быть так центрирована, чтобы центрировка [она будет, по самому определению центрировки (см. стр. 18), также ν-того измерения] также повторялась в K_n умножением, то O_1 называется **максимальной подрешеткой**.

Теорема 1. *Измерение ν максимальной подрешетки O_1 неприводимой максимальной n-мерной решетки O может быть только делителем n, причем такая максимальная подрешетка есть ν-мерная совокупность всех точек решетки O, лежащих в некоторой ν-мерной биссектрисе, и наоборот, если решетка O имеет ν-мерную совокупность точек, лежащую в некоторой ν-мерной биссектрисе, то совокупность эта есть ее ν-мерная максимальная подрешетка. Такая максимальная подрешетка, — если ее рассматривать в пространстве биссектрисы и принять за оси в нем оси биссектрисы, а за масштабную единицу на осях $\sqrt{\delta}$, где $\nu \cdot \delta = n$, — есть ν-мерная максимальная решетка в этих осях.*

Рассмотрим любую точку ω неприводимой максимальной решетки; координаты $\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)}$ этой точки суть корни уравнения n-ой степени $f(x) = 0$ с целыми рациональными коэффициентами и старшим коэффициентом, равным 1. Покажем, что это уравнение либо неприводимо, либо является степенью неприводимого уравнения. Т. е. что любая точка неприводимой решетки является или точкой общего положения или точкой некоторой биссектрисы. Действительно, если $f(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_k(x)$, где $g_1(x), g_2(x), \ldots, g_k(x)$ неприводимы, и $g_1(x)$ — неприводимый множитель наинизшей степени (если степени этих множителей не одинаковы), то рассмотрим точку $\theta = g_1(\omega)$, т. е. точку с координатами $g_1(\omega^{(1)}), g_1(\omega^{(2)}), \ldots, g_1(\omega^{(k)})$. Тогда координаты θ, соответствующие тем $\omega^{(i)}$, которые суть корни $g_1(x)$, равны нулю, а так как

решетка предположена неприводимой (не имеющей делителей нуля), то эта точка 0 есть начало координат, т. е. и все остальные координаты ее равны нулю; другими словами, корни всех остальных неприводимых множителей $g_2(x), \ldots, g_k(x)$ суть корни $g_1(x)$. Но неприводимое уравнение не имеет кратных корней, и следовательно, во-первых, степени всех g совпадают со степенью ν первого множителя g_1 и, во-вторых, и сами g совпадают с g_1.

Пусть теперь O_1 — некоторая подрешетка решетки O. O_1 не может иметь точки общего в K_n положения, т. е. все n координат которой были бы различны, так как тогда (см. стр. 15) O_1 была бы, против предположения, n-мерна. Все точки O_1 суть, следовательно, точки некоторых биссектрис.

Пусть ω_1 — некоторая точка подрешетки O_1, имеющая наинизшие кратности δ своих координат в K_n; в силу сказанного $\delta_1 \neq 1$.

Рассмотрим любую другую точку ω_2 решетки O_1; у этой точки должны быть равны друг другу те координаты, которые равны друг другу у ω_1, так как иначе у точки $q \cdot \omega_1 + \omega_2$, где q — очень большое целое рациональное число, было бы еще больше неравных друг другу координат, чем у ω_1, так как координаты того комплекса, в котором они равны у ω_1, но не равны у ω_2, стали бы не равны, а координаты разных комплексов ω_1 остались бы не равны, так как их разности по абсолютной величине были бы больше любой разности координат ω_2.

Итак, все точки подрешетки O_1 лежат в биссектрисе, определенной точкой ω_1. Если биссектриса это ν-мерна, то степени точки ω_1, как легко видеть, лежат в ней ν-мерно. Рассмотрим совокупность всех точек n-мерной максимальной решетки O, которые лежат в этой биссектрисе; эта совокупность представляет собою, как легко видеть, переходя в сигнатурное пространство O, ν-мерную подрешетку решетки O. Эта ν-мерная подрешетка, очевидно, повторяется умножением, так как, с одной стороны, произведение любых двух ее точек есть опять точка решетки O и, с другой стороны, произведение любых двух точек некоторой биссектрисы, очевидно, лежит в этой же биссектрисе. Если O_1 максимальна, то она, следовательно, совпадает с этой решеткой. Последнее утверждение теоремы следует из того, что в осях биссектрисы, если на них взять за масштабную единицу $\sqrt{\delta}$, решетка O будет неприводимою ν-мерною максимальною решеткою, повторяющейся в этих осях умножением, (т. е. совокупностью всех целых точек некоторого алгебраического поля ν-того порядка).

2. Нормальные решетки

Мы будем называть осеподстановкой K_n всякое ортогональное преобразование 1-го или 2-го рода пространства K_n, оставляющее начало на месте, при котором совмещается с собою совокупность положительных координатных полуосей K_n. Осеподстановку, после которой решетка O совмещается с собою, мы будем называть осеподстановкой этой решетки в себя. Легко видеть, что у неприводимой n-мерной решетки не может быть больше, чем n осеподстановок в себя. Действительно, пусть $\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)}$ — координаты какой-нибудь точки этой решетки общего положения; тогда координаты тех точек, в которые эта точка перейдет осеподстановками, те же числа, но в другом порядке. Никакие две различные осеподстановки не могут привести эту точку в одно и то же место, так как точка эта — общего положения и, следовательно, не имеет одинаковых координат, а различные подстановки по крайней мере две оси переставляют на разные места. Если бы осеподстановок, преобразующих данную решетку в себя, было больше чем n, то было бы две различных точки в этой решетке, которые имели бы одинаковые, например 1-ые, координаты, но тогда разность этих точек, будучи отлична от начала, имела бы 1-ую координату равную нулю, т. е. была бы делителем нуля, и решетка не могла бы быть неприводимой. Неприводимую максимальную решетку, которая имеет ровно n осеподстановок в себя, мы будем называть нормальной.

Теорема 2. *Всякая неприводимая максимальная n-мерная решетка Ω, повторяющаяся в K_n умножением, есть либо нормальная решетка, либо максимальная подрешетка низшего измерения некоторой нормальной m-мерной решетки, где m — целое, кратное n.*

Для доказательства построим сначала некоторую вспомогательную $n!$-мерную решетку Ω следующим образом. Напишем рядом колонки номеров $1, 2, \ldots, n$ координат точек Ω во всех возможных $n!$ расположениях и рассмотрим получающуюся прямоугольную матрицу этих номеров:

$$\left.\begin{array}{cccccc} 1 & 1 & \cdots & \cdots & \cdots & n \\ 2 & 2 & \cdots & \cdots & \cdots & n-1 \\ \cdot & \cdot & \cdots & \cdots & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdots & \cdots & \cdot \\ n-1 & n & \cdots & \cdots & \cdots & 2 \\ n & n-1 & \cdots & \cdots & \cdots & 1 \end{array}\right\} \quad (*)$$

Каждая из ее строчек будет характеризовать свою n-мерную биссекториальную плоскость пространства $K_{n!}$. Эта матрица (*) задает, таким образом, n вполне определенных n-мерных биссекториальных плоскостей в $K_{n!}$. Рассмотрим в $K_{n!}$ точки, координаты которых будут соответствовать строчкам матрицы (*), выписаниым по порядку для всех точек Ω. Так, получатся в рассматриваемых n биссекториальных плоскостях $K_{n!}$ решетки $\Omega_1, \Omega_2, \ldots, \Omega_n$, подобные решетке Ω, но в $\sqrt{\frac{n!}{n}}$ раз большие ее. Рассмотрим совокупность Ω^* всех точек $K_{n!}$, которые получаются, если всеми возможными способами соединять при помощи сложения, вычитания и умножения все точки всех этих n решеток. Если $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ — координаты в K_n какой-нибудь точки Ω общего в K_n положения, то любая точка Ω^* имеет своей первою координатой $\Phi(\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)})$, где Φ — некоторая целая рациональная фуикция от $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ (может быть, и с дробными коэффициентами, так как координаты некоторых точек Ω могут выражаться через соответственные координаты θ цело, рационально, с дробными коэффициентами), второю координатою — ту же функцию Φ, но от 2-го расположения $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}, \theta^{(n-1)}$, и т. д. Координаты любой точки Ω^* суть, следовательно, в силу теоремы о симметрических функциях, корни уравнения $F(x) = 0$ степени $n!$ со старшим коэффициентом 1 и рациональными коэффициентами. Но так как корни эти получаются сложением, вычитанием и умножением целых алгебраических чисел, коэффициенты F — целые, рациональные. Координаты $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ распадаются на пары комплексно сопряженных и, следовательно, независимо от выбора Φ, все $n!$ Φ будут также распадаться на пары комплексно сопряженных, причем комплексно сопряженными будут те Φ, которые получаются друг из друга перестановкой координат θ^i во всех комплексно сопряженных парах. Все точки Ω^* лежат, следовательно, в соответственном $W_{n!,\tau}$, т. е. система точек Ω^* дискретна. Но, например, точка $V = A_1\theta_1 + A_2\theta_2 + \ldots + A_n\theta_n$, где $\theta_1, \theta_2, \ldots, \theta_n$ обозначают те точки, где окажется точка θ решетки во вставленных решетках $\Omega_1, \Omega_2, \ldots, \Omega_n$, с целыми рациональными и лексикографически выбранными A_i, есть точка общего в $K_{n!}$ положения, так как различные ее координаты в $K_{n!}$ получатся из $A_1\theta^{(1)} + A_2\theta^{(2)} + \ldots + A_n\theta^{(n)}$, если здесь сделать все $n!$ перестановок $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$, и, следовательно система Ω^* $n!$-мерна. В силу самого образования системы Ω^*, она повторяется сложением и вычитанием, т. е. является $n!$-мерной решеткой, повторяющейся умножением в $K_{n!}$.

Обозначим через Ω максимальную для Ω^* в $K_{n!}$ решетку, если бы сама Ω^* была не максимальна. Решетка Ω^* имеет $n!$ осеподстановок $K_{n!}$, совмещающих ее с собою, а именно те $n!$ осеподстановок $K_{n!}$, которые соответствуют $n!$ перестановкам колонн матрицы (*), вызываемым всеми $n!$ перестановками ее строчек, так как каждая из этих $n!$ осеподстановок $K_{n!}$ только переставляет

между собою решетки $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_n$, при помощи которых построена Ω^*. Очевидно, что эти $n!$ осеподстановок $K_{n!}$ будут совмещать и Ω самое с собою.

Пусть теперь $\Omega_1, \Omega_2, \ldots, \Omega_k$ — неприводимые части прямой, суммой которых является максимальная решетка Ω, и $K_{m_1}, K_{m_2}, \ldots, K_{m_k}$ — координатные пространства, в которых они лежат; покажем, что все неприводимые части не только одного измерения, но даже просто одинаковы. Для этого возьмем какую-нибудь из рассмотренных осеподстановок s решетки Ω в себя, которая совмещает какую-нибудь координату K_{m_1} с какой-нибудь координатой некоторой другой K_{m_i}; среди $n!$ наших осеподстановок такая осеподстановка будет, так как есть осеподстановка, которая любую координату ставит на любое из $n!$ мест [иначе существовали бы две разные осеподстановки, которые одну и ту же координату ставят на одно и то же место, что противоречит самому образованию этих осеподстановок перестановками строчек матрицы (*)]. В любой точке ω решетки Ω либо участвует какой-нибудь вектор, отличный от нуля неприводимой части Ω_l, и тогда все координаты этой точки, соответствующие K_{m_i}, не равны нулю, так как в Ω_l только точка 0 имеет координаты в K_{m_i}, равные нулю, либо в точке ω не участвует вектор неприводимой части Ω_i, и тогда все координаты, соответствующие K_{m_i}, равны нулю.

Предположим, что $m_1 \leqslant m_2 \leqslant \ldots \leqslant m_k$; тогда подстановка s дает из точки Ω_l какую-то точку Ω, одна из координат которой есть координата K_{m_1} и которая имеет $m_1 \leqslant m_l \neq 0$ координат, но это, в силу выше сказанного о точках $\mathfrak{Q}$, возможно только, если $m_l = m_1$ и если все координаты точки Ω_1 после осеподстановки s превращаются в координаты K_{m_i}. Кроме того, мы видим, что Ω_1 после этой осеподстановки просто совмещается с Ω_l, так как Ω_l есть совокупность всех точек Ω, лежащих в K_{m_i}. Мы видим, таким образом, что все Ω_i — одного измерения m и одинаковы. Это рассуждение также показывает, что Ω_1 имеет m осеподстановок в себя, так как если координаты K_{m_1} суть $1, 2, \ldots, m_1$, то всякой из рассмотренных $n!$ осеподстановок Ω в себя, которая переставляет 1-ую координату на 2-е, 3-е, $\ldots, m_1$-ое места, Ω_1, в силу сказанного выше, будет совмещаться сама с собой. Таким образом, всякая из неприводимых частей Ω нормальна. Наконец, не трудно видеть, что $\mathfrak{Q}$ „вставлено“ в любое Ω_l.

Действительно, пусть θ_1, точка $\mathfrak{Q}_1$ в $\mathfrak{Q}$, — общего положения. Точка θ_1, как всякая точка Ω, имеет вид $\theta_{11} + \theta_{12} + \ldots + \theta_{1k}$, где θ_{1l} — точки в соответственных неприводимых частях: пусть θ_{1l} не есть начало координат, тогда в Ω_i есть точка θ_{1l}, причем θ_{1l} имеет все различные координаты точки θ_1, так как если бы ее координатами были только часть различных координат точки θ_1, то θ_1 не могла бы быть точкой общего положения в неприводимой $\mathfrak{Q}$, — что и требовалось доказать.

Группу G всех m осеподстановок Ω в себя мы будем называть группой Галуа неприводимой максимальной решетки Ω, а также группой Галуа неприводимой максимальной решетки $\mathfrak{Q}$. Нормальную решетку Ω мы будем называть нормой решетки $\mathfrak{Q}$. В случае, когда максимальная решетка $\mathfrak{Q}$ не неприводима, все предыдущие рассуждения повторяются, и только нельзя утверждать, что сама решетка $\mathfrak{Q}$ будет максимальной подрешеткой нормальной неприводимой решетки Ω, а можно лишь доказать, что каждая из ее неприводимых частей будет такой подрешеткой. В этом случае, когда максимальная решетка $\mathfrak{Q}$ не неприводима, мы будем также называть ее группой Галуа группу G всех m осеподстановок в себя неприводимой нормальной решетки Ω, составленной при помощи $\mathfrak{Q}$, как это выше было сделано, когда $\mathfrak{Q}$ предполагалась неприводимой; самую же эту решетку Ω мы опять будем называть нормой решетки $\mathfrak{Q}$. В случае, когда $\mathfrak{Q}$ неприводима, число измерений m решетки Ω есть кратное $m = n \cdot d$ от числа измерений решетки $\mathfrak{Q}$, так как решетка $\mathfrak{Q}$ является в этом случае подрешеткой низшего измерения решетки Ω, повторяющейся умножением, т. е.

имеет число измерений, равное числу измерений некоторой биссектрисы K_m; если же Ω приводима, то m может быть и не кратным n, и даже меньше n.

3. Подгруппы группы G и максимальные подрешетки решетки Ω

Пусть H — некоторая подгруппа группы G порядка δ, так что $m = \mu\delta$, где μ — целое. Рассмотрим, в какие оси переходит 1-ая ось K_m при помощи всех подстановок H. В виду того, что группа перестановок осей $1, 2, \ldots, m$ пространства K_m правильная, это будут различные δ осей $1, 2, \ldots, \delta$. Ось 2-ая при помощи подстановок H, следовательно, переходит тоже лишь в эти же 1-ую, 2-ую, ... и т. д. до δ-ой оси. Таким образом, эти оси переходят при помощи подстановок H только друг в друга. Аналогично получим, если исходить от $\delta + 1$ оси в δ расположениях номеров осей K_m, соответствующих H, квадрат со стороной δ, составленной из номеров δ следующих осей K_m, переводимых подгруппой H только друг в друга, и т. д.

$$G\left\{\begin{array}{l} H\left\{\begin{array}{|c|c|c|c|}\hline 1, 2, 3 \ldots \delta & \delta+1 \ldots 2\delta & \ldots & (\mu-1)\delta+1 \ldots m \\ 2, \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ 3, \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ \ldots & \ldots\ldots & \ldots & \ldots\ldots \\ \delta, \ldots\ldots & \ldots & \ldots & \ldots \\ \hline \end{array}\right. \\ \delta+1 \\ \ldots \\ m \end{array}\right.$$

Очевидно, что совокупность всех подстановок подгруппы H оставляет на месте те и только те точки пространства K_m, которые соответствуют μ-мерной биссекториальной плоскости K_m, которая получается, если приравнять между собою координаты в отдельных квадратах подгруппы H.

Теорема 3. *Всякой подгруппе H группы G соответствует μ-мерная максимальная подрешетка решетки Ω, и наоборот.*

Действительно, если мы возьмем любую точку Ω, сделаем над ней все δ осеподстановок H и сложим все δ получившихся точек, то получится точка Ω, лежащая в биссекториальной плоскости, соответствующей подгруппе H. Если мы это сделаем для всякой точки Ω, то получим μ-мерную решетку в этой биссекториальной плоскостн, так как можно взять такие точки Ω, чтобы суммы координат в отдельных комплексах были все различны и не равны нулю, т. е. чтобы получилась точка общего в соответственной биссектрисе положения.

Итак, всякой подгруппе H соответствует подрешетка, а следовательно, и максимальная подрешетка решетки Ω, повторяющаяся умножением, лежащая в биссектрисе соответствующей H и имеющая то же измерение, что и эта биссектриса. Измерение этой подрешетки равно индексу подгруппы H по отношенню к группе G.

Предположим теперь, что, наоборот, в нормальной решетке Ω есть μ-мерная подрешетка $\mathfrak{Q}$, повторяющаяся умножением, и пусть α — точка общего в ней положения. Пусть H—подгруппа всех подстановок G, оставляющих α на месте. Число подстановок в H не больше, чем δ, так как, например, 1-ая координата точки α может занимать после этих перестановок не более чем δ мест, тех, на которых координаты α равны ее 1-ой координате, а в G нет различных подстановок, которые оставляют некоторую координату на месте. С другой стороны, число подстановок в H и не меньше, чем δ, так как иначе при

переставлении α всеми G мы получили бы больше, чем μ различиых точек и, например, 1-ые координаты этих точек должны были бы иметь больше, чем μ различных значений, чего быть не может, так как у α лишь μ различных координат. Всякая подстановка H, таким образом, лишь переставляет координаты внутри комплексов, координаты которых равны между собою. Подрешетка Ω, следовательно, принадлежит подгруппе H в вышеуказанном смысле, — чем и доказана теорема.

Посмотрим, что такое точки, которые суть делители нуля в решетке $\mathbf{\Omega}$? Это суть целые рациональные соотношения между корнями, написаиные в форме $\Phi(x^{(1)}, x^{(2)}, \ldots, x^{(n)}) = 0$, в каковой можно написать любое рациональное соотиошение между корнями. Если в $\mathbf{\Omega}$ нет делителей нуля, т. е. нет рациональных соотношений между корнями, нарушаемых хотя бы одною из $n!$ подстановок, то Ω — неприводимая решетка, и группа Галуа решетки Ω — симметрическая.

§ 4. Автоморфизмы умножения (единицы) решеток в K_n

Если мы помножим все точки некоторой решетки в K_n на одну и ту же совершенно произвольную зафиксированиую точку ω из K_n, которая ие есть делитель нуля, то очевидно, что сумме или разности двух точек исходной решетки будет соответствовать сумма или разность соответственных точек (т. е. точек, получаемых от умножения этих точек иа ω) умиоженной решетки, и комплексный объем (т. е. численная величина определителя из координат в K_n) точек, получившихся из каких-нибудь n основных точек исходной решетки умножением их на ω, будет равен соответственному комплексному объему для исходной решетки, помноженному иа норму точки ω. Отсюда выходит, что после умножения n-мерной решетки из K_n на некоторую точку из K_n, которая не есть делитель нуля, получается опять n-мерная решетка в K_n.

Всякая точка ε в K_n, после умножения на которую некоторая решетка в K_n преобразуется сама в себя, есть точка K_n, дающая *автоморфизм умножения* этой решетки. Мы будем такую точку иазывать единицей рассматриваемой решетки, так как всякая такая точка играет такую же роль для данной решетки, какую играют для иее точки $(1, 1, \ldots, 1)$ и $(-1, -1, \ldots, -1)$, умиожение на каждую из которых (на вторую вследствие симметрии всякой решетки в K_n отиосительно точки 0), очевидно, дает автоморфизм умиожения для любой решетки в K_n. Очевидно, что любой автоморфизм умножения любой решетки в K_n не есть делитель нуля и имеет иорму ± 1. Последнее следует из того, что комплексные объемы всех основных параллелепипедов одной и той же решетки в K_n отличаются множителями, равными переходным определителям от одного параллелепипеда к другому, а определители эти равны ± 1; между тем мы видели, что при умножении на точку комплексный объем параллелепипеда умножается иа иорму этой точки.

В этом параграфе мы покажем, что всякая решетка, повторяющаяся умножением, а также всякая решетка, рационально связанная с такой решеткой (хотя бы и ие повторяющаяся умножением), вообще говоря, имеет бесконечно много автоморфизмов умножения, отличных от 1 и -1, и что, наоборот, если решетка в K_n имеет такие автоморфизмы умножения общего положения, то она есть либо решетка, повторяющаяся умиожением, либо подрешетка некоторой решетки, повторяющейся умножением, либо же получается из такой решетки умножением на какую-нибудь точку K_n. При этом оказывается, что если решетка не максимальная, то ее автоморфизмы умножения могут ей и не принадлежать.

Теорема 1. *Если* $[\omega_1, \omega_2, \ldots, \omega_n]$ — *неприводимая максимальная решетка, и притом не первого измерения и не двухмерная комплексная* (т. е. число $\sigma + \tau - 1 > 0$), *то она имеет бесконечно много автоморфизмов умножения* ε, *которые все суть ее собственные точки и выражаются*

формулой $\varepsilon = E_l \cdot \varepsilon_1^{m_1} \cdot \varepsilon_2^{m_2} \cdot \ldots \cdot \varepsilon_{\sigma+\tau-1}^{m_{\sigma+\tau-1}}$, где $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\sigma+\tau-1}$ — *некоторые, так называемые, основные автоморфизмы умножения нашей решетки,* $m_1, m_2, \ldots, m_{\sigma+\tau-1}$ — *все возможные целые рациональные показатели, а* E_l — *некоторые специальные автоморфизмы умножения нашей решетки, в конечном числе являющиеся корнями из единицы.*

Пусть M — некоторая точка в соответствующем нашей решетке $R_{n,\tau}$. Координаты точки M в $R_{n,\tau}$ суть $\zeta', \zeta'' \ldots \zeta^{(\sigma)}, \xi', \eta', \xi'', \eta'' \ldots\ldots \xi^{(\tau)}, \eta^{(\tau)}$. Назовем положительные числа $|\zeta'|, |\zeta''| \ldots |\zeta^{(\sigma)}|, \rho' = |\xi'^2 + \eta'^2|, \rho'' = |\xi''^2 + \eta''^2|, \ldots, \rho^{(\tau)} = |\xi^{(\tau)2} + \eta^{(\tau)2}|$ параметрами точки M. Совокупность всех точек $R_{n,\tau}$, параметры которых не больше, чем соответственные параметры точки M, образует, в силу того, что векторная сумма выпуклых тел есть выпуклое тело, выпуклое тело в $R_{n,\tau}$ с центром в начале координат. Мы будем его называть норменным телом точки M. Для $\sigma = 3$, $\tau = 0$, например, это будет в соответственном $R_{3,0}$ прямоугольный параллелепипед, имеющий одну из своих вершин в точке M, имеющий центр в начале и грани которого параллельны координатным плоскостям. Для $\sigma = 3$, $\tau = 1$ это будет прямой круговой цилиндр с центром в начале, ось которого идет по оси ζ' и на окружности одного из оснований которого лежит точка M.

Мы будем называть точку решетки M относительным минимумом в решетке, если она отличается от точки 0 и внутри ее норменного тела нет других точек этой решетки, кроме точки 0 в его центре. Точка $1 = (1, 1, \ldots, 1)$ решетки $[\omega_1, \omega_2, \ldots, \omega_n]$ есть ее относительный минимум, так как норма всякой точки этой решетки есть целое рациональное число, а норма точки, лежащей внутри норменного тела точки 1, очевидно, меньше 1 по абсолютной величине. Норма же равна нулю только у точки 0, так как решетка $[\omega_1, \omega_2, \ldots, \omega_n]$, как неприводимая, не имеет делителей нуля.

Покажем, что в решетке $[\omega_1, \omega_2, \ldots, \omega_n]$ существует бесконечный ряд относительных минимумов, у которых один из параметров, например k-тый, по абсолютной величине бесконечно возрастает с номером минимума, а остальные все убывают с номером минимума. Такую совокупность мы будем называть цепочкой относительных минимумов, идущей по увеличению k-того параметра. Покажем, что для любого номера $k = 1, 2, \ldots, \sigma + \tau$ параметра имеется такая бесконечная цепочка. Точка 1 — относительный минимум, все параметры ее равны 1. Не будем изменять всех параметров норменного тела точки 1, кроме k-того, который начнем увеличивать. При этом объем тела будет расти, и, следовательно, по лемме 3 приложения (лемма Минковского), когда объем этот перерастет 2^n раз взятый объем в $R_{n,\tau}$ основного параллелепипеда рассматриваемой решетки, внутри этого тела будут лежать по крайней мере две точки решетки, симметричные друг другу относительно начала координат. Пусть φ_1 — одна из точек первой пары таких точек, на которую, при описанном увеличении k-того параметра норменного тела, тело это наткнется своей поверхностью, и которая из таких пар имеет наименьшую норму или точка одной из таких пар с наименьшей нормой, если их несколько. В виду того, что наша решетка не имеет делителей нуля, объем норменного тела точки φ_1 не равен нулю, так как произведение ее параметров не равно нулю. k-тый параметр этой точки φ_1 больше 1 по абсолютной величине, а остальные меньше 1, так как, если, не меняя этих остальных параметров, сколь угодно мало увеличим k-тый параметр, то точка φ_1 уже оказывается внутри получающегося таким образом норменного тела. Точка φ_1 есть также относительный минимум, так как, если бы была точка решетки внутри ее норменного тела, то все ее параметры были бы по абсолютной величине меньше, чем параметры φ_1, т. е. все параметры ее были бы меньше, чем параметры точки 1, а k-тый меньше, чем k-тый параметр точки φ_1, и тогда φ_1 не была бы первой точкой решетки, на которую наткнулось бы рассматривавшееся нами увеличивавшееся нормеиное тело. Более того, точка φ_1 даже первая точка, смежная с точкой 1 в цепочке, исходящей от точки 1 в сто-

рону возрастания k-того параметра или одна из первых, если таких несколько, т. е. первый от 1 в сторону возрастания этого k-того параметра относительный минимум, который имеет остальные параметры, по абсолютной величине меньшие, чем соответственные параметры точки 1.

В виду потребованиой минимальности нормы точки φ_1, на поверхности ее нормеиного тела могут лежать только точки с такой же нормой, но тогда и их параметры равиы соответственным параметрам точки φ_1, так как, если бы хоть один был меньше, то эта точка имела бы меньшую норму, чем φ_1. Закрепим теперь все параметры норменного тела точки φ_1, кроме k-того, который будем увеличивать в силу сказаиного сейчас, при этом не сразу войдет точка решетки в увеличивающееся норменное тело. Пусть φ_2 — первая точка решетки, на которую наткнется это увеличивающееся тело. Аналогичио предыдущему мы убедимся, что φ_2 — первый относительный мииимум, смежный с φ_1 в сторону увеличения k-того параметра; и т. д. В виду возможности иа каждом теле иескольких подходящих φ, вопрос об однозначности такого построения цепочки остается открытым.

Легко видеть, что объем иорменного тела иекоторой точки равен $\pm 2^{\sigma}\cdot\pi^{\tau}$ раз взятой норме этой точки. В виду того, что в силу упомяиутой леммы Мииковского объем пустого внутри выпуклого тела с центром в точке решетки не больше, чем 2^n раз взятый объем основного параллелепипеда этой решетки, иормы всех относительных минимумов данной решетки по абсолютной величине ограничены. Будем помножать нашу решетку $[\omega_1, \omega_2, \ldots, \omega_n]$ последовательно на относительные мииимумы $\varphi_1, \varphi_2, \varphi_3, \ldots$; тогда, в силу того, что решетка эта повторяется умножением, будут получаться некоторые ее подрешетки, индексы которых ограничены. Но всех различных таких подрешеток (см. „Приложение“), ограниченное число, и следовательно, в виду того, что относительных минимумов бескоиечно много, будет содержаться среди них сколь угодно много таких, от умножения на которые нашей решетки $[\omega_1, \omega_2, \ldots, \omega_n]$ будет получаться все одна и та же подрешетка $[\psi_1, \psi_2, \ldots, \psi_n]$. Пусть, например, $\varphi_\lambda\cdot[\omega_1, \omega_2, \ldots, \omega_n]=[\psi_1, \psi_2, \ldots, \psi_n]$ и $\varphi_\mu\cdot[\omega_1, \omega_2, \ldots, \omega_n]=[\psi_1, \psi_2, \ldots, \psi_n]$; тогда $\frac{1}{\varphi_\mu}[\psi_1, \varphi_2, \ldots, \psi_n]=[\omega_1, \omega_2, \ldots, \omega_n]$, и следовательно $\frac{\varphi_\lambda}{\varphi_\mu}[\omega_1, \omega_2, \ldots, \omega_n]=[\omega_1, \omega_2, \ldots, \omega_n]$.

Таким образом, точка $\varepsilon=\frac{\varphi_\lambda}{\varphi_\mu}$ есть автоморфизм умножения нашей решетки. Но в нашей решетке, как в максимальной, есть точка 1, и следовательно $1\cdot\varepsilon$ есть точка нашей решетки, т. е. сама точка ε есть точка нашей решетки. Если φ_λ — минимум, следуюший за φ_μ в рассматриваемой k-цепочке, то, в виду того, что параметры произведения или частного двух точек суть соответственно произведения и частные соответственных параметров умножаемых или делимых друг на друга точек, ε имеет k-тый параметр, по абсолютной величине больший едииицы, а остальные — по абсолютной величиие меньшие едииицы. Степеии $\varepsilon, \varepsilon^2, \varepsilon^3 \ldots$ дают, следовательно, всё новые и новые автоморфизмы, так как k-тые параметры этих степеней, с возрастанием показателя, по абсолютной величиие возрастают, а остальные убывают.

Таким образом доказано существование бесконечного числа различных автоморфизмов умножения для всякой неприводимой максимальной решетки, у которой $\sigma+\tau-1>0$, так как в этом случае число параметров норменного тела точки больше 1. Если бы число этих параметров равнялось 1, что будет, если $n=1$, или если $n=2$ и $\sigma=1$, т. е. координаты — комплексно сопряженные, то нельзя было бы увеличивать норменное тело точки 1, не вводя внутрь его самой этой точки. Когда число параметров больше 1, это можно было сделать потому, что все параметры, кроме одного, мы оставляли постоянными, и следовательно при этом точка 1 не становилась внутренней точкой увеличенного норменного тела, а оказывалась лежащей иа его поверхиости.

Всякий автоморфизм умножения (т. е. единица) нашей решетки $[\omega_1, \omega_2, \ldots, \omega_n]$ есть ее точка с нормой ± 1, так как при умножении на эту точку не меняется объем основного параллелепипеда этой решетки, ибо она при этом обращается сама в себя. Наоборот, всякая точка решетки $[\omega_1, \omega_2, \ldots, \omega_n]$, имеющая норму ± 1, есть ее автоморфизм умножения (единица), так как от умножения ее на эту точку, в виду того, что она повторяется умножением, мы получаем ее подрешетку, но, в виду того, что норма этой точки есть ± 1, индекс этой подрешетки равен 1, и, стало быть, это — вся решетка $[\omega_1, \omega_2, \ldots, \omega_n]$. Мы, следовательно, доказали, что в максимальной неприводимой решетке, если $\sigma + \tau - 1 > 0$, есть бесконечно много точек с нормой ± 1.

Перейдем теперь ко второй части теоремы, а именно, к вопросу об основных автоморфизмах умножения, через которые выражаются все остальные.

Заметим, во-первых, что две различные точки решетки $[\omega_1, \omega_2, \ldots, \omega_n]$ могут тем не менее иногда иметь одни и те же параметры. Дело в том, что у двух различных точек решетки $[\omega_1, \omega_2, \ldots, \omega_n]$, в силу неприводимости решетки, т. е. отсутствия делителей нуля, не могут быть одинаковы два из первых σ параметров, т. е. две из координат, так как тогда у разности этих точек одна из координат была бы равна нулю, без того, чтобы сама эта разность была началом координат; но два из последних τ параметров, т. е. два (и даже хотя бы все) из параметров ρ, могут быть одинаковыми у двух различных точек.

Таким образом, мы видим, что если $\sigma = 0$, т. е. $n = 2\tau$, то в $[\omega_1, \omega_2, \ldots, \omega_n]$ могут существовать различные точки, имеющие тождественные наборы параметров $\rho', \rho'', \ldots, \rho^{(\tau)}$. Примеры показывают, что это и бывает иногда. Посмотрим, в каком случае при $\sigma = 0$ два автоморфизма умножения нашей решетки имеют одинаковые наборы параметров. Пусть, например, параметры автоморфизмов ε_1 и ε_2 одинаковы, т. е. $\rho_1' = \rho_2'$, $\rho_1'' = \rho_2''$, $\ldots$, $\rho_1^{(\tau)} = \rho_2^{(\tau)}$. Рассмотрим точку $E = \frac{\varepsilon_1}{\varepsilon_2}$; она есть, очевидно, также автоморфизм умножения нашей решетки. Все ее параметры равны 1. Таких точек E, все параметры которых равны 1, если они в нашей решетке и есть, то во всяком случае в ограниченном числе, так как в $R_{n,\tau}$ они лежат на шаре $\xi'^2 + \eta'^2 + \xi''^2 + \eta''^2 + \ldots + \xi^{(\tau)2} + \eta^{(\tau)2} = \tau$. Произведение таких двух точек $E_1 \cdot E_2$ есть опять такая же точка E_3, и, следовательно, в частности любая степень E^m такой точки с целым положительным показателем m есть опять такая же точка. Отсюда следует, в виду конечности числа таких точек в нашей решетке, что $E^{m_1} = E^{m_2}$ при некоторых целых положительных $m_1 > m_2$ и, следовательно, что $E^{m_1 - m_2} = 1$, т. е. что точки эти имеют своими координатами корни из единицы. Мы видим, что два автоморфизма умножения нашей решетки тогда и только тогда имеют одинаковые параметры, когда они отличаются одним из конечного числа этих множителей E. Среди единиц E всегда есть единицы $+1$ и -1.

Рассмотрим теперь $(\sigma + \tau)$-мерное вещественное пространство $R_{\sigma+\tau}$, причем мы будем обозначать координаты в $R_{\sigma+\tau}$ буквой y. Сопоставим всякому автоморфизму ε умножения рассматриваемой неприводимой и максимальной решетки $[\omega_1, \omega_2, \ldots, \omega_n]$ точку $\bar{\varepsilon}$, координатами $y', y'', \ldots y^{(\sigma+\tau)}$ которой являются параметры $|\zeta'|, |\zeta'|, \ldots, |\zeta^{(\sigma)}|, \rho', \rho'', \ldots \rho^{(\tau)}$ этого автоморфизма ε. Система точек $\bar{\varepsilon}$ лежит в $R_{\sigma+\tau}$ на поверхности $y' \cdot y'' \cdot \ldots \cdot y^{(\sigma+\tau)} = +1$ и, очевидно, повторяется умножением, если под произведением двух точек в $R_{\sigma+\tau}$ понимать точку, координаты которой суть просто произведения соответственных координат умножаемых точек, так как система точек ε в $R_{n,\tau}$ повторяется умножением, а произведению двух ε соответствует произведение соответствующих $\bar{\varepsilon}$. Рассмотрим, соответственно всем $\bar{\varepsilon}$, точки $\bar{\bar{\varepsilon}}$ в $R_{\sigma+\tau}$, координаты которых суть

логарифмы соответственных координат $\bar{\varepsilon}$. Система всех точек ε лежит — в виду того, что произведение координат любой точки $\bar{\varepsilon}$ есть $+1$ — в $(\sigma+\tau-1)$-мерной плоскости P, проходящей через начало $R_{\sigma+\tau}$ и имеющей в $R_{\sigma+\tau}$ уравнение $y'+y''+\ldots+y^{(\sigma+\tau)}=0$, причем точка $\bar{\varepsilon}$ для $\varepsilon=1$ лежит в начале координат в плоскости P. Произведению двух точек $\bar{\varepsilon}$ соответствует сумма двух точек $\bar{\bar{\varepsilon}}$ в плоскости P, так как, когда числа перемножаются, логарифмы их складываются; то, что система $\bar{\varepsilon}$ повторяется умножением, перефразируется на систему $\bar{\bar{\varepsilon}}$ так, что она повторяется сложением. Из того, что среди точек ε есть точки, у которых любой один параметр большой, а остальные малые, следует то, что точки $\bar{\bar{\varepsilon}}$ лежат в плоскости P $(\sigma+\tau-1)$-мерно.

Действительно, рассмотрим, например, случай, когда плоскость P 3-мерная, т. е. когда $\sigma+\tau-1=3$. Координатные плоскости пространства $R_{\sigma+\tau}$, которое в этом случае 4-мерно, в пересечении с P дадут четыре двухмерные плоскости в P, составляющие такие углы друг с другом, какие составляют грани правильного тетраэдра, но проходящие через одну точку в P, а именно, через начало координат O. Передвинем эти плоскости весьма мало в P параллельно самим себе в отрицательную сторону так, чтобы вокруг начала образовался маленький правильный тетраэдр T, и будем обозначать номерами 1, 2, 3, 4 трехгранные углы, вертикальные трехгранным углам этого тетраэдра. В таком случае то, что есть точки ε, у которых один, какой угодно, из параметров большой (больше, чем 1), т. е. логарифм его больше нуля, а остальные малые (меньше, чем 1), т. е. логарифмы их меньше нуля, равносильно, очевидно, тому, что внутри каждого из трехгранных углов 1, 2, 3, 4 есть точки $\bar{\bar{\varepsilon}}$. Надо показать, что в таком случае система точек $\bar{\bar{\varepsilon}}$ в P трехмерна. Действительно, возьмем по одной точке $\bar{\bar{\varepsilon}}_1$, $\bar{\bar{\varepsilon}}_2$, $\bar{\bar{\varepsilon}}_3$, $\bar{\bar{\varepsilon}}_4$ внутри каждого из трехгранных углов 1, 2, 3, 4. Повернем плоскости боковых граней тетраэдра T вокруг ребер его основания так, чтобы они прошли через точку $\bar{\varepsilon}_3$: получится тетраэдр T_4, содержащий тетраэдр T внутри себя, у которого точки $\bar{\bar{\varepsilon}}_1$, $\bar{\bar{\varepsilon}}_2$, $\bar{\bar{\varepsilon}}_3$ будут попрежнему лежать внутри трехгранных углов, вертикальных трехгранным углам соответствующих его вершин, и у которого точка $\bar{\bar{\varepsilon}}_4$ будет одной из его вершин. Аналогично, поворачивая плоскости граней тетраэдра T_4, мы получим охватывающий его тетраэдр $T_{3,4}$, у которого уже две из наших точек — вершины, затем такой его охватывающий, у которого три из наших точек суть вершины, и, наконец, такой тетраэдр $T_{1,2,3,4}$, у которого все четыре наши точки являются вершинами. Но тетраэдр $T_{1,2,3,4}$ охватывает все предыдущие, а следовательно и тетраэдр T, т. е. он трехмерен, а потому и точки $\bar{\bar{\varepsilon}}_1$, $\bar{\bar{\varepsilon}}_2$, $\bar{\bar{\varepsilon}}_3$, $\bar{\bar{\varepsilon}}_4$ лежат трехмерно.

Рассуждение в том случае, когда P выше трех измерений, совершенно аналогично.

Система точек $\bar{\bar{\varepsilon}}$ дискретна, так как каждая часть логарифмического пространства ограниченного диаметра есть изображение ограниченной же части пространства $R_{n,\tau}$, следовательно $\bar{\bar{\varepsilon}}$, в силу леммы 1 „Приложения“ есть $(\sigma+\tau-1)$-мерная решетка. Пусть $\bar{\bar{\varepsilon}}_1$, $\bar{\bar{\varepsilon}}_2$, $\ldots$, $\bar{\bar{\varepsilon}}_{\sigma+\tau-1}$ — основные точки этой решетки. Тогда любая точка $\bar{\bar{\varepsilon}}$ этой решетки имеет вид $\bar{\bar{\varepsilon}}=m_1\bar{\bar{\varepsilon}}_1+m_2\bar{\bar{\varepsilon}}_2+\ldots+m_{\sigma+\tau-1}\bar{\bar{\varepsilon}}_{\sigma+\tau-1}$, где m_1, m_2, $\ldots$, $m_{\sigma+\tau-1}$ — некоторое целые рациональные числа.

Возвращаясь к точкам $\bar{\varepsilon}$, мы видим, что любая точка $\bar{\varepsilon}$ имеет вид $\bar{\varepsilon}=\bar{\varepsilon}^{m_1}\bar{\varepsilon}^{m_2}\ldots\bar{\varepsilon}^{m_{\sigma+\tau-1}}$. Но, кроме того, еще надо принять во внимание, что самое сопоставление точек ε точкам $\bar{\varepsilon}$ делалось с точностью до миожителей E_l, т. е. что все точки $\varepsilon\cdot E_l$ сопоставлялись одной и той же точке $\bar{\varepsilon}$, и, следова-

тельно, общий вид точки ε есть $\varepsilon = E_i \cdot \varepsilon_1^{m_1} \cdot \varepsilon_2^{m_2} \dots \varepsilon_{\sigma+\tau-1}^{m_{\sigma+\tau-1}}$, как это и утверждалось в теореме. В случае если имеется хотя бы одна вещественная координата, точки E_i суть только точки $+1$ и -1.

Теорема 2. *Если* $[\omega_1, \omega_2, \dots, \omega_n]$ — *приводимая максимальная решетка, причем* χ *есть число ее неприводимых частей и* $\sigma+\tau-\chi>0$, *то она имеет бесконечно много автоморфизмов умножения* ε, *которые все суть ее собственные точки и выражаются формулой:*

$$\varepsilon = E_1 \cdot \varepsilon_1^{m_1} \cdot \varepsilon_2^{m_2} \dots \varepsilon_{\sigma_1+\tau_1-1}^{m_{\sigma_1+\tau_1-1}} \cdot E_2 \cdot \varepsilon_{(\sigma_1+\tau_1-1)+1}^{m_{(\sigma_1+\tau_1-1)+1}} \dots \varepsilon_{\sigma+\tau-\chi}^{m_{\sigma+\tau-\chi}},$$

где показатели $m_1, m_2, \dots, m_{\sigma+\tau-\chi}$ — *все возможные целые рациональные числа, а* E_i *и* ε_k — *основные автоморфизмы предыдущей теоремы для неприводимых частей, дописанные единицами 1 для всех тех координат* K_n, *которые не входят в данную неприводимую часть.*

Действительно, как в предыдущей теореме, убеждаемся в том, что всякий автоморфизм умножения ε рассматриваемой приводимой решетки есть точка ее с нормой единица, и обратно. Всякий такой автоморфизм, очевидно, превращает в себя любое линейное подпространство, натянутое на некоторый комплекс осей K_n, а следовательно превращает в себя отдельные неприводимые части рассматриваемой решетки, т. е., если координаты ε суть $x, x', \dots, x^{(n-1)}$, то $(x, x', \dots, x^{(n_1-1)})$ есть автоморфизм умножения первой неприводимой части, $(x^{n_1}, x^{n_1+1}, \dots, x^{n_1+n_2-1})$ — автоморфизм умножения второй неприводимой части и т. д., и обратно, если это координаты автоморфизмов умножения отдельных неприводимых частей, то $(x, x', \dots, x^{(n-1)})$ есть автоморфизм умножения всей рассматриваемой решетки, так как точка эта имеет норму ± 1 и лежит в этой решетке. Обозначив через $E_1, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\sigma_1+\tau_1-1}$ точки нашей решетки, первые n_1 координат которых совпадают с координатами соответственных основных автоморфизмов умножения первой неприводимой части, а остальные $n-n_1$ координат которых равны 1 [такие точки в нашей решетке есть, а именно они получаются, если к соответственным автоморфизмам умножения первой неприводимой части прибавлять тривиальные автоморфизмы умножения $(00\dots0\overbrace{11\dots1}^{n_2}00\dots0)$, $(00\dots0\overbrace{11\dots1}^{n_3}00\dots0)$, $\dots$ $(00\dots\overbrace{00\dots0\,11\dots1}^{n_k})$ остальных неприводимых частей], и соответственно через $E_2, \varepsilon_{(\sigma_1+\tau_1-1)+1}, \dots, \varepsilon_{(\sigma_1+\tau_1-1)+(\sigma_2+\tau_2+1)}$ то же самое для второй неприводимой части, и т. д., мы и получаем теорему.

Подобными мы называем две решетки в K_n, из которых одна получается из другой умножением на точку из K_n, не являющуюся делителем нуля.

Теорема 3. *Любая решетка в* K_n *(n-мерная), рациональная по отношению к решетке, повторяющейся умножением в* K_n, *или подобная такой рациональной решетке, если* $\sigma+\tau-\chi>0$, *имеет бесконечно много автоморфизмов умножения, которые, однако, вообще говоря, уже не являются ее собственными точками.*

Действительно, такая решетка отличается лишь множителем от рациональной по отношению к некоторой максимальной решетке, с тем же $\sigma+\tau-\chi$, а именно той, в которой лежит рассматриваемая решетка, повторяющаяся умножением. Будем умножать рассматриваемую решетку на все автоморфизмы умножения этой максимальной решетки; все время будут получаться решетки подобные рациональным по отношению к этой же максимальной решетке с тем же индексом и с тем же знаменателем, но число различных автоморфизмов умножения рассматриваемой максимальной решетки бесконечно велико, а число различных рациональных по отношению к ней решеток с данным знаменателем и данным индексом (см. лемму III[II] „Приложения") ограничено, и, следовательно, сколько

угодно ее автоморфизмов умножения будут давать одну и ту же такую решетку. Частное от деления любых двух таких автоморфизмов будет давать автоморфизм умножения заданной решетки.

Теорема 4. *Если совершенно произвольная решетка* (n-*мерная*) *в* K_n *имеет хоть один автоморфизм умножения* ε, *который есть точка общего положения в* K_n, *то решетка эта либо рациональна по отношению к некоторой максимальной решетке, повторяющейся умножением, для которой* $\sigma+\tau-\chi>0$, *либо подобна такой рациональной решетке.*

Действительно, пусть ε — автоморфизм умножения некоторой решетки $[\omega_1, \omega_2, \ldots, \omega_n]$ в K_n и точка ε в K_n — общего положения. Мы имеем:

$$\begin{aligned}
\omega_1\varepsilon &= a_{11}\omega_1 + a_{12}\omega_2 + \ldots + a_{1n}\omega_n \\
\omega_2\varepsilon &= a_{21}\omega_1 + a_{22}\omega_2 + \ldots + a_{2n}\omega_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\omega_n\varepsilon &= a_{n1}\omega_1 + a_{n2}\omega_2 + \ldots + a_{nn}\omega_n
\end{aligned}$$

где коэфициенты a_{ik} — целые рациональные. Точка ε имеет, следовательно, своими координатами (так как она общего положения, т. е. все координаты ее различны) все корни уравнения

$$F(\varepsilon)=\begin{vmatrix} a_{11}-\varepsilon, & a_{12}, & \ldots, & a_{1n} \\ a_{21}, & a_{22}-\varepsilon, & \ldots, & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1}, & a_{n2}, & \ldots, & a_{nn}-\varepsilon \end{vmatrix}=0$$

с целыми рациональными коэффициентами и старшим коэффициеитом, равным 1. Если точка ε общего положения, то векторы $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-2}$ лежат n-мерно в K_n, и если ω_1 не делитель нуля, что всегда можно предполагать, то векторы $\omega_1\varepsilon, \omega_1\varepsilon^2, \ldots, \omega_1\varepsilon^n$ тоже лежат n-мерно в K_n, и следовательно определитель матрицы целых рациональных коэффициентов b_{ik} системы

$$\left.\begin{aligned}
\omega_1 &= \omega_1 \\
\omega_1\varepsilon &= b_{21}\omega_1 + b_{22}\omega_2 + \ldots + b_{2n}\omega_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\omega_1\varepsilon^{n-1} &= b_{n1}\omega_1 + b_{n2}\omega_2 + \ldots + b_{nn}\omega_n
\end{aligned}\right\}$$

не равен нулю, откуда следует, что хоть один из миноров элементов 1-ой колонны этой матрицы имеет определитель, не равный нулю. Возьмем соответствеиные $n-1$ уравнений и разделим их на ω_1 (ω_1, по предположению, — не делитель нуля, значит — разделить можно), мы найдем, что $\frac{\omega_2}{\omega_1}, \frac{\omega_3}{\omega_1}, \ldots, \frac{\omega_n}{\omega_1}$ выражаются линейно однородно с рациональными коэффициентами через $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$, т. е. что решетка $\left[1=\frac{\omega_1}{\omega_1}, \frac{\omega_2}{\omega_1}, \frac{\omega_3}{\omega_1}, \ldots, \frac{\omega_n}{\omega_1}\right]$ рациональна по отношению к решетке $[1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}]$, а следовательно рациональна и по отношению к максимальной решетке, повторяющейся умножением, в которой лежит эта решетка, т. е. к максимальной решетке, определяемой уравнением $F(\varepsilon)=0$. Решетка же $[\omega_1, \omega_2, \ldots, \omega_n]$, следовательно, либо рациональна по отношению к этой максимальной решетке, либо пропорциональна такой рациональной решетке.

§ 5. Идеалы максимальной решетки, группа их классов, одиозначиость разложения

1. Определение понятня идеал. Произведением двух совершенно произвольных решеток L_1 и L_2 в K_n называется совокупность точек, получаемых так: все точки L_1 умножаются на все точки L_2 и из всех полученных

произведений составляются все возможные суммы и разности. Эта совокупность может быть, вообще говоря, не решеткой; если же эта совокупность тоже решетка L_3 в K_n, то, если L_1 и L_2 n-мерные решетки в K_n, она n-мерная решетка, так как даже от умножения решетки L_1 на одну точку решетки L_2 общего положения мы уже получаем n-мерную решетку в K_n. Решетку L_3 мы называем произведением решеток L_1 и L_2. Если решетка L_2 такова, что произведение решеток $L_1 \cdot L_2$ есть вся решетка L_2 или ее подрешетка, то решетка L_2 называется идеалом решетки L_1. Если решетка L_1 содержит точку $(1, 1, \ldots, 1)$ и L_2 идеал решетки L_1, то $L_1 \cdot L_2 = L_2$. Всякая максимальная решетка O, повторяющаяся умножением, содержит точку $(1, 1, \ldots, 1)$, и поэтому всякая решетка L, которая есть идеал O, имеет то свойство, что она после умножения на O совпадает сама с собою. Мы будем в этом параграфе рассматривать только идеалы максимальной решетки O. Две решетки в K_n мы будем, как и раньше, называть подобными, если одна получается из другой помножением на некоторую точку K_n; точка эта, конечно, не должна быть делителем нуля, так как иначе решетка от умножения на нее перестала бы быть n-мерной в K_n, а между тем мы условились, если не указано противного, словами „решетка в K_n" всегда обозначать n-мерную решетку в K_n. Все подобные между собою решетки в K_n мы называем классом решеток, в частности совокупность подобных между собою идеалов называется классом идеалов. Очевидно, что если L — идеал O, то $\varphi \cdot L$, где φ — какая угодно точка K_n, которая не есть делитель нуля, — также идеал O; мы видим, таким образом, что идеал решетки O может быть иррационален по отношению к решетке O. Вообще идеал решетки O может быть целым, т. е. состоящим из точек этой решетки (быть подрешеткой решетки O), дробным по отношению к O, т. е. являться решеткой рациональной по отношению к O, и иррациональным по отношению к O. Если ω — точка O, не являющаяся делителем нуля, то подрешетка $\omega \cdot O$ решетки O есть идеал решетки O; такой идеал называется главным идеалом и обозначается значком (ω). Если $\omega = \varepsilon$, где ε — некоторая единица O, то $\varepsilon \cdot O = O$. Таким образом, сама решетка O есть также главный идеал в O, называемый единичным идеалом.

2. Теорема 1. *Если O приводима, то всякий идеал j из O есть прямая сумма идеалов из неприводимых частей O.*

Действительно, пусть $\varphi_1, \varphi_2, \ldots, \varphi_n$ — базис рассматриваемого идеала; будем составлять произведение $O \cdot j$ так: помножим O сначала на φ_1, затем на φ_2 и т. д., и наконец на φ_n. Так получится n решеток $O \cdot \varphi_1, O \cdot \varphi_2, \ldots, O \cdot \varphi_n$, каждая из которых, если O есть прямая сумма подрешеток $O_1, O_2, \ldots, O_z$, лежащих в координатных подпространствах $K_{n_1}, K_{n_2}, \ldots, K_{n_\chi}$, есть также прямая сумма некоторых решеток, лежащих в этих подпространствах. Действительно, всякая точка ψ решетки O имеет вид $\psi = \psi_1 + \psi_2 + \ldots + \psi_\chi$, где $\psi_1, \psi_2, \ldots, \psi_\chi$ — некоторые точки этих подрешеток. Следовательно, при умножении ее на φ_i, например, мы можем умножать ее так: $\psi\varphi_i = \psi_1\varphi_i + \psi_2\varphi_i + \ldots + \psi_\chi\varphi_i$, где $\varphi_{i_1}, \varphi_{i_2}, \ldots, \varphi_{i_\chi}$ — точки K_n, лежащие в подпространствах $K_{n_1}, K_{n_2}, \ldots, K_{n_\chi}$ и сумма которых равна φ_i, т. е. это точки, которых координаты в K_n, соответствующие данному подпространству K_{ni}, — такие же, как соответствующие координаты φ_i, а все остальные координаты равны нулю. Произведение $O\varphi_i$ есть, следовательно, прямая сумма решеток $O_1\varphi_{i_1}, O_2\varphi_{i_2}, \ldots, O_\chi\varphi_{i_\chi}$, лежащих в этих подпространствах. Так как сама решетка j получается сложением и вычитанием точек $\varphi_1, \varphi_2, \ldots, \varphi_n$, то мы получим всё произведение $O \cdot j$, если мы составим суммы и разности всех точек решеток $O\varphi_1, O\varphi_2, \ldots, O\varphi_n$; но каждая из них есть прямая сумма решеток, лежащих в подпространствах $K_{n_1}, K_{n_2}, \ldots, K_{n_\chi}$, а следовательно, и само это произведение есть прямая сумма решеток, лежащих в этих подпространствах. Но в O есть точка $(1, 1, \ldots, 1)$ и, следовательно, произведение $O \cdot j$ совпадает с j, т. е. j есть прямая сумма решеток, лежащих в подпространствах $K_{n_1}, K_{n_2}, \ldots, K_{n_z}$.

Пусть, например, $j=j_1+j_2+\ldots+j_\varkappa$, где $j_1, j_2, \ldots, j_\varkappa$ — эти решетки. Мы имеем тогда $O_i\cdot j_i=j_i$, так как $O_i\cdot j_i$ вся состоит из точек $O\cdot j$, т. е. из точек j, лежащих в подпространстве K_{ni}; все же такие точки j составляют в K_{ni} решетку j_i, и, следовательно, все точки $O_i\cdot j_i$ лежат в j_i, но в O_i есть точка $\overbrace{(1,\ 1,\ \ldots,\ 1)}^{n_i}$, и потому $O_i\cdot j_i$ совпадает с j_i, т. е. j_i есть идеал O_i.

3. Теорема 2. *Всякий идеал O подобен некоторой подрешетке решетки O.*

Действнтельно, пусть φ — некоторая точка общего в K_n положения идеала j решетки O. Разделим j на эту точку φ; тогда получится решетка $j'=\frac{j}{\varphi}$, в которой есть точка $(1,\ 1,\ \ldots,\ 1)$. Раз j — идеал, то и j' — идеал O, следовательно, в j' есть все точки $j'\cdot O$, в частности и все точки $1\cdot O$, т. е. j' есть центрировка O. Помножив теперь j' на общий знаменатель Q этой центрировки, мы получаем решетку $j''=j'\cdot Q$, которая есть подрешетка O и которой j подобен. Итак, всякий, даже иррациональный, идеал O есть целый идеал O, помноженный на некоторую точку K_n.

4. Теорема 3. *Число h классов идеалов данной максимальной решетки O ограничено.*

В силу предыдущей теоремы, это, очевидно, достаточно доказать лишь для идеалов O, которые суть подрешетки решетки O, т. е. целые идеалы O. Будем, для краткости, такие идеалы решетки O называть идеалами в O. Пусть j — некоторый идеал в O; тогда (теор. 1) $j=j_1=j_2+\ldots+j_\varkappa$, где $j_1, j_2, \ldots, j_\varkappa$ суть идеалы в неприводимых частях $O_1, O_2, \ldots, O_\varkappa$. Если V_j — объем основного параллелепипеда j, рассматриваемый в сигнатурном пространстве $R_{n,\tau}$, соответствующем O, и $V_{j_1}, V_{j_2}, \ldots, V_{j\varkappa}$ — объемы основных параллелепипедов идеалов $j_1, j_2, \ldots, j_\varkappa$ в сигнатурных пространствах $R_{n_1\tau_1}, R_{n_2\tau_2}, \ldots, R_{n\varkappa\tau\varkappa}$, соответствующих неприводимым частям O, то, очевидно, $V_j=V_{j_1}\cdot V_{j_2}\cdot\ldots\cdot V_{j\varkappa}$.

Пусть ψ_1 — относительный минимум решетки j_1, рассматриваемый в пространстве $R_{n_1\tau_1}$, ψ_2 — относительный минимум решетки j_2, рассматриваемый в пространстве $R_{n_2\tau_2}$, и т. д. Тогда норма ψ_1, по лемме Минковского о выпуклом теле, не больше, чем $\left(\frac{4}{\pi}\right)^{\tau_1}V_{j_1}$, норма j_2 не больше, чем $\left(\frac{4}{\pi}\right)^{\tau_2}V_{j_2}$ и т. д., и следовательно норма точки $\psi=\psi_1+\psi_2+\ldots+\psi_k$ (которая лежит в j и не есть делитель нуля) не больше, чем $\left(\frac{4}{\pi}\right)^{\tau}V_j$. Решетка $\psi\cdot O$ есть подрешетка j, объем основного параллелепипеда которой равен $N_\psi\cdot V_O$ (где V_O — объем основного параллелепипеда O), т. е. не больше, чем $\left(\frac{4}{\pi}\right)^{\tau}V_j\cdot V_O$, — другими словами, $\frac{j}{\psi}$ есть центрировка O с индексом, не меньшим $\left[\left(\frac{4}{\pi}\right)^{\tau}\cdot V_O\right]^{-1}$. Но всех различных центрировок O с ограниченным снизу индексом — ограниченное число, и следовательно наш произвольно взятый идеал j в O подобен одной из ограниченного числа этих решеток.

5. Умножение идеалов и композиция классов. Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — некоторые идеалы O; тогда они подобны подрешеткам $\bar{\mathfrak{a}}$ и $\bar{\mathfrak{b}}$ решетки O, так как O повторяется умножением и сложением; произведение решеток $\bar{\mathfrak{a}}$ и $\bar{\mathfrak{b}}$ будет состоять из точек O и, следовательно, будет также некоторой подрешеткой $\bar{\mathfrak{c}}$ решетки O. Решетка $\bar{\mathfrak{c}}$ опять идеал в O, так как, если ω — любая точка из O, то $\omega\bar{\mathfrak{b}}$ суть точки в $\bar{\mathfrak{b}}$, так как $\bar{\mathfrak{b}}$ — идеал в O, и следовательно $\bar{\mathfrak{a}}\cdot\bar{\mathfrak{b}}\omega$ состоит из точек $\bar{\mathfrak{a}}\cdot\bar{\mathfrak{b}}$, т. е. из точек $\bar{\mathfrak{c}}$, и, стало быть, при умножении $\bar{\mathfrak{c}}$ на любые точки из O получаются опять точки из $\bar{\mathfrak{c}}$. Поэтому, если мы перемножим решетки $\mathfrak{a}$ и $\mathfrak{b}$, мы получим некоторую решетку $\mathfrak{c}$ (подобную идеалу $\bar{\mathfrak{c}}$), которая, следовательно, также будет идеалом O.

Идеал $\mathfrak{c}$ называется произведением идеалов $\mathfrak{a}$ и $\mathfrak{b}$.

Если взять два другие идеала $\mathfrak{a}^*$ и $\mathfrak{b}^*$ тех же классов, как $\mathfrak{a}$ и $\mathfrak{b}$, т. е. такие, что $\mathfrak{a}^* = \mathfrak{a}\cdot\lambda$; $\mathfrak{b}^* = \mathfrak{b}\cdot\mu$, где λ и μ — некоторые точки K_n, не делители нуля, то $\mathfrak{a}^*\cdot\mathfrak{b}^* = \mathfrak{c}^*$, где $\mathfrak{c}^* = \mathfrak{c}\cdot\lambda\mu$, т. е. того же класса, как $\mathfrak{c}$, поэтому перемножение идеалов ведет к понятию о композиции классов.

Мы будем называть любые решетки в K_n, подобные решеткам идеалов O, решетками классов; тогда имеет место —

Теорема 4. *Произведение двух классов есть определенный класс.*

Легко видеть, что умножение решеток ассоциативно; отсюда и следует теорема:

Теорема 5. *Композиция классов ассоциативна.*

Помножим любой идеал j решетки O на самую эту решетку, которая есть, как мы видели, также ее идеал, а именно так называемый единичный идеал.

В виду того, что j — идеал O, от умножения точек j на точки O будут получаться точки j, а в виду того, что в O есть точка $1 = (1, 1, \ldots, 1)$, так получатся все точки j, и мы имеем, следовательно, $jO = j$, т. е. теорему —

Теорема 6. *Главный класс, т. е. решетки, подобные решетке O (а, следовательно, и решеткам любых главных идеалов), играет при композиции классов роль единицы.*

Докажем еще следующую теорему.

Теорема 7. *Для всякого класса идеалов O имеется обратный ему класс, т. е. такой, что произведение рассматриваемого класса на этот класс дает главный класс.*

Прежде всего докажем, что единственным идеалом, умножение на который не меняет первого множителя, является сама максимальная решетка O. Пусть действительно

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a}.$$

Рассмотрим совокупность всех точек пространства K_n, умножение на которые превращает решетку $\mathfrak{a}$ в ее часть. Такие точки, очевидно, повторяются сложением, вычитанием, умножением и образуют дискретную совокупность, расположенную в K_n n-мерно, ибо все точки решетки O входят в состав этой совокупности. Следовательно, эта совокупность точек есть решетка, повторяющаяся умножением. В виду того, что она содержит все точки O, она может только совпадать с O, так как O — максимальна. В виду того, что при умножении на любую точку идеала $\mathfrak{b}$ идеал $\mathfrak{a}$ превращается в свою часть, все точки идеала $\mathfrak{b}$ должны входить в O, т. е. $\mathfrak{b}$ есть целый идеал.

Докажем теперь, что идеал $\mathfrak{b}$ содержит среди своих точек точку 1, чего, очевидно, будет достаточно, чтобы убедиться в том, что $\mathfrak{b} = O$, ибо мы уже доказали, что $\mathfrak{b}$ содержится в O, но $\mathfrak{b}$, будучи идеалом для O, будет содержать, вместе с точкой 1, все точки O. Обозначим через $a_1, a_2, \ldots, a_n$ базис идеала $\mathfrak{a}$.

Каждая из точек базиса $\mathfrak{a}$ должна принадлежать решетке $\mathfrak{a}\mathfrak{b}$ и, следовательно, представляться в виде суммы произведений точки из $\mathfrak{a}$ на точку из $\mathfrak{b}$, которая, очевидно, может быть всегда преобразована к виду $\beta_1 a_1 + \beta_2 a_2 + \ldots + \beta_n a_n$, где $a_1, a_2, \ldots, a_n$ — точки базиса $\mathfrak{a}$, $\beta_1, \beta_2, \ldots, \beta_n$ — какие-то точки из $\mathfrak{b}$.

Применив это рассуждение к точкам базиса $\mathfrak{a}$, получим:

$$\begin{aligned}
a_1 &= \beta_{11} a_1 + \beta_{12} a_2 + \ldots + \beta_{1n} a_n,\\
a_2 &= \beta_{21} a_1 + \beta_{22} a_2 + \ldots + \beta_{2n} a_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
a_n &= \beta_{n1} a_1 + \beta_{n2} a_2 + \ldots + \beta_{nn} a_n,
\end{aligned}$$

откуда

$$\begin{vmatrix} \beta_{11}-1, & \beta_{12}, & \dots, & \beta_{1n} \\ \beta_{21}, & \beta_{22}-1, & \dots, & \beta_{2n} \\ \dots & \dots & \dots & \dots \\ \beta_{n1}, & \beta_{n2}, & \dots, & \beta_{nn}-1 \end{vmatrix} = 0.$$

Из этого равенства заключаем, что точка 1 получается действием умножения, сложения и вычитания над точками идеала $\mathfrak{b}$ и, следовательно, содержится в $\mathfrak{b}$. Итак, $\mathfrak{b} = O$.

Пусть теперь $\mathfrak{c}$ — идеал некоторого класса. В виду того, что число h классов конечно, среди степеней идеала $\mathfrak{c}$ с положительными показателями найдется сколь угодно много принадлежащих к одному и тому же классу. Пусть $\mathfrak{c}^m$ и $\mathfrak{c}^{m+k}$ принадлежат к одному классу, и пусть γ есть точка K_n, умножение на которую превращает идеал $\mathfrak{c}^m$ в $\mathfrak{c}^{m+k}$. Рассмотрим идеал $\mathfrak{b} = \frac{1}{\gamma}\mathfrak{c}^k$. Очевидно, что

$$\mathfrak{c}^m\mathfrak{b} = \frac{1}{\gamma}\mathfrak{c}^{m+k} = \mathfrak{c}^m.$$

Отсюда следует, что $\mathfrak{b} = O$ и, следовательно, $\mathfrak{c}^k = \gamma O$ принадлежит главному классу. Очевидно, что $\mathfrak{c}^{k-1}$ принадлежит классу, обратному для класса, содержащего $\mathfrak{c}$, ибо

$$\mathfrak{c}^{k-1}\cdot\mathfrak{c} = \mathfrak{c}^k = \gamma O.$$

Четыре теоремы (4, 5, 6 и 7) настоящего пункта показывают, что решетки классов образуют своей композицией группу. Вследствие теоремы о конечности числа h классов, группа эта конечна, а в виду того, что умножение идеалов, как это непосредственно следует из его определения, очевидно коммутативно, группа эта абелева. Итак мы имеем следующую теорему:

Теорема 8. *Решетки классов образуют композицией конечную абелеву группу.*

Начиная с пункта 6 мы будем в этом параграфе рассматривать только идеалы в O.

6. Теорема 9. *Делитель и центрирующий идеал — одно и то же.*

Пусть идеал $\mathfrak{a}$ есть произведение идеалов $\mathfrak{m}$ и $\mathfrak{t}$; тогда, как мы видели при доказательстве предыдущей теоремы, любая точка $\mathfrak{a}$ составляется из точек базиса $\mathfrak{t}$ линейно, с коэффициентами, которые суть точки из $\mathfrak{m}$, т. е., в виду того, что $\mathfrak{t}$ есть идеал в O, решетка $\mathfrak{a}$ есть подрешетка решетки $\mathfrak{t}$ и, следовательно, $\mathfrak{t}$ есть центрировка $\mathfrak{a}$.

Предположим, наоборот, что идеал $\mathfrak{t}$ есть центрировка идеала $\mathfrak{a}$, и пусть $\mathfrak{t}^*$ — какой-нибудь идеал класса, обратного классу идеала $\mathfrak{t}$, так что $\mathfrak{t}\mathfrak{t}^* = \tau O$, где τ некоторая точка O. В таком случае идеал $\tau O = \mathfrak{t}\cdot\mathfrak{t}^*$ есть центрировка идеала $\mathfrak{a}\mathfrak{t}^*$, — так как из того, что всякая точка α идеала $\mathfrak{a}$ есть одновременно точка идеала $\mathfrak{t}$, следует, что все точки $\alpha_i\cdot t_k^*$, где α_i — точки базиса $\mathfrak{a}$, а t_k^* — точки базиса $\mathfrak{t}^*$, суть точки идеала $\mathfrak{t}\mathfrak{t}^*$, а следовательно и любая сумма и разность таких точек есть также точка идеала $\mathfrak{t}\cdot\mathfrak{t}^*$. Таким образом, все точки идеала $\mathfrak{a}\cdot\mathfrak{t}^*$ заключаются среди точек идеала $\mathfrak{t}\cdot\mathfrak{t}^* = \tau O$ и, следовательно, $\mathfrak{a}\cdot\mathfrak{t}^* = \tau\mathfrak{m}$, где $\mathfrak{m}$ — некоторая решетка из O, причем решетка эта является идеалом в O, так как она подобна идеалу $\mathfrak{a}\mathfrak{t}^*$.

Умножим обе части последнего равенства на идеал $\mathfrak{t}$; тогда мы получим $\mathfrak{a}\mathfrak{t}^*\mathfrak{t} = \tau\mathfrak{m}\mathfrak{t}$ или, так как $\mathfrak{t}^*\mathfrak{t} = \tau O$ и $\mathfrak{a}O = \mathfrak{a}$, мы получаем $\mathfrak{a}\tau = \tau\mathfrak{m}\mathfrak{t}$, откуда, деля обе решетки на τ, мы получаем $\mathfrak{a} = \mathfrak{m}\mathfrak{t}$.

7. Конечность числа делителей идеала, простые идеалы.

Теорема 10. *Число различных делителей данного идеала конечно.*

В виду того, что число различных центрировок любой данной подрешетки решетки O таких, которые состоят только из точек O, ограниченно, следует,

в силу предыдущей теоремы, что и подавно различных решеток, которые суть решетки идеалов делителей данного идеала, ограниченное число.

Пусть некоторый данный идеал в O, отличный от самой O, не имеет собственных делителей, т. е. делителей, отличных от него самого и единичного идеала O; тогда он называется простым; если же он таких делителей имеет, то идеал называется не простым.

Теорема 11. *Всякий идеал либо сам простой, либо может быть представлен как произведение простых идеалов.*

Рассмотрим произвольный идеал в O. Если он сам не простой, то он имеет собственного делителя. Рассмотрим этот собственный делитель; если он не простой, то он в свою очередь имеет собственного делителя, и т. д. Получающаяся так цепочка идеалов представляет собою цепочку последовательных центрировок исходного идеала, состоящих из точек O, со все уменьшающимся объемом основного параллелепипеда. Число различных таких центрировок ограничено, и, следовательно, цепочка эта должна обрываться; т. е. некоторый из ее последовательных идеалов, наконец, не будет содержать собственных делителей, т. е. будет простым. Выделив этот простой идеальный множитель из рассматриваемого идеала, мы получаем идеал, который есть также центрировка заданного, т. е. имеет меньший, чем заданный, объем основного параллелепипеда. С этим идеалом мы можем производить тот же процесс, причем оставшийся множитель будет иметь еще меньший объем. В виду конечности числа различных центрировок данной подрешетки O, состоящих из точек O, таким образом, можно выделять лишь конечное число раз простые множители, и исходный идеал, очевидно, равен их произведению. Всякий идеал есть, следовательно, произведение конечного числа простых идеалов.

8. Однозначность разложения идеала на простые идеалы.

Теорема 12. *Если идеалы* $\mathfrak{a}$ *и* $\mathfrak{b}$ *не имеют общего делителя, отличного от* O, *то в* $\mathfrak{a}$ *можно найти такую точку* α, *а в* $\mathfrak{b}$ *такую точку* β, что $\alpha+\beta=1$.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — базис идеала $\mathfrak{a}$, а $\beta_1, \beta_2, \ldots, \beta_n$ — базис идеала $\mathfrak{b}$. Составим совокупность $\lambda_1\alpha_1+\lambda_2\alpha_2+\ldots+\lambda_n\alpha_n+\mu_1\beta_1+\mu_2\beta_2+\ldots+\mu_n\beta_n$, где λ_i и μ_i — произвольные точки из O. Это будет, очевидно, n-мерная решетка в O, такая, что произведение любой ее точки на любую точку ω из O есть ее же точка, т. е. это идеал в O. В виду того, что в O есть точка 1, в этом идеале, очевидно, лежат как все точки $\alpha_1, \alpha_2, \ldots, \alpha_n$, так и все точки $\beta_1, \beta_2, \ldots, \beta_n$, т. е. вся решетка $\mathfrak{a}$ и вся решетка $\mathfrak{b}$. Этот идеал есть, следовательно, как центрировка $\mathfrak{a}$, так и центрировка $\mathfrak{b}$.

Предположим теперь, что $\mathfrak{a}$ и $\mathfrak{b}$ идеалы взаимно простые, т. е. что они не имеют общего делителя, отличного от O. Тогда идеал этот есть O. Но в таком случае точка 1 также имеет такой вид, т. е. $1=\alpha+\beta$, где α и β суть некоторые точки из идеалов $\mathfrak{a}$ и $\mathfrak{b}$.

Теорема 13. *Если произведение двух идеалов делится на простой идеал* $\mathfrak{p}$, *то на* $\mathfrak{p}$ *делится хоть один из множителей.*

Пусть произведение двух идеалов $\mathfrak{a}\cdot\mathfrak{b}$ делится на простой идеал $\mathfrak{p}$. Предположим, что $\mathfrak{a}$ не делится на $\mathfrak{p}$, т. е., другими словами, что $\mathfrak{a}$ и $\mathfrak{p}$ — взаимно простые, так как, в силу простоты $\mathfrak{p}$, $\mathfrak{p}$ не имеет делителей, отличных от O, кроме самого себя. В таком случае в $\mathfrak{a}$ имеется такая точка α, а в $\mathfrak{p}$ такая точка π, что $\alpha+\pi=1$. Если β — любая точка из $\mathfrak{b}$, то точка $\alpha\cdot\beta$ заключается в $\mathfrak{a}\cdot\mathfrak{b}$, и так как $\mathfrak{p}$, как делитель $\mathfrak{a}\cdot\mathfrak{b}$, есть центрировка $\mathfrak{a}\cdot\mathfrak{b}$, то точка $\alpha\cdot\beta$ заключается и в $\mathfrak{p}$. Но так как $\mathfrak{p}$ — идеал, точка $\pi\cdot\beta$ заключается в $\mathfrak{p}$. Тогда и точка $\alpha\cdot\beta+\pi\beta$ заключается в $\mathfrak{p}$, и так как $\alpha\beta+\pi\beta=(\alpha+\pi)\beta=\beta$, то любая точка $\mathfrak{b}$, а следовательно и вся решетка $\mathfrak{b}$, заключается в решетке $\mathfrak{p}$, т. е. $\mathfrak{p}$ есть центрировка, а следовательно, по теореме 9-ой и делитель идеала $\mathfrak{b}$. Итак, если произведение двух идеальных множителей делится на простой идеал $\mathfrak{p}$, то хоть один из этих множителей сам делится на этот простой идеал.

Теорема 14. *Всякий идеал только одним способом разлагается на простые множители.*

Пусть теперь некоторый идеал имел бы два разложения на простые множители: $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_k=\mathfrak{q}_1\mathfrak{q}_2\ldots\mathfrak{q}_l$. Хоть один из $\mathfrak{q}$ должен делиться на $\mathfrak{p}_1$, т. е., так как все $\mathfrak{q}$ — простые, с ним совпадать. Действительно, в силу предыдущего, если бы ни один из $\mathfrak{q}$ не делился на $\mathfrak{p}_1$, то и все произведение $\mathfrak{a}=\mathfrak{q}_1\mathfrak{q}_2\ldots\mathfrak{q}_l$ не могло бы делиться на $\mathfrak{p}_1$, а между тем оно на $\mathfrak{p}_1$ делится. Выберем так нумерацию множителей $\mathfrak{q}$, чтобы было $\mathfrak{q}_1=\mathfrak{p}_1$; в таком случае идеалы $\mathfrak{p}_2\ldots\mathfrak{p}_k$ и $\mathfrak{q}_2\ldots\mathfrak{q}_l$ одинаковы, так как из $\mathfrak{bc}=\mathfrak{bd}$ следует всегда $\mathfrak{c}=\mathfrak{d}$, в чем можно убедиться следующим образом.

Помножим обе части на идеал $\mathfrak{b}^*$ из класса, обратного классу $\mathfrak{b}$. Тогда $\mathfrak{bb}^*=\tau O$, где τ — точка O, и, следовательно, мы получим $\tau O\mathfrak{c}=\tau O\mathfrak{d}$ или, деля обе решетки на τ, $O\mathfrak{c}=O\mathfrak{d}$. Но $O\mathfrak{c}=\mathfrak{c}$, $O\mathfrak{d}=\mathfrak{d}$, и, следовательно, $\mathfrak{c}=\mathfrak{d}$.

Повторяя теперь то же рассуждение с произведениями $\mathfrak{p}_2\ldots\mathfrak{p}_k$ и $\mathfrak{q}_2\ldots\mathfrak{q}_l$ и предполагая $k\leqslant l$, мы получим наконец $O=\mathfrak{q}_{k+1}\ldots\mathfrak{q}_l$, т. е. что $l=k$ и что исходные произведения, если и отличаются, то только порядком множителей.

9. Теорема 15. *В любых двух классах идеалов можно указать целые взаимно простые идеалы.*

Доказательство. Пусть даны два класса K_1 и K_2. Возьмем в классе K_1 какой угодно целый идеал $\mathfrak{a}$ и в классе K_2^{-1} — какой угодно целый идеал $\mathfrak{b}$. Пусть $\mathfrak{v}_1, \mathfrak{v}_2, \ldots, \mathfrak{v}_k$ — все различные простые идеалы, входящие в $\mathfrak{a}$. Возьмем в идеале $\mathfrak{bv}_2\mathfrak{v}_3\ldots\mathfrak{v}_k$ точку π_1, не принадлежащую идеалу $\mathfrak{bv}_1$. Такая точка, наверное, найдется, ибо иначе идеал $\mathfrak{bv}_2\mathfrak{v}_3\ldots\mathfrak{v}_k$ содержался бы в идеале $\mathfrak{bv}_1$, а следовательно делился бы на него, и следовательно идеал $\mathfrak{v}_2\mathfrak{v}_3\ldots\mathfrak{v}_k$ делился бы на $\mathfrak{v}_1$, что невозможно. Таким же образом найдем точку π_2, принадлежащую идеалу $\mathfrak{bv}_1\mathfrak{v}_3\ldots\mathfrak{v}_k$ и не принадлежащую $\mathfrak{bv}_2$ и т. д.

Точка $\beta=\pi_1+\pi_2+\ldots+\pi_k$, очевидно, будет принадлежать идеалу $\mathfrak{b}$, но не принадлежать ни одному из идеалов $\mathfrak{bv}_1, \mathfrak{bv}_2, \ldots, \mathfrak{bv}_k$. Идеал $\mathfrak{c}=\beta\mathfrak{b}^{-1}$ будет целым идеалом, так как β принадлежит $\mathfrak{b}$, и не будет делиться ни на один из идеалов $\mathfrak{v}_1, \mathfrak{v}_2, \ldots, \mathfrak{v}_k$, т. е. будет взаимно прост с $\mathfrak{a}$. Идеал $\mathfrak{c}$ принадлежит классу K_2. Итак, в любых двух классах K_1 и K_2 мы можем найти взаимно простые идеалы. Тем самым теорема доказана полностью.

Отметим одно *следствие* из доказанной теоремы. *Каждый целый идеал есть общий наибольший делитель двух главных идеалов.* Действительно, пусть $\mathfrak{a}$ — идеал из некоторого класса K. Возьмем в этом идеале произвольное число α. Тогда идеал $[\alpha]$ будет делиться на $\mathfrak{a}$. $[\alpha]=\mathfrak{ab}$. Найдем в классе K^{-1} идеал $\mathfrak{c}$, взаимно простой с $\mathfrak{b}$. Идеал $\mathfrak{ac}$ будет главным, $\mathfrak{ac}=[\beta]$ и общий наибольший делитель идеалов $[\alpha]$ и $[\beta]$ будет равен $\mathfrak{a}$, так как идеалы $\mathfrak{b}$ и $\mathfrak{c}$ взаимно просты.

10. Теорема о нормах идеалов. Индекс решетки целого идеала по отношению к решетке O, т. е. число, показывающее, во сколько раз объем основного параллелепипеда решетки идеала больше объема основного параллелепипеда решетки O, называется нормой идеала. Так как решетка всякого идеала в O есть подрешетка решетки O, норма всякого идеала и O — число целое, рациональное и положительное.

Теорема 16. *Норма произведения двух идеалов равна произведению норм множителей.*

Заметим прежде всего, что эту теорему достаточно доказать для какой-либо пары представителей из двух данных классов, чтобы убедиться в ее справедливости для всех пар идеалов, принадлежащих этим же классам.

Действительно, пусть теорема справедлива для идеалов $\mathfrak{a}$ и $\mathfrak{b}$, и пусть $\mathfrak{a}_1$ и $\mathfrak{b}_1$ — идеалы, эквивалентные соответственно идеалам $\mathfrak{a}$ и $\mathfrak{b}$. В виду того, что решетки идеалов $\mathfrak{a}$ и $\mathfrak{a}_1$ и $\mathfrak{b}$ и $\mathfrak{b}_1$ подобны, мы можем написать, что

$\mathfrak{a}_1 = \alpha\mathfrak{a}$, $\mathfrak{b}_1 = \beta\mathfrak{b}$, где α и β — некоторые точки из K_n, и следовательно $\mathfrak{a}_1\mathfrak{b}_1 = \alpha\beta\mathfrak{a}\mathfrak{b}$.

Очевидно, далее, что при умножении какого-либо идеала на точку из K_n норма его приобретает множителя, равного абсолютной величине нормы точки, на которую производится умножение, ибо именно таким образом изменяется объем основных параллелепипедов решетки. Следовательно,

$$N(\mathfrak{a}_1\mathfrak{b}_1) = |N(\alpha\beta)|\,N(\mathfrak{a}\mathfrak{b}) = |N(\alpha)|\cdot|N(\beta)|\cdot N(\mathfrak{a})\,N(\mathfrak{b}) = \\ = |N(\alpha)|\,N(\mathfrak{a})\cdot|N(\beta)|\,N(\mathfrak{b}) = N(\mathfrak{a}_1)\,N(\mathfrak{b}).$$

Уже из этого замечания следует справедливость теоремы для случая, когда один из идеалов — главный, ибо она правильна для случая, когда одним из множителей является единичный идеал O.

На основании теоремы 15, доказательство теоремы в общем случае сводится к случаю взаимно простых идеалов, ибо в любых двух классах можно найти взаимно простых представителей.

Докажем теперь теорему для двух взаимно простых идеалов $\mathfrak{a}$ и $\mathfrak{b}$. Их объединение $(\mathfrak{a}, \mathfrak{b})$ равно O. Легко видеть, что произведение идеалов $\mathfrak{a}$ и $\mathfrak{b}$ равно их пересечению. Действительно, каждая точка произведения идеалов $\mathfrak{a}$ и $\mathfrak{b}$ принадлежит им обоим, а следовательно и их пересечению. Обратно, пусть γ — точка, принадлежащая пересечению идеалов $\mathfrak{a}$ и $\mathfrak{b}$. Так как $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты, в $\mathfrak{a}$ найдется точка α и в $\mathfrak{b}$ точка β такие, что $\alpha + \beta = 1$.

Следовательно, $\gamma = \alpha\gamma + \beta\gamma$. Точка $\beta\gamma$ принадлежит идеалу $\mathfrak{a}\mathfrak{b}$, ибо α принадлежит $\mathfrak{a}$, γ принадлежит $\mathfrak{b}$. Точка $\beta\gamma$ также приналлежит $\mathfrak{a}\mathfrak{b}$, ибо β принадлежит $\mathfrak{b}$, γ принадлежит $\mathfrak{a}$. Следовательно, γ принадлежит $\mathfrak{a}\mathfrak{b}$. Применяя лемму 4 „Приложения“ к решеткам O, $\mathfrak{a}$, $\mathfrak{b}$ и $\mathfrak{a}\mathfrak{b}$, получим:

$$\frac{N(\mathfrak{a}\mathfrak{b})}{N(\mathfrak{a})} = \frac{N(\mathfrak{b})}{N(O)},$$

и следовательно $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\,N(\mathfrak{b})$.

Теорема доказана полностью.

§ 6. Основная фигура, состоящая из главной решетки O и h—1 побочных решеток

Выберем по одному идеалу из каждого из h классов. Из главного класса возьмем именно идеал O, а идеалы остальных $h-1$ классов нормируем каждый помножением на такую точку K_n, не являющуюся делителем нуля, чтобы объемы всех получившихся решеток сделались такими же, как объем V_O решетки O.

Начиная с этой нормировки, эти $h-1$ решеток, вообще говоря, уже перестанут быть подрешетками O.

Пусть $g_1 = O$, g_2, g_3, ..., g_h — получившиеся таким путем решетки. Покажем, что умножение таких двух решеток g_i, g_k дает решетку g_l опять с таким же объемом.

Действительно, пусть $\lambda g_l = j_i$; $\mu g_k = j_k$, где j_i и j_k суть те идеалы в O, из которых мы получали решетки g_l и g_k, а точки λ и μ суть точки, обратные тем множителям, при помощи которых мы нормировали эти идеалы для получения этих решеток. В таком случае $N(\lambda)$ и $N(\mu)$ суть нормы идеалов j_i и j_k. Но $N(j_ij_k) = N(j_i)\,N(j_k) = N(\lambda)\,N(\mu) = N(\lambda\mu)$, и, следовательно, g_l имеет опять тот же объем V_O, что и g_l и g_k.

Так нормированные решетки классов g_1, g_2, ..., g_h своей композицией образуют группу классов, с точностью до множителей точек K_n имеющих нормы 1. Мы будем называть такие множители *поворотными*.

Нормируем теперь еще дальше наши решетки, а именно нормируем их еще умножением на некоторые определенным образом выбранные поворотные множители. Начиная с этой второй нормировки, эти $h-1$ решеток, вообще говоря, уже не будут лежать в K_n в том же сигнатурном подпространстве, где лежит O, — так, например, O может быть чисто вещественно, а координаты точек этих решеток могут при этом быть комплексными. Поступим так: оставим $g_1 = O$ в том положении, в котором она находится: каждую из тех остальных g_i, которые являются элементами базиса абелевой группы классов, помножим на такой поворотный множитель e_i, чтобы, если порядок g_i есть q, т. е. g_i^q — решетка, подобная g_1, она после этого помножения просто совпадала с решеткой g_1, т. е. чтобы было $(g_i e_i)^q = g_1$. Если λ_i — точка K_n, на которую надо помножить g_i^q, чтобы получить g_1, то, очевидно, необходимо и достаточно, чтобы $e_i^q = \lambda_i$, т. е. чтобы было $e_i = \sqrt[q]{\lambda_i}$. Точка e_i, вообще говоря, может уже не лежать в сигнатурном подпространстве, соответствующем O. [Так, например, в случае, когда все координаты O вещественны, может случиться (и примеры показывают, что это бывает), что не все координаты точки λ_i положительны, и тогда, если при этом q четно (что также бывает), то уже не все координаты e_i вещественны].

После такого дополнительного нормирования тех решеток g_i, которые образуют базис группы классов, т. е. после замены их решетками $e_i g_i$, они уже окажутся так „повернуты“ в пространстве K_n, что соответствующие их степени будут не только подобны решетке $g_1 = O$ главного класса, а даже просто будут с ней совпадать. Если мы теперь через эти основные g_i выразим все остальные g_i, то все так полученные g_i будут уже в том смысле повернуты правильно в K_n, что если $g_i g_k$ подобна g_l, то она просто с ней совпадает, т. е. $g_i g_k = g_l$. Совокупность всех h так *правильно* расположенных решеток g_i мы будем называть основной фигурой, соответствующей данной максимальной решетке O, повторяющейся умножением.

Из самого способа построения основной фигуры мы видим, что для заданной O можно ее построить различными способами. Посмотрим, чем будут при этом друг от друга отличаться получаемые основные фигуры. Во-первых, если λ_i — точка, от умножения на которую g_i^q мы получаем точно $g_1 = O$, то $\lambda_i \cdot \varepsilon$, где ε — любой автоморфизм O, — также такая точка; и обратно, если $\bar{\lambda}_i$ — другая такая точка и $\bar{\lambda}_i = \lambda_i \bar{\varepsilon}$, то $\bar{\varepsilon}$ есть автоморфизм O. Таким образом, общий вид точки, на которую надо помножить g_i^q, чтобы получить g_1, есть $\lambda_i \cdot \varepsilon$, где ε — любые автоморфизмы O. Отсюда мы видим, что $e_i = \sqrt[q]{\lambda_i}\varepsilon$ имеет, если автоморфизмов у O бесконечно много, бесконечно много значений. Но два различных e_i и $\bar{e}_i$, которые сами друг от друга отличаются лишь на автоморфизм умножения O, будут давать из даиной g_i одну и ту же решетку, так как, если $\bar{e}_i = e_i \cdot \varepsilon$, то $g_i e_i = g_i e_i \varepsilon$. В этом последнем легко убедиться, если заметить, что $g_i = j_i \cdot \mu_i$, где μ_i — некоторая точка K_n; тогда $g_i e_i = j_i \mu_i e_i$, а $g_i e_i \varepsilon = j_i \mu_i e_i \varepsilon$. Но $j_i \varepsilon = j_i$, так как от умножения всех точек идеала на некоторую точку ε из O получаются опять точки этого же идеала (норма ε равна ± 1 и, следовательно, получаются все точки этого идеала). Таким образом, различные окончательно нормированные решетки g_i будут давать из предварительно нормированной решетки g_i только те множители, которые не отличаются просто автоморфизмом умножения решетки O. Таким образом, если $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\sigma+\tau-\varkappa}$ — основные автоморфизмы умножения решетки O, то за множитель ε, стоящий под корнем в e_i, достаточно взять лишь множители вида $E_1 E_2 \ldots E_\varkappa \varepsilon_1^{q_1} \varepsilon_2^{q_2} \ldots \varepsilon_{\sigma+\tau-\varkappa}^{q_{\sigma+\tau-\varkappa}}$, где все показатели $q_1, q_2, \ldots, q_{\sigma+\tau-\varkappa}$ больше или равны нулю и меньше чем q, а E_l — различные рассмотренные в § 4 автоморфизмы конечных порядков. Кроме того, можно еще брать любое из значений радикала $\sqrt[q]{\ }$.

Рассмотрим для заданной максимальной решетки O, повторяющейся умножением, какую-нибудь одну (все равно какую) из этого конечного числа различных возможных для нее основных фигур.

Теорема 1. *Основная фигура повторяется умножением.*

Действительно, если θ_i — точка, принадлежащая решетке g_i основной фигуры, а θ_j принадлежит ее решетке g_j (где $j =$ или $\neq i$) и $g_i g_j = g_k$, то точка $\theta_i\theta_j = \theta_k$ принадлежит решетке g_k.

Замечание. Легко убедиться на примерах, что если $h > 1$ (если $h = 1$, то основная фигура есть сама O), то основная фигура не есть решетка, т. е. не повторяется сложением.

Теорема 2. *Абсолютная величина нормы любой точки основной фигуры есть целое рациональное число.*

Действительно, если точка решетки есть делитель нуля, то норма ее равна нулю (и обратно). Пусть теперь θ — точка решетки g_i, которая не есть делитель нуля. Помножив на нее все точки решетки g_i^{-1}, соответствующей классу, обратному g_i, получим некоторую подрешетку решетки $g_1 = O$. Следовательно, объем основного параллелепипеда решетки g_i^{-1}, который равен объему основного параллелепипеда $g_1 = O$, увеличится при этом в целое число раз. Но при умножении на точку объем решетки увеличивается в число раз, равное абсолютной величине нормы этой точки, т. е. абс. вел. нормы точки — целое рациональное число.

Теорема 3. *Всякий автоморфизм умножения ε всей основной фигуры все равно, что автоморфизм любой из ее решеток и, следовательно, есть автоморфизм главной решетки, и обратно.*

Действительно, если ε есть автоморфизм умножения $g_1 = O$, то εg_k суть точки g_k, так как ε принадлежит к главной решетке. Но норма ε равна ± 1, и, следовательно, объем основного параллелепипеда $\varepsilon \cdot g_k$ равен объему основного параллелепипеда g_k, т. е. $\varepsilon g_k = g_k$. Таким образом, любой автоморфизм умножения ε главной решетки есть автоморфизм умножения системы совокупности всех h решеток $g_1, g_2, \ldots, g_h$, и даже автоморфизм умножения каждой из них в отдельности. Наоборот, если ε — автоморфизм умножения системы совокупности всех h решеток $g_1, g_2, \ldots, g_h$, то абсолютная величина его нормы равна 1. ε есть точка основной фигуры, так как в основной фигуре есть точка 1 и $\varepsilon \cdot 1$ должна быть точкой основной фигуры. Точка ε лежит в главной решетке потому, что, если бы она лежала в побочной решетке g_k, то решетка $g_k^{-1} \cdot \varepsilon$ состояла бы из точек главной решетки g_1 и с нею бы совпадала, так как объемы решеток g_k^{-1} и g_1 одинаковы, а абсолютная величина нормы точки ε равна 1; но побочная решетка не может быть подобна главной. Итак, всякий автоморфизм ε основной фигуры есть точка главной решетки с нормой ± 1, т. е. автоморфизм главной решетки.

Мы будем называть две точки основной фигуры, получающиеся друг из друга, ее автоморфизмами умножения, т. е. автоморфизмами умножения решетки O, союзными. Совокупность всех точек основной фигуры союзных с некоторой ее точкой, которая не есть делитель нуля, мы будем называть сеткой союзных точек. Очевидно, что все точки сетки точек, союзных некоторой точке основной фигуры, принадлежащей ее решетке g_i, принадлежат той же ее решетке g_i, так как все автоморфизмы ε принадлежат главной решетке.

Теорема 4. *Любая точка θ основной фигуры, которая не есть делитель нуля (вместе со всеми точками сетки союзных ей точек), однозначно соответствует некоторому идеалу решетки O, и обратно, причем произведению двух таких точек соответствует произведение соответствующих им идеалов, и обратно.*

Действительно, пусть θ_i некоторая точка решетки g_i. Решетка $\mathfrak{a}_i = g_i^{-1}\theta_i$ лежит в $g_1 = O$ и является идеалом O. Действительно, пусть ω — любая

точка O. Тогда $g_i^{-1}\theta_i\omega$ суть опять точки из O и притом принадлежащие той же решетке $\mathfrak{a}_i$, так как от умножения на ω того идеала из O, нормированием которого получилась решетка g_i^{-1}, получатся точки того же идеала, а, следовательно, от умножения на ω решетки g_i^{-1} получается точка той же решетки, и потому от умножения на ω решетки $\mathfrak{a}_i = g_i^{-1}\theta_i$ получатся точки той же решетки $\mathfrak{a}_i$. Идеал $\mathfrak{a}_i$ мы будем называть соответствующим точке θ_i основной фигуры. Очевидно, что любой точке $\theta_i\varepsilon$, где ε — любой автоморфизм O (а, следовательно, и основной фигуры), соответствует тот же идеал $\mathfrak{a}_i$, так как ε есть автоморфизм того идеала в O, нормированием которого получилась решетка g_i^{-1}. Таким образом, ε есть автоморфизм и самой g_i^{-1}, т. е. $g_i^{-1}\varepsilon\theta_i = g_i^{-1}\theta_i$. Наоборот, если $\mathfrak{a}$ — идеал i^{-1}-того класса решетки O и, следовательно, $\mathfrak{a} = g_i^{-1}\mu$, где μ — некоторая точка K_n, не являющаяся делителем нуля, то $\mathfrak{a}g_i = g_1\mu$, и, так как в $g_1 = O$ есть точка 1, точка μ содержится в $\mathfrak{a}g_i$, т. е. μ содержится в g_i.

Произведению точек $\theta_i\theta_j \dots \theta_k$ основной фигуры, принадлежащих к i-ой, j-ой, ..., k-ой решеткам g, где $i, j, \dots, k$ могут быть как равны, так и различны, соответствует, очевидно, в этом смысле идеал $\mathfrak{a} = g_i^{-1}\theta_i \cdot g_j^{-1}\theta_j \dots g_k^{-1}\theta_k$, т. е. идеал $g_e^{-1}\cdot\theta_i\theta_j \dots \theta_k$.

Теорема 5. *В любом классе идеалов в O есть идеал, норма которого* $< \left(\frac{4}{\pi}\right)^\tau \sqrt{|D|}$.

Действительно, любая побочная решетка g главной решетки $g_1 = O$ получается из некоторого идеала j в O умножением его на нормирующую точку, абс. вел. нормы которой равна $\frac{1}{N(j)}$. Пусть $\overline{O}$ — решетка в $R_{n,\tau}$, соответствующая O, и $\overline{j}$ — идеал в $\overline{O}$, соответствующий j. Как мы показали в п. 4 § 5, в $\overline{j}$ существуют точки $\overline{\omega}$, которые не являются делителями нуля и суть относительные минимумы в $\overline{j}$, в том смысле, что внутри нормированного тела такой точки $\overline{\omega}$ нет других точек $\overline{j}$, кроме точки 0. Объем нормированного тела такой точки, $2^\sigma\pi^\tau N(\omega)$, в таком случае, по лемме Минковского о выпуклом теле, меньше объема $\frac{\sqrt{|D|}}{2^\tau}N(j)$ основного параллелепипеда $\overline{j}$, взятого 2^n раз, т. е. $N(\omega) < \left(\frac{2}{\pi}\right)^\tau \sqrt{|D|}\,N(j)$. После нормировки идеала j к соответствующей ему побочной решетке g мы получаем, что в этой решетке g есть точка $\overline{\overline{\omega}}$, норма которой $N(\overline{\overline{\omega}}) < \left(\frac{2}{\pi}\right)^\tau \sqrt{|D|}$. Если мы помножим побочную решетку g^{-1} на точку $\overline{\overline{\omega}}$, то получим, по предыдущей теореме, идеал в O, имеющий норму, равную $N(\overline{\overline{\omega}})$, т. е. норму $< \left(\frac{2}{\pi}\right)^\tau \sqrt{|D|}$.

Для неприводимых решеток оценка, данная в теореме 5, может быть еще улучшена. Именно, имеет место следующая теорема.

Теорема 6. *В любом классе идеалов в неприводимой решетке есть идеал, норма которого меньше*

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^\tau \sqrt{|D|}.$$

Доказательство. Пусть K — некоторый класс идеалов, и K^{-1} — обратный ему класс. Возьмем в классе K^{-1} какой-либо идеал $\mathfrak{a}$. Идеал $\mathfrak{a}$ в пространстве $R_{n,\tau}$ изобразится как решетка, с объемом основного параллелепипеда $\frac{1}{2^\tau}\sqrt{|D|}\,N(\mathfrak{a})$.

Рассмотрим тело

$$|x^{(1)}|+|x^{(2)}|+\ldots+|x^{(\sigma)}|+2\sqrt{\xi^{(1)2}+\eta^{(1)2}}+\ldots+$$
$$+2\sqrt{\xi^{(\tau)2}+\eta^{(\tau)2}}\leqslant T.$$

Легко видеть, что это тело выпуклое и имеет центром симметрии начало координат. Объем его равен

$$2^{\sigma}\left(\frac{\pi}{2}\right)^{\tau}\cdot\frac{1}{n!}T^{n}.$$

Подберем T так, чтобы объем был равен объему основного параллелепипеда идеала $\mathfrak{a}$, умноженному на 2^n.

$$2^{\sigma}\left(\frac{\pi}{2}\right)^{\tau}\cdot\frac{1}{n!}T^{n}=2^{n}\cdot\frac{1}{2^{\tau}}\sqrt{|D|}\,N(\mathfrak{a}).$$

Тогда, по лемме 5 дополнения, внутри или на границе тела найдется хотя бы одна точка α идеала $\mathfrak{a}$, отличная от нуля. Так как решетка $\mathfrak{a}$ не имеет делителей нуля, $N(\alpha)\neq 0$.

Среднее геометрическое положительных чисел не превосходит их среднего арифметического. Поэтому

$$N(\alpha)=|x^{(1)}|\cdot|x^{(2)}|\cdot\ldots\cdot|x^{(\sigma)}|\cdot(\sqrt{\xi^{(1)2}+\eta^{(1)2}})^{2}\cdot\ldots\cdot(\sqrt{\xi^{(\tau)2}+\eta^{(1)2}})^{2}\leqslant$$
$$\leqslant\left(\frac{|x^{(1)}|+|x^{(2)}|+\ldots+|x^{(\sigma)}|+2\sqrt{\xi^{(1)2}+\eta^{(1)2}}+\ldots+2\sqrt{\xi^{(\tau)2}+\eta^{(\tau)2}}}{n}\right)^{n}\leqslant$$
$$\leqslant\frac{T^{n}}{n^{n}}=\frac{2^{n-\sigma}}{\pi^{\tau}}\cdot\frac{n!}{n^{n}}\sqrt{|D|}\,N(\mathfrak{a})=\left(\frac{4}{\pi}\right)^{\tau}\frac{n!}{n^{n}}\sqrt{|D|}\,N(\mathfrak{a}).$$

Главный идеал $[\alpha]$ делится на идеал $\mathfrak{a}$, $[\alpha]=\mathfrak{a}\mathfrak{b}$. Частное $\mathfrak{b}$ есть целый идеал из класса K. В виду того, что $|N(\alpha)|=N(\mathfrak{a})\cdot N(\mathfrak{b})$, заключаем:

$$N(\mathfrak{b})\leqslant\left(\frac{4}{\pi}\right)^{\tau}\frac{n!}{n^{n}}\sqrt{|D|},$$

что и требовалось доказать.

Из доказанной теоремы следует, что

$$\left(\frac{4}{\pi}\right)^{\tau}\frac{n!}{n^{n}}\sqrt{|D|}\geqslant 1,$$

ибо $N(\mathfrak{b})\geqslant 1$, и следовательно

$$\sqrt{|D|}\geqslant\frac{n^{n}}{n!}\cdot\left(\frac{\pi}{4}\right)^{\tau}.$$

Это неравенство показывает, во-первых, что $\sqrt{|D|}>1$, во-вторых, что наименьший дискриминант неприводимой решетки, повторяющейся умножением, данного числа измерений растет с возрастанием числа измерений n.

Теорема 7. *Любая точка основной фигуры однозначно (с точностью до автоморфизмов O) разлагается в произведение простых ее точек.*

Эта теорема следует для не-делителей нуля непосредственно из однозначности разложения идеалов O на простые идеалы и из 4-ой теоремы. Для делителей нуля получается то же самое, если рассмотреть вместо O соответственную этому делителю нуля частичную прямую сумму неприводимых частей O, т. е. ту, которая лежит в том же координатном подпространстве, где лежит рассматриваемый делитель нуля.

§ 7. Квадратичные формы решетки в K_n

1. Формы, связанные с решеткой в K_n. Каждой n-мериой решетке пространства K_n, как повторяющейся, так и не повторяющейся умножением, могут быть соотнесены некоторые формы от n переменных, введе-

ние которых иногда бывает полезно при исследовании тех или иных свойств решеток. К рассмотрению важнейших форм этого рода мы и переходим.

Прежде всего сопоставим решетки с системами линейных форм. Пусть решетка задана координатами точек базиса

$$\begin{aligned}
&\Phi_1(\varphi_1^{(1)}, \varphi_1^{(2)}, \ldots, \varphi_1^{(n-1)}),\\
&\Phi_2(\varphi_2^{(1)}, \varphi_2^{(2)}, \ldots, \varphi_2^{(n-1)}),\\
&\quad\ldots\ldots\ldots\ldots\\
&\Phi_n(\varphi_n^{(1)}, \varphi_n^{(2)}, \ldots, \varphi_n^{(n)}).
\end{aligned}$$

Координаты любой точки $(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)})$ решетки выражаются через координаты точек базиса в виде линейных ковариантных (т. е. зависящих от одной и той же системы переменных) форм:

$$\begin{aligned}
\omega^{(1)} &= x_1\varphi_1^{(1)} + x_2\varphi_2^{(1)} + \ldots + x_n\varphi_n^{(1)},\\
\omega^{(2)} &= x_1\varphi_1^{(2)} + x_2\varphi_2^{(2)} + \ldots + x_n\varphi_n^{(2)},\\
&\quad\ldots\ldots\ldots\ldots\ldots\ldots\\
\omega^{(n)} &= x_1\varphi^{(n)} + x_2\varphi_2^{(n)} + \ldots + x_n\varphi_n^{(n)},
\end{aligned}$$

при целых рациональных значениях переменных $x_1, x_2, \ldots, x_n$. Таким образом, каждому базису решетки однозначно сопоставляется система n ковариантных линейных форм с n переменными. Обратно, каждой системе n ковариантных линейных форм от n переменных этим способом сопоставляется базис некоторой решетки так, что значения форм при всевозможных целочисленных значениях переменных дают координаты всех точек решетки. Необходимо только потребовать, чтобы определитель, составленный из коэффициентов системы форм, был отличен от нуля.

Выясним теперь, каким образом связаны друг с другом системы ковариантных форм, соответствующие различным базисам одной и той же решетки пространства.

Пусть $(\varphi_1, \varphi_2, \ldots, \varphi_n)$ и $(\phi_1, \phi_2, \ldots, \phi_n)$ — два n-векториика пространства K_n, связаниые подстановкой

$$\phi_i = a_{i1}\varphi_1 + a_{i2}\varphi_2 + \ldots + a_{in}\varphi_n \quad (i = 1, 2, \ldots, n)$$

с матрицей $A = \| a_{ik} \|$. Если n-векторники $(\varphi_1, \varphi_2, \ldots, \varphi_n)$ и $(\phi_1, \phi_2, \ldots, \phi_n)$ являются базисами одной и той же решетки, то матрица A целочисленна, и определитель ее равен ± 1.

Соответствующие этим n-векторникам системы линейных форм будут

$$(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)}) \quad \text{и} \quad (\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)}),$$

где

$$\omega^{(s)} = x_1\varphi_1^{(s)} + x_2\varphi_2^{(s)} + \ldots + x_n\varphi_n^{(s)}$$

и

$$\tau^{(s)} = x_1'\phi_1^{(s)} + x_2'\phi_2^{(s)} + \ldots + x_n'\phi_n^{(s)}. \quad (s = 1, 2, \ldots, n)$$

Выражая $\tau^{(s)}$ иепосредственно через $\varphi^{(s)}$, получим

$$\begin{aligned}
\tau^{(s)} = {} & (a_{11}x_1' + a_{21}x_2' + \ldots + a_{n1}x_n')\,\varphi_1^{(s)} +\\
& + (a_{12}x_1' + a_{22}x_2' + \ldots + a_{n2}x_n')\,\varphi_2^{(s)} +\\
& + \ldots\ldots\ldots\ldots\ldots\ldots +\\
& \quad\ldots\ldots\ldots\ldots\ldots\\
& + (a_{1n}x_1' + a_{2n}x_2' + \ldots + a_{nn}x_n')\,\varphi_n^{(s)}, \qquad (s = 1, 2, \ldots, n)
\end{aligned}$$

откуда следует, что формы $(\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)})$ могут быть получены из форм $(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)})$ линейным преобразованием переменных

$$\begin{aligned} x_1 &= a_{11}x_1' + a_{21}x_2' + \ldots + a_{n1}x_n', \\ x_2 &= a_{12}x_1' + a_{22}x_2' + \ldots + a_{n2}x_n', \\ &\ldots\ldots\ldots\ldots\ldots \\ x_n &= a_{1n}x_1' + a_{2n}x_2' + \ldots + a_{nn}x_n', \end{aligned}$$

матрица которого A^* транспонирована с матрицей A подстановки, переводящей координаты n-векторника $[\varphi_1, \varphi_2, \ldots, \varphi_n]$ в координаты $[\psi_1, \psi_2, \ldots, \psi_n]$. В случае, если эти n-векторники являются базисами одной решетки, то матрица A^* вместе с матрицей A целочисленна, и определитель равен ± 1.

Очевидно и обратное: если взять две системы ковариантных линейных форм $(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)})$ и $(\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)})$ с определителями, не равными нулю, и такие, что $(\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)})$ получается из $(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)})$ линейным преобразованием переменных с целочисленной матрицей и с определителем, равным ± 1, то эти системы определят базисы одной и той же решетки.

Связанные таким образом системы ковариантных форм называются эквивалентными, а множество всех эквивалентных между собой систем форм называется классом систем ковариантных форм. Таким образом, каждой решетке соответствует вполне определенный класс систем ковариантных форм с определителями, не равными нулю, и обратно, каждому классу систем ковариантных форм с определителями, не равными нулю, соответствует вполне определенная решетка.

Пусть $(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(n)})$ — система ковариантных форм, соответствующая некоторому базису решетки, и пусть $\varphi(u^{(1)}, u^{(2)}, \ldots, u^{(n)})$ — некоторая форма от n переменных. Очевидно, что

$$\varphi(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{n}) = F(x_1, x_2, \ldots, x_n)$$

будет представлять собой форму той же степени от переменных $x_1, x_2, \ldots, x_n$. Различным базисам одной и той же решетки, при одной и той же форме φ, будут соответствовать эквивалентные формы F, т. е. формы, переходящие одна в другую линейной подстановкой переменных с целыми рациональными коэффициентами и с определителем, равным ± 1, так что решетке в целом этим способом сопоставляется класс эквивалентных между собой форм F.

Если при этом рассматриваемая решетка рациональна по отношению к решетке, повторяющейся умножением, а форма φ является симметрической функцией от $u^{(1)}, u^{(2)}, \ldots, u^{(n)}$, то форма $F(x_1, x_2, \ldots, x_n)$ будет иметь рациональные коэффициенты, так как они будут являться симметрическими функциями координат любой точки общего положения рассматриваемой решетки, а координаты каждой такой точки суть корни некоторого уравнения n-ой степени с рациональными коэффициентами.

Важнейшими формами, связанными с такими решетками, являются формы

$$B_0(x_1, x_2, \ldots, x_n) = u^{(1)2} + u^{(2)2} + \ldots + u^{(n)2}$$

и

$$N(x_1, x_2 \ldots x_n) = u^{(1)}u^{(2)} \ldots u^{(n)}.$$

Первую из этих форм назовем эрмитианом, вторую — формою Дирихле. Если рассматриваемая решетка рациональна по отношению к некоторой решетке, повторяющейся умножением, то обе эти формы имеют рациональные коэффициенты, причем, если решетка — целая рациональная по отношению к некоторой решетке, повторяющейся умножением, то коэффициенты форм будут целыми рациональными.

2. Эрмитиан представляет собою квадратичную форму от n переменных. Она будет определенной положительной, если решетка расположена в чисто

вещественном сигнатурном подпространстве пространства K_n, и неопределенной, с числом отрицательных квадратов в каноническом разложении равным числу пар τ комплексных координат точек решетки, т. е. тому числу, которое мы называем сигнатурой решетки.

В чисто вещественном случае задание эрмитиана вполне определяет решетку в себе, но совершенно не определяет ее расположение относительно осей, так что одному эрмитиану соответствует бесконечно много решеток, получающихся одна из другой вращением, как твердого тела, или вращением и отражением относительно какой-либо $(n-1)$-мерной плоскости.

В том случае, когда эрмитиан имеет целые рациональные коэффициенты, можно было бы ожидать, что среди бесконечного множества соответствующих ему решеток найдется одна решетка, повторяющаяся умножением, или подрешетка такой решетки. Однако на самом деле это не имеет места. Именно, может случиться, что данная целочисленная квадратичная форма не является эрмитианом ни для одной решетки, повторяющейся умножением, или ее подрешетки. Так, например, для $n=3$, такова форма $x_1^2+x_2^2+2x_3^2$, в чем нетрудно убедиться. Возможно также, что две или несколько различных решеток, повторяющихся умножением, имеют одинаковые эрмитианы. Так, решетки, построенные на базисах $[1, \lambda, \lambda^2-9\lambda+7]$, где $\lambda^3=9\lambda^2-6\lambda-1$, и $\left[1, \mu, \frac{\mu^2-9\mu+10}{2}\right]$, где $\mu^3=9\mu^2-6\mu-8$, имеют один и тот же эрмитиан

$$x_1^2+69x_2^2+69x_3^2+18x_1x_2+18x_1x_3+12x_2x_3.$$

Аналогичные обстоятельства имеют место и для решеток, расположенных в других сигнатурных пространствах.

3. Безутианы. Кроме сопоставления квадратичной формы со всею решеткою, полезно в некоторых случаях сопоставлять тем же способом квадратичные формы с проекциями решетки — параллельно n-мерным „биссектрисам“ K_n, где m — некоторый делитель n, — на пространства низшего числа измерений, $n-m$, дополнительные к пространствам этих биссектрис.

Пусть дана решетка S в пространстве K_n, повторяющаяся умножением (или часть такой решетки) и имеющая m-мерную подрешетку R, расположенную на „биссектрисе“

$$\begin{aligned}
u^{(1)}=u^{(2)} &= \ldots = u^{(\mu)},\\
u^{(\mu+1)}=u^{(\mu+2)} &= \ldots = u^{(2\mu)},\\
&\cdots\cdots\cdots\cdots\\
u^{(n-\mu+1)}=u^{(n-\mu+2)} &= \ldots = u^{(n)}. \qquad \left(\mu=\frac{n}{m}\right)
\end{aligned}$$

Покажем, что если спроектировать решетку S параллельно биссектрисе на дополнительное к ней пространство $n-m$ измерений:

$$\begin{aligned}
u^{(1)}+u^{(2)} &+ \ldots + u^{(\mu)}=0,\\
u^{\mu+1}+u^{(\mu+2)} &+ \ldots + u^{(2\mu)}=0,\\
&\cdots\cdots\cdots\cdots\\
u^{(n-\mu+1)}+u^{(n-\mu+2))} &+ \ldots + u^{(n)}=0,
\end{aligned}$$

то получим решетку, для которой квадратичная форма, составленная по тому же способу, после умножения на μ будет иметь целые рациональные коэффициенты.

Чтобы не усложнять рассуждений, положим, что в качестве решетки S взята максимальная решетка, повторяющаяся умножением. Это не нарушает общности, так как всякая другая решетка, повторяющаяся умножением, содержится в максимальной.

Прежде всего отметим, что если на биссектрисе существует m-мерная подрешетка решетки S, то, какова бы ни была точка ω решетки S с коорди-

натами

$$(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(\mu)}, \ldots, \omega^{(n-\mu+1)}, \omega^{(n-\mu+2)}, \ldots, \omega^{(n)})$$

и целая симметрическая функция с целыми коэффициентами от μ переменных $\phi(u^{(1)}, u^{(2)}, \ldots, u^{(\mu)})$, точка с координатами $(\phi^{(1)}, \phi^{(1)}, \ldots, \phi^{(1)}, \ldots, \phi^{(m)}, \phi^{(m)}, \ldots, \phi^{(m)})$, где

$$\begin{aligned}
\phi^{(1)} &= \phi(\omega^{(1)}, \omega^{(2)} \quad , \ldots, \omega^{(\mu)}),\\
\phi^{(2)} &= \phi(\omega^{(\mu+1)}, \omega^{(\mu+2)} \quad , \ldots, \omega^{(2\mu)}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\phi^{(m)} &= \phi(\omega^{(n-\mu+1)}, \omega^{(n-\mu+2)}, \ldots, \omega^{n})
\end{aligned}$$

будет являться точкой решетки R.

Действительно, из соображений теории Галуа известно, что эта точка рационально связана с точкой общего положения решетки R, а следовательно, и с точкой общего положения решетки S. Кроме того, она имеет своими координатами целые алгебраические числа, как результаты целых алгебраических действий под целыми числами. Следовательно, она принадлежит решетке S, так как последняя предположена максимальной решеткой, повторяющейся умножением, и потому должна содержать все точки с целыми алгебраическими координатами, рационально связанными с точкой общего положения. Наконец, она лежит на биссектрисе и, следовательно, принадлежит решетке R.

Сопоставим решетке R решетку $\bar{R}$ в пространстве K_m, координатами точек которой являются координаты точек из R, взятые по одному разу из каждой группы разных координат. Решетка $\bar{R}$ будет максимальной решеткой в K_m, повторяющейся в K_m умножением.

Пусть дана точка в $K_n(\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(\mu)}, \ldots, \omega^{(n-\mu+1)}, \ldots, \omega^{(n)})$. Точка σ пространства K_m с координатами

$$(\sigma^{(1)}, \sigma^{(2)}, \ldots, \sigma^{(m)}),$$

где

$$\begin{aligned}
\sigma^{(1)} &= \omega^{(1)} + \omega^{(2)} + \ldots + \omega^{(\mu)},\\
\sigma^{(2)} &= \omega^{(\mu+1)} + \omega^{(\mu+2)} + \ldots + \omega^{(2\mu)},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\sigma^{(m)} &= \omega^{(n-\mu+1)} + \omega^{(n-\mu+2)} + \ldots + \omega^{(n)}
\end{aligned}$$

будет, в силу сделанных замечаний, принадлежать решетке $\bar{R}$. Точку σ будем называть с л е д о м точки ω относительно рассматриваемой биссектрисы. Очевидно, что если точку ω представить через базис системы S и ее след σ — через базис системы $\bar{R}$, то коэффициенты второго представления будут целочисленными линейными формами от коэффициентов первого представления.

Найдем теперь проекцию точки ω на пространство, дополнительное к биссектрисе. Для этого представим ω в виде суммы двух точек так, чтобы одна из них τ принадлежала биссектрисе, вторая φ дополнительному пространству. Слагаемое φ и будет искомой проекцией.

Легко проверить, что τ следует взять имеющую координаты

$$\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(\mu)}, \ldots, \tau^{(n-\mu+1)}, \ldots, \tau^{(n)},$$

где

$$\begin{aligned}
\tau^{(1)} = \tau^{(2)} = \ldots = \tau^{(\mu)} &= \frac{\omega^{(1)} + \omega^{(2)} + \ldots + \omega^{(\mu)}}{\mu} = \frac{\sigma^{(1)}}{\mu},\\
\tau^{(\mu+1)} = \tau^{(\mu+2)} = \ldots = \tau^{(2\mu)} &= \frac{\omega^{(\mu+1)} + \omega^{(\mu+2)} + \ldots + \omega^{(2\mu)}}{\mu} = \frac{\sigma^{(2)}}{\mu},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

$$\tau^{(n-\mu+1)} = \tau^{(n-\mu+2)} = \ldots = \tau^{(n)} = \frac{\omega^{(n-\mu+1)} + \omega^{(n-\mu+2)} + \ldots + \omega^{(n)}}{\mu} = \frac{\sigma^{(m)}}{\mu}.$$

Действительно, относительный след взятой таким образом точки τ равен относительному следу точки ω, и, следовательно, относительный след точки φ равен нулю; это значит, что точка φ лежит в пространстве, дополнительном к биссектрисе.

Представим точку ω через базис системы S.

$$\omega = x_1\omega_1 + x_2\omega_2 + \ldots + x_m\omega_m + x_{m+1}\omega_{m+1} + \ldots + x_n\omega_n.$$

Базис можно выбрать таким образом, что его первые m точек $\omega_1, \omega_2, \ldots, \omega_m$ принадлежат решетке R. Проекция точки ω на пространство, дополнительное к биссектрисе, будет иметь вид

$$\varphi = x_{m+1}\varphi_{m+1} + \ldots + x_n\varphi_n,$$

где $\varphi_{m+1}, \ldots, \varphi_n$ — проекции точек $\omega_{n+1}, \ldots, \omega_n$. Проекции точек $\omega_1, \omega_2, \ldots \omega_m$ будут, очевидно, равны нулю. Таким образом, проекция решетки S будет действительно $(n-m)$-мерной решеткой.

Подсчитаем соответствующую ей квадратичную форму, предварительно умножив последнюю на μ.

$$B_m(x_{m+1}, x_{m+2}, \ldots, x_n) = \mu \sum_{i=1}^{n} (\varphi^{(i)})^2 = \mu \sum_{i=1}^{n} (\omega^{(i)} - \tau^{(i)})^2 =$$

$$= \mu \sum_{i=1}^{n} (\omega^{(i)})^2 - 2\mu \sum_{i=1}^{n} \omega^{(i)}\tau^{(i)} + \mu \sum_{i=1}^{n} (\tau^{(i)})^2 =$$

$$= \mu \sum_{i=1}^{n} (\omega^{(i)})^2 - 2\mu \sum_{j=1}^{m} \sigma^{(j)} \cdot \frac{\sigma^{(j)}}{\mu} + \mu^2 \sum_{j=1}^{m} \left(\frac{\sigma^{(j)}}{\mu}\right)^2 =$$

$$= \mu \sum_{i=1}^{n} (\omega^{(i)})^2 - \sum_{j=1}^{m} (\sigma^{(j)})^2 =$$

$$= \mu \cdot B_0(x_1, x_2, \ldots, x_n) - B_0'(y_1, y_2, \ldots, y_m).$$

Здесь B_0 обозначает эрмитиан решетки S, B_0' — эрмитиан решетки $\overline{R}$, $y_1, y_2, \ldots, y_m$ — линейные формы от $x_1, x_2, \ldots, x_n$, являющиеся коэффициентами в представлении относительного следа точки ω через базис решетки $\overline{R}$.

Так как эрмитианы для решеток, повторяющихся умножением, представляют собой квадратичные формы с целыми коэффициентами, то из полученной нами формулы можно заключить, что форма B_m имеет целые коэффициенты.

Форму B_m будем называть обобщенным безутианом решетки S, а именно безутианом относительно данной биссектрисы. Обобщенный безутиан B_1 решетки, имеющей степенной базис $[1, \rho, \ldots, \rho^{n-1}]$ относительно единственной 1-мерной биссектрисы, т. е. относительно „рациональной прямой“ $u^{(1)} = u^{(2)} = \ldots = u^{(n)}$, представляет собой квадратичную форму, обычно называемую просто безутианом числа ρ, или безутианом уравнения $f(\rho) = 0$, которому удовлетворяет число ρ.

§ 8. Разложимые формы решетки в K_n

Форма Дирихле, т. е. форма $N(x_1, x_2, \ldots, x_n) = u^{(1)} \cdot u^{(2)} \cdot \ldots \cdot u^{(n)}$ для решетки представляет собой форму n-ой степени с n переменными, допускающую разложение на линейные множители, причем эти множители линейно независимы. Формы, обладающие этим свойством, будем называть разложимыми формами.

Каждую разложимую форму можно рассматривать как форму Дирихле для некоторой решетки, однако задание разложимой формы не вполне определяет базис решетки, для которой она будет формой Дирихле, так как разложение формы на множители не однозначно. Именно, в разложении формы на множители

$$F(x_1x_2\ldots x_n)=\prod_{i=1}^{n}(x_1\omega_1^{(i)}+x_2\omega_2^{(i)}+\cdots+x_n\omega_n^{(i)})$$

можно каждого множителя умножать, соответственно, на такие постоянные числа $\lambda^{(i)}$, что $\prod_{i=1}^{n}\lambda^{(i)}=1$. Это значит, что точки базиса решетки ω_1, ω_2, ..., ω_n, для которого форма F является формой Дирихле, можно одновременно множить на произвольную точку $(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(n)})$ с нормой, равной 1. „Комплексные объемы" основных параллелепипедов всех таких решеток будут очевидно одинаковы. Квадрат объема, т. е. дискриминант решетки, называется *дискриминантом разложимой формы*. Очевидно, далее, что подобным решеткам, при соответствующем выборе базисов, соответствуют формы Дирихле, отличающиеся постоянным множителем, равным норме коэффициента подобия, и обратно — разложимым формам, отличающимся постоянным множителем, соответствуют подобные решетки. Отсюда следует, что дискриминанты разложимых форм, отличающихся множителем e, будут отличаться множителем e^2, т. е. дискриминант формы является однородной функцией второй степени от коэффициентов формы.

Форма Дирихле для решетки, подобной решетке, рационально расположенной относительно решетки, повторяющейся умножением, будет, с точностью до множителя, в силу сказанного в начале предыдущего параграфа, формой с рациональными коэффициентами.

Докажем теперь обратное, что разложимая форма с рациональными коэффициентами задает решетку, подобную решетке, рационально расположенной по отношению к некоторой решетке, повторяющейся умножением.

Пусть

$$F(x_1, x_2\ldots x_n)=\sum_{i_1+i_2+\cdots+i_n=n}A_{i_1,i_2\ldots i_n}\cdot x_1^{i_1}\cdot x_2^{i_2}\ldots x_n^{i_n}=$$

$$=\prod_{s=1}^{n}(x_1\omega_1^{(s)}+x_2\omega_2^{(s)}+\cdots+x_n\omega_n^{(s)}) \qquad (*)$$

— разложимая форма с рациональными коэффициентами.

Без нарушения общности можно считать что коэффициент $A_{n,0,0\cdots0}$ при x_1^n равен 1 и что $\omega_1^{(1)}=\omega_1^{(2)}=\cdots=\omega_1^{(n)}=1$. Действительно, в решетке, заданной формой F, найдется точка общего положения, которую можно было бы принять за первую точку базиса. Изменив таким образом базис и поделив на первую точку базиса, перейдем к подобной решетке, удовлетворяющей поставленному требованию. Ее разложимая форма будет лишь рациональным множителем отличаться от формы, эквивалентной данной. По тем же соображениям можно считать точку $(\omega_2^{(1)}, \omega_2^{(2)}, \ldots, \omega_2^{(n)})$ точкой общего положения.

Покажем теперь, что координаты точки ω_2 являются корнями алгебраического уравнения с рациональными коэффициентами и что все остальные точки базиса $\omega_3, \omega_4, \ldots, \omega_n$ рационально выражаются через ω_2. Тем самым высказанное утверждение будет доказано.

Положим в равенстве (*) $x_2=-1$, $x_3=x_4=\cdots=x_n=0$. Получим

$$\prod_{s=1}^{n}(x_1-\omega_2^{(s)})=x_1^n-A_{n-1,1,0\cdots0}x_1^{n-1}+A_{n-2,2,0\cdots0}x_1^{n-2}-\cdots=\varphi(x_1).$$

Отсюда следует, что координаты точки ω_2 являются корнями уравнения n-ой степени с рациональными коэффициентами.

Далее, выпишем выражение некоторых коэффициентов через координаты точек базиса. При этом для сокращения письма введем некоторые обозначения. Символами $\lambda_1^{(1)}, \lambda_2^{(1)}, \ldots, \lambda_{n-1}^{(1)}$ обозначим основные симметрические функции от координат точки ω_2, кроме $\omega_2^{(1)}$. Соответственно, через $\lambda_1^{(2)}, \lambda_2^{(2)}, \ldots, \lambda_{n-1}^{(2)}$ обозначим основные симметрические функции от координат точки ω_2, кроме $\omega_2^{(2)}$, и т. д.

Получим:

$$\begin{aligned}
&\omega_3^{(1)} + \omega_3^{(2)} + \cdots + \omega_3^{(n)} = A_{n-1,\,0,\,1,\,0\ldots0} = a_1\\
&\omega_3^{(1)}\lambda_1^{(1)} + \omega_3^{(2)}\lambda_1^{(2)} + \cdots + \omega_3^{(n)}\lambda_1^{(n)} = A_{n-2,\,1,\,1,\,0\ldots0} = a_2\\
&\omega_3^{(1)}\lambda_2^{(1)} + \omega_3^{(2)}\lambda_2^{(2)} + \cdots + \omega_3^{(n)}\lambda_2^{(n)} = A_{n-3,\,2,\,1,\,0\ldots0} = a_3\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\omega_3^{(1)}\lambda_{n-1}^{(1)} + \omega_3^{(2)}\lambda_{n-1}^{(2)} + \cdots + \omega_3^{(n)}\lambda_{n-1}^{(n)} = A_{0,\,n-1,\,1,\,0\ldots0} = a_n
\end{aligned}$$

Умножим первое равенство на $\omega_2^{(1)n-1}$, второе на $-\omega_2^{(1)n-2}$, третье на $\omega_2^{(1)n-3}$ и т. д. и сложим:

$$\begin{aligned}
&\omega_3^{(1)}(\omega_2^{(1)n-1} - \lambda_1^{(1)}\omega_2^{(1)n-2} + \lambda_2^{(1)}\omega_2^{(1)n-3} - \cdots) +\\
&+ \omega_3^{(2)}(\omega_2^{(2)n-1} - \lambda_1^{(2)}\omega_2^{(1)n-2} + \lambda_2^{(2)}\omega_2^{(1)n-3} - \cdots) +\\
&+ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&+ \omega_3^{(n)}(\omega_2^{(n)n-1} - \lambda_1^{(n)}\omega_2^{(1)n-2} + \lambda_2^{(n)}\omega_2^{(1)n-3} - \cdots) =\\
&= a_1\omega_2^{(1)n-1} - a_2\omega_2^{(1)n-2} + a_3\omega_2^{(1)n-3} - \cdots
\end{aligned}$$

Очевидно, что коэффициент при $\omega_3^{(1)}$ в левой части равенства равен $(\omega_2^{(1)} - \omega_2^{(2)})(\omega_2^{(1)} - \omega_2^{(3)})\ldots(\omega_2^{(1)} - \omega_2^{(n)}) = \varphi'(\omega_2^{(1)})$, отличен от нуля и рационально выражается через $\omega_2^{(1)}$. Коэффициенты же при $\omega_3^{(2)}, \ldots, \omega_3^{(n)}$ все равны нулю. Следовательно,

$$\omega_3^{(1)} = \frac{a_1\omega_2^{(1)n-1} - a_2\omega_2^{(1)n-2} + a_3\omega_2^{(1)n-3} - \cdots}{\varphi'(\omega_2^{(1)})}.$$

Числа $\omega_3^{(2)}, \omega_3^{(3)}, \ldots, \omega_3^{(n)}$ точно таким же образом выражаются через $\omega_2^{(2)}, \omega_2^{(3)}, \ldots, \omega_2^{(n)}$:

$$\omega_3^{(i)} = \frac{a_1\omega_2^{(i)n-1} - a_2\omega_2^{(i)n-2} + a_3\omega_2^{(i)n-3} - \cdots}{\varphi'(\omega_2^{(i)})}.$$

Тем же приемом получим рациональные выражения остальных точек базиса через точку ω_2.

Утверждение доказано.

Как мы уже видели, подобным решеткам соответствуют пропорциональные разложимые формы, и обратно. Естественно ставится вопрос о нормализации разложимых форм с рациональными коэффициентами, т. е. о выборе из совокупности всех пропорциональных друг другу разложимых форм одной формы, наиболее естественно связанной с решеткой, повторяющейся умножением. Задача о нормализации решается посредством введения так называемого кольца множителей решетки.

Пусть дана решетка S в пространстве K_n. Рассмотрим совокупность всех точек λ пространства K_n, обладающих тем свойством, что произведение любой точки решетки S на точку λ принадлежит снова решетке S. Совокупность точек λ, очевидно, содержит все целые рациональные точки и повторяется сложением, вычитанием и умножением. Будем называть эту совокупность кольцом множителей решетки S.

Покажем, что если решетка S подобна решетке, рационально расположенной по отношению к некоторой решетке, повторяющейся умножением, то кольцо множителей будет решеткой пространства K_n, т. е. оно будет n-мерно и дискретно.

Действительно, пусть решетка S подобна решетке, рациональной относительно решетки, повторяющейся умножением. Без нарушения общности можно считать, что решетка S сама рациональна относительно решетки, повторяющейся умножением, и содержит единицу. В самом деле, от решетки S делением на любую ее точку общего положения можно перейти к подобной решетке, удовлетворяющей поставленным требованиям, а подобные решетки имеют, очевидно, одинаковые кольца множителей.

Пусть $[\omega_1, \omega_2, \ldots, \omega_n]$ базис решетки S и ω — какая-либо точка решетки S. Произведения точки ω на точки базиса можно представить через базис:

$$\begin{aligned}
\omega\omega_1 &= a_{11}\omega_1 + a_{12}\omega_2 + \cdots + a_{1n}\omega_n \\
\omega\omega_2 &= a_{21}\omega_1 + a_{22}\omega_2 + \cdots + a_{2n}\omega_n \\
&\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots \\
\omega\omega_n &= a_{n1}\omega_1 + a_{n2}\omega_2 + \cdots + a_{nn}\omega_n,
\end{aligned}$$

причем коэффициенты этого представления будут рациональными числами, так как решетка S рациональна относительно решетки, повторяющейся умножением. Обозначим через d общий знаменатель коэффициентов a_{ik}. Очевидно, что точка $d\omega$ принадлежит кольцу множителей, так как в результате умножения этой точки на точки базиса решетки S мы получим линейные комбинации этих точек с целыми рациональными коэффициентами, т. е. точки решетки S. Таким образом мы видим, что на любом луче, соединяющем начало координат с точками решетки S, существуют точки кольца множителей. Следовательно, кольцо множителей n-мерно. Дискретность доказывается еще проще. Именно, кольцо множителей должно целиком содержаться в решетке S, так как эта последняя содержит единицу. Решетка S дискретна, следовательно и кольцо множителей дискретно.

Итак, кольцо множителей решетки, рационально расположенной относительно некоторой максимальной решетки, повторяющейся умножением, образует решетку, повторяющуюся умножением, очевидно содержащуюся в той же максимальной решетке.

Совершенно очевидно и обратное, что если решетка S имеет своим кольцом множителей n-мерную решетку, то решетка S подобна решетке, рационально расположенной относительно решетки, повторяющейся умножением, именно относительно кольца множителей.

Можно доказать точно так же, как доказывалась конечность числа классов идеалов, что не подобных между собой решеток, имеющих данное кольцо множителей, может быть лишь конечное число. Таким образом, все решетки, подобные решеткам, рационально расположенным относительно решеток, повторяющихся умножением, могут быть расклассифицированы по своим кольцам множителей, причем каждому кольцу соответствует лишь конечное число не подобных друг другу решеток.

Покажем теперь, что в совокупности пропорциональных друг другу разложимых форм с рациональными коэффициентами можно найти форму с дискриминантом, равным дискриминанту кольца множителей, причем эта форма будет иметь целые рациональные коэффициенты.

Пусть $[\omega_1, \omega_2, \ldots, \omega_n]$ — базис решетки S', форма Дирихле которой равна данной разложимой форме $N(x_1, x_2 \ldots x_n)$ и пусть $[\lambda_1, \lambda_2, \ldots, \lambda_n]$ — базис кольца множителей этой решетки. Умножим кольцо множителей на точку $\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$.

Получим новую решетку, которая будет содержаться в решетке S. Базисом этой решетки будет система точек

$$[\omega\lambda_1, \omega\lambda_2, \ldots, \omega\lambda_n] =$$
$$= [l_{11}\omega_1 + l_{12}\omega_2 + \cdots + l_{1n}\omega_n, \ldots, l_{n1}\omega_1 + l_{n2}\omega_2 + \cdots + l_{nn}\omega_n],$$

где l_{ik} представляет собой линейные формы от $x_1, x_2, \ldots, x_n$ с целыми рациональными коэффициентами. Подсчитаем объем (комплексный) основного параллелепипеда этой решетки двумя способами.

С одной стороны, он, очевидно, равен

$$N(x_1, x_2, \ldots, x_n) \cdot V[\lambda_1, \lambda_2, \ldots, \lambda_n],$$

где $V[\lambda_1, \lambda_2, \ldots, \lambda_n]$ — объем основного параллелепипеда кольца множителей. С другой стороны, он равен

$$V[\omega_1, \omega_2, \ldots, \omega_n] \cdot \begin{vmatrix} l_{11}, \ldots, l_{1n} \\ \cdot \cdot \cdot \cdot \cdot \\ \cdot \cdot \cdot \cdot \cdot \\ l_{n1}, \ldots, l_{nn} \end{vmatrix} = V[\omega_1, \omega_2, \ldots, \omega_n] \cdot F(x_1, x_2, \ldots, x_n).$$

Здесь $V[\omega_1, \omega_2, \ldots, \omega_n]$ обозначает объем основного параллелепипеда решетки S. Форма

$$F(x_1, x_2, \ldots, x_n) = \begin{vmatrix} l_{11}, \ldots, l_{1n} \\ \cdot \cdot \cdot \cdot \cdot \\ l_{n1}, \ldots, l_{nn} \end{vmatrix}$$

имеет, очевидно, целые рациональные коэффициенты.

Сопоставляя результаты, получим:

$$N(x_1, x_2, \ldots, x_n) = \frac{V[\omega_1, \omega_2, \ldots, \omega_n]}{V[\lambda_1, \lambda_2, \ldots, \lambda_n]} \cdot F(x_1, x_2, \ldots, x_n).$$

Покажем теперь, что дискриминант формы F равен дискриминанту кольца множителей. Обозначив через D_N и D_F дискриминанты форм N и F, из соотношения между формами получим:

$$D_N = \left(\frac{V[\omega_1, \omega_2, \ldots, \omega_n]}{V[\lambda_1, \lambda_2, \ldots, \lambda_n]}\right)^2 \cdot D_F.$$

Но D_N, по определению, равно $(V[\omega_1, \omega_2, \ldots, \omega_n])^2$, следовательно, $D_F = (V[\omega_1, \omega_2, \ldots, \omega_n])^2$, т. е. действительно дискриминант формы F равен дискриминанту кольца множителей.

Итак, для данной разложимой формы $N(x_1, x_2, \ldots, x_n)$ нам удалось подобрать пропорциональную ей форму $F(x_1, x_2, \ldots, x_n)$ с целыми коэффициентами и с дискриминантом, равным дискриминанту кольца множителей. Форму F будем называть нормализованной разложимой формой. Тот же термин будет применяться к соответствующей ей решетке.

§ 9. Взаимные решетки и взаимные разложимые формы

В теории квадратичных форм и в кристаллографии бывает полезно ввести в рассмотрение, на ряду с данной решеткой, связанную с ней взаимную решетку. Под этим названием, для трехмерных вещественных решеток, подразумевается совокупность концов векторов, перпендикулярных к каждой паре векторов исходной решетки и имеющих длину, равную площади параллелограмма, построенного на паре. Напомним некоторые свойства взаимной решетки.

Пусть S — трехмерная вещественная решетка с базисом $(\omega_1^{(1)}, \omega_1^{(2)}, \omega_1^{(3)})$, $(\omega_2^{(1)}, \omega_2^{(2)}, \omega_2^{(3)})$ и $(\omega_3^{(1)}, \omega_3^{(2)}, \omega_3^{(3)})$. Запишем базис решетки в виде матрицы

$$\begin{pmatrix} \omega_1^{(1)}\omega_1^{(2)}\omega_1^{(3)} \\ \omega_2^{(1)}\omega_2^{(2)}\omega_2^{(3)} \\ \omega_3^{(1)}\omega_3^{(2)}\omega_3^{(3)} \end{pmatrix},$$

расположив в каждой строчке матрицы координаты одной и той же точки базиса.

Рассмотрим пару векторов, идущих в точки решетки:

$$\tau = x_1\omega_1 + x_2\omega_2 + x_3\omega_3 \quad \nu = y_1\omega_1 + y_2\omega_2 + y_3\omega_3.$$

Обозначим через $(\mu^{(1)}, \mu^{(2)}, \mu^{(3)})$ точку взаимной решетки, соотнесенную паре (τ, ν). Ее координаты, очевидно, вычисляются по формулам:

$$\mu^{(1)} = \begin{vmatrix} x_1\omega_1^{(2)} + x_2\omega_2^{(2)} + x_3\omega_3^{(2)}, & x_1\omega_1^{(3)} + x_2\omega_2^{(3)} + x_3\omega_3^{(3)} \\ y_1\omega_1^{(2)} + y_2\omega_2^{(2)} + y_3\omega_3^{(2)}, & y_1\omega_1^{(3)} + y_2\omega_2^{(3)} + y_3\omega_3^{(3)} \end{vmatrix} =$$

$$= \begin{vmatrix} x_2, x_3 \\ y_2, y_3 \end{vmatrix} \cdot \begin{vmatrix} \omega_2^{(2)}, \omega_3^{(2)} \\ \omega_2^{(3)}, \omega_3^{(3)} \end{vmatrix} + \begin{vmatrix} x_3, x_1 \\ y_3, y_1 \end{vmatrix} \cdot \begin{vmatrix} \omega_3^{(2)}, \omega_1^{(2)} \\ \omega_3^{(3)}, \omega_1^{(3)} \end{vmatrix} + \begin{vmatrix} x_1, x_2 \\ y_1, y_2 \end{vmatrix} \cdot \begin{vmatrix} \omega_1^{(2)}, \omega_2^{(2)} \\ \omega_1^{(3)}, \omega_2^{(3)} \end{vmatrix};$$

$$\mu^{(2)} = \begin{vmatrix} x_2, x_3 \\ y_2, y_3 \end{vmatrix} \cdot \begin{vmatrix} \omega_2^{(3)}, \omega_3^{(3)} \\ \omega_2^{(1)}, \omega_3^{(1)} \end{vmatrix} + \begin{vmatrix} x_3, x_1 \\ y_3, y_1 \end{vmatrix} \cdot \begin{vmatrix} \omega_3^{(3)}, \omega_1^{(3)} \\ \omega_3^{(1)}, \omega_1^{(1)} \end{vmatrix} + \begin{vmatrix} x_1, x_2 \\ y_1, y_2 \end{vmatrix} \cdot \begin{vmatrix} \omega_1^{(3)}, \omega_2^{(3)} \\ \omega_1^{(1)}, \omega_2^{(1)} \end{vmatrix};$$

$$\mu^{(3)} = \begin{vmatrix} x_2, x_3 \\ y_2, y_3 \end{vmatrix} \cdot \begin{vmatrix} \omega_2^{(1)}, \omega_3^{(1)} \\ \omega_2^{(2)}, \omega_3^{(2)} \end{vmatrix} + \begin{vmatrix} x_3, x_1 \\ y_3, y_1 \end{vmatrix} \cdot \begin{vmatrix} \omega_3^{(1)}, \omega_1^{(1)} \\ \omega_3^{(2)}, \omega_1^{(2)} \end{vmatrix} + \begin{vmatrix} x_1, x_2 \\ y_1, y_2 \end{vmatrix} \cdot \begin{vmatrix} \omega_1^{(1)}, \omega_2^{(1)} \\ \omega_1^{(2)}, \omega_2^{(2)} \end{vmatrix}.$$

Из этих формул следует, что взаимная решетка есть действительно *решетка*, с базисом, координаты точек которого образуют матрицу, в обычном смысле взаимную матрице, составленной из координат исходного базиса. Такой базис взаимной решетки называется взаимным по отношению к базису исходной решетки.

Для решетки в пространстве K_n назовем *взаимной решеткой* решетку, построенную на базисе, координаты которого образуют матрицу, взаимную с матрицей, образованной координатами точек базиса данной решетки. Геометрический смысл взаимной решетки для вещественной n-мерной решетки — такой же, как для трехмерной, с той только разницей, что перпендикуляры строятся для всех совокупностей из $(n-1)$ некомпланарных векторов решетки.

Введение взаимной решетки оказывается очень полезным и в теории решеток, повторяющихся умножением. Как обычно, целесообразно взаимную решетку скалярно поделить на объем основного параллелепипеда решетки. В дальнейшем, под взаимной решеткой мы будем подразумевать взаимную решетку, уже поделенную на объем основного параллелепипеда.

Отметим несколько свойств такой взаимной решетки:

1. Взаимная решетка к взаимной есть исходная.

Действительно, если (ω) есть матрица, составленная из координат базиса данной решетки, то такая же матрица для взаимной решетки есть $(\bar{\omega})^{-1}$ (черточка сверху — знак транспонирования), а для взаимной к взаимной $\overline{((\omega)^{-1})}^{-1} = \omega$.

2. Если два базиса $(\tau_1, \tau_2, \ldots, \tau_n)$ и $(\omega_1, \omega_2, \ldots, \omega_n)$ связаны преобразованием, имеющим матрицу A:

$$\begin{aligned} \tau_1 &= a_{11}\omega_1 + a_{12}\omega_2 + \cdots + a_{1n}\omega_n, \\ \tau_2 &= a_{21}\omega_1 + a_{22}\omega_2 + \cdots + a_{2n}\omega_n, \\ &\cdots\cdots\cdots\cdots\cdots \\ \tau_n &= a_{n1}\omega_1 + a_{n2}\omega_2 + \cdots + a_{nn}\omega_n, \end{aligned}$$

то взаимные базисы связаны преобразованием с матрицей $\overline{A}^{-1}$.

Действительно, переход к координатным матрицам дает

$$(\tau) = A\,(\omega),$$

откуда

$$(\overline{\tau})^{-1} = (\overline{A\cdot(\omega)})^{-1} = ((\overline{\omega})\cdot\overline{A})^{-1} = \overline{A}^{-1}\cdot(\overline{\omega})^{-1}.$$

3. Если решетку S умножить на точку $(\lambda^{(1)}, \lambda^{(2)}, \ldots \lambda^{(n)})$, то взаимная решетка умножается на точку $\left(\frac{1}{\lambda^{(1)}}, \frac{1}{\lambda^{(2)}}, \ldots, \frac{1}{\lambda^{(n)}}\right)$.

Действительно, умножить решетку S на точку $(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(n)})$ — все равно, что умножить матрицу из координат базиса на матрицу

$$\Lambda = \begin{vmatrix} \lambda^{(1)}, 0, 0 \ldots 0 \\ 0, \lambda^{(2)}, 0 \ldots 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0,\ 0,\ 0, \ldots \lambda^{(n)} \end{vmatrix}$$

справа; тогда

$$(\overline{(\omega)\,\Lambda})^{-1} = (\overline{\omega})^{-1}\overline{\Lambda}^{-1} = (\overline{\omega})^{-1}\Lambda^{-1},$$

ибо

$$\overline{\Lambda} = \Lambda.$$

4. Пусть λ принадлежит кольцу множителей решетки с базисом $(\omega_1, \omega_2 \ldots \omega_n)$ и при умножении на λ базис претерпевает преобразование с матрицей L. Тогда взаимный базис при умножении на ту же точку λ претерпевает преобразование с матрицей $\overline{L}$.

Доказательство. Запишем в матричной форме то обстоятельство, что при умножении на λ базис претерпевает преобразование с матрицей L.

Мы видим, что умножение базиса на λ равносильно умножению координатной матрицы базиса на матрицу

$$\Lambda = \begin{pmatrix} \lambda^{(1)} & & & \\ & \lambda^{(2)} & & \\ & & \cdot & \\ & & & \lambda^{(n)} \end{pmatrix}$$

справа, а преобразование базиса с матрицей L равносильно умножению координатной матрицы на L слева. Итак

$$(\omega)\,\Lambda = L\,(\omega).$$

Умножение справа на Λ^{-1}, слева на L^{-1} дает:

$$(\omega)\,\Lambda^{-1} = L^{-1}\,(\omega).$$

Переход в этом равенстве к матрицам, транспонированным к обратным, дает

$$(\overline{\omega})^{-1}\,\Lambda = \overline{L}\ (\overline{\omega})^{-1}.$$

Это равенство и содержит в себе доказываемое утверждение.

5. Кольца множителей для данной решетки и для взаимной решетки совпадают.

Действительно, в силу предыдущего свойства, каждая точка из кольца множителей для решетки S является точкой из кольца множителей для взаимной решетки S^*, ибо матрица $\overline{L}$ целочисленна вместе с L. Далее, каждая точка из кольца множителей для решетки S^* есть точка из кольца множителей для ее взаимной решетки, т. е. для S. Следовательно, кольца множителей для S и S^* совпадают.

Из последнего свойства вытекает, что если решетка S является идеалом для максимальной решетки O, то взаимная решетка S^* также является идеалом для O.

В частности, решетка O^* является идеалом для O, играющим весьма важную роль в теории алгебраических чисел.

Докажем несколько теорем, касающихся решеток, взаимных с идеалами максимального кольца.

Теорема 1. *Норма идеала* $\mathfrak{a}^*$ *равна*

$$\frac{1}{|D|N(\mathfrak{a})},$$

где D *— дискриминант максимальной решетки.*

Доказательство. По определению,

$$N(\mathfrak{a}) = \left|\frac{V(\mathfrak{a})}{V(O)}\right|,$$

где $V(\mathfrak{a})$ — объем основного параллелепипеда идеала $\mathfrak{a}$,
а $V(O)$ — объем основного параллелепипеда максимального кольца O.

Таким же образом

$$N(\mathfrak{a}^*) = \left|\frac{V(\mathfrak{a}^*)}{V(O)}\right|.$$

Из определения взаимной решетки с очевидностью следует, что

$$V(\mathfrak{a})\,V(\mathfrak{a}^*) = 1.$$

Следовательно,

$$N(\mathfrak{a})\,N(\mathfrak{a}^*) = \left|\frac{V(\mathfrak{a})\,V(\mathfrak{a}^*)}{[V(O)]^2}\right| = \frac{1}{D},$$

что и требовалось доказать.

Следствие.

$$N(O^*) = \frac{1}{D}.$$

Теорема 2. *След произведения любой точки* α *из* $\mathfrak{a}$ *на любую точку* α^* *из* $\mathfrak{a}^*$ *есть целое число. Обратно, любая точка* α^**, обладающая тем свойством, что след* $\alpha\alpha^*$ *есть целое число, при любом* α *из* $\mathfrak{a}$ *входит в* $\mathfrak{a}^*$.

Доказательство. Пусть $[a_1, a_2, \ldots, a_n]$ — базис идеала $\mathfrak{a}$, $[a_1^*, a_2^*, \ldots, a_n^*]$ — взаимный с ним базис идеала $\mathfrak{a}^*$. На основании определения взаимной решетки очевидно, что $S(a_i a_j^*) = 0$, если $i \neq j$, и равна 1, если $i = j$.

Пусть

$$\alpha = x_1a_1 + x_2a_2 + \ldots + x_na_n \text{ точка из } \mathfrak{a},$$
$$\alpha^* = y_1a_1^* + y_2a_2^* + \ldots + y_na_n^* \text{ точка из } \mathfrak{a}^*.$$

Числа $x_1, x_2, x_3, \ldots, x_n$ и $y_1, y_2, y_3, \ldots, y_n$ — целые рациональные. Тогда

$$S(\alpha\alpha^*) = x_1y_1 + x_2y_2 + \ldots + x_ny_n$$

есть целое рациональное число.

Обратно, пусть $S(\alpha^*\alpha)$ есть целое число при любом α из $\mathfrak{a}$, в частности при $\alpha = a_1, a_2, \ldots, a_n$. Тогда, представив α^* в виде

$$a_1^*y_1 + a_2^*y_2 + \ldots + a_n^*y_n,$$

получим, что

$$y_1 = S(\alpha^*\alpha_1), \quad y_2 = S(\alpha^*\alpha_2), \ldots, y_n = S(\alpha^*\alpha_n)$$

все целые рациональные числа и, следовательно,

$$\alpha^* = y_1\alpha_1^* + y_2\alpha_2^* + \ldots + y_n\alpha_n^*$$

принадлежит решетке $\mathfrak{a}^*$.

Следствие. Решетка O^* есть идеал, все точки которого имеют целые следы. Обратно, каждый идеал, обладающий этим свойством, входит в O^*. В частности, $O \subset O^*$ и, следовательно, $\mathfrak{D} = O^{*-1}$ есть целый идеал. Этот идеал называется дифферентой максимального кольца O. Норма дифферениты, на основании первой теоремы, равна дискриминанту максимального кольца O.

Теорема 3.

$$\mathfrak{a}\mathfrak{a}^* = O^*.$$

Доказательство. На основании первой теоремы,

$$N(\mathfrak{a}\mathfrak{a}^*) = N(\mathfrak{a}) \cdot N(\mathfrak{a}^*) = \frac{1}{|D|} = N(O^*).$$

С другой стороны, $\mathfrak{a}\mathfrak{a}^*$ есть *идеал*, все точки которого имеют целые рациональные следы. Следовательно,

$$\mathfrak{a}\mathfrak{a}^* \subset O.$$

На основании этого включения и равенства норм, заключаем, что

$$\mathfrak{a}\mathfrak{a}^* = O^*,$$

что и требовалось доказать.

Теорема 4. *Произведение дифференты любой точки максимальной решетки O на решетку O^* есть целый идеал.*

Дифферентой точки $(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(n)})$ называется точка с координатами

$$\begin{aligned}
&[(\lambda^{(1)} - \lambda^{(2)})(\lambda^{(1)} - \lambda^{(3)}) \ldots (\lambda^{(1)} - \lambda^{(n)}),\\
&(\lambda^{(2)} - \lambda^{(1)})(\lambda^{(2)} - \lambda^{(3)}) \ldots (\lambda^{(2)} - \lambda^{(n)}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&(\lambda^{(n)} - \lambda^{(1)})(\lambda^{(n)} - \lambda^{(2)}) \ldots (\lambda^{(n)} - \lambda^{(n-1)})].
\end{aligned}$$

Доказательство. Пусть λ — точка максимальной решетки; умножим ее на все точки ее базиса:

$$\begin{aligned}
\lambda\omega_1 &= l_{11}\omega_1 + l_{12}\omega_2 + \ldots + l_{1n}\omega_n,\\
\lambda\omega_2 &= l_{21}\omega_1 + l_{22}\omega_2 + \ldots + l_{2n}\omega_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\lambda\omega_n &= l_{n1}\omega_1 + l_{n2}\omega_2 + \ldots + l_{nn}\omega_n.
\end{aligned}$$

В виду того, что λ принадлежит решетке O, все числа $l_{i,k}$ будут целыми рациональными. Точка 1 принадлежит решетке. Следовательно,

$$1 = t_1\omega_1 + t_2\omega_2 + \ldots + t_n\omega_n$$

при целых рациональных $t_1, t_2, \ldots, t_n$. Рассмотрим точку μ_1, координата $\mu_1^{(1)}$ которой имеет вид:

$$\begin{vmatrix}
t_1, & t_2, & \ldots, & t_n\\
l_{21}, & l_{22} - \lambda^{(1)}, & \ldots, & l_{2n}\\
\ldots & \ldots & \ldots & \ldots\\
l_{n1}, & l_{n2}, & \ldots, & l_{nn} - \lambda^{(1)}
\end{vmatrix}$$

а остальные выражаются через $\lambda^{(2)}, \ldots, \lambda^{(n)}$, так же как $\mu_1^{(1)}$ через $\lambda^{(1)}$. Точка μ_1 принадлежит решетке O, ибо λ ей принадлежит, а все $l_{i,k}$ и t_i — целые рациональные числа.

Умножим скалярно μ_1 на объем основного параллелепипеда решетки O. Получим, по правилу умножения определителей:

$$\begin{vmatrix} t_1, & t_2, & \dots, & t_n \\ l_{21}, & l_{22}-\lambda^{(1)}, & \dots, & l_{2n} \\ \dots & \dots & \dots & \dots \\ l_{n1}, & l_{n2}, & \dots, & l_{nn}-\lambda^{(1)} \end{vmatrix} \cdot \begin{vmatrix} \omega_1^{(1)}, & \omega_1^{(2)}, & \dots, & \omega_1^{(n)} \\ \omega_2^{(1)}, & \omega_2^{(2)}, & \dots, & \omega_2^{(n)} \\ \dots & \dots & \dots & \dots \\ \omega_n^{(1)}, & \omega_n^{(2)}, & \dots, & \omega_n^{(n)} \end{vmatrix} =$$

$$= \begin{vmatrix} t_1\omega_1^{(1)}+t_2\omega_2^{(1)}+\dots+t_n\omega_1^{(1)}, & t_1\omega_1^{(2)}+t_2\omega_2^{(2)}+\dots+t_n\omega_n^{(2)}, \\ l_{21}\omega_1^{(1)}+l_{22}\omega_2^{(1)}+\dots+l_{2n}\omega_1^{(1)}-\lambda\omega_1^{(1)}, & l_{21}\omega_1^{(2)}+\quad+\dots+l_{2n}\omega_n^{(2)}-\lambda\omega_n^{(2)}, \\ \dots\dots\dots\dots\dots\dots & \dots\dots\dots\dots\dots\dots \\ l_{n1}\omega_1^{(1)}+l_{n2}\omega_2^{(1)}+\dots+l_{nn}\omega_n^{(1)}-\lambda\omega_n^{(1)}, & l_{n1}\omega_1^{(2)}+\quad+\dots+l_{nn}\omega_n^{(2)}-\lambda\omega_n^{(2)}, \end{vmatrix}$$

$$\begin{vmatrix} t_1\omega_1^{(n)}+t_2\omega_2^{(n)}+\dots+t_n\omega_n^{(n)} \\ l_{21}\omega_1^{(n)}+\dots\quad+l_{2n}\omega_n^{(n)}-\lambda\omega_2^{(n)} \\ \dots\dots\dots\dots\dots\dots \\ l_{n1}\omega_1^{(n)}+\dots\quad+l_{nn}\omega_n^{(n)}-\lambda\omega_n^{(n)} \end{vmatrix} =$$

$$= \begin{vmatrix} 1, & 1, & \dots & 1 \\ 0, & \omega_2^{(2)}(\lambda^{(2)}-\lambda^{(1)}), & \dots & \omega_2^{(n)}(\lambda^{(n)}-\lambda^{(1)}) \\ \dots & \dots & \dots & \dots \\ 0, & \omega_n^{(2)}(\lambda^{(2)}-\lambda^{(1)}) & \dots & \omega_n^{(n)}(\lambda^{(n)}-\lambda^{(1)}) \end{vmatrix} =$$

$$= (\lambda^{(2)}-\lambda^{(1)})\dots(\lambda^{(n)}-\lambda^{(1)}) \cdot \begin{vmatrix} \omega_2^{(2)}, & \dots & \omega_2^{(n)} \\ \dots & \dots & \dots \\ \omega_n^{(2)}, & \dots & \omega_n^{(n)} \end{vmatrix}.$$

Поделив снова на объем, получим

$$\mu_1^{(1)} = (\lambda^{(2)}-\lambda^{(1)})\dots(\lambda^{(n)}-\lambda^{(1)})\,\omega_1^{*(1)},$$

где ω_1^* есть первая точка базиса взаимной решетки O^* с решеткой O.

Взяв

$$\mu_2 = \begin{vmatrix} l_{11}-\lambda, & l_{12}, & \dots & l_{1n} \\ t_1, & t_2, & \dots & t_n \\ \dots & \dots & \dots & \dots \\ l_{n1}, & l_{n2}, & \dots & l_{nn}-\lambda \end{vmatrix},$$

получим

$$\mu_2^{(1)} = (\lambda^{(2)}-\lambda^{(1)})\dots(\lambda^{(n)}-\lambda^{(1)})\,\omega_2^{*(1)},$$

и т. д.

Таким образом, произведения дифференты точки λ на все точки базиса решетки O^* суть точки $\mu_1, \mu_2, \dots \mu_n$, принадлежащие решетке O. Следовательно, произведение дифференты λ на O^* есть целый идеал, что и требовалось доказать.

Теорема 4 может быть иначе сформулирована следующим образом: *Дифференты всех точек максимального кольца O делятся на дифференту самого кольца O.*

В заключение отметим некоторые свойства разложимых форм, соответствующих некоторой решетке S и ее взаимной S^*. Нормализовав решетки S и S^*, в смысле предыдущего параграфа, мы получим для них целочисленные разложимые формы одинакового дискриминанта, равного дискриминанту их общего кольца множителей. Такую разложимую форму для решетки S^* мы будем называть формой Кэли для решетки S.

Из свойств взаимных решеток вытекают следующие свойства формы Кэли:

1. Форма Кэли для формы Кэли есть исходная форма.

2. Если разложимую форму подвергнуть линейному преобразованию, то форма Кэли подвергнется контравариантному преобразованию.

Для трехмерных решеток форма Кэли в нашем смысле лишь постоянным множителем отличается от формы, известной в литературе под названием контравариантa Кэли.

ПРИЛОЖЕНИЕ

НЕКОТОРЫЕ ВСПОМОГАТЕЛЬНЫЕ ЛЕММЫ О РЕШЕТКАХ В ВЕЩЕСТВЕННОМ ЭВКЛИДОВОМ ПРОСТРАНСТВЕ

Под суммой (разностью) двух точек n-мерного вещественного эвклидова пространства R_n мы будем понимать точку, каждая из декартовых прямоугольных координат которой есть сумма (разность) соответственных координат складываемых (вычитаемых) точек. Мы будем говорить, что система точек повторяется сложением, если сумма или разность любых двух ее точек является также ее точкой. Так как прибавление точки ко всем точкам системы эквивалентно параллельному переносу системы, то такую систему можно также называть параллельно-переносной. Систему точек мы называем дискретной, если существует такое, не равное нулю, расстояние r, что никакие две точки рассматриваемой системы не лежат друг от друга ближе, чем на расстоянии r. Параллелепипедальной системой точек, или точечной решеткой, или просто решеткой, как мы будем говорить дальше, мы называем систему всех точек, имеющих целые рациональные координаты по отношению к некоторой системе n некомпланарных векторов, которую мы рассматриваем как координатную. Этот n-векторник мы называем основным n-векторником рассматриваемой параллелепипедальной системы, а построенный на этих векторах параллелепипед основным ее параллелепипедом.

Лемма I. *Всякая дискретная система точек, повторяющаяся сложением и вычитанием, есть решетка.*

Пусть дана дискретная система точек E, повторяющаяся сложением и вычитанием. Предположим, что все точки E лежат в R_n в m-мерной плоскости, но не лежат все одновременно в одной $(m-1)$-мерной плоскости.

Тогда в E есть m точек $A, B, C, \ldots, L$, которые лежат m-мерно с началом координат O (которое мы будем считать точкой системы), и все другие точки E лежат в m-мерной плоскости R_m, определяемой этими точками. Пусть $\bar{A}$ — ближайшая к O точка E, принадлежащая отрезку OA (такая точка существует, так как в области любого ограниченного диаметра в R_m лежит лишь ограниченное число точек E, потому что, если описать вокруг всех точек, как вокруг центров, шары радиусов $\frac{r}{2}$, то, в силу условия дискретности, шары эти не будут входить друг в друга). Если A — ближайшая такая точка, то мы возьмем за точку $\bar{A}$ саму точку A. Пусть $\bar{B}$ — ближайшая к прямой $O\bar{A}$ точка E, принадлежащая параллелограмму $O\bar{A}B$. Если такой точкой будет сама точка B, мы возьмем за $\bar{B}$ точку B. Пусть $\bar{C}$ — ближайшая к плоскости $O\bar{A}\bar{B}$ точка, принадлежащая параллелепипеду $O\bar{A}\bar{B}C \ldots L$, и т. д. В силу повторяемости E сложением, все вершины параллелепипеда $O\bar{A}\bar{B}\bar{C} \ldots \bar{L}$ суть точки E, а в силу выбора точек $\bar{A}, \bar{B}, \ldots, \bar{L}$, никакая другая точка E не лежит ни внутри этого параллелепипеда, ни на его границе. Построим на параллелепипеде $O\bar{A}\bar{B} \ldots \bar{L}$ параллелепипедальную систему точек и обозначим ее через $\bar{E}$. В силу повторяемости системы E сложением и вычитанием, все точки $\bar{E}$ принадлежат системе E, но никаких других точек в системе E быть не может. Действительно, если бы внутри или на границе какого-нибудь из параллелепипедов $\bar{E}$, гомологичных параллелепипеду $O\bar{A}\bar{B} \ldots \bar{L}$ (мы называем две фи-

гуры гомологичными друг другу по отношению к данной решетке $\bar{E}$ тогда, когда одна из них получается из другой параллельным переносом на вектор $\bar{E}$, т. е. на вектор, соединяющий две точки этой решетки), была точка E, то, в силу повторяемости системы E сложением и вычитанием, какая-нибудь точка E лежала бы внутри или на границе (не в вершине) параллелепипеда $O\bar{A}\bar{B}\ldots\bar{L}$, чего нет.

Лемма II. *Объемы всех основных параллелепипедов данной решетки одинаковы.*

Предположим теперь, что $m = n$. И будем предполагать это же и во всем дальнейшем. Пусть $OAB\ldots L$ — основной n-векторник решетки и $OA'B'\ldots L'$ — некоторый другой ее n-векторник, т. е. $A', B', \ldots, L'$ — точки этой решетки. В таком случае координаты точек $A', B', \ldots, L'$ относительно основного n-векторника этой решетки $OAB\ldots L$ — целые рациональные числа. Объем n-векторника $OA'B'\ldots L'$ больше объема n-векторника $OAB\ldots L$, как это следует из геометрии матриц, в Δ раз, где Δ — определитель из этих координат. Объем всякого n-векторника решетки, следовательно, больше объема основного ее n-векторника в целое число раз. Если $OA'B'\ldots L'$ — основной n-векторник рассматриваемой решетки, то объемы этого n-векторника и n-векторника $OAB\ldots L$ получаются каждый из другого умножением на целое число, что может быть, только если они равны.

Мы будем говорить, что мы центрируем решетку, если мы добавляем так новые точки в пространство R_n, в котором она лежит, чтобы они вместе с точками заданной решетки образовали в R_n опять решетку, но уже, конечно, более густую. (Термин этот взят из кристаллографии, где играют большую роль три специальные центрировки: добавление одной точки в центре каждого параллелепипеда, из которых составлена решетка; добавление по одной точке в центры всех граней этих параллелепипедов и добавление по одной точке в центры обоих оснований каждого из этих параллелепипедов. Как легко убедиться, такие добавления точек превращают решетку опять в решетку и сгущают ее соответственно в 2, 4 и 2 раза. Получаемые три решетки называются по отношению к исходной: просто центрированной, центрогранной и базоцентрированной).

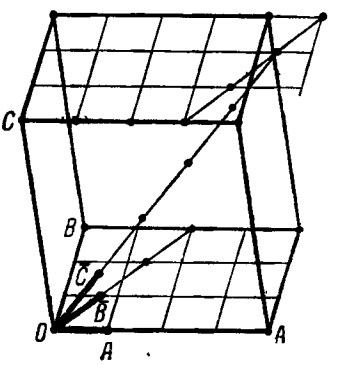
Лемма III. *Число различных центрировок решетки с данным индексом δ ограничено.*

Индексом центрировки называется число $\delta = \frac{1}{\Delta}$, на которое надо помножить объем основного параллелепипеда данной решетки, чтобы получить объем основного параллелепипеда центрировки. Самую решетку, получаемую после центрировки, мы будем, для краткости, называть центрировкой заданной решетки. Индекс центрировки всегда, очевидно, равен единице, делению на целое рациональное число, как это следует из параллельной переносности полученной параллелепипедальной системы. В каждом основном параллелепипеде заданной решетки одно и то же число добавленных точек, $\Delta = \frac{1}{\delta}$, равное числу точек, добавленных в один параллелепипед, увеличенному на 1. В виду того, что дать способ находить все центрировки с данным индексом и вывести точную формулу их числа не многим труднее, чем лишь доказать конечность их числа, мы сделаем первое.

Заметим прежде всего, что точки $\bar{A}, \bar{B}, \ldots, \bar{L}$ леммы I имеют координаты

$$\begin{array}{l}(x_{11}\ 0\ \ 0\ \ \ldots 0)\\ (x_{21}\ x_{22}\ 0\ \ \ldots 0)\\ (x_{31}\ x_{32}\ x_{33}\ \ldots 0)\\ \cdots\cdots\cdots\\ (x_{n1}\ x_{n2}\ \ \ldots\ x_{nn})\end{array}$$

относительно основного n-векторника $OAB\ldots L$. Рассматривая решетку $\overline{E}$ как центрировку решетки E, построенной на n-векторнике $OAB\ldots L$, и обозначив целое число, обратное индексу δ этой центрировки, которое показывает, во сколько раз объем параллелепипеда $O\overline{A}\overline{B}\ldots\overline{L}$ меньше объема параллелепипеда $OAB\ldots L$, через Δ, мы видим, что $\Delta=\Delta_1\cdot\Delta_2\cdot\ldots\cdot\Delta_n$, где Δ_1 — положительное целое рациональное число, показывающее, во сколько раз точка $\overline{A}$ ближе к O, чем точка A, Δ_2 — положительное целое рациональное число, показывающее, во сколько раз точка $\overline{B}$ ближе к прямой $O\overline{A}$, чем точка B, и т. д. Что числа $\Delta_1, \Delta_2, \ldots, \Delta_n$ — положительные целые рациональные, следует просто из того, что все точки $\overline{E}$, лежащие на прямой $O\overline{A}$, имеют все координаты свои относительно n-векторника $O\overline{A}\overline{B}\ldots\overline{L}$ равные нулю, кроме первой, и если точка A параллелепипедальной системы E, лежащая на прямой $O\overline{A}$, имеет координату эту равную Δ_1, то Δ_1 — целое рациональное число и т. д. Кроме того, мы видим, что $x_{11}=\frac{1}{\Delta_1}$, $x_{22}=\frac{1}{\Delta_2}$, $\ldots$, $x_{nn}=\frac{1}{\Delta_n}$. Итак, всякой центрировке с индексом Δ соответствует вполне определенное (принимается во внимание и порядок) разложение Δ на целые положительные множители, причем некоторые из них могут быть равны и 1. Пусть взято одно из таких разложений, т. е. зафиксированы числа Δ_1, $\Delta_2, \ldots, \Delta_n$. Как это видно из черт. 1, где взято $\Delta_1=4$, $\Delta_2=3$, $\Delta_3=5$ (т. е. $\Delta=60$), вектор $O\overline{B}$, увеличенный в Δ_2 раз, имеет конец B' в целой точке $\overline{E}$, лежащей на ребре основания центрируемого параллелепипеда $OAB\ldots L$, противоположном OA, а вектор $O\overline{C}$, увеличенный в Δ_3 раз, имеет конец свой C' в целой точке плоскости основания центрируемого параллелепипеда, противоположного OAB, и т. д. Пусть точка B' на ребре BB' достигается из точки B прибавлением γ_{21} раз вектора $O\overline{A}$, а точка C' на плоскости верхнего основания центрируемого параллелепипеда достигается из точки C прибавлением γ_{31} раз вектора $O\overline{A}$ и γ_{32} раз вектора $O\overline{B}$, и т. д. Тогда очевидно, что координаты точек $\overline{A}, \overline{B}, \overline{C}\ldots$ по отношению к n-векторнику $OAB\ldots L$ получаются по следующему правилу: по диагонали надо написать числа $\frac{1}{\Delta_1}$, $\frac{1}{\Delta_2}, \ldots, \frac{1}{\Delta_n}$, над диагональю нули, и затем справа от вычисляемой квадратной матрицы — колонки чисел $\gamma_{21}; \gamma_{31}; \gamma_{32}; \gamma_{41}; \gamma_{42}; \gamma_{43}; \ldots$; причем числа этих колонок можно предполагать неотрицательными и меньшими, чем соответственно $\Delta_2, \Delta_3, \Delta_4\ldots$; тогда каждой такой записи однозначно соответствует определенная центрировка с разложением $\Delta_1\cdot\Delta_2\cdot\ldots\cdot\Delta_n$, и обратно.



Черт. 1.

$$\left(\begin{array}{ccccc} \frac{1}{\Delta_1} & & & & \\ & \frac{1}{\Delta_2} & & & \\ & & \frac{1}{\Delta_3} & & \\ & & & \ddots & \\ & & & & \frac{1}{\Delta_n} \end{array}\right) \begin{array}{l} \gamma_{21}\,\gamma_{31}\,\gamma_{41}\cdots\gamma_{n1} \\ \quad\gamma_{32}\,\gamma_{42}\cdots\gamma_{n2} \\ \qquad\gamma_{43}\cdots\gamma_{n3} \\ \qquad\quad\cdots \\ \qquad\qquad\gamma_{n(n-1)} \end{array}$$

Для вычисления координат точек $\overline{B}, \overline{C}, \ldots, \overline{L}$, стоящих под диагональю, надо поступать так: сначала вычислить координату $\overline{B}$, затем, когда она уже получена, вычислять координаты $\overline{C}$ и т. д., составляя их как линейные комбинации уже имеющихся в матрице соответственных координат, коэффициентами которых служат числа колонки, и деля на соответственное Δ_i.

Пример:

$$\begin{pmatrix} \frac{1}{4} & & & \\ \frac{1}{6} & \frac{1}{3} & & \\ \frac{13}{60} & \frac{2}{15} & \frac{1}{5} & \\ \frac{53}{180} & \frac{7}{45} & \frac{1}{15} & \frac{1}{3} \end{pmatrix} \begin{matrix} 2\ 3\ 2 \\ 2\ 1 \\ 1 \end{matrix} \qquad \frac{2\cdot\frac{1}{4}}{3}=\frac{1}{6};\quad \frac{3\cdot\frac{1}{4}+2\cdot\frac{1}{6}}{5}=\frac{13}{60};\quad \frac{2\cdot\frac{1}{3}}{5}=\frac{2}{15};$$

$$\frac{2\cdot\frac{1}{4}+1\cdot\frac{1}{6}+1\cdot\frac{13}{60}}{3}=\frac{53}{180};\quad \frac{1\cdot\frac{1}{3}+1\cdot\frac{2}{15}}{3}=\frac{7}{45};\quad \frac{1\cdot\frac{1}{5}}{3}=\frac{1}{15}.$$

Число $I_{n,\Delta}$ всех возможных различных центрировок n-мерной решетки с индексом $\delta=\frac{1}{\Delta}$ равно, следовательно, $\Sigma\Delta_2\cdot\Delta_3^2\cdot\Delta_4^3\ldots\Delta_n^{n-1}$, где Σ распространена на все возможные различные разложения числа Δ на n множителей $\Delta_1, \Delta_2, \ldots, \Delta_n$, причем порядок множителей принимается во внимание. Например, $I_{3,6}=91$, так как $6=6\cdot1\cdot1=3\cdot2\cdot1=3\cdot1\cdot2=2\cdot3\cdot1=2\cdot1\cdot3=1\cdot6\cdot1=$ $=1\cdot1\cdot6=1\cdot2\cdot3=1\cdot3\cdot2$; $1\cdot1^2+2\cdot1^2+1\cdot2^2+3\cdot1^2+1\cdot3^2+6\cdot1^2+$ $+1\cdot6^2+3\cdot2^2+2\cdot3^2=1+2+4+3+9+6+36+12+18=91$.

Лемма III′. *Число различных подрешеток n-го измерения данной решетки n-го измерения с данным индексом Δ ограничено и равно также $I_{n,\Delta}$.*

Подрешеткой заданной решетки мы называем всякую решетку, которая есть часть заданной решетки. Если решетка E_2 есть подрешетка решетки E_1, то решетка E_1 есть центрировка решетки E_2. Индексом подрешетки мы опять называем число δ, на которое надо помножить объем основного параллелепипеда заданной решетки, чтобы получить объем основного параллелепипеда рассматриваемой подрешетки.

Индекс δ подрешетки есть, в силу сказанного в лемме II, всегда целое рациональное число Δ. В виду того, что заданная решетка E_1 может рассматриваться как центрировка рассматриваемой ее подрешетки E_2 с индексом $\frac{1}{\Delta}$ и что, если разные подрешетки с индексом Δ аффинно преобразовать в одну и ту же решетку, то данная решетка, очевидно, преобразуется в разные центрировки этой решетки с индексом $\frac{1}{\Delta}$ (так как иначе обратные преобразования не могли бы дать разных подрешеток), то число различных подрешеток с индексом Δ равно $I_{n,\Delta}$.

Лемма III″. *Число различных n-мерных решеток, рациональных по отношению к данной n-мерной решетке данного индекса, с заданным знаменателем, ограниченно.*

Мы называем решетку рациональной по отношению к данной решетке, если координаты всех n основных ее точек (а следовательно и всех вообще ее точек) по отношению к основному n-векторнику заданной решетки рациональны. Как любая подрешетка данной решетки, так и любая ее центрировка есть решетка, рациональная по отношению к данной решетке, но рациональная решетка по отношению к данной решетке может не быть ни ее подрешеткой, ни ее центрировкой.

Индексом такой решетки мы называем опять число δ, на которое надо умножить объем основного параллелепипеда заданной решетки, чтобы получить объем основного параллелепипеда этой решетки. В этом случае индекс может быть любым целым или дробным числом. Знаменателем Q такой решетки мы называем общий знаменатель всех координат всех n основных (а следовательно и вообще всех) точек этой решетки, взятых по отношению к основному n-стороннику заданной решетки. Все решетки, рациональные по отношению к заданной решетке с данным знаменателем Q, суть, очевидно, подрешетки

той центрировки заданной решетки с индексом $\delta = \frac{1}{Qn}$, которая получается, если просто уменьшить каждый из основных векторов заданной решетки в Q раз. Если рациональная по отношению к заданной решетке решетка с знаменателем Q имеет по отношению к ней индекс δ, то индекс ее по отношению к рассмотренной решетке, линейно в Q раз меньшей, чем заданная, есть целое число и равен $\delta_1 = \frac{Qn}{\delta}$, и, следовательно, число разных таких решеток не больше, чем I_{n,δ_1}. Вообще говоря, это число меньше, так как некоторые из таких центрировок могут иметь по отношению к заданной уже знаменателем не Q, а какого-нибудь делителя Q.

В виду того, что знаменатели Q — числа целые рациональные, из ограниченности числа различных решеток, рациональных по отношению к данной с данным индексом и данным знаменателем, следует ограниченность этого числа при данном индексе и лишь ограниченном знамеиателе.

Лемма IV. *Пусть R_1 и R_2 — две рационально связанные n-мерные решетки. Обозначим через $T=[R_1, R_2]$ пересечение этих решеток, т. е. совокупность всех общих точек. Через $S=(R_1, R_2)$ обозначим объединение решеток R_1 и R_2, т. е. совокупность всех точек R_1 и R_2 и их сумм. Тогда индекс, с которым решетка R_1 центрирует T, равен индексу, с которым решетка S центрирует R_2.*

Доказательство. Прежде всего убедимся в том, что S и T представляют собой решетки. Обе эти совокупности, очевидно, повторяются сложением и вычитанием. Обозначим через N общий знаменатель коэффициеитов, посредством которых базис решетки R_2 выражается через базис R_1; тогда $R_2 \subset \frac{1}{N} R_1$, $R_1 \subset NR_2$. Совокупность T n-мерна, ибо она содержит в себе n-мерную решетку NR_2. Совокупность T n-мерна, так как содержит n-мерные решетки R_1 и R_2. Совокупность T дискретна, так как она содержится в дискретных решетках R_1 и R_2. Совокупность S дискретна, так как оиа содержится в решетке $\frac{1}{N} R_1$. В силу леммы I, обе совокупности S и T суть решетки. Назовем две точки иекоторой решетки сравнимыми по подрешетке, если их разность приналлежит этой подрешетке, и не сравнимыми — в обратном случае. Совокупность точек решетки, попарно не сравнимых по подрешетке, но таких, что каждая точка решетки сравнима с одной из них, назовем полиой системой вычетов решетки по подрешетке. Примером полной системы вычетов может служить совокупность всех точек решетки, лежаших внутри и на негомологичных частях границы основного параллелепипеда подрешетки. Число точек, образующих полную систему вычетов, очевидно, равно индексу, с которым решетка центрирует подрешетку.

Для доказательства нашей леммы сравним полную систему вычетов решетки R_1 относительно T и решетки S относительно R_2.

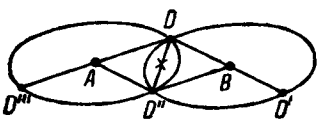
Пусть $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ — полная система вычетов решетки R_1 относительно T. Докажем, что она является также полной системой вычетов S относительно R_2. Для этого нужно доказать три вещи: во-первых, что точки $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ принадлежат S, во-вторых, что они попарно иесравнимы по R_2, и, наконец, что каждая точка решетки S сравнима с одною из точек $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ по решетке R_2.

Первое очевидио, так как все точки решетки R_1, в том числе и $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, принадлежат решетке S.

Допустим теперь, что $\alpha_i \equiv \alpha_j \pmod{R_2}$ при $i \neq j$. Тогда разность $\alpha_i - \alpha_j$ принадлежит одновременно и решетке R_2 и решетке R_1, а следовательно, и их пересечению T, что противоречит тому, что $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ — полиая система вычетов по решетке T. Таким образом, точки $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ попарно не сравнимы по решетке R_2. Пусть теперь σ — какая-либо точка решетки S.

Очевидно, что σ может быть представлено в виде $\sigma = \alpha + \beta$, где α — точка из R_1, β — точка из R_2, и следовательно $\sigma \equiv \alpha\ (R_2)$. Но $\alpha \equiv \alpha\ (T)$, ибо $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ есть полная система вычетов решетки R_1 относительно T, а следовательно $\sigma - \alpha_i = (\sigma - \alpha) + (\alpha - \alpha_i)$ принадлежит решетке R_2', ибо и $\sigma - \alpha$ и $\alpha - \alpha_i$ принадлежат R_2. Итак, $\sigma \equiv \alpha_i\ (R_2)$ и, следовательно, $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ есть действительно полная система вычетов решетки S относительно R_2. В виду того, что решетки R_1 относительно T и решетки S относительно R_2 имеют одинаковые полные системы вычетов, индексы центрировки R_1 относительно T и S относительно R_2 одинаковы,— что и требовалось доказать.

Лемма V (Минковского). *Выпуклое тело с центром в точке решетки, объем которого более чем в 2^n раз превосходит объем основного параллелепипеда решетки, имеет внутри себя по крайней мере две (симметричные друг другу относительно центра) точки решетки.*



Черт. 2.

Тело называется выпуклым, если вместе с любыми двумя его точками ему же принадлежит и любая точка соединяющего эти точки отрезка. Точка O называется центром тела, если вместе с любой точкой тела ему же принадлежит и точка, ей симметричная по отношению к точке O, т. е. такая, что O является серединой отрезка, соединяющего обе точки.

Пусть имеется выпуклое тело M, имеющее центр в точке O решетки E и такое, что оно не содержит никаких других точек E ни внутри себя, ни на своей границе. Уменьшим это тело M линейно вдвое, стянув его гомотетично к точке O, и обозначим уменьшенное тело через M_1. Построим тела, равные и параллельные M_1, вокруг всех точек E как центров. Такие тела M_1 не будут иметь общих точек, так как если бы такие два тела с центрами в точках A и B решетки имели общую точку, то,— в силу того, что они выпуклы, имеют центры симметрии в точках A и B, равны и параллельно расположены,— и середина C отрезка AB была бы их общей точкой. Действительно, из того, что точка D есть общая точка этих двух тел, следует, что точка D' есть точка тела B, а следовательно точка D'' есть точка тела A; аналогично следует, что точка D''' есть точка тела A, а, следовательно, точка D'' есть точка тела B. Итак точка D'' — тоже общая точка обоих тел, но тогда и точка C, являющаяся серединой отрезка DD'', а следовательно и серединой отрезка AB, есть, в силу выпуклости тел A и B, общая точка этих тел.

Объемы тел M_1, следовательно, не больше объема основного параллелепипеда.

Итак, если выпуклое тело M с центром в некоторой точке O решетки E не имеет ни внутри, ни на границе, кроме центральной, ни одной другой точки решетки E, то объем его не больше, чем 2^n раз взятый объем основного параллелепипеда решетки E.

Следовательно, если объем выпуклого тела M' более чем в 2^n раз превышает объем основного параллелепипеда решетки, то внутри тела M' найдутся по крайней мере две точки решетки, кроме центра O.

ГЛАВА II

НЕКОТОРЫЕ ВЫЧИСЛЕНИЯ ДЛЯ КУБИЧЕСКИХ ЧИСЕЛ

§ 10. Кубическое поле, преобразование Чирнгаузена, целые числа поля

Пусть числа s, q, n — целые рациональные, и уравнение

$$x^3 = sx^2 + qx + n \tag{1}$$

ие имеет целого рационального кория, т. е. никакой из делителей его постоянного члена не есть его корень. Тогда оно иеприводимо в абсолютном рациональном поле и его корни ρ, ρ', ρ'' называются кубическими числами. Если коэффициенты уравиения не целые, а только рациональные, то всегда можно найти такое целое рациональное число k, что при умножении этих коэффициентов соответствеино на k, k^2, k^3 получатся уже числа целые; этому помножению соответствует увеличение корней в k раз, и, таким образом, со всяким уравнением вида (1) с дробными рациональными коэффициентами тесно связано такое же уравнение с целыми рациональными коэффициентами.

В рассматриваемом случае, когда уравнение (1) неприводимо, совокупность всех чисел ω, которые являются рациональными функциями от одного из его корней, например от ρ (т. е. получаются из ρ комбинированием ρ самого с собой ограниченным числом действий сложения, вычитания, умножения и деления), образует так иазываемое поле кория ρ и обозначается Ω_ρ. Очевидно, что комбинация любого ограниченного числа чисел поля при помощи ограниченного числа действий сложеиия, вычитания, умножения и деления (кроме деления иа нуль), есть опять число поля. Поля

$$\Omega_\rho, \quad \Omega_{\rho'}, \quad \Omega_{\rho''},$$

вообще говоря, различны.

Всякая рациональная функция от ρ может быть, как известно, после избавления дроби от многоэтажности, понижения полиномов от ρ, стоящих в числителе и зиаменателе, до 2-ой степени, путем деления на $\rho^3 - s\rho^2 - q\rho - n$ и избавления от иррациоиальности в знамеиателе, приведена к виду:

$$\omega = \frac{u\rho^2 + v\rho + w}{\Delta}, \tag{2}$$

где числа u, v, w, Δ — целые рациональные. Практическое правило для освобождения от иррациональности в знаменателе, основанное на способе неопределенных коэффициентов, будет дано дальше.

Легко видеть, что если предполагать целые числа u, v, w, Δ ие имеющими общего делителя, то число ω может быть только одним способом представлено в виде (2), так как два различные представления (2), приравненные друг другу, дали бы уравнение 2-ой степени, которому должно было бы удовлетворять ρ, чего быть не может, так как ρ удовлетворяет, по предположению, неприводимому уравнению 3-ей степени (1).

Поле Ω_ρ есть, следовательно, не что иное, как совокупность всех чисел вида (2).

Нетрудно составить уравненне 3-ей степенн, которому удовлетворяет число $z = u\rho^2 + v\rho + w = \varphi(\rho)$, т. е. произвести так называемое *преобразование Чирнгаузена*. Действительно, для этого достаточно написать z, $z\cdot\rho$, $z\cdot\rho^2$, пониженные до 2-ой степени относительно ρ, и затем написать, что определитель, составленный из коэффициентов при $1, \rho, \rho^2$, равен нулю.

Пример. Пусть $\rho^3 = \rho + 1$, и требуется составить уравнение, которому удовлетворяет $z = 2\rho^2 + 3\rho + 1$. Пишем

$$\left.\begin{aligned} z &= 2\rho^2 + 3\rho + 1 \\ z\cdot\rho &= 3\rho^2 + \rho + 2(\rho+1) = 3\rho^2 + 3\rho + 2 \\ z\cdot\rho^2 &= 3\rho^2 + 2\rho + 3(\rho+1) = 3\rho^2 + 5\rho + 3 \end{aligned}\right\},$$

откуда:

$$\begin{vmatrix} z-1, & -3, & -2 \\ -2, & z-3, & -3 \\ -3, & -5, & z-3 \end{vmatrix} = 0$$

или, раскрывая этот определитель, лучше по Саррюсу, получаем:

$$(z^2 - 6z + 9)(z-1) - 27 - 20 - 6(z-3) - 6(z-3) - 15(z-1) = 0,$$

т. е. окончательно:

$$z^3 - 7z^2 - 27z - 5 = 0.$$

Если коэффициенты преобразуемого уравнения (1) и преобразующей функции $\varphi(\rho)$ — целые, то и коэффициенты преобразованного уравнения — тоже целые. Уравнение, которому удовлетворяет ω, получается из уравнення, которому удовлетворяет z, путем делення его коэффициентов на $\Delta, \Delta^2, \Delta^3$. Если они разделятся, то уравнение, которому удовлетворяет ω, будет иметь тоже целые коэффициенты. Числа поля Ω_ρ, удовлетворяющие уравнениям вида (1) с целыми рациональными коэффициентами s, q, n, так называемым целым уравнениям, называются целыми числами поля. Очевидно, что если само ρ — целое число, то все числа вида (2), у которых $\Delta = \pm 1$, — целые. Однако может быть, как легко видеть, что знаменатель Δ числа ω не равен ± 1 и тем не менее число это целое, в виду только что указанной возможности, что коэффициенты того уравнения, которому удовлетворяет $z = u\rho^2 + v\rho + w$, окажутся делимыми на $\Delta, \Delta^2, \Delta^3$.

Корни уравнения, получаемого из (1) преобразованнем Чирнгаузена $z = u\rho^2 + u\rho + w$, суть

$$z = u\rho^2 + v\rho + w; \quad z' = u\rho'^2 + v\rho' + w; \quad z'' = u\rho''^2 + v\rho'' + w.$$

Если бы уравнение это вышло приводимым, то один из его корней оказался бы рациональным числом r. Пусть, например, $u\rho'^2 + v\rho' + w = r$; тогда, вследствие однозначности формы (2), должно быть $u = v = 0$; $w = r$. Таким образом $z = w$, и уравненне, которому удовлетворяет z, имеет вид $(z-w)^3 = 0$. Итак, всякое число кубического поля либо удовлетворяет неприводимому уравнению 3-ей степеии, т. е. есть кубическое число, и тогда по крайней мере один из двух коэффициентов u, v не равен нулю, илн же оно рациональное число (это будет, если $u = v = 0$). Числа поля Ω_ρ, удовлетворяющие неприводимым уравнениям 3-ей степенн, называются примитивными числами поля.

Все примитивные числа поля выражаются друг через друга рационально, так что вместо исходного кубического числа ρ можно любое из них взять для образования того же кубического поля. Действительно, пусть z — примитивное число, и

$$z = u\rho^2 + v\rho + w, \tag{3}$$

$$z^2 = u_1\rho^2 + v_1\rho + w_1; \tag{4}$$

тогда $\begin{vmatrix} u & v \\ u_1 & v_1 \end{vmatrix} \neq 0$, так как иначе было бы $u_1 = \delta \cdot u$, $v_1 = \delta \cdot v$, где δ — целое или дробное рациональное число, и, следовательно, было бы $z^2 = \delta \cdot z + (w_1 - \delta w)$, т. е. z удовлетворяло бы, против предположения, уравнению с рацнональными коэффициентами ниже 3-ей степени. Но, если $\begin{vmatrix} u & v \\ u_1 & v_1 \end{vmatrix} \neq 0$, то из (3) и (4), как из двух уравнений 1-ой степени, можно найтн ρ рационально через z.

Пример. Выразить ρ через $z = 2\rho^2 + 3\rho + 1$, если $\rho^3 = \rho + 1$. Мы имеем $z^2 = 4\rho^4 + 9\rho^2 + 1 + 12\rho^3 + 4\rho^2 + 6\rho = 4(\rho + 1)^2 + 13\rho^2 + 6\rho + 1 + 12(\rho + 1) = 17\rho^2 + 26\rho + 17$, т. е. имеем для определения ρ систему:

$$\left.\begin{aligned} 3\rho + 2\rho^2 &= z - 1 \\ 26\rho + 17\rho^2 &= z^2 - 17 \end{aligned}\right\},$$

откуда $\rho = 2z^2 - 17z - 17$.

Совокупность всех целых чисел поля Ω_ρ образует кольцо, т. е. воспроизводится действиями сложения, вычитания и умножения. Действительно, пусть, например, $\omega_1 = \frac{u_1\rho^2 + v_1\rho + w_1}{\Delta_1}$; $\omega_2 = \frac{u_2\rho^2 + v_2\rho + w_2}{\Delta_2}$ — целые числа поля Ω_ρ. Составим уравнение:

$$F(x) = [x - (\omega_1 + \omega_2)][x - (\omega_1' + \omega_2')][x - (\omega_1'' + \omega_2'')], \tag{5}$$

где ω_1', ω_2'; ω_1'', ω_2'' — чнсла сопряженные с ω_1, ω_2, т. е. получаемые из них заменой в них ρ на ρ' и на ρ''. В силу теоремы о симметрических функциях, коэффициенты уравнення (5) как симметрические функции от S, S', S'' — рациональные. Составим теперь уравненне 9-ой степени:

$$F(x) = [x - (\omega_1 + \omega_2)][x - (\omega_1 + \omega_2')][x - (\omega_1 + \omega_2'')][x - (\omega_1' + \omega_2'')][x - (\omega_1' + \omega_2')]\cdot$$
$$\cdot[x - (\omega_1' + \omega_2'')][x - (\omega_1'' + \omega_2)][x - (\omega_1'' + \omega_2')][x - (\omega_1'' + \omega_2'')]. \tag{6}$$

Все коэффицненты этого уравнения целые рациональные и симметрические функции как от ω_1, ω_1', ω_1'', так и от ω_2, ω_2', ω_2'' и, следовательно, выражаются цело рационально через коэффициенты тех уравнений вида (1), которым удовлетворяют числа ω_1 и ω_2. Но, по предположению, числа эти целые, а, следовательно, и коэффициенты уравнения (6) целые. Итак, многочлен $F(x)$, старший коэффициент которого единица, а остальные — целые рациональные числа, делится на многочлен $F(x)$, старший коэффициент которого единица, а остальные коэффициенты которого рациональные числа; но тогда, по известной лемме Гаусса, коэффициенты $F(x)$ — все целые рациональные. Таким образом выходит, что, если ω_1 и ω_2 — целые числа поля Ω_ρ, то $\omega_1 + \omega_2$ — тоже целое число этого поля. Совершенно такое же доказательство для разности $\omega_1 - \omega_2$ и произведения $\omega_1 \cdot \omega_2$. Если целое число поля рационально, то оно — обыкновенное целое рациональное число, так как, как мы видели, уравнение, которому оно удовлетворяет, имеет вид $(x - w)^3 = 0$ и таким образом w^3, а следовательно и w, — целое.

§ 11. Действия сложения, вычитания, умножения, деления, возвышения в степень и извлечения корня для чисел кубического поля и вычисление их нормы и дискриминанта

Если $\omega_1 = u_1\rho^2 + v_1\rho + w_1$; $\omega_2 = u_2\rho^2 + v_2\rho + w_2$, то $\omega_1 \pm \omega_2 = (u_1 \pm u_2)\rho^2 + (v_1 \pm v_2)\rho + (w_1 \pm w_2)$. В произведение $\omega_1 \cdot \omega_2$ число ρ войдет в 3-ей и 4-ой степени, поэтому для быстрого выполнения умножений надо себе заготовить „понижающие тождества“, а именно, если

$$\rho^3 = s\rho^2 + q\rho + n,$$

то

$$\rho^4 = (s^2 + q)\rho^2 + (sq + n)\rho + sn.$$

Пользуясь этими тождествами, можно быстро выполнять умножения.

Пример. Пусть $\rho^3 = 3\rho^2 + \rho + 2$; тогда $\rho^4 = 10\rho^2 + 5\rho + 6$, и произведение вычисляется так, например:

$$\begin{aligned}(5\rho^2 + 2\rho - 1)(2\rho^2 - 3\rho + 2) &= 10(10\rho^2 + 5\rho + 6) + 4(3\rho^2 + \rho + 2) - 2\rho^2 - \\ &- 15(3\rho^2 + \rho + 2) - 6\rho^2 + 3\rho + 10\rho^2 + 4\rho - 2 = \\ &= 69\rho^2 + 46\rho + 36.\end{aligned}$$

Действие деления выполняется проще всего способом неопределенных коэффициентов, например:

$$\frac{5\rho^2 + 2\rho - 1}{2\rho^2 - 3\rho + 2} = A\rho^2 + B\rho + C,$$

откуда получаем:

$$\begin{aligned}&2A\rho^4 - 3A\rho^3 + 2A\rho^2 + \\ &+ 2B\rho^3 - 3B\rho^2 + 2B\rho^2 + \\ &+ 2C\rho^2 - 3C\rho + 2C = 5\rho^2 + 2\rho + 1\end{aligned}$$

или в силу понижающих тождеств:

$$\begin{aligned}&2A(10\rho^2 + 5\rho + 6) - 3A(3\rho^2 + \rho + 2) + 2A\rho^2 + \\ &+ 2B(3\rho^2 + \rho + 2) - 3B\rho^2 + 2B\rho + \\ &+ 2C\rho^2 - 3C\rho + 2C = 5\rho^2 + 2\rho + 1;\end{aligned}$$

сравнение коэффициентов при степенях ρ дает:

$$\left.\begin{aligned}13A + 3B + 2C &= 5 \\ 7A + 4B - 3C &= 2 \\ 6A + 4B + 2C &= -1\end{aligned}\right\},$$

и, следовательно, $A = \frac{121}{172}$; $B = -\frac{185}{172}$; $C = -\frac{79}{172}$.

Это вычисление является наиболее удобным для избавления от иррациональности в знаменателе.

Можно иначе производить деление, а именно, можно и числитель, и знаменатель помножить на множитель, „дополнительный" к знаменателю, т. е. на произведение двух чисел, кубически сопряженных с знаменателем, но для этого надо иметь готовую формулу этого множителя. Если число ω имеет вид $\omega = u\rho^2 + v\rho + w$, то дополнительный множитель

$$\begin{aligned}\omega'\omega'' = &(-u^2q + uvs - uw + v^2)\rho^2 + (u^2sq + u^2n - uvs^2 - v^2s - vw)\rho + \\ &+ (u^2q^2 - u^2sn - uvsq - uvn + uws^2 + 2uwq - v^2q + vws + w^2).\end{aligned}$$

Перейдем теперь к возвышению в степень. Если нужно возвышать кубическое число $\omega = u\rho^2 + v\rho + w$ в степень, например вычислить табличку последовательных степеней до какой-нибудь данной, то самое лучшее составить рекурсионную формулу, ведущую от ω^m к ω^{m+1}. Пусть, например: $\rho^3 = \rho^2 + 2\rho + 2$; $\omega = -\rho^2 + \rho + 3$. Мы имеем тогда $\rho^4 = 3\rho^2 + 4\rho + 2$, и, следовательно, если $\omega^m = A\rho^2 + B\rho + C$, то $\omega^{m+1} = (A\rho^2 + B\rho + C)(-\rho^2 + \rho + 3) = (A - C)\rho^2 + (-2A + B + C)\rho + (-2B + 3C)$. Получается такая табличка коэффициентов последовательных степеней:

m	A	B	C
1	— 1	1	3
2	— 4	6	7
3	—11	21	9
4	—20	52	— 15
5	— 5	77	—149
....	....	....	....
			и т. д.

Этот способ безусловно самый удобный, когда надо вычислять последовательные степени кубического числа. Существует, однако, и прямая формула, сразу позволяющая выписать коэффициенты любой требуемой степени, без необходимости вычислять все промежуточные. Действительно, пусть возвышаемое в сте-

пень число есть $\omega = u\rho^2 + v\rho + w$. Составим при помощи преобразования Чирнгаузена то уравнение $\omega^3 = S\omega^2 + Q\omega + N$, которому удолетворяет ω; тогда, если

$$\omega^m = U_m \cdot \omega^2 + V_m \cdot \omega + W_m, \tag{1}$$

то имеет место следующая формула:

$$U_m = \sum \frac{(\alpha+\beta+\gamma)!}{\alpha!\,\beta!\,\gamma!} \cdot S^\alpha \cdot Q^\beta \cdot N^\gamma; \tag{2}$$

сумма распространена на все неотрицательные целые числа α, β, γ, удовлетворяющие уравнению $\alpha + 2\beta + 3\gamma = m - 2$.

Доказательство этой формулы получается способом полной индукции.

Для того, чтобы вычислить V_m, W_m, достаточно заметить, что $\omega^{m+1} = (U_m S + V_m)\,\omega^2 + \ldots$; $\omega^{m+2} = [(U_m S + V_m)\,S + U_m Q + W_m]\,\omega^2 + \ldots$ (члены, не содержащие ω и содержащие ω в 1-ой степени, мы тут опустили), и, следовательно,

$$V_m = U_{m+1} - U_m \cdot S; \quad W_m = U_{m+2} - U_{m+1} \cdot S - U_m Q.$$

По этим формулам легко вычислить V_m, W_m, если U_m, U_{m+1}, U_{m+2} вычислены по формуле (2). Дальше останется только подставить в (1) выражение ω через ρ.

Что касается извлечения корня, то можно порекомендовать следующий прием.

Пусть

$$\omega^3 = S\omega^2 + Q\omega + N \tag{3}$$

— уравнение, которому удовлетворяет кубическое число ω, и пусть $\omega = \rho^k$, где ρ — также кубическое число, заданное уравнением

$$\rho^3 = s\rho^2 + q\rho + n. \tag{4}$$

Основные симметрические функции S, Q, N от корней уравнения (3) суть также симметрические функции от корней уравнения (4) и, следовательно, рационально выражаются через основные симметрические функции s, q, n. В частности, очевидно, $N = n^k$.

Выражения для S и Q сложнее, но они также без труда могут быть выписаны при каждом численно данном k.

Задача извлечения корня k-той степени из ω сводится к разысканию s, q, n по данным S, Q, N и k, т. е. к решению системы трех уравнений с тремя неизвестными, в том случае, когда эта система допускает рациональные решения, причем одно из уравнений системы решается сразу.

Очевидно, что задачу извлечения корня достаточно уметь решать лишь для простого показателя.

Рассмотрим прежде всего $k = 2$.

В этом случае

$$\left.\begin{aligned} S &= s^2 + 2q \\ Q &= 2sn - q^2 \\ N &= n^2 \end{aligned}\right\}. \tag{5}$$

Из последнего уравнения находим $n = \sqrt{N}$. Значение корня можно брать всегда со знаком $+$. При этом будет получаться то из двух значений $\sqrt{\omega}$, норма которого положительна.

Исключаем затем q из первых двух уравнений. Получим:

$$(s^2 - S)^2 - 8ns + 4Q = 0.$$

Рациональный корень этого уравнения, если таковой существует, принимаем за s и затем находим q из первого уравнения системы (5).

При исследовании задачи для других значений k ограничимся случаем *целых* рациональных S, Q, N. В этом случае s, q, n также должны быть целыми рациональными. Покажем, что решение системы уравнений для определения s и q сводится к конечному числу испытаний и сравнительно небольшому, как будет видно из примеров.

Пусть $k=p$ — нечетному простому числу. Выпишем систему уравнеиий для s и q:

$$\left.\begin{aligned}\Phi_p(s,q)&=S,\\ \Psi_p(s,q)&=Q.\end{aligned}\right\} \tag{6}$$

Рассмотрим затем число $1+\omega=1+\rho^p$. Это число при делеиии на $1+\rho$ дает в частном целое алгебраическое число. Следовательно, $N(1+\omega)$ делится на $N(1+\rho)$. Кроме того, легко видеть, что эти нормы должны иметь одинаковые знаки.

Точно так же, $N(1-\omega)$ должно делиться на $N(1-\rho)$ и иметь тот же знак. Выражая $N(1\pm\omega)$ и $N(1\pm\rho)$ через коэффициенты уравнений, которым удовлетворяют ω и ρ, получим:

$$\left.\begin{aligned}&1+S-Q+N \text{ делится на } 1+s-q+n \text{ и имеет тот же знак;}\\ &1-S-Q-N \text{ делится на } 1-s-q-n \text{ и имеет тот же знак.}\end{aligned}\right\} \tag{7}$$

Перебирая всевозможные делители для $1+S-Q+N$ и $1-S-Q-N$, получим конечное число возможностей для s и q, которые затем все должны быть испытаны подстановкой в (6).

Количество испытаний может быть уменьшено в силу следующих соображений.

Очевидно, что $N=n^p\equiv n \pmod p$ в силу известной теоремы Ферма. Покажем, что $S\equiv s \pmod p$.

Действительно, $S=\omega^p+\omega'^p+\omega''^p=(\omega+\omega'+\omega'')^p-p.A$, где A — симметрическая функция от $\omega, \omega', \omega''$ с целыми рациональными коэффициентами, так как все полиномиальные коэффициенты в разложении $(\omega+\omega'+\omega'')^p$ делятся на p. Следовательно, A — целое рациональное число и

$$S\equiv s^p \pmod p,$$

откуда следует, в силу теоремы Ферма:

$$S\equiv s \pmod p.$$

Тем же способом легко получить, что $Q\equiv q \pmod p$. Следовательно,

$$\left.\begin{aligned}1+s-q+n&\equiv 1+S-Q+N\\ 1-s-q-n&\equiv 1-S-Q-N\end{aligned}\right\} \pmod p. \tag{8}$$

Эти сравиения уменьшают число комбинаций значений s и q, которые должны быть подвергнуты испытанию.

В случае задачи об извлечении кубического корня система (6) превращается в

$$\begin{aligned}S&=s^3+3sq+3n,\\ Q&=q^3-3nsq-3n^2.\end{aligned}$$

Решение для этого случая облегчается, по сравнению с общим случаем, тем, что s является делителем $S-3n$ и q — делителем $Q+3n^2$. Следует отметить также соотношение $Q+nS=q^3+ns^3$, применение которого облегчает испытания.

Все приведенные выше соображения дают возможность решить в конечном числе действий также следующую задачу.

Дано целое кубическое число ω. Выяснить, является ли это число какой либо степенью другого кубического числа, и если да, то найти основание и показатель степени.

В самом деле, если $N \neq 1$, то показатель ограничивается сразу, ибо N должен быть полной степенью целого рационального числа с тем же показателем. Если $N = 1$, то можно прежде всего извлекать квадратный корень до тех пор, пока это возможно. После того как это будет проделано, показатель степени сможет делиться лишь на нечетные простые числа.

Из соображений делимости (7) мы получим конечное число комбинаций для s и q, и для каждой комбинации — конечное число возможных значений для показателя p. В самом деле, в силу сравнений (8) p должно входить в общий наибольший делитель $S - s$ и $Q - q$.

Поясним все сказанное примерами.

Пример 1.

$$\omega^3 = 22\omega^2 - 89\omega + 484. \text{ Найти } \sqrt{\omega}.$$

Прежде всего находим $n = \sqrt{484} = 22$.

Затем составляем систему:

$$s^2 + 2q = 22,$$
$$q^2 - 44s = 89.$$

Исключая q, получим

$$s^4 - 44s^2 - 176s + 128 = 0,$$

откуда находим $s = 8$, $q = 21$.

Следовательно, $\omega = \rho^2$, где ρ удовлетворяет уравнению

$$\rho^3 = 8\rho^2 - 21\rho + 22.$$

Пример 2. $\omega^3 = -6\omega^2 - 29\omega + 1$. Найти $\sqrt[3]{\omega}$.

Составляем систему (6), принимая во внимание, что $n = 1$

$$s^3 + 3sq = -9,$$
$$q^3 - 3sq = -26,$$

складывая получим

$$q^3 + s^3 = -35,$$

откуда $q + s = -1; -5; -7; -35$

Но $q + s \equiv q^3 + s^3 = -35 \equiv 1 \pmod 3$. Остаются возможности $q + s = -5$ и $q + s = -35$.

Первая приводит к решению задачи:

$$q = -2; \quad s = -3.$$

Следовательно, $\omega = \rho^3$, где $\rho^3 = -3\rho^2 - 2\rho + 1$.

Пример 3. $\varepsilon^3 = 7\varepsilon^2 - 68\varepsilon + 1$. Узнать, является ли ε степенью какого-либо другого кубического числа.

Решение. Прежде всего смотрим, является ли ε квадратом кубического числа. Пусть $\varepsilon = \rho^2$.

Тогда

$$\rho^3 = s\rho^2 + q\rho + 1; \quad s^2 + 2q = 7; \quad q^2 - 2s = 68.$$

Исключая q, получим

$$s^4 - 14s^2 - 8s - 223 = 0.$$

Это уравнение не имеет рациональных корней, следовательно $\varepsilon \neq \rho^2$.

Пусть $\varepsilon = \rho^p$, где p — нечетное простое число, а $\rho^3 = s\rho^2 + q\rho + 1$.

Из (7) получим:

61 делится на $-q-s$,
77 делится на $-q+s+2$.

Составляем таблицу для возможных значений $s+q$, сопоставляя каждому из них возможные p, исходя из сравнения $S+Q \equiv s+q \pmod{p}$.
То же самое делаем для $s-q+2$.

$s+q$	-1	-61
p	3; 5	любое

;

$s-q+2$	1	7	11	77
p	19	5; 7	3; 11	любое

Комбинируя случаи с одинаковыми p, получим следующие возможности:

$-q$	5	38	3	30	33	35
s	4	37	2	-31	-28	-26
p	3	3; 5	5	19	5; 7	3; 11

Испытание первой комбинации дает положительный результат. Получим:

$$\varepsilon = \rho^3, \quad \text{где} \quad \rho^3 = 4\rho^2 - 5\rho + 1.$$

Повторяем тот же процесс:

s_1+q_1	-1
p_1	любое

;

s_1-q_1+2	1	11
p_1	5	любое

Единственная возможность: $q_1 = 0$, $s_1 = -1$, $p_1 = 5$.
Испытание ее дает положительный результат:

$$\rho = \rho_1^5, \text{ где } \rho_1^3 = -\rho_1^2 + 1.$$

Повторяем процесс еще раз:

s_2+q_2	-1
p_2	любое

;

s_2-q_2+2	1
p_2	любое

Возможных комбинаций нет, и ρ_1 не является степенью. Итак, $\varepsilon = \rho_1^{15}$.

Вычисление нормы и дискриминанта. Непосредственная формула для нормы числа $\omega = u\rho^2 + v\rho + w$ довольно сложна и неудобна.

Для дискриминанта числа ρ имеем следующую формулу:

$$D\rho = [(\rho-\rho')(\rho-\rho'')(\rho'-\rho'')]^2 = \begin{vmatrix} 1 & \rho & \rho^2 \\ 1 & \rho' & \rho'^2 \\ 1 & \rho'' & \rho''^2 \end{vmatrix}^2 = s^2q^2 - 18sqn + 4q^3 - 4s^3n - 27n^2$$

Удобно вычислять норму и дискриминант следующим образом. Для вычисления нормы начнем преобразование Чирнгаузена от ρ к ω; тогда определитель, состоящий только из коэффициентов при 1, ρ, ρ^2, и есть норма числа ω. Дискриминант числа ω, взятый с обратным знаком, есть норма его „дифференты“ $\delta(\omega) = (\omega - \omega')(\omega - \omega'') = F'(\omega)$, где $F(\omega) = 0$ — уравнение, которому удовлетворяет ω, т. е. $-D_\omega = N(F'(\omega))$. Вычисление же нормы от $F'(\omega)$ производится предыдущим методом преобразования Чирнгаузена.

§ 12. Дробнолинейное представление чисел кубического поля

Ранее было показано, что каждое целое число кубического поля Ω_ρ может быть представлено через производящее число ρ в виде квадратичного трехчлена с рациональными коэффициентами, причем такое представление единственно. В некоторых случаях является удобной другая форма представления кубического числа, именно представление в виде дробнолинейной функции

$$\omega = \frac{\alpha\rho + \beta}{\gamma\rho + \delta}$$

с целыми рациональными коэффициентами α, β, γ, δ. Докажем возможность такого представления.

Пусть $\omega = a\rho^2 + b\rho + c$ — число поля Ω_ρ. Сопряженные с ω числа суть $\omega' = a\rho'^2 + b\rho' + c$ и $\omega'' = a\rho''^2 + b\rho'' + c$. Произведение чисел ω' и ω'' является, очевидно, числом поля Ω_ρ. Представим его в канонической форме:

$$\omega'\omega'' = A\rho^2 + B\rho + C.$$

Тогда

$$\omega''\omega = A\rho'^2 + B\rho^1 + C,$$
$$\omega\omega' = A\rho''^2 + B\rho'' + C.$$

Очевидно, что

$$\omega = \frac{\omega\omega' - \omega\omega''}{\omega' - \omega''} = -\frac{A(\rho''^2 - \rho'^2) + B(\rho'' - \rho')}{a(\rho''^2 - \rho'^2) + b(\rho'' - \rho')} = -\frac{A(\rho'' + \rho') + B}{a(\rho'' + \rho') + b}.$$

Принимая во внимание, что $\rho'' + \rho' = s - \rho$, получим:

$$\omega = \frac{A\rho - As - B}{-a\rho + as + b} = \frac{\alpha'\rho + \beta'}{\gamma'\rho + \delta'}.$$

Числа α', β', γ' и δ' рациональны. Умножив числитель и знаменатель на подходящее рациональное число, получим представление

$$\omega = \frac{\alpha\rho + \beta}{\gamma\rho + \delta},$$

в котором числа α, β, γ, δ — целые рациональные, общий наибольший делитель которых равен 1.

Такое представление единственно, с точностью до знаков α, β, γ и δ. В самом деле, если

$$\frac{\alpha\rho + \beta}{\gamma\rho + \delta} = \frac{\alpha_1\rho + \beta_1}{\gamma_1\rho + \delta_1},$$

то

$$(\alpha\gamma_1 - \alpha_1\gamma)\rho^2 + (\beta\gamma_1 - \beta_1\gamma + \alpha\delta_1 - \alpha_1\delta)\rho + \beta\delta_1 - \beta_1\delta = 0,$$

откуда

$$\alpha\gamma_1 - \alpha_1\gamma = 0;\ \beta\gamma_1 - \beta_1\gamma + \alpha\delta_1 - \alpha_1\delta = 0;\ \beta\delta_1 - \beta_1\delta = 0, \qquad (1)$$

так как кубическое число ρ не может быть корнем квадратного уравнения с отличными от нуля рациональными коэффициентами. Переписав первое и третье равенство из (1) в виде

$$\frac{\alpha_1}{\alpha} = \frac{\gamma_1}{\gamma} = t,\quad \frac{\beta_1}{\beta} = \frac{\delta_1}{\delta} = u$$

и подставив во второе равенство $\alpha_1 = \alpha t$, $\gamma_1 = \gamma t$, $\beta_1 = \beta u$, $\delta_1 = \delta u$, получим

$$(\alpha\delta - \beta\gamma)(t - u) = 0.$$

Очевидно, что $\alpha\delta - \beta\gamma \neq 0$, ибо иначе кубическое число ω было бы рациональным. Следовательно, $t = u$, и числа α_1, β_1, γ_1, δ_1 пропорциональны числам α, β, γ, δ.

Если потребовать, чтобы как числа α_1, β_1, γ_1, δ_1, так и α, β, γ, δ не имели общего делителя, отличного от 1, то возможно только

$$\frac{\alpha_1}{\alpha} = \frac{\beta_1}{\beta} = \frac{\gamma_1}{\gamma} = \frac{\delta_1}{\delta} = \pm 1,$$

что и требовалось доказать.

Фактически искать дробнолинейное представление проще всего способом неопределенных коэффициентов.

Пример. Представить в дробнолинейной форме число $\omega = \rho^2 - 3\rho + 1$; ρ задано уравнением $\rho^3 = \rho + 1$.

Пусть

$$\omega = \frac{\alpha\rho + \beta}{\gamma\rho + \delta} = \rho^2 - 3\rho + 1.$$

Умножив на $\gamma\rho + \delta$ и заменив в правой части ρ^3 на $\rho + 1$, получим:

$$\alpha\rho + \beta = (\delta - 3\gamma)\rho^2 + (2\gamma - 3\delta)\rho + \delta + \gamma,$$

откуда

$$\delta - 3\gamma = 0;\ 2\gamma - 3\delta = \alpha;\ \delta + \gamma = \beta,$$

и, следовательно, $\delta = 3\gamma$; $\alpha = -7\gamma$; $\beta = 4\gamma$.

Подставив эти значения в выражение для ω, получаем:

$$\omega = \frac{-7\gamma\rho + 4\gamma}{\gamma\rho + 3\gamma} = \frac{-7\rho + 4}{\rho + 3}.$$

§ 13. Решение задачи, обратной задаче Чирнгаузена, для двух кубических уравнений

Пусть имеются два целочисленные неприводимые кубические уравнения. Как узнать, образуют ли они одно и то же кубическое поле или разные? Самое естественное — это преобразовать первое уравнение по Чирнгаузену при помощи преобразующей функции $\varphi(z) = \alpha z^2 + \beta z + \gamma$, коэффициенты α, β, γ которой неопределенны, и посмотреть, можно ли так подобрать эти коэффициенты, чтобы коэффициенты получившегося уравнения совпадали с соответственными коэффициентами второго заданного уравнения. Дело сведется к тому, чтобы найти рациональный корень некоторого уравнения 6-й степени, либо показать, что это уравнение рационального корня не имеет. К сожалению, коэффициенты этого уравнения 6-й степени выражаются через коэффициенты обоих заданных кубических уравнений сложно и поэтому бывают велики, если даже коэффициенты кубических уравнений малы. Особое обстоятельство позволяет, однако, так изменить этот метод, что получается практически весьма удобное решение.

Предположим, во-первых, что в обоих заданных уравнениях произведены преобразования, уничтожающие члены, содержащие квадрат неизвестной, т. е. что заданные уравнения суть:

$$z^3 = qz + n, \tag{1}$$

$$z^3 = \bar{q}z + \bar{n}, \tag{2}$$

причем мы предположим еще, что q, n, $\bar{q}$, $\bar{n}$ — целые рациональные и что оба уравнения неприводимы. Преобразуем уравнение (1) формулой преобразования $\varphi(z) = \alpha z^2 + \beta z + \gamma$, где коэффициенты α, β, γ пока неизвестны, и приравняем коэффициенты преобразованного уравнения коэффициентам уравнения (2). Мы получим так три равенства: $2\alpha q + 3\gamma = 0$ и еще два другие. Если получаемое отсюда $\gamma = -\frac{2}{3}\alpha q$ подставить в эти два другие, то получатся равенства:

$$(3q\cdot\beta^2 + 9n\alpha\beta + q^2\alpha^2) - 3\bar{q} = 0, \tag{3}$$

$$[27n\beta^3 + 18q^2\beta^2\alpha + 27qn\beta\alpha^2 + (27n^2 - 2q^2)\alpha^3] - 27\bar{q} = 0, \tag{4}$$

где выражения, стоящие в скобках, суть квадратичный и кубический коварианты $-H(x, y)$ и $-Q(x, y)$ кубической двойничной формы $f(x, y) = x^3 - qxy^2 - ny^3$, куда подставлены $x = \beta$, $y = \alpha$. Но, как известно, имеет место тождество Кэли (Cayley) (в x, y):

$$27Df^2 = -4H^3 - Q^2,$$

где $D = 4q^3 - 27n^2$ — дискриминант формы f, т. е. дискриминант уравнения (1). В силу (3) и (4), отсюда получается $D\cdot[f(\beta, \alpha)]^2 = \bar{D}$, если обозначить через $\bar{D}$ дискриминант $\bar{D} = 4\bar{q}^3 - 27\bar{n}^2$ уравнения (2), т. е. известное обстоятельство, — что если уравнения (1) и (2) образуют одно и то же поле, то дискриминанты их могут отличаться лишь квадратными множителями.

Если это не так, то рационального преобразования (1) в (2) не имеется, если же это имеет место, то можно положить $D = D_1\cdot\Delta^2$, $\bar{D} = D_1\cdot\bar{\Delta}^2$, где D_1 уже не имеет квадратных делителей, и Δ и $\bar{\Delta}$ — положительные целые рациональные числа. В таком случае

$$f(\beta, \alpha) \mp \frac{\bar{\Delta}}{\Delta} = 0. \tag{5}$$

Исключим из (3), (4) и (5) β, для чего составим комбинацию $-(4) + 27n(5) + 6\alpha q(3)$, равную нулю. Комбинация эта равна $8\alpha^3q^3 - 54\alpha^3n^2 - 18\alpha q\bar{q} + 27\bar{n} \mp 27\frac{\bar{\Delta}}{\Delta}n$; следовательно, если мы положим $\alpha = \frac{3u_1}{\Delta}$, то мы получим

$$D_1u_1^3 - q\bar{q}u_1 + \frac{\Delta\bar{n} \mp \bar{\Delta}n}{2} = 0. \tag{*}$$

С другой же стороны, равная нулю комбинация $[\beta(3) - 3q(5)]q - 3\alpha n(3)$ есть $\beta(\alpha^2\Delta^2D_1 - 3q\bar{q}) + 9\alpha q\bar{n} \mp 3\frac{\bar{\Delta}}{\Delta}q^2 = 0$, и поэтому, если положить $\beta = \frac{v}{\Delta}$ и $\gamma = \frac{w}{\Delta}$, то мы получаем

$$u = 3u_1; \quad v = \frac{\mp q^2\bar{\Delta} \mp 9\bar{q}nu_1}{3D_1u_1^2 - q\bar{q}}; \quad w = -2qu_1. \tag{**}$$

Тут $3D_1u_1^2 - q\bar{q}$ равно нулю, только если u_1 — кратный корень уравнения (*).

Но тогда третий корень (*) — тоже рациональный и уже отличается от этого кратного корня u_1, так как (*) не имеет всех трех корней одинаковыми, ибо не имеет члена с квадратом неизвестной и потому не есть полный куб. Следовательно, если только уравнение (*) имеет рациональный корень вообще, то оно имеет и не кратный рациональный корень, который мы и будем обозначать через u_1, и тогда $3D_1u_1^2 - q\bar{q}$ не равен нулю, и формулы (**) дают преобразование Чирнгаузена.

Остается еще возможность, что уравнение (*) имеет вид $D_1u_1^3 = 0$; но это может быть, как легко видеть, только если $q = \bar{q} = 0$, т. е. если уравнения

(1) и (2) имеют вид $z^3 = n$, $z^3 = \bar{n}$; но в таком случае они образуют одно и то же поле тогда и только тогда, когда либо $n\bar{n}$, либо $\frac{\bar{n}}{n}$ есть полный куб.

Уравнения (1) и (2) образуют, следовательно, одно и то же кубическое поле тогда и только тогда, когда их дискриминанты отличаются лишь квадратными множителями и когда по крайней мере одно из уравнений (*) (тут, собственно, два уравнения, вследствие знака $\mp$ при $\bar{\Delta}n$) имеет рациональный корень u_1. Корень этот u_1 может быть только целым рациональным, так как D_1 не делится на квадрат, и, следовательно, если бы p был какой-нибудь простой множитель знаменателя u_1 и входил бы в этот знаменатель в степени $\varkappa$, то в первом члене после сокращения он остался бы, по крайней мере, в степени $3\varkappa - 1$, а во втором и третьем, если их привести к общему знаменателю, он был бы не больше, чем в степени $\varkappa$. Число $\frac{\Delta\bar{n} + \Delta\bar{n}}{2}$ таким образом тоже должно быть целое рациональное. Коэффициенты α, β, γ переходной функции φ равны $\frac{u}{\Delta}$, $\frac{v}{\Delta}$, $\frac{w}{\Delta}$, где u, v, w — целые рациональные числа, вычисляемые по формулам (**). Целость v есть хорошая проверка вычислениям.

Мы не нашли никакого простого критериума, чтобы a priori решать, какое из двух уравнений (*) имеет рациональный корень.

Пример. Пусть даны кубические уравнения $z^3 = -3z - 2$ (I) и $116z^3 + 219z^2 + 138z + 29 = 0$. Первое уравнение уже имеет требуемую форму, второе же должно быть предварительно преобразовано. Оно имеет вид $z^3 = -\frac{219}{116}z^2 - \frac{138}{116}z - \frac{29}{116}$; полагая $z^1 = 116z + 73$, мы получаем для z^1 уравнение $z'^3 = -21z' + 326$ (II). Будем искать переходную функцию от (I) к (II). Мы имеем $q = -3$, $n = -2$; $\bar{q} = -21$, $\bar{n} = 326$; $D = -216$; $\bar{D} = -216 \cdot 116^2$; D и $\bar{D}$ отличаются лишь квадратными множителями, первый критериум выполнен. Мы имеем $D_1 = -6$; $\Delta = 6$; $\bar{\Delta} = 696$, уравнение (*), следовательно, $-6u_1^3 - 63u_1 + \frac{6 \cdot 326 \mp 696 \cdot 2}{2} = 0$, откуда $u_1 = 6$, при верхнем знаке, и, таким образом, по формулам (**) мы получаем $\alpha = 3$, $\beta = 2$, $\gamma = 6$, т. е. переходная функция от (I) к (II) есть $\varphi(z) = 3z^2 + 2z + 6$.

§ 14. Базис целых чисел поля

В поле Ω_ρ всегда имеются три таких целых числа $\omega_0, \omega_1, \omega_2$ (в случае кубического поля мы первое число базиса будем обозначать не ω_1, а ω_0, и соответственно два другие — не ω_2, ω_3, а ω_1, ω_2), что всякое целое число ω поля Ω_ρ выражается через них линейно однородно, с целыми рациональными коэффициентами:

$$\omega = u\omega_0 + v\omega_1 + w\omega_2, \tag{1}$$

где u, v, w — целые рациональные. Такие три числа называются *базисом поля*.

Если подходить к этому вопросу геометрически, то существование базиса совокупности целых чисел алгебраического поля любого порядка n либо вовсе не надо доказывать, если сама эта совокупность введена, как это было сделано в главе I, как решетка в K_n, повторяющаяся умножением, либо если только сказано, что это совокупность всех целых чисел поля, надо показать, что в соответствеином сигнатурном пространстве R_n: *во-первых*, совокупность точек, координатами которых являются эти числа и их сопряженные [если какие-нибудь два из сопряженных чисел $\omega^{(l)}$, $\omega^{(k)}$ — комплексно сопряженные, т. е. $\omega^{(l)} = \xi + i\mu$; $\omega^{(k)} = \xi - i\mu$, то соответствующие им две координаты берутся ξ и μ], повторяется сложением и вычитанием (что следует из того,

что сумма и разность двух целых чисел поля есть опять целое число этого же поля), *во-вторых*, что точки эти лежат n-мерно [что следует из того, что если ω — корень неприводимого уравнения n-ой степени, то все сопряженные с ω числа различны, так как неприводимое уравнение не имеет кратных корней, но тогда уже точки $1, \omega, \omega^2, \ldots \omega^{n-1}$ лежат n-мерно с началом, так как определитель

$$\begin{vmatrix} 1, \omega, \omega^2 \ldots\ldots \omega^{n-1} \\ 1, \omega', \omega'^2 \ldots\ldots \omega'^{n-1} \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ 1, \omega^{(n-1)}, \omega^{(n-1)^2} \ldots \omega^{(n-1)^{n-1}} \end{vmatrix} \neq 0$$

есть определитель Вандермонда и он равен $(\omega - \omega')(\omega - \omega'') \ldots (\omega^{(n-2)} - \omega^{(n-1)})]$, и, *в-третьих*, что точки эти лежат дискретно, например, нет точек близких к точке 0, так как, если бы все координаты точки ω в R_n были очень малы по абсолютной величине, то и коэффициенты того уравнения, которому удовлетворяет ω, были бы все очень малы по абсолютной величине, но, например, постоянный член его — целый рациональный и не равен нулю, и, следовательно, абсолютная величина его не меньше 1.

Из этих трех фактов, в силу леммы 1 „Прилложения" к главе I — о решетках в вещественном эвклидовом пространстве, следует, что совокупность всех целых чисел данного поля образует n-мерную решетку, т. е. что в ней есть такие n чисел $\omega_1, \omega_2, \ldots, \omega_n$, что всякое вообще ее число ω имеет вид $\omega = u_1\omega_1 + u_2\omega_2 + \ldots + u_n\omega_n$, где $u_1, u_2, \ldots, u_n$ — целые рациональные.

Дадим однако и чисто арифметическое доказательство, причем проведем его только для кубического поля, хотя оно совершенно так же проводится и для поля любого порядка. Рассмотрим, каковы могут быть знаменатели рациональных коэффициентов α, β, γ в выражении ω через ρ: $\omega = \alpha\rho^2 + \beta\rho + \gamma$. Мы имеем равенства $\omega = \alpha\rho^2 + \beta\rho + \gamma$; $\omega' = \alpha\rho'^2 + \beta\rho' + \gamma$; $\omega'' = \alpha\rho''^2 + \beta\rho'' + \gamma$. Складывая эти равенства, затем помножая их на ρ, ρ', ρ'' и складывая, и наконец, помножая на $\rho^2, \rho'^2, \rho''^2$ и складывая, мы получим

$$\left.\begin{aligned} S(\omega) &= \alpha \cdot s_2 + \beta \cdot s_1 + \gamma \cdot 3 \\ S(\omega\rho) &= \alpha \cdot s_3 + \beta \cdot s_2 + \gamma \cdot s_1 \\ S(\omega\rho^2) &= \alpha \cdot s_4 + \beta \cdot s_3 + \gamma \cdot s_2 \end{aligned}\right\}, \qquad (2)$$

где коэффициенты S и s — целые симметрические функции от целых алгебраических чисел, т. е. числа целые рациональные. Определитель при неизвестных α, β, γ в системе (2) есть квадрат определителя

$$\begin{vmatrix} 1 & \rho & \rho^2 \\ 1 & \rho' & \rho'^2 \\ 1 & \rho'' & \rho''^2 \end{vmatrix},$$

т. е. дискриминант D_ρ числа ρ (см. § 11), и, следовательно, знаменатели α, β, γ суть делители D_ρ. Итак, всякое целое число поля Ω_ρ имеет вид:

$$\omega = \frac{a\rho^2 + b\rho + c}{D_\rho}, \qquad (3)$$

где a, b, c — целые рациональные. Обратное не всегда имеет место, т. е. число вида (3) при целых рациональных a, b, c может быть не целым, а дробным алгебраическим.

Среди целых чисел Ω_ρ имеются числа трех видов:

нулевой степени относительно ρ $\omega = \frac{c}{D_\rho}$,

первой степени „ „ $\omega = \frac{b'\rho + c'}{D_\rho}$,

и второй степени „ „ $\omega = \frac{a''\rho^2 + b''\rho + c''}{D_\rho}$.

Действительно, например 1, ρ, ρ^2 таковы.

Из целых чисел 1-го вида, т. е. целых рациональных, наименьшее c, неравное нулю, имеет число $\frac{D_\rho}{D_\rho} = 1$; примем его за ω_0. Пусть наименьшее b', встречающееся у чисел второго вида, есть b'_0; примем одно из таких чисел за ω_1. Пусть наименьшее a'', встречающееся у чисел третьего вида, есть a''_0; примем одно из чисел третьего вида с таким a'' за ω_2. Иначе говоря, пусть

$$\left.\begin{aligned} \omega_0 &= 1 \\ \omega_1 &= \frac{b'_0\rho + c'_0}{D_\rho} \\ \omega_2 &= \frac{a''_0\rho^2 + b''_0\rho + c''_0}{D_\rho} \end{aligned}\right\}. \qquad (4)$$

Покажем, что через числа (4) можно представить всякое целое число ω поля Ω_ρ в форме (1) с целыми рациональными u, v, w.

Действительно, пусть задано некоторое целое число ω; оно имеет форму (3). Коэффициент a этого числа либо равен нулю, либо делится на a''_0, так как иначе, прибавляя к ω или вычитая из него соответственное, целое число раз взятое, число ω_2, мы получили бы целое число Ω_ρ третьего вида, у которого a меньше, чем a''_0, что противоречит сделанному относительно a''_0 предположению.

Пусть $a = w \cdot a''_0$. Тогда целое число $\omega - w\omega_2$ имеет $a = 0$, т. е. либо второго, либо первого вида. Аналогично, прибавляя или вычитая из этого числа $\omega - w\omega_2$ соответственное, целое число раз взятое, число ω_1, мы покажем, что его $b = v \cdot b'_0$, где v — целое рациональное число или нуль. Тогда целое число $\omega - w\omega_2 - v\omega_1$ имеет $a = b = 0$, т. е. целое рациональное число. Пусть оно равно u, мы видим тогда, что $\omega = u \cdot 1 + v \cdot \omega_1 + w \cdot \omega_2$, где u, v, w — целые рациональные, т. е. числа $1, \omega_1, \omega_2$ образуют базис поля.

Если $\omega_0, \omega_1, \omega_2$ — базис поля, то целые числа поля

$$\bar{\omega}_0 = u_0\omega_0 + v_0\omega_1 + w_0\omega_2;\ \bar{\omega}_1 = u_1\omega_0 + v_1\omega_1 + w_1\omega_2;\ \bar{\omega}_2 = u_2\omega_0 + v_2\omega_1 + w_2\omega_2$$

очевидно, образуют тоже базис поля тогда и только тогда, когда определитель

$$\begin{vmatrix} u_0 & v_0 & w_0 \\ u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \end{vmatrix} = \pm 1.$$

Действительно, если этот определитель равен ± 1, то сами числа исходного базиса, а, следовательно, и все целые числа поля, выражаются через $\bar{\omega}_0, \bar{\omega}_1, \bar{\omega}_2$ линейно однородно, с целыми рациональными коэффициентами; наоборот, если $\bar{\omega}_0, \bar{\omega}_1, \bar{\omega}_2$ — тоже базис поля, т. е. $\omega_0, \omega_1, \omega_2$ выражаются линейно однородно, с целыми рациональными коэффициентами, через $\bar{\omega}_0, \bar{\omega}_1, \bar{\omega}_2$, то определитель этот равен ± 1, так как если коэффициенты преобразования от $\bar{\omega}_0, \bar{\omega}_1, \bar{\omega}_2$ к $\omega_0, \omega_1, \omega_2$ суть $\bar{u}_0, \bar{v}_0, \bar{w}_0$; $\bar{u}_1, \bar{v}_1, \bar{w}_1$; $\bar{u}_2, \bar{v}_2, \bar{w}_2$, то определитель преобразова-

ния от $\omega_0, \omega_1, \omega_2$ к $\omega_0, \omega_1, \omega_2$ (определитель тождественного преобразования) есть произведение определителей

$$\begin{vmatrix} u_0 v_0 w_0 \\ u_1 v_1 w_1 \\ u_2 v_2 w_2 \end{vmatrix} \cdot \begin{vmatrix} \overline{u}_0 & \overline{v}_0 & \overline{w}_0 \\ \overline{u}_1 & \overline{v}_1 & \overline{w}_1 \\ \overline{u}_2 & \overline{v}_2 & \overline{w}_2 \end{vmatrix},$$

т. е. это произведение равно $+1$. Но каждый из этих определителей, как имеющий своими элементами целые рациональные числа, есть целое рациональное число, т. е. равен ± 1.

Квадрат определителя

$$\begin{vmatrix} \omega_0 \omega_1 \omega_2 \\ \omega_0' \omega_1' \omega_2' \\ \omega_0'' \omega_1'' \omega_2'' \end{vmatrix}$$

будет, очевидно, один и тот же для любого базиса поля. Он называется дискриминантом поля и обозначается D_Ω.

Дискриминант поля, как симметрическая функция от ρ, ρ', ρ'', есть рациональное число, а в виду того, что он — целая рациональная функция от целых алгебраических чисел, он есть целое рациональное число.

Геометрический смысл всего этого — см. в главе I.

§ 15. Связь между кольцами целых чисел кубических полей, содержащими 1, и классами неприводимых кубических двойничных форм с целыми рациональными коэффициентами

Мы будем в этом параграфе рассматривать кольца целых чисел кубического поля, которые заключают в себе число 1 и какие-нибудь примитивные числа рассматриваемого кубического поля. Таким кольцом является совокупность всех целых чисел поля. Таким же кольцом будет, например, каждая совокупность числа $u\rho^2 + v\rho + w$, где u, v, w пробегают все целые рациональные значения. Пусть ρ — примитивное число кубического поля, заключающееся в некотором кольце рассматриваемого типа. Тогда числа ρ^2, ρ, 1 заключаются в этом кольце O и, следовательно, если числа поля Ω выражать через ρ^2, ρ, 1, то в кольце O будут находиться числа всех трех сортов, рассмотренные при выводе базиса поля в предыдущем параграфе, и мы, дословно как там, покажем, что кольцо O имеет базис $\omega_0, \omega_1, \omega_2$, причем за ω_0, в частности, можно будет взять 1. Такие базисы $1, \omega_1, \omega_2$ кольца O мы будем называть *единичными*. Совокупность всех чисел, выражаемых через некоторые три числа $\omega_0, \omega_1, \omega_2$ поля линейно однородно с целыми рациональными коэффициентами, мы будем называть *модулем* с базисом $\omega_0, \omega_1, \omega_2$ и обозначать $[\omega_0, \omega_1, \omega_2]$. Кольцо с базисом $\omega_0, \omega_1, \omega_2$ мы будем обозначать $O[\omega_0, \omega_1, \omega_2]$.

Не всякие два целые числа ω_1, ω_2 поля Ω вместе с числом 1 дают базис кольца. Действительно, например, модуль $[1, \rho, 2\rho^2]$, где ρ — некоторое целое примитивное число Ω, — не кольцо, так как произведение $\rho \cdot \rho = \rho^2$ его чисел ρ и ρ не лежит в нем. Для того чтобы узнать, является ли модуль $[1, \omega_1, \omega_2]$ кольцом, достаточно узнать, лежат ли все произведения его чисел в нем самом. Для этого необходимо и достаточно, чтобы в $[1, \omega_1, \omega_2]$ лежали числа $\omega_1^2, \omega_2^2, \omega_1\omega_2$. Выразим в Ω эти три числа линейно через $1, \omega_1, \omega_2$ с рациональными коэффициентами, что можно всегда сделать, если определитель перехода от базиса поля Ω к тройке чисел $1, \omega_1, \omega_2$ отличен от нуля (что мы предполагаем относительно рассматриваемого модуля).

Пусть

$$\left.\begin{aligned}\omega_1^2 &= A_0 + A_1\omega_1 + A_2\omega_2\\ \omega_2^2 &= B_0 + B_1\omega_1 + B_2\omega_2\\ \omega_1\omega_2 &= C_0 + C_1\omega_1 + C_2\omega_2\end{aligned}\right\}. \tag{1}$$

Если 9 чисел $A_0, A_1, A_2, B_0, B_1, B_2, C_0, C_1, C_2$ — целые, то модуль $[1, \omega_1, \omega_2]$ — кольцо, в противном случае — нет. Эти 9 чисел, которые достаточно знать для того, чтобы производить все умножения в кольце, мы будем называть „умножающими" коэффициентами.

Умножающие коэффициенты не независимы, а именно:

$$\left.\begin{aligned}A_0 &= A_2(C_1 - B_2) - C_2(A_1 - C_2),\\ B_0 &= B_1(C_2 - A_1) - C_1(B_2 - C_1),\\ C_0 &= A_2B_1 - C_1C_2,\end{aligned}\right\} \tag{2}$$

что легко видеть, если вычислить $\omega_1^2\cdot\omega_2$ и $\omega_1\omega_2\cdot\omega_1$ и приравнять коэффициенты, опустив предварительно до первых степеней относительно ω_1, ω_2 при помощи (1).

Квадрат определителя $\begin{vmatrix}1 & \omega_1 & \omega_2\\ 1 & \omega_1' & \omega_2'\\ 1 & \omega_1'' & \omega_2''\end{vmatrix}$, где верхними значками обозначены сопряженные по рассматриваемому кубическому полю с Ω числа, и $1, \omega_1, \omega_2$ — базис кольца O, называется дискриминантом кольца O и обозначается D_O. Если $1, \theta_1, \theta_2$ — другой единичный базис того же кольца O и

$$\begin{aligned}\theta_1 &= u_1 + v_1\omega_1 + w_1\omega_2,\\ \theta_2 &= u_2 + v_2\omega_1 + w_2\omega_2,\end{aligned}$$

то $\begin{vmatrix}v_1 & w_1\\ v_2 & w_2\end{vmatrix} = \pm 1$; и наоборот, если $u_1, v_1, w_1, u_2, v_2, w_2$ — целые рациональные и $\begin{vmatrix}v_1 & w_1\\ v_2 & w_2\end{vmatrix} = \pm 1$, то $1, \theta_1, \theta_2$ — другой единичный базис того же кольца. Если ρ — какое-нибудь число кольца O и если $\rho = a_0 + a_1\omega_1 + a_2\omega_2$, $\rho^2 = b_0 + b_1\omega_1 + b_2\omega_2$, то дискриминант $D_\rho = \begin{vmatrix}1 & \rho & \rho^2\\ 1 & \rho' & \rho'^2\\ 1 & \rho'' & \rho''^2\end{vmatrix}^2$ числа ρ равен, очевидно, дискриминанту кольца D_O, помноженному на квадрат определителя $\Delta = \begin{vmatrix}a_1 & a_2\\ b_1 & b_2\end{vmatrix}$.

Находя из ρ и ρ^2 ω_1 и ω_2, мы получаем

$$\omega_1 = \frac{-a_2\rho^2 + b_2\rho + a_2b_0 - a_0b_2}{\Delta},$$

$$\omega_2 = \frac{a_1\rho^2 - b_1\rho + a_0b_1 - a_1b_0}{\Delta},$$

и следовательно любое число ω кольца O имеет вид: $\frac{u\rho^2 + v\rho + w}{\Delta}$, где u, v, w — целые рациональные числа.

Всякое число кольца O выражается, таким образом, через $1, \rho, \rho^2$ линейно однородно с рациональными коэффициентами, общий знаменатель которых есть Δ. Определитель Δ называется индексом числа ρ относительно кольца O. В частности, если O — максимальное кольцо целых чисел поля, т. е. совокупность всех целых чисел поля, то Δ просто называется индексом числа ρ.

Вычислим индекс Δ числа ρ относительно кольца O через коэффициенты a_1, a_2 числа ρ и через умножающие коэффициенты (1). Мы получим:

$$\Delta = a_1^3 A_2 + a_1^2 a_2 (2C_2 - A_1) + a_1 a_2^2 (B_2 - 2C_1) - a_2^3 B_1.$$

Мы видим, что индекс числа ρ относительно кольца O представляет собою значение кубической двойничной формы

$$(A_2,\ 2C_2 - A_1,\ B_2 - 2C_1,\ -B_1) = f(x, y) \tag{3}$$

при значениях переменных $x = a_1$, $y = a_2$. Эту форму мы называем индекс-формой базиса 1, ω_1, ω_2 кольца O и будем также обозначать $f[1, \omega_1, \omega_2]$.

Базисы 1, ω_1, ω_2 и 1, $\omega_1 + c_1$, $\omega_2 + c_2$, где c_1, c_2 — любые целые рациональные числа, мы называем параллельными единичными базисами, а совокупность всех таких параллельных между собою базисов — параллелью единичных базисов. Если произведение $\omega_1\omega_2$ — рациональное число, мы будем называть единичный базис 1, ω_1, ω_2 нормальным.

Теорема I. *Среди параллельных единичных базисов кольца есть всегда один, и только один, нормальный.*

Действительно, рассмотрим произведение:

$$(\omega_1 + c_1)(\omega_2 + c_2) = \omega_1\omega_2 + \omega_1 c_2 + \omega_2 c_1 + c_1 c_2 = \\ = (C_1 + c_1)\omega_1 + (C_2 + c_2)\omega_2 + C_0 + c_1 c_2.$$

Мы видим, что если положить $c_1 = -C_1$, $c_2 = -C_2$, то мы перейдем к нормальному базису 1, $\omega_1 + c_1$, $\omega_2 + c_2$.

Теорема II. *Параллельным единичным базисом кольца O соответствует одна и та же индексформа.*

Пусть умножающие коэффициенты параллельного базиса суть

$$\overline{A}_0,\ \overline{A}_1,\ \overline{A}_2,\quad \overline{B}_0,\ \overline{B}_1,\ \overline{B}_2,\quad \overline{C}_0,\ \overline{C}_1,\ \overline{C}_2.$$

Тогда

$$\overline{A}_1 = A_1 + 2C_1;\ \overline{B}_1 = B_1;\ \overline{C}_1 = C_1 + C_2;$$
$$\overline{A}_2 = A_2;\ \overline{B}_2 = B_2 + 2C_2;\ \overline{C}_2 = C_2 + C_1.$$

Написав по (3) индексформу, соответствующую этому базису, мы убеждаемся, что

$$f[1,\ \omega_1 + c_1,\ \omega_2 + c_2] = f[1,\ \omega_1,\ \omega_2].$$

Теорема III. *Всякой неприводимой целочисленной кубической двойничной форме соответствует параллель единичных базисов некоторого кольца целых чисел кубического поля, содержащего 1.*

Пусть $f = (A_2, -A_1, B_2, -B_1)$ — некоторая неприводимая целочисленная кубическая двойничная форма. Рассмотрим числа ω_1 и ω_2 — такие, что ω_1 — корень уравнения

$$z^3 - A_1 z^2 + A_2 B_2 z - A_2^2 B_1 = 0, \tag{4}$$

а ω_2 — корень уравнения

$$z^3 - B_2 z^2 + A_1 B_1 z - A_2 B_1^2 = 0. \tag{5}$$

Тогда $\frac{1}{\omega_2}$ — корень уравнения

$$-z^3 A_2 B_1^2 + z^2 A_1 B_1 - z B_2 + 1 = 0, \text{ или } z^3 - \frac{A_1}{A_2 B_1} z^2 + \frac{B_2 A_2}{A_2^2 B_1^2} z - \frac{A_2^2 B_1}{A_2^3 B_1^3} = 0,$$

т. е.

$$\frac{A_2 B_1}{\omega_2} = \omega_1, \text{ или } \omega_1\omega_2 = A_2 B_1.$$

Следовательно 1, ω_1, ω_2 — нормальный базис некоторого модуля.

Не трудно видеть, что модуль $[1, \omega_1, \omega_2]$ есть кольцо. Действительно, положим $\omega_1^2 = \overline{A}_0 + \overline{A}_1\omega_1 + \overline{A}_2\omega_2$, $\omega_2^2 = \overline{B}_0 + \overline{B}_1\omega_1 + \overline{B}_2\omega_2$, $\omega_1\omega_2 = \overline{C}_0 + \overline{C}_1\omega_1 + \overline{C}_2\omega_2$, что всегда можно сделать, если дискриминант базиса $1, \omega_1, \omega_2$ не равен нулю. Но он, если форма f неприводима, как легко видеть, не равен нулю. Принимая во внимание, что $\omega_2 = \frac{A_2B_1}{\omega_1}$, мы получаем

$$\omega_1^3 - \overline{A}_1\omega_1^2 - \overline{A}_0\omega_1 - \overline{A}_2B_1A_2 = 0;$$

сравнивая это с уравнением (4), мы получаем:

$$\overline{A}_0 = -A_2B_2; \quad \overline{A}_1 = A_1; \quad \overline{A}_2 = A_2;$$

совершенно аналогично мы получаем:

$$\overline{B}_0 = -A_1B_1; \ \overline{B}_1 = B_1; \ \overline{B}_2 = B_2, \text{ и } \overline{C}_0 = A_2B_1; \ \overline{C}_1 = 0; \quad \overline{C}_2 = 0.$$

Мы видим, таким образом, по (1) и (2), что $[1, \omega_1, \omega_2]$ есть кольцо и что индексформа единичного нормального базиса его $1, \omega_1, \omega_2$ есть как раз $(A_2, -A_1, B_2, -B_1)$.

Теорема IV. *Эквивалентным единичным базисам кольца O соответствуют эквивалентные индексформы, и обратно, причем* $f[1, \theta_1, \theta_2] = f[1, \omega_1, \omega_2]\binom{v_1w_1}{v_2w_2}$.

Действительно, пусть задано кольцо, причем $1, \omega_1, \omega_2$ — его нормальный единичный базис, так что

$$\left.\begin{aligned} \omega_1^2 &= -A_2B_2 + A_1\omega_1 + A_2\omega_2 \\ \omega_2^2 &= -A_1B_1 + B_1\omega_1 + B_2\omega_2 \\ \omega_1\omega_2 &= A_2B_1 \end{aligned}\right\} \tag{6}$$

Пусть $\theta_1 = u_1 + v_1\omega_1 + w_1\omega_2$; $\theta_2 = u_2 + v_2\omega_1 + w_2\omega_2$ — другой единичный базис того же кольца, т. е. $\begin{vmatrix} v_1w_1 \\ v_2w_2 \end{vmatrix} = \pm 1$. В виду того, что индексформы, соответствующие параллельным базисам, одинаковы, мы можем предполагать, что $u_1 = u_2 = 0$. Пользуясь (6), мы получим тогда:

$$\theta_1^2 = -v_1^2A_2B_2 - w_1^2A_1B_1 + 2v_1w_1A_2B_1 + (v_1^2A_1 + w_1^2B_1)\omega_1 + (v_1^2A_2 + w_1^2B_2)\omega_2.$$

Если мы подставим сюда выражения

$$\omega_1 = w_2\theta_1 - w_1\theta_2; \ \omega_2 = v_1\theta_1 - v_2\theta_2,$$

дающие ω_1, ω_2 через θ_1, θ_2, то мы вычислим умножающие коэффициенты базиса $1, \theta_1, \theta_2$, а по ним и по (3) коэффициенты индексформы $f[1, \theta_1, \theta_2]$.

Если мы, с другой стороны, просто преобразуем форму $f[1, \omega_1, \omega_2]$ подстановкой $\binom{v_1w_1}{v_2w_2}$, то мы получим, что $f[1, \omega_1, \omega_2]\binom{v_1w_1}{v_2w_2} = f[1, \theta_1, \theta_2]$.

Таким образом установлено взаимно однозначное соответствие между классами целочисленных неприводимых кубических двойничных форм и кольцами O целых чисел кубических полей, содержащими 1, или, собственно, тройками таких сопряженных колец, т. е. неприводимыми трехмерными решетками, повторяющимися умножением и содержащими точку 1.

Если форму f писать так: $f = (a, b, c, d)$, и если ω_1, ω_2 — корни уравнений (4) и (5), соответствующих этой форме, т. е. уравнений

$$z^3 + bz^2 + acz + a^2d = 0, \tag{4'}$$

$$z^3 - cz^2 + dbz - d^2a = 0, \tag{5'}$$

то мы будем ω_1 и ω_2 называть левым и правым корнями формы f. Тогда 1, ω_1, ω_2 образует нормальный единичный базис кольца O, соответствующего форме (a, b, c, d), причем схема его умножающих коэффициентов следующая:

$$\left.\begin{aligned} \omega_1^2 &= -ac - b\omega_1 + a\omega_2, \\ \omega_2^2 &= -bd - d\omega_1 + c\omega_2, \\ \omega_1\omega_2 &= -ad. \end{aligned}\right\} \tag{7}$$

Теорема V. *Дискриминант индексформы равен дискриминанту соответствующего этой форме кольца.*

Действительно, дискриминант базиса 1, ω_1 ω_2 равен

$$|1, \omega_1, \omega_2|^2 = \left|1, \omega_1, \frac{\omega_1^2 + b\omega_1 + ac}{a}\right|^2 = \frac{1}{a^2}|1, \omega_1, \omega_1^2|^2,$$

но $|1, \omega_1, \omega_1^2|^2$ есть дискриминант числа ω_1 или, что все равно, уравнение (4′). Вычислив его и разделив на a^2, мы получаем дискриминант формы f:

$$D_f = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

§ 16. Решение задачи эквивалентности для двух целочисленных неприводимых кубических двойничных форм

Пусть даны две кубические двойничные формы (a, b, c, d) и $(\bar{a}, \bar{b}, \bar{c}, \bar{d})$ с целыми рациональными коэффициентами и одинаковыми дискриминантами, и требуется узнать, эквивалентны ли они, т. е. существует ли такая подстановка $x = \alpha\bar{x} + \beta\bar{y}$; $y = \gamma\bar{x} + \delta\bar{y}$ с целыми рациональными коэффициентами $\alpha, \beta, \gamma, \delta$ и определителем $\alpha\delta - \beta\gamma = \pm 1$, что $ax^3 + bx^2y + cxy^2 + dy^3 = \bar{a}\bar{x}^3 + \bar{b}\bar{x}^2\bar{y} + \bar{c}\bar{x}\bar{y}^2 + \bar{d}\bar{y}^3$. Для этого заметим, что, если

$$f = (a, b, c, d) = a(x - \xi y)(x - \xi' y)(x - \xi'' y),$$

где ξ, ξ', ξ'' — корни уравнения $f(x, 1) = 0$, то

$$\bar{f}(\bar{x}, \bar{y}) = a(\alpha\bar{x} + \beta\bar{y} - \xi(\gamma\bar{x} + \delta\bar{y}))\cdot(\alpha\bar{x} + \beta\bar{y} - \xi'(\gamma\bar{x} + \delta\bar{y}))\cdot (\alpha\bar{x} + \beta\bar{y} - \xi''(\gamma\bar{x} + \delta\bar{y})),$$

т. е. корни уравнения $\bar{f}(\bar{x}, 1) = 0$ будут, следовательно, $\bar{\xi} = \frac{\delta\xi - \beta}{-\gamma\xi + \alpha}$. Таким образом $\bar{\xi}$ выражается рационально через ξ. Пусть $\bar{\xi} = u\xi^2 + v\xi + w$. Тогда, если положить $-\frac{b}{a} = s$; $-\frac{c}{a} = q$; $-\frac{d}{a} = n$, числа $\alpha, \beta, \gamma, \delta$ пропорциональны числам

$$\alpha'' = us + v;\ \beta'' = u^2n - vw - uws;\ \gamma'' = u;\ \delta'' = v^2 - uw - u^2q + uvs. \tag{1}$$

Приведя эти рациональные числа к общему знаменателю, мы рассмотрим числители; сократив их на общий множитель, если таковой у них будет, мы получим наименьшие целые числа $\alpha', \beta', \gamma', \delta'$, пропорциональные $\alpha, \beta, \gamma, \delta$ и соответственно тех же знаков. Предположим еще, что $a > 0$ и $\bar{a} > 0$ (если бы этого не было, мы обеспечим это, сделав предварительное преобразование подстановкой $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$). Тогда имеет место следующая

Теорема: *Формы f и $\bar{f}$ эквивалентны тогда и только тогда, когда* $\alpha'\delta' - \beta'\gamma' = \pm 1$, *причем переходная подстановка* $\begin{pmatrix}\alpha\beta\\ \gamma\delta\end{pmatrix}$ *есть* $\begin{pmatrix}\alpha'\beta'\\ \gamma'\delta'\end{pmatrix}$, *если* $\alpha'\delta' - \beta'\gamma' = 1$, *и* $\begin{pmatrix}-\alpha' & -\beta'\\ -\gamma' & -\delta'\end{pmatrix}$, *если* $\alpha'\delta' - \beta'\gamma' = -1$.

Действительно, $\alpha''\delta'' - \beta''\gamma'' = -u^3(sq+n) + u^2v(s^2-q) + 2uv^2s + v^3 = f(-\gamma'', \alpha'') = N(-u\xi + v + us) = N\left(\frac{\bar{\xi}' - \bar{\xi}''}{\xi' - \xi''}\right) = \pm\frac{a}{\bar{a}^2}$. Последнее равенство имеет место потому, что $D_f = D_{\bar{f}}$ (тут мы обозначаем знаком N норму в кубическом поле Ω_ξ). Пусть $\alpha'' = \lambda\alpha'$; $\beta'' = \lambda\beta'$; $\gamma'' = \lambda\gamma'$; $\delta'' = \lambda\delta'$, где $\lambda > 0$. В таком случае, если $\alpha'\delta' - \beta'\gamma' = \pm 1$, то $\alpha''\delta'' - \beta''\gamma'' = \pm\lambda^2$, и, следовательно, $\lambda = \left|\frac{a}{\bar{a}}\right|$, и мы получаем $N(-\gamma'\xi + \alpha') = \pm\left|\frac{\bar{a}}{a}\right|$. Но мы имеем $\bar{f}(\bar{x}, 1) = \bar{a}\cdot N\left(\bar{x} - \frac{\delta'\xi - \beta'}{-\gamma'\xi + \alpha'}\right)$, и, следовательно $\bar{f}(\bar{x}, \bar{y}) = \frac{\bar{a}}{N(-\gamma'\xi + \alpha')}\cdot N(\alpha'\bar{x} + \beta'\bar{y} - \xi(\gamma'\bar{x} + \delta'\bar{y}))$, откуда, принимая во внимание найденное значение для $N(-\gamma'\xi + \alpha')$, мы получаем

$$\bar{f}(\bar{x}, \bar{y}) = \pm a\cdot N(\alpha'\bar{x} + \beta'\bar{y} - \xi(\gamma'\bar{x} + \delta'\bar{y})) = \pm f(x, y)\ \binom{\alpha'\beta'}{\gamma'\delta'}$$

Пример. Пусть заданы формы $(a, b, c, d) = (1, 0, 3, 2)$ и $(\bar{a}, \bar{b}, \bar{c}, \bar{d}) = (116, 219, 138, 29)$; $f(z, 1) = z^3 + 3z + z$; $\bar{f}(z, 1) = 116z^3 + 219z^2 + 138z + 29$; $D_f = D_{\bar{f}} = -216$; ξ — корень уравнения $z^3 = -3z - 2$ (I); $\bar{\xi}$ — корень уравнения $z^3 = -\frac{219}{116}z^2 - \frac{138}{116}z - \frac{29}{116}$; $\zeta = 116\bar{\xi} + 73$ — корень уравнения $z^3 = -21z + 326$ (II). В примере § 5 мы нашли переходную функцию φ от уравнения (I) к уравнению (II), а именно $\zeta = 3\xi^2 + 2\xi + 6$ и, следовательно, $\bar{\xi} = \frac{3}{116}\xi^2 + \frac{2}{116}\xi - \frac{67}{116}$, откуда по формулам (1) мы получаем

$$\alpha' = 2;\ \beta' = 1;\ \gamma' = 3;\ \delta' = 2;\ \alpha'\delta' - \beta'\gamma' = 1.$$

Таким образом $(116, 216, 138, 29) = (1, 0, 3, 2)\ \binom{2, 1}{3, 2}$, и формы эквивалентны.

Решение задачи об эквивалентности двух целочисленных кубических двоичных форм получается, таким образом, при помощи соединения теоремы этого параграфа с решением задачи, обратной задаче Чирнгаузена, данным в § 13, и не нуждается в теории приведения форм.

§ 17. Вычисление базиса кубического поля по Вороному

Рассмотрим вычисление базиса любого кольца O, содержащего данное примитивное целое число ρ кубического поля, и вычисление базиса кольца всех целых чисел кубического поля по Вороному. Пусть ρ — некоторое примитивное заданное целое число кубического поля Ω и $\rho^3 = s\rho^2 + q\rho + n$ — то уравнение, которому оно удовлетворяет, и пусть O — некоторое кольцо целых чисел поля Ω, заключающее в себе 1 и содержащее число ρ.

Определения. Базис кольца O мы называем „единичным", как мы уже это сказали в § 15, если он имеет вид:

$$1,\ \omega_1,\ \omega_2,$$

„нормальным" — если он единичный, а $\omega_1\cdot\omega_2$ — рациональное число, и

„ступенчатым в ρ" — если он имеет вид

$$1, \quad \frac{u\rho+v}{\Delta}, \quad \frac{\lambda\rho^2+\mu\rho+\nu}{\Delta},$$

где u, v, λ, μ, ν, Δ — целые рациональные числа.

Лемма: *Всякое кольцо O указанного типа имеет единичный нормальный ступенчатый базис.*

Это очевидно, так как нормализовать можно, переходя к параллельному базису (см. § 15), а это изменит в ступенчатом базисе, который во всяком таком кольце есть (см. § 14 и § 15), только коэффициенты v и ν, следовательно, не нарушает его ступенчатости.

В методе Вороного ищется именно такой базис кольца O, который одновременно — единичный, нормальный и ступенчатый в ρ.

Пусть $1, \varphi, \psi$ — один из нормальных ступенчатых в ρ базисов заданного кольца O. Из $\varphi=\frac{u\rho+v}{\Delta}$ мы получаем $\rho=\frac{\Delta}{u}\varphi-\frac{v}{u}$.

В виду того, что ρ, по предположению, — число кольца O, ρ должно линейно целочисленно представляться через числа базиса кольца O. Следовательно, $\Delta=u\cdot\delta$; $v=-u\cdot t$, где δ и t — целые рациональные числа. Таким образом

$$\varphi=\frac{\rho-t}{\delta}. \tag{1}$$

Из $\rho=\delta\cdot\varphi+t$ мы видим, что $D_\rho=\delta^6\cdot D_\varphi$, т. е. что δ входит в D_ρ в шестой степени. В виду того, что O — кольцо и 1, φ, ψ — единичный нормальный базис этого кольца, мы имеем

$$\varphi^2=-ac-b\varphi+a\psi, \tag{2}$$
$$\psi^2=-bd-d\varphi+c\psi, \tag{3}$$
$$\varphi\psi=-ad. \tag{4}$$

Напишем теперь то уравнение, которому удовлетворяет φ, в двух различных формах и сравним. Исключением ψ из (2) и (4) мы получаем

$$\varphi^3+b\varphi^2+ac\varphi+a^2d=0; \tag{5}$$

с другой стороны, мы имеем

$$F(\rho)=F(t+\delta\varphi)=F(t)+F'(t)\cdot\delta\varphi+\frac{F''(t)}{1\cdot2}\delta^2\varphi^2+\delta^3\varphi^3=0,$$

где

$$F(z)=z^3-sz^2-qz-n=0$$

то уравнение, которому удовлетворяет ρ, т. е.

$$\varphi^3+\frac{F''(t)}{2\delta}\cdot\varphi^2+\frac{F'(t)}{\delta^2}\cdot\varphi+\frac{F(t)}{\delta^3}=0. \tag{6}$$

Сравнение коэффициентов (5) и (6) дает

$$b=\frac{F''(t)}{2\delta}; \quad c=\frac{F'(t)}{\delta^2a}; \quad d=\frac{F(t)}{\delta^3a^2}, \tag{7}$$

или, в форме сравнений:

$$\frac{1}{2}F''(t)\equiv0 \pmod{\delta}; \quad F'(t)\equiv0 \pmod{\delta^2a}; \quad F(t)\equiv0 \pmod{\delta^3a^2}. \tag{7'}$$

Дискриминант O равен

$$D_O=|1, \varphi, \psi|^2=\left|1, \varphi, \frac{\varphi^2+b\varphi+ac}{a}\right|^2=\frac{1}{a^2}|1, \varphi, \varphi^2|^2=\frac{1}{a^2}\cdot D_\varphi,$$

т. е. a — квадратичный делитель D_φ, а именно

$$D_\rho=\delta^6\cdot a^2\cdot D_O. \tag{8}$$

Из (4) и (7) мы получаем

$$\psi = -\frac{ad}{\varphi} = -\frac{F(t)}{\delta^3 a\varphi} = \frac{F(\rho)-F(t)}{\delta^2 a(\rho - t)},$$

откуда

$$\psi = \frac{1}{\delta^2 a}[\rho^2 + F_1(t)\rho + F_2(t)], \tag{9}$$

где

$$F_1(t) = t - s,$$
$$F_2(t) = t^2 - st - q.$$

В любом кольце O целых чисел кубического поля Ω_ρ, которое содержит 1 и число ρ, числа его иормальиого ступенчатого в ρ базиса имеют вид (1) и (9). Наоборот, если целые рацноиальные числа δ, a, D_O, t удовлетворяют условиям (7′) и (8), то 1, φ, ψ — иормальный ступенчатый базис такого кольца.

Действительио, из (9) получается $\varphi\cdot\psi = -ad$, затем из (6) $\varphi^2 = -ac - b\varphi + a\psi$, и из этого уравнеиия, помножением иа ψ, $\psi^2 = -bd - d\varphi + c\psi$, если принять во виимаиие $\varphi\psi = -ad$, и, наконец, исключением из этих двух уравнений ψ и φ, получаем

$$\varphi^3 + b\varphi^2 + ac\varphi + a^2 d = 0$$

и

$$\psi^3 + c\psi^2 + bd\psi + ad^2 = 0.$$

Числа φ и ψ, следовательно, — целые числа одного и того же кубического поля, и 1, φ, ψ — иормальиый базис кольца O ее целых чисел, содержащего 1.

Таким образом доказана следующая теорема:

Теорема I. *Если ρ — примитивное целое кубическое число, которое удовлетворяет уравнению*

$$F(\rho) = \rho^3 - s\rho^2 - q\rho - n = 0,$$

дискриминант которого равен D_ρ, и числа δ, a, D_O, t — целые рациональные числа, удовлетворяющие условию $D_\rho = \delta^6 a^2 D_O$ и сравнениям

$$\frac{1}{2}F''(t) \equiv 0 \pmod{\delta}; \quad F'(t) \equiv 0 \pmod{\delta^2 a}; \quad F(t) \equiv 0 \pmod{\delta^3 a^2},$$

то числа

$$1, \quad \frac{\rho - t}{\delta}, \quad \frac{\rho^2 + (t-s)\rho + (t^2 - st + q)}{\delta^2 a}$$

образуют нормальный ступенчатый в ρ базис кольца O целых чисел поля Ω_ρ, содержащего 1 и число ρ, дискриминант которого равен D_O. Таким образом получаются все нормальные ступенчатые в ρ базисы всех таких колец. Тут можно предполагать, что $-\frac{a\delta}{2} < t \leqslant \frac{a\delta}{2}$.

Последнее утверждеиие следует из того, что если t — решение вышеуказаиных сравиеиий при заданиых δ и a, то $t + \delta a\cdot j$, где j — любое целое рациональное число, тоже решеиие этих сравнений, как в этом легко убедиться прямым вычислениём. Теорема I показывает, что можио легко найти все кольца целых чисел кубического поля, содержащие 1 и содержащие данное примитивное целое число ρ этого поля.

Замечание. Иидексформа (a, b, c, d) найдеииого базиса имеет

$$a = a; \qquad b = \frac{F''(t)}{2\delta}; \quad c = \frac{F'(t)}{\delta^2 a}; \qquad d = \frac{F(t)}{\delta^3 a^2}.$$

Если желательно вычислить базис совокупиости всех целых чисел поля Ω_ρ, то надо найти те δ и a, для которых вышеуказанные сравиеиия имеют корень $-\frac{a\delta}{2} < t \leqslant \frac{a\delta}{2}$ и для которых число $\delta^6 a^2$ имеет иаибольшее возможное значе-

ние, что совсем не трудно, так как $\delta^6 a^2 D_O = D_\rho$, и, следовательно, придется в каждом данном случае испытать, вообще говоря, лишь небольшое число и, вообще говоря, небольших делителей D_ρ.

Однако вычисление базиса поля Ω_ρ можно еще упростить. А именно, возьмем то уравнение, которому удовлетворяет ρ, не содержащим члена ρ^2, т. е. вида $\rho^3 = q\rho + n$, и предположим еще, что нет такого целого рационального числа τ, на квадрат которого делилось бы q, а на куб делилось бы n; если бы такое τ было, мы бы его присоединили к ρ, в том смысле, что за ρ взяли бы $\tau\rho$, и тогда в коэффициентах уравнения такие множители уже отсутствовали бы. При сделанных предположениях

$$\frac{1}{2} F''(t) = 3t = b\delta. \tag{10}$$

Числа δ и t не могут иметь общего делителя τ, отличного от 1, так как из $F'(t) = 3t^2 - q \equiv 0 \pmod{\delta^2 a}$ следует, что q делится на τ^2, а приняв это во внимание, из $F(t) = t^3 - qt - n \equiv 0 \pmod{\delta^3 a^2}$ следует, что n делится на τ^3. Но мы предположим, что такого числа τ нет. Из (10) получается поэтому $\delta = 1$ или 3. Если число $\frac{\rho \pm 1}{3}$ — не целое алгебраическое, то $\delta = 1$, если же это целое число, то $\delta = 3$. Это сейчас же следует из свойств ступенчатого базиса. Это же число, как легко видеть, целое или не целое — в зависимости от того, удовлетворяются ли сравнения

$$\left.\begin{aligned} 3 - q &\equiv 0 \pmod 9, \\ n \pm (q - 1) &\equiv 0 \pmod{27}. \end{aligned}\right\} \tag{*}$$

Таким образом получается следующая теорема Вороного:

Теорема II. *Если ρ — примитивное целое кубическое число, удовлетворяющее уравнению $F(\rho) = \rho^3 - q\rho - n = 0$, и нет целого рационального числа τ такого, на квадрат которого делится q, а на куб его n, то базис поля Ω_ρ может быть найден так:*

1°. *Если сравнения (*) не выполняются, то надо найти наибольший квадратный делитель a дискриминанта D_ρ уравнения $F(\rho) = 0$, для которого система сравнений*

$$\begin{aligned} F'(t) &\equiv 0 \pmod a; \\ F(t) &\equiv 0 \pmod{a^2} \end{aligned}$$

имеет решение $-\frac{a}{2} < t \leqslant \frac{a}{2}$, и тогда базис —

$$1, \quad \rho, \quad \frac{\rho^2 - t\rho + (t^2 - q)}{a}.$$

2°. *Если сравнения (*) выполняются, то надо найти наибольший квадратный делитель числа $\frac{D_\rho}{729}$ (которое в этом случае целое), для которого система сравнений*

$$\begin{aligned} F'(t) &\equiv 0 \pmod{9a}; \\ F(t) &\equiv 0 \pmod{27a^2} \end{aligned}$$

имеет решение $-\frac{3a}{2} < t \leqslant \frac{3a}{2}$, тогда базис —

$$1, \quad \frac{\rho - t}{3}, \quad \frac{\rho^2 + t\rho + (t^2 - q)}{9a}.$$

§ 18. Разложение простых целых рациональных чисел на простые идеалы в кубическом поле

Весьма любопытно, что разложение простого целого рационального числа p на простые идеальные множители в любом алгебраическом поле n-го порядка совпадает по существу с легко выполнимым на практике разложением на про-

стые множители по модулю p целочисленного многочлена n-ой степени $f(x)$, старший коэффициент которого равен 1 и корень ρ которого является одним из производящих целых чисел этого поля, если только p не входит в индекс этого числа ρ.

Будем, для краткости, всякий целочисленный многочлен, старший коэффициент которого равен 1, называть примарным. Заметим, что во всем дальнейшем изложении у нас будет итти речь только о разложении примарного многочлена на примарные же множители по модулю p. Мы будем говорить, что примарный многочлен $f(x)$ разлагается на примарные множители $U_t(x)$ по модулю p, если имеет место тождество:

$$f(x) = U_1(x) \cdot U_2(x) \cdot \ldots \cdot U_k(x) + p \cdot G(x), \tag{1}$$

где $G(x)$ — некоторый целочислеиный многочлен, который, вообще говоря, может уже быть не примарным. Мы будем говорить, что примарные многочлены $U_t(x)$ простые по модулю p, если каждый из этих многочленов уже не может быть в этом же смысле представлен по модулю p в виде произведения примарных многочленов более низких степеней.

Основные теоремы, принадлежащие Золотареву, состоят в следующем. Если $U_1(x)$, $U_2(x)$, ..., $U_k(x)$ — простые примарные множители $f(x)$ по модулю p и p не входит в индекс ρ, то

$$p = (p, U_1(\rho)) \cdot (p, U_2(\rho)) \ldots (p, U_k(\rho)), \tag{2}$$

где $(p, U_t(\rho)) = p \cdot \lambda + U_t(\rho) \cdot \mu$ (тут λ и μ — всевозможные целые числа поля Ω_ρ) простые идеальные множители числа p. Степени e_t многочленов U_t суть показатели тех степеней p, которые суть нормы соответственных идеалов, т. е. так называемые порядки этих идеалов. Если простое число p входит в индекс ρ, то, если p не есть общий делитель индексов всех целых чисел Ω_ρ, можно в Ω_ρ найти другое целое образующее Ω_ρ число $\bar{\rho}$, в индекс которого p уже не входит, и тогда разложение p на простые идеалы производится аналогично при помощи того уравнения, которому удовлетворяет $\bar{\rho}$. Если p есть общий делитель индексов всех целых чисел, образующих Ω_ρ, то p разлагается на простые идеалы другим, но аналогичным этому, способом.

Бывают поля, не имеющие таких общих делителей индексов всех их целых чисел. Если же такие общие делители есть, то их во всяком случае немного, например все они, во всяком случае, суть делители любого индивидуального такого индекса, а Хензель и Жилинский показали даже, что все они всегда меньше n.

В частном случае кубического поля общим делителем всех индексов может, следовательно, быть, как мы это дальше и покажем, только число 2; мы дадим разложение числа 2 в кубическом поле на простые идеалы и в этом случае. В виду того, что общая теория Золотарева излагается совершенно так же для любого n, как для $n = 3$, мы изложим ее для любого n и затем только рассмотрим разложение простых чисел p на простые идеальные множители специально в кубическом поле.

1. Разложение целого рационального простого числа p, не входящего в индекс ρ, для любого n

Теорема I. *Если примарные многочлены A и B взаимно просты, т. е. не имеют общего им примарного множителя по модулю p, то существуют такие примарные многочлены M и N, что $AM - BN \equiv c \pmod p$, где c — целое рациональное число, не делящееся на p.*

Действительно, будем производить над многочленами A и B алгорифм Эвклида, причем все члены, имеющие коэффициенты, делящиеся на p, будем при этом просто отбрасывать. Так как целое частное Q_1 примарных многочле-

нов A и B также примарно, то не может быть, чтобы остаток от деления A на B (мы предполагаем, что A не более низкой степени, чем B) равнялся нулю по модулю p, так как в таком случае A и B имели бы общего примарного делителя, а именно B, чего мы не предполагаем. Этот остаток R_1^*, вообще говоря, не будет уже примарным многочленом. Помножим его мысленно на целое рациональное число r_1^* такое, что $r_1 r_1^* \equiv 1 \pmod p$, где r_1 — его старший коэффициент. Тогда $r_1^* R_1^* \equiv R_1$ будет уже примарным многочленом, и

$$R_1^* \equiv r_1 R_1 \pmod p.$$

Таким образом, мы можем написать первый шаг алгорифма так:

$$A = BQ_1 + r_1 R_1 \pmod p,$$

где многочлены A, B, Q_1, R_1 уже примарны, а целое рациональное число r_1 не делится на p. Продолжая так дальше, мы получим:

$$\begin{aligned} B &\equiv R_1 Q_2 + r_2 R_2, \\ R_1 &\equiv R_2 Q_3 + r_3 R_3, \\ &\cdots\cdots\cdots \\ R_{n-2} &\equiv R_{n-1} Q_n + r_n, \end{aligned}$$

причем все большие буквы A, B, Q_l, R_l обозначают примарные многочлены, а все малые r — целые рациональные числа, не делящиеся на p. Последнее будет потому, что если бы какой-нибудь остаток равнялся нулю $(\mathrm{mod}\, p)$, то, возвращаясь обратно, мы убедились бы, что $A \equiv R_l K$, $B \equiv R_l L$, где R_l — примарный множитель последнего остатка, не равного нулю, и многочлены K и L примарны, т. е. A и B не были бы взаимно простые.

Из полученных равенств мы имеем последовательно: $r_1 R_1 \equiv A - BQ_1$; $r_1 r_2 R_2 \equiv -AQ_2 + B(r_1 + Q_1 Q_2)$ и т. д. и, наконец, $r_1 r_2 \ldots r_n \equiv AM - BN \pmod p$, где многочлены M и N примарны, что и доказывает теорему.

Теорема II. *Всякий примарный многочлен лишь одним способом разлагается на простые примарные множители по модулю p.*

Пусть произведение двух примарных многочленов $\varphi \cdot \theta$ делится на простой примарный многочлен ϕ по модулю p, и многочлен φ не делится на многочлен ϕ; тогда θ делится на многочлен ϕ.

Действительно, в таком случае примарные многочлены φ и ϕ — взаимно простые по модулю p, так как делителем простого примарного многочлена ϕ, по самому определению простоты, является только он сам, и, следовательно, если бы φ и ϕ имели общего делителя, то φ делилось бы на ϕ, что противоречит предположению. В силу теоремы I, есть, следовательно, такие примарные многочлены M и N, что $\varphi \cdot M - \phi N \equiv c \pmod p$, где c не делится на p. Помножим обе части этого равенства на θ, мы получим $\varphi\theta M - \phi\theta N \equiv c\theta \pmod p$, и, следовательно, если $\varphi\theta$ делится на ϕ, то $c\theta \equiv \phi\theta N \pmod p$, причем $\theta \cdot N$ примарный многочлен, т. е. во-первых, $c \equiv 1 \pmod p$ и, во-вторых, θ делится на ϕ.

Предположим теперь, что $f \equiv U_1 U_2 \ldots U_k \equiv V_1 V_2 \ldots V_l \pmod p$, где все U_i и V_i — простые $(\mathrm{mod}\, p)$ примарные многочлены. В таком случае, в силу сейчас доказанного, хоть один из множителей V_j, например V_1, делится на U_1 $(\mathrm{mod}\, p)$, т. е., так как оба они простые, с ним совпадает $(\mathrm{mod}\, p)$. Мы можем в таком случае откинуть этот множитель, так как из $U_1 K \equiv U_1 L \pmod p$, где U_1, K, L — некоторые примарные многочлены, следует $K \equiv L \pmod p$, в чем легко убедиться сравнением коэффициентов. Поступая аналогично с получающимся равенством $U_2 \ldots U_k \equiv V_2 \ldots V_l \pmod p$ и т. д., мы приходим к нужной нам теореме.

Теорема III. *Если p не входит в индекс ρ, то любое целое число поля Ω_ρ сравнимо по модулю p с целым числом этого поля, выражающимся линейно с целыми коэффициентами через степенной базис* $1, \rho, \rho^2 \ldots \rho^{n-1}$.

Действительно, всякое целое число ω поля Ω_ρ имеет вид

$$\omega = \frac{a_1\rho^{n-1} + a_2\rho^{n+2} + \ldots + a_n}{\Delta},$$

где $a_1, a_2, \ldots, a_n$ — целые рациональные, а Δ — индекс числа ρ (см. § 15). Если Δ не делится на p, то можно всегда найти такие два целых рациональных числа α и β, что $\alpha\Delta - \beta \cdot p = 1$. Отсюда мы получаем, что

$$\omega + p\beta\omega = \alpha\Delta\omega = \alpha(a_1\rho^{n-1} + a_2\rho^{n+2} + \ldots + a_n),$$

т. е. что, если Δ не делится на p, то любое целое число ω поля Ω_ρ отличается на целое число этого поля, линейно целочисленно выражающегося через степенной базис $1, \rho, \rho^2, \ldots, \rho^{n-1}$.

Теорема IV. *Если p не входит в индекс ρ, то $(p, U(\rho))$ простой идеал.*

Пусть целое число ω поля Ω_ρ не входит в идеал $(p, U_t(\rho))$. Рассмотрим целое число $\bar{\omega}$, сравнимое с ω по модулю p, выражающееся линейно целочисленно через степенной базис $1, \rho, \rho^2, \ldots, \rho^{n-1}$. Число $\bar{\omega}$ имеет вид $\phi(\rho)$, где ϕ — целочисленный полином от ρ. Будем делить многочлен $\phi(x)$ на многочлен $U_t(x)$. Он не разделится нацело, иначе было бы $\phi(\rho) = U_t(\rho)\lambda(\rho)$, где λ — многочлен, получающийся в частном, все коэффициенты которого тоже целые рациональные, так как старший коэффициент U_t равен единице. $\lambda(\rho)$ было бы целое число Ω_ρ, и $\phi(\rho)$, т. е. $\bar{\omega}$, а следовательно, и ω, против предположения, принадлежало бы идеалу $(p, U_t(\rho))$. Заменим $\phi(x)$ остатком $r(x)$, получаемым от деления его на $U_t(x)$. Остаток этот имеет степень ниже, чем $U_t(x)$, и следовательно не делится на $U_t(x) \pmod p$ и, в силу простоты $U_t(x)$ по модулю p_1, взаимно прост с $U_t(x) \pmod p$. В силу теоремы I, в таком случае существуют такие два целочисленных многочлена $r_1(x)$ и $U_{t1}(x)$, что $U_t(x)r_1(x) - r(x)U_{t_1}(x) \equiv c \pmod p$, где c не делится на p. Отсюда мы видим (см. § 5), что $r(\rho)$, а, следовательно, и $\phi(\rho)$ и ω — взаимно простые с $(p, U_t(\rho))$. Но если любое целое число ω поля Ω_ρ, не входящее в идеал $(p, U_t(\rho))$, взаимно просто с этим идеалом, то идеал этот простой, так как, если бы он не был простой, и $\mathfrak{p}$ был бы какой-нибудь его простой делитель, то всякое число, входящее в $\mathfrak{p}$, но не входящее в $(p, U_t(\rho))$, не входило бы в $(p, U_t(\rho))$ и, тем не менее, не было бы с $(p, U_t(\rho))$ взаимно простым.

Теорема V. *Порядок простого идеала $(p, U_t(\rho))$ равен степени f_t многочлена $U_t(x)$.*

Рассмотрим классы целых чисел поля Ω_ρ, несравнимые по идеалу $(p, U_t(\rho))$. Число этих классов есть, как известно (см. § 5), норма идеала $(p, U_t(\rho))$. В виду того, что, в силу теоремы III, всякое целое число поля Ω_ρ сравнимо по модулю p с числом кольца $[1, \rho, \rho^2, \ldots, \rho^{n-1}]$, достаточно рассмотреть вопрос только для чисел этого кольца.

Очевидно, что если мы выпишем все целочисленные полиномы $u(x)$ $(n-1)$-ой степени, несравнимые по модулю p, то всякое число этого кольца будет сравнимо по идеалу $(p, U_t(\rho))$ с одним из таких полиномов, куда подставлено ρ, так как можно всякое число кольца понизить до такого числа делением на p и $(U_t(\rho))$. С другой же стороны, два несравнимых таких полинома дают числа $u_1(\rho)$ и $u_2(\rho)$, разность $u_1(\rho) - u_2(\rho)$ которых не лежит в идеале $(p, U_t(\rho))$, и, следовательно, они несравнимы по модулю этого идеала. Мы видим таким образом, что норма этого идеала равна p^{f_t}, где f_t — степень $U_t(x)$, и следовательно порядок идеала $(p, U_t(\rho))$ равен f_t.

Теорема VI. $p = (p, U_1(\rho)) \cdot (p, U_2(\rho)) \ldots (p, U_k(\rho))$.

Действительно, если перемножить идеалы

$$p\lambda_1 + U_1(\rho)\mu_1,\ p\lambda_2 + U_2(\rho)\mu_2,\ \ldots p\lambda_k + U_k(\rho)\mu_k,$$

то, очевидно, получится идеал

$$p^k\nu_1 + p^{k-1}U_1(\rho)\nu_2 + p^{k-1}U_2(\rho)\nu_3 + \ldots + pU_1(\rho)U_2(\rho)\cdot\ldots\cdot U_{k-1}(\rho)\nu_{2^k-1} + \\ + U_1(\rho)\cdot\ldots\cdot U_k(\rho)\nu_{2^k},$$

где λ, μ, ν — произвольные целые числа поля Ω_ρ. Но $U_1(\rho)\,U_2(\rho)\ldots U_k(\rho) = p\cdot G(\rho)$, т. е. делится на p, а следовательно, все числа этого идеала делятся на p, т. е. и сам этот идеал делится на p; но из теоремы о норме произведения идеалов следует, что порядок произведения идеалов делителей p есть произведение порядков этих идеалов, и следовательно, рассмотренное произведение равно p.

Замечание I. Для того чтобы, в случае произвольного n, найти целое число ρ, индекс которого не делится на p, или показать, что p есть общий делитель всех индексов, достаточно, если ω_1, ω_2, ..., ω_n — базис всех целых чисел Ω_ρ, рассмотреть только p^n чисел $\omega = u_1\omega_1 + u_2\omega_2 + \ldots = u_n\omega_n$, где u_1, u_2, ..., u_n — все возможные целые рациональные коэффициенты, меньшие p, и вычислить индексы Δ_ω этих p^n чисел, пользуясь соотношением

$$D_\omega = D_\Omega\,\Delta_\omega^2.$$

Замечание II. Для того чтобы, при произвольном n, разложить p на простые идеалы в поле Ω_ρ в том случае, когда p есть общий делитель всех индексов, заметим следующее. Пусть 1, ω_2, ..., ω_n — базис Ω_ρ. В таком случае в идеале $\mathfrak{p}$ есть числа всех n сортов по отношению к этому базису, т. е. выражающиеся линейно однородно с целыми рациональными коэффициентами только через одно первое, через два первые (причем второе входит), три первые (причем третье входит) и т. д. чисел базиса, так как, например, числа p, $p\omega_2$, ..., $p\omega_n$ таковы. Если, следовательно, поступать, как в § 14, получится ступеичатый базис идеала, причем все его диагональные коэффициенты, как делители p (что следует из существования в идеале чисел p, $p\omega_2$, ..., $p\omega_n$ и минимальности этих коэффициентов) суть или p или 1. Если соответственно перенумеровать числа базиса поля Ω_ρ, то можно считать, что те из диагональных коэффициентов, которые равны p, стоят у первых f чисел базиса идеала, где f — порядок идеала, т. е. что базис идеала имеет вид:

$$\begin{aligned}
\theta_1 &= p,\\
\theta_2 &= a_{21} + p\omega_2,\\
&\cdots\cdots\cdots\\
\theta_f &= a_{f1} + a_{f2}\omega_2 + \ldots + a_{ff-1}\omega_{f-1} + p\omega_f,\\
\theta_{f+1} &= a_{f+11} + a_{f+12}\omega_2 + \ldots + a_{f+1f}\omega_f + \omega_{f+1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\theta_n &= a_{n1} + a_{n2}\omega_2 + \ldots + a_{nf}\omega_f + \omega_n,
\end{aligned}$$

причем можно еще предполагать, что все a_{ik} не отрицательны и меньше диагонального коэффициента, начинающего ту колонну, в которой стоит соответственное a_{ik} (т. е. либо меньшее p, если этот диагональный элемент равен p, либо равно 0, если он равен 1). Можно еще, наконец, предполагать, что $a_{21} = 0$, если $f \geqq 2$, так как в этом случае θ_2 имеет вид $a_{21} + p\omega_2$ и должно делиться на рассматриваемый идеал $\mathfrak{p}$, но он, по предположению, составлен только из делителей p, и, следовательно, a_{21} должно делиться на p. Тогда, вычитая из θ_2 соответственную кратность θ_1, мы получим новое θ_2, у которого уже $a_{21} = 0$.

Отсюда следует, в частности, что базисы простых идеалов 1-го и 2-го порядка кубического поля имеют вид:

$$\left.\begin{aligned}\theta_1 &= p\\ \theta_2 &= y + \omega_1\\ \theta_3 &= z + \omega_2\end{aligned}\right\} \quad \text{и} \quad \left\{\begin{aligned}\theta_1 &= p\\ \theta_2 &= p\omega_1\\ \theta_3 &= y + z\omega_1 + \omega_2,\end{aligned}\right.$$

если 1, ω_1, ω_2 — базис целых чисел этого поля, причем y и z — некоторые целые рациональные числа, неотрицательные и меньше p.

Такой вид базиса идеала делителя p можно считать нормальным. Однако не всякий такой базис будет давать идеал. Для того чтобы это получался идеал делителя $\mathfrak{p}$, необходимо и достаточно, чтобы, во-первых, решетка $[\theta_1, \theta_2, \ldots, \theta_n]$ была кольцом, т. е. чтобы все попарные произведения чисел ее базиса лежали

в ней самой, в выполнении чего можно убедиться, если имеется таблица умножающих коэффициентов для базиса $1, \omega_2, \ldots, \omega_n$, так как тогда можно получать произведения чисел, выраженные опять через тот же базис, и затем смотреть, выражаются ли они через базис $\theta_1, \theta_2, \ldots, \theta_n$, вычитая последовательно соответственные кратности θ_n, θ_{n-1} и т. д. Если $[\theta_1, \theta_2, \ldots, \theta_n]$ — кольцо, то надо еще проверить, идеал ли это (будет ли произведение любого из чисел базиса $\theta_1, \theta_2, \ldots, \theta_n$ на любое целое число ω поля Ω_ρ лежать в нем самом), для чего достаточно, в виду того, что эта решетка — кольцо, брать только числа ω, лежащие внутри параллелепипеда, построенного на $\theta_1, \theta_2 \ldots \theta_n$, т. е. числа ω такого же вида, как $\theta_1, \theta_2, \ldots, \theta_n$.

Таким образом мы сможем выписать конечное число идеалов, состоящих из делителей p, среди которых есть все простые и не простые делители p. Для любых таких двух идеалов легко убедиться, является ли один из них делителем другого или нет, для чего достаточно посмотреть, выражается ли каждое из чисел базиса второго целочисленно через числа базиса первого, что можно сделать последовательным вычитанием, как указано выше.

Те из найденных нами идеалов, которые имеют наинизший порядок, очевидно, все простые, и мы сможем только что указанным способом выделить из них те, которые различны. Затем мы так же выделим из найденных идеалов следующего порядка те, которые различны, и тем же способом проверим, не делятся ли некоторые из них на найденные простые идеалы наинизшего порядка, и оставим только те, которые не делятся, и т. д. Так мы получим в конце концов все простые идеальные делители p.

Если p — не делитель дискриминанта D_Ω поля, то разложение p на простые идеалы тем самым и найдено, так как (см. следующий параграф) в этом случае все простые идеальные делители p входят в p лишь в 1-й степени. Если же p — делитель D_Ω, то хоть один из этих делителей входит в p выше, чем в первой степени. Для того чтобы найти, какая степень $\mathfrak{p}$ входит в p, достаточно посмотреть, какой из рассматривавшихся ранее идеалов, имевших наивысший порядок, кратный порядку $\mathfrak{p}$, не делился на другие простые делители p — вопрос, решение которого заключается в уже выполненных вычислениях.

2. Переход в случае $n=3$ к другому ρ, индекс которого не делится на p

Имея то целочисленное уравнение $\rho^3 = s\rho^2 + q\rho + n$, которому удовлетворяет ρ, мы можем способом Вороного (§ 17) найти базис поля Ω_ρ, и тогда индексформа этого базиса есть (a, b, c, d), где

$$a = a; \quad b = \frac{F''(t)}{2\delta}; \quad c = \frac{F'(t)}{\delta^2 a}; \quad d = \frac{F(t)}{\delta^3 a^2}.$$

Если (a, b, c, d) — индексформа поля, т. е. индексформа кольца всех целых чисел поля, то a, b, c, d не имеют общего делителя, так как корни форм (a, b, c, d) и $k\cdot(a, b, c, d)$, где k — целый рациональный множитель, выражаются рационально друг через друга, т. е. обе эти формы соответствуют кольцам одного и того же кубического поля, а между тем дискриминант второй больше дискриминанта первой.

Теорема. *В случае кубического поля общим делителем всех индексов может быть только простое число 2, и это будет тогда и только тогда, когда оба крайние коэффициента индексформы (a, b, c, d) четные, а оба средние нечетные.*

Действительно, каково бы ни было простое число $p > 2$, можно найти такие целые рациональные числа, u и v, что индекс числа $u\omega_1 + v\omega_2$, т. е $f(u, v) = (a, b, c, d) = au^3 + bu^2v + cuv^2 + dv^3$ не делится на p. Таковою будет хоть одна из пар (1,0) (0,1) (1,1) (1,—1), так как значения f, им соответствующие, будут a, d, $a+b+c+d$, $a-b+c-d$, и если бы все они делились на p, то делились бы на p и числа a, d, $b+c$, $b-c$, $2b$, $2c$, легко из них

получаемые, и a, b, c, d должны были бы иметь общего делителя p, чего, как мы сейчас показали, быть не может. Если $p=2$, то рассмотрение этих шести чисел дает то же самое, кроме случая, когда a и d — оба четные, а b и c — оба нечетные. В этом случае $au^3+bu^2v+cuv^2+dv^3$ при любых целых рациональных u и v любой комбинации четностей, очевидно, делится на 2.

Мы видим таким образом, что если $p>2$ или $p=2$ и нет этого исключительного случая и p входит в индекс ρ, то мы найдем такие u и v, что $f(u, v)$ не делится на это p. В таком случае, $\overline{\rho}=u\omega_1+v\omega_2$, где ω_1 и ω_2 — числа базиса Вороного, будет уже целое число поля Ω_ρ, индекс $\overline{\Delta}$ которого не делится на p. Разлагая левую часть уравнения $x^3-\overline{s}x^2-\overline{q}x-\overline{u}=0$, которому оно удовлетворяет, на простые множители по модулю p, мы получим разложение p на простые идеалы.

3. Разложение простого числа 2 на простые идеалы в кубическом поле в том случае, когда 2 есть общий делитель индексов всех его целых чисел

Пусть a, d — четные и b, c — нечетные, т. е. 2 — общий делитель всех индексов. Докажем следующую теорему:

Теорема. *Если a, d, — четные и b, c — нечетные, то* $2=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, *где* $\mathfrak{p}_1=(2, \omega_1+1)$; $\mathfrak{p}_2=(2, \omega_2+1)$; $\mathfrak{p}_3=(2, \omega_1+\omega_2)$ *три различных простых идеала первого порядка, где*

$$\omega_1^3+b\omega_1^2+ac\omega_1+a^2d=0, \quad \omega_2^3+c\omega_2^2+bd\omega_2+ad^2=0.$$

Действительно, все эти три идеала отличны от единичного, так как нормы $N(\omega_1+1)=1-b+ac-a^2d$, $N(\omega_2+1)=1-c+bd-ad^2$, $N(\omega_1+\omega_2)=a^2d+ad^2+ac^2-b^2d+2acd$ делятся каждая на 2. Кроме того, идеалы $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ попарно взаимно просты, так как идеал $(\mathfrak{p}_1, \mathfrak{p}_2)$, т. е. общий делитель идеалов $\mathfrak{p}_1$ и $\mathfrak{p}_2$, содержит число $2\cdot\varphi+(\omega_1+1)\psi+(\omega_2+1)\chi$, где φ, ψ, χ — любые целые числа поля, и, в частности, содержит число $-2\frac{ad}{2}+\omega_2+1-\omega_2(\omega_1+1)=1$; аналогично идеалы $(\mathfrak{p}_1, \mathfrak{p}_3)$ и $(\mathfrak{p}_2, \mathfrak{p}_3)$ содержат каждый число $(\omega_1+1)(\omega_2+1)+2\frac{ad}{2}-(\omega_1+\omega_2)=1$. Но идеалы $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ суть делители числа 2, и, следовательно, они все три первого порядка, и $2=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Можно доказать и обратное, а именно, что если в кубическом поле $2=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, где $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ три различных простых идеала 1-го порядка, то 2 есть общий делитель индексов всех целых чисел поля.

4. Вычисление базиса для простого идеала

Мы будем предполагать, что p не входит в индекс Δ числа ρ.

1-й случай. $\mathfrak{p}=(p, \rho+\chi)$ (тут $\rho+\chi=U(\rho)$) простой идеальный делитель p 1-го порядка. Пусть $\omega_1=\frac{\rho+A}{\delta}$, $\omega_2=\frac{\rho^2+B\rho+C}{\delta^2 a}$ второе и третье числа базиса Вороного рассматриваемого поля. В силу сказанного в пункте 1-ом, базис идеала $\mathfrak{p}$ имеет вид $[p, y+\omega_1, z+\omega_2]$, где y и z — некоторые целые рациональные числа, т. е. второе и третье числа базиса θ_1 и θ_2 простого идеала имеют вид:

$$\theta_1=\frac{\rho+A+\delta y}{\delta}; \quad \theta_2=\frac{\rho^2+B\rho+C+\delta^2 az}{\delta^2 a}.$$

Для того, чтобы числа θ_1 и θ_2 делились на $\mathfrak{p}$, необходимо и достаточно, чтобы их числители делились на $\mathfrak{p}$, так как знаменатели их суть делители индекса Δ числа ρ и, следовательно, не делятся на p, т. е. взаимно простые с $\mathfrak{p}$. Разделив каждый из этих числителей на $\rho+\chi$, мы получим остатки $A+\delta y-\chi$ и $C-Bk+\delta^2 az+\chi^2$. Для делимости числителей на $\mathfrak{p}$, следовательно, достаточно, чтобы эти остатки делились на p, т. е. чтобы y и z удовлетворяли сравнениям

$A+\delta y\equiv x \pmod p$; $C+\delta^2 az\equiv -x^2+Bx \pmod p$. В виду того, что δ и a не делятся на p, эти сравнения всегда имеют решения в целых рациональных числах y и z. Если взять такие y и z, то θ_1 и θ_2 и представляют собою числа базиса $\mathfrak{p}$; действительно, в этом случае, с одной стороны, решетка $[p, \theta_1, \theta_2]$ заключается в решетке $\mathfrak{p}$, а, с другой стороны, объем основного параллелепипеда ее такой же, как и у $\mathfrak{p}$, а именно в p раз больше, чем объем основного параллелепипеда $[1, \omega_1, \omega_2]$, так как для нее переходный определитель есть

$$\begin{vmatrix} p & 0 & 0 \\ y & 1 & 0 \\ z & 0 & 1 \end{vmatrix} = p.$$

2-й случай. Пусть теперь $\mathfrak{q}$ — простой идеальный делитель p 2-го порядка, т. е. $\mathfrak{q}=(p, \rho^2+l\rho+m)$, где $\rho^2+l\rho+m$ есть $U(\rho)$. В силу сказанного в пункте 1, базис идеала $\mathfrak{q}$ в этом случае можно искать в виде $[p, p\omega_1, y+z\omega_1+\omega_2]$, где y, z — некоторые неотрицательные целые рациональные числа, меньшие p.

Таким образом, второе и третье числа базиса $\mathfrak{q}$ имеют вид

$$\theta_1 = p\omega_1; \quad \theta_2 = \frac{y\delta^2 a + z\delta a\rho + z\delta a A + \rho^2 + B\rho + C}{\delta^2 a}.$$

Рассуждая совершенно как в предыдущем случае, мы видим, что для того, чтобы это были числа базиса $\mathfrak{q}$, достаточно, чтобы y и z были таковы, что числитель θ_2 делится на $\mathfrak{q}$ (так как θ_1 делится на $\mathfrak{q}$). Разделив этот числитель на $\rho^2+l\rho+m$, мы получим в остатке $(z\delta a+B-l)\rho+(y\delta^2 a+z\delta a A+C-m)$. Очевидно, если мы найдем z и y, удовлетворяющие сравнениям:

$$\left.\begin{aligned} z\delta a + B - l &\equiv 0 \pmod p, \\ y\delta^2 a + z\delta a A + C - m &\equiv 0 \pmod p, \end{aligned}\right\}$$

числитель θ_2 будет делиться на $\mathfrak{q}$, и θ_1 и θ_2 дадут базис $\mathfrak{q}$.

Остается найти базисы для простых делителей $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ числа 2, когда 2 есть общий делитель всех индексов. Из совершенно аналогичных соображений мы находим, что они суть: $[2, \omega_1+1, \omega_2]$, $[2, \omega_1, \omega_2+1]$ и $[2, \omega_1, \omega_2]$.

§ 19. Разложение простых рациональных чисел на простые идеалы в любой максимальной трехмерной решетке

В виду того, что совокупность всех целых чисел некоторого кубического поля представляет собою совокупность одноименных координат точек неприводимой максимальной 3-мерной решетки, повторяющейся умножением, и обратно, результаты предыдущего параграфа дают, таким образом, способ в действительности разлагать простые целые рациональные числа p на простые идеалы в любой 3-мерной максимальной решетке, если она неприводима. В виду того, что нам в дальнейшем при классификации областей 4-го порядка придется разлагать простые числа на простые идеалы и в приводимых трехмерных максимальных решетках, посмотрим как это сделать.

Мы показали (см. § 5), что всякий идеал в приводимой максимальной решетке есть прямая сумма некоторых идеалов ее неприводимых частей, причем простой идеал есть, очевидно, прямая сумма опять простых же идеалов. Если максимальная решетка $O_3 = O_1 \oplus O_2$, то разложение p на простые идеалы в O_3 обусловлено его разложением в решетке всех целых чисел квадратичного поля O_2. А именно, если $p=\mathfrak{p}_1'\mathfrak{p}_2'$ в O_2, то $p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ в O_3, где

$$\begin{aligned} \mathfrak{p}_1 &= (p)\oplus(1), \\ \mathfrak{p}_2 &= (1)\oplus(\mathfrak{p}_1'), \\ \mathfrak{p}_3 &= (1)\oplus(\mathfrak{p}_2'). \end{aligned}$$

Если же p в O_2 не разлагается, то в O_3 $p = \mathfrak{p}\pi$, где

$$\mathfrak{p} = (p) \oplus (1),$$
$$\pi = (1) \oplus (p).$$

Если же O_3 есть прямая сумма трех колец первой степени, то O_3 есть просто вещественная решетка всех точек с целыми рациональными координатами. Очевидно, что каждое простое число p разлагается в этом случае на три простых идеала 1-го порядка: $p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$, где

$$\mathfrak{p}_1 = (p) \oplus (1) \oplus (1),$$
$$\mathfrak{p}_2 = (1) \oplus (p) \oplus (1),$$
$$\mathfrak{p}_3 = (1) \oplus (1) \oplus (p).$$

§ 20. Теорема о дискриминанте поля

Существует известная теорема Дедекинда, что простые числа p, вообще говоря, не содержат простых идеальных делителей в более высокой степени, чем в 1-ой, а именно, что простое число p тогда и только тогда содержит хоть один простой идеальный делитель в степени более высокой, чем 1-ая, когда оно есть делитель дискриминанта D_Ω поля. Мы докажем эту теорему для поля любого порядка n только для простых чисел, которые не суть общие делители всех индексов, а затем для кубических полей мы докажем ее полностью, рассмотрев и простое число 2, которое единственно может быть общим делителем всех индексов в случае кубического поля.

Теорема. *Простое число p, не являющееся общим делителем индексов всех целых чисел поля Ω_ρ (любого порядка n), содержит простые идеальные делители этого поля в более высокой степени, чем в 1-ой, тогда и только тогда, когда оно есть делитель дискриминанта D_Ω поля.*

Покажем, что, если p не входит в индекс ρ и $f(\rho) = 0$ — неприводимое уравнение n-ой степени, которому удовлетворяет ρ, то в равенстве

$$f(x) = U_1(x)\ U_2(x)\ \dots\ U_k(x) + p \cdot G(x) \qquad (1)$$

будут встречаться одинаковые множители $U_t(x)$ по модулю p тогда и только тогда, когда p есть делитель дискриминанта D_f. Действительно, продифференцируем равенство (1) по x и подставим $x = \rho$; мы получим

$$f'(\rho) = U_1'(\rho)\ U_2(\rho)\ \dots\ U_k(\rho) + U_1(\rho)\ U_2'(\rho)\ \dots\ U_k(\rho) + \dots +$$
$$+ U_1(\rho)\ U_2(\rho)\ \dots\ U_k'(\rho) + p\ G'(\rho). \qquad (2)$$

Предположим сначала, что все множители $U_1(x), U_2(x), \dots, U_k(x)$ различны по модулю p. Тогда все члены правой части (2) делятся на простой идеал $(p, U_1(\rho))$, а первый член не делится, так как множители $U_2(x) \dots U_k(x)$ — взаимно простые с $U_1(x)$ по модулю p (в силу нашего предположения, что все множители U_t — простые и различные по модулю p), а множитель $U_1'(x)$ — более низкой степени, чем $U_1(x)$, и потому взаимно простой с $U_1(x)$ (mod p) [$U_1'(x)$ — не примарный многочлен, но та его целая рациональная кратность, которая примарна по модулю p, взаимно проста с $U_1(x)$, чего для нас здесь достаточно]. В силу теоремы 1 § 18, все множители $U_1'(\rho), U_2(\rho), \dots, U_k(\rho)$ первого члена правой части (2) не делятся на $(p\ U_1(\rho))$, а следовательно, и сам первый член не делится на $(p, U_1(\rho))$.

Таким образом, если все множители $U_1(x), U_2(x), \dots, U_k(x)$ различны по модулю p, то $f'(\rho)$ не делится на $(p, U_1(\rho))$.

Аналогично покажем, что $f'(\rho)$ не делится и на $(p, U_2(\rho))$ и т. д., т. е. что $f'(\rho)$ взаимно просто с p. Но в таком случае и $N(f'(\rho)) = D_f$ — взаимно просто с p, т. е. p не входит делителем в D_f и, следовательно, подавно не входит в дискриминант D_Ω поля Ω_ρ.

Предположим теперь, наоборот, что среди множителей $U_1(x) \ldots U_k(x)$ есть одинаковые по модулю p, например $U_1(x)$ и $U_2(x)$. В таком случае, очевидно, все члены правой части (2) делятся на $(p, U_1(\rho))$. Тогда и левая часть (2) делится на $(p, U_1(\rho))$, а, следовательно, и $D_f = N(f'(\rho))$ делится на p. Но так как, по предположению, p не входит в индекс Δ_ρ числа ρ, а $D_f = D_{\mathfrak{Q}} \cdot \Delta_\rho^2$, то p есть делитель дискриминанта $D_{\mathfrak{Q}}$ поля $\mathfrak{Q}_\rho$.

Теорема Дедекинда, таким образом, доказана для всех простых чисел p, которые не суть общие делители всех индексов.

В случае кубического поля, т. е. когда $n = 3$, общим делителем всех индексов может быть только число 2. Но мы видели, что если 2 есть общий делитель всех индексов, т. е. если индекс-форма (a, b, c, d) поля имеет оба крайние коэффициента четные, а оба средние нечетные, то 2 разлагается на три различных простых идеала 1-го порядка, и вместе с тем в этом случае 2 не есть делитель дискриминанта $D_{\mathfrak{Q}}$ поля, так как $D_{\mathfrak{Q}} = D_{(a, b, c, d)} = b^2c^2 + 18\,abcd - 4\,ac^3 - 4b^3d - 27\,a^2d^2$ — в этом случае число нечетное; поэтому для кубического поля получается полная теорема Дедекинда.

Замечание. Теорема Дедекинда верна также и для любой приводимой максимальной трехмерной решетки, так как в простое число p может входить простой идеал в степени выше, чем в 1-й, как это ясно из разложений, выписанных в § 19, тогда и только тогда, когда $O_3 = O_1 \oplus O_2$, p имеет разложение $p = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$ и в идеалах $\mathfrak{p}_2 = (1) \oplus (\mathfrak{p}_1')$; $\mathfrak{p}_3 = (1) \oplus (\mathfrak{p}_2')$ оба идеала $\mathfrak{p}_1'$, $\mathfrak{p}_2'$ квадратичного поля O_2, одинаковые, т. е. в p входит его простой идеальный множитель квадратичного поля O_2 выше, чем в 1-й степени. Но это будет тогда и только тогда, когда p есть делитель дискриминанта D_{o_3} этого квадратичного поля, так как в квадратичном поле, как легко видеть, нет общих делителей индексов. Но $D_{o_3} = D_{o_1} \cdot D_{o_2}$ (тут D_{o_1} даже равен 1) и, следовательно, p имеет кратный простой идеальный делитель в O_3 тогда и только тогда, когда p есть делитель D_{o_2}.

Аналогично можно показать, что теорема Дедекинда верна и для любой приводимой максимальной решетки любого числа измерений.

§ 21. Дальнейшие теоремы о разложении рациональных простых чисел на простые идеалы в кубическом поле

Будем обозначать через $\mathfrak{p}$ простые идеалы 1-го, через $\mathfrak{q}$ 2-го, а через π 3-го порядка. В таком случае, если простое число p не есть делитель дискриминанта рассматриваемого кубического поля $\mathfrak{Q}_\rho$, то возможны только три случая:

$$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,$$
$$p = \mathfrak{p}\mathfrak{q},$$
$$p = \pi,$$

где $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ — различные простые идеалы 1-го порядка. Можно показать, что если кубическое $\mathfrak{Q}_\rho$ не циклическое, то есть бесконечно много простых чисел p, имеющих разложение как 1-го, так и 2-го и 3-го сорта. А именно, что плотности простых чисел этих сортов равны $\frac{1}{6}$, $\frac{3}{6}$, $\frac{2}{6}$. Если же кубическое поле циклическое, то все простые числа p имеют разложение либо 1-го, либо 3-го сорта, причем плотности соответствующих простых чисел равны $\frac{1}{3}$ и $\frac{2}{3}$. Наконец, если O_3 приводимая максимальная решетка типа $O_1 \oplus O_2$, то существуют только разложения 1-го и 2-го сорта, причем плотности соответственных простых чисел суть $\frac{1}{2}$ и $\frac{1}{2}$; если же она типа $O_1 \oplus O_1 \oplus O_1$, то все простые числа имеют только разложения 1-го сорта. Теорема о решетке $O_1 \oplus O_1 \oplus O_1$ очевидна из § 19, теорема о решетке типа $O_1 \oplus O_2$ следует из легко получаемых теорем о разложении простых чисел p в квадратичном поле. Теоремы же о неприводимой решетке O_3, т. е. о разложении простых чисел

p собственно в кубическом поле, получаются из следующей глубоко лежащей теоремы Дедекинда — Фробениуса, доказательство которой существенно связано с методами аналитической теории чисел (аналогичными методу доказательства существования бесконечного числа простых чисел в прогрессии), почему мы ее доказательства здесь приводить и не будем.

Теорема. *Если в заданном поле Ω n-го порядка порядки простых идеальных множителей простого числа p, т. е. порядки простых многочленов $U_i(x)$ в разложении $f(x)$ по модулю p (так как достаточно рассматривать лишь простые числа p, не входящие в дискриминант f), суть $f_1, f_2, \ldots, f_k$, то в группе Галуа Γ этого поля, рассматриваемой как группа перестановок его n координат, существует подстановка, неприводимые циклы которой — как раз этих порядков.* [Эта первая часть теоремы была впервые доказана Дедекиндом и может быть доказана (см., напр., Чеботарев, „Теорема Галуа“) совсем элементарно при помощи теории конечного поля.] *Обратно, если в группе Галуа Γ есть подстановка, неприводимые циклы которой имеют порядки $f_1, f_2, \ldots, f_k$, то существует бесконечно много простых чисел p, в разложении которых простые идеалы (простые множители $U_i(x)$) имеют как раз эти порядки, причем плотности совокупностей таких простых чисел равны $\frac{l}{N}$, где l — число подстановок такого циклового типа в группе Γ, а N — порядок группы Γ.* (Эта обратная часть теоремы была доказана в 1896 году Фробениусом и требует пока для своего доказательства методов аналитической теории чисел.)

Существует простой критерий для того, чтобы узнать, имеет ли простое число p разложение 1-го или 3-го рода, или разложение 2-го рода; этот критерий дан в диссертации Вороного. А именно, первый случай будет тогда, и только тогда, когда D_Ω — квадратичный вычет, а второй, когда D_Ω — квадратичный невычет по модулю p. Этот критерий есть также лишь частный случай некоторого общего критериума для полей n-го порядка, найденного впервые Штикельбергером в 1897 г. Оба эти критерия доказываются совсем просто при помощи теории конечного поля. Мы, однако, доказательства приводить не будем.

Наконец, наиболее полное решение задачи о том, какие простые числа имеют разложение 1-го, какие 2-го и какие 3-го сорта в данном кубическом поле, дает теорема Такаги — Гассе, доказательство которой требует не только методов аналитической теории чисел, но и теорем теории поля классов (см. Hasse [1]). Она состоит в следующем.

Теорема. *Пусть D_Ω — дискриминант кубического поля Ω; тогда все целочисленные квадратичные двойничные формы этого дискриминанта D_Ω распадаются на число классов h, которое делится на 3. Вполне определенная треть этих классов квадратичных форм представляет те и только те простые числа p, которые имеют разложение 1-го сорта, а остальные две трети — те и только те, которые имеют разложение 3-го сорта. Если D_Ω — не полный квадрат, т. е. поле Ω — не циклическое, то все остальные простые числа, т. е, те, для которых D_Ω — квадратичный невычет и которые, следовательно, не представляются никаким из классов рассматриваемых квадратичных форм, имеют разложение 2-го сорта.*

Доказательства этой теоремы мы здесь также приводить не будем.

Надо заметить, что эта теорема была высказана без доказательства Вороным еще в 1898 году в его докладе на Съезде естествоиспытателей и врачей в Тбилиси, поэтому, может быть, следует называть эту теорему теоремой Вороного.

§ 22. Определение группы классов идеалов кубического поля

Определить число классов идеалов неприводимого максимального кольца можно, используя то обстоятельство, что в каждом классе существует идеал, норма которого не превосходит некоторой границы, известной, как только

известен дискриминант кольца. В I главе такая граница была указана в § 5 для неприводимых максимальных колец любого порядка. Она равна

$$\left(\frac{4}{\pi}\right)^{\tau}\frac{n!}{n^n}\sqrt{|D|},$$

где n — порядок кольца, D — дискриминант и τ — число пар комплексных координат. Отсюда для интересующего нас случая $n=3$ мы получим следующие границы:

$$\frac{2}{9}\sqrt{D} \quad \text{для} \quad D>0,$$
$$\frac{8}{9\pi}\sqrt{|D|} \quad \text{для} \quad D<0.$$

Однако эти границы могут быть еще немного улучшены посредством использования оценки минимума кубической двоичной формы, что будет сделано в следующей главе в § 34. Этим способом получаются границы:

$$\frac{4}{27}\sqrt{D} \quad \text{для} \quad D>0,$$
$$\left(\frac{8}{7.53\sqrt{3}}\right)^3\sqrt{|D|} \quad \text{для} \quad D<0.$$

Эти оценки немного точнее тех, которые были получены из общих оценок при $n=3$. Из этих оценок следует, что для $D<182$, $D>0$ и $|D|<83$, $D<0$ число классов идеалов равно 1, ибо при выполнении этих неравенств в каждом классе найдется идеал, норма которого меньше 2.

Для определения числа классов в общем случае можно предложить следующий порядок действий.

1. Установить границу L для норм представителей каждого класса идеалов.
2. Выбрать в кольце число ρ, по возможности с меньшим индексом.
3. Разложить на простые множители нормы чисел $\rho+\varkappa$ для

$$-\frac{L}{2}\leqslant\varkappa<\frac{L}{2},$$

для того чтобы найти простых делителей 1-го порядка этих норм.

4. Составить базисы для всех простых и составных идеалов, имеющих нормы, не превосходящие L.

5. При помощи метода, о котором будет итти речь в главе III, испытать все пары решеток, соответствующих построенным идеалам, на подобие.

Тогда неподобные решетки дадут представителей всех классов идеалов. Таким образом, число классов идеалов может быть найдено в конечном числе действий.

При фактическом определении числа классов, количество испытаний на подобие может быть значительно уменьшено благодаря тому, что в процессе разложения числа $\rho+\varkappa$ на простые идеалы устанавливается большое количество отношений эквивалентности между различными простыми идеалами. Иногда даже удается совершенно избежать испытаний на подобие.

Иллюстрируем все сказанное примером.

Пример. Определить число классов идеалов в $\Omega\sqrt[3]{7}$.

В этом случае $D_\Omega=-27\cdot 7^2$ и, следовательно,

$$L=\left(\frac{8}{7.53\sqrt{3}}\right)^3 7\sqrt{27}=8.5\ldots$$

Берем $\rho=\sqrt[3]{7}$. Индекс ρ равен 1.

Для решения задачи нам прежде всего нужно разложить на простые идеалы числа 2, 3, 5 и 7.

Имеем

$$\begin{aligned} N(\rho-3) &= -20 = -2^2\cdot 5 \\ N(\rho-2) &= -1 \\ N(\rho-1) &= 6 = 2\cdot 3 \\ N(\rho) &= 7 \\ N(\rho+1) &= 8 = 2^3 \\ N(\rho+2) &= 15 = 3\cdot 5 \\ N(\rho+3) &= 34 = 2\cdot 17 \end{aligned}$$

Из этих разложений заключаем, что

$$2=\mathfrak{p}_2\mathfrak{q}_2,\quad 3=\mathfrak{p}_3^3,\quad 5=\mathfrak{p}_5\mathfrak{q}_5,\quad 7=\mathfrak{p}_7^3.$$

При этом $\rho-1=\mathfrak{p}_2\mathfrak{p}_3$, $\rho+2=\mathfrak{p}_3\mathfrak{p}_5$, $\rho=\mathfrak{p}_7$.

Из того, что $\mathfrak{p}_3^3=3$, следует, что класс, которому принадлежит $\mathfrak{p}_3$, утроением дает главный класс. Обозначим этот класс через K. Из равенства

$$\rho-1=\mathfrak{p}_2\mathfrak{p}_3$$

следует, что $\mathfrak{p}_2$ принадлежит классу K^2 и $\mathfrak{q}$ — классу K. Из равенства $\rho+2=\mathfrak{p}_3\mathfrak{p}_5$ следует, что $\mathfrak{p}_5\in K^2$, $\mathfrak{q}_5\in K$.

Таким образом, число классов идеалов равно 1 или 3, в зависимости от того, будет ли класс K, которому принадлежит $\mathfrak{p}_3$, главным или нет.

Выяснить этот вопрос можно, не обращаясь к алгорифмам четвертой главы. Действительно, для нашего кольца известна единица $\varepsilon=2-\rho$, которая, как легко проверить при помощи „извлечения корня", будет основной единицей. Если бы $\mathfrak{p}_3$ было главным идеалом, произведенным некоторым числом α, то имело бы место равенство

$$3=\alpha^3\varepsilon^n,$$

откуда следовало бы, что или 3, или 3ε, или $3\varepsilon^2$ представляет собой куб некоторого числа кольца. Легко проверить посредством извлечения корня, что это не имеет места.

Следовательно $h=3$, и представителями классов являются 1, $\mathfrak{p}_3$ и $\mathfrak{p}_3^2$.

§ 23. Различные формы, связанные с кубическим полем

Во вводной главе было показано, что с решеткой, повторяющейся умножением, а также с решетками, рационально расположенными относительно таких решеток, связаны некоторые формы от n переменных, именно эрмитиан, форма Дирихле и форма Кэли.

Приведем формулы, дающие возможность фактически написать эти формы для $n=3$, в случае если решетка дана. При этом условимся тройничную кубическую форму, для краткости записи, писать в виде треугольной таблицы коэффициентов. Так, форма

$$\begin{aligned} F(x_1, x_2, x_3) = {} & Ax_1^3 + Bx_1^2x_2 + Cx_1^2x_3 + Ex_1x_2^2 + Fx_1x_2x_3 + \\ & + Gx_1x_3^2 + Hx_2^3 + Kx_2^2x_3 + Lx_2x_3^2 + Mx_3^3 \end{aligned}$$

будет нами записываться в виде

$$\begin{array}{c} H,\ K,\ L,\ M \\ E,\ F,\ G \\ B,\ C \\ A \end{array}$$

Пусть решетка представляет собою кольцо, заданное индексформой

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Ее эрмитианом будет форма

$$D_0(x_1, x_2, x_3) = 3x_1^2 + 2bx_1x_2 + 2cx_1x_3 + (b^2 - 2ac)x_2^2 + 6adx_2x_3 + (c^2 - 2bd)x_3^2.$$

Форма Дирихле:

$$N(x_1, x_2, x_3) = \begin{matrix} -a^2d, & a(c^2 - 2bd), & d(b^2 - 2ac), & ad^2 \\ ac, & bc - 3ad, & bd & \\ b, & c & & \\ 1 & & & \end{matrix}$$

Форма Кэли:

$$N^*(x_1, x_2, x_3) = \begin{matrix} d, & c, & b, & a \\ -2bd, & -bc - 3ad, & -2ac & \\ d(b^2 + ac), & a(c^2 + bd) & & \\ ad(ad - bc) & & & \end{matrix}$$

Наконец, приведем некоторые факты из теории разложимых тройничных кубических форм.

Во-первых, укажем, что необходимым и достаточным условием для того, чтобы форма была разложимой, является равенство гессиана формы самой форме, с точностью до постоянного множителя.

Доказывать это утверждение не будем. Найти доказательство можно в любом курсе высшей алгебры или аналитической геометрии, в котором излагаются элементы теории инвариантов.

Гессиан (точнее, половина гессиана)

$$\begin{matrix} H', K', L', M' \\ E', F', G' \\ B', C' \\ A' \end{matrix}$$

формы

$$\begin{matrix} H, K, L, M \\ E, F, G \\ B, C \\ A \end{matrix}$$

может быть вычислен по формулам:

$$A' = 12AEG - 3AF^2 + 4BCF - 4C^2E - 4B^2G,$$
$$B' = 12AEL + 8BCK + BF^2 - 12AKF - 4B^2L + 36AHG - 12C^2H - 4BEG,$$
$$F' = F^3 - 4F(CK + BL + EG) + 12(BKG + CEL - CHG - AKL - BEM) + 108AHM.$$

Выражения для остальных коэффициентов аналогичны, если только треугольную схему заданной формы соответственно повернуть.

Миожитель, которым отличается гессиан разложимой формы от самой формы, представляет собой не что иное, как дискриминант формы, который, таким образом, может быть непосредственно выражен через коэффициенты формы в виде дробной рациональной функции. В виде целой рациональнй функци от коэффициентов формы дискриминант не может быть представлен, однако квадрат дискримннанта, в силу соотношений между коэффициентами формы, представляется целым рациональным образом. Именно,

$$D^2 = F^4 - 8F^2(EG + BL + CK) + 24F(BGK + ECL + AKL + HCG + MBE) - 216FAHM + 16(B^2L^2 + C^2K^2 + E^2G^2 - BLEG - CKEG - BLCK) - 48(AEL^2 + AGK^2 + HBG^2 + HLC^2 + MKB^2 + MCE^2) + 144(AHGL + AMEK + HMBC).$$

Квадрат дискриминанта разложимой формы совпадает с одним из инвариантов общей кубической тройничной формы.

Наконец, коэффициенты формы Кэли, будучи умножены на дискриминант, могут быть представлены через коэффициенты исходной формы, по формулам:

$$A^* = F(9HM - KL) - 2E(3KM - L^2) - 2G(3HL - K^2),$$
$$B^* = 12BKM - 4BL^2 - 18CMH + 2CKL + F^2L + 6G^2H - 3EFM + 2EGL - 3FKG,$$
$$F^* = -F^3 + 54AHM + 4F(KC + LB + EG) - 6(AKL + BEM + CGH + KGB + LEC)$$

Остальные коэффициенты представляются аналогичными формулами, если только треугольную схему заданной формы соответственно повернуть. Форма, коэффициенты которой вычисляются по этим формулам, будет контравариантом формы $N(x_1, x_2, x_3)$ также и в том случае, когда эта последняя неразложима.

§ 24. Кубические циклические поля

Кубическим циклическим полем называется кубическое поле, совпадающее с сопряженными. Если ρ — производящее число такого поля, то сопряженные с ним числа ρ' и ρ'' рационально выражаются через ρ.

Покажем, что для того, чтобы поле Ω_ρ было циклическим, необходимо и достаточно, чтобы дискриминант неприводимого уравнения, корнем которого является производящее число ρ, был полным квадратом рационального числа.

В самом деле, пусть поле Ω_ρ — циклическое. Тогда ρ' рационально выражается через ρ. Представим ρ' через ρ в канонической форме:

$$\rho' = a\rho^2 + b\rho + c.$$

Рассмотрим числа $\omega_1 = a\rho'^2 + b\rho' + c$ и $\omega_2 = a\rho''^2 + b\rho'' + c$. Они, вместе с $\rho' = a\rho^2 + b\rho + c$, являются корнями некоторого кубического уравнения с рациональными коэффициентами. Так как это уравнение имеет общий корень ρ' и одинаковую степень с неприводимым уравнением, которому удовлетворяет ρ, то они должны совпадать. Следовательно, или $\omega_1 = \rho$, $\omega_2 = \rho''$, или $\omega_1 = \rho''$, $\omega_2 = \rho$. Первая возможность, очевидно, отпадает, ибо ρ'' не может быть корнем квадратного уравнения с рациональными коэффициентами. Остается вторая возможность:

$$\rho'' = \omega_1 = a\rho'^2 + b\rho' + c,$$
$$\rho = \omega_2 = a\rho''^2 + b\rho'' + c.$$

Таким образом, ρ'' выражается через ρ' и ρ через ρ'' точно так же, как ρ' через ρ.

Рассмотрим число $\lambda = \rho' - \rho''$. Это число принадлежит полю Ω_ρ. В силу сказанного выше сопряженные с ним числа суть $\lambda' = \rho'' - \rho$ и $\lambda'' = \rho - \rho'$. Норма числа λ, $N(\lambda) = (\rho' - \rho'')(\rho'' - \rho)(\rho - \rho')$ представляет собой рациональное число. Но число

$$(N(\lambda))^2 = [(\rho' - \rho'')(\rho'' - \rho)(\rho - \rho')]^2$$

равно дискриминанту числа ρ. Тем самым доказано, что если поле Ω_ρ — циклическое, то дискриминант производящего числа ρ равен квадрату рационального числа.

Обратно, пусть ρ — корень неприводимого уравнения $\rho^3 = s\rho^2 + q\rho + n$, дискриминант которого равен полному квадрату рационального числа l:

$$(\rho - \rho')^2(\rho' - \rho'')^2(\rho'' - \rho)^2 = l^2.$$

Тогда

$$(\rho - \rho')(\rho' - \rho'')(\rho'' - \rho) = l.$$

Но $(\rho-\rho')(\rho-\rho'')=\delta(\rho)=3\rho^2-2s\rho+q$. Следовательно,

$$\rho'-\rho''=-\frac{l}{3\rho^2-2s\rho+q}.$$

С другой стороны, $\rho'+\rho''=s-\rho$. Таким образом, $\rho'-\rho''$ и $\rho'+\rho''$, а следовательно также ρ' и ρ'', рационально выражаются через ρ, то есть поле Ω_ρ циклическое, что и требовалось доказать.

Неприводимые кубические уравнения, корнями которых являются числа циклических полей, называются циклическими кубическими уравнениями. Для кубических циклических уравнений легко дать параметрическое представление, а именно выразить коэффициенты через некоторые два параметра α, β так, что при рациональных значениях этих параметров уравнение будет циклическим или приводимым, и наоборот, для каждого циклического уравнения найдутся соответствующие рациональные значения этих параметров.

Покажем, что для уравнений, в которых коэффициент при ρ равен нулю, таким представлением будет:

$$\rho^3=3(\alpha^2+\alpha\beta+\beta^2)\cdot\rho+(\alpha-\beta)(\alpha^2+\alpha\beta+\beta^2). \tag{1}$$

Действительно, дискриминант D такого уравнения

$$D=4\cdot27(\alpha^2+\alpha\beta+\beta^2)^3-27(\alpha-\beta)^2\cdot(\alpha^2+\alpha\beta+\beta^2)^2=$$
$$=81(\alpha+\beta)^2(\alpha^2+\alpha\beta+\beta^2)^2$$

представляет собой полный квадрат рационального числа, при рациональных значениях параметров α и β. Обратно, если дискриминант уравнения $\rho^3=q\rho+n$ представляет собой полный квадрат, легко найти соответствующие рациональные значения для параметров α и β. Достаточно положить

$$\alpha-\beta=\frac{3n}{q},$$

$$\alpha+\beta=-\frac{\sqrt{D}}{3q}$$

и решить эту систему относительно α и β.

Тем самым доказано, что уравнение (1) дает параметрическое представление для кубических циклических уравнений, в которых $s=0$.

Скажем несколько слов о единицах циклической области. В циклических областях, так же как и во всяких кубических областях положительного дискриминанта, все единицы могут быть представлены в виде произведения степеней двух основных единиц. При этом, если ε_1 и ε_2 — пара основных единиц, то всякая пара η_1, η_2, где $\eta_1=\varepsilon_1^a\varepsilon_2^b$, $\eta_2=\varepsilon_1^c\varepsilon_2^d$, есть также пара основных единиц, если $ad-bc=\pm1$. Покажем, что в каждом циклическом кольце существует пара сопряженных основных единиц, причем если ε_0, ε_0' одна из таких пар, то все остальные возможные пары будут ε_0', ε_0''; ε_0'', ε_0; $\frac{1}{\varepsilon}$, $\frac{1}{\varepsilon'}$; $\frac{1}{\varepsilon'}$, $\frac{1}{\varepsilon''}$; $\frac{1}{\varepsilon''}$, $\frac{1}{\varepsilon}$.

Для доказательства рассмотрим какую-нибудь пару основных единиц ε_1 и ε_2 и введем в рассмотрение сопряженные числа ε_1' и ε_2'. Они будут являться также единицами рассматриваемого кольца, и, следовательно,

$$\varepsilon_1'=\varepsilon_1^{m_1}\varepsilon_2^{n_1},$$

$$\varepsilon_2'=\varepsilon_1^{m_2}\varepsilon_2^{n_2}.$$

Показатели m_1, n_1, m_2, n_2, конечно, должны быть связаны некоторыми соотношениями. Найдем эти соотношения. Для этого перейдем к единицам ε_1'' и ε_2''.

$$\varepsilon_1'' = (\varepsilon_1')^{m_1}(\varepsilon_2')^{n_1} = \varepsilon_1^{m_1^2 + n_1 m_2} \cdot \varepsilon_2^{n_1 m_1 + n_1 n_2},$$
$$\varepsilon_2'' = (\varepsilon_1')^{m_2}(\varepsilon_2')^{n_2} = \varepsilon_1^{m_1 m_2 + m_2 n_2} \cdot \varepsilon_2^{n_1 m_2 + n_2^2}.$$

В виду того, что $\varepsilon_1\varepsilon_1'\varepsilon_1'' = \varepsilon_2\varepsilon_2'\varepsilon_2'' = 1$, между показателями m_1, n_1, m_2, n_2 должны быть выполнены соотношения

$$\left.\begin{aligned} 1 + m_1 + m_1^2 + n_1 m_2 &= 0 \\ n_1 + n_1 m_1 + n_1 n_2 &= 0 \\ m_2 + m_1 m_2 + n_2 m_2 &= 0 \\ 1 + n_2 + n_2^2 + n_1 m_2 &= 0 \end{aligned}\right\}$$

Если $1 + m_1 + n_2 \neq 0$, то $n_1 = m_2 = 0$ и удовлетворить первому соотношению $1 + m_1 + m_1^2 = 0$ невозможно.

Следовательно, $1 + m_1 + n_2 = 0$.

При этом второе и третье соотношения будут удовлетворены, а первое и четвертое превращаются в

$$m_1 n_2 - m_2 n_1 = 1,$$

ибо

$$1 + m_1 + m_1^2 + n_1 m_2 = 1 - (m_1 n_2 - m_2 n_1) + m_1 (1 + m_1 + n_2),$$
$$1 + n_2 + n_2^2 + n_1 m_2 = 1 - (m_1 n_2 - m_2 n_1) + n_2 (1 + m_1 + n_2).$$

Итак, показатели удовлетворяют двум соотношениям

$$1 + m_1 + n_2 = 0,$$
$$m_1 n_2 - m_2 n_1 = 1.$$

Пусть $\varepsilon_0 = \varepsilon_1^x \varepsilon_2^y$ некоторая единица. Тогда сопряженная с ней единица ε_0' представится в виде:

$$\varepsilon_0' = \varepsilon_1^{m_1 x + m_2 y} \cdot \varepsilon_2^{n_1 x + n_2 y}.$$

Для того, чтобы ε_0, ε_0' была парой основных единиц, необходимо и достаточно, чтобы было:

$$x(n_1 x + n_2 y) - y(m_1 x + m_2 y) = \pm 1,$$

или

$$n_1 x^2 + (n_2 - m_1) xy - m_2 y^2 = \pm 1.$$

Дискриминант квадратичной формы, находящейся в левой части последнего равенства, равен

$$(n_2 - m_1)^2 + 4 n_1 m_2 = (n_2 + m_1)^2 - 4(m_1 n_2 - n_1 m_2) = -3.$$

Известно, что каждая квадратичная форма с целыми рациональными коэффициентами и с дискриминантом, равным -3, эквивалентна одной из форм $\pm(x^2 + xy + y^2)$ и представляет $+1$ (или -1) шестью способами. Эти шесть представлений определяют шесть возможных пар $\varepsilon_0, \varepsilon_0'$ сопряженных основных единиц. При этом, если ε_0, ε_0' — одна из таких пар, то остальные пять будут:

$$\varepsilon_0', \varepsilon_0''; \quad \varepsilon_0'', \varepsilon_0; \quad \frac{1}{\varepsilon_0}, \frac{1}{\varepsilon_0'}; \quad \frac{1}{\varepsilon_0'}, \frac{1}{\varepsilon_0''}; \quad \frac{1}{\varepsilon_0''}, \frac{1}{\varepsilon_0}.$$

Это нам и нужно было доказать.

В заключение отметим некоторые особенности в разложении простых чисел на простые идеалы в случае циклических кубических максимальных колец. В виду того, что дискриминанты таких колец представляют собой полные квадраты, легко усмотреть из теоремы V, что для данного простого числа p имеются только следующие возможности разложения на простые идеалы:

$p = \mathfrak{p}^3$, если p входит в дискриминант. При этом p не может быть равно 2.

$$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$$

и (p) — простой идеал.

Простых идеалов второго порядка в циклических кольцах не существует.

Легко видеть далее, что если $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, то простые идеалы $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ суть сопряженные идеалы, т. е. $\mathfrak{p}_2$ и $\mathfrak{p}_3$ могут быть получены из $\mathfrak{p}_1$ циклическими перестановками координат или, в геометрическом представлении, решетки соответствующих идеалов $\mathfrak{p}_2$ и $\mathfrak{p}_3$ получаются из решетки идеала $\mathfrak{p}_1$ вращением вокруг рациональной прямой на углы $\frac{2\pi}{3}$ и $\frac{4\pi}{3}$.

Действительно, если $\mathfrak{p}_1$ — простой идеал первого порядка, то решетки $\mathfrak{p}_1'$ и $\mathfrak{p}_1''$, получающиеся из $\mathfrak{p}_1$ вращением на углы $\frac{2\pi}{3}$ и $\frac{4\pi}{3}$ вокруг рациональной прямой, будут также идеалами простыми и первого порядка, входящими в то же простое число p. Если $\mathfrak{p}_1$, $\mathfrak{p}_1'$ и $\mathfrak{p}_1''$ различны, то число p, делясь на каждый из них порознь, должно делиться и на их произведение. Следовательно, в этом случае

$$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3.$$

Нам остается показать, что если $\mathfrak{p}_1 = \mathfrak{p}_1' = \mathfrak{p}_1''$, то $p = \mathfrak{p}_1^3$. Для этого возьмем число ρ, делящееся на $\mathfrak{p}_1$ и не делящееся на $\mathfrak{p}_1^2$ и на другие идеалы, входящие в p, если бы таковые существовали. Число ρ будет корнем некоторого кубического уравнения:

$$\rho^3 = s\rho^2 + q\rho + n.$$

В виду того, что $\mathfrak{p} = \mathfrak{p}' = \mathfrak{p}''$, числа ρ' и ρ'' вместе с ρ будут делиться на $\mathfrak{p}$. Следовательно, коэффициенты

$$s = \rho + \rho' + \rho'', \quad -q = \rho\rho' + \rho'\rho'' + \rho''\rho \quad \text{и} \quad n = \rho\rho'\rho''$$

будут также делиться на $\mathfrak{p}$ и, будучи целыми рациональными числами, будут делиться на p. Следовательно, ρ^3 делится на p, что возможно, только если $p = \mathfrak{p}^3$, так как ρ не делится ни на один из идеалов, входящих в p, кроме $\mathfrak{p}$.

Укажем, наконец, что простые числа p, для которых имеет место разложение $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, расположены в нескольких арифметических прогрессиях с разностью, равною $\sqrt{D}$; простые же числа, остающиеся простыми в циклическом кольце, расположены в остальных арифметических прогрессиях с разностью $\sqrt{D}$.

Доказывать это утверждение не будем. Оно является частным случаем более общей теоремы Кронекера об абелевых полях.

§ 25. Чисто кубические поля

Чисто кубическим полем называется поле, производящим числом которого является кубический корень из рационального числа. Такие поля играют существенную роль в теории кубических чисел, как наиболее простые из кубических полей отрицательного дискриминанта; они были рассмотрены в работах Маркова [29] и Дедекинда [10].

Для чисто кубических полей очень просто решается задача о базисе для целых чисел поля. Пусть $\rho=\sqrt[3]{A}$ — производящее число поля. Без нарушения общности можно считать A положительным целым рациональным числом, свободным от кубических множителей. Положим $A=fg^2$, где f и g — целые числа, свободные от квадратичных множителей. Введем обозначения $\bar{A}=f^2g$ и $\bar{\rho}=\sqrt[3]{\bar{A}}$. Каждое число поля Ω_ρ

$$\omega=\alpha+\beta\rho+\gamma'\rho^2$$

может быть представлено в виде $\alpha+\beta\rho+\gamma\bar{\rho}$, ибо $\rho^2=\sqrt[3]{f^2g^4}=g\bar{\rho}$.

Пусть $\omega=\alpha+\beta\rho+\gamma\bar{\rho}$ — целое число поля Ω_ρ и $\omega^3=s\omega^2+q\omega+n$ — уравнение, корнем которого является ω. Коэффициенты s, q, n этого уравнения суть целые рациональные числа. Легко подсчитать, что

$$s=3\alpha;$$
$$q=-3\alpha^2+3\beta\gamma fg;$$
$$n=\alpha^3+\beta^3A+\gamma^3\bar{A}-3\alpha\beta\gamma fg$$

и дискриминант $D(\omega)=-27(\beta^3A-\gamma^3\bar{A})^2$.

Из этих равенств прежде всего заключаем, что числа

$$3\alpha=s;\quad 9\beta\gamma fg=(3\alpha)^2+q \quad\text{и}\quad 27\beta^3A+27\gamma^3\bar{A}=27n-(3\alpha)^3+3\cdot(3\alpha)\cdot(9\beta\gamma fg)$$

суть целые числа. Следовательно, $27\beta^3A$ и $27\gamma^3\bar{A}$ суть также целые числа, ибо их сумма и произведение, равное $(9\beta\gamma fg)^3$, числа целые. Отсюда, наконец, следует, что 3β и 3γ — целые, так как A и $\bar{A}$ не содержат кубических множителей. Итак, если ω — целое число поля Ω_ρ, то оно может быть представлено в виде $\omega=\frac{a+b\rho+c\bar{\rho}}{3}$ с целыми коэффициентами a, b и c. Эти коэффициенты должны удовлетворять сравнениям:

$$a^2-bcfg\equiv 0, \pmod 3 \tag{1}$$
$$a^3+b^3A+c^3\bar{A}-3abcfg\equiv 0. \pmod{27} \tag{2}$$

Покажем, что если одно из чисел a, b и c делится на 3, то делятся на 3 и остальные два. Достаточно рассмотреть случай, когда a делится на 3. Тогда $b^3A+c^3\bar{A}$ делится на 9, $bcfg$ делится на 3. Числа b^3A и $c^3\bar{A}$ оба делятся на 9, ибо их сумма делится на 9, а произведение на 27. Так как одно из чисел A, $\bar{A}$ не делится на 9, то одно из чисел b, c должно делиться на 3, но тогда, в силу сравнения (2), другое также должно делиться на 3.

Исследуем, при каких условиях число $\omega=\frac{a+b\rho+c\bar{\rho}}{3}$ может быть целым при a, не делящемся на 3. Вместо чисел a, b и c можно ввести в рассмотрение их абсолютно-наименьшие вычеты по модулю 3, причем a можно положить равным 1. Положим $b\equiv\sigma_1=\pm 1$; $c\equiv\sigma_2=\pm 1$. Сравнения (1) и (2) перепишутся в виде:

$$\sigma_1\sigma_2fg\equiv 1, \pmod 3,$$
$$1+\sigma_1fg^2+\sigma_2f^2g-3\sigma_1\sigma_2fg\equiv 0. \pmod{27}.$$

Из первого сравнения заключаем, что f и g не делятся на 3 и $\sigma_1f\equiv\sigma_2g \pmod 3$. Положим $\sigma_1f=3k+\lambda$, $\sigma_2g=3l+\lambda$; $\lambda=\pm 1$. Подставив во второе сравнение, получим

$$1+2\lambda^3-2\lambda^2+9(k+l)(\lambda-\lambda^2)+9(k-l)^2\lambda\equiv 0 \pmod{27},$$

откуда следует, что $\lambda=+1$ и $k\equiv l \pmod 3$.

Итак, число $\omega = \frac{1+\sigma_1\rho+\sigma_2\bar{\rho}}{3}$ при $\sigma_1 = \pm 1$, $\sigma_2 = \pm 1$ будет целым тогда и только тогда, если $\sigma_1 f \equiv \sigma_2 g \pmod 9$, $\sigma_1 \equiv f \pmod 3$ и $\sigma_2 \equiv g \pmod 3$. Удовлетворить этим условиям можно, только если $A \equiv \pm 1 \pmod 9$.

Действительно, если $\sigma_1 f \equiv \sigma_2 g \pmod 9$, то $A = fg^2 \equiv f^3 \equiv \pm 1 \pmod 9$. Обратно, если $A = fg^2 \equiv \pm 1 \pmod 9$, то $fg^3 \equiv \pm g \pmod 9$, но $g^2 = \pm 1 \pmod 9$. Следовательно, $f \equiv \pm g \pmod 9$, и можно подобрать числа σ_1 и σ_2, удовлетворяющие всем требованиям.

Окончательно, за базис чисто кубического поля может быть принята система чисел 1, ρ, $\bar{\rho}$, если $A \not\equiv 1 \pmod 9$, и система чисел 1, ρ, $\frac{1+f\rho+\sigma_2\bar{\rho}}{3}$, если $A \equiv 1 \pmod 9$.

Дадим теперь параметрическое представление для уравнений, корнями которых являются числа чисто кубических полей. Для этого прежде всего покажем, что необходимым и достаточным условием для того, чтобы кубическое число ω было чисто кубическим, является

$$D(\omega) = -3d^2$$

при рациональном d.

Необходимость этого условия вытекает из проведенного выше подсчета дискриминанта чисто кубического числа.

Докажем достаточность. Пусть $\omega^3 = s\omega^2 + q\omega + n$ — уравнение, дискриминант которого есть $-3d^2$. Без нарушения общности можно считать $s = 0$. По известному правилу Кардана, $\omega = \alpha + \beta$, где α и β суть числа, удовлетворяющие системе уравнений:

$$\alpha^3 + \beta^3 = n, \quad \alpha\beta = \frac{q}{3}.$$

Очевидно, что $(\alpha^3 - \beta^3)^2 = n^2 - \frac{4q^3}{27} = -\frac{D}{27} = \left(\frac{d}{3}\right)^2$. Следовательно, $\alpha^3 - \beta^3$ — рациональное число и числа α и β — чисто кубические. Так как $\beta = \frac{q}{3\alpha}$, они принадлежат одному и тому же чисто кубическому полю, которому, вместе с ними, будет принадлежать и $\omega = \alpha + \beta$. Тем самым достаточность высказанного условия доказана.

Легко теперь проверить, что уравнение

$$\omega^3 = 3\alpha\beta\omega + \alpha\beta(\alpha - \beta)$$

дает параметрическое представление всех уравнений, которым удовлетворяют числа чисто кубических полей, имеющие $s = 0$.

В самом деле, дискриминант этого уравнения $D = -27\alpha^2\beta^2(\alpha+\beta)^2$ удовлетворяет необходимому и достаточному условию при рациональных значениях параметров α и β. Обратно, если дискриминант D уравнения $\omega^3 = q\omega + n$ удовлетворяет условию $D = -3d^2$, то можно найти подходящие рациональные значения для параметров из уравнений

$$\alpha + \beta = -\frac{d}{q};$$

$$\alpha - \beta = \frac{3n}{q}.$$

Вычислим еще дискриминант кубического поля $\Omega\sqrt[3]{A}$; он равен

$$D_\Omega = \begin{vmatrix} 1, & \rho, & \bar{\rho} \\ 1, & \rho', & \bar{\rho}' \\ 1, & \rho'', & \bar{\rho}'' \end{vmatrix}^2 = -27f^2g^2,$$

если $A \not\equiv 1 \pmod 9$, и равен

$$D_\Omega = \begin{vmatrix} 1, & \rho, & \dfrac{1+f\rho+\sigma_2\overline{\rho}}{3} \\ 1, & \rho', & \dfrac{1+f\rho'+\sigma_2\overline{\rho}'}{3} \\ 1, & \rho'', & \dfrac{1+f\rho''+\sigma_2\overline{\rho}''}{3} \end{vmatrix}^2 =$$

$$= \frac{1}{9}\begin{vmatrix} 1, & \rho, & \overline{\rho} \\ 1, & \rho', & \overline{\rho}' \\ 1, & \rho'', & \overline{\rho}'' \end{vmatrix}^2 = -3f^2g^2,$$

если $A \equiv 1 \pmod 9$.

В 1928 году Артии предполагал, что возможно, пользуясь теорией поля классов, показать, что не может быть двух различных кубических полей с одним и тем же дискриминантом. Это, как легко видеть, неверно. Действительно, возьмем некоторую зафиксированную конечную совокупность различных простых чисел, среди которых есть число 3, и будем ее разными способами разбивать на две части, причем произведение простых чисел первой ее части будем принимать за f, а произведение остальных за g, и будем рассматривать все чисто кубические поля вида $\Omega\sqrt[3]{f^2g}$, где f и g — такие пары чисел. В виду того, что либо f, либо g делится на 3, так как среди нашей совокупности простых чисел, по предположению, есть число 3, $A = f^2g \not\equiv 1 \pmod 9$ и, следовательно, дискриминанты всех рассматриваемых полей равны $D = -127f^2g^2$, т. е. одинаковы. А между тем, как легко видеть, все эти поля различны.

Действительно, пусть A_1 и A_2 — два из рассматриваемых A, и притом $p_1p_2 \dots p_k$ — все те простые числа нашей совокупности, которые в оба эти A входят в 1-й степени, $q_1q_2 \dots q_l$ — все те, которые в оба A входят во 2-й, $r_1r_2 \dots r_m$ — те из остальных простых чисел, которые в A_1 входят в 1-й, а в A_2 во 2-й, $s_1s_2 \dots s_n$ — оставшиеся простые числа, входящие в A_1 во 2-й и в A_2 в 1-й степени. Если бы $\rho_1 = \sqrt[3]{A_1}$ и $\rho_2 = \sqrt[3]{A_2}$ образовали одно и то же поле, то и числа

$$\theta_1 = r_1r_2 \dots r_m\frac{\rho_1}{\rho_2} = \sqrt[3]{s_1s_2 \dots s_n r_1^2r_2^2 \dots r_m^2}$$

и

$$\theta_2 = \frac{\rho_2^2}{r_1r_2 \dots r_m\rho_1} = \sqrt[3]{p_1p_2 \dots p_kq_1^2q_2^2 \dots q_l^2}$$

также образовали бы то же поле. Но дискриминанты полей Ω_{θ_1} и Ω_{θ_2} равны $D_1 = -27f_1^2g_1^2$ или $-3f_1^2g_1^2$ и $D_2 = -27f_2^2g_2^2$ или $-3f_2^2g_2^2$, причем f_1g_1 взаимно просто с f_2g_2, и, следовательно, не может быть $-27f_1^2g_1^2 = -27f_2^2g_2^2$ и не может быть $-3f_1^2g_1^2 = -3f_2^2g_2^2$. Не может быть также и $-27f_1^2g_1^2 = -3f_2^2g_2^2$, так как это равносильно $9f_1^2g_1^2 = f_2^2g_2^2$, но $f_2^2g_2^2$ не делится ни на один простой делитель числа $f_1^2g_1^2$.

Мы видим, таким образом, что могут быть такие дискриминанты, для которых имеется сколь угодно много не только вообще разных кубических полей, а даже разных чисто кубических полей; стоит только взять достаточно большую совокупность простых чисел, рассматриваемую выше. (Это замечание принадлежит Нагелю.)

ТАБЛИЦА ВСЕХ УРАВНЕНИЙ ВИДА $x^3+bx+c=0$ ДЛЯ ВСЕХ ЦЕЛЫХ РАЦИОНАЛЬНЫХ b и $c<0$, ПО АБСОЛЮТНОЙ ВЕЛИЧИНЕ МЕНЬШИХ 10, ДИСКРИМИНАНТОВ ПОЛЕЙ, СООТВЕТСТВУЮЩИХ ЭТИМ УРАВНЕНИЯМ, БАЗИСОВ ЭТИХ ПОЛЕЙ, ЕСЛИ ОНИ НЕ СТЕПЕННЫЕ, НЕКОТОРЫХ ЕДИНИЦ ЭТИХ ПОЛЕЙ И ЧИСЕЛ КЛАССОВ ИДЕАЛОВ ЭТИХ ПОЛЕЙ

(Таблица вычислена Reid'ом [45])

x^3+bx+c

bc	d_Ω	Базис	ε	h_Ω	bc	d_Ω	Базис	ε	h_Ω
01	red				56	red			
11	— 31		$\alpha,\ \alpha+1$	1	—56	— 472			1
—11	— 23		$\alpha,\ \alpha-1,\ \alpha+1$	1	66	—1836		$\alpha+1$	3
02	—108		$\alpha+1;\ \alpha^2-\alpha+1$	1	—66	— 108			1
12	red				61	— 891		$\alpha;\ 6\alpha+1$	3
—12	—104		$\alpha^2+\alpha-1$	1	—61	+ 837		α	1
22	—140		$\alpha+1$	1			$\frac{\alpha^2+\alpha+1}{3};\ \alpha;\ 1$		
—22	— 76		$\alpha-1;\ \alpha^2+\alpha-1$	1	62	— 108			1
21	— 59		α	1	—62	+ 756		$3\alpha-1$	1
—21	red				63	—1107		$2\alpha+1$	2
03	—243		α^2-2	1	—63	+ 621		$\alpha-2$	1
13	—247		$\alpha+1$	1			$\frac{\alpha^2}{2};\ \alpha;\ 1$		
—13	—239		$\alpha^2+\alpha-1$	1	64	— 324		$\alpha^2-\alpha-1$	1
23	red				—64	red			
—23	—211		$\alpha^2-2\alpha+2$	1	65	—1539		$2\alpha^2-34\alpha-27$	1
33	—351		$\alpha+1$	1	—65	red			
—33	—135		$\alpha-1,\ \alpha+2$	1	07	—1323		$\alpha+2$	3
31	—135		$\alpha,\ 3\alpha+1,\ \alpha^2+3$	1	17	—1327			1
—31	+ 81		$\alpha,\ \alpha-1,\ \alpha+2$	1	—17	—1319		$\alpha+2$	1
32	—216		$-\alpha^2+\alpha+1$		27	—1355			1
—32	red				—27	—1291			1
04	—108	$\frac{\alpha^2}{2};\ \alpha;\ 1$	$\frac{\alpha^2-2}{2}$	1	37	—1431		$-\alpha^2+2$	1
14	—436		$21\alpha^2-29\alpha+61$	1	—37	— 135	$\frac{\alpha^2-\alpha+1}{3};\ \alpha;\ 1$	$\frac{\alpha^2-\alpha+1}{3}$	1
			$5\alpha^2-9\alpha+11\ \alpha^2-\alpha-5;$		47	—1579			1
—14	—107	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$	$\frac{\alpha^2-\alpha+2}{2}$	1	—47	—1067			1
					57	—1823		$\alpha+1$	2
24	—116	$\frac{\alpha^2}{2};\ \alpha;\ 1$	$\alpha+1$	1	—57	— 823			1
—24	red				67	red			
34	red				—67	— 459		$2\alpha^2+2\alpha-11$	1
—34	—324		$\alpha^2-\alpha-7$	1	77	—2695		$\alpha+1$	3
					—77	+ 49			1
					71	—1399		α	2

44	— 172	$\frac{\alpha^2}{2};\ \alpha;\ 1$	$\alpha+1;\ \alpha^2-\alpha+5$	1
—44	— 44	$\frac{\alpha^2}{2};\ \alpha;\ 1$	$\alpha-1$	1
41	— 283		$\alpha;\ 4\alpha+1$	2
—41	+ 229		$\alpha,\ \alpha+2,\ \alpha-2$	1
42	— 364		$2\alpha+1$	1
—42	+ 148		$\alpha-1.-2\alpha+1$	1
43	— 499		$3\alpha+2$	1
—43	red			
05	— 675		$2\alpha^2+4\alpha+1$	1
15	— 679		$-4\alpha^2+6\alpha-13$	1
—15	— 671		$\alpha+2$	1
25	— 707		$3\alpha+4$	1
—25	— 643		$\alpha+2$	2
35	— 87	$\frac{\alpha^2+\alpha+1}{3};\ \alpha;\ 1$	$\alpha+1,\ \frac{\alpha^2+\alpha+1}{3}$	1
—35	— 567		$\alpha^2-2\alpha+2$	1
45	red			
—45	— 419		$2\alpha^2-5\alpha+4$	1
55	—1175		$\alpha+1$	1
—55	— 175		$\alpha-1$	1
51	— 527		α	1
—51	+ 473		α	1
52	— 152	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$		1
—52	red			
53	— 743			1
—53	+ 257		$\alpha-1$	1
54	— 932			1
—54	red			
06	— 972		$3\alpha^2+6\alpha+1$	1
16	— 244	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$		1
—16	red			
26	—1004		$7\alpha^2+15\alpha+7$	1
—26	— 940		$3\alpha^2+7\alpha+1$	1
36	—1080			1
—36	— 216	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$	$\frac{-\alpha^2+\alpha+8}{2}$	1
46	—1228		$\alpha+1$	3
—46	— 716		$40\alpha^2-101\alpha+95$	1
—71	+1345			1
72	—1480			1
—72	+ 316	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$	$\frac{\alpha^2-\alpha}{2};\ 3\alpha^2+\alpha-2$	1
73	—1615			1
—73	+1129		α^2-8	1
74	— 451	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$		1
—74	+ 940		$-2\alpha^2+6\alpha-3$	1
75	—2047			1
—75	+ 697		$\alpha-2$	1
76	—2344			1
—76	red			
08	red			
18	—1732		$6\alpha+11$	2
—18	— 431	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$	$6\alpha-11$	1
28	— 440	$\frac{\alpha^2}{2};\ \alpha;\ 1$		1
—28	— 424	$\frac{\alpha^2}{2};\ \alpha;\ 1$		1
38	— 459	$\frac{\alpha^2+\alpha}{2};\ \alpha;\ 1$	$2\alpha+3$	1
—38	—1620		$2\alpha+5$	3
48	— 31	$\frac{\alpha^2}{4};\ \frac{\alpha}{2};\ 1$		1
—48	— 23	$\frac{\alpha^2}{4};\ \frac{\alpha}{2};\ 1$		1
58	—2228			1
—58	— 307	$\frac{\alpha^2-\alpha}{2};\ \alpha;\ 1$		1
68	— 648	$\frac{\alpha^2}{2};\ \alpha;\ 1$	$\alpha+1$	3
—68	— 216	$\frac{\alpha^2}{2};\ \alpha;\ 1$	$\alpha+3$	1
78	red			
—78	— 356			1
88	— 59	$\frac{\alpha^2}{4};\ \frac{\alpha}{2};\ 1$		1
—88	red			

			α	1
				1
			$\frac{\alpha^2-\alpha}{2};\ 3\alpha^2+\alpha-2$	1
				1
			α^2-8	1
				1
			$-2\alpha^2+6\alpha-3$	1
				1
			$\alpha-2$	1
				1
			$6\alpha+11$	2
			$6\alpha-11$	1
				1
				1
			$2\alpha+3$	1
			$2\alpha+5$	3
				1
				1
				1
				1
			$\alpha+1$	3
			$\alpha+3$	1
				1
				1

Продолжение

bc	d_Ω	Базис	ε	d_Ω
81	— 83	$\frac{\alpha^2+2\alpha+2}{5}$; α; 1	α	1
−81	+2021		α	
82	— 44	$\frac{\alpha^2-3\alpha+3}{7}$; α; 1		1
−82	+1940		$\alpha^2+3\alpha+1$	
83	−2291			1
−83	red			
84	— 610	$\frac{\alpha^2}{2}$; α; 1	$2\alpha+1$	1
−84	+ 404	$\frac{\alpha^2}{2}$; α; 1	$2\alpha-1$	1
85	−2723			1
−85	+1373			1
86	−3020			3
−86	+1076		$3\alpha^2-10\alpha+7$	1
87	red			
09	— 243			1
19	−2191		$\alpha-2$	2
−19	−2183		α^2-5	2
29	−2219			2
−29	−2155		$16\alpha^2-25\alpha-152$	1
39	— 255	$\frac{\alpha^2}{3}$; α; 1		1
−39	— 231	$\frac{\alpha^2}{3}$; α; 1		1
49	−2443		$\alpha^2-4\alpha-8$	2
−49	−1931			2
59	−2687		$3\alpha+4$	2
−59	−1687		$7\alpha^2-20\alpha+22$	1
69	— 339	$\frac{\alpha^2}{3}$; α; 1		1
−69	red			

bc	d_Ω	Базис	ε	d_Ω
79	−3559		$\alpha+1$	2
−79	— 815			1
89	red			
−89	— 139		$\alpha-2$	1
99	— 567	$\frac{\alpha^2}{3}$; α; 1	$\alpha+1$	1
−99	+ 81			1
91	— 327	$\frac{\alpha^2-\alpha+1}{3}$; α; 1	α; $9\alpha+1$	1
−91	+ 321	$\frac{\alpha^2-\alpha+1}{3}$; α; 1	α; $\alpha+3$; $\alpha-3$	1
92	— 756	$\frac{\alpha^2+\alpha}{2}$; α; 1	$\frac{5\alpha^2-17\alpha-4}{2}$	1
−92	+2808			1
93	−3159			1
−93	+2673		$3\alpha-1$	1
94	−3348			1
−94	+ 621	$\frac{\alpha^2+\alpha}{2}$; α; 1	$-4\alpha^2+26\alpha-3$	1
95	−3591		$-4\alpha^2+22\alpha+13$	1
−95	+1241		$-\alpha^2-4\alpha-2$	1
96	— 243			1
−96	+1944			1
97	−4239		$\alpha^2-2\alpha-2$	1
−97	+1593		$\alpha-1$	1
98	— 516	$\frac{\alpha^2+\alpha+1}{3}$; α; 1		1
010	— 300		$-3\alpha^2-6\alpha+1$	1

ТАБЛИЦА, АНАЛОГИЧНАЯ ПРЕДЫДУЩЕЙ, ДЛЯ НЕКОТОРЫХ УРАВНЕНИЙ ВИДА $x^3 + ax^2 + bx + c = 0$

(Таблица вычислена Reid'ом [45])

abc	d_Ω	Базис	ε	*h*	*abc*	d_Ω	Базис	ε	*h*
—1 1 1	— 44		α	1	—2 1 2	—116			1
1 1 2	— 83		$\alpha+1$	1	—1 1 2	—503	$\frac{\alpha^2+\alpha}{2}; \alpha; 1$		1
—1 1 2	—139		$\alpha+1$	1	—1 2 8	—503			1
—1 —2 1	— 59		$\alpha-1$; $\alpha+1$	1	—2 2 2	—204		$-\alpha^2-5\alpha+7$	1
1 2 1	— 23		α	1	2 —2 2	—268		$\alpha+3$	1
—1 2 1	— 87		α	1	—2 —2 2	+148		$\alpha+1$, $\alpha-1$	1
1 —2 1	— 31		α	1	1 4 8	—356	$\frac{\alpha^2+\alpha}{2}; \alpha; 1$		1
—1 —2 1	+ 49		α	1	—1 4 8	—628	$\frac{\alpha^2+\alpha}{2}; \alpha; 1$		1
—1 2 2	—200			1	1 —4 8	—516	$\frac{\alpha^2+\alpha}{2}; \alpha; 1$		1
1 —2 2	—152		$\alpha^2-\alpha+1$	1	—1 —4 8	—212	$\frac{\alpha^2+\alpha}{2}; \alpha; 1$	$\alpha^2+\alpha-3$	1

ТАБЛИЦА ЧИСЕЛ КЛАССОВ ЧИСТО КУБИЧЕСКИХ ПОЛЕЙ $\Omega_{\sqrt[3]{A}}$

(Таблица вычислена Дедекиндом [10])

$D_\Omega = -3k^2$ $\quad A = f \cdot g^2$

A =	2	3	5	6	12	7	10	20	11	13	14	28	15	45	17	19	21	63	22	44	23
k =	6	9	15	18	18	21	10	30	33	39	42	14	45	45	17	19	63	63	66	22	69
h =	1	1	1	1	1	3	1	3	2	3	3	3	2	1	1	3	3	6	3	1	1

ГЛАВА III

ГЕОМЕТРИЯ, ТАБУЛЯРИЗАЦИЯ И КЛАССИФИКАЦИЯ АЛГЕБРАИЧЕСКИХ ПОЛЕЙ 3-й И 4-й СТЕПЕНИ

А. ТАБУЛЯРИЗАЦИЯ ПОЛЕЙ 3-й СТЕПЕНИ

§ 26. Система W и ее сетки $\overline{W}_0$, $\overline{W}_1$ для $n=3$, $\tau=0.1$

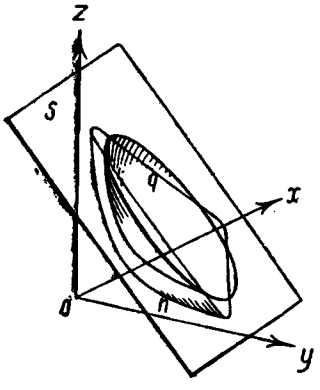
В § 1 были введены в рассмотрение системы $W_{n,\tau}$ всех точек всех решеток, повторяющихся умножением, данного числа n измерений и с данным числом τ пар комплексно сопряженных координат. В случае кубических иррациональностей $n=3$, $\tau=0$ или 1. Мы рассмотрим оба эти случая отдельно.

Случай, когда $\tau=0$, *т. е.* $D>0$. Всякая точка ω системы W в этом случае имеет координаты, которые являются корнями кубического уравнения

$$\rho^3 - s\rho^2 + q\rho - n = 0, \tag{1}$$

с целыми рациональными коэффициентами s, q, n (в гл. III мы обозначаем через $-q$ тот же коэффициент, который обозначали в гл. II через q), все три корня которого вещественны (так как число τ пар комплексно сопряженных корней по предположению равно 0), т. е. дискриминант D которого положителен. Будем обозначать координаты точек соответствующего этому случаю вещественного сигнатурного пространства $R_{3,0}$ через x, y, z. Тогда система точек W определяется системами уравнений

$$\left.\begin{aligned} x+y+z &= s,\\ xy+xz+yz &= q,\\ xyz &= n, \end{aligned}\right\} \tag{2}$$



Черт. 3.

где s, q, n — все возможные целые рациональные числа, удовлетворяющие условию, что все три корня уравнения (1) вещественны. Последнее, очевидно, равносильно тому, что целые рациональные числа s, q, n должны удовлетворять условию, чтобы поверхности (2) пересекались, т. е. имели хоть одну общую им всем троим точку. Всякой точке W соответствует одно определенное уравнение (1), а одному уравнению (1) соответствует 6 точек W, в соответствии с возможностью различно нумеровать корни.

Система W представляет собою, таким образом, совокупность всех точек пересечения семейств плоскостей s, делающих одинаковые отрезки на осях соасимптотических гиперболоидов q вращения вокруг рациональной прямой (однополых, если $q<0$, и двухполых, если $q>0$), и поверхностей 3-го порядка n, асимптотически приближающихся к плоскостям координат, при целых s, q, n.

Норма точки $N(x, y, z)=xyz$ равна объему координатного параллелепипеда точки (x, y, z), положительна, если точка лежит в одном из 4 нечет-

ных, и отрицательна, если она лежит в одном из 4 четных координатных октантов. След $S(x, y, z) = x + y + z$ равен расстоянию до плоскости n от начала, взятому с соответственным знаком и помноженному на $\sqrt{3}$. Дифферента $\delta(x, y, z) = (x - y)(x - z) = (y - x)(z - x)$ равна площади координатного прямоугольника в плоскости YZ той точки $(\bar{y}, \bar{z})$ этой плоскости, которая является проекцией на эту плоскость точки (x, y, z) параллельно так называемому „рациональному направлению", т. е. прямой $x = y = z$. Таким образом, „дифферента" равна гиперболическому расстоянию от начала до этой точки $(\bar{y}, \bar{z})$, если за асимптоты приняты оси Y и Z. Дискриминант точки (x, y, z)

$$D(x, y, z) = [(x - y)(x - z)(y - z)]^2 = \\ = s^2q^2 + 18sqn - 4q^3 - 4s^3n - 27n^2$$

равен, как это следует из § 1 вводной части, квадрату объема параллелепипеда, построенного на точках $(0, 0, 0), (1, 1, 1), (x, y, z), (x, y, z)^2$.

Все точки (x, y, z) с одним и тем же дискриминантом D лежат на цилиндре 6-го порядка

$$(x - y)(x - z)(y - z) = \pm\sqrt{D},$$

прямолинейные образующие которого параллельны рациональной прямой и который пересекает, например, плоскость XY по кривой $(x - y) \cdot x \cdot y = \pm\sqrt{D}$. Мы будем называть две точки W параллельными, если они связаны соотношением: одна (x, y, z), а другая $(x + k, y + k, z + k)$, где k — целое рациональное. В виду того, что, если коэффициенты уравнения, соответствующего первой точке, целые рациональные, то и коэффициенты уравнения, соответствующего второй, тоже целые рациональные, следует, что всякая точка, параллельная некоторой точке W, есть опять точка W. Система W распадается, таким образом, на ряды параллельных точек, каждый из которых представляет собой правильный ряд точек, лежащих на прямой, параллельной рациональной прямой, в расстояниях $\sqrt{3}$ друг от друга. Какая бы точка W ни была точка (x, y, z), можно всегда так подобрать целое рациональное число k, чтобы у точки $(x + k, y + k, z + k)$ было $s = -1$, 0 или 1, так как при переходе от первой точки ко второй целый рациональный коэффициент s (след) изменяется на $3k$. Но соседние плоскости s идут на расстоянии $\frac{\sqrt{3}}{3}$ друг от друга, и, следовательно, всякая параллель точек W имеет одну и только одну из своих точек, которую можно назвать начальной ее точкой либо в плоскости $s = -1$, либо в плоскости $s = 0$, либо в плоскости $s = 1$. Систему W можно наиболее наглядно себе представить, если заметить, что достаточно знать двухмерные сетки ее точек $\overline{W}_{-1}$, $\overline{W}_0$, $\overline{W}_1$, лежащие в плоскостях $s = -1$, $s = 0$ и $s = 1$, так как все остальные точки W исчерпываются пернодическим параллельным переносом этих сеток в плоскости $s = \ldots \underbrace{2, 3, 4,}\ \underbrace{5, 6, 7}\ \ldots$ Но, собственно говоря, даже достаточно знать только сетки $\overline{W}_0$ и $\overline{W}_1$, так как сетка $\overline{W}_{-1}$ симметрична сетке $\overline{W}_1$ по отношению к началу координат. Гиперболоиды q пересекают плоскость $s = 0$ по системе концентрических окружностей с центром в начале координат. Плоскости координат пересекают эту плоскость $s = 0$ по трем прямым, проходящим через начало и образующим 6 равных углов по 60° между собою. Кривые 3-го порядка, по которым пересекают плоскость $s = 0$ поверхности n, имеют эти прямые своими асимптотами. Аналогичное получается для плоскости $s = 1$, только в $s = 1$ точка пересечения этой плоскости с рациональной прямой $x = y = z$, являющаяся центром кругов q, не есть точка пересечения прямых, даваемых плоскостями координат, а центр тяжести равностороннего треугольника, ими

образуемого, кривые же 3-го порядка n и тут асимптотически приближаются к этим прямым.

Заметим еще, что дискриминантные цилиндры пересекают плоскость нулевого следа $s=0$ и плоскость $s=1$ по одним и тем же кривым, совершенно аналогичным кривым n, но повернутым на 30° по отношению к ним вокруг начала.

Вся система кривых, нанесенных на плоскости $s=0$, имеет 6-ную ось симметрии, а система кривых на плоскости $s=1$ 3-ную ось симметрии.

В конце книги приложены тщательно изготовленные чертежи сеток $\overline{W}_0$ и $\overline{W}_1$ для $R_{3,0}$.

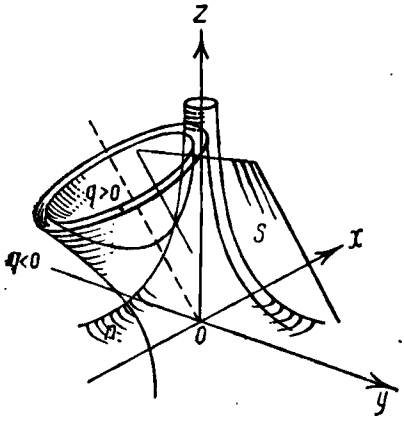
Случай, когда $\tau=1$, *т. е.* $D<0$. Будем в этом случае считать, что z вещественный корень ρ уравнения

$$\rho^3-s\rho^2+q\rho-n=0,$$

а $x+iy$, $x-iy$ комплексно сопряженные его корни ρ' и ρ''. Тогда мы имеем систему

$$\left.\begin{aligned} 2x+z&=s,\\ x^2+y^2+2xz&=q,\\ (x^2+y^2)z&=n,\end{aligned}\right\} \qquad (3)$$

где s, q, n — все возможные целые рациональные числа, удовлетворяющие условию $D<0$, но это опять все равно, что удовлетворяющие тому условию, что поверхности s, q, n пересекаются. Система W, таким образом, в этом случае представляет собою совокупность всех точек пересечения плоскостей s, параллельных оси Y и делающих по оси z вдвое больший отрезок, чем на оси X, соасимптотических гиперболоидов q (однополых при $q>0$ и двуполых при $q<0$), для которых ось Z служит одной из образующих общего им асимптотического конуса и поверхностей вращения вокруг оси Z 3-го порядка n, которые асимптотически приближаются к оси Z ($+z$ при $n>0$ и $-z$ при $n<0$) и к плоскости XY, при целых s, q, n.



Черт. 4.

Норма точки $N(x, y, z)$ равна делению на π объему цилиндра вращения вокруг оси Z, одно основание которого находится в плоскости XY, а окружность другого основания которого проходит через эту точку, взятому со знаком $+$, если цилиндр этот над плоскостью XY, и со знаком $-$, если он под плоскостью XY. След $S(x, y, z)$ равен s. Дискриминант $d(x, y, z)=[(\rho-\rho')(\rho-\rho'')(\rho'-\rho'')]^2=$ $=s^2q^2+18sqn-4q^3-4s^3n-27n^2$ равен учетверенному квадрату объема параллелепипеда, построенного на точках $(0, 0, 0)$, $(1, 0, 1)$, (x, y, z), $(x^2-y^2, 2xy, z^2)$. Все точки, которые имеют один и тот же дискриминант d, лежат на цилиндре 6-го порядка

$$4(x^2+y^2+z^2-2xz)y=\pm\sqrt{|d|},$$

который с плоскостью XY пересекается по кривой $4(x^2+y^2)y=\pm\sqrt{|d|}$, которая расположена симметрично по отношению к оси X и приближается к ней асимптотически. Образующие этого цилиндра параллельны так называемой рациональной прямой $z=x+iy=x-iy$, т. е. прямой $x=z$; $y=0$, на которой лежит в этом случае точка $\rho=\rho'=\rho''$, имеющая своими координатами $(1, 0, 1)$.

Две точки тут называются параллельными, если они связаны соотношением (ρ, ρ', ρ''), $(\rho + k, \rho' + k, \rho'' + k)$, т. е. соотношением (x, y, z), $(x + k, y, z + k)$, где k целое рациональное, иначе говоря, получаются одна из другой переносом параллельно рациональной прямой $x = z$, $y = 0$ на расстояние $k\sqrt{2}$. Как в предыдущем случае, следует, что всякая точка, параллельная точке W, есть опять точка W. Система W, таким образом, распадается на ряды параллельных точек, каждый из которых представляет собою правильный ряд точек, лежащих на прямой, параллельной рациональной прямой, на расстояниях $\sqrt{2}$ друг от друга. Совершенно аналогично предыдущему случаю система W распадается на сетки W_1, $\overline{W}_0$, $\overline{W}_1$, лежащие в плоскостях s и периодически повторяющиеся на плоскостях $s = \ldots \underbrace{2, 3, 4,}\ \underbrace{5, 6, 7}\ldots$

Тут сетки $\overline{W}_{-1}$ и $\overline{W}_1$ опять симметричны друг другу по отношению к началу, так как и система s, и система q, и система поверхностей n симметричны по отношению к началу, и поэтому опять достаточно рассматривать только сетки $\overline{W}_0$ и $\overline{W}_1$. Сетка $\overline{W}_0$ составлена системой соасимптотических гипербол q и системой кривых 3-го порядка n, асимптотически приближающихся к прямой пересечения плоскости $s = 0$ с плоскостью XY, которая является одновременно одной из осей симметрии гипербол. Сетка эта имеет оси симметрии гипербол своими осями симметрии. Сетка $\overline{W}_1$ менее симметрична, у нее асимптота кривых 3-го порядка n только параллельна соответственной оси симметрии соасимптотических гипербол, но с ней не совпадает. Кривые пересечения цилиндров равных дискриминантов совершенно аналогичны кривым n на сетке $\overline{W}_0$, но повернуты к ним на 90°. Вся система кривых, нанесенных на плоскости $s = 0$, имеет две оси симметрии, являющиеся осями симметрии гипербол, а система кривых на плоскости $s = 1$ имеет одну ось симметрии, являющуюся одной из осей симметрии гипербол.

В конце книги приложены тщательно изготовленные чертежи проекций $\overline{\overline{W}}_0$, $\overline{\overline{W}}_1$ сеток, $\overline{W}_0$ и $\overline{W}_1$ на плоскость XY параллельно рациональному направлению.

§ 27. Выключение приводимых точек в обоих случаях

Если мы хотим вычеркнуть те точки сеток $\overline{W}_0$, $\overline{W}_1$, которые соответствуют приводимым уравнениям $x^3 - sx^2 + qx - n = 0$, в соответствии с общей теорией § 2, достаточно заметить, что любая такая точка есть сумма точек системы W_1 (ряд целых рациональных точек), лежащей на одной из осей, и точки системы W_2, лежащей в плоскости, образованной двумя другими осями.

Для случая $D > 0$ совокупность точек W_2, лежащих в плоскости XY, определяется уравнениями

$$\left.\begin{aligned} x + y &= s, \\ xy &= q. \end{aligned}\right\} \qquad (1)$$

Эта совокупность есть в данном случае система W_2 для 2-мерного пространства и $\tau = 0$. Все ее точки лежат на параллельных прямых $x + y = s$, идущих в расстоянии $\frac{\sqrt{2}}{2}$ друг от друга, причем ряды точек, расположенные на этих прямых $s = 0$ и $s = 1$, параллельно переносно, по перпендикуляру к этим прямым, периодически повторяются на прямых $s = \ldots \underbrace{2, 3,}\ \underbrace{4, 5}\ldots$.

Легко подсчитать, что уравнения (1) для точек W, лежащих в плоскостях $s = 0$ и соответственно $s = 1$, имеют вид:

$$\left.\begin{aligned} x + y &= -3r \\ xy &= 3r^2 + q \end{aligned}\right\} \quad \text{и} \quad \left.\begin{aligned} x + y &= 1 - 3r \\ xy &= 3r^2 - 2r + g \end{aligned}\right\},$$

где r — целые рациональные числа, т. е. что для выключения приводимых точек в $\overline{W}_0$ надо брать только прямые s с s, делящимся на 3, а для выключения в $\overline{W}_{-1}$ прямые s с $s \equiv 1 \pmod 3$. Надо рассмотреть системы W_2, лежащие в плоскостях XY, XZ, YZ. Спроектировав эти системы точек, лежащие в плоскостях XY, XZ, YZ, соответственно на плоскости $s=0$ и $s=1$, параллельно рациональному направлению, мы получим на каждой из этих плоскостей по три системы параллельных рядов точек, лежащих на равноотстоящих друг от друга прямых, параллельных асимптотам кривых 3-го порядка n, причем в каждой из этих систем ряды эти параллельно переносно, по перпендикуляру к этим прямым, периодически повторяются через один. Один из этих рядов есть ряд всех точек $\overline{W}_0$ или $\overline{W}_1$, лежащих на соответственной асимптоте (т. е. точек пересечения этой асимптоты с окружностями q), а другой получается в результате пересечения прямой, параллельной этой асимптоте. Если выключить получившиеся так приводимые точки из $\overline{W}_0$ и $\overline{W}_1$, мы получим уже системы в плоскостях $s=0$ и $s=1$, состоящие только из неприводимых точек.

На чертежах в конце книги вычерчены эти три ряда параллельных прямых. Для случая $D<0$ мы получаем соответственно уравнения

$$\left.\begin{aligned} 2x &= s, \\ x^2+y^2 &= q, \end{aligned}\right\} \tag{2}$$

дающие систему W_2 для $\tau=1$ в плоскости XY. Система W_2 в плоскости XZ или YZ лежать не может, так как у системы W_2 или обе координаты соответствуют вещественным, или, как здесь, обе — комплексным корням. Все точки системы W_2 лежат на параллельных прямых $2x=s$, идущих на расстояниях $^1/_2$ друг от друга, причем ряды точек, расположенные на прямой $s=0$ и $s=1$, параллельно переносно, по перпендикуляру к этим прямым, повторяются на прямых $s=\ldots 2, 3, 4, 5 \ldots$. Уравнения (2) для точек W, лежащих в плоскости $s=0$ и соответственно $s=1$, суть

$$\left.\begin{aligned} 2x &= -3r \\ x^2+y^2 &= 3r^2+q \end{aligned}\right\} \quad \text{и} \quad \left.\begin{aligned} 2x &= 1-3r \\ x^2+y^2 &= 3r^2-2r+q \end{aligned}\right\},$$

где r — целые рациональные числа, т. е. для выключения приводимых точек в $\overline{W}_0$ надо брать только прямые s с s, делящимся на 3, а для $\overline{W}_1$ только с $s \equiv 1 \pmod 3$. В самих плоскостях $s=0$ и $s=1$, аналогично предыдущему, выходит, что надо выключить все точки W, лежащие на асимптоте кривых 3-го порядка n, затем точки, лежащие на прямой, ей параллельной, и такие же системы (периодически параллельно переносно в направлении перпендикуляра к этим прямым) через одну, лежащие на прямых, им параллельных и проходящих все на тех же расстояниях друг от друга.

На чертежах в конце книги вычерчены эти прямые.

Для того чтобы особенно наглядно убедиться, что, скажем, в $\overline{W}_0$ для $D<0$ есть сколь-угодно много неприводимых точек, возьмем место, окружающее далекую от начала точку на асимптоте кривых n. Сетка $\overline{W}_0$ около такого места, как это очевидно из ее геометрической формы, представляет собою густую, почти ортогональную сеть, так как в таком месте гиперболы q и кривые n примерно ортогональны друг другу и как гиперболы q, так и кривые n идут очень густо друг возле друга; таким образом, в полоске между асимптотой и соседней ей параллельной прямой приводимых точек лежит сколь-угодно много точек $\overline{W}_0$, а между тем в этой полоске приводимых точек нет, т. е. все эти точки неприводимы. Совершенно аналогичное имеет место и в других случаях, только при $D>0$ три системы прямых, на которых могут лежать

приводимые точки, образуют сетку равных равносторонних треугольников, и дело будет идти о том, что внутри такого треугольника, достаточно далеко расположенного вдоль асимптоты, есть сколь-угодно много неприводимых точек. В случае $D>0$ и $\overline{W}_1$ одним из треугольников этой сетки треугольников будет, например, треугольник, составленный асимптотами кривых n.

§ 28. Ограничение коэффициентов q и n для данного s для ближайших к началу точек в кольцах целых кубических чисел, содержащих число 1, дискриминанты которых не больше L по абсолютной величине

Случай $D>0$. Площадь $\overline{V}_0$ основного параллелограмма той решетки $\overline{O}$, которая получается ортогональным проектированием некоторого кольца O целых кубических точек положительного дискриминанта, содержащего точку 1, параллельно рациональному направлению на плоскость $s=0$, равна $\frac{1}{\sqrt{3}}V_O$, где V_O — объем основного параллелепипеда O, так как такой параллелограмм получается проектированием параллельно 01 некоторого основного параллелепипеда, у которого 01 есть одно из ребер, плоскость s перпендикулярна к 01, а длина ребра 01 равна $\sqrt{3}$.

Но $D_O=V_O^2$, и, следовательно, $\overline{V}_O=\frac{1}{\sqrt{3}}\sqrt{D}$. Если же $D\leqslant L$, то $\overline{V}_O\leqslant\frac{1}{\sqrt{3}}\sqrt{L}$. Все приводимые точки O, если O неприводимая решетка, лежат в единственной биссектрисе $x=y=z$, т. е. на рациональной прямой, и, следовательно, проектируются на плоскость $s=0$ в начало координат, где эта плоскость пересекается рациональной прямой, в центре окружностей q. Все остальные точки $\overline{O}$ суть, следовательно, проекции неприводимых точек O. Опишем в плоскости $s=0$ из начала координат такой круг, чтобы внутрь или на границу его наверное попала хоть одна точка любого $\overline{O}$, имеющего $\overline{V}_O\leqslant\frac{1}{\sqrt{3}}\sqrt{L}$. Из известного плотнейшего параллелограмматического расположения равных кружочков (по равносторонним треугольникам) следует, что наименьшее расстояние между двумя точками плоской решетки, площадь основного параллелограмма которой равна σ, не превышает $\sqrt{\frac{2\sigma}{\sqrt{3}}}$. Следовательно, радиус такого круга равен $r=\sqrt{\frac{2}{3}}\sqrt[4]{L}$. Для того чтобы наверняка уловить хотя бы по одной непривводимой точке каждого O с $0<D_O\leqslant L$, надо, следовательно, рассмотреть $\overline{W}_0$ и $\overline{W}_1$ для $0<D$ и в них найти все точки, для которых круг q имеет радиус, меньший r. Радиус круга q легко подсчитывается, а именно, он равен $\sqrt{-2q}$ для $s=0$ и $\sqrt{-\frac{2}{3}2q}$ для $s=1$, и, следовательно, мы получаем для $s=0$ и соответственно для $s=1$ такие ограничения для коэффициента q:

$$-q\leqslant\frac{\sqrt{L}}{3}, \tag{1}$$

$$-q\leqslant\frac{\sqrt{L}-1}{3}. \tag{1'}$$

Теперь остается для $s=0$ и $s=1$ для каждого данного q ограничить то n, для которого последняя кривая n еще пересекает круг q. Это неравенство для n получается из условия

$$27D_p=4(s^2-3q)^3-(27n-9sq+2s^3)^2>0,$$

откуда

$$-2\sqrt{(s^2-3q)^3}+9sq-2s^3<27n<2\sqrt{(s^2-3q)^3}+9sq-2s^3.$$

Таким образом, мы получаем окончательно следующие ограничения для n соответственно при $s=0$ и $s=1$:

$$-6q\sqrt{-3q}<27n<6q\sqrt{-3q}, \tag{2}$$

$$-2\sqrt{(1-3q)^3}+9q-2<27n<2\sqrt{(1-3q)^3}+9q-2. \tag{2'}$$

Случай $D<0$. Площадь V_O основного параллелограмма той решетки O, которая получается проектированием некоторого кольца O целых кубических точек отрицательного дискриминанта, содержащего точку 1, параллельно рациональному направлению на плоскость XY, равна V_O, так как за одно из двух ребер основного параллелепипеда O можно принять отрезок 01 рациональной прямой, и тогда, если перенести концы двух других его ребер, исходящих из точек O параллельно рациональной прямой, на плоскость XY, то мы получим равновеликий параллелепипед, площадь основания которого равна $\overline{V_0}$, а высота равна 1. Но в случае $D<0$

$$|D_O|=4V_O^2,$$

и, следовательно, мы имеем

$$\overline{V_O}=\frac{\sqrt{|D_O|}}{2}.$$

Использовав опять то же ограничение для наименьшего расстояния между двумя точками плоской решетки с площадью σ основного параллелограмма, мы получаем, что в круге с радиусом $r=\sqrt[4]{\frac{L}{3}}$, описанном в плоскости XY из начала, как из центра, наверняка есть хоть одна точка, являющаяся проекцией параллельно рациональному направлению точки любого кольца O отрицательного дискриминанта D_O, по абсолютной величине меньшего, чем L. Рассмотрим теперь, в каких границах находятся все те коэффициенты q и n, которые для $s=0$ и $s=1$ дают точки W, проекции которых параллельно рациональному направлению лежат в указанном круге.

Обозначим через $\overline{\overline{W_0}}$ и $\overline{\overline{W_1}}$ проекции сеток $\overline{W_0}$, $\overline{W_1}$, лежащих в плоскостях $s=0$ и $s=1$, на плоскость XY параллельно рациональному направлению. Найдем уравнения сеток $\overline{\overline{W_0}}$ и $\overline{\overline{W_1}}$. Для этого обозначим через v и w координаты x и y точек в плоскости XY. Заметим, что если спроектировать точку (x, y, z) на плоскость XY параллельно рациональному направлению, то координаты v и w проекции будут $v=x-z$, $w=y$. Исключив из этих двух уравнений и уравнений (3) § 26 буквы x, y, z, получим уравнения

$$v^2-3w^2=-3q+s^2, \tag{3}$$

$$(v^2+2uv+s^2+9w^2)(s-2v)=27n, \tag{4}$$

которые и дают сетки $\overline{\overline{W_0}}$ и $\overline{\overline{W_1}}$ при $s=0$ и $s=1$, если придавать q и n все возможные целые рациональные значения.

Принимая во внимание величину r и рассматривая крайние гиперболы, которые еще пересекают окружность r, мы получаем соответственно для $s=0$ и $s=1$ такие ограничения для q:

$$-\frac{1}{3}\sqrt{\frac{L}{3}}\leqslant q\leqslant\sqrt{\frac{L}{3}}, \tag{5}$$

$$-\frac{1}{3}\sqrt{\frac{L}{3}}+\frac{1}{3}\leqslant q\leqslant\sqrt{\frac{L}{3}}+\frac{1}{3}. \tag{5'}$$

Теперь надо еще ограничить n, т. е. найти, какая крайняя кривая n пересекает каждую гиперболу q еще внутри круга L. Для этого заметим, что

$$r^2 = v^2 + w^2 = (x - z)^2 + y^2,$$

откуда

$$r^2 = 3z^2 - 2sz + q = F'(z),$$

где F — левая часть уравнения, корнями которого являются $\rho = z$, $\rho' = x + iy$, $\rho'' = x - iy$, т. е. r^2 равно дифференте ρ. Дифферента $\delta = F'(\rho)$ есть корень уравнения

$$\delta^3 - \delta^2(s^2 - 3q) + (-4q^3 - 27n^2 + s^2q^2 + 18sqn - 4s^3n) = 0.$$

Если при данных s и q увеличивать n, то при некотором $n = n'$, δ станет равным r^2, т. е. будет

$$r^6 - r^4(s^2 - 3q) + D_\rho = 0.$$

При меньших же n, r будет уже велико и даст значение большее нуля (так как для $r = 0$ получаем $D_\rho < 0$, т. е. значение меньшее нуля), таким образом, в каждом из случаев $s = 0$, 1 надо для каждого q, удовлетворяющего соответственному неравенству (5) или (5'), брать n, при котором

$$r^6 - r^4(s^2 - 3q) + D_\rho < 0.$$

§ 29. Нахождение 3-го числа базиса для каждой из пойманных точек

Рассмотрим все неприводимые кольца O, положительного или отрицательного дискриминанта — все равно, дискриминанты D_O которых по абсолютной величине меньше L. В силу рассмотренного, внутри найденных для $s = 0$ и $s = 1$ в предыдущем параграфе пределов для q и n будет наверняка находиться одно или несколько уравнений $\rho^3 - s\rho^2 + q\rho - n = 0$ с целыми рациональными коэффициентами, соответствующих неприводимым точкам любого такого кольца. Но не всякое, конечно, уравнение с целыми рациональными коэффициентами, находящимися в этих пределах, непременно соответствует точке одного из таких колец. Во-первых, оно может быть приводимым, и тогда оно вообще ие соответствует нн одной точке ни одного из таких колец O, кроме как когда оно есть $x^3 = 0$, но тогда оно дает приводимую точку, начало, принадлежащую всем таким кольцам и иам неинтересную. Затем может быть, что дискримииант такого уравнения

$$D_\rho = s^2q^2 + 18sqn - 4q^3 - 4s^3n - 27n^2,$$

после выделения из него наибольшего квадратного множителя, даст число, все же по абсолютной величине большее L; такое уравнение также не может соответствовать никакой точке ни одного из этих колец, так как дискриминант любой точки кольца равен, очевидно, дискриминанту кольца, помноженному на квадрат целого рационального числа, а именно на квадрат индекса этой точки. Такие уравнения, подобно приводимым, надо, конечно, отбросить. Однако, если дискриминант D_O содержит такой квадратный множитель, после выделения которого получается число, по абсолютной величине не больше L, то это еще ие зиачит, что существует кольцо O, точкой которого является ρ, которое имеет дискриминант D_O, по абсолютной величине не больший L. Может быть, что все-таки точка ρ прииадлежит только кольцам, дискриминанты которых по абсолютной величине больше L. Для того чтобы узнать, есть ли такие кольца, дискриминанты которых по абсолютной величине не больше L, и, если такие кольца есть, их все найти, достаточио применить способ для вычисления базисов всех колец, содержащих данную точку ρ, рассмотреиный в § 17, причем в данном случае дело несколько упрощается, так как нам нужно найти только такие кольца O, у которых само ρ является вторым числом базиса (как в § 17, так и здесь мы рассматриваем вообще лишь такие кольца, в которых

есть точка 1, а следовательно, за первую точку базиса мы всегда и можем принять как раз эту точку 1, и, следовательно, остается только найти третье число базиса ϕ, для чего пользуемся способом § 17).

§ 30. Таблица действий для нахождения всех неприводимых колец, состоящих из целых кубических точек и содержащих точку 1, дискриминанты которых по абсолютной величине не превосходят данного числа

Последовательность необходимых действий такая:

1) ограничиваем q в зависимости от выбранного L для $s=0$ и $s=1$ по формулам (1) и (1′) § 28 для $D>0$ и по формулам (5) и (5′) § 28 для $D<0$;

2) ограничиваем n для каждого из так полученных q, по формулам (2) и (2′) § 28 для $D>0$, и способом, указанным в конце § 28, для $D<0$. Таким образом, получаются как в случае $D>0$, так и в случае $D<0$ две таблички уравнений, проекции точек которых лежат в круге r; эти таблички можно и прямо получить, тщательно вычерчивая сетки $\overline{W_0}$, $\overline{W_1}$ для $D>0$ или, соответственно для $D<0$, сетки $\overline{\overline{W_0}}$, $\overline{\overline{W_1}}$, как это сделано на чертежах в конце книги;

3) исключаем все приводимые уравнения;

4) вычисляем все D_ρ оставшихся уравнений (это действие отнимает наибольшее время);

5) разлагаем все эти D_ρ на множители и вычеркиваем все те уравнения, у дискриминантов которых, после выделения наибольшего квадрата, все же остается число, по абсолютной величине большее L;

6) находим для каждого из оставшихся уравнений по правилам § 17 для каждого соответствующие ему третьи числа базиса ϕ, причем оставляем только те, которые дают $|D_O| = \left|\frac{D_\rho}{\Delta^2}\right|$ не большие, чем L. Таким образом, мы получим все кольца O, дискриминанты которых не больше L по абсолютной величине, но некоторые из них могут так получиться по нескольку раз, поэтому надо еще проделать следующее действие:

7) узнать при помощи способа, обратного преобразованию Чирнгаузена (см. § 13), для колец, так полученных, дискриминанты которых одинаковы, одинаковы ли эти кольца, или различны. Наконец, если нам желательно найти именно лишь все различные кубические поля, дискриминанты которых по абсолютной величине не больше L, то надо еще:

8) для колец, дискриминанты которых равны дискриминантам других колец, помноженным на квадраты целых рациональных чисел, опять-таки при помощи указанного в § 13 способа, обратного способу Чирнгаузена, убедиться, соответствуют ли эти кольца некоторым независимым кубическим полям, или же они—лишь надкольца соответственных колец.

Заключение. Когда уже вычислена этим способом таблица кубических колец O, так что для каждого $|D| \leqslant L$ даны все различные кольца O, т. е. даны коэффициенты s, q, n уравнения $\rho^3 - s\rho^2 + q\rho - n = 0$, которому удовлетворяет ρ, и числа Δ, b, c в выражении $\phi = \frac{\rho^2 + b\rho + c}{\Delta}$, где 1, ρ, ϕ базис соответственного кольца O, то можно затем, если угодно, переписать эту таблицу в виде таблицы представительниц всех классов с $|D| \leqslant L$ целочисленных кубических двойничных форм (индексформ этих колец). Действительно, соответствующая кольцу $[1, \rho, \phi]$ индексформа (a, b, c, d) имеет коэффициенты (см. § 17)

$$a = -C; \quad b = \frac{1}{6}F''(\bar{b}); \quad c = \frac{1}{2\Delta}F'(\bar{b}); \quad d = \frac{1}{\Delta^2}F(\bar{b}),$$

где $F(z) = z^3 - sz^2 + qz - n$.

ТАБЛИЦА МАКСИМАЛЬНЫХ И НЕМАКСИМАЛЬНЫХ КУБИЧЕСКИХ РЕШЕТОК ПОЛОЖИТЕЛЬНЫХ ДИСКРИМИНАНТОВ (КУБИЧЕСКИХ КОЛЕЦ ПОЛОЖИТЕЛЬНЫХ ДИСКРИМИНАНТОВ) ДЛЯ ВСЕХ $D \leqslant 1296$

Вычислена Д. К. Фаддеевым

№	D	Индексформа	Примечание	№	D	Индексформа	Примечание
1	49	(1,—1,—2, 1)	Макс.	21	761	(1,—1,—6,—1)	Макс.
2	81	(1, 0,—3,—1)	„	22	784	(2,—2,—4, 2)	Содерж. в № 1
3	148	(1,—1,—3, 1)	„	23	785	(1,—1,—6, 5)	Макс.
4	169	(1,—1,—4,—1)	„	24	788	(1,—1,—7,—3)	„
5	229	(1, 0,—4,—1)	„	25	837	(1, 0,—6,—1)	„
6	257	(1,—1,—4, 3)	„	26	892	(1,—1,—8, 10)	„
7	316	(1,—1,—4, 2)	„	27	916	(1,—1,—6, 4)	Содерж. в № 5
8	321	(1,—1,—4, 1)	„	28	940	(1, 0,—7,—4)	Макс.
9	361	(1,—1,—6, 7)	„	29	961	(2,—1,—5, 2)	„
10	404	(1,—1,—5,—1)	„	30	985	(1,—1,—6, 1)	„
11	469	(1,—1,—5, 4)	„	31	993	(1,—1,—6, 3)	„
12	473	(1,0,—5,—1)	„	32	1016	(1,—1,—6, 2)	„
13	564	(1,—1,—5, 3)	„	33	1076	(1, 0,—8,—6)	„
14	568	(1,—1,—6,—2)	„	34	1101	(1,—1,—9, 12)	„
15	592	(1,—1,—5, 1)	Содерж. в № 3	35	1129	(1, 0,—7,—3)	„
16	621	(1, 0,—6,—3)	Макс.	36	1229	(1,—1,—7, 6)	„
17	697	(1, 0,—7,—5)	„	37	1257	(1,—1,—8, 9)	„
18	729	(1, 0,—9,—9)	Содерж. в № 2	38	1264	(1, 0,—7,—2)	Содерж. в № 7
19	733	(1, —1,—7, 8)	Макс.	39	1264	(1,—1,—7,—1)	„ в № 7
20	756	(1, 0,—6,—2)	„	40	1296	(2, 0,—6,—2)	„ в № 2

Замечание. Число классов идеалов во всех *максимальных* кольцах таблицы равно 1.

§ 31. Непосредственная табуляризация кубических циклических максимальных решеток

Для циклических максимальных решеток задача табуляризации может быть решена посредством очень простых соображений, отличных от соображений предыдущих параграфов и приводящих к приему табуляризации, требующему весьма небольшого количества вычислений.

Будем называть решетку, повторяющуюся умножением, образованную числами кубической циклической области, симметричною, если она переходит в себя при циклических перестановках корней производящего уравнения. Такая решетка переходит в себя при поворотах вокруг рациональной прямой на углы в 120° и 240°.

Способ табуляризации, которому посвящен этот параграф, даст возможность построить все такие решетки в порядке возрастания дискриминантов. Нетрудно подтвердить примерами, что не каждое кольцо, образованное числами циклической области, будет симметричным, однако максимальные кольца, построение которых нас особенно интересует (см. § 3), очевидно, все симметричны.

Докажем две леммы, необходимые для дальнейшего.

Лемма 1. *В каждом кольце существует „симметричный" базис вида* $(1, \rho, \rho')$, *где* ρ' *— число, сопряженное с* ρ. *Все такие базисы распределяются по шести „параллелям". Именно, если* $[1, \rho, \rho']$ *один из симметричных базисов, то все остальные имеют вид:*

$$[1, \rho + k, \rho' + k]; \quad [1, \rho' + k, \rho'' + k]; \quad [1, \rho'' + k, \rho + k];$$
$$[1, -\rho + k, -\rho' + k]; \quad [1, -\rho' + k, -\rho'' + k]; \quad [1, -\rho'' + k, -\rho + k],$$

где k *— целое рациональное число.*

ТАБЛИЦА МАКСИМАЛЬНЫХ РЕШЕТОК ОТРИЦАТЕЛЬНЫХ ДИСКРИМИНАНТОВ ДЛЯ ВСЕХ $|D| < 1000$

(Вычислена Bervick'ом и Mathevs'ом и перевычислена Б. Н. Делоне)

№	$-D$	Индексформы	№	$-D$	Индексформы	№	$-D$	Индексформы	№	$-D$	Индексформы
1	23	(1, 1, 2, 1)	34	324	(1, 0,—3,4,)	65	527	(1, 0, 5, 1)	97	780	(1, 4, 4, 6)
2	31	(1, 0, 1, 1)	35	327	(1, 4, 3, 3)	66	543	(1, 1, 2, 5)	98	804	(1, 1, 4, 6)
3	44	(1,—1, 1, 1)	36	331	(1,—2, 4, 1)	67	547	(1, 4, 2, 3)	99	808	(1, 0, 2, 6)
4	59	(1, 0, 2, 1)	37	335	(1,—1, 4, 1)	68	563	(1, 2, 6, 1)	100	812	(1, 4,—2, 2)
5	76	(1, 1, 3, 1)	38	339	(1, 2, 0, 3)	69	567	(1, 3, 0, 3)	101	815	(1, 6, 5, 3)
6	83	(1,—2, 2, 1)	39	351	(1, 3, 6, 1)	70	588	(1,—1, 5, 1)	102	823	(1, 3,—2, 3)
7	87	(1,—1, 2, 1)	40	356	(1, 0—7, 8)	71	620	(1, 4, 0, 2)	103	835	(1, 2, 0, 5)
8	104	(1, 0—1, 2)	41	364	(1, 0, 4, 2)	72	628	(2, 5, 6, 5)	104	839	(1, 4, 3, 5)
9	107	(1, 2, 4, 1)	42	367	(1, 4, 7, 1)	73	643	(1,—6, 10, 1)	105	843	(3, 3, 5, 2)
10	108	(1, 0, 0, 2)	43	379	(1, 1, 1, 4)	74	648	(2, 0, 3, 2)	106	856	(2, 2, 1, 3)
11	116	(1, 1, 0, 2)	44	411	(1, 1, 5, 2)		aus.		107	863	(1, 2, 3, 7)
12	135	(1, 0, 3, 1)	45	419	(1, 3—1, 2)	75	652	(1, 6, 4, 2)	108	867	(1, 7, 5, 2)
13	139	(1, 4, 6, 1)	46	424	(1,8—7, 2)	76	655	(1, 2, 1, 5)	109	876	(3, 2, 4, 2)
14	140	(1, 3, 5, 1)	47	431	(2, 1, 3, 2)	77	671	(1, 3, 2, 5)	110	883	(1, 5,—5, 2)
15	152	(1, 1,—2, 2)		aus.		78	675	(1, 0, 0, 5)	111	888	(2, 2, 5, 3)
16	172	(1, 2, 0, 2)	48	432	(1, 0, 0, 4)	79	676	(2, 2, 5, 2)	112	891	(1, 0, 6, 1)
17	175	(1,—2, 3, 1)	49	436	(1, 3, 4, 6)	80	679	(1, 3, 4, 7)	113	907	(1, 5, 1, 2)
18	199	(1, 1, 4, 1)	50	439	(1, 2,—1, 3)	81	680	(1, 5, 2, 2)	114	908	(2, 6, 4, 3)
19	200	(1, 2, 3, 4)	51	440	(1, 7, 6, 2)	82	687	(1, 2, 5, 7)	115	931	(1,—2, 6, 1)
20	204	(1, 1, 1, 3)	52	451	(1, 5, 3, 2)	83	695	(1,—5, 8, 1)	116	932	(1, 0, 5, 4)
21	211	(1, 6, 10, 1)	53	459	(1, 3,—3, 2)	84	796	(1, 2—1, 4)	117	940	(1, 3, 1, 5)
22	212	(1, 1, 4, 2)	54	460	(1, 1, 5, 3)	85	707	(1, 3, 5, 8)	118	948	(1, 2, 1, 6)
23	216	(1, 0, 3, 2)	55	472	(1, 3,—2, 2)	86	716	(1, 3,—1, 3)	119	959	(1,—1, 6, 1)
24	231	(1,—4, 5, 1)	56	484	(1, 2, 5, 6)	87	728	(1, 1, 6, 2)	120	964	(2, 6, 5, 4)
25	239	(1, 0,—1, 3)	57	491	(1,—4, 6, 1)	88	731	(1, 4, 8, 1)	121	971	(2, 3, 1, 3)
26	243	(1, 0, 0, 3)	58	492	(1, 2, 4, 6)	89	743	(1, 0, 5, 3)	122	972	(1, 0, 0, 6)
27	244	(1, 5, 4, 2)	59	499	(1, 0, 4, 3)	90	744	(1, 4—1, 2)	123	972	(2, 6, 6, 5)
28	247	(1,—3, 4, 1)	60	503	(2, 5, 5, 4)	91	748	(1, 2, 2, 6)	124	980	(2, 4, 5, 5)
29	255	(1, 5, 8, 1,)		aus.		92	751	(1, 1, 6, 1)	125	983	(1, 1, 6, 5)
30	268	(1, 7, 13, 1)	61	515	(1, 4, 4, 5)	93	755	(1, 2, 6, 7)	126	984	(2, 1, 0, 3)
31	283	(1, 0, 4, 1)	62	516	(3, 3, 4, 2)	94	756	(2, 3, 6, 3)	127	996	(1, 4, 5, 8)
32	300	(1, 4, 2, 2)	63	519	(1, 5, 4, 3)	95	759	(1, 1, 6, 3)	128	999	(2, 3, 3, 4)
33	307	(1, 2, 4, 1)	64	524	(1, 1, 3, 5)	96	771	(1, 1, 3, 6)		aus.	

Замечание. Даны, по возможности, индексформы с первым коэффициентом, равным 1 (т. е. обнаруживающие степенной базис), а из таких, по возможности, с 4-м коэффициентом 1. Не имеют степенного базиса решетки с общим делителем индексов, отмеченные знаком „aus.", а также решетки №№ 62 и 72; решетки №№ 79, 94, 105, 106 и т. д. в этом смысле под сомнением.

ТАБЛИЦА НЕМАКСИМАЛЬНЫХ РЕШЕТОК, СОДЕРЖАЩИХ 1 с $|D| < 1000$

$-D$	Индексформы	$-D$	Индексформы	$-D$	Индексформы
176	(1,—1, 3, 1) ⊂ № 3	556	(1, 4, 3, 4) ⊂ № 13	816	(1, 5, 3, 3) ⊂ № 20
236	(1,—2, 1, 2) ⊂ № 4	560	(1, 2, 0, 4) ⊂ № 14	844	(1, 1, 6, 4) ⊂ № 21
279	(1, 2, 5, 1) ⊂ № 2	575	(1,—2, 5, 1) ⊂ № 1	848	(1, 4, 2, 4) ⊂ № 22
304	(1, 5, 7, 1) ⊂ № 5	608	(1, 5, 9, 1) ⊂ № 15	848	(1, 5, 4, 4) ⊂ № 22
332	(1, 1, 2, 4) ⊂ № 6	608	(1, 1, 1, 5) ⊂ № 15	864	(1, 9, 21, 1) ⊂ № 23
368	(2, 2, 4, 2) ⊂ № 1	684	(1, 4—4, 2) ⊂ № 5	864	(1,0,—3,6) ⊂ № 23
416	(1, 1, 5, 1) ⊂ № 8	688	(1, 3, 7, 1) ⊂ № 16	944	(1, 2, 5, 8) ⊂ № 4
416	(1, 2, 1, 4) ⊂ № 8	704	(2, 4, 4, 4) ⊂ № 3	944	(2, 0, 4, 2) ⊂ № 4
428	(1, 3, 2, 4) ⊂ № 9	783	(1, 4, 1, 3) ⊂ № 7	972	(1, 0, 6, 2) ⊂ № 10
432	(1, 0, 0, 4) ⊂ № 10	783	(1, 3, 6, 9) ⊂ № 7	972	(1, 6, 3, 2) ⊂ № 26
464	(1,—3, 5, 1) ⊂ № 11	800	(1, 5, 5, 5) ⊂ № 19	976	(1, 2, 6, 8) ⊂ № 27
464	(1, 3, 5, 7) ⊂ № 11	800	(2, 3, 4, 4) ⊂ № 19	976	(1, 3, 4, 8) ⊂ № 27
496	(2, 0, 2, 2) ⊂ № 2				

Доказательство. Спроектируем симметричное кольцо параллельно рациональному направлению на перпендикулярную плоскость $x+y+z=0$. Проекция представляется как плоская решетка, совмещающаяся с собой при поворотах на 120° и 240° вокруг начала координат. Рассмотрим точку α проекции, ближайшую к началу координат. Вместе с ней решетка-проекция должна содержать точку $-\alpha$ и точки, получающиеся из α и $-\alpha$ поворотами на 120° и 240°. Эти шесть точек образуют правильный шестиугольник с центром в начале координат. Каждый параллелограмм, построенный на начале и трех смежных вершинах шестиугольника, будет пуст внутри и на границе и, следовательно, может быть принят за основной параллелограмм решетки. Всякий же другой параллелограмм, построенный на точке решетки и на точке, получающейся из первой поворотом на угол 120°, будет содержать внутри себя или на границе, по крайней мере, одну из вершин основного шестиугольника и потому не может быть принят за основной. Поэтому за числа симметричного базиса кольца могут быть приняты только те числа, которые проектируются в вершины основного шестиугольника. Каждое же такое число может быть принято за число симметричного базиса, ибо если точка $(\omega, \omega', \omega'')$ проектируется в вершину α, то сопряженная с ней точка $(\omega', \omega'', \omega)$ проектируется в вершину α'.

Тем самым лемма доказана.

Лемма 2. *Пусть ρ — число циклической области и ρ' — сопряженное с ρ число. Коэффициенты a, b, c, d дробнолинейного представления $\rho' = \frac{a\rho+b}{c\rho+d}$ числа ρ' через ρ удовлетворяют соотношению*

$$ad - bc = (a+d)^2.$$

Доказательство. Пусть

$$\rho' = \frac{a\rho+b}{c\rho+d}.$$

Тогда

$$\rho'' = \frac{a\rho'+b}{c\rho'+d} \quad \text{и} \quad \rho = \frac{a\rho''+b}{c\rho''+d}.$$

Подставив в последнее равенство выражение ρ'' через ρ', получим

$$\rho = \frac{a\dfrac{a\rho'+b}{c\rho'+d}+b}{c\dfrac{a\rho'+b}{c\rho'+d}+d} = \frac{(a^2+bc)\rho'+b(a+d)}{c(a+d)\rho'+(d^2+bc)},$$

откуда

$$\rho' = \frac{-(d^2+bc)\rho+b(a+d)}{c(a+d)\rho-(a^2+bc)}.$$

Из однозначности дробнолинейного представления следует необходимость равенств

$$-(d^2+bc)=a\lambda,\quad b(a+d)=b\lambda,\quad c(a+d)=c\lambda,\quad -(a^2+bc)=d\lambda,$$

откуда

$$\lambda=a+d.$$

1-е и 4-е соотношения дают

$$a^2+ad+d^2+bc=0,$$

или, что то же самое,

$$(a+d)^2=ad-bc,$$

что и требовалось доказать.

Перейдем теперь к изложению способа табуляризации. Идея способа состоит в том, что в каждом симметричном кольце можно указать в некотором смысле приведенные числа, однозначно определяемые в кольце и в свою очередь задание каждого из которых однозначно определяет кольцо.

Такими числами являются компоненты нормального базиса, выбранного для параллели симметричных базисов. Симметричное кольцо содержит двенадцать приведенных чисел, так как в таком кольце существует шесть параллелей симметричных базисов и каждая параллель приводит к построению двух приведенных чисел.

Пусть ρ — одно из приведенных чисел. Другое приведенное число, образующее с ним нормальный базис, должно иметь вид $\rho'-m$, ибо оно должно находиться в „параллели", содержащей сопряженное с ρ число ρ'. По определению нормального базиса должно иметь место равенство

$$\rho(\rho'-m)=k,$$

где k — целое рациональное число, откуда

$$\rho'=\frac{m\rho+k}{\rho}.$$

В силу второй леммы, между числами m и k должно быть выполнено соотношение $k=-m^2$ и, следовательно,

$$\rho'=\frac{m\rho-m^2}{\rho}.$$

Легко видеть, что $\rho=\frac{-m^2}{\rho'-m}$, откуда следует, что

$$\rho''=\frac{-m^2}{\rho-m}.$$

Составим уравнение, корнями которого являются ρ, ρ' и ρ''. Обозначим через s первый коэффициент этого уравнения

$$s=\rho+\rho'+\rho''.$$

Остальные коэффициенты легко определяются:

$$q=\rho\rho'+\rho'\rho''+\rho''\rho=m\rho-m^2+m\rho'-m^2+m\rho''-m^2=ms-3m^2,$$

$$n=\rho\rho'\rho''=\rho\frac{m\rho-m^2}{\rho}\cdot\frac{-m^2}{\rho-m}=-m^3.$$

Таким образом, ρ удовлетворяет уравнению

$$\rho^3=s\rho^2-m(s-3m)\rho-m^3.$$

Легко видеть, что если ρ — одно из приведенных чисел, то все приведенные числа суть

$$\begin{array}{ccc}\rho, & \rho', & \rho''\\ -\rho, & -\rho', & -\rho''\\ \rho-m, & \rho'-m, & \rho''-m\\ m-\rho, & m-\rho', & m-\rho''\end{array}$$

Все эти числа являются корнями четырех уравнений

$$\rho^3 = s\rho^2 - m(s - 3m)\rho - m^3,$$
$$\rho_1^3 = s_1\rho_1^2 - m_1(s_1 - 3m_1)\rho_1 - m_1^3,$$
$$\rho_2^3 = s_2\rho_2^2 - m_2(s_2 - 3m_2)\rho_2 - m_2^3,$$
$$\rho_3^3 = s_3\rho_3^2 - m_3(s_3 - 3m_3)\rho_3 - m_3^3,$$

параметры s_i и m_i которых связаны с параметрами s и m одного из них посредством соотношений

$$s_1 = -s, \quad s_2 = s - 3m, \quad s_3 = 3m - s,$$
$$m_1 = -m, \quad m_2 = -m, \quad m_3 = m.$$

Из этих четырех уравнений легко выбрать одно, потребовав выполнения неравенств $m > 0$; $s \geqslant \frac{3}{2} m$.

Таким образом, каждому симметричному кольцу однозначно сопоставляется уравнение вида

$$\rho^3 = s\rho^2 - m(s - 3m)\rho - m^3,$$

параметры которого s и m удовлетворяют неравенствам $m > 0$; $s \geqslant \frac{3}{2} m$.

Любая пара корней такого уравнения вместе с числом 1 образует симметричный базис кольца.

Обратно, каждое такое уравнение однозначно определяет симметричное кольцо при любых целочисленных значениях параметров s и m. Действительно, дискриминант такого уравнения

$$D(\rho) = s^2m^2(s - 3m)^2 + 4s^3m^3 - 4m^3(s - 3m)^3 - 18m^4s(s - 3m) - 27m^6 = \\ = m^2(s^2 - 3ms + 9m^2)^2$$

представляет собою полный квадрат, и, следовательно, корни уравнения рационально выражаются друг через друга. Легко найти, что один из корней ρ' выражается через другой корень ρ в виде $\rho' = \frac{m\rho - m^2}{\rho}$.

Числа ρ и ρ' вместе с числом 1 могут быть приняты за симметричный базис кольца, так как числа ρ^2, $\rho\rho'$ и ρ'^2 выражаются линейно с целыми коэффициентами через 1, ρ и ρ'. В самом деле

$$\rho^2 = s\rho - m(s - 3m) - \frac{m^3}{\rho} = s\rho + m\rho' - m(s - 2m),$$
$$\rho\rho' = m\rho - m^2,$$
$$\rho'^2 = s\rho' + m\rho'' - m(s - 2m) = -m\rho + (s - m)\rho' + 2m^2.$$

Дискриминант кольца, которое получится этим способом, равен

$$D = \begin{vmatrix} 1, & \rho, & \rho' \\ 1, & \rho', & \rho'' \\ 1, & \rho'', & \rho \end{vmatrix}^2 = (\rho^2 + \rho'^2 + \rho''^2 - \rho\rho' - \rho'\rho'' - \rho'\rho)^2 = (s^2 - 3ms + 9m^2)^2.$$

Таким образом, придавая параметрам s и m всевозможные целочисленные значения, удовлетворяющие неравенствам $m > 0$ и $s \geqslant \frac{3}{2} m$, мы получим все симметричные кольца и каждое по одному разу. В виду того, что $\sqrt{D} = s^2 - 3ms + 9m^2$ представляет собой положительную квадратичную форму, легко задавать значения m и s так, чтобы получать симметричные кольца в порядке возрастания дискриминантов. Среди колец, получаемых этим способом, будут получаться, кроме неприводимых, также и приводимые кольца.

Построив все кольца, дискриминанты которых не превосходят данной границы, легко выбрать из них максимальные.

Таким образом, приведенный способ дает полное решение задачи табуляризации симметричных колец и, в частности, максимальных колец циклических областей.

ТАБЛИЦА ОБРАЗУЮЩИХ УРАВНЕНИЙ НЕПРИВОДИМЫХ МАКСИМАЛЬНЫХ ЦИКЛИЧЕСКИХ КОЛЕЦ ДЛЯ ВСЕХ $\sqrt{D} < 100$

$\sqrt{D}$	s	q	n	$\sqrt{D}$	s	q	n	$\sqrt{D}$	s	q	n	$\sqrt{D}$	s	q	n
7	2	1	—1	31	5	2	— 8	63	9	—6	— 1	79	10	— 7	— 1
9	3	0	—1	37	7	— 4	— 1	63	9	—6	— 8	91	11	—10	— 8
13	4	—1	—1	43	7	— 2	— 8	67	7	6	—27	91	10	— 3	—27
19	5	—2	—1	61	5	12	—27	73	8	3	—27	97	11	— 8	— 1

Б. НЕКОТОРЫЕ ГЕОМЕТРИЧЕСКИЕ ТЕОРЕМЫ

§ 32. Геометрия кубической двойничной формы и ее ковариантов

Хорошо известна (см., например, приложение к русскому переводу лекций по теории чисел Дирихле) интерпретация квадратичной двойничной формы с вещественными коэффициентами при помощи двухсторонника, заданного в плоскости с точностью до обычного поворота, в случае $D > 0$, и с точностью до гиперболического поворота, в случае $D < 0$. Мы покажем в этом параграфе, как кубическая двойничная форма f с вещественными коэффициентами может быть интерпретирована при помощи двухсторонника в плоскости, но такого, который вполне задан. Все коварианты f, H, Q, D полной системы ее ковариантов интерпретируются тем же двухсторонником, которым интерпретируется сама форма f, причем квадратичная форма H и дискриминант D — в обычном смысле.

Пусть $f(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3$ — какая-угодно кубическая двойничная форма с вещественными или комплексными коэффициентами a, b, c и d. Мы будем, как в § 15, называть корни ρ_1, ρ_1', ρ_1'' уравнения $f(X, a) = 0$ левыми, а корни ρ_2, ρ_2', ρ_2'' уравнения $f(d, -Y) = 0$ правыми корнями формы f.

Если t_1 — левый кореиь, то, как легко видеть, $t_2 = -\frac{ad}{t_1}$ — правый корень f. Такие два корня f мы будем называть соответственными и будем предполагать, что ρ_1 и ρ_2, ρ_1' и ρ_2', ρ_1'' и ρ_2'' — попарно соответственные.

Начнем со следующей леммы, являющейся перефразировкой способа Лагранжа для решения кубического уравнения при помощи резольвент на случай кубической двойничной формы.

Лемма I. *Если коэффициенты a, b, c, d формы f — какие угодно вещественные или комплексные числа, то имеет место тождество в XY:*

$$f(X, Y) = \frac{1}{3\Delta}(\xi^3 - \eta^3),$$

где $\xi = \xi_1 X + \xi_2 Y$; $\eta = \eta_1 X + \eta_2 Y$; $\xi_1 = \rho_1 + \varepsilon\rho_1' + \varepsilon^2\rho_1''$; $\eta_1 = \rho_1 + \varepsilon^2\rho_1' + \varepsilon\rho_1''$;

$\xi_2 = \rho_2 + \varepsilon\rho_2' + \varepsilon^2\rho_2''$; $\eta_2 = \rho_2 + \varepsilon^2\rho_2' + \varepsilon\rho_2''$, *причем* $\varepsilon = e^{\frac{2\pi i}{3}}$ *и* $\Delta = \begin{vmatrix} \xi_1 & \eta_1 \\ \xi_2 & \eta_2 \end{vmatrix}$.

Действительно, принимая во внимание, что $\rho_1\rho_2 = -ad$, мы получаем $a\rho_2 = \rho_1^2 + b\rho_1 + ac$; $d\rho_1 = -\rho_2^2 + c\rho_2 - bd$. Подставляя это в Δ и, далее, полученное Δ в коэффициенты $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$ выражения $\frac{1}{3\Delta}(\xi^3 - \eta^3)$, мы убеждаемся прямым вычислением, что они равны a, b, c, d.

Определение ковариантов, т. е. гессиана H, якобиана Q и дискриминанта D кубической двойничной формы f — следующее:

$$H = -\frac{1}{4}\begin{vmatrix} \frac{\partial^2 f}{\partial x^2}, & \frac{\partial^2 f}{\partial x\,\partial y} \\ \frac{\partial^2 f}{\partial x\,\partial y}, & \frac{\partial^2 f}{\partial y^2} \end{vmatrix} = (b^2 - 3ac)X^2 + (bc - 9ad)XY + (c^2 - 3bd)Y^2 =$$
$$= AX^2 + BXY + CY^2;$$

$$Q=\begin{vmatrix}\frac{\partial f}{\partial x}, & \frac{\partial f}{\partial y}\\ \frac{\partial H}{\partial x}, & \frac{\partial H}{\partial y}\end{vmatrix}=(9abc-2b^3-27a^2d)X^3+$$
$$+(18ac^2-3b^2c-27abd)X^2Y+$$
$$+(27acd+3bc^2-18b^2d)XY^2+$$
$$+(27ad^2+2c^3-9bcd)Y^3=$$
$$=a'X^3+b'X^2Y+c'XY^2+d'Y^3;$$

$$D=\frac{1}{3}\begin{vmatrix}\frac{\partial^2 H}{\partial x^2}, & \frac{\partial^2 H}{\partial x\,\partial y}\\ \frac{\partial^2 H}{\partial y\,\partial x}, & \frac{\partial^2 H}{\partial y^2}\end{vmatrix}=b^2c^2-4ac^3-4b^3d+18abcd-27a^2d^2,$$

причем численные коэффициенты перед определителями здесь выбраны так, чтобы в случае, когда коэффициенты a, b, c, d заданной кубической двойничной формы $f(X, Y)=aX^3+bX^2Y+cXY^2+dY^3$ — целые рациональные, коэффициенты каждой из форм H, Q, D, т. е. A, B, C; a', b', c', d'; D, получались также целыми рациональными и без тождественного общего делителя и чтобы, если $D>0$, форма H была положительная.

Лемма II. *Ковариаиты кубической двойничной формы равны*

$$H=\xi\eta,\quad Q=\xi^3+\eta^3,\quad D=-\frac{\Delta^2}{3}.$$

Действительно, принимая во вниманне, что $f=\frac{1}{3\Delta}(\xi^3-\eta^3)$, $\xi=\xi_1X+\xi_2Y$, $\eta=\eta_1X+\eta_2Y$, $\Delta=\begin{vmatrix}\xi_1 & \eta_1\\ \xi_2 & \eta_2\end{vmatrix}$, мы непосредственно вычислением проверяем эти выражения.

Эти две чисто алгебраические леммы дают тождества, верные для кубической двойничной формы f с какими угодно вещественными или комплексными коэффициентами a, b, c, d. Мы будем теперь дальше все время предполагать, что коэффициенты a, b, c, d — действительные. Тогда имеют место следующие дальнейшие леммы.

Лемма III. (А): *Если a, b, c, d действительны и $D>0$, то ρ_1, ρ_1', ρ_1'', а следовательно и ρ_2, ρ_2', ρ_2'' — действительные, и тогда ξ_1 и ξ_2 — комплексные, причем площадь s параллелограмма, построенного на векторах, идущих по комплексной плоскости к точкам ξ_1 и ξ_2, не равна нулю; η_1 и η_2 — числа комплексные, сопряжвнные с ξ_1 и ξ_2; наоборот, если ξ_1 и ξ_2 — комплексные, площадь s, на них построенная, нв равна нулю, и η_1, η_2 — числа, им комплексно сопряженные, то коэффициенты a, b, c, d — действительные, и $D>0$.* (Б): *Если a, b, c, d действительны и $D<0$, то один из левых корней формы (мы будем за него принимать ρ_1) действителен, а два других ρ_1', ρ_1'' — комплексно сопряженные, и, аналогично, — соответственные им ρ_2, ρ_2', ρ_2''; в этом случае ξ_1, ξ_2, η_1, η_2 — действительнын, причем площадь s параллелограмма, построенного на векторах (ξ_1, η_1), (ξ_2, η_2), не равна нулю; наоборот, если ξ_1, η_1, ξ_2, η_2 — действительные и площадь s* этого *параллелограмма не равна нулю, то коэффициенты a, b, c, d — действительные, и $D<0$.*

Эта лемма непосредственно следует из формул, доказанных в лемме I, и того, что по лемме II $D=-\frac{\Delta^2}{3}$. Геометрическое толкование кубической двойничной формы с действительными коэффициентами и ее ковариантов, в силу лемм II и III, может быть следующим.

Случай $D>0$. В этом случае мы считаем соответствующим заданной кубической двойничной форме $f=\frac{1}{3\Delta}(\xi^3-\eta^3)$ двухсторонник, состоящий из векторов, идущих из начала плоскости комплексной переменной $\alpha+\beta i$ в точки $\xi_1=\alpha_1+\beta_1 i$, $\xi_2=\alpha_2+\beta_2 i$. Гессиан $H=\xi\eta$ будет в этом случае определенной квадратичной двойничной формой и будет интерпретироваться этим же двухсторонником в обычном смысле. Якобиан же $Q=\xi^3+\eta^3$ будет интерпретироваться так же, как и заданная форма f, двухсторонником, симметричным с двухсторонником (α_1, β_1), (α_2, β_2) по отношению к биссектрисе нечетных углов плоскости α, β и притом увеличенным линейно в $\sqrt[3]{6s}$ раз, так как, в случае $D>0$, $\Delta=-i\cdot 2s$, и мы имеем

$$f=\frac{1}{6s}\{[(\beta_1+\alpha_1 i)X-(\beta_2+\alpha_2 i)Y]^3+$$
$$+[(\beta_1-\alpha_1 i)X-(\beta_2-\alpha_2 i)Y]^3\},$$

а форма $Q=[(\alpha_1+\beta_1 i)X-(\alpha_2+\beta_2 i)Y]^3+[(\alpha_1-\beta_1 i)X-(\alpha_2-\beta_2 i)Y]^3$.
Наконец,

$$D=\frac{4}{3}s^2.$$

И наоборот, всякий заданный двухсторонник плоскости $\alpha+\beta i$ с площадью s, не равною нулю, соответствует в этом смысле некоторой кубической двойничной форме f с вещественными коэффициентами и положительным определителем D и ее ковариантам H, Q, D.

Случай $D<0$. В этом случае соответствующим заданной кубической двойничной форме $f=\frac{1}{3\Delta}(\xi^3-\eta^3)$ мы считаем двухсторонник, состоящий из векторов, идущих в плоскости ξ, η из начала к точкам $(\xi_1\ \eta_1)$, $(\xi_2,\ \eta_2)$.

Гессиан $H=\xi\eta$ будет в этом случае неопределенной квадратичной двойничной формой и будет интерпретироваться этим же двухсторонником по отношению к асимптотам ξ, η.

Якобиан $Q=\xi^3+\eta^3$ будет интерпретироваться так же, как и заданная форма f, двухсторонником, симметричным с двухсторонником $(\xi_1,\ \eta_1)$, $(\xi_2,\ \eta_2)$ по отношению к оси ξ и увеличенным линейно в $\sqrt[3]{3s}$ раз, так как, в случае $D<0$, $\Delta=s$ и мы имеем

$$f=\frac{1}{3s}[(\xi_1X+\xi_2Y)^3-(\eta_1X+\eta_2Y)^3],$$
$$Q=(\xi_1X+\xi_2Y)^3+(\eta_1X+\eta_2Y)^3;$$

наконец, дискриминант $D=-\frac{s^2}{3}$.

Если произвести вещественное линейное однородное преобразование переменных X, Y с определителем $\delta=\pm 1$, то форма f и ее коварианты H, Q, D преобразуются к некоторой новой форме $\bar{f}$ и ее ковариантам $\bar{H}$, $\bar{Q}$, $\bar{D}$, причем эти новые формы будут в вышеописанном смысле соответствовать тому новому двухстороннику, который получится из старого этим преобразованием. Если же определитель $\delta\neq\pm 1$, то для H, Q это будет так; что же касается самой формы f, то форма $\bar{f}$, соответствующая новому двухстороннику, будет не преобразованная форма $\bar{f}$, а $\frac{1}{\delta}\bar{f}$, так как в выражение формы через ее двухсторонник входит множитель $\frac{1}{\Delta}$, который при преобразовании переменных формы вовсе не изменяется, а между тем, если $\delta\neq\pm 1$, коэффициенты при X и Y в ξ и η, т. е. ξ_1, ξ_2, η_1, η_2 изменяются соответственно изменению

двухсторонника, и Δ должно было бы быть в δ раз бо́льшим. Что касается $\overline{\overline{D}}$, соответствующего преобразованному двухстороннику, то он будет равен $\delta^2 D$, а $\overline{D}$ преобразованной формы будет равен $\delta^4 D$.

Перейдем теперь к дальнейшему углублению геометрического толкования кубической двойничной формы с вещественными коэффициентами и неравным нулю определителем и ее ковариантов, а именно, будем рассматривать плоскость α, β в случае $D>0$ и плоскость ξ, η в случае $D<0$, на которой мы интерпретируем двухсторонником форму f и ее коварианты, расположенную в пространстве $R_{3,0}$ и соответственно $R_{3,1}$, причем, если нужно, мы преобразуем эту плоскость афинно. Это позволит нам установить связь между только что рассмотренным геометрическим толкованием и теорией, развитой в § 15.

Прежде всего мы докажем две леммы, связанные с произведением пары точек в пространстве $R_{3,0}$ или $R_{3,1}$. Будем попрежнему называть рациональной прямой в $R_{3,0}$ прямую $x=y=z$, а в $R_{3,1}$ прямую $x=z$, $y=0$; будем называть точку B параллельной точке A, если она получается из точки A перенесеннем параллельно рациональной прямой; и наконец, будем называть пару точек B_1, B_2 нормальной, если произведение их (в $R_{3,0}$ или соотв. $R_{3,1}$) есть точка рациональной прямой.

Лемма IV. *Если A_1 A_2 какая угодно пара точек в $R_{3,0}$ или $R_{3,1}$ некомпланарная с рациональной прямой, то существует одна и только одна ей параллельная нормальная пара B_1, B_2.*

Пусть координаты точек A_1 и A_2 суть (x_1, y_1, z_1) и (x_2, y_2, z_2), и мы имеем случай $R_{3,0}$. В таком случае параллельные им точки суть $(x_1+r_1, y_1+r_1, z_1+r_1)$ и $(x_2+r_2, y_2+r_2, z_2+r_2)$. Произведеиие их лежит на рациональной прямой тогда и только тогда, когда произведения их соответственных координат одинаковы. Получается система двух линейных уравнений для определения r_1 и r_2, определитель которой $\neq 0$, если точки A_1, A_2 некомпланарны рациональной прямой. В случае $R_{3,1}$, если $x \pm iy$ комплексные координаты точек, а z — веществеиные, то точки, параллельные A_1 и A_2, суть (x_1+r_1, y_1, z_1+r_1) и (x_2+r_2, y_2, z_2+r_2), и мы получаем то же самое.

Лемма V. *Левые и правые корни всякой кубической двойничной формы с вещественными коэффициентами и неравным нулю определителем D определяют (в случае $D>0$ в $R_{3,0}$, в случае $D<0$ в $R_{3,1}$) нормальную пару точек, и обратно, всякая нормальная пара точек определяет в этом смысле некоторую такую форму.*

Следует из определения левых и правых корней формы и из того, что произведение соответственных таких корней равно ad.

Перейдем, наконец, к доказательству леммы, связывающей рассмотренную геометрическую интерпретацию кубической двойничной формы двухсторонником на плоскости (α, β в случае $D>0$ и ξ, η в случае $D<0$) с теорией решения кубического уравнения, а для форм с целыми рациональными коэффициентами — с теорией, рассмотренной в § 15.

Лемма VI. *Если B_1, B_2 — нормальная пара точек пространства $R_{3,0}$, некомпланарная рациональной прямой, соответствующая кубической двойничной форме f с $D>0$, и A_1, A_2 — ортогональные (т. е. параллельные рациональной прямой) проекции точек B_1, B_2 на плоскость S нулевого следа $s=0$, т. е. на плоскость $x+y+z=0$ пространства $R_{3,0}$, то двухсторонник, образованный векторами, идущими из начала в точки A_1, A_2, интерпретирует форму f в выше рассмотренном смысле, если за ось α плоскости S взять ортогональную проекцию на плоскость S одной из осей координат (например, оси X) пространства $R_{3,0}$, а за ось β — ось, ей перпендикулярную, и взять соответствующие единичные отрезки на этих осях, и обратно.*

Действительно, обозначим расстояние, измеренное в отрезке e от точки пространства $R_{3,0}$ до плоскости S, через h. Тогда всякая точка пространства $R_{3,0}$

будет иметь, с одной стороны, прямоугольные координаты x, y, z, а с другой стороны — прямоугольные координаты α, β, h, причем между ними имеют место формулы перехода

$$\left.\begin{aligned} x &= \frac{1}{\sqrt{6}}(2\cdot\alpha + 0\cdot\beta + \sqrt{2}\cdot h), \\ y &= \frac{1}{\sqrt{6}}(-\alpha + \sqrt{3}\cdot\beta + \sqrt{2}\cdot h), \\ z &= \frac{1}{\sqrt{6}}(-\alpha - \sqrt{3}\cdot\beta + \sqrt{2}\cdot h). \end{aligned}\right\}$$

Непосредственное вычисление дает, если координаты x, y, z точек B_1 и B_2 суть ρ_1, ρ_1', ρ_1''; ρ_2, ρ_2', ρ_2'', что $\xi_1 = \alpha_1 + \beta_1 i$, $\xi_2 = \alpha_2 + \beta_2 i$ суть $\xi_1 = \rho_1 + \varepsilon\rho_1' + \varepsilon^2\rho_1''$; $\xi_2 = \rho_2 + \varepsilon\rho_2' + \varepsilon^2\rho_2''$.

Лемма VI'. *Если B_1, B_2 нормальная пара точек в пространстве $R_{3,1}$, некомпланарная рациональной прямой, соответствующая кубической двойничной форме f с $D < 0$, и A_1, A_2 — проекции точек B_1, B_2 параллельно рациональной прямой пространства $R_{3,1}$ на плоскость S нулевого слева $s = 0$, т. е. на плоскость $2x + z = 0$ пространства $R_{3,1}$ и если эту плоскость принять за плоскость ξ, η, причем подвергнуть плоскость ξ, η такому аффинному преобразованию, чтобы оси ξ, η шли по прямым, симметричным друг другу по отношению к плоскости $y = 0$, а именно, по прямым пересечения плоскости S с конусом $q = 0$, и взять за единичные на этих осях соответствующие отрезки, то двухсторонник A_1, A_2 плоскости ξ, η будет интерпретировать в выше рассмотренном смысле форму f, и обратно.*

Доказательство такое же, как для леммы VI, непосредственным вычислением ξ_1 и η_2.

Надо, однако, заметить, что для случая $D < 0$ выгоднее располагать плоскость ξ, η в плоскости XY пространства $R_{3,1}$, а не в плоскости $s = 0$, т. е. проектировать точки B_1, B_2 не на плоскость $s = 0$, а на плоскость $z = 0$, и кроме того брать за оси не ξ, η, а оси $\bar{\xi}$, $\bar{\eta}$, „повернутые“ по отношению к ним в плоскости на 45°. В таких осях, которые просто совпадают с осями X, Y плоскости XY и единицы на которых совпадают с бывшими на X, Y единицами, форма f при $D < 0$, выражается особенно удобно.

Действительно, если

$$\rho_1' = \alpha_1 + \beta_1 i, \quad \rho_2' = \alpha_2 + \beta_2 i,$$

то

$$(\xi_1 = \alpha_1 - \rho_1,\ \eta_1 = \beta_1), \quad (\xi_2 = \alpha_2 - \rho_2,\ \eta_2 = \beta_2),$$

и мы имеем

$$\rho_1\rho_2 = \rho_1'\rho_2' = -ad,$$

т. е.

$$\left.\begin{aligned} \alpha_1\alpha_2 - \beta_1\beta_2 &= -ad, \\ \alpha_1\beta_2 + \alpha_2\beta_1 &= 0, \end{aligned}\right\}$$

или

$$\left.\begin{aligned} (\xi_1 + \rho_1)(\xi_2 + \rho_2) - \eta_1\eta_2 &= ad, \\ (\xi_1 + \rho_1)\eta_2 + (\xi_2 + \rho_2)\eta_1 &= 0, \end{aligned}\right\}$$

откуда, если рассматривать квадратичную положительную форму

$$Ax^2 + 2Bxy + Cy^2,$$

соответствующую двухстороннику $(\xi_1\ \eta_1)(\xi_2\ \eta_2)$, т. е. положить

$$\xi_1^2 + \eta_1^2 = A; \quad \xi_1\xi_2 + \eta_1\eta_2 = B; \quad \xi_2^2 + \eta_2^2 = C,$$

мы получим

$$\rho_1 = -\frac{A\eta_2}{\Delta}, \quad \rho_2 = \frac{C\eta_1}{\Delta},$$

где

$$\Delta=\begin{vmatrix}\xi_1 & \eta_1\\ \xi_2 & \eta_2\end{vmatrix}.$$

Подставляя эти выражения ρ_1 и ρ_2 в выражения коэффициентов a, b, c, d кубической формы через ρ_1, ρ_1', ρ_1'', ρ_2, ρ_2', ρ_2'',

$$a=\frac{\rho_1\rho_1'+\rho_1\rho_1''+\rho_1'\rho_1''}{\rho_2+\rho_2'+\rho_2''};\quad -b=\rho_1+\rho_1'+\rho_1'';$$

$$c=\rho_2+\rho_2'+\rho_2'';\qquad -d=\frac{\rho_2\rho_2'+\rho_2\rho_2''+\rho_2'\rho_2''}{\rho_1+\rho_1'+\rho_1''},$$

мы получаем следующие их выражения через ξ_1, η_1, ξ_2, η_2:

$$a=\frac{A\eta_1}{\Delta};\quad b=\frac{A\eta_2+2B\eta_1}{\Delta};\quad c=\frac{C\eta_1+2B\eta_2}{\Delta};\quad d=\frac{C\eta_2}{\Delta}. \qquad (*)$$

Но форма $\eta(\xi^2+\eta^2)=a'X^3+b'X^2Y+c'XY^2+d'Y^3$, где, как раньше, $\xi=$ $=\xi_1X+\xi_2Y$; $\eta=\eta_1X+\eta_2Y$, имеет коэффициенты

$$a'=A\eta_1;\quad b'=A\eta_2+2B\eta_1;\quad c'=C\eta_1+2B\eta_2;\quad d'=C\eta_2. \qquad (**)$$

Сравнивая (*) и (**), мы получаем лемму:

Лемма VII. *Если* $\xi=\xi_1X+\xi_2Y$, $\eta=\eta_1X+\eta_2Y$ и (ξ_1, η_1) и $(\xi_2\eta_2)$ *суть координаты* x, y *проекций на плоскость* XY *параллельно рациональному направлению точек* $R_{3,1}$, *соответствующих корням некоторой формы* $f(X, Y)$ с $D<0$, *то форма* $\eta(\xi^2+\eta^2)$ *отличается лишь множителем* Δ *от формы* $f(X, Y)$".

§ 33. Теория приведения кубической двойничной формы

Мы будем, по определению, из всех кубических двойничных форм, эквивалентных данной кубической двойничной форме $f(X, Y)$, с вещественными коэффициентами, т. е. получаемых из нее целочисленными линейными подстановками с определителем 1, считать приведенными те шесть форм, для которых приведен в смысле Зеллинга (см. приложение к русскому переводу Дирихле) двухсторонник, соответствующий этой форме, в случае $D>0$, рассматриваемый на плоскости нулевого следа пространства $R_{3,0}$, а в случае $D<0$ — на плоскости XY пространства $R_{3,1}$.

В случае $D>0$, следовательно, для приведения $f(X, Y)$ надо вычислить ковариант $H(X, Y)$ и приводить его тем способом, который описан в пунктах 19, 49, 50 указанного приложения к русскому переводу Дирихле. Если f — целочисленная форма, то и H — целочисленная, и потому в этом случае приведение H не представляет труда. Если $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ подстановка, преобразующая H в приведенную форму, т. е. $\overline{H}=H_{\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)}$, приведенная по Зеллингу форма, эквивалентная H, то $\overline{f}=f_{\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)}$ приведенная кубическая двойничная форма, эквивалентная f. Другие приведенные формы тогда получаются из $\overline{f}$ подстановками:

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix},\ \begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix},\ \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\ \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix},\ \begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix}.$$

В случае $D<0$, то же самое надо было бы делать при помощи квадратичной формы $AX^2+BXY+CY^2$, рассмотренной в конце предыдущего параграфа. Эта форма, как это геометрически очевидно, также ковариант формы f, но

иррациональный ковариант, так как ее коэффициенты A, B, C выражаются иррационально при помощи коэффициентов a, b, c, d формы f. Приведение самой формы (A, B, C) при помощи вычисления с ее коэффициентами поэтому неудобно.

Заметим, однако, что, как это следует из формул (*) предыдущего параграфа, выражение $bc - ad$ имеет следующий вид:

$$bc - ad = \frac{2}{\Delta^2}(A\eta_{i_2}^2 + 2B\eta_{i_1}\eta_{i_2} + C\eta_{i_1}^2)\cdot B,$$

и, следовательно, в виду того, что (A, B, C) положительна, если только не равны нулю одновременно η_{i_1}, η_{i_2} (чего быть не может, так как точки B_{i_1}, B_{i_2} некомпланарны рациональной прямой), мы видим, что знак B совпадает со знаком $bc - ad$. Для приведения формы f надо, следовательно, приводить ее по Зеллингу, требуя, чтобы $bc - ad$ было $\geqslant 0$.

А именно:

1°. Если сначала $bc - ad < 0$, делаем подстановку $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ несколько раз до тех пор, пока в первый раз не получится $bc - ad \geqslant 0$.

2°. Производим подстановку $\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$ максимально возможное число раз без нарушения неотрицательности $bc - ad$.

3°. Производим подстановку $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ максимально возможное число раз без нарушения неотрицательности $bc - ad$. Затем чередуем операции 2° и 3° до тех пор, пока не станет невозможным их дальнейшее применение.

Форма $\bar{f}$, которую мы при этом получим, и будет приведенная.

§ 34. Двойничные кубические формы как нормы

Дана решетка O, повторяющаяся умножением, и некоторая решетка, имеющая O своим кольцом множителей.

Назовем примарной точкой решетки точку, обладающую тем свойством, что внутри отрезка, соединяющего точку с началом координат, нет точек решетки. Каждая примарная точка может быть принята за одну из точек базиса решетки. Следовательно, если преобразовывать форму Дирихле к эквивалентным всеми возможными способами, то числа, появляющиеся на вершинах символа, задающего коэффициенты формы, будут представлять собой нормы всех примарных точек решетки.

Рациональным сечением решетки назовем совокупность всех точек решетки, лежащих в плоскости, проходящей через начало координат и содержащей по крайней мере две не коллинеарные с началом координат точки решетки. Рациональное сечение решетки является двухмерной решеткой. Каждому рациональному сечению можно сопоставить класс кубических двойничных форм следующим образом. Выбрав базис сечения и представив все точки сечения через базис в виде линейной формы с двумя целочисленными переменными, получим нормы всех точек сечения в виде кубической двойничной формы. Таким образом, с базисом рационального сечения связана кубическая двойничная форма, а с сечением в целом — класс кубических двойничных форм. Двойничные формы, сопоставленные этим способом с рациональными сечениями, представляют собой, очевидно, те и только те двойничные формы, которые появляются на сторонах символа формы Дирихле решетки при всевозможных преобразованиях этой последней к эквивалентным формам.

Каждому базису рационального сечения соответствует взаимная точка, которая, после нормализации взаимной решетки, переходит в вполне определенную

точку полярной решетки. Эта точка, очевидно, не зависит от выбора базиса сечения и, следовательно, сопоставляется сечению в целом. Очевидно, она будет примариой точкой полярной решетки.

Обратно, каждой примарной точке решетки можно сопоставить в этом смысле рациональное сечение полярной решетки. Для этого нужно построить взаимные точки для всех пар, образованных взятой точкой и всеми остальными точками решетки.

Покажем, что двойничная форма — норма сечения полярной решетки, сопоставленного некоторой примарной точке исходной решетки, является в некотором смысле обобщением индексформы.

Для этого обобщим понятие индекса числа на точки любой нормализованной решетки следующим образом. Взаимным индексом двух точек Ω и T, принадлежащих одной и той же нормализованной решетке, назовем квадратный корень из отношения дискриминанта формы $N(x\Omega + yT)$ к дискриминанту решетки. Выясним, чему равен взаимный индекс.

Пусть $N(x\Omega + yT) = ax^3 + bx^2y + cxy^2 + dy^3$.

По определению дискриминанта двойничной кубической формы, он равен

$$a^4 D\left(-\frac{T}{\Omega}\right) = (\omega\omega'\omega'')^4 \cdot \left(\frac{\tau}{\omega} - \frac{\tau'}{\omega'}\right)^2 \cdot \left(\frac{\tau'}{\omega'} - \frac{\tau''}{\omega''}\right)^2 \cdot \left(\frac{\tau''}{\omega''} - \frac{\tau}{\omega}\right)^2 =$$

$$= (\tau\omega' - \tau'\omega)^2 (\tau'\omega'' - \tau''\omega')^2 (\tau''\omega - \tau\omega'')^2 = N^2(T \times \Omega).$$

В этом равенстве τ, τ', τ'', ω, ω', ω'' обозначают координаты точек T и Ω, а $T \times \Omega$ — точку, взаимную паре T, Ω.

После нормализации взаимной решетки точка $T \times \Omega$ перейдет в точку Φ полярной решетки, и $N(T \times \Omega) = \sqrt{D} \cdot N(\Phi)$, где D — дискриминант решетки. Следовательно, взаимный индекс пары T, Ω равен норме точки полярной решетки, сопоставляемой паре T, Ω.

Из определения взаимного индекса следует, что обыкновенный индекс числа, принадлежащего кольцу, представляет собой взаимный индекс пары, образованной изображениями этого числа и единицы при геометрическом представлении кольца как решетки.

Считая точку Ω фиксированной примарной точкой и точку T пробегающей все точки решетки, получим взаимные индексы пар (T, Ω) в виде кубической двойничной формы, которую мы будем называть индексформой решетки по отношению к примарной точке Ω. Обыкновенная индексформа кольца будет, таким образом, индексформой кольца по отношению к точке 1. Индексформа решетки по отношению к точке Ω является не чем иным, как формой-нормой сечения полярной решетки, соответствующего примарной точке Ω исходной решетки. Наоборот, каждая форма-норма рационального сечения данной решетки может рассматриваться как индексформа полярной решетки по отношению к ее точке, сопоставляемой взятому рациональному сечению исходной решетки.

§ 35. Оценка минимума кубической двойничной формы

Представление кубической двойничной формы как индексформы некоторого целочисленного кубического кольца позволяет оценить сверху минимум значений такой формы при целочисленных значениях переменных в зависимости от дискриминанта формы, т. е. указать такую границу, ниже которой наверное существуют значения формы.

Дадим эту оценку, рассмотрев порознь формы положительного и отрицательного дискриминанта.

Начнем с первого случая. Пусть дана кубическая двойничная форма $f(x, y)$, с целыми рациональными коэффициентами и с положительным дискриминан-

том D. Соответствующее этой форме кольцо изобразится в вещественном пространстве трех измерений как решетка, повторяющаяся умножением. Возьмем точку $(\omega', \omega'', \omega''')$, принадлежащую кольцу, и представим ее через нормальный базис кольца

$$\omega = x\omega_1 + y\omega_2 + z.$$

Индекс точки ω по отношению к кольцу будет как раз равен значению формы $f(x, y)$. Через координаты точки ω он представится в виде

$$f(x, y) = \frac{1}{\sqrt{D}}(\omega'' - \omega''')(\omega''' - \omega')(\omega' - \omega'').$$

Индекс $f(x,y)$ имеет одно и то же значение для всех точек, лежащих на одной параллели, и, следовательно, может быть выражен через координаты проекции точки ω на плоскость нулевого следа $\omega' + \omega'' + \omega''' = 0$. Примем за оси координат в плоскости $\omega' + \omega'' + \omega''' = 0$ прямую $O\xi$, являющуюся проекцией оси $O\omega'$, и перпендикулярную к ней прямую $O\eta$. При этом выборе осей проекция точки ω будет иметь координаты

$$\xi = \frac{2\omega' - \omega'' - \omega'''}{\sqrt{6}},$$

$$\eta = \frac{\omega'' - \omega'''}{\sqrt{2}}.$$

Из этих формул легко получим

$$f(x,y) = \frac{1}{\sqrt{D}}(\omega'' - \omega''')(\omega''' - \omega')(\omega' - \omega'') =$$

$$= \frac{1}{\sqrt{D}} \cdot \eta\sqrt{2} \cdot (-1) \cdot \frac{\xi\sqrt{6} + \eta\sqrt{2}}{2} \cdot \frac{\xi\sqrt{6} - \eta\sqrt{2}}{2} =$$

$$= \frac{\eta(\eta^2 - 3\xi^2)}{\sqrt{2D}}.$$

Если точка ω будет пробегать все кольцо, то ее проекция будет пробегать параллелограмматическую решетку, с площадью основного параллелограмма, равной $\frac{\sqrt{D}}{\sqrt{3}}$, ибо эта решетка представляет собой ортогональную проекцию пространственной решетки с объемом $\sqrt{D}$, параллельно направлению, на котором кратчайший вектор решетки имеет длину, равную $\sqrt{3}$.

Таким образом,

$$f(x,y) = \frac{\eta(\eta^2 - 3\xi^2)}{\sqrt{2D}},$$

причем целочисленным значениям (x, y) соответствуют точки (ξ, η), образующие решетку с площадью основного параллелограмма, равной $\sqrt{\frac{D}{3}}$.

Рассмотрим кривую с уравнением

$$\eta(\eta^2 - 3\xi^2) = \pm c.$$

Эта кривая состоит из шести „гиперболических" ветвей, которые могут быть получены из одной из них посредством вращения на углы, кратные 60°. Построим шестиугольник из касательных к кривой в точках, ближайших к началу

координат. Этот шестиугольник целиком уместится внутри звездчатой фигуры, ограниченной кривой, и, следовательно, для координат всех его точек имеет место неравенство

$$|\eta(\eta^2 - 3\xi^2)| \leqslant c.$$

Если выбрать c так, чтобы площадь шестиугольнника равнялась учетверенной площади основного параллелограмма решетки, то, по теореме Минковского о выпуклом теле, внутри или на границе шестиугольника найдется хотя бы одна точка (ξ_0, η_0) решетки, отличная от начала координат. Подберем такое c. Так как площадь шестиугольника равна

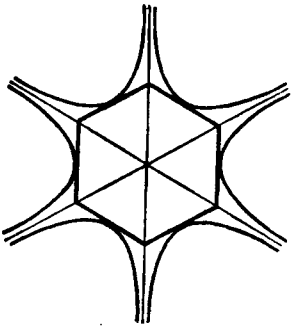
$$2\sqrt{3}\, c^{\frac{2}{3}},$$

нам нужно, чтобы

$$2\sqrt{3}\, c^{\frac{2}{3}} = 4\sqrt{\frac{D}{3}},$$

откуда

$$c = \left(\frac{2}{3}\right)^{\frac{3}{2}} \cdot D^{\frac{3}{4}}.$$



Черт. 5.

Обозначив через (x_0, y_0) значения переменных (x, y) для точки, проекция которой (ξ_0, η_0) находится внутри шестиугольника, будем иметь

$$|f(x_0, y_0)| = \left|\frac{\eta_0(\eta_0^2 - 3\xi_0^2)}{\sqrt{2D}}\right| \leqslant \left(\frac{2}{3}\right)^{\frac{3}{2}} \cdot \frac{D^{\frac{3}{4}}}{\sqrt{2D}} = \sqrt{\frac{4}{27}} \cdot D^{\frac{1}{4}}.$$

Таким образом, для бинарной кубической формы $f(x, y)$ положительного дискриминанта D всегда существуют такие целочисленные значения аргументов (x_0, y_0), что

$$|f(x_0, y_0)| \leqslant \sqrt{\frac{4}{27}} \cdot D^{\frac{1}{4}}.$$

Для форм отрицательного дискриминанта проведем аналогичное рассуждение.

Рассмотрим кольцо, для которого данная форма $f(x, y)$ отрицательного дискриминанта является индексформой, как решетку в пространстве K_3. Затем введем вещественные координаты в сигнатурном пространстве, в котором расположены точки кольца, с сохранением метрики пространства. Для этого мы должны принять в качестве вещественных координат точки $(\omega', \omega'', \omega''') = (\omega', \alpha + \beta i, \alpha - \beta i)$ числа $(\alpha\sqrt{2}, \beta\sqrt{2}, \omega')$. При этом выборе масштаба точка 1 будет иметь координаты $(\sqrt{2}, 0, 1)$, и, следовательно, длина кратчайшего целого рационального вектора будет равна $\sqrt{3}$, так же как в вещественном случае. Плоскость нулевого следа будет перпендикулярна к рациональной прямой, и объем основного параллелепипеда решетки, изображающей кольцо, будет равен $\sqrt{|D|}$. Следовательно, площадь основного параллелограмма проекции кольца на плоскость нулевого следа будет равна $\sqrt{\frac{|D|}{3}}$, так же как и в вещественном случае.

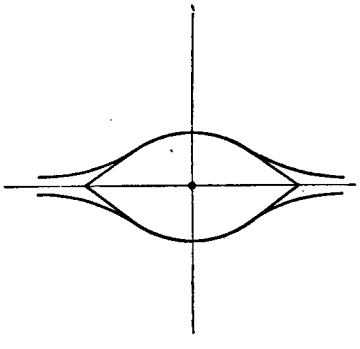
На плоскости нулевого следа примем за ось $O\eta$ „мнимую ось“ трехмерного пространства. За ось $O\xi$ примем перпендикулярную к ней проекцию „вещественной оси“. Координаты проекциии точки $(\omega', \omega'', \omega''')$ относительно этих осей будут, очевидно,

$$\eta = \frac{\omega'' - \omega'''}{\sqrt{2}i}; \qquad \xi = \frac{2\omega' - \omega'' - \omega'''}{\sqrt{6}}.$$

Посредством этих формул, так же как в предыдущем случае, легко представим значения индекс-формы $f(x, y)$ через координаты проекции точки ω на плоскость нулевого следа

$$f(x, y) = \frac{(\omega'' - \omega''')(\omega''' - \omega')(\omega' - \omega'')}{\sqrt{D}} = \frac{\eta(\eta^2 + 3\xi^2)}{\sqrt{2|D|}}.$$

Кривая $\eta(\eta^2 + 3\xi^2) = \pm c$ состоит из двух ветвей, асимптотически приближающихся к оси $O\xi$. Обе ветви этой кривой имеют точками перегиба точки пересечения с биссектрисами координатных углов. Касательные в точках перегиба образуют с осью $O\xi$ углы в 45°. Очевидно, фигура, ограниченная касательными в точках перегиба и участками кривой между точками перегиба, является центрально симметрической выпуклой фигурой. По теореме о выпуклом теле, фигура будет содержать внутри или на границе точку решетки, если площадь фигуры будет равна учетверенной площади основного параллелограмма решетки. Площадь фигуры легко подсчитывается приближенно, она равна $7{,}53\ldots \left(\frac{c}{4}\right)^{\frac{2}{3}}$. Следовательно, внутри или на границе фигуры найдется проекция (ξ_0, η_0) некоторой точки $\omega_0 = x_0\omega_1 + y_0\omega_2 + z$ кольца, если



Черт. 6.

$$c = \frac{32}{(7{,}53)^{\frac{3}{2}}} \left(\frac{|D|}{3}\right)^{\frac{3}{4}}.$$

Для точек, лежащих внутри или на границе фигуры, очевидно, выполнено неравенство $|\eta(\eta^2 + 3\xi^2)| \leqslant c$. Следовательно, для индекса точки ω_0 имеем:

$$|f(x_0, y_0)| = \frac{1}{\sqrt{2|D|}} |\eta_0(\eta_0^2 + 3\xi_0^2)| \leqslant \left(\frac{8}{7{,}53\ldots\sqrt{3}}\right)^{\frac{3}{2}} D^{\frac{1}{4}}.$$

Из приведенных оценок вытекают такие следствия:

1. $$D \geqslant \left(\frac{\sqrt{27}}{4}\right)^4 = 44{,}5\ldots \text{ для } D > 0,$$

$$|D| \geqslant 27 \cdot \left(\frac{7{,}53\ldots}{8}\right)^6 = 18{,}8\ldots \text{ для } D < 0.$$

Эти оценки снизу для величины дискриминанта кубического кольца более точны, чем те, которые получаются из общих оценок, приведенных в гл. I при $n = 3$, и, как мы уже видим из таблиц, очень близки к истинным.

2. При $0 < D < 729$ и $0 < -D \leqslant 300$

все кольца имеют степенной базис. Действительно, для таких дискриминантов в кольце всегда найдется число, индекс которого меньше 2 и, следовательно, равен единице. Такое число вместе со своим квадратом и единицей образует степенной базис кольца.

На основании этих оценок легко дать оценку сверху минимальной нормы идеала в каждом классе, ту самую оценку, на которую мы ссылались в § 22 гл. II.

В самом деле, пусть Γ_0, Γ_1, Γ_2... — главная и побочные решетки максимального кубического кольца и пусть L — наименьшее число, обладающее тем свойством, что в каждой решетке существует точка, норма которой не превосходит L, или, что то же самое, в каждом классе идеалов существует идеал, норма которого не превосходит L. Возьмем в некоторой решетке точку A такую, что $N(A) \leqslant L$. Точку A можно считать примарной, ибо если бы мы взяли непримарную точку, то ближайшая к началу координат точка решетки, лежащая на том же луче, что и точка A, имела бы еще меньшую норму. В полярной решетке найдется рациональное сечение, соответствующее точке A. Форма-норма этого сечения будет иметь дискриминант, равный $D \cdot N^2(A)$, и, по теореме о минимуме, среди значений этой формы найдется значение, меньшее чем

$$kD^{\frac{1}{4}}[N(A)]^{\frac{1}{2}} \leqslant kD^{\frac{1}{4}}L^{\frac{1}{2}},$$

где $k = \sqrt{\frac{4}{27}}$ для $D > 0$ и $k = \left(\frac{8}{7{,}53\sqrt{3}}\right)^{\frac{3}{2}}$ для $D < 0$. Но значения формы-нормы суть нормы точек взятого сечения. Следовательно, в каждой решетке существует точка, норма которой не превосходит $kD^{\frac{1}{4}}L^{\frac{1}{2}}$, ибо каждая решетка есть полярная для некоторой другой. В виду того, что L представляет собой наименьшее из чисел, для которых в каждой решетке существует точка с нормой, не превосходящей такого числа, должно иметь место неравенство:

$$L \leqslant L^{\frac{1}{2}} k |D|^{\frac{1}{4}},$$

откуда

$$L \leqslant k^2 |D|^{\frac{1}{2}} = \frac{4}{27}\sqrt{D} \quad \text{для } D > 0,$$
$$= \left(\frac{8}{7{,}53\sqrt{3}}\right)^3 \sqrt{|D|} \quad \text{для } D < 0.$$

§ 36. Одна теорема Тартаковского

Рассмотрим те целые кубические числа, у которых ограничены по абсолютной величине и их нормы и их дискриминанты, например,

$$|n| < N, \quad |D| < L,$$

где N и L — заданные положительные константы. Может ли быть таких чисел бесконечно много, или их только конечное число? Оказывается, что таких чисел только конечное число, и они все могут быть найдены.

Мы докажем эту теорему только для чисел, норма которых равна ± 1, т. е. для кубических единиц. Общая теорема доказывается аналогично.

Теорема. *Кубических единиц, дискриминанты которых по абсолютной величине меньше заданного числа L, ограниченное число, и они все могут быть найдены.*

Докажем сначала эту теорему для случая $D < 0$, т. е. для $W_{3,1}$. Очевидно; во-первых, что достаточно рассматривать только единицы ε с положительной нормой, т. е. имеющие в $R_{3,1}$ $z > 0$, так как если ε имеет отрицательную норму, то — ε имеет положительную, а $D_\varepsilon = D_{-\varepsilon}$. Заметим также, что $D_\varepsilon = D_{\varepsilon^{-1}}$, так как

$$D_{\varepsilon^{-1}} = [(\varepsilon^{-1} - \varepsilon'^{-1})(\varepsilon^{-1} - \varepsilon''^{-1})(\varepsilon'^{-1} - \varepsilon''^{-1})]^2 =$$
$$= [(\varepsilon - \varepsilon')(\varepsilon - \varepsilon'')(\varepsilon' - \varepsilon'')]^2 \cdot (\varepsilon^{-1}\varepsilon'^{-1})^2 \cdot (\varepsilon^{-1}\varepsilon''^{-1})^2 \cdot (\varepsilon'^{-1}\varepsilon''^{-1})^2 =$$
$$= D_\varepsilon \cdot ((\varepsilon\varepsilon'\varepsilon'')^{-1})^2 = D_\varepsilon,$$

и поэтому из каждых двух взаимнообратных единиц ε и ε^{-1} с положительной нормой достаточно рассматривать только ту, z которой <1. Такие единицы мы называем прямыми положительными единицами и только такие единицы мы и будем сейчас рассматривать. Все они лежат в $R_{8,1}$ на „нижней“ (ниже $z=1$) части поверхности вращения $(x^2+y^2)z=1$, которая асимптотически приближается к плоскости x, y. Все эти единицы лежат на этой части поверхности на линиях ее пересечения с плоскостями $2x+z=s$, где s пробегали все возможные целые рациональные значения. Каждая такая линия, в виду того, что нижняя часть поверхности $(x^2+y^2)z=1$ очень близко прилегает к плоскости x, y, представляет собою почти прямую „параллельную“ оси y.

Будем называть эти линии линиями s. Точки $W_{8,1}$, лежащие на данной линии s, имеют тем меньший дискриминант, чем ближе они лежат к плоскости $y=0$. Будем на каждой из линий s рассматривать точку $W_{3,1}$, на ней лежащую, самую близкую к плоскости $y=0$ (в самой плоскости $y=0$, среди точек $W_{8,1}$, лежат только точки рациональной прямой, т. е. из единиц только точка 1). Для доказательства теоремы (для $D<0$), очевидно, достаточно будет доказать, что даже среди этих точек есть лишь ограниченное число таких, дискриминант которых $<L$ по абсолютной величине.

Мы имеем

$$s=2x+z;\quad q=x^2+y^2+2xz;\quad n=(x^2+y^2)z,$$

откуда

$$x=\frac{s-z}{2};\quad q=\frac{(s-z)^2}{4}+y^2+(s-z)z,$$

или

$$s^2+2sz-3z^2-4q=-4y^2,$$

и мы получаем

$$-2\sqrt{q+z^2}<s-z<2\sqrt{q+z^2}.$$

Заметим еще, что для всех целых точек любой линии s $q>0$ и что самая близкая к плоскости $y=0$ целая точка данной линии s та, в которой эту линию пересекают поверхность q с самым малым q, с которым она еще пересекает эту линию s. Мы имеем $sz=z^2+2xz$. Но $(x^2+y^2)z=1$ для точек на s, и, следовательно, $x^2z<1$, т. е. $|xz|$ при увеличивающемся x уменьшается. Итак (это нам будет дальше важно) *при растущем* x z и $|sz|$ *уменьшаются* (*).

Пусть $s>0$. В таком случае самое малое q, при данном s, которое еще дает поверхность q, пересекающую линию s, есть то, для которого последнего удовлетворяется неравенство $s+z<2\sqrt{q+z^2}$.

α) пусть $s=2\sigma-1$ (где $\sigma>0$), т. е. нечетное. Тогда искомое $q=\sigma^2-\sigma+1$, так как $2\sqrt{\sigma^2-\sigma+1-1+z^2}<2\sigma-1+z<2\sqrt{\sigma^2-\sigma+1+z^2}$. Эти неравенства равносильны $0<4\sigma z-2z-3z^2<4$; правое при больших x следует из (*), левое равносильно $0<4\sigma-2-3z$ и следует тоже из (*).

β) Пусть $s=2\sigma$ (где $\sigma>0$), т. е. четное. Тогда искомое $q=\sigma^2+1$, так как $2\sqrt{\sigma^2+z^2}<2\sigma+z<2\sqrt{\sigma^2+1+z^2}$. Эти неравенства равносильны $0<4\sigma z-3z^2<4$. Правое при больших x следует из (*), левое равносильно $0<4\sigma-3z$ и следует тоже из (*).

Пусть $s<0$. В таком случае самое малое q при данном s, которое еще дает поверхность q, пересекающую линию s, есть то, для которого последнего удовлетворяется неравенство $-2\sqrt{q+z^2}<s+z$.

γ) *Пусть* $s=-2\sigma+1$ (где $\sigma>0$), т. е. нечетное. Тогда искомое $q=\sigma^2-\sigma$, так как $2\sqrt{\sigma^2-\sigma+z^2}<2\sigma-1-z<2\sqrt{\sigma^2-\sigma+1+z^2}$. Эти неравенства равносильны $0<1-4\sigma z+2z-3z^2<4+4z^2$, и как правое, так и левое следуют из (*).

б) *Пусть* $s=-2\sigma$ (где $\sigma>0$), т. е. четное. Тогда искомое $q=\sigma^2-1$, так как $2\sqrt{\sigma^2-1}+z^2<2\sigma-z<2\sqrt{\sigma^2+z^2}$. Эти неравенства равносильны $0<4\sigma z-3z^2<4$; правое следует из (*), левое равносильно $0<4\sigma-3z$ и также следует из (*).

В результате всего сказанного мы имеем следующее. На кривой s точка с наименьшим дискриминантом

при $s=-2\sigma$; $s=-2\sigma+1$; $s=2\sigma+1$; $s=2\sigma$ $(\sigma>0)$
имеет $q=\sigma^2-1$; $q=\sigma^2-\sigma$; $q=\sigma^2-\sigma+1$; $q=\sigma^2+1$.

D этих точек получается, таким образом, в виде одного из 4-х вполне определенных полиномов 4-й степени от σ, которые при увеличении σ (как и любой полином) увеличиваются сверх всякого предела, и, следовательно, есть только ограниченное число таких σ, а следовательно, и таких s, на которых есть точки с $|D|<L$.

Из доказательства этой теоремы для $D<0$ следует сейчас же ее доказательство для $D>0$, так как, как легко видеть,

$$q=\sigma^2-2;\quad q=\sigma^2-\sigma-1;\quad q=\sigma^2-\sigma;\quad q=\sigma^2,$$

т. е. на 1 меньшие q дают как раз единицы $W_{3,0}$ с наименьшими дискриминантами для соответственных s, и опять получается 4 (уже других, конечно) полинома 4-й степени от σ, выражающих эти дискриминанты.

В. ТАБУЛЯРИЗАЦИЯ ПОЛЕЙ 4-й СТЕПЕНИ

В этом и следующих параграфах мы рассматриваем вопрос табуляризации всех неприводимых колец O, состоящих из целых точек 4-й степени, содержащих точку 1, а тем самым и табуляризацию полей 4-й степени. Сверх чисто тривиальных усложнений, получающихся просто вследствие увеличения числа измерений, тут появляется еще одна привходящая трудность — проекция параллельно рациональному направлению, не лежащая в начале, тем не менее может быть проекцией не примитивной точки кольца, а именно может случиться, что это проекция квадратичной точки кольца. Для того чтобы обойти эту трудность, мы проектируем кроме того 2-мерными лучами параллельно биссектрисам, в которых лежат квадратичные точки. Мы даем в этих параграфах табуляризацию колец (и полей) 4-й степени, так как во второй части этой главы рассматриваем классификацию кубических полей по квадратичным и полей 4-й степени по кубическим. Обе эти классификации идейно тесно связаны между собою.

§ 37. Система W и ее сетки $\overline{W}_0$, $\overline{W}_1$, $\overline{W}_2$ для $n=4$, $\tau=0$

Будем писать уравнение 4-й степени в форме

$$x^4-sx^3+px^2-qx+n=0. \tag{1}$$

Как известно, условиями вещественности корней такого уравнения являются неравенства:

$$p-\frac{3}{8}s^2<0, \tag{2}$$

$$p^2-s^2p+\frac{3}{16}s^4+sq-4n<0, \tag{3}$$

и дискриминант уравнения положителен, т. е.

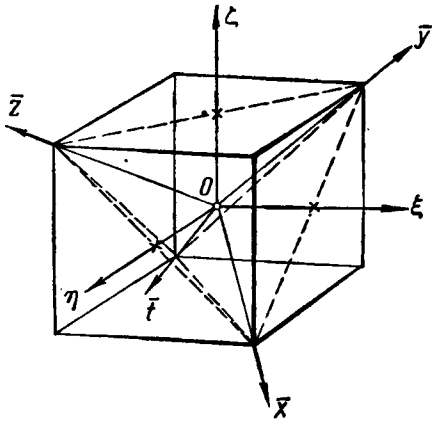
$$27D=4(p^2-3sq+12n)^3-(2p^3-72pn+27s^2n-9spq+27q^2)^2>0. \tag{4}$$

Это и будут условия того, что число τ пар комплексно сопряженных корней уравнения 4-й степени равно нулю.

Будем обозначать координаты точек соответствующего этому случаю вещественного 4-мерного сигнатурного пространства $R_{4,0}$ через x, y, z, t. Система точек W в этом случае определяется системой уравнений

$$\left.\begin{array}{c} x+y+z+t=s, \\ xy+xz+xt+yz+yt+zt=p, \\ xyz+xyt+xzt+yzt=q, \\ xyzt=n, \end{array}\right\} \qquad (5)$$

где s, p, q, n — все возможные целые рациональные числа, удовлетворяющие условиям (2), (3), (4). Условие вещественности всех четырех корней уравнения (1), очевидно, равносильно тому, что целые рациональные числа s, p, q, n таковы, что поверхности (5) пересекаются, т. е. имеют хоть одну общую им всем четырем точку.



Черт. 7.

Всякой точке W соответствует одно вполне определенное уравнение (1), а одному уравнению (1) соответствуют 24 точки W, в соответствии с возможностью различно нумеровать его корни.

Поверхности s суть 3-мерные „плоскости“, делающие одинаковые отрезки на осях координат. Преобразованием $x=x_1+k$, где k — целое рациональное число, можно преобразовать уравнение (1) в другое уравнение, опять с целыми рациональными коэффициентами и старшим коэффициентом 1, у которого след, т. е. коэффициент s, равен 0, 1, 2 или 3. Такое преобразование переносит точку, соответствующую уравнению, параллельно рациональному направлению $x=y=z=t$ на „плоскость“

$$x+y+z+t=s$$

(где $s=0$, 1, 2 или 3).

Обозначим через $\overline{W}_0$, $\overline{W}_1$, $\overline{W}_2$, $\overline{W}_3$ трехмерные системы точек W, лежащих в „плоскостях“ $s=0$, 1, 2, 3. Из сказанного ясно, что вся система W состоит из периодически повторяющихся систем, получающихся из $\overline{W}_0$, $\overline{W}_1$, $\overline{W}_2$, $\overline{W}_3$ путем параллельных переносов этих систем параллельно рациональному направлению на векторы (1,1,1,1), (2, 2, 2, 2), ... Заметим еще, что система $\overline{W}_3$ получается из системы $\overline{W}_{-1}$, симметричной с системой $\overline{W}_1$ по отношению к началу координат, переносом ее на вектор (1, 1, 1, 1). В силу того, что любое кольцо O само симметрично относительно начала, систему $\overline{W}_3$ можно в дальнейшем не рассматривать и ограничиться лишь системами $\overline{W}_0$, $\overline{W}_1$, $\overline{W}_2$.

Очевидно, что оси координат X, Y, Z, T при проектировании параллельно рациональному направлению на „плоскость“ $s=0$ нулевого следа, вследствие симметрии этого направления с осями координат, дадут в проекции прямые $\overline{X}$, $\overline{Y}$, $\overline{Z}$, $\overline{T}$, лежащие в этой „плоскости“ (3-мерном пространстве), которые исходят из начала и делают одинаковые углы между собою. Отметим от начала координат на этих прямых равные отрезки. Тогда концы этих отрезков образуют правильный тетраэдр. Построим куб, для которого вершины этого тетраэдра будут четырьмя из его вершин, и выберем в „плоскости“ $s=0$ прямые ξ, η, ζ, исходящие из начала координат, т. е. центра этого куба, и идущие параллельно ребрам этого куба, за оси координат. Не трудно видеть, что между координатами x, y, z, t какой-либо точки в нашем четырехмерном

пространстве и координатами ξ, η, ζ ее проекции параллельно рациональному направлению на „плоскость“ $s=0$ существуют следующие соотношения:

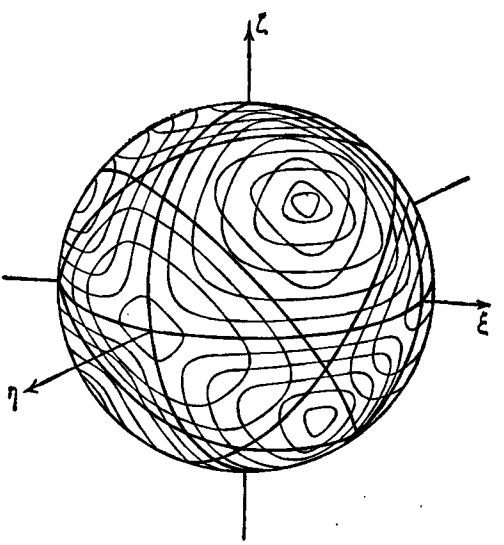
$$\left.\begin{aligned} x+y+z+t&=s\ ; & x&=\frac{2\xi+2\eta-2\zeta+s}{4};\\ x+y-z-t&=2\xi; & y&=\frac{2\xi-2\eta+2\zeta+s}{4};\\ x-y+z-t&=2\eta; & z&=\frac{-2\xi+2\eta+2\zeta+s}{4};\\ -x+y-z+t&=2\zeta; & t&=\frac{-2\xi-2\eta-2\zeta+s}{4}. \end{aligned}\right\} \quad (6)$$

Если теперь в уравнениях (5) замеиить x, y, z, t их выражениями через ξ, η, ζ из (6), то мы получим уравнения проекций на „плоскость“ $s=0$ пересечения каждой из этих поверхностей с „плоскостью“ s. Уравнения проекций сечений, образуемых поверхностями p с „плоскостью“ s, будут иметь вид:

$$\xi^2+\eta^2+\zeta^2=\frac{3s^2}{4}-2p, \quad (7)$$

т. е. это будут шары. Каждый такой шар делится плоскостями координат $XYZT$ на 14 сферических многоугольников, 8 из которых будут четырехугольниками, а 6 — треугольными (черт. 8). Для проекций сечений поверхностей q с „плоскостью“ s аналогично мы получаем уравнения

$$\xi\eta\zeta=-\frac{s^3+4sp}{8}+q. \quad (8)$$



Черт. 8.

Эти поверхности пересекают каждый из шаров p внутри каждого октанта осей ξ, η, ζ, как показано на черт. 8. Наконец, сечения поверхностей $n=xyzt$ „плоскостями“ s, как это видно непосредственно в координатах x, y, z, t, дают в проекции поверхности, пересекающие те же шары внутри каждого из упомянутых 14 сферических многоугольников, как это показано на черт. 8. В случае чисто вещественных полей четырех измерений каждая из фигур, данных нами в конце книги для $s=0$ и $s=1$ для случая трех измерений, заменяется рядом таких шаров, которые, собственно говоря, надо мыслить концентрическими друг другу (но если бы их все нарисовать один в другом, то картина очень бы запуталась).

§ 38. Выключение приводимых точек

В случае 4-мерной W_4 точка ее может быть приводима либо потому, что она есть сумма точки W_1, лежащей на одной из осей, и точки W_3, лежащей в 3-мерном пространстве, определяемом остающимися тремя осями, либо же точка приводима потому, что она есть сумма точки W_2, лежащей в плоскости, определяемой одною из пар осей, и точки W_2, лежащей в плоскости, определяемой другою парою осей. Если W_4 имеет $\tau=0$, то система W_1, в случае приводимых точек вида W_1+W_3, может лежать на любой из осей системы W_2,

в случае приводимых точек вида W_2+W_2, могут лежать на плоскостях, определяемых любою парою осей, причем обе системы W_2 имеют $\tau=0$. Если же W_4 имеет $\tau=1$, то система W_1 может лежать только на одной из двух осей, соответствующих вещественным корням, а из систем W_2 и W_2' первая W_2 имеет $\tau=0$ и лежит в плоскости, соответствующей вещественным корням, а другая W_2' имеет $\tau=1$ и лежит в плоскости, соответствующей паре комплексно сопряженных корней. Наконец, если W_4 имеет $\tau=2$, то приводимых точек вида W_1+W_3 быть не может, а могут быть только приводимые точки вида $W_2'+W_2'$, причем каждая из систем W_2' имеет $\tau=1$ и лежит в плоскости, соответствующей паре комплексно сопряженных корней.

Случай $\tau=0$. Приводимые точки $W_{4,0}$ вида $W_{1,0}+W_{3,0}$ лежат на 4 системах плоскостей, параллельных асимптотическим плоскостям поверхностей n 4-го порядка, причем одной из плоскостей каждой из этих 4 систем является сама соответственная асимптотическая плоскость. Совокупность этих 4 систем плоскостей образует разбиение 3-мерного пространства „плоскости“ $s=0$ (и аналогично $s=1$ и $s=2$) на правильные тетраэдры. В каждой из этих систем периодически (через каждые 3 плоскости) повторяются сетки, лишь аффинно отличающиеся от сеток $\overline{W}_3$. Приводимые точки $W_{4,0}$ вида $W_{2,0}+W_{2,0}$ лежат на 4 системах плоскостей, параллельных асимптотическим плоскостям поверхностей q 3-го порядка, причем одной из плоскостей каждой из этих 3 систем является сама соответственная асимптотическая плоскость. Совокупность этих 3 систем плоскостей образует разбиение 3-мерного пространства „плоскости“ $s=0$ (и аналогично $s=1$ и $s=2$) на кубы. В каждой из этих систем периодически (через каждые 2 плоскости) повторяются сетки, лишь аффинно отличающиеся от сеток $\overline{W}_2$.

Практически приводимые точки выключаются просто испытанием уравнения $x^4-3x^3+px^2-qx+n=0$ на приводимость, которая наступает (вида W_1+W_3), если уравнение это имеет рациональный корень, т. е. если один из целых рациональных делителей n есть его корень (вида W_2+W_2), если

$$x^4-sx^3+px^2-qx+n=(x^2+\alpha x+\beta)(x^2+\gamma x+\delta),$$

где α, β, γ, δ — целые рациональные. Но тогда $\beta\delta=n$, откуда для β и δ получается ограниченное число возможностей. Затем $\alpha\gamma+(\beta+\delta)=p$, откуда для α и γ имеется также, для каждой пары β и δ, лишь конечное число возможностей, и, наконец, $\alpha+\gamma=-s$.

§ 39. Ограничение коэффициентов p, q, n

Зададимся некоторым числом L и будем искать все максимальные неприводимые кольца O целых точек 4-го порядка, дискриминанты которых по абсолютной величине не больше L.

Случай $\tau=0$. Выше были выписаны условия вещественности всех 4 корней ρ, ρ', ρ'', ρ''' уравнения $x^4-sx^3+px^2-qx+n=0$. То, что $D_O\leqslant L$, геометрически обозначает, что объемы V_O основных параллелепипедов в $R_{4,0}$ искомых $O\leqslant\sqrt{L}$.

В виду того, что объем $\overline{V}_O$ основного параллелепипеда той решетки $\overline{O}$, которая получается проектированием O параллельно рациональному направлению, т. е. вектору $\overrightarrow{0\,1}$ на „плоскость“ s, равен $\frac{1}{2}V_O$, где V_O — объем основного параллелепипеда O, мы получаем, что $\overline{V}_O\leqslant\frac{1}{2}\sqrt{L}$. Нам необходимо уловить в проекции по крайней мере по одной неприводимой точке каждой из таких O,

имеющих $V_O \leqslant \sqrt{L}$. Для этого опишем в „плоскости" $s=0$ из начала координат такой 3-мерный шар, чтобы внутри него или на его поверхности оказалось по крайней мере по одной точке, являющейся проекцией нерациональной точки каждого из таких O. Для этого необходимо и достаточно, чтобы радиус этого шара был не меньше наименьшего из векторов $\overline{O}$.

Таким образом, вопрос сводится к нахождению maximum'a длины наименьшего вектора решетки при заданном объеме $\overline{V}$ ее основного параллелепипеда. Из плотнейшего расположения одинаковых шариков по правильным тетраэдрам следует, что maximum длины такого вектора

$$l \leqslant \sqrt[6]{2\overline{V}^2}$$

(см. мемуары Коркина и Золотарева или, например, Б. Делоне. Труды Матем. ин-та Академии Наук им. Стеклова, т. IV). В нашем случае $\overline{V} \leqslant \frac{\sqrt{L}}{2}$, поэтому радиус такого шара

$$r \leqslant \sqrt[6]{\frac{L}{2}}. \tag{1}$$

Итак, в каждом O, дискриминант которого $\leqslant L$, имеются точки, отличающиеся от рациональных, лежащие в „плоскостях" $s=0$, 1 или 2, проекции которых параллельно рациональному направлению на плоскость $s=0$ попадают в шар такого радиуса или на его поверхность. Остается посмотреть, как ограничены p, q, n уравнений этих точек, и тогда можно будет выписать таблицу уравнений, являющихся представителями этих колец O. Из формулы (7) мы непосредственно получаем ограничения для p

$$\left|\frac{3s^2}{4} - 2p\right| \leqslant \sqrt[3]{\frac{L}{2}}. \quad (s=0,\ 1,\ 2) \tag{2}$$

Таким образом, выделяется ограниченное число шаров p для каждого из $s=0$, 1, 2, на которых надо искать интересующие нас точки, являющиеся представителями колец O с дискриминантами $\leqslant L$. Теперь надо посмотреть, какую сетку линий (расчертку) образуют поверхности q и n на каждом из этих шаров (s, p), чтобы найти ограничение для величины q, в зависимости от s, p, и затем для каждого n, в зависимости от s, p, q. Для ограничения q надо найти, какая последняя поверхность $\xi\eta\zeta = -\frac{s^3+4sp}{8} + q$ еще имеет общие точки с шаром (s, p), т. е. пересекается с прямою $\xi=\eta=\zeta$ еще не вне этого шара. Мы получаем:

$$|q| \leqslant \left|\frac{r\sqrt[3]{3}}{27} - \frac{s^3+4sp}{8}\right|. \quad (s=0,\ 1,\ 2) \tag{3}$$

Аналогично, рассматривая сетку линий (черт. 8), мы видим, что для ограничения n надо будет рассмотреть, какие последние поверхности n еще пересекают либо одну из осей ξ, η, ζ, либо прямую $\xi=\eta=\zeta$ не вне шара. В первом случае мы получим

$$|n| \leqslant \left|\frac{3sq-p^2}{12}\right|, \quad (s=0,\ 1,\ 2) \tag{4}$$

а во втором

$$|n| \leqslant \left(\frac{s^2-4r^2}{16}\right)^2. \quad (s=0,\ 1,\ 2) \tag{4'}$$

Таким образом, получается таблица уравнений, среди которых заключается хотя бы по одному уравнению, соответствующему каждому из колец O, дискриминант которого $\leqslant L$, для $\tau = 0$.

Этот способ шара представляет для $\tau = 0$ то преимущество над способом параллелепипеда, примененным в доказательстве теоремы Эрмита (стр. 25), что сами поверхности (s, p) представляют собою шары, и таким образом используется вся симметрия, присущая сетке W в этом случае.

Заметим, между прочим, что если бы тщательно вычертить расчертки шаров, подобно тому, как это было сделано на черт. 8, то, имея ограничения для номера шара, мы могли бы всю остальную таблицу прямо прочесть по этой расчертке, не прибегая к вычислениям.

Все O, пойманные так при помощи их неприводимых точек, найдены в том смысле, что, исходя от каждой такой точки ρ, можно получить кольцо со степенным базисом $[1, \rho, \rho^2, \rho^3]$ и затем способом, аналогичным тому, который был применен при вычислении базиса по Вороному, можно найти все кольца O, центрирующие это кольцо, и, в частности, максимальное кольцо, его центрирующее. Надо будет вовсе отбросить это ρ, если дискриминант даже этого максимального кольца будет больше L.

Если из неприводимого кольца O поймана приводимая его точка, то точка эта только и может быть типа $W_2 + W_2$, так как уравнение, соответствующее точке неприводимого кольца O, либо неприводимо, либо есть квадрат неприводимого уравнения 2-й степени, либо есть 4-я степень уравнения 1-й степени; но в последнем случае проекция соответствующей точки на „плоскости“ $s = 0$ лежала бы в начале координат, и, следовательно, возможны только два первых случая. Таким образом, если пойманная точка неприводимого кольца приводима, то она — типа $W_2 + W_2$. Мы видим, следовательно, что все точки рассматриваемых расчерток шаров (s, p), уравнения которых приводимы и не суть квадраты неприводимых уравнений 2-й степени, надо просто отбросить. Если пойманная точка кольца O типа $W_2 + W_2$, то само кольцо еще не поймано, так как остается еще найти квадратное уравнение с коэффициентами из квадратичного поля, определяемого неприводимым множителем этого уравнения, которое неприводимо и даст точку ρ системы W_4, содержащуюся в неприводимом кольце O, дискриминант которого $\leqslant L$. Но это сделать не так просто.

Для поимки безусловно всех неприводимых колец O, дискриминанты которых $\leqslant L$, и, в частности, нужных нам максимальных неприводимых колец необходимо будет проектировать эти кольца не параллельно рациональному направлению, а 2-мерными лучами параллельно их квадратичным подкольцам, что мы сейчас и сделаем.

§ 40. Проектирование параллельно квадратичному подполю и ограничение коэффициентов α_1 и α_2

Из сказанного в гл. I, § 3, ясно, что поля 4-го порядка могут иметь в качестве своих подполей (кроме рационального) только подполя 2-го порядка и что подполей 2-го порядка у данного поля 4-го порядка не может быть больше трех, так как 2-мерных „биссектрис“ 4-мерных осей только три.

Покажем, что если этих подполей два, то есть и вполне определенное третье. Действительно, пусть, например, две из „биссектрис“ 1 и 2 заняты квадратичными подполями рассматриваемого поля 4-го порядка. Вследствие симметрии системы целых точек вещественного квадратичного поля относительно рациональной прямой, следует, что в нем есть целые точки, координаты которых равны по абсолютной величине и обратны по знаку. Следовательно, в первой „биссектрисе“ имеется целая точка вида $(a, a, -a, -a)$ и во второй „биссектрисе“ — целая точка вида $(b, -b, b, -b)$. Произведение $(ab, -ab,$

$-ab$; ab) есть тоже целая точка системы целых точек рассматриваемого поля 4-го порядка; она лежит в 3-й „биссектрисе" и не лежит на рациональной прямой, а следовательно, и в 3-й „биссектрисе" лежит квадратичное подполе.

Следующие примеры показывают, что все три возможности, а именно, что чисто вещественное поле 4-го порядка вовсе не имеет квадратичных подполей, что оно имеет лишь одно и что оно имеет 3 квадратичных подполя, осуществляются:

1. Поле 4-го порядка с дискриминаитом 1957 не имеет квадратичных подполей.

2. Поле 4-го порядка с дискриминантом 725 имеет одно квадратичное подполе (с дискриминантом 5).

3. Поле 4-го порядка с дискриминантом 1 600 имеет три квадратичных подполя (с дискриминантами 5, 8 и 40).

Рассмотрим прежде всего ограничение для тех квадратичных подколец $\underline{O}$, содержащих 1, которые дают при проектировании соответственного надкольца O 4-го порядка параллельно рациональному направлению на „плоскость" $s=0$ точки внутри или на границе шара радиуса $r=\sqrt[6]{\frac{L}{2}}$. В виду того, что проектирование происходит параллельно рациональному направлению, т. е. вектору $\overrightarrow{0\,1}$, который можно принять за одну из сторон основного параллелограмма подрешетки $\underline{O}$, длина проекции второй стороны этого параллелограмма будет равна площади этого параллелограмма, деленной на длину вектора $\overrightarrow{0\,1}$, которая равна 2. Сам же этот параллелограмм линейно в $\sqrt{2}$ раз больше основного параллелограмма квадратичного кольца $\underline{O}$, рассматриваемого в его собственном 2-мерном пространстве. Пусть площадь этого параллелограмма есть S. Тогда $S=\sqrt{d}$, где d — дискриминант этого квадратичного кольца, и, следовательно, площадь основного параллелограмма подкольца $\underline{O}$ равна $2\sqrt{d}$, т. е. проекция второй стороны параллелограмма равна $\frac{2\sqrt{d}}{2}=\sqrt{d}$. Но она должна быть $\leqslant\sqrt[6]{\frac{L}{2}}$, откуда мы получаем, что дискриминанты тех квадратичных колец, которые нас здесь интересуют, не превосходят $\sqrt[6]{\frac{L}{2}}$.

Перейдем теперь к проектированию колец 4-го порядка O параллельно квадратичным „биссектрисам". Для того чтобы найти те кольца O 4-го порядка, которые имеют рассмотренные сейчас квадратичные кольца своими подкольцами, надо для каждого из этих подколец спроектировать 2-мерными лучами, параллельными плоскости „биссектрисы" P, в которой это кольцо лежит, все построенные над ним надкольца O 4-го порядка на плоскость Q, ортогональную плоскости P.

Можно предполагать, не нарушая общности, что „биссектриса" эта

$$\left.\begin{aligned} x&=y,\\ z&=t. \end{aligned}\right\}$$

Тогда ортогональной ей плоскостью будет

$$\left.\begin{aligned} x+y&=0,\\ z+t&=0. \end{aligned}\right\}$$

Рассмотрим те квадратные уравнения, которым удовлетворяют точки тех O 4-го порядка, для которых квадратичное кольцо O, рассматриваемое в 4-мер-

ном пространстве $R_{4,0}$, является подкольцом, с коэффициентами, принадлежащими квадратичному полю, соответствующему O:

$$\omega^2+\alpha_1\omega+\alpha_2=0,\ \text{имеющее своими корнями}\ \omega\omega'$$

и

$$\omega^2+\alpha_1'\omega+\alpha_2'=0,\ \text{имеющее своими кориями}\ \omega_{,}\omega''',$$

где ω, ω', ω'', ω''' — координаты точки такого O. В таком случае α_1', квадратично сопряженное с α_1 и α_2', квадратично сопряжено с α_2.

Рассмотрим сиачала сетку (Q_a), образуемую (двухмерной) плоскостью

$$x+y=-\alpha_1,\quad z+t=-\alpha_1',$$

перпендикулярной к двухмерной „биссектрисе“ P, в которой лежит O, в пересечении с поверхностями 2-го порядка α_2.

Эта сетка задается системамн уравнений

$$\left.\begin{aligned}x+y&=-\alpha_1,\\ z+t&=-\alpha_1',\end{aligned}\right\}\qquad\left.\begin{aligned}xy&=\alpha_2,\\ zt&=\alpha_2'.\end{aligned}\right\}$$

Перегруппируем эти системы иначе:

$$\left.\begin{aligned}x+y&=-\alpha_1,\\ xy&=\alpha_2,\end{aligned}\right\}\qquad\left.\begin{aligned}z+t&=-\alpha_1',\\ zt&=\alpha_2'.\end{aligned}\right\}$$

Совокупность этих систем эквивалентна предыдущей. Их можно написать иначе:

$$x=-\frac{\alpha_1}{2}+\sqrt{\frac{\alpha_1^2}{4}-\alpha_2};\quad y=-\frac{\alpha_1}{2}-\sqrt{\frac{\alpha_1^2}{4}-\alpha_2};$$

$$z=-\frac{\alpha_1'}{2}+\sqrt{\frac{\alpha_1'^2}{4}-\alpha_2'};\quad t=-\frac{\alpha_1'}{2}-\sqrt{\frac{\alpha_1'^2}{4}-\alpha_2'}.$$

Примем $\xi=\frac{x-y}{2}$; $\eta=\frac{z-t}{2}$ и возьмем в плоскости Q за координатные оси ξ, η:

$$(\xi)\quad\left.\begin{aligned}x+y&=-\alpha_1,\\ z+t&=-\alpha_1,\\ z-t&=0,\end{aligned}\right\}\qquad(\eta)\quad\left.\begin{aligned}x+y&=-\alpha_1,\\ z+t&=-\alpha_1,\\ x-y&=0.\end{aligned}\right\}$$

Не трудно видеть, что эти оси ортогональны.

Тогда $\xi^2=\frac{\alpha_1^2}{4}-\alpha_2$, $\eta^2=\frac{\alpha_1'^2}{4}-\alpha_2'$, и, следовательно, при заданном α_1 всякой точке α_2 кольца O будет соответствовать вполне определенная точка ξ, η, и сетка (Q_a) определяется системой:

$$\left.\begin{aligned}\xi^2+\eta^2&=\frac{\alpha_1^2+\alpha_1'^2}{4}-(\alpha_2+\alpha_2'),\\ \xi^2-\eta^2&=\frac{\alpha_1^2-\alpha_1'^2}{4}-(\alpha_2-\alpha_2').\end{aligned}\right\}$$

Сетки (Q_α) достаточно найти для $\alpha_1 = 0,\ 1,\ \omega_1,\ 1+\omega_1$, где $1,\ \omega_1$ — базис кольца $\underline{O}$. Действительно, уравнение

$$\omega^2 + \alpha_1\omega + \alpha_2 = 0$$

подстановкой $\omega = \omega - \alpha$ преобразуется в

$$\bar{\omega}^2 - (\alpha_1 - 2\alpha)\,\bar{\omega} + (\alpha^2 - \alpha\alpha_1 - \alpha_2) = 0,$$

или, положив

$$\alpha = a + b\omega_1; \quad \alpha_1 = a_1 + b_1\omega_1,$$

мы получим

$$\bar{\omega}^2 - (a_1 + b_1\omega_1 - 2a - 2b\omega_1)\,\bar{\omega} + (a + b\omega_1)^2 - (a + b\omega_1)(a_1 + b_1\omega_1) - \alpha_2 = 0.$$

Очевидно, можно подобрать такие целые a и b, чтобы коэффициент при $\bar{\omega}$ был равен одному из значений $0,\ 1,\ \omega_1,\ 1+\omega_1$. Обозначим

$$\begin{aligned} a_1 + b_1\omega_1 - 2a - 2b\omega_1 &= \bar{a}_1 = \bar{a} + \bar{b}\omega_1, \\ (a + b\omega_1)^2 - (a + b\omega_1)(a_1 + b_1\omega_1) - \alpha_2 &= \bar{\alpha}_2 = u + v\omega_1. \end{aligned}$$

Мы получим

$$\omega^2 + (\bar{a} + \bar{b}\omega_1)\,\omega + (u + v\omega_1) = 0$$

и для сетки (Q_α) систему

$$\xi^2 + \eta^2 = \frac{\bar{a}_1^2 + \bar{a}_1'^2}{4} - (\bar{\alpha}_2 + \bar{\alpha}_2'),$$

$$\xi^2 - \eta^2 = \frac{\bar{a}_1^2 - \bar{a}_1'^2}{4} - (\bar{\alpha}_2 - \bar{\alpha}_2').$$

Нам нужно в проекции на плоскость Q уловить хоть по одной целой точке из всех чисто вещественных O 4-го порядка, дискриминанты которых $\leqslant L$ и которые имеют при этом данное $\underline{O}$ 2-го порядка своим подкольцом. Для этого в плоскости Q опишем из начала окружность такого радиуса, чтобы внутри ее или на ее границе оказалось по крайней мере по одной точке, являющейся проекцией параллельно P примитивной точки каждого из указанных колец O. Для этого достаточно, чтобы радиус такой окружности был не меньше наименьшего вектора каждой из 2-мерных решеток, получающихся от такого проектирования каждого из этих O на плоскости Q. Основной параллелограмм каждой из рассматриваемых решеток имеет площадь $S \leqslant \frac{\sqrt{L}}{2\sqrt{d}}$, так как объем 4-мерного параллелепипеда O, который $\leqslant \sqrt{L}$, равен, очевидно, произведению площади проекции S на площадь $2\sqrt{d}$ решетки $\underline{O}$. Дело в том, что вообще, когда мы проектируем n-мерную вещественную решетку параллельно какой-нибудь ее m-мерной подрешетке на линейное $n-m$-мерное пространство, дополнительное ее собственному m-мерному подпространству и ему ортогональное, то объем основного параллелепипеда n-мерной решетки равен произведению объемов осиовных параллелепипедов рассматриваемой m-мерной подрешетки и ее $n-m$-мерной проекции. Вопрос сводится, таким образом, к нахождению максимума длины l наименьшего вектора двухмерной решетки при заданной площади S ее основного параллелограмма. Из плотнейшего расположения кружочков по равносторонним треугольникам мы получаем $\frac{l^2\sqrt{3}}{4} \leqslant \frac{S}{2} \leqslant \frac{\sqrt{L}}{4\sqrt{d}}$ и, следовательно, $l^4 \leqslant \frac{L}{3d}$.

Пусть $\bar{a}_1$, $\bar{a}_2$ определяют точку M сетки (P_a), проекция которой $\bar{M}$ на плоскости P есть ближайшая к началу точка решетки, получаемой при проектировании Q. Тогда $O\bar{M}^2 = \frac{\bar{a}_1^2 + \bar{a}_1'^2}{2} - 2(\bar{a}_2 + \bar{a}_2')$, и, следовательно, для получения в проекции на плоскость P хоть по одной целой точке интересующих нас областей достаточно рассмотреть такие a_1, a_2, для которых

$$\frac{\bar{a}_1^2 + \bar{a}_1'^2}{2} - 2(\bar{a}_2 + \bar{a}_2') \leqslant \sqrt{\frac{L}{3d}},$$

и таким образом в сетке (Q_a) достаточно построить окружности ξ, η, радиус которых не превышает $\frac{1}{2}\sqrt{\frac{L}{3d}}$, и гиперболы, вещественная полуось которых не превосходит радиуса наибольшей из окружностей сетки.

Таким образом, имеем:

$$0 < \frac{\bar{a}_1^2 + \bar{a}_1'^2}{4} - (\bar{a}_2 + \bar{a}_2') \leqslant \frac{1}{2}\sqrt{\frac{L}{3d}},$$

$$\left| \frac{a_1^2 - \bar{a}_1'^2}{4} - (\bar{a}_2 - \bar{a}_2') \right| \leqslant \frac{1}{2}\sqrt{\frac{L}{3d}},$$

или

$$0 < \frac{2\bar{a}^2 + 2\bar{a}\bar{b}(\omega_1 + \omega_1') + \bar{b}^2(\omega_1^2 + \omega_1'^2)}{4} - 2u - v(\omega_1 + \omega_1') \leqslant \frac{1}{2}\sqrt{\frac{L}{3d}},$$

$$\left| \frac{2\bar{a}\bar{b}(\omega_1 - \omega_1') + \bar{b}^2(\omega_1^2 - \omega_1'^2)}{4} - v(\omega_1 - \omega_1') \right| \leqslant \frac{1}{2}\sqrt{\frac{L}{3d}}.$$

Рассмотрим отдельно два случая:

1. *Дискриминант квадратичного поля* $d \equiv 0 \pmod 4$.

В этом случае $\omega_1 = \frac{1}{2}\sqrt{d}$; $\omega_1' = -\frac{1}{2}\sqrt{d}$, и система (Q_a) принимает вид:

$$\xi^2 + \eta^2 = \frac{4\bar{a}^2 + \bar{b}^2 d}{8} - 2u,$$

$$\xi^2 - \eta^2 = \frac{\bar{a}\bar{b}\sqrt{d}}{2} - v\sqrt{d},$$

и, следовательно, при данных $\bar{a}$, $\bar{b}$, $\bar{d}$ достаточно брать u и v такие, чтобы:

$$0 < \frac{4\bar{a}^2 + \bar{b}^2 d}{4} - 4u \leqslant \sqrt{\frac{L}{3d}}, \tag{1}$$

$$|\bar{a}\bar{b} - 2v| \leqslant \sqrt{\frac{L}{3d}}. \tag{2}$$

2. *Дискриминант квадратичного поля* $d \equiv 1 \pmod 4$. В этом случае $\omega_1 = \frac{1+\sqrt{d}}{2}$; $\omega_1' = \frac{1-\sqrt{d}}{2}$ и система (Q_a) имеет вид:

$$\left.\begin{aligned} \xi^2 + \eta^2 &= \frac{2\bar{a}^2 + 2\bar{a}\bar{b} + \bar{b}^2(1+d)}{4} - 2u - v, \\ \xi^2 - \eta^2 &= \left(\frac{2\bar{a}\bar{b} + \bar{b}^2}{4} - v\right)\sqrt{d}. \end{aligned}\right\}$$

Таким образом, для u и v получаются следующие ограничения:

$$0 < \frac{2\bar{a}^2 + 2\bar{a}\,\bar{b} + \bar{b}^2(1+d)}{2} - 4u - 2v \leqslant \sqrt{\frac{L}{3d}}, \tag{1'}$$

$$\left| \frac{2\bar{a}\,\bar{b} + \bar{b}^2}{2} - 2v \right| \leqslant \sqrt{\frac{L}{3d}}. \tag{2'}$$

Коэффициентам $\bar{a}$, $\bar{b}$, как было уже показано, достаточно придать лишь одну из следующих пар значений: 0, 0; 0, 1; 1, 0; 1, 1. При каждой паре этих значений при данном d по приведенным формулам ограничиваются u и v.

Легко видеть, что, спроектировав все максимальные кольца O, имеющие квадратичные подкольца параллельно квадратичной биссектрисе, на плоскость P, ей ортогональную, мы по наименьшим векторам полученной в проекции решетки восстановим не только интересующие нас максимальные кольца O 4-го порядка с одним квадратичным подкольцом, но также и те из них, которые имеют 3 таких подкольца. В самом деле, в проекции на плоскость P параллельно плоскости Q соответствующей биссектрисы мы получим либо проекцию неприводимой точки кольца O 4-го порядка, либо проекцию примитивной точки ω_2, принадлежащей другому квадратичному подкольцу. Если имеет место первое, то мы восстановим O по неприводимой ее точке ρ так же, как делали раньше. Если же имеет место второе, то по ω_1 и ω_2 мы составляем, как это было описано выше, примитивную точку ω_3 третьего квадратичного подкольца, и тогда 1, ω_1, ω_2, ω_3 лежат некомпланарно с началом, и, следовательно, по ним мы можем либо найти неприводимую точку ρ кольца O, либо непосредственно найти базис O.

§ 41. Таблица действий для получения всех чисто вещественных полей 4-го порядка, дискриминанты которых $< L$

Последовательность действий для вычисления таблицы таких полей, расположенных по их дискриминантам, следующая:

1) Ограничение p в зависимости от выбора L (L удобно брать вида $2\cdot\gamma^6$, чтобы r вышло целое рациональное) по формуле (2) § 39.

2) Ограничение q и n для каждого из этих p по формулам (3), (4) и (4') § 39. Эти вычисления надо произвести для $s = 0, 1, 2$. Таким образом, получатся три таблицы уравнений, лежащих в сфере r.

3) Исключение из этих таблиц всех приводимых уравнений.

4) Вычисление всех дискриминантов всех оставшихся уравнений.

5) Разложение на множители всех этих дискриминантов и отчеркивание всех тех, которые за выделением наибольшего квадратного множителя дают числа, бо́льшие L.

6) Нахождение базисов полей, определяемых оставшимися уравнениями.

Пусть ω_0, ω_1, ω_2, ω_3 образуют базис всех целых чисел поля 4-го порядка, образуемого корнем ρ уравнения $x^4 - sx^3 + px^2 - qx + n = 0$ (1). Как известно (см. § 14), за ω_0 можно принять число 1, а ω_1, ω_2, ω_3 искать в виде

$$\frac{\rho + c_2}{\Delta_1}, \quad \frac{\rho^2 + b_1\rho + c_1}{\Delta_2}, \quad \frac{\rho^3 + a\rho^2 + b\rho + c}{\Delta_3},$$

где a, b, b_1, c, c_1, c_2, Δ_1, Δ_2, Δ_3 — коэффициенты и знаменатели чисел базиса. Для вычисления этих коэффициентов и знаменателей преобразуем уравнение (1) § 37 по Чирнгаузену, приняв

$$y = \frac{u\rho^3 + v\rho^2 + w\rho + t}{\Delta},$$

$$y^4 + F_1y^3 + F_2y^2 + F_3y + F_4 = 0,$$

где

$$\Delta^4 \cdot F_4 = t^4 + At^3 + Bt^2 + Ct + D = \Phi(t),$$

$$\Delta^3 \cdot F_3 = \Phi'(t), \quad \Delta^2 \cdot F_2 = \frac{1}{2!}\Phi''(t), \quad \Delta \cdot F_1 = \frac{1}{3!}\Phi'''(t),$$

если положить

$$A = w \cdot s + v \cdot (s^2 - 2p) + u \cdot (s^3 - 3sp + 3q);$$

$$B = w^2 \cdot p + vw \cdot (sp - 3q) + uw \cdot (s^2 - 2p^2 - sq + 4n) + v^2 \cdot (p^2 - 2sq + 2n) + uv \cdot (sp^2 - 2s^2q - pq - 5sn) + u^2 \cdot (p^3 - 3spq + 3s^2n + 3q^2 - 3pn);$$

$$C = w^3 \cdot q + vw^2 \cdot (sq - 4n) + v^2w \cdot (pq - 3sn) + uw^2 \cdot (s^2q - 2pq - sn) + v^3 \cdot (q^2 - 2pn) + uvw \cdot (spq - 3s^2n - 3q^2 + 4pn) + uv^2 \cdot (sq^2 - 2spn - qn) + u^2w \cdot (p^2q - 2sq^2 + spq + 5qn) + u^2v \cdot (pq^2 - 2p^2n - sqn + 4n^2) + u^3 \cdot (q^3 - 3pqn + 3sn^2);$$

$$D = w^4 \cdot n + vw^2sn + uw^3 \cdot (s^2n - 2pn) + v^2w^2 \cdot pn + uvw^2(spn - 3qn) + v^3wqn + uv^2w \cdot (sqn - 4n^2) + u^2w^2 \cdot (p^2n - 2sqn + 2n^2) + u^2vw \cdot (pqn - 3sn^2) + u^3w \cdot (q^2n - 2pn^2) + v^4 \cdot n^2 + uv^3 \cdot sn^2 + u^2v^2pn^2 + u^3v \cdot qn^2 + u^4.$$

Придавая числам u, v, w, t, Δ значения, соответствующие отдельным числам базиса, и имея в виду, что коэффициенты уравнения относительно y должны быть целыми рациональными числами, легко получить все сравнения, необходимые для определения коэффициентов базиса. Когда базис поля, соответствующего рассматриваемому ρ, т. е. рассматриваемому уравнению, вычислен, мы получаем, что дискриминант D этого поля равен $D = \frac{D_\rho}{\Delta_1 \Delta_2 \Delta_3}$.

Все уравнения, для которых $D > L$, мы отбрасываем.

7) Аналогичные вычнсления надо проделать для полей, получаемых при помощи квадратичных подполей в соответствии с § 40, а именно, выписать все квадратичные поля, дискриминанты которых $< \sqrt[3]{\frac{L}{2}}$; для каждого из этих квадратичных полей найти для $\alpha_1 = 0$, 1, ω_1, $1 + \omega_1$ ограничения для u и v по формулам (1), (2) или (1'), (2') § 40; тогда получится еще таблица уравнений 4-й степени, с которыми надо проделать все то, что сказано в пуиктах 3, 4, 5 и 6.

В результате всего этого мы получим все чисто вещественные поля 4-го порядка, дискриминанты которых $< L$, причем каждое поле будет представлено своим базисом. Если для какого-нибудь дискриминанта D так получится несколько базисов, то надо еще посмотреть, не будут ли некоторые из этих базисов лишь разными базисами одного и того же поля, для чего надо для уравнений, определяющих соответственные ρ, решить задачу, обратную задаче Чирнгаузена. Для решения задачи, обратной задаче Чирнгаузена, для двух уравнеиий 4-й степени имеется способ Чеботарева [66], являющийся обобщением способа решения этой же задачи для двух уравнений 3-степени, изложенного в § 13, но этот способ ведет к большим вычислениям. В случае, когда все 4 корня уравнений 4-й степени вещественны, удобен способ, предложенный в работе Делоне [18], основанный на приведении безутиана. Но лучше всего пользоваться (во всех случаях) способом, предлагаемым Фаддеевым в § 49.

После разрешения этого вопроса о тождественности или различии получившихся полей 4-й степени таблица готова.

Так была вычислена И. Соминским и К. Биллевичем прилагаемая таблица чисто вещественных ($\tau = 0$) полей 4-й степени (см. [18]). Таблицы полей 4-й степени для двух других случаев, $\tau = 1$ и $\tau = 2$, были вычислены Ч. Поплавским для $\tau = 1$ и Д. К. Фаддеевым для $\tau = 2$ для тех полей, которые имеют квадратичные подполя.

ТАБЛИЦА ЧИСТО ВЕЩЕСТВЕННЫХ ПОЛЕЙ 4-го ПОРЯДКА, ДИСКРИМИНАНТЫ КОТОРЫХ НЕ ПРЕВЫШАЮТ 8112

(Таблица вычислена И. Соминским и К. Биллевичем)

Дискриминант поля	Коэффициенты у-ния $x^4 - sx^3 + px^2 - qx + n = 0$	Базис поля	Дискриминант подполя	Группа
725	s = 1, p = −3, q = −1, n = 1	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
1125	1, −4, −4, 1	$[1, \rho, \rho^2, \rho^3]$	5	Циклическая
1600	0, −6, 0, 4	$\left[1, \rho, \frac{\rho^2}{2}, \frac{\rho^3}{2}\right]$	5, 8, 40	Vierergruppe
1957	0, −4, −1, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
2000	0, −5, 0, 5	$[1, \rho, \rho^2, \rho^3]$	5	Циклическая
2048	0, −4, 0, 2	$[1, \rho, \rho^2, \rho^3]$	8	Циклическая
2225	1, −5, −2, 4	$\left[1, \rho, \rho^2, \frac{\rho^3+\rho^2+\rho^2}{2}\right]$	5	8-го порядка
2304	0, −4, 0, 1	$[1, \rho, \rho^2, \rho^3]$	8, 12, 24	Vierergruppe
2525	2, −4, −5, 5	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
2624	2, −3, −2, 1	$[1, \rho, \rho^2, \rho^3]$	8	8-го порядка
2777	1, −4, −1, 2	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
3600	2, −7, −8, 1	$\left[1, \rho, \rho^2, \frac{\rho^3+2\rho^2+\rho-3}{7}\right]$	5, 12, 60	Vierergruppe
3981	1, −4, −2, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
4205	1, −5, 1, 1	$[1, \rho, \rho^2, \rho^3]$	29	8-го порядка
4225	0, −9, 0, 4	$\left[1, \rho, \frac{\rho^2+\rho}{2}, \frac{\rho^3+\rho+2}{4}\right]$	5, 13, 65	Vierergruppe
4352	0, −6, −4, 2	$[1, \rho, \rho^2, \rho^3]$	8	8-го порядка
4400	0, −7, 0, 11	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
4525	1, −7, −3, 9	$\left[1, \rho, \rho^2, \frac{\rho^3-\rho^2-\rho}{3}\right]$	5	8-го порядка
4752	2, −3, −4, 1	$[1, \rho, \rho^2, \rho^3]$	12	8-го порядка
4913	1, −6, −1, 1	$\left[1, \rho, \rho^2, \frac{\rho^3+1}{2}\right]$	17	Циклическая
5125	2, −6, −7, 11	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
5225	1, −8, −1, 11	$\left[1, \rho, \rho^2, \frac{\rho^3+1}{2}\right]$	5	8-го порядка
5725	1, −8, −6, 11	$\left[1, \rho, \rho^2, \frac{\rho^3+\rho+1}{3}\right]$	5	8-го порядка
5744	0, −5, −2, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
6125	1, −9, −9, 11	$[1, \rho, \rho^2, \rho^3]$	5	Циклическая
6224	2, −4, −2, 2	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
6809	0, −5, −1, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
7053	2, −4, −3, 3	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
7056	0, −5, 0, 1	$[1, \rho, \rho^2, \rho^3]$	12, 21, 28	Vierergruppe
7168	0, −6, 0, 7	$[1, \rho, \rho^2, \rho^3]$	8	8-го порядка
7225	0, −11, 0, 9	$\left[1, \rho, \frac{\rho^2+\rho+1}{2}, \frac{\rho^3-2\rho+3}{6}\right]$	5, 17, 85	Vierergruppe
7232	2, −5, −4, 4	$\left[1, \rho, \rho^2, \frac{\rho^3+\rho}{2}\right]$	8	8-го порядка
7260	1, −7, −8, −2	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
7488	2, −4, −2, 1	$[1, \rho, \rho^2, \rho^3]$	12	8-го порядка
7537	1, −5, −4, 3	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
7600	0, −9, 0, 19	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
7625	1, −9, −4, 1	$\left[1, \rho, \rho^2, \frac{\rho^3-\rho^2-\rho}{4}\right]$	5	8-го порядка
8000	0, −10, 0, 20	$\left[1, \rho, \frac{\rho^2}{2}, \frac{\rho^3}{2}\right]$	5	Циклическая
8069	1, −5, −5, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
8112	0, −5, 0, 3	$[1, \rho, \rho^2, \rho^3]$	13	8-го порядка

ТАБЛИЦА ПОЛЕЙ 4-го ПОРЯДКА СИГНАТУРЫ $\tau=1$, для которых $|D|\leqslant 848$

(Таблица вычислена Ч. Поплавским)

Дискриминант поля	Коэффициенты у-ния $x^4-sx^3+px^2-qx+n=0$	Базис поля	Дискриминант подполя	Группа
—275	1, 0, —2, —1	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
—283	0, 0, 1, —1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—331	0, —2, 3, —1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—430	0, 1, 0, —1	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
—448	2, 1, 2, 1	$[1, \rho, \rho^2, \rho^3]$	8	8-го порядка
—475	1, —2, 2, —1	$[1, \rho, \rho^2, \rho^3]$	5	8-го порядка
—491	2, 2, —3, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—507	1, —1, 1, 1	$[1, \rho, \rho^2, \rho^3]$	13	8-го порядка
—563	1, 1, 1, —1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—643	1, 0, 2, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—688	2, 0, 0, —1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—731	0, —2, 1, —1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—751	0, —3, 1, 2	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая
—775	1,0,3,1	$\left[1, \rho, \rho^2 \frac{\rho^2+\rho^3}{2}\right]$	5	8-го порядка
—848	0, 1, 2, 1	$[1, \rho, \rho^2, \rho^3]$	—	Симметрическая

ТАБЛИЦА ПОЛЕЙ 4-го ПОРЯДКА СИГНАТУРЫ $\tau=2$, ДИСКРИМИНАНТЫ КОТОРЫХ НЕ БОЛЬШЕ 1296, ИМЕЮЩИХ КВАДРАТИЧНЫЕ ПОДПОЛЯ

(Таблица вычислена Д. К. Фаддеевым)

Обозначения: $i=\sqrt{-1}$, $\xi=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$

№	Производящее число	D	Группа	№	Производящее число	D	Группа
1	$\sqrt{4+\xi}$	117	$\mathfrak{G}$	20	$\sqrt{5+4i}$	656	$\mathfrak{G}$
2	$\sqrt{\frac{-5+\sqrt{5}}{2}}$	125	$\mathfrak{G}$	21	$\sqrt{-9-\xi}$	657	$\mathfrak{G}$
				22	$\sqrt{-7}$, i	784	$\mathfrak{B}$
3	ξ, i	144	$\mathfrak{B}$	23	$\sqrt{3+2i}$	832	$\mathfrak{G}$
4	$\sqrt{-5-\xi}$	189	$\mathfrak{G}$	24	$\sqrt{-11-4\xi}$	837	$\mathfrak{G}$
5	ξ, $\sqrt{5}$	225	$\mathfrak{B}$	25	$\sqrt{11+3\xi}$	873	$\mathfrak{G}$
6	i, $\sqrt{2}$	256	$\mathfrak{B}$	26	$\sqrt{12+5\xi}$	981	$\mathfrak{G}$
7	$\sqrt{1+4i}$	272	$\mathfrak{G}$	27	$\sqrt{3+\xi}$	1008	$\mathfrak{G}$
8	$\sqrt{1+2i}$	320	$\mathfrak{G}$	28	$\sqrt{-3-\xi}$	1008	$\mathfrak{G}$
9	$\sqrt{7+3\xi}$	333	$\mathfrak{G}$	29	$\sqrt{\frac{-13+\sqrt{5}}{2}}$	1025	$\mathfrak{G}$
10	$\sqrt{\frac{-1+\sqrt{-7}}{2}}$	392	$\mathfrak{G}$				
				30	$\sqrt{7+4i}$	1040	$\mathfrak{G}$
11	i, $\sqrt{5}$	400	$\mathfrak{B}$	31	$\sqrt{1+8i}$	1040	$\mathfrak{G}$
12	$\sqrt{-1-2\xi}\,(\sqrt[4]{-3})$	432	$\mathfrak{G}$	32	$\sqrt{3+2\sqrt{-2}}$	1088	$\mathfrak{G}$
13	ξ, $\sqrt{-7}$	441	$\mathfrak{B}$	33	$\sqrt{-5+2\sqrt{2}}$	1088	$\mathfrak{G}$
14	$\sqrt{1+i}$	512	$\mathfrak{G}$	34	ξ, $\sqrt{-11}$	1089	$\mathfrak{B}$
15	$\sqrt{8+\xi}$	513	$\mathfrak{G}$	35	$\sqrt{-13-5\xi}$	1141	$\mathfrak{G}$
16	$\sqrt{9+4\xi}$	549	$\mathfrak{G}$	36	$\sqrt{3+8i}$	1168	$\mathfrak{G}$
17	$\sqrt{2}$, ξ	576	$\mathfrak{B}$	37	$\sqrt{12+\xi}$	1197	$\mathfrak{G}$
18	$\sqrt{-2}$, ξ	576	$\mathfrak{B}$	38	$\sqrt{13+4\xi}$	1197	$\mathfrak{G}$
19	$\sqrt{\frac{3+\sqrt{-11}}{2}}$	605	$\mathfrak{G}$	39	$\sqrt{-7}$, $\sqrt{5}$	1225	$\mathfrak{B}$
				40	$\sqrt{2+i}$	1280	$\mathfrak{G}$

Г. ПОСТРОЕНИЕ КУБИЧЕСКИХ ОБЛАСТЕЙ ПО КВАДРАТИЧНЫМ

§ 42. Опирание кубических областей на квадратичные

В основу положим следующие простые геометрические соображения.

Пусть $(\omega, \omega', \omega'')$ точка в пространстве $R_{3,0}$. (Для простоты мы будем сначала считать, что ω, ω', ω'' вещественны. Однако это ограничение не является существенным, и мы его дальше снимем.)

Будем подвергать пространство $R_{3,0}$ осесовмещениям, т. е. преобразованиям, заключающимся в одновременных одинаковых перестановках координат всех точек пространства. Осесовмещения образуют группу преобразований, изоморфную симметрической группе перестановок трех элементов.

Все эти преобразования оставляют инвариантной рациональную прямую и преобразуют в себя плоскость „нулевого следа“ $u+u'+u''=0$. В этой плоскости они индуцируют преобразования, заключающиеся в поворотах на углы $\frac{2\pi}{3}$ и $\frac{4\pi}{3}$ вокруг начала координат и в отражениях относительно проекций осей координат, которые все можно составить из одного только поворота и одного отражения. Эти преобразования особенно удобно алгебраически записать, если принять плоскость нулевого следа за комплексную „ось“, вещественное направление которой совпадает с проекцией одной из осей координат трехмерного пространства; тогда мы получим, что осесовмещения индуцируют группу преобразований, вышеуказанными производящими элементами которой являются умножение на $\varepsilon = e^{\frac{2\pi i}{3}}$ (поворот) и переход к сопряженным числам (отражение).

Легко видеть, что проекция точки $(\omega, \omega', \omega'')$ на плоскость нулевого следа параллельно рациональной прямой имеет координаты $\left(\frac{2\omega-\omega'-\omega''}{\sqrt{6}}, \frac{\omega'-\omega''}{\sqrt{2}}\right)$, если за оси принять проекцию оси OX и перпендикулярную к ней прямую, при сохранении масштаба. Комплексная координата проекции будет

$$\frac{2\omega-\omega'-\omega''}{\sqrt{6}}+i\frac{\omega'-\omega''}{\sqrt{2}}=\frac{2}{\sqrt{6}}(\omega+\omega'\varepsilon+\omega''\varepsilon^2).$$

Изменив надлежащим образом масштаб, получим для комплексной координаты проекции более простое выражение:

$$\eta=\omega+\omega'\varepsilon+\omega''\varepsilon^2,$$

представляющее собой не что иное, как резольвенту Лагранжа точки $(\omega, \omega', \omega'')$. Если не предполагать точку $(\omega, \omega', \omega'')$ лежащей в вещественном сечении пространства K_3, то мы должны рассматривать плоскость нулевого следа как комплексно двухмерное многообразие. Легко видеть, что проекция, если за оси выбрать векторы $(1, \varepsilon, \varepsilon^2)$, $(1, \varepsilon^2, \varepsilon)$ и взять соответственный масштаб, будет задаваться двумя комплексными координатами η и $\bar{\eta}$, где

$$\eta=\omega+\omega'\varepsilon+\omega''\varepsilon^2, \quad \bar{\eta}=\omega+\omega'\varepsilon^2+\omega''\varepsilon.$$

Такая проекция будет точкой комплексного пространства, в случае если ω, ω', ω'' вещественны, и точкой вещественного пространства, если ω — вещественное, а ω', ω'' — комплексные сопряженные.

При осесовмещениях проекция $(\eta, \bar{\eta})$ точки ω, ω', ω'' будет подвергаться преобразованиям:

$$\begin{matrix}\eta\to\eta\\ \bar{\eta}\to\bar{\eta}\end{matrix}; \quad \begin{matrix}\eta\to\eta\varepsilon\\ \bar{\eta}\to\bar{\eta}\varepsilon^2\end{matrix}; \quad \begin{matrix}\eta\to\eta\varepsilon^2\\ \bar{\eta}\to\bar{\eta}\varepsilon\end{matrix}; \quad \begin{matrix}\eta\to\bar{\eta}\\ \bar{\eta}\to\eta\end{matrix}; \quad \begin{matrix}\eta\to\bar{\eta}\varepsilon\\ \bar{\eta}\to\eta\varepsilon\end{matrix}; \quad \begin{matrix}\eta\to\bar{\eta}\varepsilon^2;\\ \bar{\eta}\to\eta\varepsilon.\end{matrix}$$

Введем в рассмотрение куб проекции, т. е. точку $(\theta, \bar{\theta})$, координаты которой $\theta = \eta^3$, $\bar{\theta} = \bar{\eta}^3$.

При первых трех осесовмещениях точка $(\theta, \bar{\theta})$ не изменится, при последних ее координаты поменяются местами. Если заменить ε на ε^2, то θ и $\bar{\theta}$ также поменяются местами. Следовательно, каждая симметрическая функция от θ и $\bar{\theta}$ будет рационально выражаться через коэффициенты уравнения, корнями которого являются ω, ω', ω''. Отсюда заключаем, что куб проекции кубического числа является точкой некоторой квадратичной области.

Выясним, что представляет собой эта область. За производящее число ее можно принять $\theta - \bar{\theta}$, если только оно отлично от нуля. Но легко видеть, что

$$\begin{aligned}\theta - \bar{\theta} = {} & (\eta - \bar{\eta})(\eta - \bar{\eta}\varepsilon)(\eta - \bar{\eta}\varepsilon^2) = \\ = {} & (\omega + \omega'\varepsilon + \omega''\varepsilon^2 - \omega - \omega'\varepsilon^2 - \omega''\varepsilon)\cdot(\omega + \omega'\varepsilon + \omega''\varepsilon^2 - \omega\varepsilon - \omega' - \omega''\varepsilon^2)\cdot \\ & \cdot(\omega + \omega'\varepsilon + \omega''\varepsilon^2 - \omega\varepsilon^2 - \omega'\varepsilon - \omega'') = \\ = {} & -(\varepsilon - \varepsilon^2)(1 - \varepsilon)(1 - \varepsilon^2)(\omega - \omega')(\omega' - \omega'')(\omega'' - \omega) = \\ = {} & -3\sqrt{-3D(\omega)},\end{aligned}$$

где $D(\omega)$ — дискриминант числа ω.

Отсюда мы можем заключить, что кубы проекций всех чисел одной и той же кубической области принадлежат одной и той же квадратичной области $R(\sqrt{-3D})$, где D — дискриминант максимального кольца области, так как все $D(\omega)$ отличаются от D множителями, являющимися квадратами рациональных чисел. Эту область мы будем называть в дальнейшем областью, на которую опирается кубическая область. В дальнейшем будем обозначать через U кубическую область, через Q квадратичную область, на которую опирается U. Дискриминанты их будем обозначать соответственно D и d. Они связаны очевидным соотношением

$$D = -3^{\pm 1} d s^2,$$

где s — целое рациональное число.

§ 43. Некоторые теоремы о проекциях кубических чисел

Теорема 1. *Для того чтобы точка η, $\bar{\eta}$ была проекцией числа кубической области, необходимо и достаточно выполнение условий:*

a) η^3 и $\bar{\eta}^3$ — *корни квадратного уравнения с рациональными коэффициентами,*

b) $\eta\bar{\eta}$ — *рациональное число.*

Доказательство. Необходимость первого условия была показана раньше. Необходимость второго проверяется непосредственно. Действительно, если $(\eta, \bar{\eta})$ проекция кубического числа ω, то

$$\begin{aligned}\eta\bar{\eta} = {} & (\omega + \omega'\varepsilon + \omega''\varepsilon^2)(\omega + \omega'\varepsilon^2 + \omega''\varepsilon) = \\ = {} & \omega^2 + \omega'^2 + \omega''^2 - \omega\omega' - \omega'\omega'' - \omega''\omega = s^2 - 3q,\end{aligned}$$

где s и q коэффициенты уравнения $\omega^3 = s\omega^2 - q\omega + n$, корнями которого являются ω, ω', ω''.

Обратно, пусть точка $(\eta, \bar{\eta})$ удовлетворяет условиям a) и b). Очевидно, что эта точка будет проекцией точки $(\omega, \omega', \omega'')$, координаты которой определяются из уравнений

$$\omega + \omega' + \omega'' = 0, \quad \omega + \omega'\varepsilon + \omega''\varepsilon^2 = \eta, \quad \omega + \omega'\varepsilon^2 + \omega''\varepsilon = \bar{\eta}.$$

Вместо первого уравнения можно было взять уравнение $\omega+\omega'+\omega''=s$ при любом рациональном значении для s. Сделанный выбор числа s обозначает, что точку $(\omega, \omega', \omega'')$ мы ищем на плоскости нулевого следа.

Решая систему, получим следующие значения для координат точки $(\omega, \omega', \omega'')$:

$$\omega=\frac{\eta_1+\bar{\eta}_1}{3};$$

$$\omega'=\frac{\eta_1\varepsilon^2+\eta\varepsilon}{3};$$

$$\omega''=\frac{\eta\varepsilon+\bar{\eta}\varepsilon^2}{3}.$$

Составляя основные симметрические функции от ω, ω', ω'', получим

$$s=\omega+\omega'+\omega''=0,$$

$$q=\omega\omega'+\omega'\omega''+\omega''\omega=-\frac{\eta\bar{\eta}}{3},$$

$$n=\omega\omega'\omega''=\frac{\eta^3+\bar{\eta}^3}{27}.$$

Все эти числа рациональны при сделанных предположениях относительно точки $(\eta_1, \bar{\eta}_1)$, и, следовательно, ω, ω', ω'' являются корнями уравнения с рациональными коэффициентами. Тем самым теорема доказана.

Теорема 2. *Для того чтобы точки* $(\eta_{11}, \bar{\eta}_1)$ *и* $(\eta_2, \bar{\eta}_2)$ *были проекциями чисел* ω_1 *и* ω_2 *одной и той же кубической области, необходимо и достаточно, чтобы были выполнены условия теоремы 1 и чтобы точка* $\left(\frac{\eta_2}{\eta_1}, \frac{\bar{\eta}_2}{\bar{\eta}_1}\right)$ *принадлежала квадратичной области* Q, *определяемой квадратным уравнением, корнями которого являются* η^3 *и* $\bar{\eta}^3$.

Доказательство. Докажем сначала необходимость. Пусть числа ω_1 и ω_2 принадлежат одной и той же кубической области. Очевидно, что координаты точки $\left(\frac{\eta_2}{\eta_1}, \frac{\bar{\eta}_2}{\bar{\eta}_1}\right)$ при осесовмещениях и при замене ε на ε^2 подвергаются таким же преобразованиям, как и координаты точки $(\eta_1^3, \bar{\eta}_1^3)$, принадлежащей области Q. Следовательно, точка $\left(\frac{\eta_2}{\eta_1}, \frac{\bar{\eta}_2}{\bar{\eta}_1}\right)$ должна принадлежать той же области Q в силу известной теоремы теории Галуа. Однако то же самое легко получить непосредственным вычислением. Сделаем это вычисление, так как оно приводит и к доказательству достаточности. Пусть

$$\omega_2=a\omega_1^2+b\omega_1+c;$$
$$\omega_1^3=s\omega_1^2-q\omega_1+n.$$

Вычислим $\frac{\eta_2}{\eta_1}$.

$$\frac{\eta_2}{\eta_1}=\frac{\omega_2+\omega_2'\varepsilon+\omega_2''\varepsilon^2}{\omega_1+\omega_1'\varepsilon+\omega_1''\varepsilon^2}=a\,\frac{\omega_1^2+\omega_1'^2\varepsilon+\omega_1''^2\varepsilon^2}{\omega_1+\omega_1'\varepsilon+\omega_1''\varepsilon^2}+b=$$

$$=a\,\frac{(\omega_1^2+\omega_1'^2\varepsilon+\omega_1''^2\varepsilon^2)(\omega_1+\omega_1'\varepsilon^2+\omega_1''\varepsilon)}{(\omega_1+\omega_1'\varepsilon+\omega_1''\varepsilon^2)(\omega_1+\omega_1'\varepsilon^2+\omega_1''\varepsilon)}+b=$$

$$=a\,\frac{2s^3-7sq+9n+\sqrt{-3D(\omega_1)}}{2(s^2-3q)}+b.$$

Мы видим, что $\frac{\eta_2}{\eta_1}$ рационально выражается через $\sqrt{-3D(\omega_1)}$. Легко получить, что $\frac{\bar{\eta}_2}{\bar{\eta}_1}$ отличается от $\frac{\eta_2}{\eta_1}$ только знаком при $\sqrt{-3D(\omega_1)}$. Тем самым теорема в части необходимости доказана. Достаточность также непосредственно следует из найденного представления $\frac{\eta_2}{\eta_1}$ и $\frac{\bar{\eta}_2}{\bar{\eta}_1}$.

Действительно, если точка $\left(\frac{\eta_2}{\eta_1}, \frac{\bar{\eta}_2}{\bar{\eta}_1}\right)$ принадлежит области Q, то ее координаты могут быть представлены соответственно в виде

$$\frac{\eta_2}{\eta_1} = u + v\sqrt{-3D(\omega_1)},$$
$$\frac{\bar{\eta}_2}{\bar{\eta}_1} = u - v\sqrt{-3D(\omega_1)}$$

с рациональными коэффициентами u и v.

Из сравнения этих формул с формулой представления $\frac{\eta_2}{\eta_1}$ через коэффициенты a и b легко найти эти последние. Они оказываются рациональными. Теорема доказана полностью.

Теорема 3. *Для того чтобы кубическая область U была приводимой, необходимо и достаточно, чтобы одна из точек* $(\eta, \bar{\eta})$; $(\eta\varepsilon, \bar{\eta}\bar{\varepsilon}^2)$; $(\eta\varepsilon^2, \bar{\eta}\bar{\varepsilon})$ *принадлежала квадратичной области Q. Здесь через* $(\eta, \bar{\eta})$ *обозначена проекция любой точки общего положения области U.*

Доказательство. Пусть область U приводима. Тогда координаты какой-нибудь ее точки общего положения суть корни приводимого кубического уравнения $\omega^3 - s\omega^2 + q\omega - n = 0$. Обозначим через ω рациональный корень уравнения, через ω' и ω'' остальные корни. Эти последние могут быть представлены в виде $u \pm v\sqrt{D}$, где u и v — рациональные числа, а D — дискриминант максимального кольца области. Координаты проекции в этом случае будут:

$$\eta = \omega + \omega'\varepsilon + \omega''\varepsilon^2 = \omega - u + v\sqrt{-3D},$$
$$\bar{\eta} = \omega + \omega'\varepsilon^2 + \omega''\varepsilon = \omega - u - v\sqrt{-3D},$$

и, следовательно, точка $(\eta, \bar{\eta})$ принадлежит области Q.

Если бы рациональным корнем было не ω, а ω' или ω'', то принадлежала бы области Q точка $(\eta\varepsilon, \bar{\eta}\varepsilon^2)$ или $(\eta\varepsilon^2, \bar{\eta}\varepsilon)$.

Обратно, если одна из точек $(\eta, \bar{\eta})$, $(\eta\varepsilon, \bar{\eta}\varepsilon^2)$, $(\eta\varepsilon^2, \bar{\eta}\varepsilon)$ принадлежит квадратичной области, то одно из чисел

$$\omega = \frac{\eta + \bar{\eta}}{3}, \quad \omega' = \frac{\eta\varepsilon + \bar{\eta}\varepsilon^2}{3}, \quad \omega'' = \frac{\eta\varepsilon^2 + \bar{\eta}\varepsilon}{3}$$

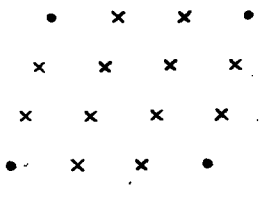
будет рациональным, и, следовательно, уравнение, которому удовлетворяют координаты точки, проекцией которой является $(\eta, \bar{\eta})$, будет приводимым.

Теорема 4. *Для того чтобы квадратичная область Q, на которую опирается кубическая область U, была приводимой, необходимо и достаточно, чтобы область U была чисто кубической или производилась уравнением $\omega^3 - 1 = 0$.*

Доказательство следует из того, что у таких, и только таких, кубических областей $-3D$ — полный квадрат.

§ 44. Свойства проекции максимальной кубической решетки

В предыдущем параграфе мы провели исследование проекций точек кубической области, т. е. точек, рационально связанных с точками некоторой максимальной кубической решетки. На основании этого исследования мы теперь имеем возможность дать способ построения кубических максимальных решеток по квадратичным, на которые они опираются.



Черт. 9.

Очевидно, что проекция параллельно рациональному направлению кубической решетки представляет собой решетку. Все точки решетки, получающиеся в проекции, удовлетворяют условиям теоремы 1 и связаны друг с другом условиями теоремы 2. Кроме того, координаты всех точек этой решетки суть целые алгебраические числа. Это непосредственно следует из формул

$$\eta = \omega + \omega'\varepsilon + \omega''\varepsilon^2;$$
$$\overline{\eta} = \omega + \omega'\varepsilon^2 + \omega''\varepsilon.$$

Однако, если точка $(\eta, \overline{\eta})$ удовлетворяет условиям теоремы 1 и координаты ее целые алгебраические, еще нельзя сделать заключение, что она будет проекцией целой точки, т. е. проекцией точки максимальной решетки. Действительно, в формулах

$$\omega = \frac{s + \eta + \overline{\eta}}{3},$$
$$\omega' = \frac{s + \eta\varepsilon^2 + \overline{\eta}\varepsilon}{3}, \qquad (*)$$
$$\omega'' = \frac{s + \eta\varepsilon + \overline{\eta}\varepsilon^2}{3},$$

выражающих координаты проектируемой точки через координаты проекции и след s, в знаменателе участвует число 3, благодаря чему координаты $\omega, \omega', \omega''$ могут оказаться дробными при любом выборе целого рационального числа s. Тем не менее нам полезно ввести в рассмотрение совокупность L всех точек, удовлетворяющих условиям теорем 1 и 2 и имеющих целые алгебраические координаты. Через $3L$ обозначим совокупность точек, получающихся умножением точек системы L на 3. Формулы (*) показывают, что каждая точка системы $3L$ является проекцией некоторой точки с целыми алгебраическими координатами, т. е. точки соответствующего максимального кольца. Достаточно в этих формулах взять $s = 0$ [или $s \equiv 0 \pmod 3$]. Система L, очевидно, повторяется сложением и вычитанием. Она двухмерна, так как содержит в себе двухмерную решетку — проекцию максимального кольца.

Она дискретна, так как подобная ей система $3L$ содержится в дискретной проекции максимального кольца. Следовательно, система L представляет собой двухмерную решетку. Система $3L$ — также решетка. Решетка L центрирует решетку $3L$ с индексом 9 (черт. 9).

Очевидно далее, что решетка L повторяется умножением на любую точку максимального кольца области Q. Следовательно, она подобна одной из решеток основной фигуры области Q:

$$L = \gamma\Gamma.$$

Здесь Γ обозначает решетку основной фигуры, которой подобна решетка L, и γ — „коэффициент" подобия. Коэффициент подобия γ имеет целые алгебраические координаты, так как все точки решетки L имеют целые алгебраи-

ческие координаты, а среди точек решетки Γ существуют точки, координаты которых взаимно просты с любым наперед заданным целым рациональным числом и, следовательно, с любым наперед заданным алгебраическим числом сколь-угодно высокого порядка. Далее, норма коэффициента γ есть рациональное число, так как нормы всех точек решеток L и Γ суть целые рациональные числа. Вследствие того, что координаты коэффициента γ *целые* алгебраические, норма γ *целая* рациональная.

Возведем решетку L в куб по правилу умножения решеток. Получим некоторую новую решетку $\Lambda = L^3$, которая будет подобна решетке Γ^3, принадлежащей вместе с Γ основной фигуре области Q. Коэффициентом подобия будет, очевидно, γ^3:

$$\Lambda = \gamma^3 \Gamma^3.$$

Решетка Λ образована числами области Q, так как куб каждой точки решетки L есть число области Q, а решетка $\Lambda = L^3$ рационально связана с решеткой, построенной на двух любых ее точках, за которые мы можем принять кубы двух точек решетки L. Далее, все точки решетки Λ являются целыми числами области Q и, следовательно, решетка Λ является подрешеткой максимального кольца области Q. Λ представляет собой идеал этого максимального кольца, так как Λ вместе с подобной ей решеткой Γ^3 повторяется умножением на все точки максимального кольца. Идеал Λ принадлежит классу, соответствующему решетке Γ^{-3}.

Коэффициент подобия γ^3 в равенстве $\Lambda = \gamma^3 \Gamma^3$ представляет собой точку решетки Γ^{-3}, которая ставится в соответствие идеалу Λ и заменяет его в вопросах делимости согласно общей теории побочных решеток.

Норма идеала Λ равна, очевидно, норме γ^3 и, следовательно, равна кубу целого рационального числа $N(\gamma)$.

Легко видеть, что Λ не может делиться на куб какого-либо идеала с отличной от единицы нормой. Действительно, если бы Λ делилось на идеал $\mathfrak{a}^3$, то миожитель γ^3 делился бы на α^3, где α — точка одной из решеток основной фигуры, сопоставляемая идеалу $\mathfrak{a}$. Отсюда следует, что $\frac{\gamma}{\alpha}$ имеет целые алгебраические координаты. Пусть α принадлежит решетке Γ_1. Тогда решетка $L_1 = \frac{\gamma}{\alpha}(\Gamma_1 \Gamma)$ будет состоять из точек с целыми алгебраическими координатами и содержать решетку $L = \gamma\Gamma$, как правильную часть, так как решетка Γ_1 содержит точку α и $\left|N\left(\frac{\gamma}{\alpha}\right)\right| < |N(\gamma)|$. Это невозможно, так как по самому определению решетки L ее нельзя центрировать точками с целыми координатами. Итак, идеал Λ не делится на куб какого-либо идеала, отличного от единичного. Отсюда легко заключить, что норма идеала Λ не делится ни на одно из неразложимых в области Q простых чисел и ни на одно из простых чисел, входящих в дискриминант. Действительно, каждое такое простое число делится только на один простой идеал, и так как норма Λ представляет собой полный куб, Λ должен был бы делиться на куб простого идеала, что, как мы видели, невозможно. Разложение идеала Λ на простые идеалы должно иметь вид:

$$\Lambda = \mathfrak{p}_1^2 \bar{\mathfrak{p}}_1 \mathfrak{p}_2^2 \bar{\mathfrak{p}}_2 \dots,$$

где $\mathfrak{p}_1, \bar{\mathfrak{p}}_1$; $\mathfrak{p}_2, \bar{\mathfrak{p}}_2, \dots$ — различные простые идеалы, входящие попарно в простые числа $p_1, p_2, \dots$

В виду того что $\mathfrak{p}_1\bar{\mathfrak{p}}_1 = p_1$, $\mathfrak{p}_2\bar{\mathfrak{p}}_2 = p_2$, $\dots$,

$$\Lambda = p_1 p_2 \dots \mathfrak{p}_1 \mathfrak{p}_2 \dots = \mathfrak{l},$$

где $\mathfrak{l} = \mathfrak{p}_1\mathfrak{p}_2\dots$, $l = p_1 p_2 \dots = N(\mathfrak{l})$.

Идеал $\mathfrak{I}$ эквивалентен идеалу Λ и, следовательно, подобен решетке Γ^3:

$$\mathfrak{I} = \lambda\Gamma^3.$$

Коэффициент подобия λ представляет собой точку решетки Γ^{-3}.

Итак, $\Lambda = \Omega\Gamma^3$. Следовательно, $\gamma^3 = \Omega$, $\gamma = \sqrt[3]{\Omega}$ и $L = \sqrt[3]{\Omega}\cdot\Gamma$.

Заметим, что извлечение кубического корня в формуле $\gamma = \sqrt[3]{\Omega}$ нужно произвести из обеих координат точки Ω. Однако из девяти возможных значений для γ нужно брать только те три, для которых произведение координат рационально.

Таким образом, решетка L обладает свойствами:

1. L подобна некоторой решетке Γ основной фигуры области Q.

2. Куб коэффициента подобия представляет собой произведение некоторой точки λ решетки Γ^{-3} на норму этой точки.

3. Норма l точки λ раскладывается на различные простые множители и взаимно проста с дискриминантом d области Q.

Очевидно и обратное, что если некоторая решетка обладает свойствами 1, 2, 3, то она может быть принята за решетку L для некоторого кубического максимального кольца. Действительно все точки такой решетки будут удовлетворять условиям теорем 1—2 предшествующего § 43 и, следовательно, являются проекциями точек некоторой кубической области, причем *все* проекции, имеющие целые алгебраические координаты, попадут в эту решетку, и, следовательно, она будет решеткой L.

Мы установили, что свойства 1, 2, 3 являются вполне характеризующими решетки L. Это позволяет фактически строить решетки L для кубических областей, исходя из данной области Q. Мы должны перебирать для этого все решетки Γ и все подходящие множители λ.

Решетки L, соответствующие приводимым кубическим областям, будут получаться только в случае, если $\lambda = 1$ и $\Gamma = \Gamma_0$ главной решетки. Это непосредственно следует из теоремы 3.

Одну и ту же кубическую область можно расположить в пространстве трех измерений шестью различными способами. Поэтому каждой кубической области соответствует шесть различных решеток L. Если L одна из них, то остальные, очевидно, будут:

$$L\varepsilon,\ L\varepsilon^2,$$
$$\overline{L},\ \overline{L}\varepsilon,\ \overline{L}\varepsilon^2,$$

где ε — точка с координатами $e^{\frac{2\pi i}{3}}$, $e^{\frac{4\pi i}{3}}$, а $\overline{L}$ — решетка, сопряженная L, т. е. решетка, координаты точек которой получаются посредством перестановки координат точек L. Следовательно, желая строить решетки L для *различных* кубических областей, мы должны брать только одно значение кубического корня в формуле $\gamma = \sqrt[3]{\Omega}$ и из двух решеток L и $\overline{L}$ брать только одну. Легко видеть, что для этого из двух решеток Γ и $\overline{\Gamma}$, соответствующих сопряженным классам идеалов, достаточно брать одну, но за то, если $\Gamma \neq \overline{\Gamma}$, для множителя λ нужно брать все возможные значения, в том числе и соответствующие сопряженным идеалам $\mathfrak{I}$ и $\overline{\mathfrak{I}}$, если эти последние принадлежат одному классу. Если же $\Gamma = \overline{\Gamma}$, то из значений λ, соответствующих сопряженным идеалам $\mathfrak{I}$ и $\overline{\mathfrak{I}}$, нужно брать одно.

Точка λ в равенстве $\mathfrak{I} = \lambda\Gamma^3$ определена с точностью до множителя, являющегося единицей максимального кольца области Q. Поэтому, если мы выберем идеал $\mathfrak{I}$ и решетку Γ, мы можем получить все же несколько различных решеток L. Однако, множители λ, отличающиеся кубом единицы максимального кольца, очевидно, определяют одну и ту же решетку. Разберем подробнее могущие представиться здесь случаи.

1. $d=-3$. В этом случае в основной фигуре существует лишь одна решетка, именно главная Γ_0. Единиц существует шесть: $1, \varepsilon, \varepsilon^2, -1, -\varepsilon, -\varepsilon^2$. В виду того, что $-1=(-1)^3$, три последних единицы не нуждаются в рассмотрении. Если $l\neq 1$, то множители λ, $\lambda\varepsilon$ и $\lambda\varepsilon^2$ дают различные решетки L, соответствующие различным кубическим областям. При $l=1$, $\lambda=1$ определяет решетку L для приводимой на три „прямых слагаемых" кубической области. $\lambda=\varepsilon$ и $\lambda=\varepsilon^2$ определяют различные решетки L, но соответствующие одной и той же кубической области, так как $\varepsilon^2=\bar{\varepsilon}$.

2. $d=-4$. Единиц в максимальном кольце существует четыре: $1, i, -1, -i$. В виду того, что $i=(-i)^3$, $-1=(-1)^3$, $-i=i^3$, присоединение единиц к множителю λ не меняет решетки L.

3. $d<-4$. В этом случае существуют только единицы ± 1. Присоединение -1 к λ не меняет решетки L.

4. $d=1$. Область Q приводима. Она содержит четыре единицы $(1, 1)$; $(1, -1)$; $(-1, 1)$; $(-1, -1)$, каждая из которых является кубом самой себя. Присоединение единиц к λ не меняет решетки L.

5. $d>1$. В этом случае все единицы представляются в виде степеней основной единицы ε_0 и могут лишь кубическим множителем отличаться от 1, ε_0 и ε_0^{-1}. Если $l\neq 1$, множители λ, $\lambda\varepsilon_0$ и $\lambda\varepsilon_0^{-1}$ определяют решетки L, соответствующие различным кубическим областям. Если $l=1$ и $\Gamma\neq\Gamma_0$, имеет место то же самое. Если же, наконец, $l=1$ и $\Gamma=\Gamma_0$, то при $\lambda=1$ мы получим решетку для приводимой кубической области, при $\lambda=\varepsilon_0$ и $\lambda=\varepsilon_0^{-1}$ получим решетки L, соответствующие одной и той же кубической области, так как они будут сопряжены.

Фактическое построение решеток L можно осуществить, не обращаясь к построению всех решеток основной фигуры максимального кольца области Q. Действительно, пусть мы выбрали идеал $\mathfrak{l}$ и класс идеалов K, соответствующий решетке Γ. Решетка Γ подобна решетке любого идеала класса K^{-1}. Возьмем произвольный идеал $\mathfrak{a}$ этого класса и конкретно зададим его при помощи базиса. Идеал $\mathfrak{l}$ должен принадлежать классу K^{-3}, и, следовательно, должен быть эквивалентен идеалу $\mathfrak{a}^3$, который мы можем фактически найти. Коэффициент подобия μ в равенстве $\mathfrak{l}=\mu\mathfrak{a}^3$ также фактически находится. Он будет, вообще говоря, дробным числом области Q.

Очевидно, что L тогда будет:

$$L=\sqrt[3]{l\mu}\cdot\mathfrak{a}.$$

Так как базис идеала $\mathfrak{a}$ нам известен, то отсюда мы найдем базис решетки L.

§ 45. Построение максимальных кубических решеток

В предыдущем параграфе мы дали способ построения решеток L, тесно связанных с проекцией максимального кольца. Теперь, считая решетку L известной, нам надлежит построить само максимальное кольцо. Мы видели, что проекция максимального кольца содержится в решетке L и содержит решетку $3L$. Отсюда следует, что проекция максимального кольца или совпадает с решеткой $3L$, или центрирует ее с индексом 3 или 9.

Обозначим совокупность всех целых точек U, имеющих своими проекциями точки $3L$, через $\mathfrak{M}$. Она представляет собой решетку, образованную точками системы $3L$, которую должно представить расположенной в плоскости $u+u'+u''=0$ трехмерного пространства, и всеми параллельными им точками. Базис решетки $\mathfrak{M}$ легко находится. Пусть точки $(\beta_1, \bar{\beta}_1)$ и $(\beta_2, \bar{\beta}_2)$ образуют базис решетки L. Базис решетки $3L$ будет образован точками $(3\beta_1, 3\bar{\beta}_1)$ и $(3\beta_2, 3\bar{\beta}_2)$. Координаты этих же точек относительно пространственных осей

координат будут:

$$\omega_1 = \beta_1 + \overline{\beta}_1; \quad \omega_1' = \beta_1 \varepsilon^2 + \overline{\beta}_1 \varepsilon; \quad \omega_1'' = \beta_1 \varepsilon + \overline{\beta}_1 \varepsilon^2;$$
$$\omega_2 = \beta_2 + \overline{\beta}_2; \quad \omega_2' = \beta_2 \varepsilon^2 + \overline{\beta}_2 \varepsilon; \quad \omega_2'' = \beta_2 \varepsilon + \overline{\beta}_2 \varepsilon^2.$$

Посредством простых вычислений, приведенных в настоящем параграфе, легко найти уравнения, определяющие точки ω_1 и ω_2, и установить связывающее их преобразование Чирнгаузена. Базис решетки $\mathfrak{M}$ будет, очевидно, $[1; \omega_1; \omega_2]$.

Дискриминант $D(\mathfrak{M})$ решетки $\mathfrak{M}$ равен:

$$\begin{vmatrix} 1, & \beta_1 + \overline{\beta}_1, & \beta_2 + \overline{\beta}_2 \\ 1, & \beta_1 \varepsilon^2 + \overline{\beta}_1 \varepsilon, & \beta_2 \varepsilon^2 + \overline{\beta}_2 \varepsilon \\ 1, & \beta_1 \varepsilon + \overline{\beta}_1 \varepsilon^2, & \beta_2 \varepsilon + \overline{\beta}_2 \varepsilon^2 \end{vmatrix}^2 = \begin{vmatrix} 1 & 1 & 1 \\ 1 & \varepsilon^2 & \varepsilon \\ 1 & \varepsilon & \varepsilon^2 \end{vmatrix}^2 \cdot \begin{vmatrix} 1 & 0 & 0 \\ 0 & \beta_1 & \beta_2 \\ 0 & \overline{\beta}_1 & \overline{\beta}_2 \end{vmatrix}^2 =$$

$$= -27 \begin{vmatrix} \beta_1, & \beta_2 \\ \overline{\beta}_1, & \overline{\beta}_2 \end{vmatrix} = -27\, D(L),$$

где $D(L)$ обозначает дискриминант решетки L. Этот последний равен произведению квадрата нормы множителя γ на дискриминант решетки Γ, который совпадает с дискриминантом максимального кольца области Q, в. силу основного свойства побочных решеток области. Таким образом

$$D(\mathfrak{M}) = -27\, dl^2,$$

ибо

$$N(\gamma) = \sqrt[3]{N(l\lambda)} = l.$$

Найдя решетку $\mathfrak{M}$, решетку максимального кольца мы можем получить посредством небольшого количества дополнительных вычислений. Нужно только посмотреть, не будут ли существовать целые числа среди чисел

$$\frac{a_1 + a_2\omega_1 + a_3\omega_2}{3} \text{ при } a_1 = 0, \pm 1; \; a_2 = 0, \pm 1; \; a_3 = 0, \pm 1.$$

Дело сводится при самом грубом способе вычислений к $13 = \frac{27-1}{2}$ испытаниям.

Изучим теперь подробнее решетку $\mathfrak{M}$.

Теорема 5. *Решетка $\mathfrak{M}$ представляет собой кольцо.*

Доказательство. Пусть ω одно из чисел решетки $\mathfrak{M}$ и

$$\omega^3 = s\omega^2 - q\omega + n$$

уравнение, корнями которого являются ω, ω' и ω''.

Координаты θ, $\overline{\theta}$ куба проекции точки ω удовлетворяют уравнению

$$\theta^2 - (2s^3 - 9sq + 27n)\theta + (s^2 - 3q)^3 = 0.$$

Для того чтобы число ω принадлежало решетке $\mathfrak{M}$, необходимо и достаточно, чтобы ее проекция принадлежала решетке $3L$ и, следовательно, чтобы координаты куба проекции делились на 27. Для этого нужно, чтобы выполнялись условия

$$2s^3 - 9sq + 27n \equiv 0 \pmod{27},$$
$$s^2 - 3q \equiv 0 \pmod{9},$$

для чего в свою очередь необходимо и достаточно выполнение условий

$$s \equiv q \equiv 0 \pmod{3}.$$

Пусть число ω принадлежит решетке $\mathfrak{M}$. Тогда ω^2 также принадлежит решетке $\mathfrak{M}$. Действительно, коэффициенты s_1, q_1 уравнения, корнем которого является ω^2, связаны соотношениями

$$s_1 = s^2 - 2q, \quad q_1 = q^2 - 2sn$$

с коэффициентами s и q и если $s \equiv q \equiv 0 \pmod 3$, то и

$$s_1 \equiv q_1 \equiv 0 \pmod 3.$$

Пусть теперь числа ω_1 и ω_2 принадлежат решетке $\mathfrak{M}$. Тогда число $2\omega_1\omega_2$ принадлежит решетке $\mathfrak{M}$, так как

$$2\omega_1\omega_2 = (\omega_1 + \omega_2)^2 - \omega_1^2 - \omega_2^2,$$

и *решетка* $\mathfrak{M}$ повторяется сложением и вычитанием.

Но число $\omega_1\omega_2$, очевидно, также принадлежит решетке $\mathfrak{M}$, так как если коэффициенты s и q для числа $2\omega_1\omega_2$ делятся на три, то же самое имеет место для коэффициентов уравнения, которому удовлетворяет $\omega_1\omega_2$.

Таким образом, решетка $\mathfrak{M}$ повторяется умножением, и тем самым теорема доказана.

Не трудно дать формулу для индексформы кольца $\mathfrak{M}$.

Пусть $\omega = x\omega_1 + y\omega_2 + z$ — общее число кольца $\mathfrak{M}$. Тогда индексформа кольца будет равна

$$f(x, y) = \frac{\sqrt{D(\omega)}}{\sqrt{D(\mathfrak{M})}} = \frac{(\omega' - \omega'')(\omega'' - \omega)(\omega - \omega')}{\sqrt{-27dl^2}}.$$

Подставив сюда вместо ω_1, ω_2 и сопряженных чисел их выражения через базис решетки L, получим после простых вычислений

$$f(x, y) = \frac{(x\beta_1 + y\beta_2)^3 - (x\bar{\beta}_1 + y\bar{\beta}_2)^3}{l\sqrt{d}}.$$

Этому выражению можно придать еще более простой вид, обратившись к представлению базиса решетки L через базис $[a_1, a_2]$ подобного идеала $\mathfrak{a}$, использовав соотношение

$$L = \sqrt[3]{l\mu}\cdot\mathfrak{a},$$

где μ — подходящим образом подобранное число области Q. Из этого соотношения мы получаем

$$\gamma_1 = \sqrt[3]{l\mu}\, a_1, \qquad \gamma_2 = \sqrt[3]{l\mu}\, a_2,$$
$$\bar{\gamma}_1 = \sqrt[3]{l\bar{\mu}}\, \bar{a}_1, \qquad \bar{\gamma}_2 = \sqrt[3]{l\bar{\mu}}\, \bar{a}_2,$$

откуда

$$f(x, y) = \frac{\mu(xa_1 + ya_2)^3 - \bar{\mu}(x\bar{a}_1 + y\bar{a}_2)^3}{\sqrt{d}},$$

т. е. $f(x, y)$ представляет собой форму, стоящую при $\sqrt{d}$ в представлении $\mu(xa_1 + ya_2)^3$ в виде $\frac{F(x, y) + f(x, y)\sqrt{d}}{2}$.

Из способа выбора множителя μ следует, что числа μa_1^3, $\mu a_1^2 a_2$, $\mu a_1 a_2^2$ и μa_2^3 суть целые числа области Q и, следовательно, $f(x, y)$ действительно имеет целые коэффициенты, причем средние коэффициенты ее делятся на 3.

Построив индексформу кольца $\mathfrak{M}$, легко узнать, каким образом максимальное кольцо центрирует кольцо $\mathfrak{M}$.

Пусть $f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + ey^3$ — индексформа кольца $\mathfrak{M}$. Очевидно, что если максимальное кольцо центрирует кольцо $\mathfrak{M}$ с индексом 9, то коэффициенты a и e должны делиться на 3. Если же максимальное кольцо

центрирует кольцо $\mathfrak{M}$ с индексом 3, то должна найтись линейная подстановка переменных, с определителем, равным 3, произведя которую в форме $f(x, y)$, мы получили бы новую форму, все коэффициенты которой делились бы на 9. Легко видеть, что это возможно в том, и только в том случае, если одно из чисел a, e, $a+3b+3c+l$ и $a-3b+3c-l$ делится на 9, а остальные не делятся на 3.

Таким образом, введение индексформы кольца $\mathfrak{M}$ позволяет найти максимальное кольцо почти без вычислений.

Выясним теперь, как связаны возможности той или другой центрировки кольца $\mathfrak{M}$ максимальным кольцом с дискриминантом квадратичной области и с числом l.

Теорема. *Если d делится на 3, то максимальное кольцо совпадает с $\mathfrak{M}$ или центрирует $\mathfrak{M}$ с индексом 9. Если d не делится на 3, а l делится на 3, то $\mathfrak{M}$ совпадает с максимальным кольцом. Если же, наконец, d не делится на 3 и l не делится на 3, то максимальное кольцо совпадает с $\mathfrak{M}$ или центрирует $\mathfrak{M}$ с индексом 3.*

Доказательство. Теорема содержит три утверждения, каждое из которых мы докажем отдельно. Начнем с первого.

Пусть d делится на 3, и

$$f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + ey^3$$

— индексформа кольца $\mathfrak{M}$. Сделаем допущение, противоположное утверждению, высказанному в формулировке теоремы. Именно, допустим, что максимальное кольцо центрирует $\mathfrak{M}$ с индексом 3. Тогда от формы $f(x, y)$ можно перейти к эквивалентной, в которой коэффициент e будет делиться на 9 и коэффициент a не будет делиться на 3. Дискриминант этой формы равен

$$D(f) = 81b^2c^2 - 4\cdot 27ac^3 - 4\cdot 27eb^3 + 18\cdot 9abce - 27e^2 \equiv$$
$$\equiv -4\cdot 27ac^3 + 81b^2c^2 \pmod{243}.$$

Дискриминант $D(f)$, по предположению, делится на 81, но не делится на 243. Последнее сравнение показывает, что это невозможно. Первое утверждение теоремы доказано.

Третье утверждение теоремы очевидно. Остается доказать второе. Пусть d не делится на 3, а e делится на 3. Тогда все точки ω, лежащие на плоскости нулевого следа и проектирующиеся в точки решетки $3L$, обладают тем свойством, что ω^3 делится на 3. Действительно, коэффициент q уравнения $\omega^3 = -q\omega + n$, корнем которого является ω, должен делиться на 3 для всякой точки, проектирующейся в точку решетки $3L$. Коэффициент n, равный $\alpha^3 + \bar{\alpha}^3$, где $(3\alpha, 3\bar{\alpha})$ проекция ω, также делится на 3, так как $\bar{\alpha}^3$ и α^3 делится на l, делящееся на 3, по предположению. Благодаря этому кольцо $\mathfrak{M}$ не может быть центрировано точками, не параллельными точкам нулевого следа. Действительно, такие точки могут быть представлены в виде $\frac{\omega + k}{3}$, где ω — точка нулевого следа, проектирующаяся в точку решетки $3L$, и k не делится на 3. Но, очевидно, что $\omega + k$ взаимно просто с 3 и $\frac{\omega + k}{3}$ не может быть целым числом. Остается предположить, что кольцо $\mathfrak{M}$ центрируется точками, параллельными точкам нулевого следа. Пусть ω одна из таких центрирующих точек и

$$\omega^3 = s\omega^2 - q\omega + n$$

уравнение, корнем которого она является. Коэффициент s этого уравнения делится на 3, но коэффициент q не делится на 3, так как иначе ω принадлежала бы решетке $\mathfrak{M}$.

Дискриминант числа ω, равный

$$s^2q^2 - 4q^3 - 4s^3n + 18snq - 27n^2 \equiv -4q^3 \pmod 3,$$

не делится на 3, и, следовательно, дискриминант максимального кольца, которому принадлежит ω, не делится на 3. Но это возможно только при d, делящемся на 3, что противоречит предположению. Таким образом, кольцо $\mathfrak{M}$ не может быть, при наших предположениях, центрировано целыми точками, и, следовательно, совпадает с максимальным кольцом.

Теорема доказана.

§ 46. Некоторые свойства дискриминантов кубических полей

Из всего сказанного можно получить некоторые интересные следствия относительно дискриминантов кубических максимальных колец.

Во-первых, мы получили, что дискриминант кубической области может делиться не выше чем на вторую степень простого числа, отличного от 2 и 3, может делиться на 2 только в квадрате или в кубе и на 3 в первой, третьей, четвертой или пятой степени.

Действительно, $D = -27dl^2$, если $l \equiv 0$ (3); $D = -27dl^2$ или $-\frac{1}{3}dl^2$, если $d \equiv 0$ (3); $D = -27dl^2$ или $-3dl^2$, если ни d ни l не делятся на 3. d и l взаимно просты и не делятся на квадрат ни одного простого числа, кроме 2. d может делиться на 2^2 или 2^3.

Во-вторых, легко получить, что дискриминанты кубических полей возрастают не быстрее чисел некоторой арифметической прогрессии.

Действительно, дискриминанты квадратичных областей возрастают не быстрее чисел некоторой арифметической прогрессии. Если $d > 0$, можно над каждой квадратичной областью построить кубическую, полагая, при составлении решетки L, $\Gamma = \Gamma_0$ и $\lambda = \varepsilon_0$. Дискриминанты соответствующих максимальных кубических колец будут не превышать по абсолютной величине $27d$ и, следовательно, будут расти не быстрее чисел некоторой арифметической прогрессии.

Над квадратичными областями отрицательного дискриминанта также легко построить кубические с маленькими дискриминантами. Рассмотрим только $d \equiv -7$ (8). Такие дискриминанты расположены не реже чисел некоторой арифметической прогрессии. Для этих областей число 2 разлагается на два различных простых множителя:

$$2 = \mathfrak{p}_2\overline{\mathfrak{p}}_2.$$

Пусть $\mathfrak{p}_2$ принадлежит некоторому классу K. Если число классов не делится на 3, то найдется класс K_1 такой, что $KK_1^3 = K_0$ — главному классу. В этом случае можно построить решетку L, взяв $\mathfrak{l} = \mathfrak{p}_2$ и взяв за решетку Γ решетку, соответствующую классу K_1.

Если же число классов делится на 3, то найдется класс K, куб которого дает главный класс. Решетку L можно построить, взяв $\lambda = 1$ и взяв за решетку Γ решетку, соответствующую классу K. Дискриминант построенного на решетке L максимального кольца не превышает в первом случае — $108d$ и во втором — $27d$ и, следовательно, возрастает не быстрее чисел некоторой арифметической прогрессии.

Можно было бы, кроме того, получить из этих рассмотрений характер разложения на простые идеалы простых чисел, входящих в дискриминант области. Мы не будем этого делать, так как относящийся к этому вопросу результат нами уже был получен другим способом.

В заключение параграфа приведем несколько примеров построения кубических областей по квадратичным.

Пример 1. Построить несколько кубических областей над $R(\sqrt{-15})$.

Квадратичная область $R(\sqrt{-15})$ имеет два класса идеалов. Представителем класса $K_1 \neq K_0$ является идеал $\mathfrak{p}_3$.

Разложим наименьшие простые числа на простые идеалы:

$$\begin{aligned}
2&=\mathfrak{p}_2\,\overline{\mathfrak{p}_2};\quad \mathfrak{p}_2\sim\overline{\mathfrak{p}_2}\sim\mathfrak{p}_3;\\
3&=\mathfrak{p}_3^2;\\
5&=\mathfrak{p}_5^2;\quad \mathfrak{p}_5\sim\mathfrak{p}_3;\\
17&=\mathfrak{p}_{17}\overline{\mathfrak{p}_{17}};\ \mathfrak{p}_{17}\sim\overline{\mathfrak{p}_{17}}\sim\mathfrak{p}_3;\\
19&=\mathfrak{p}_{19}\overline{\mathfrak{p}_{19}};\ \mathfrak{p}_{19}\sim\overline{\mathfrak{p}_{19}}\sim 1;\\
23&=\mathfrak{p}_{23}\overline{\mathfrak{p}_{23}};\ \mathfrak{p}_{23}\sim\overline{\mathfrak{p}_{23}}\sim\mathfrak{p}_3;\\
31&=\mathfrak{p}_{31}\overline{\mathfrak{p}_{31}};\ \mathfrak{p}_{31}\sim\overline{\mathfrak{p}_{31}}\sim 1.
\end{aligned}$$

Решетки L можно строить, исходя из решетки Γ_0 или из решетки Γ_1. Так как $\Gamma^{-s}=\Gamma_0$, $\Gamma_1^{-s}=\Gamma_1$, множители λ нужно брать, соответственно, из решеток Γ_0 и Γ_1.

Пусть $\rho=\frac{1+\sqrt{-15}}{2}$.

При построении решетки L, исходя из решетки Γ_0, получим для индексформы кольца $\mathfrak{M}$ значение

$f(x, y)=$ коэффициенту при ρ в выражении

$\varphi_0(x, y)=\mu(x+y\rho)^3=\mu[x^3-12xy^2-4y^3+\rho(3x^2y+3xy^2-3y^3)]$,

где μ — любое число главного класса, норма которого не делится на квадрат простого числа и не делится на 3 и на 5.

При построении решетки L, исходя из решетки Γ_1, получим для индексформы представление в виде коэффициента при ρ в выражении

$$\varphi_1(x, y)=\mu[3x+(1+\rho)y]^3,$$

где μ — переходный множитель от идеала $\mathfrak{l}$ к идеалу $\mathfrak{p}_3^3$, т. е. $[\mu]=\frac{\mathfrak{l}\mathfrak{p}_3}{9}$.

Преобразуя несколько $\varphi_1(x, y)$, получим:

$$\varphi_1(x, y)=\tfrac{\mathfrak{l}\mathfrak{p}_3}{3}[9x^3+9x^2y-9xy^2-5y^3+\rho(9x^2y+9xy^2+y^3)].$$

Множитель $\mathfrak{l}\mathfrak{p}_3$ может быть любым целым числом, норма которого делится на 3, не делится на 5 и не делится на квадрат ни одного простого числа.

Выпишем несколько наименьших значений для μ и для $\mathfrak{l}\mathfrak{p}_3$.

$$\mu:\ \mathfrak{p}_{19}=1+2\rho;\quad \mathfrak{p}_{31}=3+2\rho;\quad \mathfrak{p}_2\mathfrak{p}_{17}=5+\rho;\quad \mathfrak{p}_2\overline{\mathfrak{p}}_{17}=-1+3\rho;$$
$$\mathfrak{l}\mathfrak{p}_3:\ \mathfrak{p}_2\mathfrak{p}_3=1+\rho;\quad \mathfrak{p}_3\mathfrak{p}_{17}=5+2\rho;\quad \mathfrak{p}_3\mathfrak{p}_{23}=1+4\rho;$$
$$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{19}=10+\rho;\quad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{19}=2+5\rho.$$

Исходя из этих множителей, получим индексформы колец $\mathfrak{M}$:

для Γ_0:

$$\begin{aligned}
f(x, y)&=2x^3+9x^2y-15xy^2-17y^3; & D&=5\cdot 3^4\cdot 19^2;\\
f(x, y)&=2x^3+15x^2y-9xy^2-23y^3; & D&=5\cdot 3^4\cdot 31^2;\\
f(x, y)&=x^3+18x^2y+6xy^2-22y^3; & D&=5\cdot 3^4\cdot 2^2\cdot 17^2;\\
f(x, y)&=3x^3+6x^2y-30xy^2-18y^3; & D&=5\cdot 3^4\cdot 2^2\cdot 17^2;
\end{aligned}$$

для Γ_1:

$$\begin{aligned}
f(x, y)&=3x^3+9x^2y+3xy^2-y^3; & D&=5\cdot 3^4\cdot 2^2;\\
f(x, y)&=6x^3+27x^2y+15xy^2-y^3; & D&=5\cdot 3^4\cdot 17^2;\\
f(x, y)&=12x^3+27x^2y+3xy^2-5y^3; & D&=5\cdot 3^4\cdot 23^4;\\
f(x, y)&=3x^3+36x^2y+30xy^2+2y^3; & D&=5\cdot 3^4\cdot 2^2\cdot 19^2;\\
f(x, y)&=15x^3+36x^2y+6xy^2-6y^3; & D&=5\cdot 3^4\cdot 2^2\cdot 19^2.
\end{aligned}$$

Из рассмотренных девяти случаев только в двух имеет место центрировка. Максимальные кольца наименьшего дискриминанта задаются формами:

$$\begin{aligned} 3x^3+9x^2y+3xy^2-y^3;&\quad D=5\cdot 3^4\cdot 2^2;\\ x^3+2x^2y-10xy^2-6y^3;&\quad D=5\cdot 2^2\cdot 17^2;\\ 5x^3+12x^2y+2xy^2-2y^3;&\quad D=5\cdot 2^2\cdot 19^2. \end{aligned}$$

Пример 2.

Построить несколько кубических областей, опирающихся на $R(\sqrt{5})$.

В области $R(\sqrt{5})$ существует лишь один класс.

Обозначим через ε_0 основную единицу $\frac{1+\sqrt{5}}{2}$ максимального кольца. Индексформы $f(x, y)$ колец $\mathfrak{M}$, опирающихся на $R(\sqrt{5})$, будут получаться из выражения

$$\mu(x+y\varepsilon_0)^3=\frac{I(x, y)+f(x, y)\sqrt{5}}{2},$$

где μ — любое число, норма которого не делится на 5 и на квадрат какого-либо простого числа.

Составим несколько множителей с наименьшими нормами:

$$\mu=\varepsilon_0;\quad \mu=\pi_{11}=3+\varepsilon_0;\quad \mu=\pi_{11}\varepsilon_0=1+4\varepsilon_0;\quad \mu=\pi_{11}\varepsilon_0^{-1}=-2+3\varepsilon_0.$$

Соответствующие индексформы колец $\mathfrak{M}$ будут:

$$\begin{aligned} f(x, y)=x^3+3x^2y+6xy^2+3y^3;&\quad D=-5\cdot 2^3;\\ f(x, y)=x^3+12x^2y+15xy^2+9y^3;&\quad D=-5\cdot 3^3\cdot 11^2;\\ f(x, y)=4x^3+15x^2y+27xy^2+24y^3;&\quad D=-5\cdot 3^3\cdot 11^2;\\ f(x, y)=3x^3+3x^2y+12xy^2+5y^3;&\quad D=-5\cdot 3^3\cdot 11^2. \end{aligned}$$

Из этих четырех случаев максимальное кольцо будет центрировать кольцо $\mathfrak{M}$ только во втором случае. Индексформа максимального кольца в этом случае будет равна $3x^3+12x^2y+5xy^2+y^3$ с дискриминантом $-5\cdot 3\cdot 11^2$. В остальных трех случаях максимальное кольцо совпадает с кольцом $\mathfrak{M}$.

Д. ПОСТРОЕНИЕ ОБЛАСТЕЙ ЧЕТВЕРТОГО ПОРЯДКА ПО КУБИЧЕСКИМ

Подобно тому как мы дали в предыдущем параграфе способ построения кубических областей, расклассифицировав их по квадратичным, на которые они опираются, можно расклассифицировать и области четвертого порядка (для краткости мы будем их в дальнейшем называть биквадратичными) по кубическим и дать способ их построения. При этом придется осуществить обращение известного способа Лагранжа решения уравнения четвертой степени в радикалах.

§ 47. Опирание областей 4-го порядка на кубические

Рассмотрим пространство четырех измерений K_4 с выбранными осями координат Ou, Ou', Ou'', Ou''', которое будем сначала, для простоты геометрических построений, считать вещественным. Каждая вещественная биквадратичная область, по определению, образована совокупностью всех точек, рационально расположенных относительно некоторой решетки, повторяющейся умножением. Данную область можно расположить в пространстве 24 различными способами. Переход от одного расположения к другому осуществляется одновременными одинаковыми перестановками координат всех точек пространства.

Такие преобразования мы назвали осесовмещениями. Осесовмещения, очевидно, образуют группу, изоморфную симметрической группе перестановок четырех элементов. При всех осесовмещениях точки „рациональной прямой“ $u=u'=u''=u'''$ не меняют своего положения. Ортогональное рациональной

прямой трехмериое „пространство иулевого следа“ $u+u'+u''+u'''=0$ переходит в себя при всех осесовмещениях.

Спроектируем пространство K_4 на пространство нулевого следа параллельно рациональному направлению. Очевидно, что проекции осей координат образуют в пространстве нулевого следа совокупность четырех прямых, образующих одна с другой попарно равные углы. Такие четыре прямых можно, очевидно, приниять за диагонали иекоторого куба, причем положительные направления этих прямых соединят центр куба с вершинами одиого из тетраэдров, вписанных в куб (см. чертеж 7). Примем оси симметрии четвертого порядка этого куба за оси координат Ov, Ov', Ov'' пространства нулевого следа, выбрав их направления согласно чертежу. Проекции точек (1, 0, 0, 0); (0, 1, 0, 0); (0, 0, 1, 0) и (0, 0, 0, 1) в этих осях, с сохранением масштаба, будут иметь, очевидно, координаты $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$; $\left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right)$; $\left(-\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right)$ и $\left(-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right)$. Следовательно, точка (u, u', u'', u''') имеет своей проекцией точку (v, v', v''), координнаты которой получаются по формулам

$$v=\frac{1}{2}(u+u'-u''-u'''),$$

$$v'=\frac{1}{2}(u-u'+u''-u'''),$$

$$v''=\frac{1}{2}(u-u'-u''+u''').$$

Для удобства вычислений уменьшаем вдвое масштаб в пространстве нулевого следа. Тогда проекцией точки (u, u', u'', u''') будет точка $(u+u'-u''-u'''; u-u'+u''-u'''; u-u'-u''+u''')$.

Заметим, что выбранные нами оси координат в пространстве нулевого следа представляют собой проекции на это пространство „биссектрисных плоскостей“

$$u=u';\quad u''=u''';$$
$$u=u'';\quad u'=u''';$$
$$u=u''';\quad u'=u''.$$

При осесовмещениях в пространстве K_4 пространство иулевого следа будет подвергаться ортогональным преобразованиям, совмещающим тетраэдр $AA'A''A'''$ с собой. Двенадцать из этих преобразований будут вращениямн пространства, двенадцать вращениями + отражение.

Координаты проекции при осесовмещениях будут переставляться между собой всеми возможными способами и, кроме того, могут попарно менять знаки.

Введем в пространстве нулевого следа действие умножения точек обычным способом по координатам. Очевидно, что координаты квадратов точек нулевого следа, а также произведений двух различных точек будут только переставляться при осесовмещениях, не меняя знаков.

Отсюда следует, что квадраты проекций точек некоторой биквадратичной области, а также пронзведения проекций двух различных точек будут принадлежать некоторой вполне определеиной кубической области. Эту область мы будем называть кубической областью, на которую опирается биквадратичная.

Биквадратичные области мы будем обозначать в дальнейшем через T, кубическую область, на которую опирается биквадратическая область T, будем обозначать U. Их дискриминанты обозначаем, соответственно, Δ и D.

Предположение о вещественностн пространства K_4 не является существениым. Для комплексного пространства проекцией точки (u, u', u'', u'''), так же как в вещественном случае, мы называем точку $(u+u'-u''-u''', u-u'+u''-u''', u-u'-u''+u''')$. Легко видеть, что это действительно проекция при подходящем выборе осей и масштаба.

§ 48. Некоторые теоремы о проекциях чисел 4-го порядка

Теорема 1. *Для того чтобы точка* (η, η', η'') *была проекцией точки биквадратичной области, необходимо и достаточно выполнение условий:*

1. *Квадрат точки* (η, η', η'') *принадлежит некоторой кубической области.*

2. $N(\eta) = \eta\eta'\eta''$ *рациональна.*

Доказательство. Пусть ω — точка биквадратичной области. Ее координаты являются корнями некоторого уравнения

$$\omega^4 - f_1\omega^3 + f_2\omega^2 - f_3\omega + f_4 = 0,$$

коэффициенты которого рациональны.

Координаты квадрата проекции точки

$$\theta = (\omega + \omega' - \omega'' - \omega''')^2,\quad \theta' = (\omega - \omega' + \omega'' - \omega''')^2,\quad \theta'' = (\omega - \omega' - \omega'' + \omega''')^2$$

представляют собою корни кубического уравнения, коэффициенты которого, будучи симметрическими функциями от ω, ω', ω'', ω''', рационально выражаются через коэффициенты f_1, f_2, f_3, f_4 и, следовательно, рациональны.

Норма проекции

$$\eta\eta'\eta'' = (\omega + \omega' - \omega'' - \omega''')(\omega - \omega' + \omega'' - \omega''')(\omega - \omega' - \omega'' + \omega''')$$

есть также симметрическая функция от ω, ω', ω'', ω''' и потому рациональна.

Общеизвестные вычисления дают, что θ является корнем уравнения

$$\theta^3 - (3f_1^2 - 8f_2)\theta^2 + (3f_1^4 - 16f_1^2f_2 + 16f_2^2 + 16f_1f_3 - 64f_4)\theta - r^2 = 0,$$

где

$$r = N(\eta) = f_1^3 - 4f_1f_2 + 8f_3.$$

Обратно, пусть координаты точки (η, η', η'') удовлетворяют условиям теоремы. Точка (η, η', η'') является проекцией точки $(\omega, \omega', \omega'', \omega''')$, координаты которой вычисляются по формулам

$$\omega = \frac{\eta + \eta' + \eta''}{4};\quad \omega' = \frac{\eta - \eta' - \eta''}{4};\quad \omega'' = \frac{-\eta + \eta' - \eta''}{4};\quad \omega''' = \frac{-\eta - \eta' + \eta''}{4},$$

что легко проверить.

Нам нужно показать, что коэффициенты уравнения, корнями которого является ω, ω', ω'', ω''', рациональны.

Составим такое уравнение:

$$\omega^4 - f_1\omega^3 + f_2\omega^2 - f_3\omega + f_4 = 0.$$

Коэффициентами его будут числа

$$\begin{aligned} f_1 &= \omega + \omega' + \omega'' + \omega''' = 0,\\ f_2 &= \omega\omega' + \ldots = -\frac{\theta + \theta' + \theta''}{8},\\ f_3 &= \omega\omega'\omega'' + \ldots = \frac{\eta\eta'\eta''}{8},\\ f_4 &= \omega\omega'\omega''\omega''' \ldots = \frac{(\theta + \theta' + \theta'')^2 - 4(\theta\theta' + \theta\theta'' + \theta'\theta'')}{256}. \end{aligned}$$

Все они рациональны в силу того, что координаты точки (η, η', η'') удовлетворяют условиям теоремы.

Теорема доказана полностью.

При доказательстве достаточности условий теоремы мы взяли точку ω, лежащую на плоскости нулевого следа, геометрически совпадающую со своей проекцией η, но только рассмотренную в других координатах. Равным образом мы могли бы взять любую параллельную ей точку $\omega + \frac{s}{4}$, лежащую на плоскости $\omega + \omega' + \omega'' + \omega''' = s$.

При рациональном s каждая такая точка, очевидно, принадлежит той же области, что и ω.

Теорема 2. *Для того чтобы точки* $(\eta_1, \eta_1', \eta_1'')$ *и* $(\eta_2, \eta_1', \eta_2'')$, *удовлетворяющие условиям теоремы 1, были проекциями точек одной и той же биквадратичной области, необходимо, чтобы точка* $(\eta_1\eta_2, \eta_1'\eta_2', \eta_1''\eta_2'')$ *принадлежала кубической области* U, *которой принадлежит* $(\eta_1^2, \eta_1'^2, \eta_1''^2)$. *Это условие также достаточно, если точка* $(\eta_1^2, \eta_1'^2, \eta_1''^2)$ *есть точка общего положения области* U.

Доказательство. Пусть ω_1 и ω_2 — две точки биквадратичной области, η_1 и η_2 — их проекции, θ_1 и θ_2 — квадраты проекций. Предположим сначала, что точка ω_1 является точкой общего положения. Тогда ω_2 можно представить в виде

$$\omega_2 = a\omega_1^3 + b\omega_1^2 + c\omega_1 + d$$

с рациональными коэффициентами a, b, c, d. Кроме того, без нарушения общности можно считать, что точка ω_1 находится в пространстве нулевого следа, так что уравнение, корнем которого является ω, имеет вид

$$\omega_1^4 + f_2\omega_1^2 - f_3\omega_1 + f_4 = 0.$$

Тогда квадрат проекции точки ω_1 удовлетворяет уравнению

$$\theta^3 + 8f_2\theta^2 + 16(f_2 - 4f_4)\theta - 64f_3^2 = 0,$$

и норма проекции $\eta_1\eta_1'\eta_1''$ равна $8f_3$.

Легко проверить непосредственным вычислением, что

$$\eta_2 = a\left(-\frac{\eta_1^3}{8} - \frac{3}{2}f_2\eta_1\right) + \frac{b}{2}\eta_1'\eta_1'' + c\eta_1,$$

откуда следует, что

$$\eta_1\eta_2 = -\frac{a}{8}\theta_1^2 + \left(-\frac{3}{2}af_2 + c\right)\theta_1 + 4bf_3;$$

это значит, что $\eta_1\eta_2$ принадлежит той же области, что и θ_1.

Если же ω_1 не является точкой общего положения, то в области T найдем точку ω общего положения, квадрат проекции которой является также точкой общего положения в своем пространстве. Такая точка ω, очевидно, существует. Обозначив через η и θ проекцию и квадрат проекции точки ω, мы будем иметь, что $\eta\eta_1$ и $\eta\eta_2$ принадлежат области, которой принадлежит θ. Но тогда той же области будет принадлежать и $\eta\eta_1\eta\eta_2 = \eta_1\eta_2\theta$, следовательно, и $\eta_1\eta_2$, так как θ не является делителем нуля. Тем самым теорема в части необходимости доказана.

Докажем теперь достаточность условия теоремы, в предположении, что $\theta_1 = \eta_1^2$ является точкой общего положения.

Пусть $\eta_1\eta_2$ принадлежит области, содержащей θ_1. Тогда $\eta_1\eta_2$ представляется в виде

$$\eta_1\eta_2 = \alpha\theta_1^2 + \beta\theta_1 + \gamma$$

с рациональными коэффициентами α, β, γ.

Пусть ω_1 — точка, проекцией которой является η_1. Очевидно, что

$$\omega_2 = -8\alpha\omega_1^3 + \frac{\gamma}{4f_3}\omega_1^2 + (\beta - 12\alpha f_2)\omega_1 + k$$

будет иметь своей проекцией η_2 при любом рациональном k. Это непосредственно следует из формул, приведенных при доказательстве необходимости.

Выражение для ω_2 имеет смысл при сделаниых предположениях, так как

$f_3=\frac{1}{8}\sqrt{\theta\theta'\theta''}\neq 0$, ибо точка $(\theta_1, \theta_1', \theta_1'')$ есть точка общего положения. Итак, ω_2 рационально выражается через ω_1, и, следовательно, ω_2 и ω_1 принадлежат одной и той же области. Теорема 2 доказана полностью.

§ 49. Решение задачи, обратной задаче Чирнгаузена, для двух уравнений 4-й степени

Заметим, что доказанные теоремы дают простой и удобный метод для решения задачи, обратной задаче преобразования Чирнгаузена для уравнений 4-й степенн. Действительно, пусть даны бнквадратичные числа ω_1 и ω_2, заданные своими уравненнями. Задача, обратная задаче преобразования Чирнгаузена, состоит в том, чтобы узнать, прнпадлежат ли заданные числа одной и той же области, и если да, то иайти выражение ω_2 через ω_1 или иаоборот. Для решения нужно составить уравнения для квадратов проекцнй точек ω_1 и ω_2 и решить для них задачу, обратную преобразованию Чиригаузена. Затем составить уравнение, которому удовлетворяет произведение $\theta_1\theta_2$ квадратов проекций. Если ω_1 и ω_2 принадлежат одной области, $\theta_1\theta_2$ должно оказаться полным квадратом. Посредством извлечения квадратного корня из кубического числа по способу, изложенному ранее, найдем произведение проекций $\eta_1\eta_2$. Представление $\eta_1\eta_2$ через θ_1 укажет нам подстановку, связывающую ω_2 с ω_1.

Пример. Решить задачу, обратную задаче преобразоваиия Чиригаузена, для уравнений

$$\omega_1^4-\omega_1-1=0, \quad \omega_2^4+\omega_2^3+5\omega_2^2-7\omega_2-1=0.$$

Решение. Составляем уравнения для квадратов проекций

$$\theta_1^3+64\theta_1-64=0; \qquad N(\eta_1)=+8,$$
$$\theta_2^3+37\theta_2^2+275\theta_2-75^2=0; \quad N(\eta_2)=+75.$$

Устанавливаем между ними преобразованне Чирнгаузена:

$$\theta_2=\frac{1}{2}\theta_1^2-\theta_1+9.$$

Составляем уравнение, корнем которого является

$$\mu=\theta_1\theta_2\doteq-\theta_1^2-23\theta_1+32,$$

$$\mu^3-7\cdot 32\mu^2+7\cdot 16^2\cdot 25\mu-8^2\cdot 75^2=0.$$

Ищем квадратиый кореиь ν из числа μ

$$\nu^3-s\cdot\nu^2+q\nu-8\cdot 75=0,$$
$$s^2-2q=7\cdot 32,$$
$$q^2-2\cdot 8\cdot 75s=7\cdot 16^2\cdot 25,$$

откуда, посредством простых вычислений, получаем:

$$s=28; \quad q=280.$$

Выражаем ν через θ_1:

$$\nu=4-\theta_1-\frac{\theta_1^2}{7}.$$

Отмечаем, что $\eta_1\eta_2=+\nu$, на основании знаков норм. Находим, наконец, подстановку, связывающую ω_2 с ω_1:

$$\omega_2=\omega_1^3+\omega_1^2-\omega_1+k.$$

Легко убедиться в том, что $k=1$. Задача решена.

§ 50. Свойства проекции максимальной решетки 4-го порядка

Переходим теперь к изучению проекции максимальной решетки 4-го порядка. Очевидно, что такая проекция представляет собой трехмерную решетку, точки которой удовлетворяют условиям теорем 1 и 2 параграфа 48 и, кроме того, имеют целые алгебраические координаты. Совокупность всех точек, рационально связанных с проекцией некоторой максимальной решетки и имеющих целые алгебраические координаты, мы обозначим через L. Нельзя утверждать, что все точки системы L являются проекциями целых точек соответствующей биквадратичной области, однако, точки системы $4L$ все являются проекциями целых точек, и, следовательно, $4L$ целиком входит в проекцию максимального кольца. Отсюда следует, что система $4L$, а следовательно, и L — дискретна. Эта последняя, очевидно, трехмерна и повторяется сложением и вычитанием и потому представляет собой решетку. Решетка L центрирует решетку $4L$ с индексом $4^3 = 64$. Проекция максимальной решетки содержится в решетке L и содержит в себе $4L$ и, следовательно, может центрировать решетку $4L$ с индексом 2^α, $0 \leqslant \alpha \leqslant 6$. Поэтому, если мы построим решетку L, задача о построении проекции максимальной решетки приводится к конечному числу испытаний.

Изучим глубже свойства решетки L.

Решетка L, очевидно, повторяется умножением на все целые точки кубической области, на которую опирается биквадратичная, и, следовательно, L подобна одной из решеток основной фигуры максимального кольца этой кубической области

$$L = \gamma\Gamma.$$

Квадрат решетки L образован *числами* кубической области U и повторяется умножением на все целые числа области, т. е. на все точки максимального кольца. Следовательно,

$$\Lambda = L^2 = \gamma^2\Gamma^2$$

представляет собой идеал максимального кольца. Этот идеал принадлежит классу K^{-2}, где K — класс, соответствующий решетке Γ. Переходный множитель $\lambda = \gamma^2$ является точкой решетки Γ^{-2}. Норма идеала Λ равна квадрату целого рационального числа, но идеал Λ не делится ни на один квадрат идеала, отличного от единичного. В противоположном случае решетку L можно было бы центрировать точками с целыми координатами, что противоречит определению решетки L.

Отсюда легко заключить, что идеал Λ может иметь только следующий вид разложения на простые идеалы:

$$\Lambda = \bar{\mathfrak{p}}_1\mathfrak{p}_1\bar{\mathfrak{p}}_2\mathfrak{p}_2 \dots \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{m}_1\bar{\mathfrak{m}}_1\mathfrak{m}_2\bar{\mathfrak{m}}_2 \dots,$$

где через $\mathfrak{p}$, $\bar{\mathfrak{p}}$ обозначены простые идеалы первого порядка, входящие попарно в разложение простых чисел, раскладывающихся на три различных простых идеала, через $\mathfrak{q}$ обозначены идеалы второго порядка и, наконец, через $\mathfrak{m}$, $\bar{\mathfrak{m}}$ обозначены идеалы, входящие в те простые делители дискриминанта, которые раскладываются на простые идеалы в виде $\mathfrak{m}^2\bar{\mathfrak{m}}$.

Норму идеала Λ можно поэтому представить в виде

$$N(\Lambda) = l^2 = k^2m^2,$$

где k^2 — произведение норм всех $\mathfrak{p}$, $\bar{\mathfrak{p}}$ и $\mathfrak{q}$ и m^2 — произведение норм всех $\mathfrak{m}$, $\bar{\mathfrak{m}}$. Числа k и m взаимно просты и не делятся ни на один квадрат простого числа. Кроме того, k взаимно просто с дискриминантом кубической области, и m состоит из простых чисел, входящих в дискриминант в первой степени,

за исключением, быть может, числа 2, которое может входить в дискриминант кубической области в кубе и тем не менее раскладываться на простые идеалы в виде $\mathfrak{m}^2\,\overline{\mathfrak{m}}$.

Множитель λ в равенстве

$$\Lambda = \lambda\Gamma^2$$

определен только с точностью до единиц максимального кольца кубической области. Однако множители λ, отличающиеся *квадратом* единицы, очевидно, определяют одну и ту же решетку L при подходящем выборе квадратного корня в равенстве $\gamma = \sqrt{\lambda}$. При извлечении корня в равенстве $\gamma = \sqrt{\lambda}$ мы можем, при данном λ, получить восемь различных значений для γ, так как при извлечении квадратного корня из каждой координаты мы можем брать два значения. Однако эти восемь значений определяют только четыре различных решетки L, так как множители $(\lambda, \lambda', \lambda'')$ и $(-\lambda, -\lambda', -\lambda'')$ определяют, очевидно, одну и ту же решетку L. И эти четыре решетки L будут связаны с одной и той же биквадратичной областью, только по-разному расположенной в пространстве четырех измерений.

Заметим также, что шесть решеток L, получающихся одна из другой осесовмещениями в пространстве трех измерений, также соответствуют одной и той же области четвертого порядка, различным образом расположенной в пространстве. Поэтому, желая строить решетки L для различных биквадратичных областей, мы должны останавливаться каждый раз на одном значении квадратного корня в равенстве $\gamma = \sqrt{\lambda}$ и не брать решеток L, получающихся одна из другой осесовмещениями.

Решетки L можно фактически строить, не обращаясь к пространству всех решеток основной фигуры кубической области, подобно тому как мы это делали при построении решеток L для кубических областей. Действительно, пусть K — класс идеалов, соответствующий решетке Γ и Λ — идеал класса K^{-2}, имеющий нужный нам вид разложения на простые идеалы. Возьмем идеал $\mathfrak{a}$ из класса K^{-1}. Решетка Γ будет подобна решетке идеала $\mathfrak{a}$. Идеал Λ будет подобен идеалу $\mathfrak{a}^2$

$$\Lambda = \mu\mathfrak{a}^2.$$

Коэффициент подобия μ представляет собой целое или дробное число кубической области, которые фактически можно найти. *При этом необходимо брать множитель μ, имеющий положительную норму*, что всегда можно сделать, умножив его в случае надобности на -1. Решетка L найдется из равенства

$$L = \sqrt{\mu}\cdot\mathfrak{a}.$$

§ 51. Построение максимальных решеток 4-го порядка по решеткам L

Обозначим через $\mathfrak{M}$ совокупность всех целых точек области T, проекции которых образуют решетку $4L$. Эта совокупность представляет собой решетку, состоящую из точек решетки $4L$, рассмотренных в четырехмерных координатах, и из параллельных им точек. Базис этой решетки образован числом 1 и базисом решетки $4L$, рассмотренной относительно четырехмерных осей координат, и, следовательно, легко находится. Максимальное кольцо центрирует решетку $\mathfrak{M}$ с индексом 2^α, $0 \leqslant \alpha \leqslant 6$. Однако, проведя более точное исследование, мы можем сузить возможности для центрировки, именно — показать, что $1 \leqslant \alpha \leqslant 4$. Этим вопросом мы сейчас и займемся.

Прежде всего докажем, что решетка $\mathfrak{M}$ представляет собой кольцо. Найдем для этого необходимые и достаточные условия того, чтобы проекция точки, заданной уравнением $\omega^4 - f_1\omega^3 + f_2\omega^2 - f_3\omega + f_4 = 0$, принадлежала решетке $4L$. Таким условием будет, очевидно, делимость всех координат квадрата проекции θ на 16.

Вспоминаем уравнение, корнем которого является θ:

$$\theta^3-(3f_1^2-8f_2)\theta^2+(3f_1^4-16f_1^2f_2+16f_2^2+16f_1f_3-64f_4)\theta-$$
$$-(f_1^3-4f_1f_2+8f_3)^2=0.$$

Таким образом, необходимым и достаточным условием является выполнение сравнений

$$3f_1^2-8f_2\equiv 0 \pmod{16},$$
$$3f_1^4-16f_1^2f_2+16f_2^2+16f_1f_3-64f_4\equiv 0 \pmod{16^2},$$
$$f_1^3-4f_1f_2+8f_3\equiv 0 \pmod{64}.$$

Из первого сравнения следует

$$f_1\equiv 0 \pmod 4;\quad f_2\equiv 0 \pmod 2.$$

Из третьего:

$$f_3\equiv 0 \pmod 4.$$

Принимая все это во внимание, можем переписать второе и третье сравнения в виде

$$\left(\frac{f_2}{2}\right)^2\equiv f_4 \pmod 4,$$

$$\frac{f_1}{4}\cdot\frac{f_2}{2}\equiv\frac{f_3}{4} \pmod 2,$$

откуда следуют две возможности:

A. $f_2\equiv 0 \pmod 4$; тогда $f_4\equiv 0 \pmod 4$; $f_3\equiv 0 \pmod 8$.
B. $f_2\equiv 2 \pmod 4$; тогда $f_4\equiv 1 \pmod 4$; $f_3\equiv f_1 \pmod 8$.

Таким образом, необходимым и достаточным условием для того, чтобы ω принадлежало решетке $\mathfrak{M}$, является выполнение одной из систем сравнений:

A)		B)	
$f_1\equiv 0$	$\pmod 4$,	$f_1\equiv 0$	$\pmod 4$,
$f_2\equiv 0$	$\pmod 4$,	$f_2\equiv 2$	$\pmod 4$,
$f_3\equiv 0$	$\pmod 8$,	$f_3\equiv f_1$	$\pmod 8$,
$f_4\equiv 0$	$\pmod 4$.	$f_4\equiv 1$	$\pmod 4$.

В соответствии с этим и все точки решетки $\mathfrak{M}$ разбиваются на два класса A и B, в зависимости от того, которая из систем сравнений удовлетворяется. Очевидно, что если ω принадлежит классу A, то $\omega+1$ принадлежит классу B и наоборот.

Легко проверить, что если ω принадлежит классу A, то $\frac{\omega^2}{2}$ принадлежит решетке $\mathfrak{M}$.

Действительно, пусть f_1', f_2', f_3', f_4' — коэффициенты уравнения, корнем которого является $\frac{\omega^2}{2}$. Они связаны с коэффициентами f_1, f_2, f_3, f_4 равенствами

$$f_1'=\frac{f_1^2-2f_2}{2}\equiv f_2 \pmod 8,$$
$$f_2'=\frac{f_2^2-2f_1f_3+2f_4}{4}\equiv\frac{f_4}{2} \pmod 4,$$
$$f_3'=\frac{f_3^2-2f_2f_4}{8}\equiv\frac{2f_4}{2} \pmod 8,$$
$$f_4'=\frac{1}{16}f_4^2.$$

Отсюда непосредственно следует, что если $f_4\equiv 4 \pmod 8$, то $\frac{\omega_1^2}{2}$ принадлежит

классу B, а если $f_4 \equiv 0 \pmod 8$, то $\frac{\omega_1^2}{2}$ принадлежит классу A, т. е. в обоих случаях $\frac{\omega_1^2}{2}$ принадлежит решетке $\mathfrak{M}$.

Легко видеть, что точки класса A образуют решетку.

Действительно, пусть ω_1 и ω_2 две точки класса A. Их разность должна принадлежать решетке $\mathfrak{M}$ и, следовательно, одному из классов A и B. Но $\omega_1 - \omega_2$ не может принадлежать классу B, так как $\frac{(\omega_1-\omega_2)^2}{2} = \frac{\omega_1^2}{2} + \frac{\omega_2^2}{2} - \omega_1\omega_2$ имеет целые координаты, в то время как половина квадрата точки класса B целых координат иметь не может.

Следовательно, совокупность точек класса A воспроизводится вычитанием и потому представляет собой решетку.

Теперь легко показать, что система $\mathfrak{M}$ является кольцом, т. е. повторяется умножением. Повторяемость умножением достаточно показать для точек класса A, так как

$$\omega_1\omega_2 = (\omega_1 + 1)\,\omega_2 - \omega_2 = \omega_1(\omega_2 + 1) - \omega_1 = (\omega_1 + 1)(\omega_2 + 1) - \omega_1 - \omega_2 - 1,$$

а одна из точек ω, $\omega + 1$ должна принадлежать классу A. Но

$$\omega_1\omega_2 = \frac{(\omega_1 + \omega_2)^2}{2} - \frac{\omega_1^2}{2} - \frac{\omega_2^2}{2}.$$

Если ω_1 и ω_2 принадлежат классу A, то этому же классу принадлежит $\omega_1 + \omega_2$. Мы уже знаем, что половина квадрата любой точки класса A принадлежит решетке $\mathfrak{M}$. Следовательно, $\omega_1\omega_2$ также принадлежит решетке $\mathfrak{M}$.

Итак, мы доказали, что решетка $\mathfrak{M}$ представляет собою кольцо. Легко видеть, что это кольцо не может быть максимальным. Действительно, его подрешетка A представляет собой идеал кольца $\mathfrak{M}$. Норма этого идеала равна 2, так как $\mathfrak{M}$ центрирует A с индексом 2. С другой стороны, квадрат каждой точки идеала A делится на 2. Эти два обстоятельства были бы несовместны одно с другим, если бы $\mathfrak{M}$ было максимальным кольцом.

Таким образом, максимальное кольцо должно центрировать кольцо $\mathfrak{M}$ по крайней мере с индексом 2.

Рассмотрим теперь проекцию максимального кольца с другой стороны. Все точки максимального кольца „параллельны" точкам, лежащим в „пространствах"

$$\omega + \omega' + \omega'' + \omega''' = 0, \qquad \omega + \omega' + \omega'' + \omega''' = 1,$$
$$\omega + \omega' + \omega'' + \omega''' = 2 \quad \text{и} \quad \omega + \omega' + \omega'' + \omega''' = 3$$

(т. е. отличаются от этих точек целыми рациональными слагаемыми). Следовательно, проекция максимального кольца получается в результате наложения проекций точек этих четырех „пространств". Эти проекции совпадать друг с другом, очевидно, не могут. Некоторые из них могут быть пустыми, но проекции непустых систем точек, лежащих в этих пространствах, будут конгруентны. Поэтому, проекция максимального кольца может или совпадать с результатом наложения проекций точек пространств $\omega + \omega' + \omega'' + \omega''' = 0$ и $\omega + \omega' + \omega'' + \omega''' = 2$ или центрировать его с индексом 2.

Но легко видеть, что все точки этих двух систем проектируются в точки решетки $2L$

Действительно, квадраты проекций таких точек будут делиться на 4. Это видно из выражений коэффициентов уравнения, корнем которого является θ:

$$3f_1^2 - 8f_2 \equiv 0 \pmod 4,$$
$$3f_1^4 - 16f_1^2f_2 + 16f_2^2 + 16f_1f_3 - 64f_4 \equiv 0 \pmod{16},$$
$$f_1^3 - 4f_1f_2 + 8f_3 \equiv 0 \pmod 8,$$

если только $f_1 \equiv 0 \pmod 2$, что имеет место для всех точек рассматриваемых нами двух пространств.

Решетка $2L$ центрирует решетку $4L$ с индексом 8, и, следовательно, проекция максимального кольца центрирует решетку $4L$, самое большее, с индексом 16. Соответственно, максимальное кольцо центрирует кольцо $\mathfrak{M}$, самое большее, с индексом 16.

Итак, мы доказали, что максимальное кольцо центрирует кольцо $\mathfrak{M}$ с индексом 2^α, $1 \leqslant \alpha \leqslant 4$.

Легко теперь подсчитать дискриминант кольца $\mathfrak{M}$ и максимального кольца.

Пусть $[(\lambda_1, \lambda_1', \lambda_1''), (\lambda_2, \lambda_2', \lambda_2''), (\lambda_3, \lambda_3', \lambda_3'')]$ — базис решетки L. Тогда, как мы видели, базис кольца $\mathfrak{M}$ будет задаваться точками

$$(1, 1, 1, 1),$$
$$(\lambda_1 + \lambda_1' + \lambda_1'', \lambda_1 - \lambda_1' - \lambda_1'', -\lambda_1 + \lambda_1' - \lambda_1'', -\lambda_1 - \lambda_1' + \lambda_1''),$$
$$(\lambda_2 + \lambda_2' + \lambda_2'', \lambda_2 - \lambda_2' - \lambda_2'', -\lambda_2 + \lambda_2' - \lambda_2'', -\lambda_2 - \lambda_2' + \lambda_2''),$$
$$(\lambda_3 + \lambda_3' + \lambda_3'', \lambda_3 - \lambda_3' - \lambda_3'', -\lambda_3 + \lambda_3' - \lambda_3'', -\lambda_3 - \lambda_3' + \lambda_3'').$$

Дискриминант кольца $\mathfrak{M}$ равен

$$\Delta(\mathfrak{M}) = \begin{vmatrix} 1, & \lambda_1 + \lambda_1' + \lambda_1'', & \lambda_2 + \lambda_2' + \lambda_2'', & \lambda_3 + \lambda_3' + \lambda_3'' \\ 1, & \lambda_1 - \lambda_1' - \lambda_1'', & \lambda_2 - \lambda_2' - \lambda_2'', & \lambda_3 - \lambda_3' - \lambda_3'' \\ 1, & -\lambda_1 + \lambda_1' - \lambda_1'', & -\lambda_2 + \lambda_2' - \lambda_2'', & -\lambda_3 + \lambda_3' - \lambda_3'' \\ 1, & -\lambda_1 - \lambda_1' + \lambda_1'', & -\lambda_2 - \lambda_2' + \lambda_2'', & -\lambda_3 - \lambda_3' + \lambda_3'' \end{vmatrix}^2 =$$

$$= \begin{vmatrix} 1, & 1, & 1, & 1 \\ 1, & 1, & -1, & -1 \\ 1, & -1, & 1, & -1 \\ 1, & -1, & -1, & 1 \end{vmatrix}^2 \cdot \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda_1 & \lambda_2 & \lambda_3 \\ 0 & \lambda_1' & \lambda_2' & \lambda_3' \\ 0 & \lambda_1'' & \lambda_2'' & \lambda_3'' \end{vmatrix}^2 =$$

$$= 256\, D(L) = 256\, D \cdot (N(\gamma))^2 = 256\, Dk^2m^2,$$

где $[N(\gamma)]^2 = N(\Lambda) = k^2m^2$.

Отсюда следует, что дискриминант максимального кольца равен

$$\Delta = 4^\alpha Dk^2m^2 \quad 0 \leqslant \alpha \leqslant 3.$$

Выведем некоторые следствия.

1. Δ может делиться самое большее на куб простого числа, отличного от 2 и 3. Наивысшей степенью 3 в дискриминанте Δ является 3^5, наивысшей степенью 2 в Δ является 2^{11}.

2. Дискриминанты биквадратичных областей, имеющих своей группой Галуа симметрическую группу, возрастают не быстрее чисел некоторой арифметической прогрессии.

Действительно, мы уже доказали аналогичную теорему для кубических областей. Над каждой же кубической областью можно построить биквадратичную с дискриминантом Δ, не превосходящим по абсолютной величине $64\,|D|$, где D — дискриминант кубической области. Для этого достаточно взять в качестве решетки Γ главную решетку и в качестве множителя λ основную единицу области. В следующем параграфе мы увидим, что построенная таким образом биквадратичная область будет иметь своей группой Галуа симметрическую группу.

Необходимо заметить, что биквадратичные области могут быть трех сигнатурных типов. Для двух из них дискриминант положителен, для третьего

отрицателен. При построении биквадратичных областей по кубическим отрицательного дискриминанта мы получаем биквадратичные отрицательного дискриминанта и, следовательно, определенного сигнатурного типа. При построении же биквадратичных областей по кубическим положительного дискриминанта мы можем получать биквадратичные области двух сигнатурных типов, и приведенный способ построения обеспечивает „медленное" возрастание дискриминанта для обоих типов, соединенных вместе. Несложным изменением рассуждения можно получить, что дискриминанты биквадратичных областей каждого из сигнатурных типов тоже возрастают не быстрее чисел некоторой арифметической прогрессии.

§ 52. Структура области 4-го порядка и кубической области, на которую она опирается, в зависимости от группы Галуа

Все что говорилось в предыдущем параграфе равным образом относилось к приводимым и неприводимым областям четвертого порядка, к приводимым и неприводимым кубическим областям, на которые опирались области 4-го порядка. Теперь займемся выяснением особенностей структуры биквадратичных областей и их проекций, обусловленных той или другой группой Галуа.

Группой Галуа биквадратичной области может быть любая группа перестановок четырех элементов. Таких групп может быть всего 11, если не считать различными те группы, которые переходят друг в друга при подходящем изменении нумерации переставляемых элементов, в данном случае координат точек области. Перечисляем все эти группы.

1. Симметрическая группа перестановок четырех элементов. Эту группу мы будем обозначать $\mathfrak{S}_4$. Ее порядок равен 24.

2. Совокупность перестановок, не меняющих элемента u и переставляющих всеми возможными способами элементы u', u'', u'''. Эту группу обозначаем $\mathfrak{S}_3$. Порядок ее равен 6.

3. Знакопеременная группа перестановок четырех элементов. Обозначаем ее $\mathfrak{A}_4$. Ее порядок равен 12.

4. Группа перестановок, не меняющих элемента u и *циклически* переставляющих u', u'', u'''. Эту группу обозначаем $\mathfrak{A}_3$. Ее порядок равен 3.

5. Группа восьмого порядка, образованная подстановками E (тождественная), (uu'), $(u''u''')$, $(uu')(u''u''')$, $(uu'')(u'u''')$, $(uu''')(u'u'')$, $(uu''u'u''')$, $(uu'''u'u'')$.

Эту группу обозначаем через $\mathfrak{G}$.

6. Группа четвертого порядка, образованная подстановками E, (uu'), $(u''u''')$, $(uu')(u''u''')$. Обозначаем ее $\mathfrak{V}$.

7. Группа второго порядка: E, (uu'). Обозначение: $\overline{Q}$.

8. Циклическая группа, образованная подстановками E, $(uu''u'u''')$, $(uu')\cdot(u''u''')$, $(uu'''u'u'')$. Обозначаем ее через $\mathfrak{C}$.

9. Vierergruppe $\overline{\mathfrak{V}}$, образованная элементами E, $(uu')(u''u''')$, $(uu'')(u'u''')$, $(uu''')(u'u'')$.

10. Группа второго порядка Q; E; $(uu')(u''u''')$.

11. Единичная группа E, состоящая из одной тождественной подстановки. Пять из этих групп $\mathfrak{S}_4$, $\mathfrak{A}$, $\mathfrak{G}$, $\mathfrak{C}$ и $\mathfrak{V}$ транзитивны и соответствуют неприводимым биквадратичным областям, остальные шесть $\mathfrak{S}_3$, $\mathfrak{A}_3$, $\overline{\mathfrak{V}}$, $\overline{Q}$, Q и E интранзитивны и соответствуют приводимым областям.

Дадим подробное описание областей, соответствующих всем этим группам, и выясним свойство их проекций.

1. $\mathfrak{S}_4$. Биквадратичная область неприводима и не имеет подобласти. Квадрат проекции принадлежит кубической области с симметрической группой, но сама проекция кубической области не принадлежит.

2. $\mathfrak{S}_3$. Биквадратичная область приводима и представляет собой прямую сумму областей первого порядка и кубической с симметрической группой.

Кубическая область, на которую опирается биквадратичная, одинакова с кубической областью, входящей в биквадратичную как прямое слагаемое. Не только квадрат проекции, но и сама проекция принадлежит этой кубической области.

3. $\mathfrak{A}_4$. Биквадратичная область неприводима и не имеет подобластей. Квадрат ее проекции принадлежит *циклической* кубической области, сама же проекция ей не принадлежит.

4. $\mathfrak{A}_8$. Биквадратичная область приводима и является прямой суммой области первого порядка и кубической циклической области. Кубическая область, на которую она опирается, одинакова с ее „прямым слагаемым". Не только квадрат проекции, но и сама проекция принадлежит этой области.

5. $\mathfrak{G}$. Биквадратичная область неприводима, имеет подобласть, расположенную на биссектрисе $u = u'$; $u'' = u'''$. Кубическая область, на которую она опирается, приводима и представляет собой прямую сумму области первого порядка и *неприводимой* квадратичной области. Соответственно проекция представляет собой прямую сумму некоторого линейного ряда и плоской совокупности точек. Линейный ряд представляет собой проекцию подобласти параллельно рациональному направлению на прямую, являющуюся линией пересечения пространства нулевого следа и биссектрисы, на которой расположена подобласть, а потому представляется в виде произведения производящего квадратного корня подобласти на совокупность всех целых рациональных чисел. Плоская же совокупность, входящая в проекцию „прямым слагаемым", представляет собой проекцию биквадратичной области параллельно подобласти. Квадрат этой проекции образует квадратичную область, входящую в кубическую область, на которую опирается биквадратичная, прямым слагаемым. В этом случае эта квадратичная область *отлична от подобласти.*

6. $\mathfrak{V}$. Биквадратичная область приводима и распадается на прямую сумму двух неприводимых различных квадратичных областей. Имеет *приводимую* квадратичную „подобласть" на биссектрисе $u = u'$; $u'' = u'''$.

Кубическая область, на которую опирается биквадратичная, приводима и представляется в виде прямой суммы области первого порядка и неприводимой квадратичной области. Проекция представляется в виде прямой суммы линейной совокупности рациональных чисел и проекции области параллельно „подобласти". Квадрат этой последней принадлежит квадратичной области, входящей в кубическую прямым слагаемым, но сама проекция параллельно подобласти вышеупомянутой квадратичной области не принадлежит.

7. $\overline{Q}$. Биквадратичная область приводима и распадается на прямую сумму двух областей первого порядка и одной квадратичной. Содержит приводимую квадратичную „подобласть" на биссектрисе $u = u'$; $u'' = u'''$. Про проекцию ее можно сказать то же самое, что и в предыдущем случае, с той только разницей, что проекция области параллельно подобласти сама принадлежит квадратичной области, входящей прямым слагаемым в кубическую, на которую опирается биквадратичная.

8. $\mathfrak{C}$. То же самое, что для $\mathfrak{G}$, с той только разницей, что квадратичная область, входящая прямым слагаемым в кубическую, на которую опирается биквадратичная, одинакова с подобластью этой последней.

9. $\mathfrak{V}$. Биквадратичная область неприводима и содержит три квадратичных подобласти на биссектрисах $u = u'$, $u'' = u'''$; $u = u''$, $u' = u'''$; $u = u'''$, $u' = u''$.

Кубическая область, на которую опирается биквадратичная, приводима на три прямых слагаемых, так что координаты всех точек квадрата проекции рациональны. Координаты же всех точек самой проекции все иррациональны (если только отличны от 0).

10. Q. Биквадратичная область приводима и распадается на прямую сумму двух *одинаковых* квадратичных областей. Кубическая область, на которую она опирается, распадается на прямую сумму трех областей первого порядка. Одна координата всех точек проекции рациональна, остальные две иррациональны;

11. *E*. Область приводима и распадается на прямую сумму четырех областей первого порядка. Все координаты проекции всех точек области рациональны.

Доказательства всех этих утверждений основаны на непосредственном применении самых элементарных соображений теории Галуа ко всем описанным частным случаям. Мы их не приводим, так как они заняли бы слишком много места.

Нас интересует главным образом построение неприводимых областей (группы $\mathfrak{S}_4$, $\mathfrak{A}_4$, $\mathfrak{S}$, $\mathfrak{E}$, $\mathfrak{B}$). Рассмотрим подробно, как строить решетки L для каждого из этих случаев.

1. $\mathfrak{S}_4$. При построении решетки L для этого случая мы должны исходить из кубической области с симметрической группой.

Выбираем в такой области некоторый класс идеалов K, соответствующий решетке Γ основной фигуры. Берем идеал $\mathfrak{a}$ в классе K^{-1}. Его решетка будет подобна решетке Γ. Возводим идеал $\mathfrak{a}$ в квадрат. В классе K^{-2} берем идеал Λ, имеющий необходимую форму разложения на простые идеалы, и находим множитель подобия идеалов $\mathfrak{a}^2$ и Λ:

$$\Lambda = \mu \mathfrak{v}^2.$$

При этом выбирается множитель, имеющий *положительную норму*. Решетка L получится по формуле

$$L = \sqrt{\mu} \cdot \mathfrak{a}.$$

Выбор знаков при извлечении корня безразличен. Остановившись на определенном классе K и выбрав определенный идеал Λ, можно получить две различных решетки L в случае $D<0$, за счет присоединения к множителю μ основной единицы, и четыре решетки L в случае $D>0$, за счет присоединения к μ единиц ε_1, ε_2, $\varepsilon_1\varepsilon_2$, где ε_1, ε_2 — основные единицы.

В случае если K — главный класс и $\Lambda=[1]$, и только в этом случае, одна из решеток L будет соответствовать приводимой области с группой γ_3. Именно в этом случае можно взять $\mathfrak{a}=[1]$, и при $\mu=1$ мы получим такую решетку L. Если же взять $\mu=\varepsilon$, где ε — одна из основных единиц, то мы получим решетку L для неприводимой области.

2. $\mathfrak{A}_4$. Исходим из кубической *циклической* области. Решетки L для биквадратичных областей с группой $\mathfrak{A}_4$ мы можем строить тем же приемом, что и для $\mathfrak{S}_4$. Однако благодаря тому, что кубическая циклическая область совмещается с собой при циклических осесовмещениях, мы, перебирая все возможные классы K и идеалы Λ, будем получать по три решетки L, соответствующие одной и той же биквадратичной области, по-разному расположенной в четырехмерном пространстве. Разберем подробнее, как этого избежать в различных, могущих представиться здесь, случаях.

α) $K \neq K'$ (через K' мы обозначаем класс, образованный идеалами, сопряженными с идеалами класса K).

В этом случае должно из трех классов K, K', K'' привлечь к построению решеток L только один, зато брать все возможные идеалы Λ и переходные множители μ, в том числе и сопряженные (в случае, если таковые принадлежат к одному классу).

β) $K=K'=K''$; $\Lambda \neq [1]$.

Легко видеть, что в этом случае $\Lambda \neq \Lambda'$, но Λ эквивалентен Λ' и Λ''. Нужно брать из трех идеалов Λ, Λ' и Λ'' только один, но зато брать все четыре возможные переходные множителя μ.

γ) $K=K'=K''$; $\Lambda=[1]$.

Это возможно только, если $K=K_0$ — главному классу, ибо, с одной стороны, $K^{-2}=K_0$, так как классу K^{-2} принадлежит главный идеал Λ, с другой стороны, $K^3=KK'K''=K_0$.

В этом случае можно взять $\mathfrak{a}=[1]$.

Переходные множители могут быть $\mu=1$, $\mu=\varepsilon_1$, $\mu=\varepsilon_2$ и $\mu=\varepsilon_1\varepsilon_2$, где ε_1, ε_2 — пара основных единиц области, $\mu=1$ определяет приводимую область с группой $\mathfrak{A}_3$, $\mu=\varepsilon_1$, ε_1 и $\varepsilon_1\varepsilon_2$ дают решетки L, соответствующие одной и той же биквадратичной области. Это вытекает из того, что за основные единицы циклической области можно принять подходящим образом подобранные сопряженные единицы ε и ε'. Тогда и $\varepsilon_1\varepsilon_2=\varepsilon''(\varepsilon'')^{-2}$ множителем, равным квадрату единицы, отличается от третьего сопряженного числа.

Заметим также одну особенность разложения идеала Λ на простые идеалы. В циклическом максимальном кольце не существует идеалов второго порядка и делителей дискриминанта, имеющих разложение $\mathfrak{m}^2\bar{\mathfrak{m}}$. Простые идеалы первого порядка, входящие в одно и то же простое число, сопряжены друг с другом. Поэтому $\Lambda=\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_2\mathfrak{p}_2'\ldots$

3. Построение областей с группами $\mathfrak{S}$ и $\mathfrak{C}$. В обоих этих случаях нужно базироваться на приводимой кубической области, распадающейся на прямую сумму области первого порядка и области второго порядка

$$U=U_1\oplus U_2.$$

Рассмотрим подробнее вид идеала Λ.

$$\Lambda=\mathfrak{p}_1\bar{\mathfrak{p}}_1\mathfrak{p}_2\bar{\mathfrak{p}}_2\ldots\ \mathfrak{q}_1\mathfrak{q}_2\ldots\ \mathfrak{m}_1\bar{\mathfrak{m}}_1\mathfrak{m}_2\bar{\mathfrak{m}}_2\ldots$$

В приводимой области идеалы второго порядка представляются в виде $[1]\oplus[p]$, где p — неразложимое в квадратичной области U_2 простое число. Идеалы первого порядка, обозначенные через p, могут быть двух сортов

$$[p]\oplus[1]\quad\text{и}\quad[1]\oplus[\pi],$$

где π — простой идеал первого порядка квадратичной области U_2. В простое число, раскладывающееся в кубической области U на три различных простых идеала, входит один из идеалов первого сорта, два второго. Поэтому произведения $\mathfrak{p}\bar{\mathfrak{p}}$, входящие в идеал Λ, могут быть двух сортов. Именно, некоторые из них имеют вид $[p]\oplus[\pi]$, другие — $[1]\oplus[\pi\pi']=[1]\oplus[p]$.

Идеалы $\mathfrak{m}$ имеют вид $[q]\oplus[1]$ и $[1]\oplus\mu$, где $[q]=\mu^2$ — простой делитель дискриминанта области U_2. Произведения $\mathfrak{m}\bar{\mathfrak{m}}$ имеют вид $[q]\oplus\mu$. Сопоставляя все сказанное, получим

$$\Lambda=[k_1m]\oplus k_2\mathfrak{l},$$

где $\mathfrak{l}$ — идеал квадратичной области U_2, норма которого равна k_1m, k_1 и k_2 взаимно просты между собой и с дискриминантом U_2, m входит в дискриминант. Все три числа m, k_1 и k_2 не делятся ни на один квадрат простого числа.

Легко видеть, что идеал $\mathfrak{l}$ должен принадлежать классу K^{-2}, равному квадрату некоторого другого класса K^{-1}. Это необходимо для того, чтобы такое же условие выполнялось для идеала Λ.

Пусть $\mathfrak{l}=\gamma\mathfrak{a}^2$, где $\mathfrak{a}$ — некоторый идеал класса K^{-1}, γ — переходной множитель. Тогда

$$\Lambda=\lambda([1]\oplus\mathfrak{a})^2,$$

где

$$\lambda=\pm k_1m\oplus k_2\gamma.$$

Знак в первой компоненте множителя λ нужно брать одинаковым со знаком нормы γ с тем расчетом, чтобы „трехмерная“ норма множителя γ была положительна. $\sqrt{\pm k_1m}$ представляет собой производящее число подобласти конструируемой биквадратичной области. Отсюда следует, что при нашем построении приводимые области могут получаться только в случае $\mathfrak{l}=[1]$ и

$N(\gamma)>0$, циклические области только в случае $\mathfrak{l}=[\sqrt{b}]$ и $bN(\gamma)>0$, где b — производящее число квадратичной области U_2. В остальных случаях будут получаться области с группой $\mathfrak{G}$.

При данном классе K и данном идеале $\mathfrak{l}$ можно получать еще различные решетки L за счет присоединения единиц к множителю γ. Если дискриминант области U_2 отрицателен, различных решеток L можно построить две посредством множителей γ и $-\gamma$ (γ и $i\gamma$ для $D=-4$). Если дискриминант области U_2 положителен, различных решеток L можно построить четыре посредством множителей $\pm\gamma$, $\pm\gamma\varepsilon_0$, где ε_0 — основная единица области.

В большинстве случаев при этих значениях получаются решетки L для различных биквадратичных областей, но некоторые случаи представляют исключения. Перечислим все случаи, которые могут здесь представиться.

1. $K\neq K'$. Для построения решеток для различных биквадратичных областей из двух классов K и K' достаточно взять один, но при этом необходимо взять все возможные идеалы $\mathfrak{l}$ и все переходные множители.

2. $K=K'$, $\mathfrak{l}\neq\mathfrak{l}'$. Из двух идеалов $\mathfrak{l}$ и $\mathfrak{l}'$ достаточно взять один, но переходные множители должно перебрать все.

3. $K=K'$, $\mathfrak{l}=\mathfrak{l}'$. Этот случай самый сложный.

В этом случае, так же как и в предыдущем, идеал $\mathfrak{l}$ может быть только главным идеалом

$$\mathfrak{l}=\lambda\cdot[1].$$

Так как $\mathfrak{l}=\mathfrak{l}'$, числа λ и λ' должны быть ассоциированные. Идеал $\mathfrak{l}$ должен быть делителем дискриминанта. Квадрат идеала $\mathfrak{l}$ есть главный идеал, построенный на целом рациональном числе. Если дискриминант области U_2 отрицателен или если основная единица области имеет отрицательную норму, λ может равняться 1 или $\sqrt{b}$. Если же дискриминант положителен и норма основной единицы положительна, есть еще две возможности. При этих возможностях $\lambda'=\pm\varepsilon_0\lambda$ (для одной возможности $+$, для другой $-$).

Пусть $\mathfrak{a}$ какой-либо идеал класса K^{-1}. Тогда $\mathfrak{a}^2=a[1]$, так как $\mathfrak{a}^2$ — главный идеал.

Обозначим норму $\mathfrak{a}$ через a. Тогда $N(a)=\pm a^2$ и $\mathfrak{a}'=\frac{a}{\mathfrak{a}}\mathfrak{a}$. Отсюда следует, что

$$\mathfrak{l}=\frac{\lambda}{a}\mathfrak{a}^2.$$

Обозначим через L_1 решетку $\sqrt{\frac{\lambda}{a}}\mathfrak{a}$. Если L_1 и L_1' — сопряженные решетки, то соответствующие им решетки L также сопряжены. Но

$$L_1'=\sqrt{\frac{\lambda'}{a'}}\mathfrak{u}'=\sqrt{\frac{\lambda'}{a'}\cdot\frac{a^2}{a^2}}\mathfrak{u}=\sqrt{\frac{\lambda'}{\lambda}}\sqrt{\pm\frac{\lambda}{a}}\mathfrak{a}=\sqrt{\pm\frac{\lambda'}{\lambda}}L_1.$$

Знаки $\pm$ под корнем находятся в соответствии с знаком нормы a.

Если $\lambda=1$ и $N(a)=+a^2$, то $L_1'=L_1$, но в этом случае соответствующая биквадратичная область приводима, и этот случай для нас не интересен.

Если $\lambda=1$ и $N(a)=-a^2$, то $L_1'=L_1\cdot\sqrt{-1}$; это значит, что присоединение множителя -1 к a меняет решетку L, но переводит в сопряженную и, следовательно, соответствующую той же биквадратичной области.

Если $\lambda=\sqrt{b}$ и $N(a)=+a^2$, то $L_1'=L_1\sqrt{-1}$, и имеет место то же самое, что в предыдущем случае.

Если $\lambda=\sqrt{b}$ и $N(a)=a^2$, то биквадратичная область имеет своей группой группу $\mathfrak{G}$.

Решетки L и L' в этом случае одинаковы; следовательно, присоединение -1 к множителю a меняет решетку L и соответствующую ей биквадратичную область.

Наконец, если $\lambda' = \varepsilon_0 \lambda$, то в зависимости от знака $N(\alpha)$ присоединение единицы $+\varepsilon_0$ или $-\varepsilon_0$ к множителю α не меняет биквадратичной области.

Таким образом, мы дали способ построения решеток L и в этом случае, причем выяснили до конца вопрос о том, когда получаются решетки L, соответствующие различным биквадратичным областям.

Заметим, что биквадратичные области с циклической группой могут быть построены не над любыми приводимыми кубическими областями. Мы видели, что для того, чтобы можно было над приводимой кубической областью построить биквадратичную область с циклической группой, необходимо и достаточно, чтобы в квадратичной составляющей кубической области нашлось число α *с отрицательной нормой*, такое, что главный идеал $[\alpha]$ был бы равен квадрату другого идеала.

Такое число может существовать только в квадратичных областях положительного дискриминанта, производящее число которого представляется в виде суммы двух квадратов.

4. Построение областей с группой $\mathfrak{V}$.

Эти области опираются на приводимую на три области первой степени кубическую область.

Легко видеть, что идеал Λ представляется в виде

$$\Lambda = [k_1] \oplus [k_2] \oplus [k_3] = (k_1, k_2, k_3), \qquad [1]$$

где целые числа k_1, k_2, k_3 — не делящиеся на квадрат ни одного простого числа, произведение которых есть полный квадрат. Четыре единицы с положительной нормой (1, 1, 1) (1, — 1, — 1), (— 1, 1, — 1) и (— 1, — 1, 1) при присоединении к переходному множителю (k_1, k_2, k_3) определяют разные биквадратичные области, если ни одно из чисел k_1, k_2, k_3 не равно единице. Если же $k_1 = 1$, то $k_2 = k_3$. Множители $(1, k_2, k_2)$ и $(1, -k_2, -k_2)$ определяют приводимые области, множители $(-1, k_2, -k_2)$ и $(-1, -k_2, k_2)$ определяют одну и ту же область с группой $\mathfrak{V}$, но по-разному расположенную.

§ 53. Другой способ построения областей 4-го порядка с группами $\mathfrak{G}$, $\mathfrak{C}$ и $\mathfrak{V}$

Кроме способа построения биквадратичных областей с группами $\mathfrak{G}$, $\mathfrak{C}$ и $\mathfrak{V}$, описанного в конце предыдущего параграфа, можно указать другой, более простой и удобный способ.

Заметим, что предшествующий способ в сущности был основан на проектировании области параллельно подобласти, так как все вычисления нами производились в квадратичной компоненте приводимой кубической области; первая же компонента не играла никакой роли. Второй способ, которым мы хотим теперь заняться, основан также на проектировании области параллельно подобласти.

Сначала для простоты предположим биквадратичную область чисто вещественной. Координаты проекции точки (u, u', u'', u''') параллельно подобласти $u = u'$, $u'' = u'''$ равны, как мы видели раньше, числам $u - u' + u'' - u'''$ и $u - u' - u'' + u'''$ при подходящем выборе осей координат. Повернем оси координат в проекции на угол в 45° и изменим масштаб в $\sqrt{2}$ раз. Мы получим для проекции точки (u, u', u'', u''') координаты $\eta = u - u'$; $\bar{\eta} = u'' - u'''$.

В этом параграфе точку с координатами η, $\bar{\eta}$ мы и будем называть проекцией точки (u, u', u'', u''') параллельно подобласти.

Очевидно, что при перестановках группы $\mathfrak{G}$ проекция подвергается преобразованиям:

$$\begin{array}{cccc} \eta \to \eta; & \eta \to -\eta; & \eta \to \bar{\eta}; & \eta \to -\bar{\eta}; \\ \bar{\eta} \to \bar{\eta} & \bar{\eta} \to \bar{\eta} & \bar{\eta} \to -\bar{\eta} & \bar{\eta} \to -\bar{\eta} \\ \eta \to \bar{\eta}; & \eta \to \bar{\eta}; & \eta \to -\bar{\eta}; & \eta \to -\bar{\eta}. \\ \bar{\eta} \to \eta & \bar{\eta} \to -\eta & \bar{\eta} \to \eta & \bar{\eta} \to -\eta \end{array}$$

Подстановки группы $\mathfrak{V}$ индуцируют преобразования:

$$\begin{matrix}\eta\to\eta\\ \bar\eta\to\bar\eta\end{matrix};\quad \begin{matrix}\eta\to-\eta\\ \bar\eta\to-\bar\eta\end{matrix};\quad \begin{matrix}\eta\to\bar\eta\\ \bar\eta\to\eta\end{matrix};\quad \begin{matrix}\eta\to-\bar\eta\\ \bar\eta\to-\eta\end{matrix}.$$

Подстановки группы $\mathfrak{E}$ индуцируют преобразования:

$$\begin{matrix}\eta\to\eta\\ \bar\eta\to\bar\eta\end{matrix};\quad \begin{matrix}\eta\to\bar\eta\\ \bar\eta\to-\eta\end{matrix};\quad \begin{matrix}\eta\to-\eta\\ \bar\eta\to-\bar\eta\end{matrix};\quad \begin{matrix}\eta\to-\bar\eta\\ \bar\eta\to-\eta\end{matrix}.$$

Отсюда следует, что квадрат проекции $(\theta, \bar\theta)$ принадлежит некоторой квадратичной области, именно подобласти биквадратичной области T, что легко видеть.

В случае, если группа Галуа равна $\mathfrak{V}$, то $\eta\bar\eta$ рациональна.

Если же группа Галуа равна $\mathfrak{E}$, то $\eta\bar\eta$ при перестановках группы меняет знак, так же как $\eta^2-\bar\eta^2$, откуда следует, что $\eta\bar\eta=\sqrt{b}\cdot r$, где b — производящее число квадратичной области и r — рациональное число.

Далее, очевидно, что отношение проекций двух различных точек одной и той же области перемещается при перестановках групп Галуа так же, как координаты квадратов проекций, откуда следует, что такое отношение принадлежит подобласти. Обратно, если η проекция биквадратичного числа и α число подобласти, то $\eta\alpha$ снова является проекцией биквадратичного числа той же области.

Будем проектировать биквадратичное максимальное кольцо. В проекции мы получим плоскую решетку точек, каждая из которых имеет целые алгебраические координаты. Введем в рассмотрение решетку L — совокупность всех точек, рационально связанных с проекцией максимального кольца и имеющих целые алгебраические координаты. Решетка L содержит в себе проекцию максимального кольца, которое в свою очередь содержится в решетке $2L$. Действительно, точка $(\eta, \bar\eta)$ имеет четырехмерные координаты $\omega, \omega', \omega'', \omega'''$, которые находятся из уравнений

$$\omega-\omega'=\eta,\quad \omega''-\omega'''=\bar\eta,$$
$$\omega+\omega'=0,\quad \omega''+\omega'''=0,$$

откуда $\omega=\frac{1}{2}\eta,\quad \omega'=-\frac{1}{2}\eta,\quad \omega''=\frac{1}{2}\bar\eta,\quad \omega'''=-\frac{1}{2}\bar\eta.$

Если $(\eta, \bar\eta)$ принадлежат решетке $2L$, то она относительно четырехмерных осей имеет целые алгебраические координаты $\omega, \omega', \omega'', \omega'''$ и, следовательно, принадлежит максимальному кольцу. Решетка L подобна одной из решеток основной фигуры максимального кольца квадратичной области, так как повторяется умножением на все точки максимального кольца:

$$L=\gamma\Gamma.$$

Решетка $\Lambda=L^2$ представляет собой идеал квадратичной области, не делящийся ни на один квадрат простого идеала и принадлежащий классу идеалов, являющемуся квадратом некоторого другого класса.

Разложение идеала Λ на простые идеалы дает:

$$\Lambda=\mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{m}_1\mathfrak{m}_2\dots=k_1\mathfrak{l},$$

где k_1 — целое рациональное число, взаимно простое с дискриминантом квадратичной области и не делящееся на квадрат ни одного простого числа; идеал же $\mathfrak{l}$ имеет норму, взаимно простую с k_1 и не делящуюся на квадрат ни одного простого числа.

В остальном идеал $\mathfrak{l}$ совершенно произволен.

Задавшись идеалом Λ и классом K, соответствующим решетке Γ, которой подобна решетка L, легко построить решетку L. Возьмем произвольный идеал $\mathfrak{a}$, принадлежащий классу K^{-1}. Решетка идеала $\mathfrak{a}$ будет подобна решетке Γ. Затем найдем множитель μ в равенстве

$$\Lambda = \mu \mathfrak{a}^2.$$

Такой множитель найдется, так как идеал Λ эквивалентен идеалу $\mathfrak{a}^2$. Тогда решетка L определится по формуле

$$L = \sqrt{\mu} \cdot \mathfrak{a}.$$

Выбор знаков при извлечении корня из μ безразличен.

Решетка L для приводимой биквадратичной области будет получаться в том и только в том случае, если $\sqrt{\mu}$ принадлежит квадратичной области. Это возможно только в случае, если K — главный класс и $\Lambda = [1]$. В этом случае можно взять $\mathfrak{a} = [1]$. Если при этом взять $\mu = 1$, то мы получим решетку L для приводимой области. Если взять $\mu = -1$ или $\mu = +\varepsilon_0$, где ε_0 — основная единица области, то мы получим решетки L для неприводимых областей.

Области с группой $\mathfrak{B}$ мы будем получать в том и только в том случае, если $\Lambda = [k]$ и $N(\mu) > 0$. Области с группой $\mathfrak{C}$ мы будем получать в том и только в том случае, если $\Lambda = [k\sqrt{b}]$ и $N(\mu) > 0$. Присоединение единиц к миожителю μ влияет при этом способе совершенно аналогично тому, как в предыдущем способе, и поэтому мы ие будем перечислять всех могущих представиться здесь случаев.

Построение максимального биквадратичного кольца по решетке L в этом способе проще, чем в предыдущем, благодаря тому, что его проекция может центрировать решетку $2L$ только с индексами 1, 2 и 4, так что для разыскания базиса максимального кольца приходится делать меньшее количество испытаний.

Совокупность всех точек максимального кольца, проектирующихся в решетку $2L$, обозначим через $\mathfrak{M}$. Можно доказать, что решетка $\mathfrak{M}$ представляет собой кольцо.

Дискриминант кольца $\mathfrak{M}$ равен

$$16d^2l,$$

где d — дискриминант квадратичной области, $l = N(\Lambda)$, причем l берется со знаком иормы множителя μ в равенстве $\Lambda = \mu \mathfrak{a}^2$.

Следовательно, дискриминант максимального кольца равен $16d^2l$, $4d^2l$ или d^2l.

В заключение рассмотрим несколько примеров.

Пример 1. Построить биквадратичные области над областью $R(\rho)$, ρ задано уравнением $\rho^3 + \rho - 1 = 0$.

Данная кубическая область есть область с симметрической группой, дискриминант ее максимального кольца равен — 31, число классов идеалов равно 1, базис максимального кольца образован числами 1, ρ, ρ^2, основная единица равна ρ. Наименьшие простые числа имеют следующие разложения: 2 — простое, $3 = \mathfrak{p}_3\mathfrak{q}_3 = (\rho + 1)(\rho^2 - \rho + 2)$, 5 — простое, 7 — простое.

Построим биквадратичные области, исходя из $\Lambda = [1]$ и $\Lambda = \mathfrak{q}_3 = [\rho^2 - \rho + 2]$.

В первом случае в равенстве $\Lambda = \mu[1]^2$ можно взять

$$\mu = \varepsilon_0 = \rho.$$

Во втором случае в равенстве $\Lambda = \mu[1]^2$ можно взять

$$\mu = \rho^2 - \rho + 2 \text{ и } \mu = -\rho^2 + \rho + 1.$$

Для первого случая базис кольца $\mathfrak{M}$ будет

$$1, \quad \omega_1, \quad \frac{\omega_1^2}{2}, \quad \frac{\omega_1^3}{2},$$

где ω_1 — корень уравнения

$$\omega_1^4 - 8\omega_1 - 4 = 0.$$

Базис максимального кольца будет

$$1, \quad \omega_1, \quad \frac{\omega_1^2}{2}, \quad \frac{\omega_1^3}{4} + \frac{\omega_1}{2}.$$

Дискриминант максимального кольца равен $-64 \cdot 31$.

Для остальных случаев максимальными кольцами будут два кольца с базисами

$$1, \omega, \frac{\omega^2}{2}, \quad \frac{\omega^3}{4} + \frac{\omega}{2}, \text{ где } \omega^4 - 8\omega^2 - 24\omega - 20 = 0,$$

$$1, \omega, \frac{\omega^2}{2}, \quad \frac{\omega^3}{4}, \text{ где } \omega^4 + 4\omega^3 - 4\omega^2 - 40\omega - 56 = 0.$$

Дискриминант в обоих случаях равен $-64 \cdot 9 \cdot 31$.

Пример 2. Построить циклические биквадратичные области над областью $R(\sqrt{5})$.

Обращаемся ко второму способу построения. Идеал Λ должен иметь вид $\Lambda = k[\sqrt{5}]$, где k — любое целое рациональное число, взаимно простое с 5. В области $R(\sqrt{5})$ существует только один класс идеалов — главный класс. Основная единица области $\varepsilon = \frac{1+\sqrt{5}}{2}$ имеет отрицательную норму. Переходный множитель в равенстве

$$\Lambda = \mu[1]$$

мы должны брать имеющим положительную норму и, следовательно, равным $\pm k\varepsilon\sqrt{5} = k_1\varepsilon\sqrt{5}$, где k_1 может быть положительным или отрицательным.

Максимальное кольцо имеет базис

$$1, \varepsilon, \sqrt{k_1\varepsilon\sqrt{5}}, \qquad \varepsilon\sqrt{k_1\varepsilon\sqrt{5}}, \quad \text{если } k_1 \not\equiv 3 \pmod 4,$$

и его дискриминант равен $16 \cdot 5^3 \cdot k_1^2$.

Максимальное кольцо имеет базис

$$1, \varepsilon, \frac{\sqrt{k_1\varepsilon\sqrt{5}} + 1 + \varepsilon}{2}, \quad \frac{\varepsilon\sqrt{\sqrt{5}\varepsilon k_1} + 1}{2}, \text{ если } k_1 \equiv 3 \pmod 4$$

и его дискриминант равен $5^3 \cdot k_1^2$.

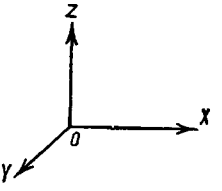
ГЛАВА IV

АЛГОРИФМ ВОРОНОГО

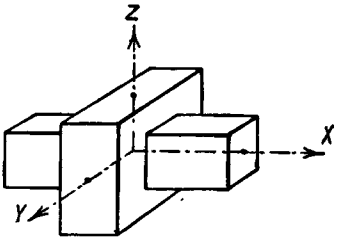
А. СЛУЧАЙ $D > 0$

§ 54. Цепочки относительных минимумов

В гл. I мы видели, что в некоторых вопросах, связанных с теорией решеток, повторяющихся умножением, играет большую роль расположение так называемых относительных минимумов решеток. Под этим названием мы подразумевали точки решетки, обладающие тем свойством, что норменное тело, построенное на каждой из них, пусто внутри и на границе от других точек решетки, кроме начала координат. В этой главе мы выясним до конца для случая $n=3$ вопрос об отыскании цепочек относительных минимумов и дадим методы для практического решения задачи о подобии двух решеток и задачи об автоморфизмах умножения решетки в том виде, с незначительными изменениями, как это было сделано Г. Ф. Вороным в его докторской диссертации. При этом, конечно, нам придется рассмотреть порознь случай вещественной и комплексной решеток. Мы начнем с первого, более сложного, случая вещественной решетки. При этом мы ограничимся рассмотрением решеток, не содержащих делителей нуля.



Черт. 10.



Черт. 11.

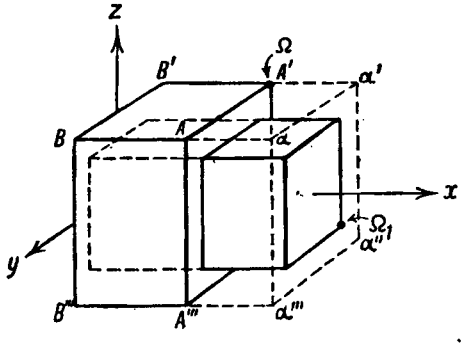
В этом случае норменное тело, построенное на точке, имеет вид прямоугольного параллелепипеда с центром в начале координат и с гранями, параллельными координатным плоскостям. Взятая точка находится в одной из вершин норменного параллелепипеда. Относительным минимумом в этом случае будет точка, норменный параллелепипед которой пуст внутри и на границе от точек решетки (кроме точки O). Мы будем часто называть относительным минимумом не только точку решетки, но и построенный на ней норменный параллелепипед.

В дальнейшем нам придется много раз сравнивать между собой такие параллелепипеды, поэтому мы введем термины, которые облегчат изложение. Будем характеризовать словами „длиннее“ и „короче“, „шире“ и „уже“, „выше“ и „ниже“ результаты сравнения параллелепипедов в направлениях, соответствующих осям OX, OY, OZ, расположение которых будем представлять себе согласно черт. 10.

Два данных норменных параллелепипеда могут быть расположены один относительно другого двумя существенно различными способами, именно их поверхности могут не пересекаться или пересекаться. В первом случае один параллелепипед заключен внутри другого. Во втором случае у одного из параллелепипедов *одно* измерение будет больше, а два измерения меньше, чем у второго параллелепипеда. В этом случае мы будем называть первый парал-

лелепипед *пронизывающим* второй, а второй — *охватывающим* первый. В случае надобности будем указывать направление, в котором происходит пронизывание или охватывание. Так, на черт. 11 параллелепипед Ω пронизывает параллелепипед T в направлении OX, а параллелепипед T охватывает параллелепипед Ω в направлении OX.

Относительным минимумом, смежным по OX с данным относительным минимумом Ω, мы будем называть самый короткий из относительных минимумов, пронизывающих по OX относительный минимум Ω. Осуществить построение смежного по OX относительного минимума для данного относительного минимума Ω можно следующим образом (черт. 12). Построив норменный параллелепипед на Ω, будем двигать его правую грань $AA'A''A'''$, перемещая ее центр в положительном направлении OX и оставляя ее параллельной плоскости YOZ. Первая точка решетки, которую встретит грань при этом движении, будет, очевидно, относительным минимумом, ибо построенный и на ней норменный параллелепипед будет содержаться внутри пустого параллелепипеда $BB'B''B'''aa'a''a'''$, и это будет смежный по OX с Ω относительный минимум. Что грань $AA'A''A'''$ обязательно встретит точку решетки, непосредственно вытекает из теоремы Минковского об объеме пустого центрально-симметрического выпуклого тела. Таким образом, для данного относительного минимума Ω существует смежный по OX относительный минимум Ω_1. Для Ω_1 в свою очередь существует смежный с ним по OX относительный минимум Ω и т. д.



Черт. 12.

Последовательность относительных минимумов $\Omega, \Omega_1, \Omega_2, \ldots$, в которой каждый последующий является смежным по OX для предыдущего, будем называть цепочкой относительных минимумов по OX или, короче, x-цепочкой, порожденной точкой Ω. Обозначать x-цепочку, порожденную точкой Ω, мы будем $\{\Omega\}_x$.

Аналогично понятию относительного минимума, смежного по OX, введем понятие смежного по OY и смежного по OZ относительного минимума. Из смежных по OY относительных минимумов могут быть составлены y-цепочки, из смежных по OZ — z-цепочки. Введенные нами понятия относительных минимумов и цепочек относительных минимумов естественно обобщают эти же понятия для плоских решеток. (См., например, статью о геометрии квадратичных форм, приложенную в конце русского перевода книги П. Л. Дирихле „Лекции по теории чисел".) Однако, в нашем случае имеется одно существенное отличие от случая плоских решеток. Для плоских решеток каждый относительный минимум может рассматриваться как смежный по OX для некоторого другого. Благодаря этому цепочка относительных минимумов может быть бесконечно продолжена в обе стороны. В пространственном же случае возможно, что данный относительный минимум является смежным по OX сразу для нескольких различных относительных минимумов или не является смежным по OX ни для одного.

Подтвердим это примерами.

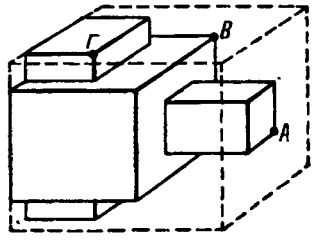
Пусть координатные параллелепипеды трех точек A, B и Γ, принадлежащих некоторой решетке, расположены так, что параллелепипед A пронизывает по OX параллелепипеды B и Γ, которые в свою очередь не пронизывают друг друга по OX, и кроме того, координатный параллелепипед, ограниченный наиболее удаленными от координатных плоскостей гранями параллелепипедов A, B и Γ, пуст внутри от точек решетки (кроме начала координат). Тогда A, B

и Γ, очевидно, суть относительные минимумы решетки, и A является смежным по OX одновременно для относительных минимумов B и Γ (черт. 13).

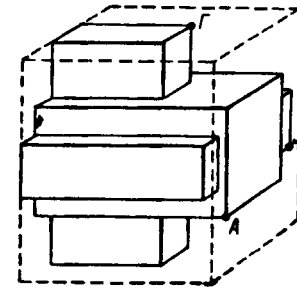
Если же параллелепипеды B и Γ пронизывают параллелепипед A в направлениях OY и OZ, и координатный параллелепипед, ограниченный наиболее удаленными от координатных плоскостей гранями параллелепипедов A, B и Γ, пуст внутри от точек решетки, то A, очевидно, являясь относительным минимумом, не может быть смежным по OX ни для одного, ни для другого относительного минимума (черт. 14).

Действительно, пусть A был бы смежным по OX для некоторого относительного минимума Ω.

Представлялись бы возможными следующие три случая.



Черт. 13.



Черт. 14.

1. Ω выше Γ. Кроме того, Ω шире Γ, так как Ω шире A и A шире Γ. Следовательно, Ω должен быть короче Γ, ибо иначе Ω не был бы относительным минимумом. Но тогда A не может быть смежным по OX с Ω, так как правая грань Ω при своем движении направо встретила бы точку Γ раньше точки A. Следовательно, эта возможность отпадает.

2. Ω шире B. Отпадает, аналогично предыдущей возможности.

3. Ω ниже Γ и уже B. Это невозможно, так как кроме того Ω короче A. В этом случае весь параллелепипед Ω содержался бы внутри параллелепипеда, ограниченного самыми удаленными от координатных плоскостей гранями параллелепипедов A, B, Γ, который, по предположению, пуст внутри от точек решетки.

Покажем, что можно на самом деле подобрать точки, удовлетворяющие требованиям для обоих примеров.

Возьмем точки с координатами $A(1, \alpha, -\beta)$; $B(-\gamma, 1, \delta)$ и $\Gamma(\varepsilon, -\theta, 1)$. Здесь α, β, γ, δ, ε и θ обозначают положительные числа, меньшие единицы.

Примем точки A, B и Γ за базис решетки и выясним, при каких условиях единичный куб, который в данном случае будет параллелепипедом, ограниченным наиболее удаленными от начала гранями параллелепипедов A, B и Γ, может содержать внутри себя точки решетки.

Координаты любой точки решетки получаются по формулам

$$\begin{aligned} \xi &= u - \gamma v + \varepsilon w, \\ \eta &= \alpha u + v - \theta w, \\ \zeta &= -\beta u + \delta v + w \end{aligned}$$

при целочисленных u, v и w.

Прежде всего заметим, что $u \neq 0$. Действительно, если $u = 0$, то либо $|\eta| = |v - \theta w|$, либо $|\zeta| = |\delta v + w|$ будет больше единицы в зависимости от того, будут ли знаки v и w различными, или одинаковыми. По той же причине $u \neq 0$ и $w \neq 0$.

Далее, u, v и w должны иметь одинаковые знаки, ибо в противном случае либо $|\xi| = |u - \gamma v + \varepsilon w|$, либо $|\eta| = |\alpha u + v - \theta w|$, либо $|\zeta| = |-\beta u + \delta v + w|$

будет больше единицы. Без нарушения общности можно считать, что u, v и w положительны. Тогда из неравенства $u-\gamma v+\varepsilon w<1$ следует, что $\gamma v>u-1$ и, следовательно, $v\geqslant u$, ибо $\gamma<1$.

Таким же образом, должны выполняться неравенства $w\geqslant v$ и $u\geqslant w$. Отсюда следует, что $u=v=w$. Если при каком-нибудь значении $u=v=w$ точка решетки попадает внутрь единичного куба, то точка, получающаяся при $u=v=w=1$, тоже попадает внутрь единичного куба. Но это возможно, очевидно, только при выполнении неравенств

$$\gamma>\varepsilon,\quad \theta>\alpha,\quad \beta>\delta.$$

Если хотя бы одно из этих неравенств не выполнено, единичный куб не содержит внутри себя ни одной точки решетки, построенной на A, B и Γ, кроме начала координат.

Взяв $\delta>\beta$ и $\theta>\alpha$, мы получим точки A, B и Γ, удовлетворяющие всем требованиям первого примера. Действительно, параллелепипед A будет пронизывать по X параллелепипеды B и Γ, и параллелепипед, ограниченный наиболее удаленными гранями параллелепипедов A, B и Γ (в нашем случае единичный куб), будет пуст внутри от точек решетки.

Взяв $\beta<\delta$ и $\theta<\alpha$, получим точки A, B и Γ, удовлетворяющие всем требованиям второго примера.

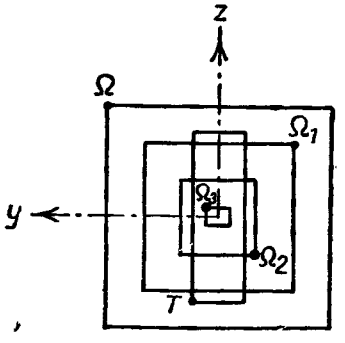
§ 55. Теорема о параллельных цепочках

Пусть дана x-цепочка относительных минимумов

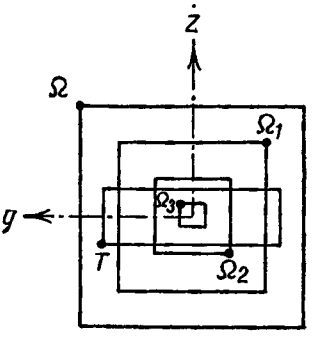
$$\{\Omega\}_x=\Omega,\ \Omega_1,\ \Omega_2,\ \ldots,$$

и относительный минимум T.

Будем говорить, что относительный минимум T расположен выше цепочки $\{\Omega\}_x$, если в ней найдется элемент, который был бы ниже и шире T. Таким же образом, если в цепочке $\{\Omega\}_x$ найдется элемент выше и уже T, будем говорить, что T расположен ниже цепочки $\{\Omega\}_x$ (черт. 15 и 16).



Черт. 15.



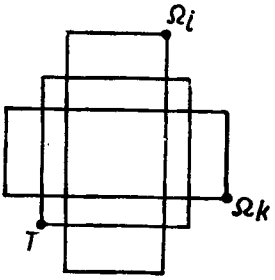
Черт. 16.

Легко видеть, что данный относительный минимум T не может быть одновременно выше и ниже данной цепочки $\{\Omega\}_x$. В противном случае в этой цепочке нашлись бы элементы Ω_i и Ω_k, не охватывающие один другого в направлении OX, что невозможно (черт. 17).

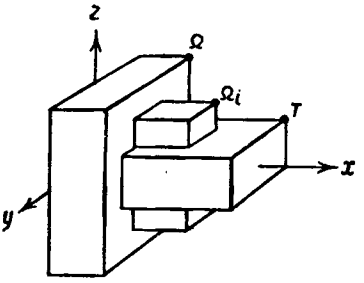
Теорема 1. *Если относительный минимум T не охватывает по OX относительный минимум Ω, то T или принадлежит x-цепочке, порожденной Ω, или расположен выше нее или ниже. Никакой четвертой возможности не существует.*

Доказательство. Имеются возможности:

1. T совпадает с Ω. Тогда T принадлежит $\{\Omega\}_x$.
2. T выше и уже Ω. Тогда T выше $\{\Omega\}_x$.
3. T шире и выше Ω. Тогда T ниже $\{\Omega\}_x$.
4. T ниже и уже Ω или, по нашей терминологии, T проиизывает Ω по OX (черт. 18).



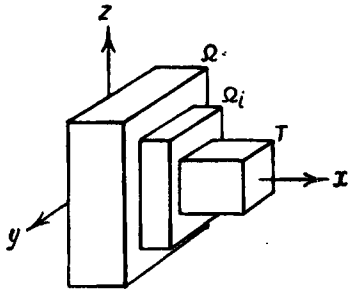
Черт. 17.



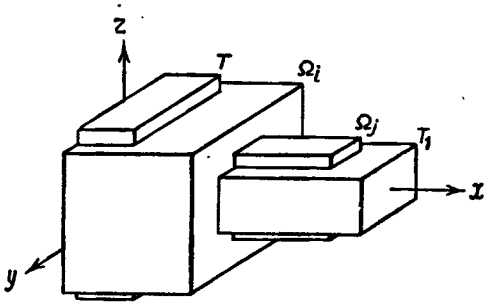
Черт. 18.

Рассмотрим самый длинный элемеит Ω_i цепочки $\{\Omega\}_x$, который еще короче T. Может быть одно из трех.

4. Ω_i выше и уже T (черт. 18). Тогда T ниже $\{\Omega\}_x$.
4. Ω_i ниже и шире T. Тогда T выше $\{\Omega\}_x$.
4. Ω_i выше и шире T (черт. 19), т. е. Ω_i охватывает T по OX. Правая грань параллелепипеда Ω_i при движении вправо встретит в первый раз точку T, ибо в противном случае в цепочке $\{\Omega\}_x$ нашелся бы элемент Ω_{i+1}, который



Черт. 19.



Черт. 20.

был бы короче T, что противоречит сделанному выбору Ω_i. Следовательно, T будет в этом случае смежным с Ω_i относительным минимумом и будет поэтому принадлежать цепочке $\{\Omega\}_x$.

Тем самым теорема доказана.

Теорема 2. *Если относительный минимум T расположен выше x-цепочки, порожденной относительным минимумом Ω, то смежный по x с T относительный минимум T_1 будет также расположен выше цепочки $\{\Omega\}_x$ или будет ее элементом.*

Доказательство. Пусть относительный минимум T расположен выше цепочки $\{\Omega\}_x$. Это значит, что в цепочке найдется элемент Ω_i, который будет ниже и шире, чем T. Сравним Ω_i с T_1. Ω_i шире, чем T_1, так как шире, чем T, а T шире, чем T_1. Если Ω_i при этом ниже, чем T_1, то T_1 расположен выше цепочки $\{\Omega\}_x$ согласно определению. Если Ω_i выше, чем T_1, то Ω_i короче T_1, иначе Ω_i не был бы относительным минимумом. Введем в рассмотрение Ω_j — самый длинный элемент цепочки $\{\Omega\}_x$, который еще короче, чем T_1. Если Ω_j выше и шире T_1, то $\Omega_{j+1} = T_1$, и элемент T_1 принадлежит цепочке

$\{\Omega\}_x$. Если Ω_j ниже и шире, чем T_1, то T_1 расположен выше цепочки $\{\Omega\}_x$. Остается случай, если Ω_j выше и уже, чем T_1. Однако этот случай невозможен (черт. 20). Действительно, Ω_j ниже, чем Ω_i, и, следовательно, ниже T. С другой стороны, Ω_j уже T_1 и, следовательно, уже T. Следовательно, Ω_j пронизывает T по OX и T_1, будучи длиннее Ω_j, не может быть смежным по OX для T относительным минимумом.

Тем самым теорема доказана.

Из теоремы 2 непосредственно вытекает, что, если относительный минимум T расположен выше цепочки $\{\Omega\}_x$, то любой элемент цепочки $\{T\}_x$ расположен выше цепочки $\{\Omega\}_x$ или в ней.

Точно так же доказывается, что если T расположен ниже $\{\Omega\}_x$, то смежный с ним по x относительный минимум T расположен ниже цепочки $\{\Omega\}_x$ или является ее элементом.

Все это дает возможность обобщить понятия — относительный минимум T расположен выше или ниже цепочки $\{\Omega\}_x$ — также и на случай, когда T охватывает по OX начальный элемент цепочки Ω. Именно, будем считать, что T расположен выше цепочки $\{\Omega\}_x$, если хотя бы один элемент цепочки $\{T\}_x$ расположен выше $\{\Omega\}_x$, T расположен ниже цепочки $[\Omega]_x$, если хотя бы один элемент цепочки $\{T\}_x$ расположен ниже цепочки $\{\Omega\}_x$, и, наконец, T будем считать принадлежащим цепочке $\{\Omega\}_x$, если Ω принадлежит цепочке $\{T\}_x$ и, следовательно, вся цепочка $\{\Omega\}_x$ целиком входит в $\{T\}_x$.

Очевидны следующие предложения:

Если T выше $\{\Omega\}_x$, то Ω ниже $\{T\}_x$.

Если Φ выше $\{T\}_x$ и T выше $\{\Omega\}_x$, то Φ выше $\{\Omega\}_x$.

Таким образом каждая x-цепочка относительных минимумов разбивает все относительные минимумы на три класса — класс расположенных выше цепочки, класс расположенных ниже цепочки и класс принадлежащих цепочке. Выясненные выше свойства этого разбиения позволяют установить некоторую аналогию между цепочкой относительных минимумов и прямолинейным рядом точек на плоскости. Различные x-цепочки играют в этой аналогии роль параллельных прямых.

Очевидно, что y-цепочки и z-цепочки производят такое же разбиение относительных минимумов. Применительно к расположениям относительных минимумов относительно этих цепочек введем термины — относительный минимум расположен выше или ниже y-цепочки, относительный минимум расположен направо или налево от z-цепочки. Для этих отношений, очевидно, справедливы теоремы, аналогичные теореме 2.

§ 56. Теоремы о цепочках разного направления

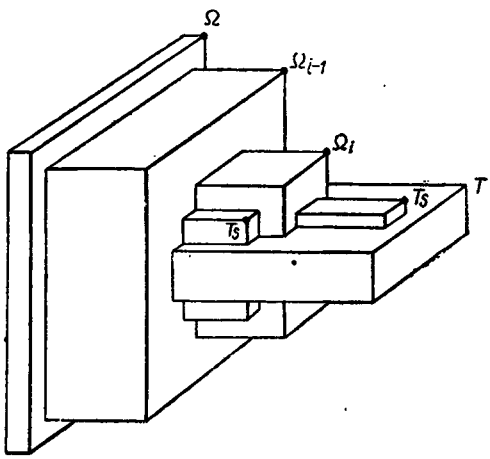
Теорема 3. *Если относительный минимум T расположен направо от $\{\Omega\}_z$ и ниже $\{\Omega\}_x$, то цепочки $\{\Omega\}_x$ и $\{T\}_z$ имеют общий элемент.*

Доказательство. Два на удачу взятых относительных минимума Ω и T могут быть расположены один относительно другого шестью различными способами: Ω охватывает T по OX, Ω пронизывает T по OX, Ω охватывает T по OY, Ω пронизывает T по OY, Ω охватывает T по OZ и, наконец, Ω пронизывает T по OZ. Из этих шести расположений удовлетворять условиям теоремы могут только два: Ω охватывает T по OX, и Ω пронизывает T по OZ.

Для определенности остановимся на первой возможности.

Итак, пусть Ω охватывает T по OX (черт. 21). По предположению, T лежит ниже $\{\Omega\}_x$. Следовательно, в цепочке $\{\Omega\}_x$ найдется элемент, который будет короче, выше и уже, чем T, ибо если бы такого элемента не нашлось и все элементы цепи $\{\Omega\}_x$ более короткие, чем T, были бы выше и шире T, то T принадлежал бы $\{\Omega\}_x$, что противоречит предположению. Пусть Ω_i первый такой элемент цепочки $\{\Omega\}_x$, т. е. такой, что предшествующий ему элемент Ω_{i-1} охватывает T по OX.

Относительный минимум T охватывает Ω_i по OZ. Покажем, что Ω_i или принадлежит цепочке $\{T\}_z$, или лежит налево от нее. В самом деле, рассмотрим элементы цепочки $\{T\}_z$, которые ниже Ω_i. Если все они охватывают Ω_i по OZ, то Ω_i принадлежит цепочке $\{T\}_z$, и тем самым теорема доказана. Если же в цепочке $\{T\}_z$ найдется элемент T_s, не охватывающий Ω_i по OZ, то он может быть или короче и шире, чем Ω_i, или длиннее и у́же. Но первая возможность отпадает, ибо тогда вершина T_s попала бы в пространство между смежными относительными минимумами Ω_{i-1} и Ω_i, что невозможно. Остается вторая возможность, что T_s длиннее и у́же, чем Ω_i. Но это и значит, что Ω_i лежит налево от цепочки $\{T\}_z$.



Черт. 21.

Таким образом, T и Ω_i снова удовлетворяют условиям теоремы, но на этот раз T охватывает Ω по OZ. Повторим то же рассуждение. Найдем первый элемент T_k цепочки $\{T\}_z$, не охватывающий Ω_i по OZ, и покажем так же, как раньше, что T_k или принадлежит цепочке $\{\Omega_i\}_x$, которая представляет собой продолжение цепочки $\{\Omega\}_x$, или лежит ниже нее. В последнем случае снова повторяем то же рассуждение и т. д. Все относительные минимумы, которые мы при этом вводим в рассмотрение, будут короче T, ниже Ω и у́же их обоих. Таких минимумов может быть лишь конечное число, и, следовательно, наш процесс должен окончиться в конечном числе шагов. Но окончиться он может только тем, что какой-нибудь элемент цепочки $\{\Omega\}_x$ совпадет с каким-нибудь элементом цепочки $\{T\}_z$. Тем самым теорема доказана.

Подобные теоремы могут быть доказаны и для других случаев цепочек разного направления. Именно, цепочки $\{\Omega\}_y$ и $\{T\}_x$ имеют общий элемент, если T расположен ниже $\{\Omega\}_x$ и ниже $\{\Omega\}_y$ и, наконец, цепочки $\{\Omega\}_y$ и $\{T\}_z$ имеют общий элемент, если T расположен ниже $\{\Omega\}_y$ и левее $\{\Omega\}_z$.

Теорема 4. *Даны два относительных минимума Ω и T. Одна из цепочек $\{\Omega\}_x$, $\{\Omega\}_y$ и $\{\Omega\}_z$ имеет общий элемент с одной из цепочек $\{T\}_x$, $\{T\}_y$ и $\{T\}_z$.*

Доказательство. Пусть Ω охватывает T по оси OX, и, следовательно, T расположен правее цепочки $\{\Omega\}_z$ и ниже цепочки $\{\Omega\}_y$. Рассмотрим самый длинный элемент Ω_i цепочки $\{\Omega\}_x$, который еще короче T. Если он шире и выше T, то T принадлежит цепочке $\{\Omega\}_x$, и, следовательно, $\{\Omega\}_x$ имеет общий элемент T с цепочками $\{\Gamma\}_y$ и $\{T\}_z$. Если Ω_i выше и у́же T, то T расположен ниже цепочки $\{\Omega\}_x$ и, по теореме 3, $\{\Omega\}_x$ и $\{\Gamma\}_z$ имеют общий элемент. Если Ω_i ниже и шире T, то T расположен выше цепочки $\{\Omega\}_x$, и по одной из теорем, аналогичных теореме 3, цепочки $\{\Omega\}_x$ и $\{T\}_y$ будут иметь общий элемент. Аналогичным образом мы можем рассмотреть и все другие случаи расположения Ω и T.

Теорема 5. *Дан относительный минимум Φ. Пусть относительный минимум Ω принадлежит $\{\Phi\}_z$, а T принадлежит $\{\Phi\}_x$. Тогда цепочки $\{\Omega\}_x$ и $\{T\}_z$ имеют общий элемент.*

Доказательство. Очевидно, что Ω и T удовлетворяют условиям теоремы 3, откуда настоящая теорема вытекает непосредственно.

Теорема 3 еще раз подтверждает наличие аналогии между расположением относительных минимумов и точек на плоскости, образующих линейные ряды.

Теорема 3 содержит утверждение, подобное тому, что две прямые разных направлений имеют общую точку.

В заключение заметим, что теоремы 1—5 верны не только для решеток, но и для любых дискретных систем точек, для которых возможно построение неограниченных цепей относительных минимумов.

§ 57. Решение задачи о подобии двух решеток, рационально связанных с неприводимой решеткой в $R_{3,0}$, повторяющейся умножением, или подобных таким решеткам

Напомним некоторые определения и результаты, изложенные в главе I.

Если решетку умножить на некоторую точку пространства, не являющуюся делителем нуля, то получится новая решетка, которую мы условились называть подобной исходной решетке. При преобразовании подобия относительные минимумы переходят в относительные минимумы, смежные в смежные и вообще взаимное расположение координатных параллелепипедов не изменяется. Среди всех решеток, подобных некоторой данной решетке, особо важную роль играют те, которые получаются из данной делением на ее относительные минимумы. Все они содержат в числе своих точек единицу (1, 1, 1), и 1 будет для каждой из них относительным минимумом. Для того чтобы среди этих решеток было лишь конечное число различных, необходимо и достаточно, чтобы решетка была подобна решетке, рационально связанной с неприводимой решеткой, повторяющейся умножением.

В следующих пунктах этого параграфа мы будем заниматься исследованием только таких решеток и под словом „решетка" будем подразумевать только решетки этого рода.

Решение задачи о подобии двух решеток. Пусть решетка S подобна решетке, рационально связанной с неприводимой решеткой, повторяющейся умножением. Найдем в ней какой-либо относительный минимум Ω и построим, исходя из него, цепочку относительных минимумов.

$$\Omega,\ \Omega_1, \Omega_2, \ldots, \Omega_m, \ldots$$

Будем делить S последовательно на Ω, Ω_1, Ω_2, ..., Ω_m, ... Получим последовательность решеток

$$S_0 = \frac{1}{\Omega} S,\ S_1 = \frac{1}{\Omega_1} S, \ldots, S_m = \frac{1}{\Omega_m} S, \ldots$$

Среди этих решеток найдутся равные. Пусть S_k первая решетка, для которой найдется равная, и S_{k+n} первая решетка, равная S_k. Тогда точка $\varepsilon_1 = \frac{\Omega_{k+n}}{\Omega_k}$ будет давать автоморфизм умножения для решетки S и всех подобных ей решеток. Точка ε_1 будет принадлежать решетке S_k и будет представлять собой в ней n-й относительный минимум в цепочке, порожденной элементом 1.

Изучим подробнее эту цепочку. Пусть ее элементы будут

$$\Phi_0 = 1,\ \Phi_1,\ \Phi_2, \ldots,\ \Phi_{n-1},\ \Phi_n = \varepsilon_1,\ \Phi_{n+1} \ldots$$

В виду того, что решетка S_k при умножении на ε_1 переходит в себя, а точка $1 = \Phi_0$ при этом переходит в $\varepsilon_1 = \Phi_n$, точка Φ_1 переходит в Φ_{n+1}, Φ_2 — в Φ_{n+2} и т. д. Следовательно,

$$\Phi_{n+s} = \varepsilon_1 \Phi_s$$

при любом s, и цепочка имеет вид

$$\Phi_0 = 1,\ \Phi_1,\ \Phi_2, \ldots,\ \Phi_{n-1},\ \Phi_n = \varepsilon_1,\ \varepsilon_1 \Phi_1,\ \varepsilon_1 \Phi_2, \ldots, \varepsilon_1^2, \ldots$$

Такую цепочку относительных минимумов будем называть *чисто периодической цепочкой.*

Приведенное рассуждение показывает, что каждая цепочка относительных минимумов в рассматриваемых решетках становится, начиная с некоторого места, чисто периодической.

Чисто периодические цепочки обладают тем замечательным свойством, что их можно бесконечно продолжать в обратную сторону. В самом деле, рассмотрим решетку S_k. Точка $\Phi_{-1}=\Phi_{n-1}\varepsilon_1^{-1}$ будет ей, очевидно, принадлежать, будет являться в ней относительным минимумом, и смежным с Φ_{-1} минимумом будет Φ_0. Точно так же, $\Phi_{-2}=\Phi_{n-2}\varepsilon_1^{-1}$ будет относительным минимумом, для которого смежный минимум будет Φ_{-1} и т. д.

Цепочку

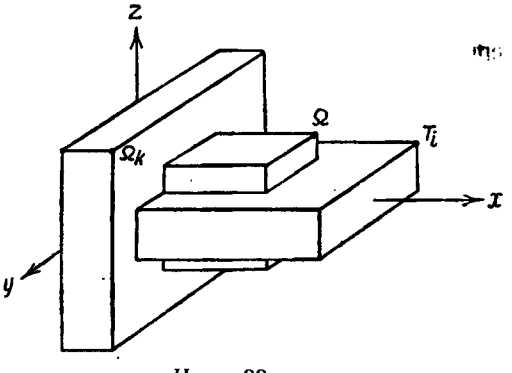
$$\ldots, \Phi_{-3}, \Phi_{-2}, \Phi_{-1}, \Phi_0, \Phi_1, \Phi_2, \Phi_3, \ldots$$

будем называть *двухсторонней цепочкой относительных минимумов.*

Обратно, каждая цепочка относительных минимумов, которая может быть безгранично продолжена в обратную сторону, должна быть чисто периодической. Действительно, пусть существует $n+1$ относительных минимумов

$$\Phi_{-n-1}, \Phi_{-n}\ \Phi_{-n+1}, \ldots, \Phi_1,$$

предшествующих относительному минимуму Φ_0. n обозначает общее число таких относительных минимумов, деление на которые исходной решетки даст различные результаты. Тогда среди этих относительных минимумов найдется пара отличающихся автоморфизмом умножения и, начиная с первого элемента этой пары, цепочка станет чисто периодической. Следовательно, цепочка



Черт. 22.

$$\Phi_0, \Phi_1 \ldots$$

также будет чисто периодической.

Теорема 6. *Две двухсторонних цепочки относительных минимумов разных направлений имеют общий элемент.*

Доказательство. Рассмотрим для определенности x-цепочку $\{\Phi\}_x$ и z-цепочку $\{T\}_z$.

Найдем в цепочке $\{T\}_z$ относительный минимум T_i (может быть, с отрицательным номером i), который охватывает Ω по OZ. Такой минимум наверное найдется, ибо в двухсторонней цепочке существуют элементы, имеющие сколь угодно большие размеры в направлениях, перпендикулярных направлению цепочки. Затем в цепочке $\{\Omega\}_x$ найдем элемент Ω_k, охватывающий T_i по OX (черт. 22). Для цепочек $\{\Omega\}_x$ и $\{T_i\}_z$ выполнены условия теоремы 3, и, следовательно, они имеют общий элемент, который и будет общим элементом двухсторонних цепочек $\{\Omega\}_x$ и $\{T\}_z$.

Теперь мы имеем возможность доказать теорему, посредством которой решается в конечном числе действий задача о подобии двух решеток и, в частности, задача об эквивалентности двух идеалов.

Теорема 7. *Для того чтобы две решетки S и R были подобны, необходимо и достаточно, чтобы одна из решеток, получающихся делением S на элементы x-цепочки в S, совпадала с одной из решеток, получающихся из R делением на элементы z-цепочки в R.*

Доказательство. Достаточность высказанного условия очевидна, так как две решетки, подобные третьей, подобны между собой.

Докажем необходимость условия.

Пусть $R=\lambda S$, где λ — „коэффициент" подобия, являющийся точкой пространства. Возьмем в S относительный минимум Ω и построим, исходя из него, двухстороннюю x-цепочку $\{\Omega\}_x$ (которая может и не содержать Ω). Затем возьмем в R какой-либо относительный минимум T и составим, исходя из него, двухстороннюю цепочку $\{T\}_z$. Делением на λ эта цепочка будет переведена в некоторую двухстороннюю z-цепочку решетки S. В силу теоремы 6, эта цепочка будет иметь с цепочкой $\{\Omega\}_x$ общий элемент Φ. Тогда $\Phi'=\lambda\Phi$ будет элементом цепочки $\{T\}_z$ в R. Но

$$\frac{1}{\Phi}S=\frac{1}{\Phi'}R.$$

Тем самым теорема доказана.

Эта теорема действительно решает задачу о подобии решеток в конечном числе действий, ибо, желая получить различные решетки $\frac{S}{\Phi}$, где Φ принадлежит двухсторонней x-цепочке в S, достаточно делить на Φ в пределах одного периода, т. е. на конечное число относительных минимумов Φ. То же самое имеет место и при делении R на элементы z-цепочки.

§ 58. Разыскание основных автоморфизмов умножения для решетки, рационально связанной с неприводимой решеткой в $R_{3,0}$, повторяющейся умножением, или подобной такой решетке

В главе I мы установили существование независимых автоморфизмов умножения для неприводимых решеток, повторяющихся умножением, число которых равно $\sigma+\tau-1$, где σ — число вещественных координат, τ — число пар комплексных сопряженных координат. Затем, перейдя в логарифмическое пространство и используя дискретность и повторяемость вычитанием системы точек, изображающих логарифмы автоморфизмов, мы доказали, что все автоморфизмы представляются в виде

$$\varepsilon=E\cdot\varepsilon_1^{a_1}\varepsilon_2^{a_2},\ \ldots,\ \varepsilon_{\sigma+\tau-1}^{a_{\sigma+\tau-1}},$$

где E — один из „особенных автоморфизмов", т. е. некоторый корень из единицы, $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\sigma+\tau-1}$ — так называемые основные автоморфизмы, и $a_1, a_2, \ldots, a_{\sigma+\tau-1}$ — числа, принимающие независимо друг от друга все целые рациональные значения. Это доказательство однако не давало удобного решения задачи об отыскании основных автоморфизмов решетки. Теперь, основываясь на теоремах о расположении цепочек относительных минимумов, мы имеем возможность дать алгорифм для фактического отыскания основных автоморфизмов для трехмерных вещественных решеток.

Итак, пусть нам нужно найти основные автоморфизмы умножения для трехмерной вещественной решетки S, повторяющейся умножением. Для упрощения рассуждений будем считать решетку содержащей точку $1=(1, 1, 1)$ и такой, что 1 является относительным минимумом, имеющим чисто периодическую x-цепочку. Переход к такой решетке можно всегда осуществить посредством деления решетки на точку любой чисто периодической x-цепочки.

Обозначим через ε_1 первый автоморфизм x-цепочки решетки S, построенной исходя из элемента 1. Все остальные автоморфизмы, содержащиеся в этой цепочке (которую будем считать двухсторонней), будут иметь вид ε_1^n, при всех целых n, положительных или отрицательных.

Элементы x-цепочки $\{1\}_x$ обозначим

$$\ldots 1=\Phi_0, \Phi_1, \Phi_2 \ldots \Phi_n'=\varepsilon_1, \ldots$$

Рассмотрим теперь другие автоморфизмы решетки S. Все они будут представлять собой относительные минимумы решетки. Исходя из каждого из них,

мы можем построить x-цепочки. Эти x-цепочки, очевидно, все будут чисто периодическими и потому двухсторонне продолжимыми, и их элементы будут ассоциированы (т. е. будут отличаться лишь множителями, являющимися автоморфизмами S) элементам цепочки $\{1\}_x$. Очевидно и обратное: если мы построим x-цепочку, исходя из точки решетки, ассоциированной какой-либо из точек цепочки $\{1\}_x$, то получится чисто периодическая цепочка, содержащая среди своих элементов автоморфизмы. Содержащиеся в каждой из таких цепочек автоморфизмы имеют вид $\varepsilon\varepsilon_1^n$, где ε — один из автоморфизмов, содержащихся в цепочке, и ε_1 — первый автоморфизм в цепочке $\{1\}_x$. Все эти цепочки можно расположить „по высоте", так как для любых двух x-цепочек мы имеем возможность сказать, которая расположена выше и которая ниже другой, и это соотношение транзитивно.

Построим теперь z-цепочку относительных минимумов, исходя из какого-либо элемента цепочки $\{1\}_x$. По теореме о пересечении цепочек каждая такая цепочка будет иметь общие элементы со всеми цепочками $\{\varepsilon\}_x$, лежащими выше цепочки $\{1\}_x$. Эти общие элементы будут расположены в z-цепочке в порядке „возрастания высот" цепочек $\{\varepsilon\}_x$. Таким образом среди цепочек $\{\varepsilon\}_x$ найдется первая цепочка, расположенная выше $\{1\}_x$, за ней вторая, третья и т. д. Каждая последующая будет расположена выше предыдущей, и все цепочки $\{\varepsilon\}_x$, построенные на автоморфизмах, лежащих выше $\{1\}_x$, попадут в эту последовательность.

Пусть ε_2 — какой-либо автоморфизм, содержащийся в первой цепочке рассматриваемой последовательности. Деление на ε_2, очевидно, переводит непосредственно следующую за $\{1\}_x$ цепочку в $\{1\}_x$, вторую в первую, третью во вторую и т. д.

Поэтому вторая цепочка содержит автоморфизм ε_2^2, третья ε_2^3, m-ая ε_2^m, при любом целом положительном m.

Пусть ε — любой автоморфизм. Возможны три случая расположения этого автоморфизма относительно цепочки $\{1\}_x$.

1. ε лежит в $\{1\}_x$.

Тогда $\varepsilon = \varepsilon_1^n$, где n — целое положительное или отрицательное число.

2. ε лежит выше $\{1\}_x$.

Тогда ε попадет в одну из x-цепочек рассмотренной выше последовательности. Пусть в m-ую. Эта последняя содержит среди своих элементов автоморфизм ε_2^m, и все другие автоморфизмы, в ней содержащиеся, представляются в виде $\varepsilon_2^m\varepsilon_1^n$.

Итак, в этом случае

$$\varepsilon = \varepsilon_2^m\varepsilon_1^n,$$

где m — целое *положительное* число.

3. ε лежит ниже $\{1\}_x$.

Тогда 1 лежит выше $\{\varepsilon\}_x$. Деление на ε переводит 1 в $\frac{1}{\varepsilon}$ и ε в 1. Следовательно, $\frac{1}{\varepsilon}$ лежит выше $\{1\}_x$ и, в силу предыдущего,

$$\frac{1}{\varepsilon} = \varepsilon_2^m\varepsilon_1^n.$$

Откуда

$$\varepsilon = \varepsilon_2^{-m}\varepsilon_1^{-n}.$$

Все это показывает, что автоморфизмы ε_1 и ε_2 могут быть приняты за основные автоморфизмы решетки S.

Укажем теперь действия, посредством которых можно на самом деле найти ε_1 и ε_2 для любой решетки, быть может, и не удовлетворяющей условию чистой периодичности цепочки $\{1\}_x$. Как найти ε_1, мы уже знаем. Нужно, исходя из любого относительного минимума, построить x-цепочку и делить каждый раз

решетку на элементы цепочки. Пусть при этом в первый раз повторится некоторая решетка S. Отношение соответствующих относительных минимумов (последующего к предыдущему) равно автоморфизму ε_1. Для решетки S элемент 1 будет иметь чисто периодическую цепочку $1, \Phi_1, \Phi_2, \ldots, \Phi_n = \varepsilon_1$. По ходу вычислений мы получим все решетки $\frac{1}{\Phi_i} S$, $i = 1, 2, \ldots, n-1$.

Дальнейшее вычисление нужно вести в решетке S.

Исходя из элемента 1, строим z-цепочку

$$1, \psi_1, \psi_2, \ldots \quad .$$

Делим решетку S последовательно на $\psi_1, \psi_2, \ldots$ и смотрим, когда при этом в первый раз получится одна из решеток $\frac{S}{\Phi_i}$, $i = 0, 1, \ldots, n-1$.

Пусть в первый раз

$$\frac{1}{\psi_k} S = \frac{1}{\Phi_i} S.$$

Тогда $\frac{\psi_k}{\Phi_i}$ будет представлять собой автоморфизм решетки S, причем тот самый автоморфизм, который мы раньше обозначали ε_2. Действительно, цепочка $\{\psi_k\}_x$ будет образована элементами, ассоциированными элементам цепочки $\{1\}_x$, и будет содержать $\frac{\psi_k}{\Phi_i}$ в качестве i-го элемента, предшествующего ψ_k, так как 1 является i-тым элементом, предшествующим Φ_i в решетке $\{1\}_x$. Из способа выбора ψ_k следует, что цепочка $\{\psi_k\}_x$ будет наименьшей по высоте среди x-цепочек, содержащих автоморфизмы, расположенные выше $\{1\}_x$. Поэтому любой автоморфизм, содержащийся в $\{\psi_k\}_x$, в частности $\frac{\psi_k}{\Phi_i}$, может быть принят за ε_2.

Таким образом нами установлено правило для отыскания основных автоморфизмов решеток посредством составления цепей относительных минимумов.

§ 59. Алгорифм для разыскания относительного минимума, смежного с данным, для решетки, рационально связанной с неприводимой решеткой в $R_{3,0}$, или подобной такой решетке

В данном параграфе предстоит решить следующую задачу. Дан трехвекторник (χ_1, χ_2, χ_3), определяющий решетку. Узнать, является ли точка χ_1 относительным минимумом. Если да, то найти смежный с ним по Ox минимум, если нет — найти точку внутри построенного на χ_1 координатного параллелепипеда.

Без нарушения общности можно считать $\chi_1 = 1$.

Для решения задачи сделаем следующие построения.

Разобьем все точки решетки на параллели. Под этим названием будем подразумевать совокупность точек решетки, лежащих на прямой, параллельной „рациональной прямой“ $x = y = z$. Совокупность точек решетки, лежащих на каждой непустой параллели, образует линейный ряд. Проекция отрезка, соединяющего две соседних точки этого ряда, на каждую из координатных осей равна 1. Каждая плоскость, не параллельная рациональной прямой, пересечет множество непустых параллелей по плоской решетке, которая будет представлять собой проекцию исходной решетки на взятую плоскость, параллельно рациональной прямой.

В качестве плоскости проекции возьмем плоскость $y + z = 0$,[1] являющуюся диагональной плоскостью единичного куба. Для удобства вычислений перейдем

[1] Г. Ф. Вороной берет в качестве плоскости проекции плоскость $z = 0$.

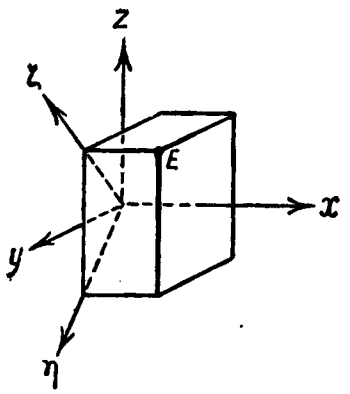
к новой системе координат (ξ, η, ζ), принимая за оси $O\eta$ и $O\zeta$ биссектрисы 4-го и 1-го координатных углов в плоскости YZ и взяв за единицу масштаба в этих осях отрезок, равный $\sqrt{2}$ единицы масштаба в прежних осях (черт. 23).

Формулы перехода к новым координатам будут:

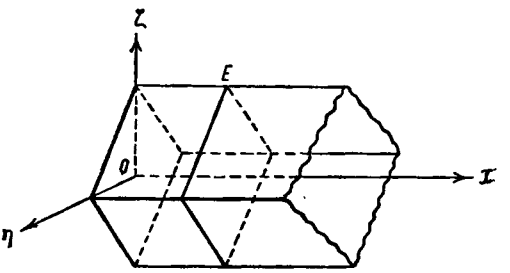
$$\xi = x, \quad \eta = \frac{y-z}{2}, \quad \zeta = \frac{y+z}{2}.$$

В частности, новые координаты точки 1 (1, 1, 1) будут (1, 0, 1).

Плоскость проекции $y+z=0$ в новых координатах будет координатной плоскостью $x\eta$. Призма, образованная гранями единичного куба, параллельными оси Ox, расположена относительно новых координатных осей согласно черт. 24. Расстояние ребер этой призмы до оси Ox будет равно 1.



Черт. 23.



Черт. 24.

Точки пересечения параллелей с плоскостью $x\eta$ будем называть проколами. Вследствие симметрии решетки относительно начала координат достаточно рассматривать точки, проколы которых лежат направо от оси $O\eta$.

Основной двухвекторник плоской решетки проколов будет, очевидно, образован векторами, соединяющими начало координат с проколами концов второго и третьего векторов основного трехвекторника (1, χ_2, χ_3) решетки.

Координаты прокола точки (x, y, z) будут

$$\xi = \frac{2x-y-z}{2}; \quad \eta = \frac{y-z}{2}; \quad \zeta = 0.$$

Тут ξ — это x прокола.

Задача, которую нам нужно решить, может быть сформулирована так. Найти точку внутри единичной призмы, расстояние от которой до плоскости $\eta\zeta$ меньше 1 или, если такой нет, найти точку внутри призмы, ближайшую к плоскости $\eta\zeta$.

Очевидно, что внутри призмы могут лежать только те точки, проколы которых лежат между ребрами призмы, т. е. в полосе $|\eta| < 1$, причем из всех точек, имеющих данный прокол, внутри призмы могут оказаться только ближайшие к проколу точки параллели, по обе стороны плоскости $x\eta$. Эти точки будем называть верхней и нижней точками, принадлежащими данному проколу.

Проколы, находящиеся внутри полосы $|\eta| < 1$ можно разбить на две категории. Именно, к первой категории отнесем проколы, лежащие в полосе $|\eta| < \frac{1}{2}$, а ко второй — лежащие вне этой полосы.

Проколы первой категории обладают тем свойством, что одна из принадлежащих им точек обязательно окажется внутри призмы, и внутри призмы могут оказаться обе точки. Это следует из того, что отсекаемый призмой отрезок параллели, проходящей через такой прокол, имеет

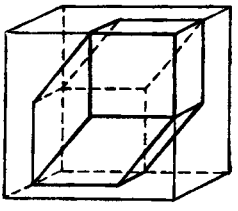
бо́льшую единицы проекцию на ось Ox, и, следовательно, на этом отрезке лежит по крайней мере одна точка решетки, и могут поместиться две.

Наоборот, из точек, принадлежащих проколам второй категории, внутри призмы может оказаться не более одной точки, и, возможно, что точки не будут находиться внутри призмы.

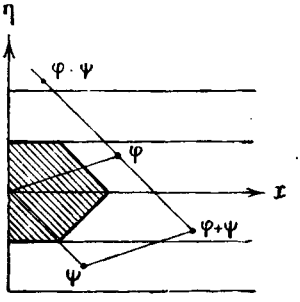
Прежде чем идти дальше, наложим еще ограничение на решетку. Именно, предположим, что координаты проколов, т. е. числа

$$\xi = \frac{2x-y-z}{2} \quad \text{и} \quad \eta = \frac{y-z}{2}$$

иррациональны для всех точек, кроме точек рациональной прямой. Это, очевидно, выполняется для интересующего нас случая неприводимых решеток, повторяющихся умножением. Это ограничение не является существенным, но



Черт. 25.



Черт. 26.

оно упрощает дальнейшие рассуждения, делая их не нуждающимися в некоторых дополнительных оговорках.

В решетке проколов найдем самый близкий к оси $O\eta$ прокол первой категории $\left(\text{т. е. лежащий в полосе } |\eta| < \frac{1}{2}\right)$. Обозначим его через φ.

В полосе между осью $O\eta$ и прямой, параллельной $O\eta$ и проходящей через прокол φ, найдем прокол ϕ, ближайший к оси Ox. Известно, что подобранные таким образом проколы φ и ϕ лежат по разным сторонам от оси Ox и образуют основной двухвекторник системы проколов. В этой системе они образуют смежные относительные минимумы в том смысле этого понятия, как оно устанавливается для плоских решеток. Разыскание их, как известно, можно осуществить при помощи алгорифма непрерывных дробей.

Теорема. *Искомая точка, т. е. внутренняя точка для единичного куба, или смежный по Ox с 1 относительный минимум, принадлежит одному из проколов:* φ, ϕ, $\varphi+\phi$, $\varphi-\phi$ *или* $2\varphi+\phi$, *причем последнему может принадлежать только в случае, если обе точки, принадлежащие проколу* $\varphi+\phi$, *лежат вне призмы и если прокол* ϕ, *а следовательно, и* $\varphi-\phi$ *лежат за пределами полосы* $|\eta| < 1$.

Прежде чем доказывать теорему, установим несколько вспомогательных предложений.

Лемма I. *Искомая точка принадлежит одному из проколов* $m\varphi + n\phi$, $0 \leqslant m \leqslant 4$, $1 \leqslant n \leqslant m+1$.

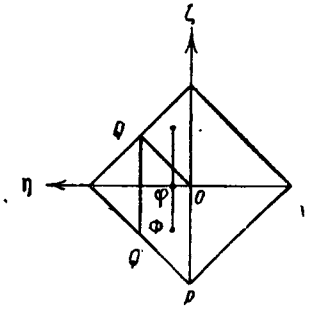
Доказательство. Рассмотрим совокупность точек единичного куба таких, что отрезок параллели внутри куба, проходящей через любую точку совокупности, имеет проекцию на Ox бо́льшую, чем 1. Эта совокупность заполняет шестигранную призму, изображенную на черт. 25. Проекция этой призмы на плоскость $O\eta$ представляет собой шестиугольник, половина которого изображена на черт. 26.

Рассмотрим решетку проколов. Может представиться два случая: или проколу φ принадлежит точка внутри единичного куба, или нет. В первом случае лемма доказана.

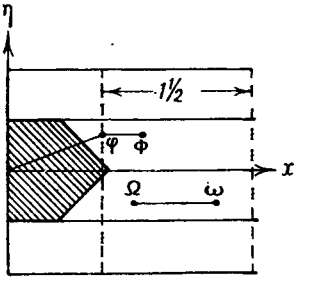
Во втором случае $\xi_\varphi > \frac{1}{2}$. Ибо, если бы ξ_φ было меньше $\frac{1}{2}$, то φ попало бы внутрь заштрихованной области (черт. 26), и проколу φ принадлежала бы точка внутри единичного куба. Обозначим через Φ — нижнюю точку, принадлежащую проколу φ, если она лежит внутри призмы, или верхнюю, если нижняя находится вне призмы. Очевидно, что

$$-1 < \zeta_\Phi < \frac{1}{2}.$$

В самом деле, спроектируем ортогонально призму на плоскость $\eta\zeta$. Проекция Φ должна быть внутри параллелограмма $OQQ'P$ (черт. 27).



Черт. 27.



Черт. 28.

Отсюда непосредственно вытекает, что прокол ω, которому принадлежит точка Ω, более близкая к плоскости yz, чем точка Φ, может отстоять от $O\eta$ не более чем на $1\frac{1}{2}$ единицы дальше, чем φ (черт. 28), ибо проекции отрезков параллели на Ox и $O\zeta$ одинаковы.

Таким образом интересующие нас проколы все лежат в прямоугольнике

$$|\eta| < 1, \quad |\xi| < \xi_\varphi + 1\frac{1}{2}.$$

Достаточно рассмотреть проколы $m\varphi + n\psi$ при $m \geqslant 0$. При $m = 0$ единственно возможно $n = 1$, ибо точка 2ψ лежит уже за пределами полосы $|\eta| < 1$.

При $m > 1$ очевидно, что $n \geqslant -1$, ибо если $n \leqslant -2$, то точка $m\varphi + n\psi$ также, наверное, окажется за пределами полосы $|\eta| < 1$, так как η_φ и η_ψ разных знаков и $|\eta_\psi| > \frac{1}{2}$.

Следовательно, $\xi_{m\varphi+n\psi} \geqslant \xi_{m\varphi-\psi} > \xi_{(m-1)\varphi} = (m-1)\xi_\varphi$.

Но должно иметь место

$$\xi_{m\varphi+n\psi} < \xi_\varphi + \frac{3}{2}.$$

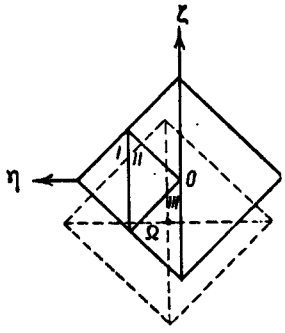
Следовательно, $(m-1)\xi_\varphi < \xi_\varphi + \frac{3}{2}$, откуда $m < 2 + \frac{3}{2\xi_\varphi} < 5$, так как $\xi_\varphi > \frac{1}{2}$.

Кроме того, проколы $\varphi + \psi$ и ψ лежат по одну сторону от оси Ox. Следовательно, проколы $m(\varphi + \psi) + k\psi$ при $k \geqslant 2$ лежат за пределами полосы $|\eta| \leqslant 1$. Итак, $m \leqslant 4$ и $-1 \leqslant n \leqslant m + 1$, что и требовалось доказать.

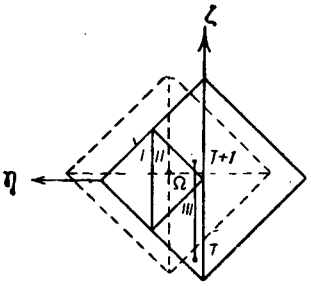
Лемма 2. *Пусть* ω *— прокол первой категории,* τ *— прокол, лежащий по одну сторону с* ω *от оси* Ox *и более удаленный, чем* ω, *от* $O\eta$. *Тогда, если проколу* τ *принадлежит точка* T *внутри призмы, более близкая к* $O\eta\zeta$, *чем точка* Ω, *принадлежащая проколу* ω, *то проколу* $\tau-\omega$ *принадлежит точка внутри единичного куба.*

Доказательство. Рассмотрим ортогональную проекцию призмы на плоскость $O\eta\zeta$ (черт. 29). Точка Ω в этой проекции может находиться в области II или III, точка T в областях I, II, III. Так как τ лежит от $O\eta$ дальше, чем ω, точка Ω должна на черт. 29 быть выше точки T.

Построим квадрат, равный и параллельный сечению основной призмы с центром в точке Ω. Если Ω принадлежит области III (черт. 29), этот квадрат будет покрывать все точки сечения основной призмы, лежащие ниже точки Ω,



Черт. 29.



Черт. 30.

следовательно, покроет точку T. Если же точка Ω лежит в области II, черт. 30, то этот квадрат покроет полностью области I и II и часть области III. Если при этом точка T находится в той части области III, которая не покрыта построенным квадратом, то точка $T+1$ все же попадет внутрь него. Это означает, что или $T-\Omega$, или $T-\Omega+1$ находится внутри призмы. Обе эти точки имеют своим проколом $\tau-\omega$, имеющую положительную абсциссу, ибо по условию прокол τ более удален от $O\eta$, чем ω. Следовательно, точка $T-\Omega$ имеет абсциссу большую -1, если она лежит внутри призмы, и большую $-1\frac{1}{2}$ в обратном случае. Но как мы видели, в этом обратном случае точка $T-\Omega+1$ лежит внутри призмы, и ее абсцисса будет больше $-\frac{1}{2}$ и меньше 1, ибо абсцисса точки $T-\Omega$ отрицательна. Таким образом или точка $T-\Omega$, или точка $T-\Omega+1$ лежит внутри единичного куба, что и требовалось доказать.

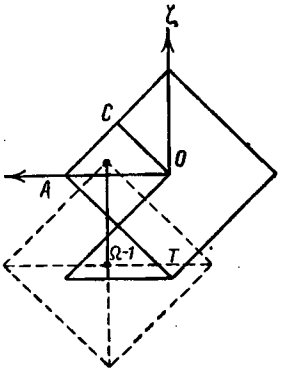
Лемма 2 позволяет исключить из рассмотрения целый ряд точек из указанных в лемме 1.

Именно, все точки $\tau=m\varphi+n\psi$ при $n=0$ и $n=-1$, кроме точки $\varphi-\psi$, удовлетворяют условию леммы для $\omega=\varphi$, так что из всех этих точек нуждается в испытании только точка $\varphi-\psi$. Далее, точки $\tau=m\varphi+n\psi$ при $n\geqslant m$, кроме точки $\varphi+\psi$, могут оказаться внутри полосы $|\eta|<1$ только в случае, если $\varphi+\psi$ лежит в полосе $|\eta|<\frac{1}{2}$, и будут удовлетворять условиям леммы 2 при $\omega=\varphi+\psi$. Следовательно, их также можно исключить из рассмотрения.

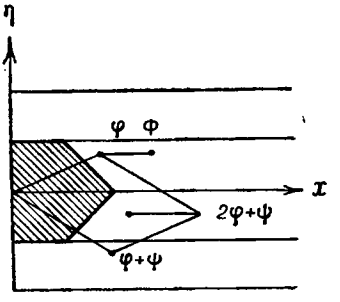
Таким образом, кроме точек φ, ψ, $\varphi-\psi$ и $\varphi+\psi$, остаются только точки $m\varphi+n\psi$ при $2\leqslant m\leqslant 4$, $1\leqslant n\leqslant m-1$.

Лемма 3. *Если прокол* τ *удален больше чем на 1 от ближележащего к* $O\eta$ *прокола* ω, *но точка* T *лежит внутри призмы и ближе к плоскости* $\zeta O\eta$, *чем точка* Ω, *лежащая также внутри призмы, то точка* $T-\Omega+1$ *лежит внутри единичного куба.*

Доказательство. В рассматриваемом случае проекция точки Ω на сечение призмы может находиться только внутри $\triangle OAC$ (черт. 31), а проекция точки T ниже проекции точки $\Omega - 1$. Построив квадрат, равный сечению призмы с центром в проекции точки $\Omega - 1$, мы увидим, что он покроет ту область сечения призмы, в которой может находиться проекция точки T. Следовательно, точка $T - \Omega + 1$ лежит внутри призмы. Абсцисса ее, очевидно,



Черт. 31.



Черт. 32.

положительна и меньше 1, так как абсцисса точки $T - \Omega$ отрицательна и больше $-\frac{1}{2}$. Следовательно, точка $T - \Omega + 1$ лежит внутри единичного куба, что и требовалось доказать.

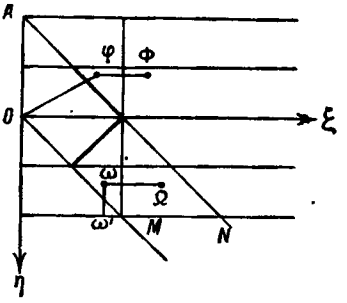
Лемма 3 исключает из рассмотрения точки $m\varphi + n\psi$ при $m \geqslant 3$. Таким образом остаются только точки φ, ψ, $\varphi - \psi$, $\varphi + \psi$ и $2\varphi + \psi$.

Исследуем подробнее прокол $2\varphi + \psi$.

Прежде всего ясно, что если абсцисса прокола $\varphi + \psi$ больше 1, то прокол $\tau = 2\varphi + \psi$ удовлетворяет требованиям леммы 3 при $\omega = \varphi$ и потому в рассмотрении не нуждается. Таким образом, нужно рассмотреть только случай, когда абсцисса $\varphi + \psi$, а следовательно, абсцисса φ, меньше 1 (черт. 32).

В этом случае, если нижняя точка, принадлежащая проколу φ или $\varphi + \psi$, окажется внутри призмы, то она будет внутри единичного куба, и точка $2\varphi + \psi$ также не нуждается в рассмотрении.

Предположим теперь, что нижние точки проколов φ и $\varphi + \psi$ лежат вне призмы. Обозначим их верхние точки соответственно через Φ и Ω. Их координаты ζ_Φ и ζ_Ω будут соответственно меньше $|\eta_\Phi|$ и $|\eta_\Omega|$. Следовательно, $\zeta_{\Phi+\Omega} < |\eta_\Phi| + |\eta_\Omega| = |\eta_\varphi - \eta_{\varphi+\psi}| = |\eta_\psi|$.



Черт. 33.

Докажем, что точка $2\varphi + \psi$ нуждается в рассмотрении только в случае, если $|\eta_\psi| > 1$. Действительно, пусть $|\eta_\psi| < 1$. Тогда $\zeta_{\Phi+\Omega} < 1$, и, следовательно, проколу $2\varphi + \psi$ будут принадлежать точки $\Phi + \Omega$ и $\Phi + \Omega - 1$.

Если абсцисса точки Ω больше 1, то точка $\Phi + \Omega - 1$ не может быть ближе, чем точка Φ, к плоскости $O\eta\zeta$ и должна быть выброшена из рассмотрения. Остается рассмотреть случай, если абсцисса Ω меньше 1. Если точка Ω окажется внутри призмы, то она вместе с тем будет находиться внутри единичного куба, и точка $2\varphi + \psi$ не нуждается в рассмотрении.

Остается случай, если абсцисса Ω меньше 1 и Ω лежит вне призмы. Однако это невозможно, если $|\eta_\psi| < 1$.

Действительно, точка Ω, находясь вне призмы, должна отстоять от своего прокола $\omega = \varphi + \psi$ в проекции на плоскость $x\eta$ на расстояние, большее $\omega\omega'$

(черт. 33). Следовательно, для того чтобы абсцисса была меньше единицы, нужно чтобы ω лежала ниже прямой OM. Но точка φ лежит выше параллельной прямой AN. Следовательно, точка $\psi = \omega - \varphi$ должна лежать ниже прямой FK, т. е. за пределами полосы $|\eta| < 1$.

Теорема доказана полностью.

Легко показать таким же образом, что точку $\varphi + \psi$ нужно исследовать только в случае, если проколу ψ не принадлежит точка внутри призмы.

Итак, мы получили, что для того, чтобы найти точку решетки, построенной на базисе $(1, \chi_2, \chi_3)$ внутри единичного куба, или показать, что единичный куб пуст, и найти точку, являющуюся смежным по Ox относительным минимумом с относительным минимумом 1, нужно произвести следующие действия:

1. Определить координаты „проколов" для точек χ_2 и χ_3 по формулам:

$$\xi = \frac{2x - y - z}{2}; \quad \eta = \frac{y - z}{2}.$$

2. Посредством алгорифма непрерывных дробей найти точки φ и ψ, являющиеся смежными относительными минимумами в решетке проколов, так что

$$\xi_\varphi > 0; \quad \xi_\psi > 0; \quad |\eta_\varphi| < \frac{1}{2}; \quad |\eta_\psi| > \frac{1}{2}.$$

Выразить эти точки через точки базиса $\bar{\chi}_2$ и $\bar{\chi}_3$ решетки проколов

$$\varphi = m_1\bar{\chi}_2 + n_1\bar{\chi}_3, \quad \psi = m_2\bar{\chi}_2 + n_2\bar{\chi}_3.$$

3. Вычислить координаты точек $\Phi = m_1\chi_2 + n_1\chi_3$ и $\Psi = m_2\chi_2 + n_2\chi_3$.

4. Подобрать целое число t_1 так, чтобы координаты y и z точки $\Phi_0 = \Phi + t\,1$ (1 — единичная точка (1, 1, 1)) были меньше единицы по абсолютной величине. Это возможно сделать. Если это можно сделать двумя способами, то взять в качестве t_1 то значение, которое дает меньшее значение для координаты x точки $\Phi + t\,1$.

5. Подобрать по тому же признаку числа t_2 и t_3 для точек Ψ и $\Phi - \Psi$. Если это возможно, то только одним способом.

6. Если для точки Ψ найдется подходящее число t_2, сравнить абсциссы точек Φ_0, Ψ_0 и $\Phi - \Psi + t_3 1$. Та точка, абсцисса которой будет наименьшая, будет лежать внутри единичного куба или будет смежным с 1 по Ox относительным минимумом.

7. Если для Ψ подходящего числа t_2 не найдется, то подыскать число t по тому же признаку для точки $\Phi + \Psi$ и, если таковое найдется, сравнить абсциссы точек Φ_0, $\Phi - \Psi + t_3 1$ и $\Phi + \Psi + t_4 1$.

8. Если для точки $\Phi + \Psi$ не найдется подходящего числа t_4 и, кроме того, $|\eta_\psi| > 1$, $\xi_{\varphi+\psi} < 1$, то подобрать число t_5 по тому же признаку для точки $2\Phi + \Psi$ и сравнить абсциссы точек Φ_0 и $2\Phi + \Psi + t_5 1$.

Пример. Найти основные единицы поля $\Omega(\rho)$, где ρ задано уравнением $\rho^3 = 6\rho + 2$.

Решение. Основные единицы изображаются геометрически в виде основных автоморфизмов умножения для решетки, изображающей совокупность всех целых алгебраических чисел поля $\Omega(\rho)$. Эта решетка будет иметь степенной базис $1, \rho, \rho^2$, в чем легко убедиться по способу отыскания базиса, описанному в главе II.

Для построения цепочек относительных минимумов нам нужно знать приближенные значения для координат точек базиса, т. е. для корней и квадратов корней уравнения $\rho^3 = 6\rho + 2$.

Приводим эти значения:

$$\rho \approx 2.6017; \quad \rho' \approx -2.2618; \quad \rho'' \approx 0.3399;$$
$$\rho^2 \approx 6.7688; \quad \rho'^2 \approx 5.1157; \quad \rho''^2 \approx 0.1155.$$

Условимся откладывать координату ρ по оси OX, ρ' по OY и ρ'' по OZ. Будем теперь строить x-цепочку, исходя из точки (1, 1, 1), являющейся, очевидно, относительным минимумом. Прежде всего мы должны спроектировать базис решетки параллельно рациональному направлению на плоскость $y+z=0$. Координаты проекций или, как мы называем, проколов находятся по формулам

$$\xi=\frac{2x-y-z}{2};\quad \eta=\frac{y-z}{2}.$$

Это нам даст для проколов ρ и ρ^2 следующие координаты:

$$\rho \ldots (3.90, \quad -0.96);$$
$$\rho^2 \ldots (4.15, \quad 2.50).$$

Делаем теперь приведение базиса для решетки проколов посредством алгорифма непрерывных дробей, который нужно применить к ординатам проколов ρ и ρ^2.

$$\rho^2+2\rho \ldots (11.96, \quad 0.58);$$
$$\rho^2+3\rho \ldots (15.86, \quad -0.38).$$

Мы должны за точку φ принять прокол $\rho^2+3\rho$ и за точку ψ прокол $\rho^2+2\rho$. Относительный минимум, смежный с (1, 1, 1), может быть только точкой, принадлежащей проколам $\varphi-\psi$, φ и ψ, так как прокол $\varphi+\psi$ отстоит от φ в направлении OX больше чем на одну единицу.

Параллель, соответствующая проколу $\varphi-\psi$, содержит точку ρ, пространственные координаты которой (2.60, -2.26, -0.34). Эта параллель не содержит точки внутри призмы $|y|\leqslant 1$, $|z|\leqslant 1$.

Параллель, соответствующая проколу ψ, содержит точку $\rho^2+2\rho$, пространственные координаты которой (11.97; 0.59; -0.56). Это будет единственная точка параллели, лежащая внутри призмы $|y|\leqslant 1$, $|z|\leqslant 1$.

Точки, соответствующие проколу φ, можно не исследовать, так как их абсциссы будут наверное больше абсциссы точки $\rho^2+2\rho$.

Итак, смежным по OX с (1, 1, 1) относительным минимумом будет точка $\rho^2+2\rho$.

Для того чтобы найти следующий относительный минимум, делим исходную решетку на $\rho^2+2\rho$. Получим новую решетку, ступенчатый базис которой будет

$$\left(1, \quad \frac{\rho}{2}, \quad \frac{\rho^2}{2}\right).$$

Затем в этой решетке повторяем тот же процесс.

Проколы базиса:

$$\frac{\rho}{2} \ldots (1.95, \quad -0.48),$$
$$\frac{\rho^2}{2} \ldots (2.08, \quad 1.25).$$

Приведенные проколы:

$$\frac{\rho}{2} \ldots (1.95, -0.48) \ldots \varphi,$$
$$\frac{\rho^2-\rho}{2} \ldots (0.13, \quad 1.73) \ldots \psi.$$

Проколы ψ, $\psi-\varphi$ и $\psi+\varphi$ находятся за пределами полосы $|\eta|<1$. Поэтому относительный минимум, смежный с (1, 1, 1), принадлежит проколу φ. В параллели, соответствующей проколу φ, содержится точка $\frac{\rho}{2}$ с пространственными координатами (1.30, -1.13, -0.17). Внутри призмы $|y|\leqslant 1$; $|z|\leqslant 1$ будет содержаться только одна точка этой параллели $\frac{\rho}{2}+1$. Эта точка

и будет смежным по OX относительным минимумом для (1, 1, 1). Деление на $\frac{\rho}{2}+1$ переводит решетку $\left(1, \frac{\rho}{2}, \frac{\rho^2}{2}\right)$ в решетку $(1, \rho, \rho^2)$. Следовательно, дальше x-цепочка будет продолжаться периодически. Единица ε_1 равна

$$(\rho^2+2\rho)\left(\frac{\rho}{2}+1\right)=2\rho^2+5\rho+1.$$

Для отыскания единицы ε_2 мы должны строить z-цепочку тем же алгорифмом.

Проколы базиса на плоскости $x+y=0$:

$$\rho \ldots (-0.51,\ 2.43),$$
$$\rho^2 \ldots (-5.83,\ 0.83).$$

Приведенный базис решетки проколов:

$$\rho-3\rho^2 \ldots (16.97,\ -0.05) \ldots \varphi,$$
$$\rho-2\rho^2 \ldots (11.14,\ -0.78) \ldots \psi.$$

Исследовать нужно точки параллелей, соответствующих проколам $\varphi-\psi$, ψ и φ.

Параллель $\varphi-\psi$ содержит точку $-\rho^2$. Ее пространственные координаты $(-6.77, -5.12, -0.12)$. В этой параллели найдется точка внутри призмы $|x|\leqslant 1$; $|y|\leqslant 1$, именно $-\rho^2+6$. Проколы φ и ψ теперь незачем исследовать, так как они отстоят больше чем на 1 от прокола $\varphi-\psi$. Итак, смежный по OZ с (1, 1, 1) относительный минимум есть $-\rho^2+6$. Деление на $-\rho^2+6$ переводит исходную решетку в решетку

$$\left(1, \frac{\rho}{2}, \frac{\rho^2}{2}\right).$$

Следовательно, $-\rho^2+6$ ассоциировано с элементом $\rho^2+2\rho$ x-цепочки. Единица ε_2 находится, как их отношение:

$$\varepsilon_2=\frac{-\rho^2+6}{\rho^2+2\rho}=2\rho^2-\rho-11.$$

Пример решен.

Б. СЛУЧАЙ $D<0$

§ 60. Теорема Вороного о соседнем относительном минимуме

После того как мы в предыдущих параграфах подробно рассмотрели обобщение алгорифма непрерывных дробей, предложенное Вороным для случая $n=3$, $\tau=0$, мы перейдем к изложению алгорифма, предложенного Вороным для случая $n=3$, $\tau=1$, т. е. сигнатурного пространства $R_{3,1}$. Мы будем рассматривать в $R_{3,1}$ совершенно произвольную трехмерную решетку, одной из точек которой является начало координат. Мы будем требовать только, чтобы решетка удовлетворяла следующим двум условиям: 1°. в решетке нет делителей нуля, т. е. точек, отличных от начала, у которых, если ξ, η, ζ координаты в $R_{3,1}$, либо $\xi+i\eta=0$, либо $\zeta=0$, иначе говоря, нет точек ни на оси ξ, ни в плоскости ξ, η, т. е. параметры $\rho=\sqrt{\xi^2+\eta^2}$ и $|\zeta|$ всякой точки, кроме точки O, не равны нулю; 2°. в решетке нет точек, кроме друг другу симметричных по отношению к началу координат, с одинаковыми параметрами ρ. Заметим, что неприводимые решетки, повторяющиеся умножением, и рационально связанные с ними решетки, которые нам будут в дальнейшем наиболее интересны, удовлетворяют обоим этим условиям, так как условие 1° и есть условие неприводимости, а условие 2° удовлетворяется потому, что, если бы в такой

решетке были две точки ξ, η, ζ и $\bar{\xi}, \bar{\eta}, \bar{\zeta}$, для которых $\rho = \bar{\rho}$, т. е. $\xi^2 + \eta^2 = \bar{\xi}^2 + \bar{\eta}^2$, то мы имели бы из $(\xi^2 + \eta^2)\zeta = n$ и $(\bar{\xi}^2 + \bar{\eta}^2)\bar{\zeta} = \bar{n}$, где n и $\bar{n}$, как нормы этих точек, числа рациональные, что $\bar{\zeta} = \zeta\frac{\bar{n}}{n}$; но тогда и $\bar{\xi} + i\bar{\eta} = (\xi + i\eta)\frac{\bar{n}}{n}$, и, следовательно, $\bar{\rho} = \pm\rho\frac{\bar{n}}{n}$, т. е. $\frac{\bar{n}}{n} = \pm 1$. Но это значит, что либо точка $\bar{\xi}, \bar{\eta}, \bar{\zeta}$, либо точка $-\bar{\xi}, -\bar{\eta}, -\bar{\zeta}$, ей симметричная по отношению к началу, имеют одинаковые ζ, и, следовательно, разность точки ξ, η, ζ и этой точки имеет $\zeta = 0$, т. е. есть точка O. Таким образом, при $\bar{\rho} = \rho$ только и может быть, что либо точка $\bar{\xi}, \bar{\eta}, \bar{\zeta}$ совпадает с точкой ξ, η, ζ, либо ей симметрична по отношению к началу, т. е. есть точка $-\xi, -\eta, -\zeta$.

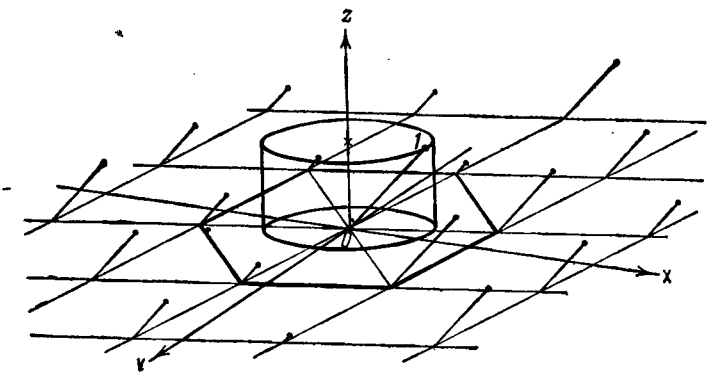
В сигнатурном пространстве $R_{3,1}$ норменное тело точки есть прямой круговой цилиндр с центром в начале координат, осью которого является ось ζ, и на окружности одного из оснований которого находится рассматриваемая точка. Если точка M решетки, удовлетворяющей условиям 1° и 2°, есть относительный минимум этой решетки, т. е. внутри ее норменного цилиндра нет других точек этой решетки, кроме точки O, лежащей в его центре, то на границе его, кроме точки M, лежащей на окружности одного из его оснований, лежит только еще одна точка $-M$, симметричная с точкой M по отношению к началу координат, на окружности другого его основания, так как иначе в решетке были бы две точки, несимметричные друг с другом по отношению к началу с одинаковыми ρ, т. е. нарушалось бы условие 2°, либо две точки, несимметричные по отношению к началу с одинаковыми ζ, но тогда разность их давала бы делитель нуль, которого не может быть в силу условия 1°. Заметим еще, что для всей теории относительных минимумов достаточно рассматривать только точки решетки верхнего полупространства $R_{3,1}$, т. е. только точки с $\zeta > 0$, так как и решетка и норменное тело симметричны по отношению к началу координат, и для всякого относительного минимума имеется относительный минимум, симметричный ему по отношению к началу координат.

Если, исходя от какого-нибудь относительного минимума ϕ_1, производить процесс, описанный для любого n и τ в § 4, а именно, в рассматриваемом случае $n = 3$, $\tau = 1$ увеличивать радиус норменного цилиндра, не меняя его высоты, то первая точка ϕ_2 с $\zeta > 0$, на которую наткнется этот цилиндр (своею боковою поверхностью), будет, во-первых, в силу условия 2° только одна; и, во-вторых, она будет опять относительным минимумом, и притом соседним с ϕ_1 относительным минимумом в сторону увеличения ρ, т. е. таким, что не будет относительных минимумов ϕ^*, для которых $\rho_1 < \rho^* < \rho_2$. Относительным минимумом точка ϕ_2 будет потому, что ее норменный цилиндр есть часть этого увеличивающегося цилиндра, который до того, как он наткнулся на эту точку ϕ_2, остается пустым внутри (кроме точки O), а соседним с ϕ_1 в сторону увеличения ρ потому, что если бы был между ними промежуточный по величине своего ρ относительный минимум ϕ^*, то высота его цилиндра была бы меньше чем у ϕ_1, так как иначе его цилиндр содержал бы внутри себя точку ϕ_1, и ϕ^* не был бы относительный минимум или содержал бы две точки на одном из своих оснований, чего быть не может. Но в таком случае при увеличении радиуса цилиндра ϕ_1 первой точкой, на которую наткнулся бы этот цилиндр, была бы, против предположения, не точка ϕ_2, а точка ϕ^*. Продолжая этот процесс дальше, так же начиная от ϕ_2, перейдем к соседнему с ϕ_2 в сторону увеличения ρ относительному минимуму ϕ_3 и т. д.

Вороной называет обобщением алгорифма непрерывных дробей на сигнатурное пространство $R_{3,1}$ всякий алгорифм, дающий возможность в данной решетке в $R_{3,1}$, удовлетворяющей условиям 1° и 2°, найти один относительный минимум ϕ_1 и затем находить друг за другом последовательные относительные минимумы, следующие за ним в сторону возрастания ρ.

(Вороной рассмотрел также еще алгорифм для $R_{3,1}$, при котором ищутся относительные минимумы в сторону возрастания ζ, но мы его рассматривать не будем.)

Пусть M некоторая точка, отличающаяся от точки O рассматриваемой решетки, удовлетворяющей условиям 1° и 2°, которая может быть и не относительным минимумом, но *примарна*, т. е. такова, что на отрезке OM нет других точек этой решетки. В таком случае OM можно принять за один из трех векторов базиса рассматриваемой решетки. Поэтому все точки решетки лежат на прямых, параллельных OM, причем на каждой из таких прямых лежит равномерный ряд точек, такой, что расстояние между двумя соседними точками в нем равно длине отрезка OM. Такой ряд точек мы называем, как в § 15, параллелью точек. Прямые, на которых лежат эти параллели точек, проходят через точки двухмерной решетки, построенной на двух других векторах базиса рассматриваемой трехмерной решетки, и, следовательно, пересекают плос-



Черт. 34.

кость $\xi\eta$ также по некоторой двухмерной решетке, которую мы будем обозначать через S и которая является проекцией этой двухмерной решетки, параллельно направлению OM. Из точек решетки S только в одной лежит точка рассматриваемой трехмерной решетки, а именно в точке O. В остальных же точках S в силу условия 1° ее точек нет. Точку S, в которой прямая параллели точек пересекает плоскость $\xi\eta$, мы будем называть *основанием* этой параллели. Отрезок прямой каждой из параллелей, кроме проходящей через точку O, от ее основания до первой на ней лежащей точки рассматриваемой 3-мерной решетки с положительным ζ мы будем называть *гвоздиком*, соответствующим этой параллели, а самую эту точку нашей рассматриваемой решетки — *шапочкой* этого гвоздика, или шапочкой, соответствующей данной точке S. Все гвоздики параллельны вектору OM и по длине больше нуля и меньше, чем длина OM (на черт. 34 точка M обозначена *1*, а оси *x*, *y*, *z*).

Рассмотрим в двухмерной решетке S оснований гвоздиков, соответствующих примарной точке M рассматриваемой трехмерной решетки, остроугольный основной треугольник, т. е. так называемый приведенный треугольник Зеллинга (см. последнее приложение к русскому переводу курса теории чисел Дирихле), и именно тот из 6 таких треугольников, сходящихся в точке O, который охватывает отрицательное направление оси ξ. Пусть его вершины суть начало координат (0, 0) и точки (1, 0), (0,1) (мы пишем координаты этих точек в плоскости $\xi\eta$, выбрав за координатные векторы стороны этого треугольника, исходящие из начала). Мы будем называть шапочками Вороного шапочки 7 гвоздиков, вбитых в точках (1, 0), (0, 1), (— 1, 0), (0, — 1), (1, — 1), (— 1, 1), (1, 1). Ту из этих 7 шапочек Вороного, которая имеет наименьшее ρ, мы будем называть приведенной шапочкой Вороного, соответствующей данной примарной точке M рассматриваемой нами решетки, удовлетворяющей условиям 1° и 2°.

Алгорифм, предложенный Вороным для розыскания в случае $n=3, \tau=1$ последовательных относительных минимумов, расположенных по возрастанию ρ, основан на следующей геометрической теореме.

Теорема. *Если приведенная шапочка Вороного ϕ, соответствующая примарной точке M рассматриваемой решетки, удовлетворяющей условиям 1° и 2°, лежит вне норменного цилиндра точки M, то M есть относительный минимум решетки и ϕ соседний с M в сторону возрастания ρ относительный минимум. Если же ϕ лежит внутри норменного цилиндра точки M, то M не относительный минимум, и найдена точка ϕ, лежащая внутри норменного цилиндра M.*

Для доказательства этой замечательной теоремы мы рассмотрим некоторые свойства систем точек, которые мы называем приближенными решетками или приближенно правильными системами. Пусть S — двухмерная решетка точек. Сопоставим в плоскости решетки S всем ее точкам одинаковые и одинаково расположенные, каждая относительно своей точки, области σ.

Под приближением решеткой S' мы будем понимать систему точек, о которых только и известно, что каждая из них находится внутри или на границе своей области σ, так что каждой точке S соответствует своя область σ, и в каждой такой области σ находится где-то одна и только одна точка S'. Точки S' могут находиться не в одинаковых местах областей σ, т. е. система S', вообще говоря, не представляет собою решетки. Область σ мы называем областью приближения, а величину радиуса r наименьшего круга, описанного вокруг точки S, такого, что вся область приближения σ, соответствующая этой точке, лежит внутри этого круга, будем называть радиусом приближения приближенной решетки S' относительно решетки S.

В общей теории двухмерных решеток S существуют следующие теоремы (см. например, приложение к русскому переводу курса теории чисел Дирихле): 1) основной треугольник решетки S всегда может быть выбран, и притом только одним способом (если не считать отличающихся от него ему гомологичных, т. е. получающихся из него параллельными переносами решетки, и им симметричных по отношению к точке O), остроугольным (а если прямоугольным, то двумя способами); такой основной треугольник называется приведенным по Зеллингу; 2) кратчайший параметр a решетки S (т. е. кратчайший отрезок, соединяющий две точки S) есть одна из сторон этого треугольника; 3) наименьшая высота h приведенного по Зеллингу основного треугольника не меньше $\frac{a}{\sqrt{2}}$.

Заметим еще, что 6 треугольников Зеллинга, сходящихся в точке O, образуют шестиугольник, который можно назвать шестиугольником Зеллинга, или 1-ым шестиугольником Зеллинга, и что все вообще точки решетки S расположены на периметрах 1-го, 2-го, 3-го и т. д., гомотетичных по отношению к точке O, шестиугольников Зеллинга, которые получаются из 1-го гомотетичным увеличением его из точки O линейно в 2, 3 и т. д. раз. (см. черт. 36).

Основываясь на этих свойствах решеток, можно доказать следующую лемму о приближенно правильных системах: *ближайшая к точке O решетки точка приближенной к ней решетки принадлежит не далее как n-му приведенному шестиугольнику, где $n \leqslant \left(\frac{2r}{a}+1\right)\sqrt{2}$.*

Доказательство. Ближайшая к точке O системы S точка системы S' должна быть от точки O, очевидно, не дальше, чем на расстоянии $a+r$, где a наименьший параметр системы S, а r радиус приближения системы S' к системе S. Пусть наименьшее расстояние от точки O до периметра 1-го шестиугольника Зеллинга есть h. Тогда соответственное расстояние для 2-го шестиугольника есть $2h$ и т. д. Если ближайшая к точке O точка S' принадлежит n-му шестиугольнику Зеллинга, то

$$nh - r \leqslant a + r,$$

откуда

$$n \leqslant \frac{a+2r}{h},$$

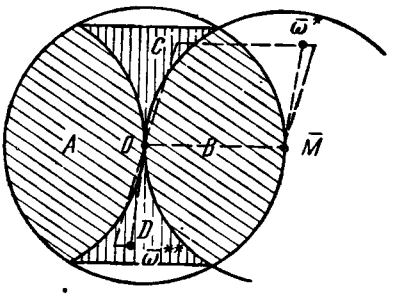
но

$$h \geqslant \frac{a}{\sqrt{2}},$$

и, следовательно, мы получаем

$$n \leqslant \left(\frac{2r}{a}+1\right)\sqrt{2}.$$

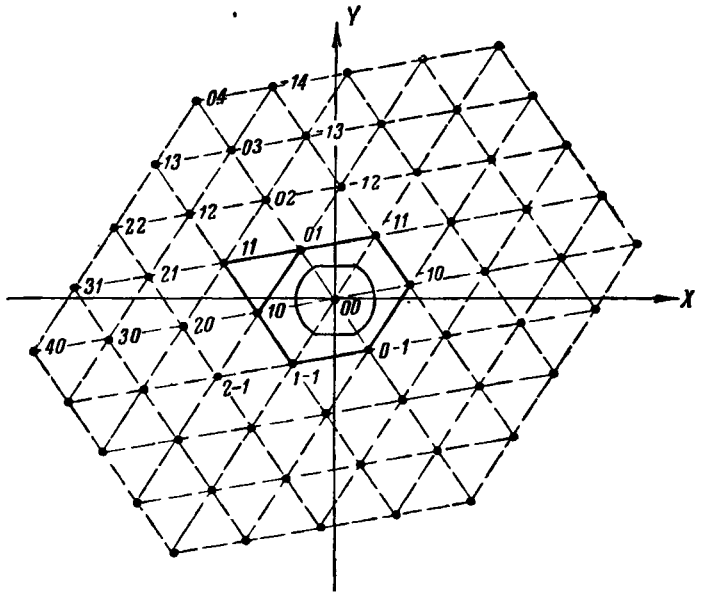
Применение этой леммы о приближенной решетке к доказательству предыдущей теоремы основано на следующем. Спроектируем ортогонально на плоскости ξ, η все шапочкн всех гвоздиков, соответствующих данной примарной точке M рассматриваемой трехмерной решетки. Получится на плоскости ξ, η неправнльная (так как гвоздики разной длины) система точек S', которая будет приближенной к двухмерной решетке S оснований гвоздиков с областью прнближения, имеющей внд отрезка, исходящего из точки S н совпадающего по длнне и направлению с ортогональной проекцией отрезка OM на плоскости $\xi\eta$. Радиусом приближения будет длина этой проекции, которую мы обозначим через r. Пусть ϕ есть та из 7 шапочек Вороного, которая имеет наименьшее ρ. Если она лежит внутри норменного цилиндра точки M, т. е. ее ортогональная проекция $\bar{\phi}$ иа плоскость $\xi\eta$ лежит внутри круга с центром в точке O и радиусом r, то M не относительный минимум, и ϕ точка, лежащая внутри норменного цилиндра точки M. Если принять эту точку ϕ за новую точку M и т. д., то мы придем, наконец, к такой точке M, что соответствующая ей проекция шапочки $\bar{\phi}$ не лежит внутри соответствующего ей круга r. Мы покажем, что в этом случае наименьший параметр a соответственной решетки S не меньше, чем $\frac{r\sqrt{3}}{2}$, и тогда, подставляя это значение a в формулу леммы, мы получим, что номер n шестиугольника Зеллинга, которому может принадлежать шапочка, имеющая наименьший радиус ρ из всех вообще шапочек, $\leqslant 4$. Исследовав затем каждую из 60 точек, лежащих на первых 4 шестиугольниках Зеллинга, мы покажем, что ближайшая шапочка есть одна из 7 шапочек Вороного, т. е. как раз, следовательно, шапочка ϕ, так как шапочкой ϕ мы назвали ту из 7 шапочек Вороного, которая имеет наименьшее ρ. А тогда и выйдет, что если $\bar{\phi}$ лежит вне круга r, то ϕ есть относительный минимум, так как при увеличении радиуса норменный цилиндр точки M может наталкиваться только на точки нашей решетки, имеющие ξ меньшее, чем у M, т. е. только на шапочки гвоздиков, а шапочка, имеющая из всего бесконечного числа шапочек наименьший ρ, есть шапочка ϕ. Кроме этого, отсюда же следует, что ϕ есть соседний с M относительный минимум.



Черт. 35.

Итак, покажем прежде всего, что если $\bar{\phi}$ лежит вне круга r, то $a \geqslant \frac{r\sqrt{3}}{2}$. Если мы предположим, что $\bar{\phi}$ лежит вне круга r, то и подавно проекции других 6 шапочек Вороного лежат вне этого круга, так как раднусы ρ их больше, чем радиус $\bar{\phi}$, т. е. все 7 шапочек Вороного лежат вне круга r. Покажем, что из этого уже следует вышенаписанное неравенство. Дело в том, что в этом случае основания (1, 0), (0, 1), (—1, 0), (0, —1), (1, —1), (—1, 1) соответ-

ствующих им гвоздиков не могут лежать внутри луночек A и B (черт. 35), так как если бы одна из этих точек лежала внутри луночки B, то симметричная с ней по отношению к началу лежала бы внутри луночки A, но тогда шапочка соответственного этой точке гвоздика лежала бы внутри норменного цилиндра точки M, а мы предполагаем, что этого нет. Покажем, что все основания эти лежат также вне областей C и D. Действительно, если бы одно их этих оснований лежало внутри одной из этих областей, например, внутри области C, то шапочка ω^* гвоздика ему соответствующего, лежала бы вне цилиндра M, так как если ϕ



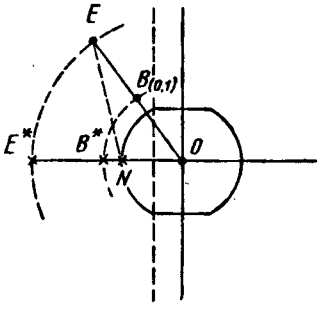
Черт. 36.

лежит вне цилиндра M, то остальные 6 шапочек Вороного, как имеющие бо́льшие ρ, и подавно, а следовательно ее проекция $\bar{\omega}^*$ лежала бы внутри внешней по отношению к кругу r части отрезка, исходящего из этого основания и равного и параллельного отрезку $O\bar{M}$. Но в таком случае, если провести из точки O вектор, равный $\bar{\omega}^*\bar{M}$, мы получим проекцию $\bar{\omega}^{**}$ шапочки Вороного, соответствующей основанию, симметричному с рассмотренным по отношению к началу, и эта шапочка ω^{**} окажется лежащей внутри цилиндра M. А между тем в рассматриваемом случае все шапочки Вороного должны лежать вне цилиндра M. Но ближайшая к точке O точка решетки S оснований гвоздиков принадлежит 1-му шестиугольнику Зеллинга, т. е. есть одна из 6 точек (1, 0), (0, 1), (—1, 0), (0, —1), (1, —1), (—1, 1), и, следовательно, наименьший параметр a решетки S в этом случае не меньше, чем расстояние от начала до периметра области ν, составленной из кусков A, B, C, D, т. е. не меньше, чем $\frac{r\sqrt{3}}{2}$.

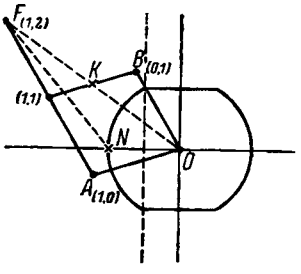
Применим теперь это ограниченне для нахождения номера шестнугольника Зеллинга, которому принадлежит шапочка, имеющая наименьшее ρ. Рассматривая, как было указано выше, систему S' ортогональных проекций шапочек на плоскость $\xi\eta$ (x, y), как приближенно правильную к решетке S, из формулы, даваемой леммой, мы получим в этом случае $n \leqslant \left(\frac{4}{\sqrt{3}}+1\right)\sqrt{2}$, т. е. $n<4, 6\ldots$, т. е. что шапочка с наименьшим ρ принадлежит, в случае когда шапочка ϕ

лежит вне цилиндра точкн M, не далее как 4-му шестнугольнику Зеллинга.

На 1-м, 2-м, 3-м и 4-м шестиугольниках Зеллинга лежнт всего 60 точек. Покажем, что 53-м из ннх не может прнпадлежать шапочка с нанменьшнм ρ, а что она может принадлежать только 7-ми из ннх, которые н суть основания Вороного. Мы будем, как раньше, обозначать основания гвоздиков координатамн (i, j), а проекцин соответствующих шапочек $(i, j)'$, так что совокупность точек (i, j) даст решетку S, а совокупность точек $(i, j)'$ систему S'. Расстояние от точки $(i, j)'$ до начала координат мы будем обозначать ρ_{ij}'. Покажем, что для каждой из точек $(i, j)'$, кроме точек $(1, 0)'$, $(0, 1)'$, $(-1, 0)'$, $(0, -1)'$,



Черт. 37.



Черт. 38.

$(1, -1)'$, $(-1, 1)'$, $(1, 1)'$, есть точка S' более близкая к точке O. Действительно, например, точка E' $(0, 2)'$ дальше от начала, чем точка B' $(0, 1)'$, что следует нз черт. 37, еслн прннять во вннмание, что точка (0, 1) лежнт вне области ν и что область приближения S' к S есть отрезок, совпадающий с $O\overline{M}$ по длнне и направлению, н, следовательно, мы можем вместо точек S', E' н B' рассматривать точкн S, E н B, но учнтывая расстояння не до точкн O, а от одной из сравниваемых точек до ближайшей, а от другой до дальнейшей точки отрезка ON. Пусть, например, B (черт. 37) лежит левее $x = -\frac{1}{2}r$, в таком случае ближайшая к точке E точка отрезка NO есть точка N, а самая далекая его точка от точкн B есть точка O, т. е. достаточно показать, что $EN > BO$. Это получается в снлу того, что B лежнт вне области ν н левее $x = -\frac{1}{2}r$, н следовательно, $BO > NO$, т. е. $E^*N > E^*B^*$, но в таком случае $EN > E^*N > E^*B^* = B^*O = BO$. Для случая, когда B лежит правее $x = -\frac{1}{2}r$, доказательство аналогнчно.

Такнм же способом можно нсключить точки $(2, 0)'$, $(2, 2)'$, $(0, 3)'$, $(0, 4)'$, $(3, 0)'$, $(4, 0)'$ н т. д.

Рассмотрнм теперь точку $F'(1, 2)'$. Предположив опять, что B лежит левее $x = -\frac{1}{2}r$, мы получнм, что достаточно доказать, что $FN > BO$. Но в снлу рассуждения, аналогичного предыдущему, $FN > KO$ (черт. 38), где K середнна FO. Но $KO > BO$, так как угол AOB острый. Аналогично можно нсключнть точку F, сравннвая ее с точкой B', н в случае, когда B лежит правее $x = -\frac{1}{2}r$.

Такнм же способом можно нсключнть точки $(2, 1)'$ $(1, 3)'$, $(-1, 3)'$, $(-1, 4)'$ н т. д. Останутся только 7 точек $(1, 0)'$, $(0, 1)'$, $(-1, 0)'$, $(0, -1)'$, $(1, -1)'$, $(-1, 1)'$, $(1, 1)'$. И, следовательно, получается, что точка M — отиосительный мннимум, так как даже из этих 7 точек та точка $\bar{\phi}$, радиус ρ которой наименьшнй, по предположенню, лежнт вне круга r, а точка ϕ — соседннй с M относительный миннмум.

Теорема Вороного, таким образом, полностью доказана.

§ 61. Алгорифм Вороного для вычисления, в случае $n=3$, $\tau=1$, цепочки последовательных относительных минимумов, идущих в сторону возрастания ρ, для того случая когда решетка рационально связана с неприводимой решеткой в $R_{3,1}$, повторяющейся умножением, или подобна такой решетке

Предположим, что решетка O состоит из целых или дробных точек кубического поля Ω_α, причем точка α удовлетворяет неприводимому кубическому уравнению $\zeta^3=q\zeta+n$ с целыми рациональными коэффициентами q и n, имеющему один вещественный корень α и два комплексно сопряженных α' и α'', т. е. отрицательный дискриминант $D=4q^3-27n^2$. Пусть M одна из „примарных" точек решетки O. Разделим все точки решетки O на точку M, тогда от деления точки M самой на себя получится точка 1, т. е. точка с координатами (1, 0, 1). Обозначим получившуюся решетку через O'. За одну из точек ее базиса, в виду того что M была примарной точкой, можно взять точку 1. Пусть базис $[1, \varphi, \psi]$ решетки O', выраженный через α, имеет вид

$$\left[1, \frac{m+m'\alpha+m''\alpha^2}{\sigma}, \frac{n+n'\alpha+n''\alpha^2}{\sigma}\right],$$

где числа $m, m', m'', n, n', n'', \sigma$ — целые рациональные. Тогда, как легко вычислить, положительная двойничная квадратичная форма, двухсторонник которой в плоскости ξ, η составлен векторами, идущими из точки O в точки этой плоскости, являющиеся проекциями параллельно отрезку 01 второй и третьей точки этого базиса, есть

$$\Phi=Ax^2+2Bxy+Cy^2,$$

где

$$\left.\begin{aligned} A&=m'^2+m'm''\alpha+m''^2(\alpha^2-q),\\ B&=m'n'+(m'n''+m''n')\frac{\alpha}{2}+m''n''(\alpha^2-q),\\ C&=n'^2+n'n''\alpha+n''^2(\alpha^2-q),\end{aligned}\right\} \qquad (1)$$

если помножить ее на σ. Заметим также еще, что если $\theta=t+t'\alpha+t''\alpha^2$, то квадрат расстояния ρ от точки θ до оси ζ есть

$$\rho^2=[(t+t''q)^2-t'(t'q+t''n)]+[t''^2n-tt']\alpha+[t'^2-t''(t+t''q)]\alpha^2. \qquad (2)$$

Мы получаем следующие шаги алгорифма.

(I). Если $m'n''-m''n'<0$, то заменяем базис $[1, \varphi, \psi]$ базисом $[1, \psi, \varphi]$. Геометрически это означает, что мы берем за первое число то из двух чисел φ, ψ, которое имеет меньший аргумент в плоскости $\xi\eta$.

(II). Вычисляем по формулам (1) коэффициенты A, B, C формы $\Phi=(A, B, C)$ Геометрически форма (A, B, C) изображает двухсторонник, задающий двухмерную решетку Y, соответствующий данному базису $[1, \varphi, \psi]$ пространственной решетки O'.

(III). Если $B<0$, то вместо A, B, C берем $C, -B, A$ и соответственно базис $[1, \varphi, \psi]$ заменяем базисом $[1, -\psi, \varphi]$.

(IV). Если условия $A-B>0$, $C-B>0$ или же хоть одно из них не удовлетворяются, то если $A<C$, преобразовываем форму подстановкой $\begin{pmatrix}1, -\delta\\ 0, 1\end{pmatrix}$, (а базис соответственно подстановкой $\begin{pmatrix}1, 0, 0\\ 0, 1, -\delta\\ 0, 0, 1\end{pmatrix}$), где $\delta=\left[\frac{B}{A}\right]$; а если $C<A$, то преобразовываем форму подстановкой $\begin{pmatrix}1, 0\\ -\delta, 0\end{pmatrix}$, где $\delta=\left[\frac{B}{C}\right]$. Эти два действия надо производить до тех пор, пока не будет одновременно $A-B>0$ и $C-B>0$. Тогда будут удовлетворяться все три „условия приведения" для формы (A, B, C), а именно $A-B>0$, $C-B>0$, $B>0$.

Все это — в соответствии с теорией приведения положительной двойничной формы, данной, например, в приложении к русскому переводу теории чисел Дирихле. Геометрически действия (III) и (IV) означают нахождение основного двухсторонника решетки S, дающего остроугольный треугольник.

(V). Если хоть одно из неравенств $\frac{m'-m''\alpha}{\sigma}=b>0$; $\frac{n'-n''\alpha}{\sigma}=d<0$ не удовлетворяется, причем тут σ, как существенно положительное число, можно не принимать во внимание, то мы находим из 6 пар чисел (b, d); $(-b, d)$; $(b-d, b)$; $(-b+d, -b)$; $(d, -b+d)$; $(-d, b-d)$ ту единственную, для которой оба эти неравенства удовлетворяются, и преобразовываем форму A, B, C) соответственной, по порядку, из 6 подстановок:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&1\\-1&0\end{pmatrix}\begin{pmatrix}-1&-1\\1&0\end{pmatrix}\begin{pmatrix}0&-1\\1&1\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix}.$$

Геометрически это преобразование означает выбор из 6 основных остроугольных треугольников системы S, сходящихся в точке 0 и составляющих 1-й шестиугольник Зеллинга, одного, именно охватывающего отрицательную ось ξ.

Заметим, что ни в одном из неравенств приведения, равно как и в неравенствах для b и d, не может быть знака равенства, так как, в силу неприводимости того уравнения, которому удовлетворяет α, мы получили бы во всех случаях из приравнивания нулю коэффициентов при 1, α, α^2, что либо $m'=m''=0$, либо $n'=n''=0$, но тогда решетка O' не была бы трехмерна.

(VI). Пусть путем всех предыдущих преобразований базис $[1, \varphi, \phi]$ преобразуется в базис $[1, \varphi_1, \phi_1]$. Тогда мы находим еще целые рациональные числа β и γ, такие, что числа $\bar{\varphi}=\varphi_1+\beta$; $\bar{\phi}=\phi_1+\gamma$ лежат между нулем и 1. Геометрически это обозначает переход к параллельному базису, точки $\bar{\varphi}$ и $\bar{\phi}$ которого на соответственных параллелях нижайшие, т. е. шапочки соответственных гвоздиков.

(VII). Вычисляем числа

$$a=\frac{2(m+m''q)-m'\alpha-m''\alpha^2}{2\sigma}; \quad c=\frac{2(n+n''q)-n'\alpha-n''\alpha^2}{2\sigma},$$

где числа $m, m', m'', n, n', n'', \sigma$, соответствующие базису $[1, \bar{\varphi}, \bar{\phi}]$. Далее мы полагаем $\theta_0=\bar{\varphi}$ или $1-\bar{\varphi}$ (в зависимости от того, какое из чисел a или $1-a<\frac{1}{2}$); $\theta_1=\bar{\phi}$ или $1-\bar{\phi}$ (в зависимости от того, какое из чисел c или $1-c<\frac{1}{2}$), если $\bar{\varphi}-\bar{\phi}>0$, то $\theta_2=\bar{\varphi}-\bar{\phi}$ или $1-\bar{\varphi}+\bar{\phi}$ (в зависимости от того, какое из чисел $a-c$ или $c-a<\frac{1}{2}$), если же $\bar{\phi}-\bar{\varphi}>0$, то $\theta_2=\bar{\phi}-\bar{\varphi}$ или $1-\bar{\phi}+\bar{\varphi}$ (в зависимости от того, какое из чисел $c-a$ или $a-c<\frac{1}{2}$). Найдя так 3 числа $\theta_0, \theta_1, \theta_2$, мы отбрасываем в них знаменатель, так как нам важна лишь относительная величина расстояний ρ, вычисляем по (2) соответственные этим точкам $\theta_0, \theta_1, \theta_2$ расстояния ρ_0, ρ_1, ρ_2 и находим два наименьших из них $\rho_g<\rho_h$. Однако если удовлетворены одновременно условия $\rho_2>\rho_0$, $\rho_2>\rho_1$, а также $\bar{\varphi}+\bar{\phi}<1$, $a+c<\frac{1}{2}$, то нужно найти еще 4-е число $\theta_3=\bar{\varphi}+\bar{\phi}$, вычислить по (2) ρ_3 ему соответственное и выбирать два наименьших $\rho_g<\rho_h$ уже из 3 чисел ρ_0, ρ_2, ρ_3.

Точки $1, \theta_g, \theta_h$ образуют базис решетки O, у которого второе число θ_g представляет собой соседний в сторону увеличения ρ с 1 относительный минимум, если $\rho_g>1$, а θ_h — следующую за θ_g по расстоянию ρ шапочку гвоздика. Если же $\rho_g<0$, точка θ_g лежит внутри нормального цилиндра точки 1.

Геометрически действия этого шага представляют собою следующее: $\bar{\varphi}$, $\bar{\psi}$ представляют собою шапочки Вороного, соответствующие основаниям (1, 0) и (0, 1); через (a, b) (c, d) обозначаем координаты ξ, η этих оснований; $1-\bar{\psi}$, $1-\bar{\varphi}$ суть шапочки Вороного, имеющие основаниями (—1, 0) и (0, —1); как легко видеть, из двух шапочек $\bar{\varphi}$ и $1-\bar{\varphi}$, если $a<\frac{1}{2}$, имеет меньшее ρ шапочка $\bar{\varphi}$, а если $1-a<\frac{1}{2}$, шапочка $1-\bar{\varphi}$; аналогично относительно шапочек $\bar{\psi}$ и $1-\bar{\psi}$: если $\bar{\varphi}-\bar{\psi}>0$, $\bar{\varphi}-\bar{\psi}$ есть шапочка (1, —1), а $1-\bar{\varphi}+\bar{\psi}$ — шапочка (—1, 1), причем, как легко видеть, из этих двух шапочек имеет меньшее ρ первая, если $a-c<\frac{1}{2}$, и вторая, если $c-a<\frac{1}{2}$; если же $\bar{\psi}-\bar{\varphi}>0$, то $\bar{\psi}-\bar{\varphi}$ есть шапочка (—1, 1) и $1-\bar{\psi}+\bar{\varphi}$ шапочка (1, —1), причем из этих двух шапочек имеет, как легко видеть, меньшее ρ первая, если $c-a<\frac{1}{2}$, и вторая, если $a-c<\frac{1}{2}$; этим способом, не вычисляя самих ρ по формуле (2) — что самое длинное — из каждой пары шапочек Вороного (1, 0) (—1, 0); (0, 1) (0, —1); (1, —1) (—1, 1) по одной отброшено, как заведомо более далекой, при помощи вычисления только a и c, которые вычисляются гораздо проще, чем ρ; остается еще вычислить ρ для 7-й шапочки Вороного (1, 1). Можно было бы это сделать и затем выбирать между тремя неотчеркнутыми из первых 6 и этой 7-й, — какая из этих 4 шапочек имеет наименьшее ρ, она и будет приведенной шапочкой Вороного. Однако, можно еще несколько сократить вычисление. Дело в том, что можно доказать (мы это доказательство опускаем), что ρ_3, соответствующее 7-й шапочке (1, 1), может быть кратчайшим только, если $\rho_2>\rho_3$, $\rho_2>\rho_1$, $\varphi+\psi<0$, $a+c<\frac{1}{2}$. Поэтому только в этом случае надо вычислять ρ_3, но зато уже не надо вовсе вычислять ρ_2 (т. е. опять за счет знания величин a и c мы избегаем вычисления одного из ρ). Точки $1, \theta_g, \theta_h$ всегда образуют базис O, так как, как легко видеть, основания их образуют в двухмерной решетке S основной ее треугольник.

(VIII). Базис $[1, \theta_g, \theta_h]$ заменяем базисом $\left[1, \frac{\theta_h}{\theta_g}, \frac{1}{\theta_g}\right]$, т. е. делим решетку O' на θ_g и приводим его к виду

$$\left[1, \frac{m+m'a+m''a^2}{\sigma}, \frac{n+n'a+n''a^2}{\sigma}\right],$$

причем числа m, m', m'' n, n', n'', σ мы вычисляем из аналогичных чисел для базиса $[1, \theta_g \theta_h]$ при помощи умножения числителей и знаменателей на ρ_g. Полученный новый базис будет базисом некоторой новой решетки O''.

Продолжая далее указанные действия, мы получаем последовательно решетки O^{III}, O^{IV} и т. д.

Если примарная точка M исходной решетки O в ней не относительный минимум, т. е. 1 не относительный минимум в решетке O', то в силу теоремы Вороного приведенная шапочка Вороного θ_g будет лежать внутри норменного цилиндра точки 1. В решетке O' уже будет эта точка точкой 1 и если она в O'' опять не относительный минимум, то приведенная шапочка Вороного этой решетки O'' будет в свою очередь лежать в ее норменном цилиндре, а следовательно, и подавно в норменном цилиндре точки M и т. д. Следовательно, через конечное число шагов мы придем, наконец, к такой решетке O^l, в которой точка 1 уже относительный минимум. Всякая из следующих решеток цепочки $O, O', O'', \ldots$ получается из предыдущей, а следовательно, и из исходной решетки O делением на некоторую точку $R_{3,1}$, т. е. все эти решетки подобны. Таким образом точка 1, являющаяся относительным миниму-

мом в решетке O^l, получилась из некоторого относительного минимума ω исходной решетки O делением на него самого, а сама решетка $O^l = \frac{1}{\omega} O$.

Решетка O, как рациональная по отношению к неприводимой кубической решетке, повторяющейся умножением, имеет автоморфизмы умножения, но в таком случае цепочка ее относительных минимумов повторяется периодически, так как всякий относительный минимум определяет всю цепочку. Поэтому, начиная с решетки O^l, решетки O^l, O^{l+1}, O^{l+2}, ... будут уже периодически повторяться, так как в силу теоремы Вороного, начиная с решетки O^l, приведенная по отношению к точке 1 этой решетки шапочка Вороного уже будет всякий раз соседним с 1 в сторону увеличения ρ относительным минимумом этой решетки. Мы будем называть базис 1, θ_g, θ_h в том случае, когда 1 относительный минимум решетки, приведенным по Вороному. В виду единственности приведенного базиса Вороного в каждой данной решетке, что следует из правила выбора точек θ_g и θ_h, выходит, что если решетка O рациональна по отношению к неприводимой кубической решетке, повторяющейся умножением, то приведенные по Вороному базисы последовательных решеток O^l, O^{l+1}, O^{l+2}, ... повторяются периодически, причем тождественность двух таких базисов будет характеризоваться просто совпадением для них соответствующих чисел m, m', m'' n, n', n'', σ.

§ 62. Решение задачи подобия для решеток, рационально связаиных с одной и той же неприводимой кубической решеткой, повторяющейся умножением (т. е. с одним и тем же кубическим полем), или подобных таким решеткам

Пусть O_1 и O_2 две решетки, связанные с данным кубическим полем Ω_α. Для одной из них вычисляем предыдущим алгорифмом полный период приведенных базисов Вороного, а для другой доходим до первого, который получится, приведенного базиса Вороного. Очевидно, что решетки O_1 и O_2 подобны тогда и только тогда, когда этот приведенный базис второй заключается среди приведенных базисов первой.

Действительно, пусть O — некоторая решетка. Будем называть все подобные ей решетки, получаемые из нее делением на различные ее относительные минимумы, т. е. такие, в которых точка 1 относительный минимум, нормированными подобными ей решетками. Если O — решетка рациональная по отношению к решетке, повторяющейся умножением, то она имеет автоморфизмы, и, следовательно, различных нормированных, ей подобных, решеток ограниченное число.

Решетка $\overline{O}$, очевидно, тогда и только тогда подобна решетке O, когда хоть одна из нормированных ей подобных решеток находится среди нормированных решеток, подобных решетке O.

§ 63. Вычисление основного автоморфизма умножения решетки, рациональной по отношеиию к неприводимой решетке, повторяющейся умножением, или подобной такой решетке, в случае $n=3$, $\tau=1$

В случае $n=3$, $\tau=1$ все автоморфизмы умножения имеют вид $\varepsilon = \pm\varepsilon_0^m$, где ε_0 — некоторый основной автоморфизм умножения, равный наименьшей степени основного автоморфизма умножения ε_0 соответственной максимальной решетки, который есть автоморфизм заданной решетки, и m — все возможные целые рациональные показатели, как положительные, так и отрицательные, и нуль. Это непосредственно следует из общей теории, рассмотренной в § 4, если принять во внимание, что точек E, все параметры которых равны 1, в максимальной неприводимой решетке с $n=3$, $\tau=1$, нет, кроме точек 1 и -1.

Действительно, если $E=\zeta$, $E'=\xi+i\eta$, $E''=\xi-i\eta$, то параметры этой точки суть $\rho=\sqrt{\xi^2+\eta^2}$, $|\zeta|$, и если $|\zeta|=1$, то $\zeta=\pm 1$, и тогда в силу неприводимости решетки $E=\pm 1$, $E'=\pm 1$, $E''=\pm 1$, но все автоморфизмы умножения любой решетки, рационально связанной с неприводимой решеткой, повторяющейся умножением, суть, как доказано в § 4, автоморфизмы соответственной максимальной решетки. Если ε и η автоморфизм умножения рассматриваемой решетки, то $\varepsilon\eta$, очевидно, тоже ее автоморфизмы умножения. Если ε_0 основной автоморфизм умножения соответственной максимальной решетки и $\varepsilon_0=\varepsilon_0^{\mu}$ наинизшая его степень, которая есть автоморфизм умножения заданной решетки, то $\varepsilon_0^{k\mu}$, где k—любое целое рациональное число, следовательно, также есть автоморфизм умножения заданной решетки, никакая же степень ε_0^{t}, у которой t не делится на μ, не есть автоморфизм умножения заданной решетки, так как иначе, помножив ее на $\varepsilon_0^{k\mu}$ с соответственно подобранным k, мы получили бы степень ε_0^{ν} с показателем $\nu<\mu$, которая тоже автоморфизм умножения заданной решетки.

Для вычисления основного автоморфизма ε_0 заданной решетки, очевидно, достаточно вычислить полный период ее приведенных базисов Вороного, и тогда произведение всех вторых чисел всех этих базисов (первые их числа суть 1) и есть ε_0. Действительно, 2-я приведенная решетка, подобная заданной, получается из 1-й делением ее на ее первый относительный минимум, смежный с 1-й в сторону увеличения ρ, т. е. на второе число ее приведенного базиса Вороного; 3-я получается аналогично из 2-й делением на второе число приведенного базиса 2-й и т. д., и, наконец, если l-тая совпадает с 1-й, т. е. замыкается период, то l-тая получается из $l-1$-й делением $l-1$-й на второе число приведенного базиса $l-1$-й, и, следовательно, l-тая, совпадающая с 1-й, получается из 1-й делением 1-й на указанное произведение вторых чисел приведенных базисов 1-й, 2-й, 3-й, ... последовательных приведенных решеток, подобных данным.

Пример. Найти период относительных минимумов, начиная с 1 в поле $\Omega\sqrt[3]{19}$. Базис этого поля, т. е. базис решетки O', есть (см. например, § 25) $\left[1, \alpha, \frac{1+\alpha+\alpha^2}{3}\right]$, т. е. $m=0$, $m'=3$, $m''=0$; $n=1$, $n'=1$, $n''=1$ и $\sigma=3$. Вычисление α дают $\alpha\approx 2.67$; $\alpha^2\approx 7.12$.

I шаг. Мы имеем $m'n''-m''n''=3>0$, т. е. оставляем тот базис, который задан.

II шаг. Вычисляя по формуле (1) § 61 коэффициенты A, B, C формы Φ, получаем $\Phi=(9, 7.02, 10.79)$.

III и *IV шаги* не нужны, так как условия $A-B>0$, $C-B>0$, $B>0$ выполняются, т. е. эта форма приведенная.

V шаг. $b=m'-m''\alpha\approx 3>0$; $d=n'-n''\alpha\approx -1.67<0$, т. е. треугольник, соответствующий рассматриваемому базису, обнимает отрицательную полуось $-X$.

VI шаг. Находим целые рациональные числа β и γ из условий

$$0<\bar{\varphi}=\varphi_1+\beta=\alpha+\beta<1;\quad 0<\bar{\psi}=\psi_1+\gamma=\frac{1+\alpha+\alpha^2}{3}+\gamma<1,$$

получаем $\beta=-2$; $\gamma=-3$ и, следовательно, $\bar{\varphi}=-2+\alpha$; $\bar{\psi}=\frac{-8+\alpha+\alpha^2}{3}$.

VII шаг. Вычисляем числа a и c, получаем $a\approx -3.34$, $c\approx -4.30$.

Так как $a<\frac{1}{2}$, мы полагаем $\theta_0=\bar{\varphi}=-2+\alpha$; так как $c<\frac{1}{2}$, то $\theta_1=\bar{\psi}=\frac{-8+\alpha+\alpha^2}{3}$; так как $\bar{\varphi}>\bar{\psi}$ и $c-a<\frac{1}{2}$, то $\theta_2=1-\bar{\varphi}-\bar{\psi}=\frac{1-2\alpha+\alpha^2}{3}$.

Вычисляем по формуле (2) ρ_0, ρ_1, ρ_2, получаем $\rho_0 = 4 + 2\alpha + \alpha^2$; $\rho_1 = 5 + 3\alpha + \alpha^2$; $\rho_2 = \frac{13 + 7\alpha + \alpha^2}{3}$, причем $\rho_2 < \rho_0 < \rho_1$ и $1 < \rho_2$, т. е. первый приведенный базис:

$$\left[1, \frac{1 - 2\alpha + \alpha^2}{3}, -2 + \alpha\right]. \tag{1}$$

VIII шаг. Преобразуя этот базис делением на его средний член и затем круговой подстановкой, мы получаем базис

$$\left[1, \frac{-7 - \alpha + 5\alpha^2}{36}, \frac{13 + 7\alpha + \alpha^2}{36}\right]$$

решетки O''.

Повторяем для этого базиса снова все 8 шагов.

I. Тут $m'n'' - m''n' = -36 < 0$, т. е. заменяем этот базис базисом

$$\left[1, \frac{13 + 7\alpha + \alpha^2}{36}, \frac{-7 - \alpha + 5\alpha^2}{36}\right].$$

II. Вычисляем по формулам (1) квадратичную форму Ф, она получается (74.81, 73.99, 165.65).

III и IV. Форма эта приведенная.

V. Дополнительные условия $b > 0$, $d < 0$ удовлетворяются.

VI. Находим целые рациональные β и γ из $0 < \frac{13 + 7\alpha + \alpha^2}{36} + \beta < 1$ и $0 < \frac{-7 - \alpha + 5\alpha^2}{36} + \gamma < 1$, и получаем

$$\beta = 1, \ \gamma = 0, \text{ откуда } \bar{\varphi} = \frac{-23 + 7\alpha + \alpha^2}{36}; \ \bar{\psi} = \frac{-7 - \alpha + 5\alpha^2}{36}.$$

VII. $\bar{\varphi} \approx 0.08$; $\bar{\psi} \approx 0.72$; $a \approx -1.00$; $c \approx -0.65$, т. е.

$$\theta_0 = \frac{-23 + 7\alpha + \alpha^2}{36}; \ \theta_1 = \frac{-7 - \alpha + 5\alpha^2}{36}; \ \theta_2 = \frac{4 - 2\alpha + \alpha^2}{9}$$

и после вычисления по формулам (2) мы получим:

$$\rho_0 = \frac{11 + 5\alpha + 2\alpha^2}{36}; \ \rho_1 = \frac{4 + 13\alpha + \alpha^2}{36}; \ \rho_2 = \frac{2 + \alpha}{3}.$$

Так как $\rho_2 > \rho_0$; $\rho_2 > \rho_1$; $\bar{\varphi} + \bar{\psi} < 1$ и $a + c < \frac{1}{2}$, то вычисляем еще $\theta_3 = \bar{\varphi} + \bar{\psi} = \frac{-5 + \alpha + \alpha^2}{6}$ и соответственно $\rho_3 = \frac{1 + 4\alpha + \alpha^2}{6}$

В виду того, что $\rho_0 < \rho_1 < \rho_3$, мы получаем, что сам базис

$$\left[1, \frac{-23 + 7\alpha + \alpha^2}{36}, \frac{-7 + \alpha + 5\alpha^2}{36}\right] \tag{2}$$

есть приведенный базис O'', т. е. второй приведенный базис.

VIII. Преобразуя его делением на средний его член и затем круговой подстановкой, мы получаем снова 1-й приведенный базис.

Приведенные базисы (1) и (2) поэтому представляют период приведенных базисов.

Основная алгебраическая единица поля $\Omega\sqrt[3]{19}$, следовательно, равна:

$$\varepsilon_0 = \frac{1 - 2\alpha + \alpha^2}{3} \cdot \frac{-23 + 7\alpha + \alpha^2}{36} =$$

$$= \frac{-23 + 46\alpha - 23\alpha^2 + 7\alpha - 14\alpha^2 + 133 + \alpha^2 - 38 + 19\alpha}{108} = \frac{2 + 2\alpha - \alpha^2}{3}.$$

§ 64. Алгорифм для $D<0$, основанный на параллельном преобразовании разложимой формы решетки и ей полярной формы

В предыдущих параграфах мы выяснили, что основной автоморфизм трехмерной решетки сигнатуры 1, т. е. имеющей $D<0$, рационально связанной с решеткой, повторяющейся умножением и содержащей точку (1, 0, 1) в качестве одной из точек базиса, находится посредством действий, указанных в § 61.

1. Решетка проектируется на комплексную плоскость XOY параллельно рациональному направлению. Проекция будет иметь вид плоской решетки.

2. В проекции разыскивается приведенный шестиугольник Зеллинга.

3. В шестиугольнике Зеллинга разыскивается пара смежных вершин φ и ψ, лежащих по разные стороны от „вещественной оси" OX комплексной плоскости. Остальные вершины будут $-\varphi$, $-\psi$, $\varphi-\psi$, $\psi-\varphi$.

4. Для вершин шестиугольника Зеллинга и для точки $\varphi+\psi$ находятся „шапочки" — ближайшие к плоскости XOY точки решетки, имеющие положительную вещественную координату, проектирующиеся в рассматриваемые точки проекции.

5. Из „шапочек", соответствующих симметричным относительно начала координат точкам проекции, выбираются более близкие к вещественной оси.

6. Из выбранных таким образом четырех точек выбирается точка, ближайшая к оси OZ.

Выбранная в результате этих действий точка будет смежным с (1, 0, 1) относительным минимумом или, если сама точка (1, 0, 1) не является относительным минимумом, выбранная точка будет внутренней точкой для иорменного цилиндра точки (1, 0, 1).

7. Делим решетку на выбранную точку и начинаем процесс сначала для получившейся решетки.

Процесс повторяем до тех пор, пока в первый раз не появится снова исходная решетка. Получающийся таким образом множитель переводит решетку в себя и представляет собой основной автоморфизм.

Дадим способ производить все эти действия без приближенных вычислений координат точек базиса.

При сделанном предположении относительно решетки [решетка содержит (1, 0, 1) в качестве одной из точек базиса] положение решетки вполне определяется заданием своей формы Дирихле (см. § 9 и 23).

Условимся в следующих обозначениях. Координаты точек решетки будем обозначать через ρ, α и β, считая ρ — вещественной координатой α и β — компонентами комплексных координат. Сами комплексные координаты $\alpha \pm \beta i$ будем обозначать через ρ' и ρ''. Точки решетки будем обозначать теми же буквами, которыми обозначаем их вещественные координаты. Базис решетки будем обозначать $(1, \rho_1, \rho_2)$. Координаты точек решетки относительно базиса будем обозначать соответственно w, u, v, форму Дирихле для решетки будем записывать, как это было указано в § 23, в виде треугольного символа

$$\begin{matrix} H, & K, & L, & M \\ E, & F, & G & \\ B, & C & & \\ 1 & & & \end{matrix}$$

читая его как

$$w^3 + w^2(Bu + Cv) + w(Eu^2 + Fuv + Gv^2) + Hu^3 + Ku^2v + Luv^2 + Mv^3.$$

Базис решетки и ее форму Дирихле нам придется неоднократно подвергать преобразованиям. Обозначать же их будем все время одинаково, никак не отмечая изменения базиса и коэффициентов формы.

Вспомним при этом, что, подвергая базис преобразованию с некоторой матрицей, мы должны форму Дирихле подвергнуть преобразованию с транспонированной матрицей.

Переходим к рассмотрению отдельных действий алгорифма.

1-е действие. Проектирование решетки.

Пусть форма Дирихле для базиса $[1, \rho_1, \rho_2]$ равна

$$N(\rho) = \begin{matrix} HKLM \\ EFG \\ BC \\ 1 \end{matrix}$$

где $\rho = w + u\rho_1 + v\rho_2$.

Проекция точки ρ на комплексную плоскость параллельно рациональному направлению имеет координаты

$$\xi = u(\alpha_1 - \rho_1) + v(\alpha_2 - \rho_2), \quad \eta = u\beta_1 + v\beta_2.$$

Сопоставим решетке двойничную кубическую форму

$$f(u, v) = \eta(\xi^2 + \eta^2) = \eta(\xi + i\eta)(\xi - i\eta) = \frac{1}{2i}(\rho' - \rho'')(\rho' - \rho)(\rho'' - \rho).$$

Форма $f(u, v)$ имеет вещественные коэффициенты. Более того, она лишь постоянным множителем отличается от некоторой формы с рациональными коэффициентами, которую легко построить, определив контравариант Кэли для исходной формы Дирихле.

Действительно, форма Кэли лишь постоянным множителем отличается от формы

$$\begin{vmatrix} w & u & v \\ 1 & \rho_1' & \rho_2' \\ 1 & \rho_1'' & \rho_2'' \end{vmatrix} \cdot \begin{vmatrix} 1 & \rho_1 & \rho_2 \\ w & u & v \\ 1 & \rho_1'' & \rho_2'' \end{vmatrix} \cdot \begin{vmatrix} 1 & \rho_1 & \rho_2 \\ 1 & \rho_1' & \rho_2' \\ w & u & v \end{vmatrix}.$$

Положив в форме Кэли $w = 0$, мы получим форму, постоянным множителем отличающуюся от формы

$$[u(\rho_2' - \rho_2'') - v(\rho_1' - \rho_1'')] \cdot [u(\rho_2'' - \rho_2) - v(\rho_1'' - \rho_1)] \cdot [u(\rho_2 - \rho_2') - v(\rho_1 - \rho_1')],$$

из которой интересующая нас форма получается делением на $2i$ и заменой v на u и u на $-v$.

Таким образом, для того чтобы найти (с точностью до постоянного вещественного множителя) двойничную форму, соответствующую проекции исходной решетки, нужно найти форму Кэли

$$\begin{matrix} H'K'L'M' \\ E'F'G' \\ B'C' \\ A' \end{matrix}$$

взять из нее верхнюю строчку (что и значит положить $w = 0$) и составить форму

$$(M', -L', K', -H') = M'u^3 - L'u^2v + K'uv^2 - H'v^3.$$

Это и будет форма с рациональными коэффициентами, от которой форма $\eta(\xi^2 + \eta^2)$ отличается лишь вещественным постоянным множителем.

В случае, если исходная решетка представляла собой кольцо, эта форма будет совпадать с индексформой кольца, и ее можно найти, не обращаясь к построению контравариантa.

Однако даже и в этом случае, на втором шагу алгорифма, когда после деления на относительный минимум решетка перестанет быть кольцом, построение контравариантa необходимо, и потому контравариант следует вычислить с самого начала.

2-е действие. Отыскаиие приведенного шестиугольника Зеллинга.

Для того чтобы найти шестиугольник Зеллинга, достаточно найти хотя бы один базис, точки которого образуют остроугольный треугольник с началом координат. Таких базисов возможно шесть, и их точки образуют вершины шестиугольника Зеллинга. Кубическую двойничную форму, соответствующую такому базису, будем называть приведенной. Приведение кубической формы можно осуществить, не обращаясь к приближенным вычислениям, по той же схеме, как выполняется аналогичиое приведение для положительных квадратичных форм, пользуясь неравенством $bc-ad>0$ между коэффициеитами, выведенным в § 33, выполнение которого необходимо и достаточно для того, чтобы базисные векторы образовали острый угол. Пользуясь этим неравенством, можно приводить, как это было указано в § 33, кубическую форму по той же схеме, по которой проводится аналогичное приведение квадратичных положительных форм. Приводим эту схему.

α) Если сначала $bc-ad<0$, делаем подстановку $\begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix}$ несколько раз до тех пор, пока в первый раз не получится положительное $bc-ad$.

β) Производим подстановку $\begin{pmatrix}1, & 0\\ -1, & 0\end{pmatrix}$ максимально возможное число раз без нарушения положительности $bc-ad$.

γ) Производим подстановку $\begin{pmatrix}1, & -1\\ 0, & 1\end{pmatrix}$ максимально возможное число раз без нарушеиия положительности $bc-ad$.

Затем чередуем операции β и γ до тех пор, пока не станет невозможным их дальиейшее применение.

Форма, которую мы получим в результате этих операций, и будет приведенной формой.

Одновременно нужно подвергать преобразоваииям форму Дирихле и форму Кэли, преобразуя переменные u и v в форме Дирихле ковариантио преобразованиям двойничной формы, а в форме Кэли коитравариантно.

3-е действие. Прежде всего нам нужно перейти от одного из остроугольных базисных треугольников ко всем остальным. Для этого нужно в приведенной форме пять раз сделать подстановку $\begin{pmatrix}0, & -1\\ 1, & -1\end{pmatrix}$. Из исходной формы и пяти новых нужно выбрать форму, соответствующую тому треугольнику, вершины которого лежат по разные стороны от оси $O\xi$. Знаки координат η_1 и η_2 вершин такого треугольника должны быть противоположиы. Из формул, определяющих коэффициенты формы через базис, мы видим, что знаки η_1 и η_2 совпадают соответственно со знаками коэффициентов a и d. Следовательно, из шести приведенных форм нужно выбрать ту, для которой знаки a и d противоположны. Таких форм обнаружится две, отличающиеся знаком. Которую избрать из этих двух,— безразлично.

Осуществив выбор двойничной формы, необходимо подвергнуть соответствующему преобразованию формы Дирихле и Кэли.

4-е, 5-е и 6-е действия целесообразно провести сначала для точек φ и ψ выбранного базиса и лишь затем обратиться к исследованию точек $\varphi-\psi$ и $\varphi+\psi$. Мы дадим описание этих действий для точек φ и ψ.

4-е действие. Пусть

$$N(w+u\varphi+v\psi)=\frac{HKLM}{EFG}{BC}{1}$$

— форма Дирихле после первых трех действий.

Мы должны теперь перейти от точек φ, ψ к их „шапочкам", т. е. точкам $\varphi+t_1$, $\psi+t_2$ при таких целых t_1, t_2, что

$$0<\varphi+t_1<1;\quad 0<\phi+t_2<1.$$

Найти числа t_1 и t_2 легко, так как знак вещественной координаты и знак нормы совпадают.

Но нормы чисел $t_1+\varphi$ и $t_2+\phi$ легко находятся из формы Дирихле

$$N(t_1+\varphi_1)=t_1^3+Bt_1^2+Et_1+H.$$

t_1 представляет собой наименьшее целое число, для которого $N(t_1+\varphi)>0$. Следовательно, t_1 будет наименьшим целым числом, бо́льшим корня уравнения

$$t^3+Bt^2+Et+H=0.$$

Таким же образом t_2 будет наименьшим целым числом, бо́льшим корня уравнения

$$t^3+Ct^2+Gt+M=0.$$

Для перехода к базису, составленному из „шапочек", нужно преобразовать форму Дирихле подстановками

$$\begin{pmatrix}1 & t_1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \quad \text{и} \quad \begin{pmatrix}1 & 0 & t_2\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Форму Кэли нужно подвергнуть контравариантным преобразованиям.

5-е действие. Если ρ есть „гвоздик" для проекции ω, то для проекции $-\omega$ гвоздиком будет $1-\rho$. Таким образом для осуществления пятого действия, нужно уметь выбрать из точек ρ и $1-\rho$ ту, которая лежит ближе к оси OZ. Квадрат расстояния точки ρ от OZ равен, очевидно, $\rho'\rho''$.

Таким же образом квадрат расстояния точки $1-\rho$ до оси OZ равен $(1-\rho')(1-\rho'')$. Составим разность этих квадратов расстояний

$$\rho'\rho''-(1-\rho')(1-\rho'')=\rho'+\rho''-1=s-1-\rho,$$

где $s=\rho+\rho'+\rho''$.

Эта разность будет положительной или отрицательной в зависимости от знака своей нормы $N(s-1-\rho)$, которую легко найти, зная форму Дирихле и выражение ρ через базис.

Итак, если $N(s-1-\rho)<0$, то точка ρ расположена ближе к OZ, чем $1-\rho$, если $N(s-1-\rho)>0$, то точка ρ дальше от OZ.

Применяя это к базису φ, ϕ решетки, с которым мы приходим после первых четырех действий, получим следующие неравенства

Если	$(E-B+1)(B-1)<H$,	то	φ	ближе к OZ,	чем $1-\varphi$,
„	$(E-B+1)(B-1)>H$,	„	φ	дальше от OZ,	„ $1-\varphi$,
„	$(G-C+1)(C-1)<M$,	„	ϕ	ближе к OZ,	„ $1-\phi$,
„	$(G-C+1)(C-1)>M$,	„	ϕ	дальше от OZ,	„ $1-\phi$.

После рассмотрения этих неравенств перейдем, в случае надобности, от базиса $[1, \varphi, \phi]$ к одному из базисов $[1, \varphi, 1-\phi]$, $[1, 1-\varphi, \phi]$ или $[1, 1-\varphi, 1-\phi]$. При этом придется подвергнуть формы Дирихле и Кэли соответствующим преобразованиям.

6-е действие. Пусть

$$N(w+u\varphi+v\phi)=\begin{matrix}HKLM\\ EFG\\ BC\\ 1\end{matrix}$$

— форма Дирихле после пятого действия.

Мы должны выяснить, которая из точек φ, ψ расположена ближе к OZ Составляем разность квадратов расстояний от этих точек до OZ.

$$\varphi'\varphi'' - \psi'\psi'' = \frac{H}{\varphi} - \frac{M}{\psi} = \frac{H\psi - M\varphi}{\varphi\psi}.$$

Знак этой разности совпадает со знаком ее нормы, которая легко находится из формы Дирихле:

$$N(\varphi'\varphi'' - \psi'\psi'') = \frac{N(H\psi - M\varphi)}{N(\varphi)\cdot N(\psi)} = \frac{MH^3 - LMH^2 + KM^2H - HM^3}{HM} =$$
$$= H^2 - LH + KM - M^2.$$

Следовательно, если $H^2 - LH + KM - M^2 < 0$, то точка φ лежит ближе к OZ, чем точка ψ, и, наоборот, ψ ближе к OZ, чем φ при противоположном неравенстве.

После этого нужно перейти (посредством соответствующих преобразований формы Дирихле) от базиса $[1, \varphi, \psi]$ к одному из базисов $[1, \varphi, \psi - \varphi]$ или $[1, \varphi - \psi, \varphi]$ в зависимости от того, которая из точек φ и ψ расположена ближе к OZ. Затем снова проделать действия 4, 5, 6 над получившейся формой Дирихле.

Если при этом окажется, что точка $\pm(\varphi - \psi)$ (или параллельная ей точка) является ближайшей к OZ по сравнению с φ и ψ, то вычисления окончены. Ближайшая точка будет представлять собой смежный с 1 относительный минимум или точку, лежащую внутри нормального цилиндра точки 1. Если же ближайшей окажется φ или ψ, то возвращаемся к форме, соответствующей базису $[1, \varphi, \psi]$.

Преобразуем снова форму, на этот раз к одному из базисов $[1, \varphi, \varphi + \psi]$ или $[1, \varphi + \psi, \psi]$ в зависимости от того, какая из точек φ или ψ расположена ближе к OZ. Над этой формой производим действия 4, 5 и 6. Ближайшая к OZ точка и будет искомой точкой — соседним с 1 относительным минимумом или внутренней точкой нормального цилиндра точки 1. Останавливаемся окончательно на базисе, образованном точками 1, искомой точкой и одной из точек φ, ψ и на соответствующих ему формах Дирихле и Кэли.

7-е действие. Деление на искомую точку достигается делением формы Дирихле на норму искомой точки, которая равна одному из угловых коэффициентов формы Дирихле. После этого для сохранения единства действия целесообразно сделать круговую перестройку переменных с тем, чтобы сохранить название w для коэффициента при 1 в выражении $w + u\rho_1 + v\rho_2$ точек решетки через базис. Для формы Дирихле эта перестановка будет выглядеть просто как поворот трехугольного символа, составленного из коэффициентов.

Форму Кэли нужно тоже „повернуть“ в ту же сторону и на тот же угол, как и форму Дирихле. Форма Кэли нам нужна только для составления двойничной формы, а эта последняя нас интересует только с точностью до постоянного множителя, поэтому форму Кэли можно ни на что не множить и не делить.

Сделав 7-е действие, нужно повторять процесс сначала до тех пор, пока не встретится форма Дирихле, тождественная с формой, получившейся в результате четырех первых действий первого шага.

Пример. Найти основную единицу поля $\Omega(\sqrt[3]{19})$.

Решение. Базис решетки: $\left[1, \rho, \frac{1+\rho+\rho^2}{3}\right]$, где $\rho = \sqrt[3]{19}$.

Форма Дирихле:

$$\begin{array}{ccccc} 19, & & 19, & & 0, \\ & 0, & & -19, & \\ & & 0, & & \end{array} \qquad \begin{array}{c} 12 \\ -6 \\ 1 \end{array}$$

Форма Кэли:

$$\begin{array}{ccccc} 2, & 1, & -3, & 3 \\ & 6, & -17, & -3 \\ & & 6, & 1 \\ & & 40 \end{array}$$

1-е действие: форма, соответствующая проекции,

$$(3,\ 3,\ 1,\ -2).$$

2-е действие: $bc - ad > 0$;

$$(3,\ 3,\ 1,\ -2)\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = (3,\ -6,\ 4,\ -3); \quad bc - ad < 0;$$

$$(3,\ 3,\ 1,\ -2)\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = (3,\ -7,\ 7,\ -2); \quad bc - ad < 0.$$

Форма (3, 3, 1, —2) приведена по Бервику и Матьюсу.

3-е действие: форма (3, 3, 1, —2) сама имеет крайние коэффициенты с противоположными знаками.

4-е действие: $t_1 = -2$; $t_2 = -3$. Новый базис: $1,\ \rho - 2,\ \frac{1 + \rho + \rho^2}{3} - 3$.

Преобразование формы Дирихле:

$$\begin{array}{ccccc} -2 & 19, & 19, & 0, & 12 \\ & 0, & -19, & -6 & \\ & 0, & 1 & & \\ & 1 & & & \end{array} = \begin{array}{ccccc} 11, & 61, & 12, & 12 \\ 12, & -23, & -6 & \\ -6, & 1 & & \\ 1 & & & \end{array}$$

(Символом $\overset{-2}{\nwarrow}$ обозначаем, в каком направлении и с каким числом проводить вычисления по схеме Горнера.)

$$\begin{array}{ccccc} 11, & 61, & 12, & 12 \\ 12, & -23, & -6 & \overset{-3}{\nearrow} \\ -6, & 1 & & \\ 1 & & & \end{array} = \begin{array}{ccccc} 11, & 25, & 27, & 12 \\ 12, & 13, & 15 & \\ -6, & -8 & & \\ 1 & & & \end{array}$$

Преобразования формы Кэли:

$$\begin{array}{ccccc} 2, & 1, & -3, & 3 & \\ 6, & -17, & -3 & \swarrow^{3} & \\ 6, & 1 & & & \\ 40 & & & & \end{array} \overset{-2}{\nwarrow} = \begin{array}{ccccc} 2, & 1, & -3, & 3 & \\ 18, & -13, & -9 & \swarrow^{3} & \\ 54, & -29 & & & \\ 92 & & & & \end{array} = \begin{array}{ccccc} 2, & 1, & -3, & 3 \\ 21, & -31, & 18 & \\ -12, & -2 & & \\ 5 & & & \end{array}$$

5-е действие:

$(E - B + 1)(B - 1) - H = -7 \cdot 19 - 11 < 0$; ρ_1 ближе к OZ, чем $1 - \rho_1$;

$(G - C + 1)(C - 1) - M = -9 \cdot 24 - 12 < 0$; ρ_2 ближе к OZ, чем $1 - \rho_2$.

Оставляем формы без изменений.

6-е действие.

$$H^2 - LH + KM - M^2 = 11^2 - 11 \cdot 27 + 25 \cdot 12 - 12^2 = -20 < 0.$$

ρ_1 ближе к OZ, чем ρ_2.

Теперь мы должны перейти к базису $[1,\ \rho_1,\ \rho_2 - \rho_1]$ и сделать действия 4, 5, 6. Для действий 4, 5 нет необходимости строить всю форму Дирихле. Достаточно построить „правое ребро“ ее, т. е. форму

$$N(w + v(\rho_2 - \rho_1)) = w^3 - 2w^2v + 14wv^2 - v^3.$$

Действие 4': $t_v = 1$; $(1,\ -2,\ 14,\ -1) \xrightarrow{1} (1,\ 1,\ 13,\ 12)$.

Действие 5': $(G - C + 1)(C - 1) - M = -12 < 0$;

$\rho_2-\rho_1+1$ ближе к OZ, чем $\rho_1-\rho_2$.

Преобразование к базису $(1,\ \rho_1,\ \rho_2-\rho_1+1)$.

Форма Дирихле:

$$11,\ 25,\ \overrightarrow{27},\ 12 \quad 11,\ -8,\ 10,\ -1 \quad 11,\ 4,\ -7,\ 12$$
$$12,\ 13,\ 15 \quad = \quad 12,\ -11,\ 14 \quad = \quad 12,\ -23,\ 13$$
$$-6,\ -8 \qquad\qquad -6,\ -2 \qquad\qquad -6,\ 1$$
$$1 \qquad\qquad 1 \qquad\qquad 1$$

6-е действие: $H^2-HL+KM-M^2=11^2+11\cdot7-4\cdot12-12^2=6>0$; $\rho_2-\rho+1$ ближе к OZ, чем ρ_1.

Следовательно, $\rho_2-\rho_1+1=\frac{1-2\rho+\rho^2}{3}$ — относительный минимум, смежный с 1.

Окончательная форма Кэли:

$$2,\ 1,\ -3,\ 3 \quad 3,\ 4,\ 6,\ 3 \quad 3,\ 4,\ 6,\ 3$$
$$21,\ -31,\ 18 \quad = \quad 8,\ 5,\ 18 \quad = \quad 4,\ -7,\ 9$$
$$-12,\ -2 \qquad\qquad -14,\ -2 \qquad\qquad -13,\ -29$$
$$5 \qquad\qquad 5 \qquad\qquad 22$$

7-е действие:

Форма Дирихле:

$$1,\ -6,\ 12,\ 11$$
$$1,\ -23,\ 4$$
$$13,\ -7$$
$$12$$

Множитель $^1/_{12}$ не пишем. О нем вспомним при пятом действии, единственном, где этот множитель нужен.

Форма Кэли:

$$22,\ -13,\ 4,\ 3$$
$$-29,\ -7,\ 4$$
$$9,\ 6$$
$$3$$

Базис: $\left[1,\frac{3}{\rho^2-2\rho+1},\frac{\rho-2}{\rho^2-2\rho+1}\right]=\left[1,\frac{\rho^2+7\rho+13}{36},\frac{5\rho^2-\rho-7}{36}\right]$.

1-е действие: форма, соответствующая проекции:

$$(3,\ -4,\ -13,\ -22).$$

2-е действие: $bc-ad>0$;

$$(3,-4,-13,-22)\begin{pmatrix}1&-1\\0&1\end{pmatrix}=(3,-13,4,-16);\qquad bc-ad<0;$$
$$(3,-4,-13-22)\begin{pmatrix}1&0\\-1&1\end{pmatrix}=(16,-44,53,-22);\quad bc-ad<0.$$

Форма $(3,-4,-13,-22)$ приведена по Бервику и Матьюсу.

3-е действие: крайние коэффициенты $(3,-4,-13,-22)$ имеют разные знаки.

4-е действие: $t=-1$; $t_2=0$.

Базис: $\left[1,\frac{\rho^2+7\rho-23}{36},\frac{5\rho^2-\rho-7}{36}\right]$.

Форма Дирихле:

$$1,\ -6,\ 12,\ 11 \qquad 1,\ 10,\ 8,\ 11$$
$$1,\ -23,\ 4 \quad = \quad 11,\ -9,\ 4$$
$$13,\ -7 \qquad\qquad -23,\ -7$$
$$12 \qquad\qquad 12$$

Форма Кэли:

$$\begin{array}{ccccccc} 22, & -13, & 4, & 3 & 22, & -13, & 4, & 3 \\ & -29, & -7, & 4 & = & 37, & -33, & 8 \\ -1 & & 9, & 6 & & & 17, & -14 \\ & & & 3 & & & & 5 \end{array}$$

5-е действие:

$$(E-B+1)(B-1)-H=\frac{1}{144}[(11+23+12)(-23-12)-1\cdot 12]<0,$$

$$(G-C+1)(C-1)-M=\frac{1}{144}[(4+7+12)(-7-12)-11\cdot 12]<0.$$

Следовательно, ρ_1 ближе к OZ, чем $1-\rho_1$, и ρ_2 ближе к OZ, чем $1-\rho_2$.

6-е действие:

$$H^2-HL+KM-M^2=1-8+10\cdot 11-11^2<0;$$

ρ_1 ближе к OZ, чем ρ_2.

Предварительное вычисление перед переходом к базису $[1,\ \rho_1,\ \rho_2-\rho_1]$:

$$N(w+v\rho_2-v\rho_1)=12w^3+16w^2v+24wv^2+12v^3.$$

Действие 4': $t_2=0$.

Действие 5':

$$(G-C+1)(C-1)-M=\frac{1}{144}[(24-16+12)(16-12)-12^2]<0;$$

$\rho_2-\rho_1$ ближе к OZ, чем $1-\rho_2+\rho_1$.

Действие 6':

Переход к базису $[1,\ \rho_1,\ \rho_2-\rho_1]$:

$$\begin{array}{ccccccc} \overrightarrow{\ \ -1} & & & & & & \\ 1, & 10, & 8, & 11 & 1, & 7, & -9, & 12 \\ & 11, & -9, & 4 & = & 11, & -31, & 24 \\ & -23, & -7 & & & -23, & 16 & \\ & & 12 & & & & 12 & \end{array}$$

$$H^2-HL+KM-M^2=1+9+7\cdot 12-12^2<0;$$

ρ_1 ближе к OZ, чем $\rho_2-\rho_1$.

Предварительное вычисление перед переходом к базису $[1,\ \rho_1,\ \rho_1+\rho_2]$:

$$N(w+v\rho_1+v\rho_2)=12w^3-30w^2v+6wv^2+30v^3.$$

Действие 4'': $t_2=0$.

Действие 5'': $(G-C+1)(C-1)-M=\frac{1}{144}[-48\cdot 31-30\cdot 12]<0$;

$\rho_1+\rho_2$ ближе к OZ, чем $1-\rho_1-\rho_2$.

Действие 6'':

Переход к базису $[1,\ \rho_1,\ \rho_1+\rho_2]$:

$$\begin{array}{ccccccc} & \overrightarrow{\ \ 1} & & & & & \\ 1, & 10, & 8, & 11 & 1, & 13, & 31, & 30 \\ & 11, & -9, & 4 & = & 11, & 13, & 6 \\ & -23, & -7 & & & -23, & -30 & \\ & & 12 & & & & 12 & \end{array}$$

$$H^2-HL+KM-M^2=1-31+13\cdot 30-30^2<0;$$

ρ_1 ближе к OZ, чем $\rho_1+\rho_2$.

Итак, ρ_1 — относительный минимум, смежный с 1.

7-е действие:

Новый базис: $\left[1,\ \frac{5\rho^2-\rho-7}{\rho^2+7\rho-23},\ \frac{36}{\rho^2+7\rho-23}\right]=\left[1,\ \frac{\rho^2+4\rho+10}{3},\ \frac{2\rho^2+5\rho+11}{3}\right]$.

Форма Дирихле:

$$\begin{matrix} 11, & 4, & -7, & 12 \\ & 8, & -9, & -23 \\ & & 10, & 11 \\ & & & 1 \end{matrix}$$

Форма Кэли:

$$\begin{matrix} 3, & 8, & -14, & 5 \\ & 4, & -33, & 37 \\ & & -13, & 37 \\ & & & 22 \end{matrix}$$

Мы могли бы уже прекратить вычисления, так как последний базис, очевидно, эквивалентен исходному. Однако для контроля проведем первые четыре действия следующего шага.

1-е действие:

Проекция: (5, 14, 8, —3).

2-е действие: $bc-ad>0$;

$$(5,\ 14,\ 8,\ -3)\begin{pmatrix}1&-1\\0&-1\end{pmatrix}=(5,\ -1,\ -5,\ -2);\quad bc-ad>0;$$

$$(5,\ -1\ -5,\ -2)\begin{pmatrix}1&-1\\0&1\end{pmatrix}=(5,\ -16,\ 12,\ -3);\quad bc-ad<0;$$

$$(5,\ -1,\ -5,\ -2)\begin{pmatrix}1&0\\-1&1\end{pmatrix}=(3,\ 3,\ 1,\ -2);\quad bc-ad>0;$$

$$(3,\ 3,\ 1,\ -2)\begin{pmatrix}1&0\\-1&1\end{pmatrix}=(3,\ -5,\ 4,\ -2);\quad bc-ad<0;$$

$$(3,\ 3,\ 1,\ -2)\begin{pmatrix}1&-1\\0&1\end{pmatrix}=(3,\ -6,\ 4,\ -3);\quad bc-ad<0.$$

Таким образом, форма (3, 3, 1, —2) — приведенная.

Преобразование формы Дирихле:

$$\begin{matrix} \xrightarrow{\ -1\ } & & & & & & & & & & & \\ 1, & 4, & -7, & 12 & 11, & -29, & 18, & 12 & 11, & -29, & 18, & 12 \\ 8, & -9, & -23 & = & 8, & -25, & -6 & & 8, & -25, & -6 & \\ & 10, & 11 & & & 10, & 1 & & & 10, & 1 & \\ & & 1 & & & & 1 & & & & 1 & \end{matrix}$$

$$\begin{matrix} & & & & & & & & & & & \xleftarrow{\ -1\ } \\ 46, & -29, & -18, & 12 & & & & & & & & \\ & 27, & -13, & -6 & = & & & & & & & \\ & & 9, & 1 & & & & & & & & \\ & & & 1 & & & & & & & & \end{matrix}$$

4-е действие: $t_1=-5$; $t_2=-3$

$$\begin{matrix} & & & & & & & & & & & \\ 46, & -29, & -18, & 12 & & & & & & & & \\ -5 & 27, & -13, & -6 & -3 & = & & & & & & \\ & & 9, & 1 & & & & & & & & \\ & & & 1 & & & & & & & & \end{matrix}\qquad \begin{matrix} & & & \\ 11, & 25, & 27, & 12 \\ & 12, & 13, & 15 \\ & & -6, & -8 \\ & & & 1 \end{matrix}$$

Мы получили форму, совпадающую с формой, полученной после четвертого действия первого шага. Следовательно, решетки первого и третьего шагов совпадают.

Основная единица ε_0 равна

$$\frac{1-2\rho+\rho^2}{3}\cdot\frac{\rho^2+7\rho-23}{36}=\frac{-\rho^2+2\rho+2}{3}.$$

Задача решена.

ТАБЛИЦА ОСНОВНЫХ ЕДИНИЦ ДЛЯ ВСЕХ КУБИЧЕСКИХ ПОЛЕЙ ОТРИЦАТЕЛЬНЫХ ДИСКРИМИНАНТОВ НЕ БОЛЬШИХ 379 ПО АБСОЛЮТНОЙ ВЕЛИЧИНЕ

(Вычислена Б. Делоне и К. Латышевой)

$-D$			$-D$		
23	$\varepsilon^3 = -\varepsilon^2 + 1$		239	$\varepsilon^3 = -\varepsilon^2 - 8\varepsilon + 1$	$\Delta = 3$
31	$\varepsilon^3 = -\varepsilon + 1$			$\varepsilon = \rho^2 - \rho - 1$	
44	$\varepsilon^3 = -\varepsilon^2 - \varepsilon + 1$			$\rho^3 = \rho + 3$	
59	$\varepsilon^3 = -2\varepsilon + 1$		243	$\varepsilon^3 = -\varepsilon^2 - 12\varepsilon + 1$	
76	$\varepsilon^3 = \varepsilon^2 - 3\varepsilon + 1$		244	$\varepsilon^3 = -5\varepsilon^2 - 27\varepsilon + 1$	$\Delta = 16$
83	$\varepsilon^3 = -2\varepsilon^2 - 2\varepsilon + 1$			$\varepsilon = -2\rho^2 + 10\rho - 7$	
87	$\varepsilon^3 = -\varepsilon^2 - 2\varepsilon + 1$			$\rho^3 = 5\rho^2 - 4\rho + 2$	
104	$\varepsilon^3 = \varepsilon^2 - 5\varepsilon + 1$	$\Delta = 2$	247	$\varepsilon^3 = -3\varepsilon^2 - 4\varepsilon + 1$	
	$\varepsilon = -\rho^2 + \rho + 1$		255	$\varepsilon^3 = 5\varepsilon^2 - 8\varepsilon + 1$	
	$\rho^3 = \rho + 2$		268	$\varepsilon^3 = 7\varepsilon^2 - 13\varepsilon + 1$	
107	$\varepsilon^3 = 2\varepsilon^2 - 4\varepsilon + 1$		279	$\varepsilon^3 = 2\varepsilon^2 - 5\varepsilon + 1$	
108	$\varepsilon^3 = -3\varepsilon^2 - 3\varepsilon + 1$		283	$\varepsilon^3 = -4\varepsilon + 1$	
116	$\varepsilon^3 = -3\varepsilon^2 - 5\varepsilon + 1$	$\Delta = 2$	300	$\varepsilon^3 = -7\varepsilon^2 - 23\varepsilon + 1$	$\Delta = 9$
	$\varepsilon = \rho^2 - \rho - 1$			$\varepsilon = -\rho^2 + 5\rho - 5$	
	$\rho^3 = \rho^2 + 2$			$\rho^3 = 4\rho^2 - 2\rho + 2$	
135	$\varepsilon^3 = -3\varepsilon + 1$		304	$\varepsilon^3 = -5\varepsilon^2 - 7\varepsilon + 1$	
139	$\varepsilon^3 = 4\varepsilon^2 - 6\varepsilon + 1$		307	$\varepsilon^3 = -5\varepsilon^2 - 19\varepsilon + 1$	$\Delta = 8$
140	$\varepsilon^3 = 3\varepsilon^2 - 5\varepsilon + 1$			$\varepsilon = 2\rho - 1$	
152	$\varepsilon^3 = 5\varepsilon^2 - 9\varepsilon + 1$	$\Delta = 2$		$\rho^3 = -\rho^2 - 3\rho + 2$	
	$\varepsilon = -\rho^2 + \rho + 3$		324	$\varepsilon^3 = -15\varepsilon^2 - 57\varepsilon + 1$	$\Delta = 6$
	$\rho^3 = \rho^2 + 2\rho + 2$			$\varepsilon = \rho^2 + \rho - 1$	
172	$\varepsilon^3 = 3\varepsilon^2 - 7\varepsilon + 1$	$\Delta = 2$		$\rho^3 = 3\rho + 4$	
	$\varepsilon = -\rho^2 + 2\rho + 1$		327	$\varepsilon^3 = -9\varepsilon + 1$	$\Delta = 3$
	$\rho^3 = 2\rho^2 + 2$			$\varepsilon = -\rho^2 + 4\rho - 2$	
175	$\varepsilon^3 = -2\varepsilon^2 - 3\varepsilon + 1$			$\rho^3 = 4\rho^2 - 3\rho + 3$	
176	$\varepsilon^3 = -\varepsilon^2 - 3\varepsilon + 1$		331	$\varepsilon^3 = -2\varepsilon^2 - 4\varepsilon + 1$	
199	$\varepsilon^3 = \varepsilon^2 - 4\varepsilon + 1$		332	$\varepsilon^3 = 7\varepsilon^2 - 23\varepsilon + 1$	$\Delta = 8$
200	$\varepsilon^3 = -7\varepsilon^2 - 13\varepsilon + 1$	$\Delta = 2$		$\varepsilon = -2\rho + 3$	
	$\varepsilon = \rho^2 - \rho - 1$			$\rho^3 = -\rho^2 - 2\rho + 4$	
	$\rho^3 = 2\rho^2 - 3\rho + 4$		335	$\varepsilon^3 = -\varepsilon^2 - 4\varepsilon + 1$	
204	$\varepsilon^3 = 5\varepsilon^2 - 11\varepsilon + 1$	$\Delta = 3$	339	$\varepsilon^3 = 11\varepsilon^2 - 35\varepsilon + 1$	$\Delta = 8$
	$\varepsilon = -\rho^2 + \rho + 1$			$\varepsilon = -2\rho + 5$	
	$\rho^3 = \rho^2 - \rho + 3$			$\rho^3 = 2\rho^2 + 3$	
211	$\varepsilon^3 = 6\varepsilon^2 - 10\varepsilon + 1$		351	$\varepsilon^3 = 3\varepsilon^2 - 6\varepsilon + 1$	
212	$\varepsilon^3 = -\varepsilon^2 - 15\varepsilon + 1$	$\Delta = 8$	356	$\varepsilon^3 = 11\varepsilon^2 - 43\varepsilon + 1$	$\Delta = 16$
	$\varepsilon = 2\rho - 1$			$\varepsilon = -2\rho^2 + 2\rho + 13$	
	$\rho^3 = \rho^2 - 4\rho + 2$			$\rho^3 = 7\rho + 8$	
216	$\varepsilon^3 = 9\varepsilon^2 - 21\varepsilon + 1$	$\Delta = 2$	364	$\varepsilon^3 = 3\varepsilon^2 - 19\varepsilon + 1$	$\Delta = 8$
	$\varepsilon = -\rho^2 - \rho + 1$			$\varepsilon = -2\rho + 1$	
	$\rho^3 = -3\rho + 2$			$\rho^3 = -4\rho + 2$	
231	$\varepsilon^3 = -4\varepsilon^2 - 5\varepsilon + 1$		367	$\varepsilon^3 = 4\varepsilon^2 - 7\varepsilon + 1$	
236	$\varepsilon^3 = 3\varepsilon^2 - 11\varepsilon + 1$	$\Delta = 4$	368	$\varepsilon^3 = -\varepsilon^2 - 7\varepsilon + 1$	$\Delta = 2$
	$\varepsilon = \rho^2 - 3\rho + 1$		379	$\varepsilon^3 = -10\varepsilon^2 - 26\varepsilon + 1$	$\Delta = 3$
	$\rho^3 = 2\rho^2 + \rho + 2$			$\varepsilon = \rho^2 - 3$	
				$\rho^3 = \rho^2 - \rho + 4$	

ТАБЛИЦА ЕДИНИЦ ДЛЯ ВСЕХ ЧИСТО КУБИЧЕСКИХ ПОЛЕЙ $\Omega(\alpha)$, ГДЕ $\alpha = \sqrt[3]{a}$, ДЛЯ ВСЕХ a НЕ БОЛЬШИХ 70

(Вычислена А. Марковым).

a		a		a	
2	$1+\alpha+\alpha^2$	31	$\frac{(1+\alpha)^2}{(\alpha-3)^5} = 101\,209 + 32\,218\alpha + 10\,256\alpha^2$	52	$\frac{12}{(4-\alpha)^3} = 209 + 56\alpha + 15\alpha^2$
3	$4+3\alpha+2\alpha^2$	33	$\frac{(\alpha-1)^3}{(2+9\alpha-3\alpha^2)^5}$	53	$\frac{(7+\alpha)^5(1+\alpha)^5}{3(4-\alpha)^5(5-\alpha)^5(2\alpha-7))^3}$
5	$41+24\alpha+14\alpha^2$	34	$\frac{(4+\alpha)^3}{2(\alpha-3)^6} = 334\,153 + 103\,146\alpha + 31\,839\alpha^2$	55	$\frac{5^5\cdot 7^{15}(7-\alpha)^{18}}{(4-\alpha)^{18}(\alpha-3)^{15}(\alpha-1)^{15}(5-\alpha)^1}$
6	$109+60\alpha+33\alpha^2$	35	$\frac{(1+\alpha)^3}{3(\alpha-2)(\alpha-3)^2} = \frac{278+85\alpha+26\alpha^2}{3}$	57	$\frac{(3-\alpha)^4(8-\alpha)}{3(4-\alpha)^4(\alpha-1)(\alpha-3)(3\alpha-11)} = 1\,460\,968 + 379\,620\alpha + 98\,641\alpha^2$
7	$4+2\alpha+\alpha^2$	37	$100+30\alpha+9\alpha^2$	58	$\frac{6}{(4-\alpha)^3} = 929 + 240\alpha + 62\alpha^2$
10	$\frac{23+11\alpha+5\alpha^2}{3}$	38	$\frac{2\cdot 3^2(8+\alpha)^3}{(\alpha-2)^6(\alpha-3)^3} = 29\,071 + 8647\alpha + 2572\alpha^2$	59	$\frac{(1+\alpha)^{15}}{3^5(3-3)^6(4-\alpha)^{15}}$
11	$89+40\alpha+18\alpha^2$	39	$\frac{3(1+\alpha)^2}{(4-\alpha)(\alpha-3)^3} = 529 + 156\alpha + 46\alpha^2$	60	$\frac{4}{(4-\alpha)^3} = 2161 + 552\alpha + 141\alpha^2$
12	$55+24\sqrt[3]{12}+21\sqrt[3]{18}$	41	$\frac{3^{10}(7+\alpha)^{12}(2+\alpha)^{21}}{(5-\alpha)^{42}}$	61	$\frac{3}{(4-\alpha)^3} = 3905 + 992\alpha + 252\alpha^2$
13	$94+40\alpha+17\alpha^2$	42	$\frac{7}{(7-2\alpha)^3} = 21\,169 + 6090\alpha + 1752\alpha^2$	62	$\frac{2}{(4-\alpha)^3} = 8929 + 2256\alpha + 570\alpha^2$
14	$29+12\alpha+5\alpha^2$	43	$49+14\alpha+4\alpha^2$	63	$16+4\alpha+\alpha^2$
15	$\frac{5}{(5-2\alpha)^3} = 5401 + 2190\alpha + 888\alpha^2$	44	$\frac{1}{2}\left(\frac{\alpha-2}{2\alpha-7}\right)^3 = \frac{4007+1135\alpha+643\alpha^2}{3}$	65	$16+4\alpha+\alpha^2$
17	$324+126\alpha+49^2$	45	$\frac{3^4(3+\alpha)^3}{(\alpha-3)^9} = 1\,477\,441 + 415\,374\alpha + 116\,780\alpha^2$	66	$\frac{3}{(\alpha-4)^3} = 9505 + 2352\alpha + 582\alpha^2$
18	$55+24\sqrt[3]{12}+21\sqrt[3]{18}$	46	$\frac{3^2\cdot 2^2(2+\alpha)^3}{(4-\alpha)^9} = 16\,449\,049 + 4\,590\,798\alpha + 1\,281\,255\alpha^2$	67	$\frac{2}{(\alpha-4)^3} = 4289 + 1056\alpha + 260\alpha^2$
19	$\frac{14+5\alpha+2\alpha^2}{3}$	47	$\frac{3(2+\alpha)^6(1+\alpha)^3}{(\alpha-3)^6(2\alpha-7)^6}$	68	$\frac{4}{(\alpha-4)^3} = 2449 + 600\alpha + 147\alpha^2$
20	$11+4\sqrt[3]{20}+3\sqrt[3]{50}$	50	$11+4\sqrt[3]{20}+3\sqrt[3]{50}$	69	$\frac{3^7\left(1+\sqrt[3]{69}\right)^{30}}{(3+\alpha)^6(6-\alpha)^{15}(\alpha-4)^{30}}$
21	$\frac{3(3+\alpha)}{(3-\alpha)^4} = 1705 + 618\alpha + 224\alpha^2$	51	$\frac{(3+\alpha)^6(\alpha-1)^3}{3(2\alpha-7)^6(\alpha-3)^3} = 107\,846\,641 + 29\,081\,484\alpha + 7\,841\,994\alpha^2$	70	$\frac{6}{(\alpha-4)^3} = 1121 + 272\alpha + 66\alpha^2$
22	$\frac{1}{6}\left(\frac{2+\alpha}{3-\alpha}\right)^3 = 793 + 283\alpha + 101\alpha^2$				
23	$\frac{(1+\alpha)^6}{9(3-\alpha)^9} = 2\,166\,673\,601 + 761\,875\,860\alpha + 267\,901\,370\alpha^2$				
26	$9+3\alpha+\alpha^2$				
28	$9+3\alpha+\alpha^2$				
29	$\frac{(19+6\alpha+2\alpha^2)^6}{3(70-32\alpha+3\alpha^2)^3}$				
30	$\frac{3}{(\alpha-3)^3} = 811 + 261\alpha + 84\alpha^2$				

ГЛАВА V

ТЕОРЕМА ТУЭ

В задаче о представлении целых чисел разложимыми формами с n переменными (формами Дирихле), как мы это видели в § 4, в том случае, когда форма неприводима, наиболее характерным является то, что, вообще говоря (а именно, кроме случаев $n=1$ и $n=2$, $\tau=1$, т. е. тех единственных случаев, когда число „параметров" точек в соответственном сигнатурном пространстве равно 1), любое данное число либо вовсе не имеет представлений, либо имеет бесконечно много представлений формой. То же самое имеет место и в задаче о представлении чисел квадратичными формами с двумя или многими переменными, если исключить единственный случай, когда форма определенная и, следовательно, представление ею заданного числа сводится на разыскание целых точек на конечной поверхности — на n-мерном эллипсоиде.

Совершенно иное имеет место в задаче о представлении чисел двойничными формами, порядок которых выше чем 2 (двойничные формы 2-го порядка суть одновременно формы Дирихле и квадратичные формы и поэтому входят в каждую из вышеупомянутых теорий). Число представлений любого заданного числа любой неприводимой двойничной формой высшего порядка оказывается всегда конечно. Это основное обстоятельство обнаружил в 1908 г. норвежский математик Туэ (1868—1919). Этот результат есть непосредственное следствие того обстоятельства, что если ρ целое алгебраическое число n-го порядка и $n>2$, то не может существовать бесконечного числа рациональных дробей $\frac{y}{x}$ таких, что разность $\rho-\frac{y}{x}$ по абсолютной величине меньше $\frac{A}{x^n}$, где A — любая заданная положительная константа. Туэ доказал даже, что не может быть бесконечного числа дробей $\frac{y}{x}$ даже таких, что

$$\left|\rho-\frac{y}{x}\right|<\frac{A}{x^{\frac{n}{2}+1}},$$

а Зигель, усовершенствовавший метод Туэ, доказал то же самое для еще меньшего показателя ν, а именно для

$$\nu>\frac{n}{s+1}+s,$$

где s — то из чисел $1, 2, \ldots, n-1$, для которого

$$\frac{n}{s+1}+s$$

наименьшее. Для случая $n=3$, который нас в настоящей книге наиболее интересует, $1, 2, \ldots, n-1$ есть $1, 2$, соответственные

$$\frac{n}{s+1}+s$$

суть

$$\frac{3}{2}+1 \quad \text{и} \quad \frac{3}{3}+2,$$

т. е. показатель ν Зигеля $\frac{3}{2}+1$ тот же самый, что и показатель Туэ. Мы рассмотрим в этой главе доказательство теоремы Туэ о конечности числа представлений числа двойничной формой выше 2-го порядка, воспользовавшись геометрическим изложением метода Туэ, данным Тартаковским.

§ 65. Гипербола Лиувилля и гипербола Туэ

Пусть $f(x, y)$ двойничная форма с целыми рациональными коэффициентами, a_0 коэффициент при y^n и $\rho, \rho_1, \rho_2, \ldots, \rho_{n-1}$ корни формы, т. е. $f(x, y) = a_0 \cdot N(x\rho + y)$. Предположим, что надо решить неопределенное уравнение $f(x, y) = \sigma$, где σ — некоторое заданное целое рациональное число. Абсолютные величины множителей $x\rho_k + y$, соответствующие комплексным корням $\rho_k = a_k + ib_k$, не меньше $|b_k x|$, т. е. с возрастанием $|x|$ бесконечно возрастают. Если все корни $\rho, \rho_1, \ldots, \rho_{n-1}$ комплексны, то, очевидно, нет решений с x, превосходящими по абсолютной величине некоторую величину, которую можно указать; например,

$$\sqrt[n]{\frac{|\sigma|}{|a_0||b_1 b_2 \ldots b_n|}}.$$

В этом случае целочисленных решений x, y уравнения $f(x, y) = \sigma$ ограниченное число, и они все могут быть найдены. Если, следовательно, есть решения с большими $|x|$, то должен быть для каждого такого решения хоть один такой вещественный корень ρ, что

$$|x\rho + y| < \sqrt[n]{\left|\frac{\sigma}{a_0}\right|}.$$

Пусть

$$x\rho + y = \theta \cdot \sqrt[n]{\left|\frac{\sigma}{a_0}\right|},$$

где

$$-1 < \theta < 1.$$

Мы имеем тогда

$$\sigma = a_0 (x\rho + y) \prod_{k=1}^{n-1} (x\rho_k + y + x\rho - x\rho) =$$

$$= a_0 (x\rho + y) x^{n-1} \cdot \prod_{k=1}^{n-1} \left(\rho_k - \rho + \theta \frac{\sqrt[n]{\left|\frac{\sigma}{a_0}\right|}}{x}\right),$$

т. е.

$$x\rho + y = \frac{\sigma}{a_0 x^{n-1} \prod_{k=1}^{n-1} \left(\rho_k - \rho + \theta \frac{\sqrt[n]{\left|\frac{\sigma}{a_0}\right|}}{x}\right)}$$

и, следовательно, если $|x|$ велико, то $\left|\theta \frac{\sqrt[n]{\left|\frac{\sigma}{a_0}\right|}}{x}\right|$ мало, и

$$|x\rho + y| = \frac{s}{|x|^{n-1}},$$

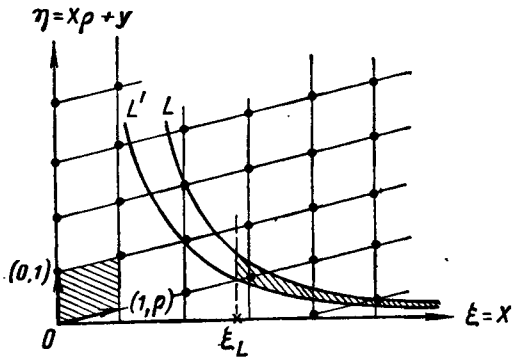
где s — число, мало отличающееся от числа

$$\frac{\sigma}{a_0\prod_{k=1}^{n-1}[(\rho_k-\rho)]}.$$

Таким образом, если $|x|$ больше некоторого ξ_L, то $L'<s<L$, где L' и L — некоторые положительные константы, зависящие только от коэффициентов формы $f(x, y)$, от представляемого числа σ и от выбранного предела ξ_L.

Будем рассматривать решения x, y, в этом смысле связанные с некоторым данным вещественным корнем ρ нашей формы геометрически. Для этого будем откладывать на оси ξ велчину x, а на оси η величину $x\rho+y$; тогда всем целым x, y будут, как легко видеть, соответствовать все точки параллелограмматической решетки, построенной на точках (0, 0), (1, ρ) и (0, 1). В этой геометрической интерпретации предыдущий результат состоит в том, что все решения, у которых $|x|>\xi_L$, лежат между „гиперболами“

$$\eta=\frac{L'}{\xi^{n-1}} \quad \text{и} \quad \eta=\frac{L}{\xi^{n-1}}.$$



Черт. 39.

Гиперболу L' Лиувилль использовал для доказательства существования трансцендентных чисел (1851). Нам будет нужна только гипербола L; ее мы будем называть *гиперболой Лиувилля*. Итак, все большие решения x, y лежат под гиперболой Лиувилля.

Сущность результата Туэ состоит в том, что он показывает существование другой гиперболы A

$$\eta=\frac{1}{\xi^{\alpha}},$$

такой, что все достаточно большие решения, например, имеющие $|x|>\xi_A$, лежат над этой гиперболой, причем при $n>2$, показатель ее $\alpha<n-1$. Какова бы ни была константа L, гипербола Туэ, следовательно, при достаточно больших $|x|$ будет итти над соответственной гиперболой Лиувилля. Таким образом, если ξ_{AL} абсцисса точки пересечения этих гипербол, то иет решений, у которых $|x|$ больше наибольшего из трех положительных чисел ξ_L, ξ_A и ξ_{AL}. Сам Туэ доказывает существование гиперболы A для показателя

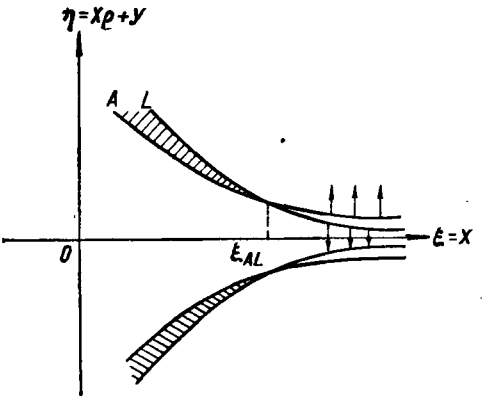
$$\alpha=\frac{n}{2}+\varepsilon,$$

где ε какое-угодно малое положительное число, но нам достаточно иметь $\alpha=n-1-\varepsilon$.

Гипербола A Туэ совершенно аналогична той гиперболе L' Лиувилля, при помощи которой Лиувилль доказал существование трансцендентных чисел, но она еще медленнее приближается к оси ξ. Стоило показать существование такой гиперболы и соединить ее с гиперболой L Лиувилля, как получилась теорема Туэ.

Как мы увидим в § 67, существенным в доказательстве Туэ (и Зигеля) существования гиперболы A является то, что для доказательства приходится

допустить существование достаточно *далекого* (т. е. с большим $|x|$) и „хорошего" (во всяком случае лучшего, чем, вообще говоря, у подходящих дробей) рационального приближения $x_0\rho + y_0$ к корню ρ, *какового в действительности может быть вовсе и нет.* Одиако, если такового нет, то уже тем самым уравнение $f(x, y) = \sigma$ не может иметь больших решений, так как большие решения суть такие хорошие приближения; таким образом, и в этом случае теорема Туэ оказывается все же доказанной.



Черт. 40.

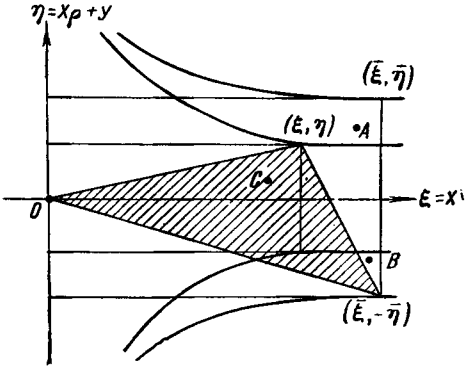
§ 66. Заградительный ряд и гипербола B

Как в основной работе Туэ, так и в его специальных исследованиях, посвященных невозможности существования бесконечного числа представлений в случае кубической двойничной формы, а также в соответственных работах Зигеля, посвященных общей теореме Туэ или частному случаю кубической двойничной формы или формы $ax^n + by^n$, везде доказательство существования гиперболы A делается при помощи предварительного доказательства существования бесконечной последовательности таких целых точек решетки x, y, которые:

1°. достаточно хорошо приближаются к оси ξ, хотя может быть и гораздо хуже, чем подходящие дроби, но зато

2°. расположеиы вдоль оси ξ достаточно близко друг за другом, т. е. не образуют больших пустых промежутков (таких, которые a priori могут давать непрерывные дроби), и

3°. все эти точки примитивны, т. е. нет целых точек внутри отрезков, соединяющих эти точки с началом координат, иначе говоря, x и y каждой точки взаимно простые между собою. Такой ряд рациональных приближений к ρ Тартаковский предлагает называть „заградительным рядом".



Черт. 41.

Будем называть координатным прямоугольником точки с положительным ξ лежащую направо от оси η половину прямоугольника, имеющего цеитр в начале координат, стороны которого параллельны осям координат и одна из вершин которого лежит в рассматриваемой точке. Мы будем называть гиперболой B или гиперболой заградительного ряда, соответствующего данному α, гиперболу $\eta = \frac{1}{\xi^\beta}$ в том случае, если, начиная с некоторого ξ, в координатном прямоугольиике любой точки этой гиперболы лежат по крайней мере две различные примитивные целые точки (x, y) и если показатель этой гиперболы $\beta > \frac{1}{\alpha}$. Заградительным же рядом, конкретно говоря, мы будем называть ряд самих таких примитивных приближений (x, y), для которого есть такая гипербола B, в любом координатном прямоугольнике которой лежат по крайней мере два таких приближения.

Покажем (см. черт. 41), что из существования заградительного ряда, т. е. из существования гиперболы B, следует существование гиперболы A. Действительно, пусть внутри гиперболы A была бы целая точка C; тогда эта точка лежала бы внутри координатного прямоугольника какой-нибудь точки (ξ, η) гиперболы A, например, той, которая получается в пересечении с гиперболой A луча OC. Возьмем координатный прямоугольник некоторой точки $(\bar{\xi}, \bar{\eta})$ гиперболы B, с достаточно большим $\bar{\xi}$, так что в нем уже лежат две примитивных целых точки A и B. Одна из этих двух точек не лежит на прямой OC и, следовательно, образует с точками O и C параллелограмм.

Параллелограмм этот, как параллелограмм нашей решетки целых точек, имеет площадь не меньшую, чем площадь основного параллелограмма этой решетки, которая равна 1. Но площадь этого параллелограмма, с другой стороны, как легко видеть, не больше площади параллелограмма (половина которого заштрихована на чертеже), построенного на точках $(0, 0)$, (ξ, η) и $(\bar{\xi}, -\bar{\eta})$. Площадь же этого последнего параллелограмма равна $|\xi\bar{\eta} + \bar{\xi}\eta|$ и наверно < 1, если одновременно

$$|\xi\bar{\eta}| < \frac{1}{2} \text{ и } |\bar{\xi}\eta| < \frac{1}{2},$$

т. е. если

$$\sqrt[\alpha]{2}\,\bar{\xi}^{\frac{1}{\alpha}} < \xi < \frac{1}{2}\bar{\xi}^{\beta}.$$

Но для всякого ξ, достаточно большого, можно найти такое $\bar{\xi}$, которое удовлетворяет этим неравенствам, если $\beta > \frac{1}{\alpha}$.

Так как нам для дальнейшего достаточно, чтобы α было на какую-угодно малую зафиксированную величину $< n - 1$, то достаточно доказать существование заградительного ряда для β на какую-угодно малую зафиксированную величину $> \frac{1}{n-1}$.

§ 67. Две леммы Туэ

Самая трудная часть всей теории Туэ — доказательство существования заградительного ряда. Мы его проведем только для $n = 3$ (хотя мы этим лишь очень немного сократим выкладки) в три этапа; сначала докажем лемму Туэ о полиномах, затем из этой леммы выведем существование некоторого ряда приближений и, наконец, покажем, что этот ряд есть заградительный в нашем смысле, установив существование гиперболы B.

Лемма I. *Для всякого целого положительного показателя m, большего чем 9, можно всегда найти такие полиномы от переменной t: $f_1(t)$, $f_2(t)$, $f_3(t)$, $P(t)$, $Q(t)$ с целыми рациональными коэффициентами, что будет иметь место равенство* $(\rho + t)^m \cdot [f_1(t)\rho^2 + f_2(t)\rho + f_3(t)] = \rho \cdot P(t) + Q(t)$, *причем степени f_i не больше, чем μ, где*

$$\mu = \left[\frac{5}{8}(m-1)\right]$$

и степени P и Q, следовательно, не больше, чем $m + \mu$, а абсолютные величины каждого из коэффициентов f меньше T^m, а каждого из коэффициентов P и Q меньше S^m, где числа T и S зависят только от коэффициентов s, q, n уравнения $\rho^3 = s\rho^2 + q\rho + n$, но не зависят от показателя m.

Доказательство. Рассмотрим степень $(\rho + t)^m$, где m — какой-угодно целый положительный показатель. Понижая при помощи уравнения $\rho^3 = s\rho^2 + q\rho + n$ $(f = 0)$, мы получим

$$(\rho + t)^m = B_1^{(0)}(t)\rho^2 + B_2^{(0)}(t)\rho + B_3^{(0)}(t),$$

где B — полиномы от t с целыми рациональными коэффициентами, причем порядок этих полиномов не выше, чем m.

Аналогично, пусть

$$\rho(\rho+t)^m = B_1^{(1)}(t)\rho^2 + B_2^{(1)}(t)\rho + B_3^{(1)}(t),$$
$$\rho^2(\rho+t)^m = B_1^{(2)}(t)\rho^2 + B_2^{(2)}(t)\rho + B_3^{(2)}(t).$$

Не трудно видеть из самого получения полиномов B, что все коэффициенты их при разных степенях t не больше, чем некоторое T_0^m, где T_0 — число, зависящее только от коэффициентов s, q, n уравнения $f=0$. Рассмотрим еще все функции $U(t) = C_1(t)\rho^2 + C_2(t)\rho + C_3(t)$, где C_1, C_2, C_3 — полиномы от t степени не выше некоторого числа μ с целыми рациональными коэффициентами, абсолютная величина которых не больше, чем некоторое число s. Специализацией чисел μ и s мы дальше воспользуемся. Всех таких функций U всего M, где $M=(2s+1)^{3(\mu+1)}$.

Будем помножать $(\rho+t)^m$ на все эти U; мы получим, понижая каждый раз при помощи $f=0$ 4-ю и 3-ю степень ρ, выражения вида

$$(\rho+t)^m \cdot U(t) = G_1(t)\rho^2 + G_2(t)\rho + G_3(t),$$

где

$$G_i(t) = B_i^{(0)}C_3 + B_i^{(1)}C_2 + B_i^{(2)}C_1 \quad (i=1, 2, 3).$$

Не трудно видеть, что все G — полиномы от t, не выше $m+\mu$-той степени, все коэффициенты которых — целые числа, по абсолютной величине меньшие N, где $N=3(m+1)sT_0^m$. Разделим интервал $-N$, N на h равных интервалов I. Мы можем тогда, очевидно, найти

$$M_1 \geqslant \frac{M}{h}$$

таких U, что первые коэффициенты всех G_1, соответствующих этим U, лежат внутри одного интервала I. Среди этих M_1 U мы можем найти, в свою очередь, по крайней мере

$$M_2 \geqslant \frac{M_1}{h} \geqslant \frac{M}{h^2}$$

таких функций U, что все вторые коэффициенты всех G_1, соответствующих этим U, лежат внутри одного интервала I (конечно, может быть, другого, чем тот, в котором лежат их первые коэффициенты). Продолжая так же дальше, ввиду того, что всех коэффициентов $G_1(t)$ всего $m+\mu+1$, мы видим, что можно найти

$$L \geqslant \frac{M}{h^{m+\mu+1}}$$

таких U, что у всех $G_1(t)$, соответствующих этим L функциям U, все коэффициенты при одинаковых степенях переменной t лежат внутри одного и того же интервала I. Пусть $L \geqslant 2$. Возьмем тогда две из этих L функций U_1 и U_2.

Пусть

$$(\rho+t)^m \cdot U_1 = G_1^{(1)}\rho^2 + G_2^{(1)}\rho + G_3^{(1)}; \quad (\rho+t)^m \cdot U_2 = G_1^{(2)}\rho^2 + G_2^{(2)}\rho + G_3^{(2)});$$

вычитая эти равенства, мы получаем

$$(\rho+t)^m \cdot (U_1 - U_2) = (G_1^{(1)} - G_1^{(2)})\rho^2 + (G_2^{(1)} - G_2^{(2)})\rho + (G_3^{(1)} - G_3^{(2)}).$$

Предположим, что $h > 2N$; тогда каждый из интервалов I меньше 1, и тогда все коэффициенты разности $G_1^{(1)} - G_1^{(2)}$ по абсолютной величине меньше 1, но они целые числа, и, значит, они все нули, т. е. $G_1^{(1)} - G_1^{(2)} = 0$.

И мы получаем

$$(\rho+t)^m\cdot[f_1(t)\rho^2+f_2(t)\rho+f_3(t)]=P(t)\cdot\rho+Q(t), \qquad (1)$$

если мы положим

$$G_2^{(1)}-G_2^{(2)}=P(t);\quad G_3^{(1)}-G_3^{(2)}=Q(t);\cdot\ U_1-U_2=f_1(t)\rho^2+f_2(t)\rho+f_3(t).$$

Вопрос только в том, может ли быть такое h, что $L\geqslant 2$, и что само $h>2N$. Приняв во внимание значения L и N, легко видеть, что эти неравенства приводят к такому ограничению для h:

$$3(m+1)\,2sT_0^m<h<(2s+1)^{\frac{3(\mu+1)}{m+\mu+1}}.$$

Таким образом, если

$$3(m+1)\,2sT_0^m<(2s+1)^{\frac{3(\mu+1)}{m+\mu+1}}-1,$$

то такое h можно найти. Последнее же неравенство будет наверное иметь место, если, например,

$$T_1^m<(2s+1)^{\frac{3(\mu+1)}{m+\mu+1}-1},$$

где $T_1>3\cdot 2T_0$, так как $(3\cdot 2)^m>3(m+1)$; $2s+1>2s$. Но, если $m>9$ и если $\mu=\left[\frac{5}{8}(m-1)\right]$, то $\frac{3(\mu+1)}{m+\mu+1}-1>\frac{1}{15}$, и, следовательно, предыдущие неравенства будут иметь место, если $T_1^m<(2s+1)^{\frac{1}{15}}$ или, если

$$2s+1>T_1^{15m}.$$

Таким образом, если число $T>T_1^{15}>(6T_0)^{15}$, то неравенства будут иметь место при s таком, что $2s-1\leqslant T^m<2s+1$. Абсолютная величина каждого коэффициента функций P и Q меньше $2N<(2s-1)\,T_1^m<(TT_1)^m=S^m$, если $S=TT_1$, что и требовалось доказать.

Лемма II. *Если числа x и y целые и такие, что $|\rho x+y|<1$, то для всякого показателя $m>9$ можно всегда найти две пары целых чисел B_0, C_0 и B_1, C_1, таких, что*

$$\frac{B_0}{C_0}\neq\frac{B_1}{C_1}$$

и что $|B_0\rho+C_0|$ и $|B_1\rho+C_1|$ меньше, чем $|[(\rho x+y)^{\frac{3}{4}}x^{\frac{5}{8}}H]|^{m-1}$, причем $|B_0|$ и $|B_1|$ меньше, чем $D^{m-1}x^{\frac{13}{8}(m-1)+1}$, где числа H и D зависят только от коэффициентов s, q, n уравнения $\rho^3=s\rho^2+q\rho+n$, но не от показателя m.

На основании предыдущей леммы не трудно доказать эту лемму. Взяв производную по t от обеих частей уравнения

$$P(t)\rho+Q(t)=(\rho+t)^mR(t), \qquad (1)$$

где мы обозначаем через $R(t)$ функцию $f_1(t)\rho^2+f_2(t)\rho+f_3(t)$, мы получим

$$\rho P'(t)+Q'(t)=(\rho+t)^{m-1}[(\rho+t)R'(t)+mR(t)];$$

помножив это на $P(t)$ и вычитая из предыдущего уравнения, помноженного на $P'(t)$, получим

$$Q(t)P'(t)-P(t)Q'(t)=(\rho+t)^{m-1}[(\rho+t)(P'(t)R(t)-R'(t)P(t))-mP(t)R(t)]$$

и значит, в виду того, что уравнение $f(\rho)=0$, которому удовлетворяет ρ, неприводимо, мы получаем

$$Q(t)P'(t)-P(t)Q'(t)=f(t)^{m-1}W(t),$$

где $W(t)$ полином от t. Так как степени $P(t)$ и $Q(t)$ не выше, чем $m+\mu$, то степень γ полинома W не выше, чем

$$2(m+\mu-1)-3(m-1)<\frac{m-1}{4}.$$

Рассмотрим все выражения

$$Z_{ab}(t)=\frac{d^a}{dt^a}P(t)\cdot\frac{d^b}{dt^b}Q(t)-\frac{d^b}{dt^b}P(t)\cdot\frac{d^a}{dt^a}Q(t)$$

для всех чисел a и b из ряда $0, 1, 2, \ldots, \gamma, \gamma+1$. Все эти выражения одновременно при подстаиовке $t=-\frac{y}{x}$, т. е. все $Z_{ab}\left(-\frac{y}{x}\right)_\lambda$, не могут равняться нулю, так как иначе мы имели бы

$$\frac{d^\lambda}{dt^\lambda}[f^{m-1}(t)W(t)]=0$$

для всех λ равных $0, 1, 2, \ldots, \gamma$; но тогда $f^{m-1}(t)W(t)$ имело бы делителя

$$\left(t+\frac{y}{x}\right)^{\gamma+1},$$

т. е. имело бы этого делителя $W(t)$, что невозможно, так как W степени γ. Пусть

$$Z_{ab}\left(-\frac{y}{x}\right)\neq 0$$

при $a=a_1$, $b=b_1$.

Рассмотрим δ-ю производную от уравнения (1)

$$\rho P^{(\delta)}(t)+Q^{(\delta)}(t)=\frac{d^\delta}{dt^\delta}[(\rho+t)^m R(t)].$$

Каждый коэффициент P^δ и Q^δ делится на $1\cdot 2\cdot 3\ldots\delta$. Разделив последнее равенство на $\delta!$, раскрыв справа производную, подставив $t=-\frac{y}{x}$, заметив, что $|\rho x+y|$ по условию меньше 1, и воспользовавшись ограничениями, наложенными на коэффициенты уравнения (1) в лемме I, мы получаем лемму II, если положим

$$\frac{x^{m-\mu-\delta}}{1\cdot 2\cdot 3\ldots\delta}Q^{(\delta)}\left(-\frac{y}{x}\right)=B,\quad \frac{x^{m+\mu-\delta}}{1\cdot 2\cdot 3\ldots\delta}P^{(\delta)}\left(-\frac{y}{x}\right)=C,$$

и если возьмем за δ число a_1, а другой раз число b_1, что и требовалось доказать.

§ 68. Вывод из этих лемм существования гиперболы B

Теперь то, что полученный в лемме II ряд приближений есть заградительный ряд, мы установим тем способом, что покажем существование гиперболы B, т. е. гиперболы $\eta=\frac{1}{\xi^\beta}$, где $\beta>\frac{1}{\alpha}$, т. е. $\beta>\frac{1}{2}$, такой, что в любом ее координатном прямоугольнике есть по крайней мере две точки нашей решетки, не лежащие на одной прямой с началом.

Теорема. *Ряд приближений, найденных в лемме II, если $x=x_0$, $y=y_0$, где (x_0, y_0) — достаточно большое решение*, т. е. *достаточно далекая точка, лежащая между гиперболами Лиувилля, есть заградительный ряд.*

Действительно, пусть (x_0, y_0) некоторая зафиксированная и *достаточно далекая* точка нашей решетки, лежащая между гиперболами Лиувилля, т. е. такая, что $|x_0|$ достаточно велико и $\rho x_0 + y_0 = \frac{\tau}{x_0^2}$, где $L' < \tau < L$. Обозначим через (ξ_{m+1}, η_{m+1}) координаты вершины координатного прямоугольника, в котором в силу леммы II, где мы положим $x = x_0$, $y = y_0$, лежат два приближения, неколлинеарные с началом и получаемые от домножения $(\rho + t)^{m+2}$, а через (ξ_m, η_m) соответственные координаты для домножения $(\rho + t)^{m-1}$. По лемме II мы будем тогда иметь

$$\xi_{m+1} = D^{m+1} x_0^{\frac{13}{8}m + \frac{13}{8} + 1}; \qquad |\eta_m| = \left| H x_0^{\frac{5}{8}} (\rho x_0 + y_0)^{\frac{3}{4}} \right|^m$$

или, если принять во внимание, что $\rho x_0 + y_0 = \tau x_0^{-2} < L x_0^{-2}$, и положить

$$D = x_0^{\mu}, \quad H L^{\frac{3}{4}} = x_0^{\lambda},$$

то мы получим

$$\xi_{m+1} = x_0^{\left(\frac{13}{8} + \mu\right) m + \frac{21}{8} + \mu}, \quad |\eta_m| < x_0^{\left(-\frac{7}{8} + \lambda\right) m}.$$

Но при достаточной удаленности точки (x_0, y_0) показатели μ и λ сколь угодно малы, и, следовательно, при достаточно больших m точки $(\xi_{m+1}, |\eta_m|)$ лежат под гиперболой

$$\eta = \frac{1}{\xi^{\beta}},$$

где $\beta = \frac{7}{13} - \varepsilon_1$, причем это $\beta > \frac{1}{2}$. Но эта гипербола, очевидно, такова, что в любом ее координатном прямоугольнике уже лежит по крайней мере один из координатных прямоугольников (ξ_m, η_m) леммы II и, следовательно, по крайней мере две точки ряда приближений леммы II, не лежащих на одной прямой с началом.

§ 69. Исследования В. А. Тартаковского, относящиеся к вопросу об ограничении величины самих решений методом Туэ

Определим при помощи предыдущих рассуждений точку ξ_{AL} по решению (x_0, y_0) $\left[x_0\rho - y_0 = \frac{\tau}{x_0^2}, \text{ где } 0 < L' < |\tau| < L \right]$. Пусть (x_1, y_1) тоже решение, т. е. $x_1\rho - y_1 = \frac{\tau_1}{x_1^2}$, где $0 < L' < |\tau_1| < L$. Построим при помощи решения (x_0, y_0) цепь приближений леммы II. Для каждого $m > 9$ там были построены два числа $B_0\rho + C_0$ и $B_1\rho + C_1$, не лежащих на одной прямой с началом. То из этих чисел, которое не лежит на одной прямой с началом и числом $x_1\rho - y_1$, обозначим $\omega_m = B^{(m)}\rho - C^{(m)}$. Тогда из двух равенств

$$x_1\rho - \left(y_1 + \frac{\tau_1}{x_1^2}\right) = 0, \tag{1}$$

$$B^{(m)}\rho - (C^{(m)} + \omega_m) = 0 \tag{2}$$

следует, что

$$\begin{vmatrix} x_1 & y_1 + \frac{\tau_1}{x_1^2} \\ B^{(m)} & C^{(m)} + \omega_m \end{vmatrix} = x_1 C^{(m)} - B^{(m)} y_1 + x_1\omega_m - B^{(m)} \frac{\tau_1}{x_1^2} = 0, \tag{3}$$

Но $|x_1 C^{(m)} - B^{(m)} y_1| \geqslant 1$. Мы докажем сейчас существование такого числа $\bar{x}$, что, если $x_1 > \bar{x}$, то

$$|x_1 \omega_m| < \frac{1}{2}, \tag{4}$$

$$\left| B^{(m)} \frac{\tau_1}{x_1^2} \right| < \frac{1}{2}. \tag{5}$$

Из (4) и (5) вытекает, что (3) невозможно, т. е. невозможно одновременное существование равенств (1) и (2), следствием которых является (3). Значит, (1) невозможно, ибо верность равенства (2) (при условии, что x_0, y_0 есть решение) была доказана в предыдущем параграфе.

Так как $|\omega_m|$ по лемме II меньше, чем

$$x_0^{\left(-\frac{7}{8}+\lambda\right)(m-1)+2}, \text{ а } |B^{(m)}| < x^{\left(\frac{13}{8}+\mu\right)(m-1)+1},$$

то, в случае выполнения условий

$$|x_1 x_0^{\left(-\frac{7}{8}+\lambda\right)(m-1)+2}| < \frac{1}{2}, \tag{4'}$$

$$\left| x_0^{\left(\frac{13}{8}+\mu\right)(m-1)+1} \cdot \frac{\tau_1}{x_1^2} \right| < \frac{1}{2}, \tag{5'}$$

условия (4) и (5) также выполняются. Покажем, что если x_1 больше некоторого $\bar{x}$, то существует $m > 9$, удовлетворяющее последним условиям. Условия существования m имеют такой вид:

$$\phi(z) = \left(\frac{8}{7}+\lambda'\right)\frac{\ln x_1}{\ln x_0} + 3\frac{2}{7} + \lambda'' < m < \left(\frac{16}{13}+\mu'\right)\frac{\ln x_1}{\ln x_0} + \frac{5}{13} + \mu'' = \varphi(z), \tag{6}$$

где

$$z = \frac{\ln x_1}{\ln x_0}.$$

Эти условия получаются из условий (4') и (5') логарифмированием. λ', λ'', μ', μ'' суть, как и λ, μ предыдущего параграфа, числа, которые по абсолютной величине могут стать меньше любой наперед заданной величины, если взять x_0 достаточно большим.

Отложим по оси абсцисс значения z, а по оси ординат ζ значения функций $\varphi(z)$ и $\phi(z)$. Если $z > \bar{z}$, $\zeta_2 = \varphi(z)$ превосходит $\zeta_1 = \phi(z)$ больше, чем на единицу, и $\zeta_1 = \phi(z) > 9$, то для каждого такого z условие (6) выполняется целым m. Разрешая неравенство

$$\left(\frac{8}{7}+\lambda'\right)z + 3\frac{2}{7} + \lambda'' + 1 < \left(\frac{16}{13}+\mu'\right)z + \frac{16}{13} + \mu'',$$

убеждаемся, что оно выполняется при достаточно малых λ', λ'', μ', μ'', т. е. при достаточно большом x_0 уже при $z \geqslant 45$. При этом также и $\phi(z) > 9$. Итак, при $z \geqslant 45$, т. е. при

$$x_1 \geqslant x_0^{45}$$

условие (6) при некотором целом $m > 9$ (своем для каждого x_1) удовлетворяется, и, значит, равенство (1) невозможно, т. е. (x_1, y_1) не есть решение. Таким образом решения, большие чем (x_0, y_0), могут лежать лишь между x_0 и x_0^{45}.

Покажем теперь, что леммы I и II значительно упрощаются для случая, когда m меньше некоторой константы m_0. В самом деле, в лемме I достаточно взять $\mu = \left[\frac{m}{2}\right]$, ибо при доказательстве этой леммы значение μ было исполь-

зовано всего лишь один раз, именно там, где мы доказываем существование числа h. Для этого необходимо было, чтобы разность $\frac{3(\mu+1)}{m+\mu+1}-1$ была больше положительной константы.

При $\mu=\left[\frac{m}{2}\right]$ и $m\leqslant m_0$ это обстоятельство имеет место, если $m=2\nu$; тогда

$$\Delta=\frac{3\nu+3-2\nu-\nu-1}{3\nu+1}>\frac{2}{\frac{3}{2}m_0+1}.$$

Если $m=2\nu+1$, то

$$\mu=\nu,\quad \Delta=\frac{3\nu+3-2\nu-1-\nu-1}{3\nu+2}>\frac{1}{\frac{3}{2}m_0+1}.$$

Итак, лемма I верна прн всяком положительном $m\leqslant m_0$ при $\mu=\left[\frac{m}{2}\right]$.

Лемма II может быть в этом случае средактирована так:

Лемма IIа. *Если числа x_0 и y_0 целые и такие, что $|\rho x_0-y_0|<1$, то для всякого положительного показателя m, такого, что $m\leqslant m_0$, можно всегда найти две пары целых чисел B_0, C_0 и B_1, C_1, таких, что $\frac{B_0}{C_0}\neq\frac{B_1}{C_1}$ и что $|B_0\rho+C_0|$ и $|B_1\rho+C_1|$ меньше, чем $D\cdot|x_0\rho-y_0|^{m-1}\cdot x_0^{\frac{m}{2}}$, причем $|B_0|$ и $|B_1|$ меньше, чем $H\cdot x_0^{\frac{3}{2}m}$.*

Доказательство. Продифференцируем равенство

$$P(t)\rho+Q(t)=(\rho-t)^m\cdot R(t),$$

установленное леммой I. Мы получим

$$P'(t)\rho+Q'(t)=(\rho-t)^{m-1}\cdot[(\rho-t)R'(t)-mR(t)].$$

Помножив это равенство на $P(t)$ и вычитая из предыдущего, помноженного на $P'(t)$, мы найдем

$$Q(t)\cdot P'(t)-P(t)\cdot Q'(t)=(\rho-t)^{m-1}\cdot\{(\rho-t)[P(t)\cdot R'(t)-P'(t)\cdot R(t)]-$$
$$-mP'(t)\cdot R(t)\}.$$

Так как уравнение $f(z)=0$, определяющее ρ, предполагается неприводимым, то полином от t с целыми рациональными коэффициентами, стоящий в левой части последнего равенства, делится на $[f(t)]^{m-1}$. Обозначив частное от деления через $W(t)$, получим:

$$Q(t)\cdot P'(t)-P(t)\cdot Q'(t)=[f(t)]^{m-1}\cdot W(t).$$

$W(t)$ — полином от t с целыми рациональными коэффициентами, ограниченными числом, не зависящим от x_0. Поэтому, если x_0 достаточно велико, то несократимая дробь $\frac{\bar{y}_0}{\bar{x}_0}$ не может быть корнем полинома $W(t)$. $\left(\text{Здесь } \bar{y}_0=\frac{y_0}{(x_0,y_0)},\ \bar{x}_0=\frac{x_0}{(x_0,y_0)}\right)$. В самом деле, $(x_0,y_0)\leqslant\sqrt[3]{\nu}$, где $\nu=f(x_0,y_0)$, т. е. $\bar{x}_0$ и $\bar{y}_0$ сколь угодно велики, если x_0 и y_0 сколь угодно велики, а $\bar{x}_0$ и $\bar{y}_0$ должны бы

быть делителями крайних коэффициентов $W(t)$, если бы $W\left(\frac{y_0}{x_0}\right)=0$. По неприводимости $f(t)$, $f\left(\frac{x_0}{y_0}\right)\neq 0$. Поэтому

$$Q\left(\frac{y_0}{x_0}\right)\cdot P'\left(\frac{y_0}{x_0}\right)-P\left(\frac{y_0}{x_0}\right)\cdot Q'\left(\frac{y_0}{x_0}\right)\neq 0$$

и, следовательно, в качестве чисел $B_0\rho+C_0$ и $B_1\rho+C_1$ можно взять

$$\rho x_0^{m+\mu}\cdot P\left(\frac{y_0}{x_0}\right)-x_0^{m+\mu}\cdot Q\left(\frac{y_0}{x_0}\right)=(x_0\rho-y_0)^m x_0^{\mu}\cdot R\left(\frac{y_0}{x_0}\right)$$

и

$$\rho x_0^{m+\mu-1}\cdot P'\left(\frac{y_0}{x_0}\right)-x_0^{m+\mu-1}\cdot Q'\left(\frac{y_0}{x_0}\right)=$$

$$=(x_0\rho-y_0)^{m-1}x_0^{\mu}\left[\left(\rho-\frac{y_0}{x_0}\right)R'\left(\frac{y_0}{x_0}\right)-mR\left(\frac{y_0}{x_0}\right)\right].$$

Отсюда видно, что

$$B_i<H\cdot x_0^{m+\left[\frac{m}{2}\right]}\leqslant H\cdot x_0^{\frac{3}{2}m}$$

и

$$|B_i\rho+C_i|<D\cdot|x_0\rho+y_0|^{m-1}x_0^{\left[\frac{m}{2}\right]}\leqslant D\cdot|x_0\rho+y_0|^{m-1}x_0^{\frac{m}{2}}.$$

Итак, лемма IIа доказана.

Повторяя рассуждения начала этого параграфа, мы убеждаемся, что (x_1, y_1) не может быть решением неопределенного уравнения, если есть такое целое положительное m, что выполняются условия:

$$\psi(z)=\frac{2}{3}\frac{\ln x_1}{\ln x_0}+\frac{4}{3}+\varepsilon<m<\frac{4}{3}\frac{\ln x_1}{\ln x_0}+\eta=\varphi(z),$$

где $z=\frac{\ln x_1}{\ln x_0}$, а ε и η — количества сколь угодно малые при достаточно большом x_0.

Если $z=\frac{\ln x_1}{\ln x}\geqslant 3.6$, то $\varphi(z)-\psi(z)>1$, и целое положительное m, удовлетворяющее условию $\psi(z)<m<\varphi(z)$, существует. Отсюда следует, что x_1 решения не может быть больше, чем $x_0^{3.6}$.

Будем далее для простоты вычислений предполагать, что неприводимый полином $f(t)$, корнем которого является ρ, есть $f(t)=t^3-at-b$ (т. е. что коэффициент при квадрате t равен нулю).

Рассмотрим два числа ω' и ω'', построенных при помощи решения (x_0, y_0),

$$\omega'=\rho x_0(3y_0^2-ax_0^2)-(2y_0^3+bx_0^3)=(\rho x_0-y_0)^2(-x_0\rho-2y_0)=B'\rho-C';$$

$$\omega''=\rho[3ay_0^4+18by_0^3x_0+6a^2y_0^2x_0^2+6aby_0x_0^3+(9b^2-a^3)x_0^4]-$$

$$-[9by_0^4+8a^2y_0^3x_0+18aby_0^2x_0^2+18b^2y_0x_0^3+a^2bx_0^4]=$$

$$=(y_0-\rho x_0)^3[9ax_0\rho^2+(3ay_0-9bx_0)\rho-(9by_0+8a^2x_0)]=B''\rho-C''.$$

Отметим, что $B'<Cx_0^3$, $B''<Cx_0^4$, $|\omega'|<Cx_0^{-3}$, $|\omega''|<Cx_0^{-5}$. Здесь и далее C, C_0, C_1, C_2, ... суть константы, зависящие лишь от a, b и ν, где ν — представляемое формою число, но не зависящие от x_0.

Докажем, что ω' и ω'' не суть решения. В самом деле,

$$|x_0\rho+2y_0|=|x_0\rho-y_0+3y_0|>3y_0-1>\frac{x_0}{C_1}, \quad \text{т. е.} \quad |\omega'|>\frac{x_0^{-3}}{C_2},$$

$$|9ax_0\rho^2+(3ay_0-9bx_0)\rho-(9by_0+8a^2x_0)|=$$
$$=|9a\rho(x_0\rho+y_0)+(12ay_0-9bx_0)\rho-(9by_0+8a^2x_0)|=$$
$$=|9a\rho(x_0\rho-y_0)-9b(x_0\rho-y_0)+12ay_0\rho-(18by_0+8a^2x_0)|=$$
$$=\left|(x_0\rho-y_0)\left[9a\rho-9b-\frac{8a^2}{\rho}\right]+\left[12a\rho-18b-\frac{8a^2}{\rho}\right]y_0\right|=$$
$$=\left|\frac{C_3}{x_0^2}+\frac{y_0}{\rho}(12a\rho^2-18b\rho-8a^2)\right|>\frac{x_0}{C_4}, \quad \text{т. е.} \quad \omega''>\frac{x_0^{-5}}{C_5}.$$

С другой стороны,

$$|B'|=\left|x_0\left[3\left(x_0\rho-\frac{\tau}{x_0^2}\right)^2-ax_0^2\right]\right|=\left|x_0^3(3\rho^2-a)-6\tau\rho+\frac{3\tau^2}{x_0^3}\right|>C_6x_0^3,$$

и аналогично

$$|B''|>C_7x_0^4.$$

Все эти неравенства основаны на том, что по неприводимости кубического полинома $f(t)$, корнем которого является ρ, все три числа

$$12a\rho^2-18b\rho-8a^2, \quad 3\rho^2-a, \quad 9a^2\rho+27ab\rho+(27b^2-a^3)$$

отличны от нуля. Итак $|B'|>C_6x_0^3$, $|\omega'|>\frac{x_0^{-3}}{C_2}$, т. е. (B', C') не есть решение.

Аналогично $|B''|>C_7x_0^4$, $|\omega''|>\frac{x_0^{-5}}{C_5}$, т. е. (B'', C'') не есть решение.

Докажем, что ω' и ω'' не лежат на одной прямой с решением. В самом деле, целая кратность ω' и ω'' не может быть решением, ибо дает еще худшее приближение к ρ, чем сами ω' и ω''. Вместе с тем, ω' и ω'' не могут быть и кратностью решения, ибо $d'=(B', C')$ и $d''=(B'', C'')$ ограничены константой d, не зависящей от x_0, а лишь от коэффициентов a, b и величины представляемого числа ν. Докажем это.

Известно, что для любых двух бинарных форм

$$\varphi(x_0, y_0)=\sum_{k=0}^{m}a_kx_0^{m-k}y_0^k \quad \text{и} \quad \psi(x_0, y_0)=\sum_{l=0}^{n}b_lx_0^{n-l}y_0^l$$

можно найти две другие бинарные формы

$$g(x_0, y_0) \quad \text{и} \quad h(x_0, y_0),$$

такие, что

$$g(x_0, y_0)\cdot\varphi(x_0, y_0)+h(x_0, y_0)\cdot\psi(x_0, y_0)=R_{\varphi,\psi}\cdot x_0^{m+n-1},$$

и две другие бинарные формы $\bar{g}(x_0, y_0)$ и $\bar{h}(x_0, y_0)$, такие, что

$$\bar{g}(x_0, y_0)\cdot\varphi(x_0, y_0)+\bar{h}(x_0, y_0)\cdot\psi(x_0, y_0)=R_{\varphi,\psi}\cdot y_0^{m+n-1}.$$

Здесь полиномы g, h, $\bar{g}$, $\bar{h}$ имеют в качестве коэффициевтов полиномы от a_k и b_l с целыми рациональными коэффициентами; $R_{\varphi,\psi}$ есть результант функций φ и ψ, т. е. тоже полином от a_k и b_l с целыми рациональными коэффициентами. Поэтому

$$(\varphi(x_0, y_0), \psi(x_0, y_0))|(R_{\varphi,\psi}\cdot x_0^{m+n-1}, R_{\varphi,\psi}\cdot y_0^{m+n-1})=R_{\varphi,\psi}\cdot(x_0, y_0)^{m+n-1}.$$

Так как в нашем случае, если под φ и ψ понимать в одном случае $B'(x_0, y_0)$ и $C'(x_0, y_0)$, а в другом $B''(x_0, y_0)$ и $C''(x_0, y_0)$, то

$$R_{B', C'} = 2\Delta, \quad R_{B'', C''} = -3\Delta^6,$$

где $\Delta = 4a^3 - 27b^2$, и, следовательно, d' и d'' меньше, чем

$$3\Delta^6 \cdot (x_0, y_0)^7 \leqslant 3\Delta^6 \cdot \nu^{\frac{7}{3}}$$

(где ν — представляемое формой число).

Условия невозможности для x_1, y_1 быть решением принимают вид:

$$|x_1\ \omega''| < \frac{1}{2}; \quad \left|B'' \frac{\tau_1}{x_1^2}\right| < \frac{1}{2}, \tag{7}$$

$$|x_1\ \omega'| < \frac{1}{2}; \quad \left|B' \frac{\tau_1}{x_1^2}\right| < \frac{1}{2}. \tag{8}$$

Условия (7) наверное выполняются, если будут выполняться условия, получающиеся из данных заменой ω'' бо́льшим числом Cx_0^{-5} и B'' бо́льшим числом Cx_0^{-4}, что дает для x_1 условия невозможности быть решеннем:

$$C_8 x_0^2 < x_1 < \frac{x_0^5}{C_9}.$$

Таким образом, x_1, большее, чем $C_8 x_0^2$, не может быть решеннем.

Аналогично, условия (8) наверное выполняются, если они будут выполнены после замены ω' бо́льшим числом Cx_0^{-3} и B' бо́льшим числом Cx_0^3, что дает для x_1 условия невозможности быть решением:

$$C_{10} x_0^{\frac{3}{2}} < x_1 < \frac{x_0^3}{C_{11}}.$$

Итак, мы получаем окончательный результат:

Если $x_1 > C_{10} x^{\frac{3}{2}}$, то x_1, y_1 не может быть решеннем.

Но в интервале $(x_0, C_{10} x_0^{\frac{3}{2}})$ решений быть не может. Докажем это.

Всякое достаточно большое решение x, y таково, что отношение $\frac{y}{x}$ равно подходящей дроби в разложении иррациональности ρ в непрерывную дробь. Пусть $\frac{y_0}{x_0}$ = одной из подходящих дробей $\frac{p_n}{q_n}$, т. е. $y_0 = dp_n$ и $x_0 = dq_n$, где $d = (x_0, y_0)$ меньше константы, не зависящей от x_0. Тогда

$$|q_n \rho - p_n| = \frac{1}{q_n a_n + q_{n-1}},$$

где a_n есть n-ное полное частное.

Отсюда

$$q_n a_n + q_{n+1} = \frac{1}{|q_n \rho - p_n|},$$

т. е.

$$a_n = \frac{1}{q_n |q_n \rho - p_n|} - \frac{q_{n-1}}{q_n} \geqslant \frac{d^2}{x_0 |x_0 \rho - y_0|} - 1 \geqslant \frac{d^2 x_0}{C_{12}} - 1,$$

т. е.

$$a_n = [a_n] \geqslant \frac{x_0}{C_{13}}.$$

Итак, $x_1 \geqslant p_{n+1} \geqslant \frac{x_0^2}{C_{14}}$, т. е. уже ближайшая к x_0 следующая за $\frac{p_n}{q_n}$ подходя-

щая дробь имеет знаменатель, превосходящий $C_{10}x^{\frac{3}{2}}$, а все остальные подходящие дроби и подавно.

Следовательно, можно указать такое число M, зависящее лишь от коэффициентов формы и представляемого числа, что решений x, y, бо́льших M, может быть только одно для каждого вещественного корня.

Аналогичный результат можно получить и для бинарных уравнений того же типа высших степеней.

§ 70. Улучшение теоремы Зигеля о числе решений неравенства $|f(x, y)| \leqslant k$, где $f(x, y)$ — кубическая двойничная форма положительного дискриминанта

1°. Постановка задачи. Элементарные неравенства. В настоящем параграфе мы помещаем изложение результата Зигеля о числе решений неопределенного уравнения $f(x, y) = k$, где $f(x, y)$ — кубическая форма с целыми коэффициентами. Зигель показал, что число решений такого уравнения для формы положительного дискриминанта не превосходит 18, если дискриминант достаточно велик по сравнению с представляемым числом k.

Мы несколько изменим рассуждения Зигеля и докажем, что число примитивных решений (с взаимно простыми x и y) неравенства

$$|f(x, y)| < k$$

не превосходит 15 [решения (x, y) и $(-x, -y)$ не считаются различными], если величина дискриминанта формы достаточно велика по сравнению с k.

Переходим к изложению.

Введем в рассмотрение кольцо кубических чисел, для которого форма $f(x, y)$ является индекс-формой. Проектируем кольцо на плоскость нулевого следа, выбрав оси координат и масштаб таким образом, чтобы комплексной координатой проекции точки $(\omega, \omega', \omega'')$ оказалась ее резольвента Лагранжа $\theta = \omega + \omega'\varepsilon + \omega''\varepsilon^2$, где $\varepsilon = e^{\frac{2\pi i}{3}}$. При этом кольцо спроектируется в плоскую решетку точек с площадью основного параллелограмма, равною $\frac{1}{2}\sqrt{3\Delta}$, где Δ — дискриминант кольца.

Пусть ω_1, ω_2 — нормальный базис кольца и $\omega = x\omega_1 + y\omega_2 + z$ — общее число кольца. Подсчитаем дискриминант числа ω двумя способами. С одной стороны,

$$D(\omega) = \Delta \cdot [f(x, y)]^2;$$

с другой стороны,

$$D(\omega) = [(\omega' - \omega'')(\omega'' - \omega)(\omega - \omega')]^2 = \frac{[(\theta - \overline{\theta})(\theta\varepsilon - \overline{\theta}\varepsilon^2)(\theta\varepsilon^2 - \overline{\theta}\varepsilon)]^2}{(\varepsilon - \varepsilon^2)^6} = \frac{(\theta^3 - \overline{\theta}^3)^2}{-27}.$$

Здесь $\overline{\theta} = \omega + \omega'\varepsilon^2 + \omega''\varepsilon$.

Сравнивая результаты, мы приходим к выводу, что решение неравенства $[f(x, y)] \leqslant k$ в целых числах равносильно решению неравенства

$$|\theta^3 - \overline{\theta}^3| \leqslant 3k\sqrt{3\Delta}$$

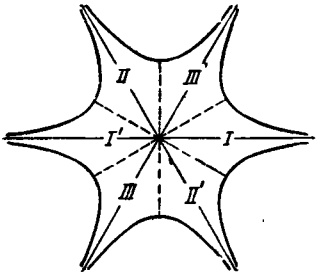
в точках решетки, в которую проектируется кольцо кубических чисел, соответствующее форме $f(x, y)$. Последнее неравенство легко изобразить геометрически. С этой целью введем полярные координаты $\theta = re^{i\varphi}$. При этом неравенство преобразуется в следующее:

$$r^3 |\sin 3\varphi| \leqslant \frac{3}{2} k\sqrt{3\Delta}.$$

Решить это неравенство в точках решетки значит найти все точки решетки в области, ограниченной кривыми $r^3 \sin 3\varphi = \pm\frac{3}{2} k\sqrt{3\Delta}$ (черт. 42).

Прямые, проведенные пунктиром, разбивают всю область на 6 частей: I, II, III, I′, II′, III′. Симметричные относительно начала координат области — I, I′; II, II′; III, III′ — определяют решения, которые мы условились не считать различными. Таким образом, нам нужно подсчитать число точек решетки в областях I, II и III.

В каждой из них подсчет производится совершенно одинаковым способом, ибо изменение нумерации величин ω, ω', ω'' влечет за собой перестановку областей I, II, III. Поэтому мы ограничимся подсчетом примитивных точек в области I и докажем, что в ней содержится не более 6 точек, если дискриминант достаточно велик.



Черт. 42.

Область (I) можно задать дополнительным неравенством

$$|\varphi| \leqslant \frac{\pi}{6}.$$

Выведем теперь некоторые простые неравенства для точек решетки, находящихся внутри области (I). Прежде всего оценим разность $\theta - \bar{\theta} = 2ri \sin\varphi$.

$$|\theta - \bar{\theta}| = 2r|\sin\varphi| \leqslant r \sin 3\varphi,$$

ибо при $|\varphi| < \frac{\pi}{6}$ имеет место $|2\sin\varphi| \leqslant \sin 3\varphi$. Следовательно,

$$r^2|\theta - \bar{\theta}| \leqslant \frac{3}{2} k\sqrt{3\Delta}. \tag{1}$$

Пусть теперь θ_1 и θ_2 — две различные примитивные точки решетки внутри области (I). В виду того, что они не лежат на одной прямой с началом координат, площадь построенного на них параллелограмма больше или равна площади основного параллелограмма решетки. Это приводит нас к неравенствам

$$\frac{1}{2}\sqrt{3\Delta} \leqslant r_1 r_2 |\sin(\varphi_1 - \varphi_2)| \leqslant r_1 r_2 (|\sin\varphi_1| + |\sin\varphi_2|) \leqslant$$

$$\leqslant \frac{1}{2} r_1 r_2 (|\sin 3\varphi_1| + |\sin 3\varphi_2|) \leqslant \frac{3}{4} k\sqrt{3\Delta}\left(\frac{r_2}{r_1^2} + \frac{r_1}{r_2^2}\right),$$

откуда

$$\frac{r_2}{r_1^2} + \frac{r_1}{r_2^2} \geqslant \frac{2}{3k}.$$

Если $r_2 \geqslant r_1$, то $\frac{r_1}{r_2^2} \leqslant \frac{r_2}{r_1^2}$ и, следовательно,

$$\frac{r_2}{r_1^2} \geqslant \frac{1}{3k}. \tag{2}$$

Это неравенство оказывается „сильным“ при больших значениях для r_1 и „слабым“ для малеиьких. Для последнего случая неравенство (2) можно заменить другим. Именно

$$\frac{1}{2}\sqrt{3\Delta} \leqslant r_1 r_2 |\sin(\varphi_1 - \varphi_2)| \leqslant r_1 r_2 \frac{\sqrt{3}}{2},$$

ибо

$$|\varphi_1 - \varphi_2| \leqslant \frac{\pi}{3}.$$

Но $r_1 \leqslant \sqrt{3k \cdot r_2}$, следовательно,

$$r_2 \cdot \sqrt{3k \cdot r_2} \cdot \frac{\sqrt{3}}{2} \geqslant \frac{1}{2}\sqrt{3\Delta},$$

откуда

$$r_2 \geqslant \left(\frac{\Delta}{3k}\right)^{\frac{1}{3}}. \tag{3}$$

Расположим теперь точки внутри области (I) в порядке возрастания радиусов-векторов:

$$r_1 \leqslant r_2 \leqslant r_3 \leqslant \ldots \leqslant r_s \leqslant r_{s+1} \leqslant \ldots$$

Из неравенства (2) выводим

$$\frac{r_{s+1}}{3k} \geqslant \left(\frac{r_s}{3k}\right)^2, \tag{4}$$

откуда

$$\frac{r_{s+m}}{3k} \geqslant \left(\frac{r_s}{3k}\right)^{2^m}.$$

При $s = 2$ получим

$$\frac{r_{m+1}}{3k} \geqslant \left(\frac{r_2}{3k}\right)^{2^{m-1}}.$$

Применяя к r_2 иеравенство (3), будем иметь

$$\frac{r_{m+1}}{3k} \geqslant \left(\frac{\Delta}{81k^4}\right)^{2^{m-1}}. \tag{5}$$

Неравенства (3), (4) и (5) приобретают более симметричную форму, если мы положим $r = (3k)^{\frac{1}{3}} \Delta^{\frac{1}{6}} t$. Именно, они перейдут в неравенства:

$$t_2 \geqslant \left(\frac{\Delta}{81k^4}\right)^{\frac{1}{6}}, \tag{3'}$$

$$t_{s+1} \geqslant \left(\frac{\Delta}{81k^4}\right)^{\frac{1}{6}} \cdot t_s^2, \tag{4'}$$

$$t_{m+1} \geqslant \left(\frac{\Delta}{81k^4}\right)^{\frac{2^m-1}{6}}. \tag{5'}$$

2°. О полиномах Туэ—Зигеля. Для дальнейших построений нам нужно исследовать некоторые полиномы, напоминающие полиномы Туэ. Именно — полиномы $A_m(z)$, $B_m(z)$, $C_m(z)$ и $D_m(z)$ возможно более низкой степени, удовлетворяющие условиям

$$\left.\begin{aligned} A_m(x^3) - xB_m(x^3) &= (1-x)^m V_m(x), \\ C_m(x^3) - x^2 D_m(x^3) &= (1-x)^m W_m(x), \end{aligned}\right\} \tag{6}$$

где V_m и W_m в свою очередь полиномы.

Мы докажем, что условиям (6) удовлетворяют следующие полиномы: при четном m, $m = 2n$:

$$\left.\begin{aligned} A_{2n}(z) &= \sum_{k=0}^{n} \binom{n-\frac{2}{3}}{k}\binom{n-\frac{1}{3}}{n-k} z^k; \\ B_{2n}(z) &= \sum_{k=0}^{n-1} \binom{n-\frac{1}{3}}{k}\binom{n-\frac{2}{3}}{n-1-k} z^k; \\ C_{2n}(z) &= \sum_{k=0}^{n} \binom{n-\frac{1}{3}}{k}\binom{n-\frac{2}{3}}{n-k} z^k; \\ D_{2n}(z) &= \sum_{k=0}^{n-1} \binom{n-\frac{2}{3}}{k}\binom{n-\frac{1}{3}}{n-1-k} z^k; \end{aligned}\right\} \tag{7}$$

при нечетном m, $m=2n+1$:

$$\left.\begin{aligned} A_{2n+1}(z) &= \sum_{k=0}^{n}\binom{n+\frac{1}{3}}{k}\binom{n-\frac{1}{3}}{n-k}z^k;\\ B_{2n+1}(z) &= \sum_{k=0}^{n}\binom{n-\frac{1}{3}}{k}\binom{n+\frac{1}{3}}{n-k}z^k;\\ C_{2n+1}(z) &= \sum_{k=0}^{n}\binom{n+\frac{2}{3}}{k}\binom{n-\frac{2}{3}}{n-k}z^k;\\ D_{2n+1}(z) &= \sum_{k=0}^{n}\binom{n-\frac{2}{3}}{k}\binom{n+\frac{2}{3}}{n-k}z^k. \end{aligned}\right\} \tag{7'}$$

Самый короткий путь для получения формул, определяющих интересующие нас полиномы, дает теория гипергеометрических функций. Не желая выходить за границы элементарных рассуждений, мы непосредственно, способом математической индукции, докажем, что полиномы (7) удовлетворяют соотношениям (6).

Для этого прежде всего введем рекуррентные формулы, связывающие полиномы с различными номерами и их производные друг с другом.

Эти формулы:

$$\left.\begin{aligned} A_{m+1}(z) &= \alpha_m A_m(z) - \beta_m(1-z)A_{m-1}(z);\\ B_{m+1}(z) &= \alpha_m B_m(z) - \beta_m(1-z)B_{m-1}(z);\\ C_{m+1}(z) &= \gamma_m C_m(z) - \delta_m(1-z)C_{m-1}(z);\\ D_{m+1}(z) &= \gamma_m D_m(z) - \delta_m(1-z)D_{m-1}(z). \end{aligned}\right\} \tag{8}$$

Здесь

$$\alpha_{2n}=2;\qquad \beta_{2n}=\frac{n-\frac{1}{3}}{n};\qquad \gamma_{2n}=2;\qquad \delta_{2n}=\frac{n-\frac{2}{3}}{n};$$

$$\alpha_{2n+1}=\frac{2n+1}{n+1};\quad \beta_{2n+1}=\frac{n+\frac{1}{3}}{n+1};\quad \gamma_{2n+1}=\frac{2n+1}{n+1};\quad \delta_{2n+1}=\frac{n+\frac{2}{3}}{n+1}.$$

$$\left.\begin{aligned} 3A'_m(z) &= \lambda_m D_{m-1}(z);\\ B_m(z)+3zB'_m(z) &= \lambda_m C_{m-1}(z);\\ 3C'_m(z) &= \mu_m B_{m-1}(z);\\ 2D_m(z)+3zD'_m(z) &= \mu_m A_{m-1}(z). \end{aligned}\right\} \tag{9}$$

Здесь

$$\lambda_{2n}=3n-2;\qquad \mu_{2n}=3n-1;$$
$$\lambda_{2n+1}=3n+1;\qquad \mu_{2n+1}=3n+2.$$

Соотношения (8) и (9) легко проверяются непосредственно.

На основании соотношений (8) и (9) легко доказать соотношения (6). Переходим к доказательству.

Соотношения (6), очевидно, выполняются для $m=1$ и $m=2$.

Допустим, что они выполняются для всех полиномов, индексы которых не превосходят m_0, и докажем в этом предположении, что они будут выполнены для полиномов с индексом m_0+1.

Тем самым соотношения (6) будут доказаны для всех полиномов.

Соотношения (9) показывают, что

$$[A_m(x^3)-xB_m(x^3)]'=-\lambda_m[C_{m-1}(x^3)-x^2D_{m-1}(x^3)],$$
$$[C_m(x^3)-x^2D_m(x^3)]'=-\mu_m x[A_{m-1}(x^3)-xB_{m-1}(x^3)].$$

Отсюда, на основании соотношений (6), справедливых, по предположению, при всех $m \leqslant m_0$, получим:

$$\begin{aligned} mV_m(x) - (1-x)\,V'_m(x) &= \lambda_m W_{m-1}(x), \\ mW_m(x) - (1-x)\,W'_m(x) &= \mu_m x V_{m-1}(x). \end{aligned} \tag{9'}$$

Положим теперь $x = 1$. Это нам даст

$$V_m(1) = \frac{\lambda_m}{m} W_{m-1}(1),$$

$$W_m(1) = \frac{\mu_m}{m} V_{m-1}(1).$$

Принимая во внимание, что

$$V_1(1) = 1; \quad W_1(1) = 2,$$

получим:

$$\left.\begin{aligned} V_{2n}(1) &= \frac{\lambda_{2n}\mu_{2n-1}\lambda_{2n-2}\cdots\lambda_2}{(2n)!}\cdot 2 = \frac{(3n)!}{3^n n!\,(2n)!}, \\ W_{2n}(1) &= \frac{\mu_{2n}\lambda_{2n-1}\mu_{2n-2}\cdots\mu_2}{(2n)!}\cdot 1 = \frac{(3n)!}{3^n n!\,(2n)!}, \\ V_{2n+1}(1) &= \frac{\lambda_{2n+1}\mu_{2n}\cdots\mu_2}{(2n+1)!}\cdot 1 = \frac{(3n+1)!}{3^n n!\,(2n+1)!}, \\ W_{2n+1}(1) &= \frac{\mu_{2n+1}\lambda_{2n}\cdots\lambda_2}{(2n+1)!}\cdot 2 = \frac{(3n+2)\cdot(3n)!}{3^n n!\,(2n+1)!}. \end{aligned}\right\} \tag{10}$$

Рассмотрим теперь выражения

$$A_{m_0+1}(x^3) - xB_{m_0+1}(x^3) \quad \text{и} \quad C_{m_0+1}(x^3) - x^2 D_{m_0+1}(x^3)$$

и докажем, что оба они делятся на $(1-x)^{m_0+1}$.

На основании соотношений (8)

$$\begin{aligned} A_{m_0+1}(x^3) - xB_{m_0+1}(x^3) &= \alpha_{m_0}[A_{m_0}(x^3) - xB_0(x^3)] - \\ &- \beta_{m_0}(1-x^3)[A_{m_0-1}(x^3) - xB_{m_0-1}(x^3)] = \\ &= (1-x)^{m_0}[\alpha_{m_0}V_{m_0}(x) - \beta_{m_0}(1+x+x^2)\,V_{m_0-1}(x)], \end{aligned}$$

$$C_{m_0+1}(x^3) - xD_{m_0+1}(x^3) = (1-x)^{m_0}[\gamma_{m_0}W_{m_0}(x) - \delta_{m_0}(1+x+x^2)\,W_{m_0-1}(x)].$$

Легко видеть, что выражения, находящиеся в квадратных скобках, делятся на $1-x$. В самом деле, оба они обращаются в нуль при $x = 1$, ибо

$$\begin{aligned} \alpha_{m_0}V_{m_0}(1) - 3\beta_{m_0}V_{m_0-1}(1) &= 0, \\ \gamma_{m_0}W_{m_0}(1) - 3\delta_{m_0}W_{m_0-1}(1) &= 0, \end{aligned}$$

что легко проверяется непосредственной подстановкой значений $V(1)$, $W(1)$, α, β, γ, δ отдельно при четном и нечетном m_0.

Тем самым, соотношения (6) доказаны полностью. Отметим еще некоторые свойства полиномов A_m, B_m, C_m, D_m, V_m, W_m, которые нам будут нужны в дальнейшем.

Свойство 1. Полиномы $V_m(x)$ и $W_m(x)$ имеют положительные коэффициенты.

Доказательство. Положим

$$V_m(x) = \sum v_m^{(k)} x^k, \quad W_m(x) = \sum w_m^{(k)} x^k.$$

Старшие коэффициенты функций V_m и W_m, очевидно, положительны, на основании соотношений (6).

Коэффициенты полиномов V_1, V_2, W_1, W_2 также положительны, в чем убеждаемся непосредственно проверкой.

Предположим, что коэффициенты полиномов $W_{m-1}(x)$ и $V_{m-1}(x)$ положительны, и в этом предположении докажем положительность коэффициентов $W_m(x)$ и $V_m(x)$. Тем самым свойство 1 будет доказано.

Соотношения (9′) дают:

$$\left.\begin{aligned}(m+k)\,v_m^{(k)} &= (k+1)\,v_m^{(k+1)} + \lambda_m w_{m-1}^{(k)},\\ (m+k)\,w_m^{(k)} &= (k+1)\,w_m^{(k+1)} + \mu_m v_{m-1}^{(k-1)}.\end{aligned}\right\} \qquad (9'')$$

На основании положительности чисел $\lambda_m v_{m-1}^{(k)}$ и $\mu_m v_{m-1}^{(k-1)}$ заключаем, что коэффициенты $v_m^{(k)}$ и $w_m^{(k)}$ положительны, если только $v_m^{(k+1)}$ и $w_m^{(k+1)}$ положительны. Следовательно, в виду того, что старшие коэффициенты функций V_m и W_m положительны, все $v_m^{(k)}$ и $w_m^{(k)}$ положительны, что и требовалось доказать.

Свойство 2.

$$|A_m(z)| < 2^{m-2},$$
$$|C_m(z)| < 2^{m-2},$$
$$|V_m(z)| < \left(\frac{3}{2}\right)^{m-2},$$
$$|W_m(z)| < \left(\frac{3}{2}\right)^{m-2},$$

последние — при $m > 3$, если только $|z| \leqslant 1$.

Доказательство. Вследствие положительности коэффициентов полиномов A, C, V и W

$$|A_m(z)| \leqslant A_m(1); \quad |C_m(z)| \leqslant C_m(1);$$
$$|V_m(z)| \leqslant V_m(1); \quad |W_m(z)| \leqslant W_m(1).$$

Значения $V_m(1)$ и $W_m(1)$ нам уже известны.

Значения $A_m(1)$ и $C_m(1)$ легко находятся из формулы (8), которые при $z = 1$ дают

$$A_{m+1}(1) = \alpha_m A_m(1); \quad C_{m+1}(1) = \gamma_m C_m(1).$$

Принимая во внимание, что $\alpha_m = \gamma_m \leqslant 2$ и что $A_2(1) = C_2(1) = 1$, получим

$$A_m(1) = C_m(1) = \alpha_{m-1}\alpha_{m-2}\ldots\alpha_2 < 2^{m-2},$$

точнее,

$$A_{2n+1}(1) = C_{2n+1}(1) = \frac{(2n)!}{(n!)^2}; \quad A_{2n}(1) = C_{2n}(1) = \frac{(2n-1)!}{n!\,(n-1)!}.$$

Для полиномов $V_m(z)$ и $W_m(z)$ имеем:

$$V_{2n}(1) = W_{2n}(1) = \frac{(3n)!}{3^n n!\,(2n)!} = \frac{3n-1}{2n}\cdot\frac{3n-2}{2n-1}\cdot\frac{3n-4}{2n-2}\cdot\frac{3n-5}{2n-3}\cdots\frac{5}{4}\cdot\frac{4}{3}\cdot\frac{2}{2}\cdot\frac{2}{1} <$$
$$< \left(\frac{3}{2}\right)^{2n-2} = \left(\frac{3}{2}\right)^{m-2},$$

$$V_{2n+1}(1) = \frac{(3n+1)!}{3^n\cdot n!\,(2n+1)!} < \frac{3n+1}{2n+1}\cdot\left(\frac{3}{2}\right)^{2n-2} < \left(\frac{3}{2}\right)^{2n-1},$$

$$W_{2n+1}(1) = \frac{3n+2}{2n+1}\cdot\frac{(3n)!}{3^n n!\,(2n)!} < \frac{3n+2}{2n+1}\cdot\frac{5}{3}\cdot\left(\frac{3}{2}\right)^{2n-4} < \left(\frac{3}{2}\right)^{2n-1}$$

при $n > 1$.

Свойство 2 доказано.

Свойство 3.

$$A_m(x^3)\,C_m(x^3) - x^3 B_m(x^3)\,D_m(x^3) \neq 0$$

при $x^3 \neq 1$.

Доказательство.

$$A_m(x^3) - x\,B_m(x^3) = (1-x)^m V_m(x),$$
$$C_m(x^3) - x^2 D_m(x^3) = (1-x)^m W_m(x).$$

Умножив первое равенство на $C_m(x^3)$, второе на $xB_m(x^3)$ и сложив, получим:

$$A_m(x^3)\,C_m(x^3) - x^3 B_m(x^3)\,D_m(x^3) = (1-x)^m [C_m(x^3)\,V_m(x) + xB_m(x^3)\,W_m(x)].$$

Левая часть есть полином степени m от x^3. В виду того, что он делится на $(1-x)^m$, он должен делиться и на $(1-x^3)^m$. Частное от деления есть постоянная, очевидно, отличная от 0, ибо она равна $A_m(0)\cdot C_m(0)$. Итак,

$$A_m(x^3)\,C_m(x^3) - x^3 B_m(x^3)\,D_m(x^3) = A_m(0)\,C_m(0)\,(1-x^3)^m \neq 0$$

при $x^3 \neq 1$, что и требовалось доказать.

Свойство 4. Для полиномов с нечетными номерами имеют место соотношения

$$z^n A_{2n+1}\left(\frac{1}{z}\right) = B_{2n+1}(z),$$
$$z^n C_{2n+1}\left(\frac{1}{z}\right) = D_{2n+1}(z),$$

— очевидно.

Свойство 5. Коэффициенты полиномов A_{2n+1}, B_{2n+1}, C_{2n+1}, D_{2n+1} становятся целыми, если их умножить на $M_n = 3^{\left[\frac{3}{2}n\right]}$. (То же самое имеет место и для полиномов с четными номерами.)

Доказательство. Рассмотрим биномиальный коэффициент

$$\binom{n+\frac{1}{3}}{k} = \frac{(3n+1)(3n-2)\ldots(3n+4-3k)}{3^k \cdot k!}.$$

Выделим в знаменателе степень тройки $k! = 3^{\varkappa}\cdot K$, где K не делится на 3. Через s обозначим решение сравнения

$$3s \equiv 1 \pmod K.$$

Тогда $(3n+1)(3n-2)\ldots(3n+4-3k) \equiv 3^k (n+s)(n+s-1)\ldots(n+s-(k-1)) \equiv 0 \pmod K$, ибо $(n+s)(n+s-1)\ldots(n+s-(k-1))$ делится на $k!$, а следовательно, и на K.

Итак, $3^{k+\varkappa}\binom{n+\frac{1}{3}}{k}$ есть число целое. Но $k+\varkappa = k+\left[\frac{k}{3}\right]+\left[\frac{k}{9}\right]+\ldots < \frac{3}{2}k$.

Таким же образом убедимся в том, что $3^{l+\lambda}\binom{n-\frac{1}{3}}{n-k}$ есть число целое, при

$$l+\lambda = n-k+\left[\frac{n-k}{3}\right]+\left[\frac{n-k}{9}\right]+\ldots < \frac{3}{2}(n-k).$$

Следовательно, $3^{\left[\frac{3}{2}n\right]}\cdot\binom{n+\frac{1}{3}}{k}\binom{n-\frac{1}{3}}{n-k}$ есть целое число, т. е. $M_n A_{2n+1}(z)$ имеет целые коэффициенты. Точно таким же способом убеждаемся в том, что $M_n C_{2n+1}(z)$ имеет целые коэффициенты.

3°. Построение заградительного ряда.

Лемма. *Если* θ *есть резольвента числа* ω *из кубического кольца, то* $\theta F_1(\theta^3, \overline{\theta}^3)$ *и* $\overline{\theta}^2 F_2(\theta^3, \overline{\theta}^3)$ *суть также резольвенты чисел того же кольца, если* F_1 *и* F_2 *— полиномы с целыми рациональными коэффициентами.*

Доказательство. В виду того, что θ^3 и $\overline{\theta}^3$ корни квадратного уравнения с целыми коэффициентами,

$$F_1(\theta^3, \overline{\theta}^3) = A + B\theta^3; \quad F_2(\theta^3, \overline{\theta}^3) = C + D\theta^3$$

при целых рациональных A, B, C и D. Следовательно, принимая во внимание, что $\theta\overline{\theta}$ — целые рациональные, числа $\theta F_1(\theta^3, \overline{\theta}^3)$ и $\overline{\theta}^2 F_2(\theta^3, \overline{\theta}^3)$ могут быть представлены в виде $A_1\theta + B_1\overline{\theta}^2$ при целых рациональных A_1 и B_1. θ есть резольвента ω, $\overline{\theta}^2 = (\omega + \omega'\varepsilon^2 + \omega''\varepsilon)^2 = \omega^2 + 2\omega'\omega'' + (\omega'^2 + 2\omega\omega'')\varepsilon + (\omega''^2 + 2\omega\omega')\varepsilon^2$ есть резольвента числа $\omega^2 + 2\omega'\omega'' = 3\omega^2 - 2s\omega + 2q$, принадлежащего кольцу вместе с ω. В виду того, что резольвенты образуют решетку, $A_1\theta + B_1\overline{\theta}^2$ является тоже резольвентой числа из кольца, что и требовалось доказать.

Переходим теперь к построению „заградительного ряда".

Пусть θ — точка в области I, дающая решение неравенства $|f(x, y)| \leqslant k$. Введем в рассмотрение точки

$$H_n = M_n A_{2n+1}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\cdot\theta^{3n+1}, \quad K_n = M_n C_{2n+1}\left(\frac{\theta^3}{\overline{\theta}^3}\right)\cdot\overline{\theta}^{3n+2}.$$

Здесь $M_n = 3^{\left[\frac{3}{2}n\right]}$, A_{2n+1} и C_{2n+1} — полиномы, введенные в предыдущем пункте параграфа.

Точки H_n и K_n принадлежат решетке, в которую проектируется кольцо, ибо $M_n A_{2n+1}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\theta^{3n}$ и $M_n C_{2n+1}\left(\frac{\theta^3}{\overline{\theta}^3}\right)\cdot\overline{\theta}^{3n}$ суть полиномы от θ^3 и $\overline{\theta}^3$ с целыми рациональными коэффициентами.

Точки H_n, K_n не лежат на одной прямой с началом координат, ибо

$$H_n\overline{K}_n - \overline{H}_n K_n = M_n^2\theta^{6n+3}\left[A_{2n+1}\left(\frac{\theta^3}{\theta^3}\right)C_{2n+1}\left(\frac{\theta^3}{\theta^3}\right) - \left(\frac{\overline{\theta}}{\theta}\right)^{6n+3} A_{2n+1}\left(\frac{\theta^3}{\overline{\theta}^3}\right)C_{2n+1}\left(\frac{\theta^3}{\overline{\theta}^3}\right)\right] =$$

$$= M_n^2\theta^{6n+3}[A_{2n+1}(x^3)C_{2n+1}(x^3) - x^3 B_{2n+1}(x^3)D_{2n+1}(x^3)] \neq 0,$$

так как $x^3 = \frac{\overline{\theta}^3}{\theta^3} \neq 1$.

Оценим модули H_n, K_n, $H_n - \overline{H}_n$, $K_n - \overline{K}_n$.

$$|H_n| = M_n\left|A_{2n+1}\left(\frac{\theta^3}{\overline{\theta}^3}\right)\right|\cdot|\theta|^{3n+1} < 3^{\frac{3}{2}n}\cdot 2^{2n-1}r^{3n+1};$$

$$|K_n| = M_n\left|C_{2n+1}\left(\frac{\theta^3}{\overline{\theta}^3}\right)\right|\cdot|\overline{\theta}|^{3n+2} < 3^{\frac{3}{2}n}\cdot 2^{2n-1}r^{3n+2};$$

$$|H_n - \overline{H}_n| = M_n\left|A_{2n+1}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\theta^{3n+1} - A_{2n+1}\left(\frac{\theta^3}{\overline{\theta}^3}\right)\overline{\theta}^{3n+1}\right| =$$

$$= M_n\left|A_{2n+1}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\theta^{3n+1} - B_{2n+1}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\theta^{3n}\overline{\theta}\right| =$$

$$= M_n r^{3n+1}\left|1 - \frac{\overline{\theta}}{\theta}\right|^{2n+1}\cdot\left|V_{2n+1}\left(\frac{\overline{\theta}}{\theta}\right)\right| <$$

$$< 3^{\frac{3}{2}n}\cdot r^n\cdot\left(\frac{3}{2}\right)^{2n-1}\cdot|\theta - \overline{\theta}|^{2n+1}.$$

Но $|\theta_1 - \theta| \leqslant \frac{3}{2} k \sqrt{3\Delta} \cdot r^{-2}$.

Следовательно,

$$|H_n - \overline{H}_n| < 3^{\frac{5n+1}{2}} \cdot \left(\frac{3}{2}\right)^{4n} \cdot k^{2n+1} \Delta^{n+\frac{1}{2}} r^{-3n-2}.$$

Таким же образом

$$|K_n - \overline{K}_n| < 3^{\frac{5n+1}{2}} \cdot \left(\frac{3}{2}\right)^{4n} \cdot k^{2n+1} \Delta^{n+\frac{1}{2}} r^{-3n-1}.$$

Пусть $\theta_1 = r_1 e^{i\varphi}$ — какая-либо точка в области I. Точка θ_1 не лежит на одной прямой с одной из точек H_n, K_n. Следовательно, площадь основного параллелограмма решетки не превосходит площади параллелограмма, построенного на θ_1 и H_n или, если эта последняя равна нулю, не превосходит площади параллелограмма, построенного на θ_1 и K_n.

Это приводит нас к тому, что должно выполняться одно из неравенств

$$\frac{1}{2}\sqrt{3\Delta} \leqslant \frac{1}{2}|\theta_1 \overline{H}_n - \overline{\theta}_1 H_n| \leqslant \frac{1}{2}|\theta_1 - \overline{\theta}_1| \cdot |\overline{H}_n| + \frac{1}{2}|\overline{\theta}_1| \cdot |\overline{H}_n - H_n| <$$

$$< \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{k\sqrt{3\Delta}}{r_1^2} \cdot 3^{\frac{3}{2}n} 2^{2n-1} r^{3n+1} + \frac{1}{2} r_1 3^{\frac{5n+1}{2}} \left(\frac{3}{2}\right)^{4n} \frac{k^{2n+1} \Delta^{n+\frac{1}{2}}}{r^{3n+2}},$$

или

$$\frac{1}{2}\sqrt{3\Delta} \leqslant \frac{1}{2}|\theta_1 \overline{K}_n - \overline{\theta}_1 K_n| <$$

$$< \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{k\sqrt{3\Delta}}{r_1^2} 3^{\frac{3}{2}n} 2^{2n-1} r^{3n+2} + \frac{1}{2} r_1 3^{\frac{5n+1}{2}} \left(\frac{3}{2}\right)^{4n} \frac{k^{2n+1} \Delta^{n+\frac{1}{2}}}{r^{3n+1}}.$$

Если невозможно второе неравенство, то невозможно и первое. Поэтому будем интересоваться только вторым неравенством. Оно значительно упрощается, если положить $r = (3k)^{\frac{1}{3}} \Delta^{\frac{1}{6}} t$, $r_1 = (3k)^{\frac{1}{3}} \Delta^{\frac{1}{6}} t$, что мы уже делали раньше для упрощения элементарных неравенств. После очевидных преобразований получим

$$1 \leqslant \frac{1}{2} c_1^n k^{n+1} \Delta^{\frac{n}{2}} \left[\frac{t^{3n+2}}{t_1^2} + \frac{t_1}{t^{3n+1}}\right],$$

где c_1 — абсолютная постоянная.

Пусть $t_1 = t^\nu$, и возьмем $n = \left[\frac{\nu}{2}\right]$. Тогда

$$\frac{\nu}{2} - 1 \leqslant n \leqslant \frac{\nu}{2},$$

что дает после упрощений

$$1 \leqslant c_1^{\frac{\nu}{2}} k^{\frac{\nu}{2}+1} \Delta^{\frac{\nu}{4}} t^{-\frac{\nu}{2}+2}.$$

Это неравенство, очевидно, невозможно при $\nu \geqslant 4 + \varepsilon$ и при достаточно больших t.

Отсюда уже следует конечность числа решений неравенства $|f(x, y)| \leqslant k$.

Положим теперь, что $\Delta \geqslant 81k^4$, и допустим, что неравенство $|f(x, y)| \leqslant k$ имеет семь решений в области (I). Примем за t число, соответствующее четвертому решению, за t_1 — число, соответствующее седьмому решению. В силу неравенств (4′) и (5′) имеем

$$t_1 \geqslant t^8, \quad \text{т. е.} \quad \nu \geqslant 8,$$

$$t \geqslant \left(\frac{\Delta}{81k^4}\right)^{\frac{7}{6}}.$$

Приимая эти неравенства во внимание, получим

$$1 \leqslant c_2^{\nu} k^{\frac{17}{6}\nu - \frac{25}{3}} \Delta^{\frac{7}{3} - \frac{\nu}{3}}.$$

Это неравенство невозможно, если

$$\Delta > c_2^{\frac{3\nu}{\nu - 7}} k^{\frac{17\nu - 50}{2\nu - 14}}.$$

Для того, чтобы последнее неравенство было невозможно при всех $\nu \geqslant 8$, нужно потребовать

$$\Delta > c_8 \cdot k^{\frac{17 \cdot 8 - 50}{2 \cdot 8 - 14}} = c_8 k^{43}.$$

Итак, если $\Delta > c_8 k^{43}$, неравенство $|f(x, y)| \leqslant k$ не может иметь больше шести примитивиых решений в области I и, следовательно, всего не более 18 решеиий. Константу c_8 можно подсчитать. Грубый подсчет дает для нее величину порядка 10^{88}.

Точно таким же способом легко доказать, что, если $f(x, y)$ кубическая форма отрицательного дискриминанта, неравенство $|(f(x, y)| \leqslant k$ имеет не более шести примитивных решений при достаточно большом дискриминанте.

В этом случае за координаты проекции нужно взять резольвенты $\theta = \omega + \omega'\varepsilon + \omega''\varepsilon^2$ и $\overline{\theta} = \omega + \omega'\varepsilon^2 + \omega''\varepsilon$, которые обе будут вещественны, если ω — вещественное, ω' и ω'' — сопряженные комплексные.

Задача сводится к подсчету точек решетки резольвент в области

$$|\theta^3 - \overline{\theta}^3| \leqslant 3k\sqrt{3\Delta}.$$

Роль „r“ в оценках будет играть бо́льшая из координат точки. Все оценки в этом случае проводятся так же, как в случае положительного дискриминанта, но только с другими константами.

4°. Дальнейшее уточнение результата Зигеля. Уточним теперь результат, полученый в предыдущем пункте, введя в рассмотрение также и полиномы с четными номерами, которые мы до сих пор не привлекали к построению „заградительного ряда“.

Предварительно докажем следующую лемму о проекции кольца.

Лемма. *Произведение резольвент двух чисел кубического кольца есть сопряженная резольвента числа того же кольца.*

Доказательство. Пусть ω_1 и ω_2 — числа, образующие нормальный базис кольца и

$$\varphi = x_1\omega_1 + y_1\omega_2 + z_1; \quad \psi = x_2\omega_1 + y_2\omega_2 + z_2$$

(x_1, y_1, z_1 и x_2, y_2, z_2 — целые рациональные числа) — произвольные числа кольца. Обозначим через θ_1 и θ_2 резольвенты чисел ω_1 и ω_2. Тогда произведение резольвент чисел φ, ψ равно

$$x_1x_2\theta_1^2 + (x_1y_2 + x_2y_1)\theta_1\theta_2 + y_1y_2\theta_2^2.$$

Мы уже доказали (лемма 3°), что θ_1^2 и θ_2^2 суть сопряженные резольвенты чисел кольца. Остается то же самое доказать для $\theta_1\theta_2$.

Но

$$\theta_1\theta_2 = (\omega_1 + \omega_1'\varepsilon + \omega_1''\varepsilon^2)(\omega_2 + \omega_2'\varepsilon + \omega_2''\varepsilon^2) =$$

$$= \omega_1\omega_2 + \omega_1'\omega_2'' + \omega_1''\omega_2' + \varepsilon^2(\omega_1'\omega_2' + \omega_1''\omega_2 + \omega_1\omega_2'') + \varepsilon(\omega_1''\omega_2'' + \omega_1\omega_2'' + \omega_1'\omega_2),$$

откуда следует, что $\theta_1\theta_2$ есть сопряженная резольвента для числа $\omega_1\omega_2 + \omega_1'\omega_2'' +$

$+\omega_1''\omega_2'$. Это число принадлежит взятому кубическому кольцу. Действительно,

$$\omega_1\omega_2+\omega_1'\omega_2''+\omega_1''\omega_2'=ad+\frac{\omega_1' ad}{\omega_1''}+\frac{\omega_1'' ad}{\omega_1'}=ad+ad\frac{\omega_1'^2+\omega_1''^2}{\omega_1'\omega_1''}=$$

$$=ad+ad\frac{b^2-2ac-\omega_1^2}{\omega_1'\omega_1''}=ad+ad\frac{(b^2-2ac)\omega_1+\omega_1^3}{a^2d}=$$

$$=ad+\frac{(b^2-2ac)\omega_1-b\omega_1^2+ac\omega_1-a^2d}{a}=$$

$$=\frac{(b^2-ac)\omega_1-b(b\omega_1-ac+a\omega_2)}{a}=$$

$$=bc-c\omega_1-b\omega_2.$$

Здесь a, b, c, d — коэффициенты индекс-формы кольца.

Тем самым лемма доказана.

Обратимся теперь к полиномам с четными номерами.

Когда мы строили заградительный ряд посредством нечетных полиномов, для нас был нажен факт ограниченности снизу модуля величины

$$\theta_1\theta^{3n+1}\cdot M_{2a+1}\left[\frac{\overline{\theta}_1}{\theta_1}A_m\left(\frac{\overline{\theta}^3}{\theta^3}\right)-\frac{\overline{\theta}}{\theta}B_m\left(\frac{\overline{\theta}^3}{\theta^3}\right)\right],$$

если только она отлична от нуля.

Ограниченность модуля этой величины снизу вытекала из того, что этот модуль представляет собою удвоенную площадь основного параллелограмма, построенного на двух точках θ_1 и $\theta^{3n+1}M_{2n+1}A_m\left(\frac{\overline{\theta}^3}{\theta^3}\right)$ решетки резольвент.

Если составить аналогичную величину

$$U_{2n}=\theta_1\theta^{3n}\cdot M_{2n}\left[\frac{\theta_1}{\theta_1}A_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right)-\frac{\overline{\theta}}{\theta}B_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\right],$$

исходя из полиномов с четным номером, то она, не имея такого простого геометрического смысла, все же будет ограничена снизу по модулю числом, зависящим только от дискриминанта области.

Действительно, в виду того, что A_{2n} является полиномом степени n, B_{2n} — полином степени $n-1$, и в силу доказанной выше леммы величина U_{2n} является сопряженной резольвентой для одного из чисел кольца, т. е. точкой, симметричной относительно вещественной оси с одной из точек интересующей нас решетки — проекции кольца.

Далее, легко видеть, что $U_{2n}\neq 0$.

Действительно, если бы $U_{2n}=0$, мы имели бы

$$\frac{\overline{\theta}_1}{\theta_1}A_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right)=\frac{\overline{\theta}}{\theta}B_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right). \qquad (*)$$

Это равенство оставалось бы верным при переходе к комплексно сопряженным числам, что дает

$$\frac{\theta_1}{\overline{\theta}_1}A_{2n}\left(\frac{\theta^3}{\overline{\theta}^3}\right)=\frac{\theta}{\overline{\theta}}B_{2n}\left(\frac{\theta^3}{\overline{\theta}^3}\right).$$

В силу доказанного ранее свойства полиномов A_{2n}, B_{2n} имеем

$$A_{2n}\left(\frac{\theta^3}{\overline{\theta}^3}\right)=\frac{\theta^{3n}}{\overline{\theta}^{3n}}C_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right),$$

$$B_{2n}\left(\frac{\theta^3}{\overline{\theta}^3}\right)=\frac{\theta^{3n-3}}{\overline{\theta}^{n-2}}D_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right),$$

откуда

$$\frac{\theta_1}{\overline{\theta}_1} C_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right) = \frac{\overline{\theta}^2}{\theta^2} D_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right).$$

Умножив почленно последние равенства (*), мы получили бы

$$A_{2n}\left(\frac{\overline{\theta}^3}{\theta^2}\right) C_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right) = \frac{\overline{\theta}^3}{\theta^3} B_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right) D_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right),$$

что невозможно, ибо

$$A_{2n}(x)\, C_{2n}(x) - x \cdot B_{2n}(x) \cdot D_{2n}(x) = A_{2n}(0) \cdot C_{2n}(0)\,(1-x)^{2n} \neq 0$$

при $x = \frac{\overline{\theta}^3}{\theta^3} \neq 1$.

Итак, $U_{2n} \neq 0$ и является точкой, сопряженной с одной из точек решетки резольвент.

Отсюда следует, что

$$|U_{2n}| \geqslant \left(\frac{3}{2}\sqrt{3\Delta}\right)^{\frac{1}{3}},$$

ибо все точки решетки резольвент расположены на кривых $r^3 |\sin 3\varphi| = \frac{3}{2} k \sqrt{3\Delta}$ при целых рациональных k, и, следовательно, модуль каждой точки решетки резольвент $r \geqslant \left(\frac{3}{2}\sqrt{3\Delta}\right)^{\frac{1}{3}}$.

Итак

$$\left|\theta_1 \theta^{3n} M_{2n} \cdot A_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right) \cdot \frac{\overline{\theta}_1}{\theta_1} - \frac{\overline{\theta}}{\theta} B_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\right| \geqslant \left(\frac{3}{2}\sqrt{3\Delta}\right)^{\frac{1}{3}}.$$

Обозначим, как раньше, $|\theta| = r$; $\theta_1 = r_1$.

Из последнего неравенства получаем

$$\left(\frac{3}{2}\sqrt{3\Delta}\right)^{\frac{1}{3}} \leqslant M_{2n} r_1 r^{3n}\left[\left|A_{2n}\left(\frac{\overline{\theta}^3}{\theta^3}\right)\right| \cdot \left|\frac{\overline{\theta}_1}{\theta_1} - 1\right| + \left|1 - \frac{\overline{\theta}}{\theta}\right|^{2n} \cdot \left|V_{2n}\left(\frac{\overline{\theta}}{\theta}\right)\right|\right] \leqslant$$

$$\leqslant M_{2n}\left[r^{3n} A_{2n}(1) \cdot |\overline{\theta}_1 - \theta_1| + r^n r_1 \cdot |\theta - \overline{\theta}|^{2n} \cdot V_{2n}(1)\right] \leqslant$$

$$\leqslant M_{2n}\left[\frac{3}{2} k \sqrt{3\Delta} \cdot A_{2n}(1) \cdot \frac{r^n}{r_1^2} + \left(\frac{3}{2} k \sqrt{3\Delta}\right)^{2n} \cdot V_{2n}(1) \cdot \frac{r_1}{r^{3n}}\right].$$

Переходя от величин r и r_1 к величинам t и t_1, получим

$$1 \leqslant c^n k^{n+\frac{1}{3}} \Delta^{\frac{n}{2}}\left[\frac{t^{3n}}{t_1^2} + \frac{t_1}{t^{3n}}\right],$$

или, положив $t_1 = t^\nu$,

$$1 \leqslant c^n k^{n+\frac{1}{3}} \Delta^{\frac{n}{2}}\left(t^{3n-2\nu} + t^{\nu-3n}\right). \qquad (**)$$

Сопоставим это неравенство с неравенством, полученным ранее из рассмотрения полиномов с нечетными номерами,

$$1 \leqslant c_1^n k^{n+1} \Delta^{\frac{n}{2}}\left(t^{3n+2-2\nu} + t^{\nu-3n-1}\right). \qquad (*_*)$$

Первое из этих неравенств дает наилучший результат, если ν близко к четному числу $2n$, второе, если ν близко к нечетному числу $2n+1$. Всю область возможных значений для ν разобьем на интервалы $2n - \alpha \leqslant \nu \leqslant 2n + \alpha$ и $2n+1-\beta \leqslant \nu \leqslant 2n+1+\beta$, окружающие все целые числа. Эти интервалы

покроют все вещественные числа, если взять $\alpha+\beta=1$. Числа α и β мы в дальнейшем выберем наиболее целесообразным образом. Для каждого значения ν подберем соответствующее значение n. Будем иметь

$$\frac{\nu-\alpha}{2}\leqslant n\leqslant\frac{\nu+\alpha}{2},$$

если ν попадает в интервал, окружающий четное число, или

$$\frac{\nu-1-\beta}{2}\leqslant n\leqslant\frac{\nu-1+\beta}{2},$$

если ν попадает в интервал, окружающий нечетное число.

В первом случае неравенство (**) дает:

$$1\leqslant c_2^{\nu}k^{\frac{\nu}{2}+\frac{1}{3}+\frac{\alpha}{2}}\cdot\Delta^{\frac{\nu+\alpha}{4}}\cdot t^{-\frac{\nu}{2}+\frac{3\alpha}{2}}. \tag{A}$$

Во втором случае неравенство (*_*) дает:

$$1\leqslant c_2^{\nu}k^{\frac{\nu}{2}+\frac{1}{2}+\frac{\beta}{2}}\Delta^{\frac{\nu-1+\beta}{4}}t^{-\frac{\nu}{2}+\frac{1}{2}+\frac{3\beta}{2}}. \tag{B}$$

Пусть t соответствует четвертому решению в области (I). Тогда на осиовании элементарных неравенств 1^0 этого параграфа $t\geqslant\left(\frac{\Delta}{81k^4}\right)^{\frac{7}{6}}$, и, следовательно,

$$1\leqslant c_3^{\nu}\cdot k^{\frac{17}{6}\nu+\frac{1}{3}+\frac{13}{2}\alpha}\cdot\Delta^{2\alpha-\frac{\nu}{3}},$$

или

$$1\leqslant c_3^{\nu}\cdot k^{\frac{17}{6}\nu-\frac{11}{6}-\frac{13}{2}\beta}\cdot\Delta^{2\beta+\frac{1}{3}-\frac{\nu}{3}}.$$

Покажем теперь, что при достаточно большом Δ количество точек в области (I) не более пяти. Действительно, для шестого решения $\nu\geqslant 4$, если только $\Delta\geqslant 81k^4$. Неравенства невозможны, если

$$\Delta>c_8^{\frac{\nu}{\frac{\nu}{3}-2\alpha}}\cdot k^{\frac{\frac{17}{6}\nu+\frac{1}{3}-\frac{13}{2}\alpha}{\frac{\nu}{3}-2\alpha}},$$

$$\Delta>c_8^{\frac{\nu}{\frac{\nu}{3}-2\beta-\frac{1}{3}}}\cdot k^{\frac{\frac{17}{6}\nu-\frac{11}{6}-\frac{13}{2}\beta}{\frac{\nu}{3}-2\beta-\frac{1}{3}}},$$

если только $\nu>6\alpha$ и $\nu>6\beta+1$, и, следовательно, неравенства невозможны, если

$$\Delta>c_4\cdot k^{\frac{\frac{35}{3}-\frac{13}{2}\alpha}{\frac{4}{3}-2\alpha}},$$

$$\Delta>c_4\cdot k^{\frac{\frac{19}{2}-\frac{13}{2}\beta}{1-2\beta}},$$

если только $\alpha<\frac{2}{3}$; $\beta<\frac{1}{2}$.

Взяв $\alpha=\frac{96}{163}$, $\beta=\frac{69}{163}$, мы получим невозможность неравенств, а следовательно, и невозможность существования шестого решения в области (I) при

$$\Delta>c_4k^{44}.$$

5°. Ограничение всех решений неравенства $|f(x, y)| \leqslant k$ в области (I), кроме двух. Из неравенств (A) и (B) очень легко получить границу для значений t в решениях неравенства $|f(x, y)| \leqslant k$, выше которой могут быть не более двух решений в области (I).

Действительно, положив в неравенствах (A) и (B) $\alpha = \frac{2}{3}$, $\beta = \frac{1}{3}$, получим

$$1 \leqslant c_2^{\nu} \cdot k^{\frac{\nu}{2}+\frac{2}{3}} \cdot \Delta^{\frac{\nu}{4}+\frac{1}{6}} \cdot t^{-\frac{\nu}{2}+1},$$

$$1 \leqslant c_2^{\nu} \cdot k^{\frac{\nu}{2}+\frac{2}{3}} \cdot \Delta^{\frac{\nu}{4}-\frac{1}{6}} \cdot t^{-\frac{\nu}{2}+1}.$$

Заменим их одним более грубым неравенством

$$1 \leqslant c_2^{\nu} \cdot (k\sqrt{\Delta})^{\frac{\nu}{2}+\frac{2}{3}} \cdot t^{-\frac{\nu}{2}+1}.$$

Оно, очевидно, невозможно при $\nu \geqslant 3$ и

$$t > c_2^6 (k\sqrt{\Delta})^{\frac{13}{3}}.$$

Пусть существует решение, для которого $t > c_2^6 (k\sqrt{\Delta})^{\frac{13}{3}}$. Тогда, если только существует решение, для которого $t_1 > t$, должно иметь место

$$t < t_1 < t^8.$$

Но в интервале $t < t_1 < t^8$ может находиться не более одного решения, если только t достаточно велико. Действительно, пусть существуют два t_1 и t_2. Тогда в силу неравенства (4)

$$t_2 > \frac{\sqrt{\Delta}}{9k^2} t^4 \geqslant t^3, \quad \text{если только } t > \frac{\sqrt{\Delta}}{9k^2}.$$

Итак, при $t > \frac{9k^2}{\sqrt{\Delta}}$ и $t > c_2^6 (k\sqrt{\Delta})^{\frac{13}{3}}$ может быть не более двух решений в области (I), что и требовалось доказать.

ГЛАВА VI

О НЕОПРЕДЕЛЕННЫХ УРАВНЕНИЯХ 3-Й СТЕПЕНИ С ДВУМЯ НЕИЗВЕСТНЫМИ

А. РЕШЕНИЕ В ЦЕЛЫХ ЧИСЛАХ

Некоторые важные задачи теории кубических иррациональностей эквивалентны задаче о решении в целых рациональных числах неопределенного уравнения 3-й степени вида $f(X, Y) = \sigma$, где f — заданная кубическая двойничная форма с целыми рациональными коэффициентами a, b, c, d, а σ — заданное целое рациональное число. К решению такого неопределенного уравнения, например, сводится вопрос о том, имеется ли в данном кольце целых кубических чисел степенной базис, в частности, имеет ли данное кубическое поле степенной базис. На такое же уравнение сводится связанный с предыдущим вопрос о том, имеются ли целые кубические уравнения с заданным дискриминантом и т. д., но и некоторые замечательные задачи элементарной теории чисел также эквивалентны задаче о решении такого уравнения. Такова, например, задача о распределении квадратов и кубов в натуральном ряду чисел. Вопрос идет о следующем: если задать некоторое положительное целое рациональное число k, то имеются ли в ряду квадратов и кубов целых рациональных чисел сколь угодно далеко такие числа, разность между которыми не больше k, или же можно указать в натуральном ряду такое место, что для всех квадратов и кубов, следующих за этим местом, разность между ними уже больше k. Теория неопределенных уравнений 3-й степени показывает, что верно последнее, причем оказывается, что число таких квадратов и кубов, разность между которыми не больше заданной величины k, может быть ограничено в зависимости от k. Любопытно, однако, что все до сих пор известное не дает еще возможности найти сами все такие квадраты и кубы..

Теория неопределенных уравнений $f(X, Y) = \sigma$ третьей степени с двумя неизвестными, т. е. теория кубических двойничных форм пока еще весьма несовершенна. Действительно, до сих пор полностью не решен еще даже вопрос о представлении чисел такими формами. Правда, замечательная теорема, данная Туэ, показывает, что число таких представлений всегда конечно. Но в смысле тех требований, которые надо предъявлять ко всякой арифметической теории, эта теорема может быть рассматриваема лишь как первый шаг, который ведет к постановке дальнейших вопросов.

Первый вопрос, который представляется, состоит в определении точной верхней границы для числа представлений.

Второй вопрос состоит в нахождении конечного и, если можно, удобного на практике, алгорифма, который в каждом данном случае давал бы возможность либо найти все представления, если они есть, либо показать, что представлений нет, если их не существует.

Первый вопрос вполне решен в работе Б. Делоне „О числе представлений числа кубической двойничной формой отрицательного определения“ (Изв. АН за 1922 г.) по крайней мере для случая, когда определитель формы отрицателен. Что касается второго вопроса, то и он для этого же случая практически также решен Б. Делоне в работе „Über den allgemeinen Algorithmus der

Erhöhung" (Журн. Ленинградского матем. об-ва за 1927 г.), где дается алгорифм, который пока во всех частных примерах либо давал все решения, либо показывал, что их нет. Однако теория этого алгорифма не закончена, так как нельзя с уверенностью утверждать, что он оборвется всегда, как он обрывался во всех пока рассмотренных, хотя и многочисленных, примерах. Некоторые специальные типы уравнений $f(X, Y)=\sigma$ были окончательно решены Б. Делоне, Т. Нагелем и Д. Фаддеевым.

Мы рассмотрим в настоящей главе все, что до сих пор получено относительно представления чисел формой $f(X, Y)$, т. е. о решениии в целых числах неопределенных уравнений 3-й степени вида:

$$aX^3+bX^2Y+cXY^2+dY^3=\sigma.$$

§ 71. Решение неопределенного уравнения $aX^3+Y^3=1$

1. Сведение задачи на разыскание двухчленных единиц. Мы будем предполагать число a положительным целым рациональным числом и неполным кубом и будем искать решения уравнения

$$aX^3+Y^3=1 \tag{1}$$

в целых рациональных числах X, Y. Всегда имеющееся решение $X=0$, $Y=1$ мы будем называть тривиальным.

Из тождества

$$aX^3+Y^3=(X\sqrt[3]{a}+Y)(X\zeta\sqrt[3]{a}+Y)(X\zeta^2\sqrt[3]{a}+Y) \quad \left(\text{где } \zeta=e^{\frac{2\pi i}{3}}\right)$$

мы видим, что каждому решению X, Y уравнения (1) соответствует некоторая положительная (т. е. норма которой $+1$) алгебраическая единица вида $X\sqrt[3]{a}+Y$ с целыми рациональными X, Y и что, наоборот, всякой такой единице соответствует решение уравнения (1). Мы будем дальше рассматривать положительные единицы вида $A(\sqrt[3]{a})^2+B\sqrt[3]{a}+C$, где A, B, C — целые рациональные числа, т. е. положительные единицы кольца $[(\sqrt[3]{a})^2, \sqrt[3]{a}, 1]$ со степенным базисом $(\sqrt[3]{a})^2$, $\sqrt[3]{a}$, 1. Мы будем для краткости это кольцо обозначать через $O\sqrt[3]{a}$. Те из таких единиц, которые имеют вид $B\sqrt[3]{a}+C$, т. е. не содержат члена с $(\sqrt[3]{a})^2$, мы будем называть двухчленными. Задача о решении уравнения (1) сводится таким образом к разыскиванию всех двухчленных единиц в кольце $O(\sqrt[3]{a})$.

2. О единицах в кольце $O\sqrt[3]{a}$. Уравнение $X^3=a$ имеет один вещественный корень и два комплексно сопряженных. Все единицы кольца $O\sqrt[3]{a}$ получатся, следовательно, от возвышения в степени со всевозможными целыми рациональными показателями некоторой одной, так называемой основной, единицы этого кольца. Если ε — какая-угодно единица, отличающаяся от ± 1, то $\varepsilon, -\varepsilon, \frac{1}{\varepsilon}, -\frac{1}{\varepsilon}$ — также единицы, причем из этих 4 единиц, очевидно, одна и только одна больше нуля и меньше 1, ее мы будем называть положительной прямой единицей, а ей обратную — положительной обратной единицей. Из 4 единиц, так связанных с основной единицей кольца $O(\sqrt[3]{a})$, мы будем обозначать через ε_0 ту, которая удовлетворяет неравенствам $0<\varepsilon_0<1$, и будем ее называть положительной прямой основной единицей, и ей обратную $\eta_0=\varepsilon_0^{-1}$ — положительной обратной основной единицей кольца $O\sqrt[3]{a}$. Все положительные прямые единицы кольца $O\sqrt[3]{a}$ суть, очевидно, степени с целыми положительными

показателями m этой прямой основной единицы ε_0, а положительные обратные — такие же степени обратной основной единицы η_0. Задача решения уравнения (1) сводится, таким образом, к разысканию всех тех целых положительных показателей m, при которых либо ε_0^m, либо η_0^m двухчленна.

3. О степени обратной положительной основной единицы η_0.

Теорема I. *Коэффициенты любой обратной единицы все три положительны.*

Эта теорема очевидна геометрически, так как плоскости, построенные на векторах $\overrightarrow{01}$, $\overrightarrow{0\sqrt[3]{a}}$, $\overrightarrow{0(\sqrt[3]{a})^2}$, как легко видеть, имеют высшие точки своих пересечений с поверхностью $(x^2+y^2)z=1$ на высоте $z=\sqrt[3]{4}$. Но на высоте между $z=1$ и $z=\sqrt[3]{4}$ лежат на поверхности $(x^2+y^2)z=1$ только две точки, принадлежащие кубическим неприводимым максимальным решеткам O, а именно, точки, принадлежащие решеткам с дискриминантами -23 и -31, решетки же $O\sqrt[3]{a}$ имеют дискриминанты <-108, и, следовательно, все точки $O\sqrt[3]{a}$, лежащие на верхней части поверхности $(x^2+y^2)z=1$ (т. е. при $z>1$), т. е. все обратные единицы, лежат в чисто положительном триэдре трехвекторника $\overrightarrow{01}$, $\overrightarrow{0\sqrt[3]{a}}$, $\overrightarrow{0(\sqrt[3]{a})^2}$. Таким образом, если $A(\sqrt[3]{a})^2+B\sqrt[3]{a}+C$ — прямая единица кольца $O\sqrt[3]{a}$, то все три коэффициента

$$A'=B^2-AC;\quad B'=A^2a-BC;\quad C'=C^2-ABa \tag{2}$$

обратной единицы положительны.

Из этой леммы следует, что двухчленные единицы надо искать только среди степеней прямой основной единицы.

4. О степенях единицы, имеющих вид $B\sqrt[3]{a}+C$ или $A(\sqrt[3]{a})^2+C$.

Теорема II. *Никакая степень с целым положительным показателем единицы, вида $B\sqrt[3]{a}+C$ или вида $A(\sqrt[3]{a})^2+C$ не может быть двухчленной.*

Нам надо показать, что при возвышении в степени с целыми положительными показателями m единиц вида $B\sqrt[3]{a}+C$ или $A(\sqrt[3]{a})^2+C$ получаются единицы вида $M(\sqrt[3]{a})^2+P\sqrt[3]{a}+Q$, у которых $M\neq 0$. Действительно, если бы $(B\sqrt[3]{a}+C)^m$ или $(A(\sqrt[3]{a})^2+C)^m$ давало $M=0$, то мы имели бы одно из следующих равенств:

для $(B\sqrt[3]{a}+C)^m$

$$\xi^\lambda+\xi^{\lambda-1}\cdot(C^3)\cdot\frac{m(m-1)(m-2)}{1\cdot2\cdot3}+\ldots+(C^3)^\lambda\cdot\frac{m(m-1)}{1\cdot2}=0,$$

если m вида $m=3\lambda+2$;

$$\xi^{\lambda-1}\cdot\frac{m(m-1)}{1\cdot2}+\xi^{\lambda-2}(C^3)\frac{m(m-1)(m-2)(m-3)(m-4)}{1\cdot2\cdot3\cdot4\cdot5}+\ldots+$$
$$+(C^3)^{\lambda-1}\cdot\frac{m(m-1)}{1\cdot2}=0,$$

если m вида $m=3\lambda+1$;

$$\xi^{\lambda-1}\cdot m+\xi^{\lambda-2}\cdot(C^3)\cdot\frac{m(m-1)(m-2)(m-3)}{1\cdot2\cdot3\cdot4}+\ldots+(C^3)^{\lambda-1}\cdot\frac{m(m-1)}{1\cdot2}=0,$$

если m вида $m=3\lambda$, причем, тут через ξ обозначено B^3a;

для $(A\sqrt[3]{a})^2 + C)^m$

$$\xi^\lambda \cdot m + \xi^{\lambda-1} \cdot (C^3) \cdot \frac{m(m-1)(m-2)(m-3)}{1\cdot 2\cdot 3\cdot 4} + \ldots + (C^3)^\lambda \cdot m = 0,$$

если m вида $m = 3\lambda + 2$;

$$\xi^\lambda + \xi^{\lambda-1} \cdot (C^3) \cdot \frac{m(m-1)(m-2)}{1\cdot 2\cdot 3} + \ldots + (C^3)^\lambda \cdot m = 0,$$

если m вида $m = 3\lambda + 1$;

$$\xi^{\lambda-1} \cdot \frac{m(m-1)}{1\cdot 2} + \xi^{\lambda-2} \cdot (C^3) \cdot \frac{m(m-1)(m-2)(m-3)(m-4)}{1\cdot 2\cdot 3\cdot 4\cdot 5} + \ldots + (C^3)^{\lambda-1} \cdot m = 0,$$

если m вида $m = 3\lambda$, причем тут везде через ξ обозначено A^3a^2.

Но в силу того, что $B\sqrt[3]{a} + C$ и $A(\sqrt[3]{a})^2 + C$ — единицы, мы имеем равенства $B^3a + C^3 = \pm 1$ и $A^3a^2 + C^3 = \pm 1$, из которых мы видим, что B^3a и A^3a^2 взаимно простые с C, т. е. что ξ и C взаимно простые. Если предположить, что $a > 2$, то мы получаем из этих равенств, что $|C| > 1$.

Пусть теперь π — простой делитель C, и пусть в том из этих шести равенств, которое мы рассматриваем, биномиальный коэффициент при высшей степени ξ делится точно на π^x. Удержим в числителе каждого из следующих биномиальных коэффициентов первые два множителя, т. е. $m(m-1)$, а в знаменателе последние два и сократим все остальные множители знаменателя с произведением остальных множителей числителя, что всегда можно сделать, так как для любого $n > 0$ и $0 < k \leqslant n$ число $\frac{n(n-1)(n-2)\ldots(n-k+1)}{1\cdot 2\cdot 3\ldots k}$ целое. Первый член рассматриваемого равенства делится точно на x-ую степень π, а в остальных степень π, которая будет утеряна вследствие возможного содержания π в обоих остальных множителях знаменателя, меньше, чем степень π, которая будет приобретена вследствие того, что C делится на π, так как даже если $\pi = 2$, все же $\pi^3 > 5$, $\pi^6 > 8$, $\pi^9 > 11$ и т. д.; кроме того, целый множитель, получившийся от сокращения указанных множителей знаменателя с указанными множителями числителя, может еще содержать простых делителей π. Все члены равенства, следовательно, делятся по крайней мере на π^{x+1}, а первый член только на π^x; такое равенство, следовательно, невозможно.

В случае $a = 2$ мы имеем $|C| = 1$, и нельзя провести предыдущего рассуждения. Но этот случай относится к уравнению $2x^3 + y^3 = 1$, которое было решено уже Эйлером, показавшим при помощи метода Ферма „de la descente infinie ou indéfinie“, что уравнение это, кроме решений $x = 0$, $y = 1$; $x = 1$, $y = -1$, не имеет никаких других решений не только в целых, но даже и в дробных числах. Теорема, следовательно, верна и для $a = 2$ и, значит, доказана полностью.

5. О квадрате единицы.

Теорема III. *Квадрат иррациональной единицы кольца $O(\sqrt[3]{a})$ не может быть двухчленной единицей.*

Доказательство. Пусть $M(\sqrt[3]{a})^2 + P\sqrt[3]{a} + Q$ единица, и квадрат ее имеет вид $B\sqrt[3]{a} + C$; тогда

$$M^3a^2 + P^3a + Q^3 - 3MPQa = 1 \qquad (3)$$

и

$$P^2 + 2MQ = 0. \qquad (4)$$

Мы покажем, что уравнения (3) и (4) не имеют общих решений в целых рациональных числах M, P, Q, кроме решений $M = P = 0$, $Q = 1$ или

$P=Q=0$, $M=1$, $a=1$, которые нам не подходят, так как тогда либо рассматриваемая единица рациональна, либо a, против предположения, равно 1. Из (4) мы получаем:

1. $Q=\gamma^2$, $M=-2\alpha^2$, $P=\pm 2\alpha\gamma$,

или 2. $Q=-\gamma^2$, $M=2\alpha^2$, $P=\pm 2\alpha\gamma$,

или 3. $Q=2\gamma^2$, $M=-\alpha^2$, $P=\pm 2\alpha\gamma$,

или 4. $Q=-2\gamma^2$, $M=\alpha^2$, $P=\pm 2\alpha\gamma$.

Если мы это подставим в (3), то получим

$$-8t^2\pm 20t\gamma^3+\gamma^6=+1, \tag{5}$$
$$-8t^2\pm 20t\gamma^3+\gamma^6=-1, \tag{6}$$
$$t^2\pm 20t\gamma^3-8\gamma^6=+1, \tag{7}$$
$$t^2\pm 20t\gamma^3-8\gamma^6=-1, \tag{8}$$

если обозначить α^2 через t. Из (5) мы имеем $t=\frac{\pm 5\gamma^3\pm\sqrt{27\gamma^6-2}}{4}$; $27\gamma^6-2$ должно, следовательно, быть квадратом, например z^2, т. е. $z^2+2=\sigma^3$, где $\sigma=3\gamma^2$, или $(z+\sqrt{-2})(z-\sqrt{-2})=\sigma^3$. Множители $z+\sqrt{-2}$ и $z-\sqrt{-2}$ не могут иметь общего делителя, взаимно простого с двойкой. Но σ — нечетное число, и числа $z+\sqrt{-2}$ и $z-\sqrt{-2}$, таким образом, взаимно простые, и следовательно представляют кубы целых алгебраических чисел в $\Omega(\sqrt{-2})$ [в $\Omega(\sqrt{-2})$ все идеалы главные и имеются только две единицы: $+1$ и -1]. Но все числа поля $\Omega(\sqrt{-2})$ имеют вид $u+v\sqrt{-2}$, где u и v — целые рациональные; мы имеем, следовательно,

$$z+\sqrt{-2}=(u+v\sqrt{-2})^3=u^3+3u^2v\sqrt{-2}-6uv^2-2v^3\sqrt{-2}.$$

Отсюда мы получаем $3u^2v-2v^3=v(3u^2-2v^2)=1$, т. е. $v=\pm 1$, и, таким образом, $3u^2-2=\pm 1$, т. е. $u=\pm 1$, и, следовательно, $z=u^3-6uv^2=\pm 5$, откуда получается $\gamma=\pm 1$ и $t=\frac{\pm 20\pm 20}{16}=0$. Если же $t=0$, то и $\alpha=0$, и мы получаем

$$M=0,\ P=0,\ Q=1.$$

Из уравнения (6) следовало бы $\gamma^6\equiv -1 \pmod 4$, что невозможно.

Уравнение (7) можно написать и так:

$$u^2-4\cdot 27\gamma^6=1,$$

если положить $t\pm 10\gamma^3=u$, или так:

$$\frac{u-1}{2}\cdot\frac{u+1}{2}=\sigma,$$

где $\sigma=3\gamma^2$. Число u — нечетное, так как t, как это видно из (7), нечетное; $\frac{u-1}{2}$ и $\frac{u+1}{2}$, следовательно,—два последовательных целых рациональных числа, и они оба, таким образом, должны быть кубами, откуда вытекает, что одно из них равно 0 и $\sigma=0$, т. е. и $\gamma=0$, и мы получаем

$$P=0,\ Q=0,\ M=1,\ a=1.$$

Уравнение (8) дает $t^2\equiv -1 \pmod 4$, что невозможно.

6. О кубе единицы

Теорема IV. *Куб иррациональной единицы кольца $Q(\sqrt[3]{a})$ не может быть двухчленной единицей.*

Доказательство. Пусть $M(\sqrt[3]{a})^2 + P\sqrt[3]{a} + Q$ — единица, т. е.

$$M^3a^2 + P^3a + Q^3 - 3MPQa = 1, \tag{9}$$

и пусть $(M(\sqrt[3]{a})^2 + P\sqrt[3]{a} + Q)^3$ — двухчленная единица, т. е. коэффициент ее при $(\sqrt[3]{a})^2$

$$M^2Pa + P^2Q + MQ^2 = 0. \tag{10}$$

Мы покажем, что уравнения (9) и (10) не имеют других совместных решений в целых рациональных числах M, P, Q, a, кроме решений $M = P = 0$, $Q = 1$ и $M = Q = 0$, $P = 1$, $a = 1$ или $P = Q = 0$, $M = 1$, $a = 1$, которые нам не подходят, так как дают, либо что возводимая в степень единица рациональна, либо что a, против предположения, равно 1.

Пусть δ — общий наибольший делитель M и P; Q, как это видно из (9), взаимно простое с a и δ. Из (10) мы видим, что $M = \delta^2 \cdot m$, $P = \delta \cdot p$, где уже m и p взаимно простые, так как иначе δ не был бы общим наибольшим делителем M и P.

Мы получаем из (10):

$$-m^2\delta^4 p\delta a = Q(p^2\delta^2 + m\delta^2 Q), \quad \text{или} \quad -m^2\delta^3 pa = Q(p^2 + mQ).$$

Но m — взаимно простое с p, а, следовательно, и с $p^2 + mQ$. Мы получаем, таким образом, $Q = m^2q$, или $-m^2\delta^3 pa = m^2q(p^2 + m^3q)$, или $-p\delta^3 a = q(p^2 + m^3q)$. Но q — взаимно простое с δ и a, так как q — делитель Q, и, следовательно, $p = q \cdot s$, или $-qs\delta^3 a = q(q^2s^2 + m^3q)$, или $-s\delta^3 a = q(qs^2 + m^3)$. Но q — взаимно простое с δ и a, и мы имеем, следовательно, $s = qe$, или $-qe\delta^3 a = q(q^3e^2 + m^3)$, или $-e\delta^3 a = q^3e^2 + m^3$. Но e — делитель s, а потому делитель и p, и значит e — взаимно простое с m, откуда получается, что $e = \pm 1$. Мы получаем, таким образом:

$$\mp\delta^3 a = q^3 + m^3, \quad M = m\delta^3, \quad P = \pm q^2\delta, \quad Q = m^2q, \quad MPQ = \pm m^3q^3\delta^3,$$

или, если мы это подставим в (1):

$$m^3\delta^6a^2 \pm q^6\delta^3 a + m^6q^3 \mp 3m^3q^3\delta^3 a = 1.$$

Но мы имеем $\delta = \mp\dfrac{q^3 + m^3}{a}$, т. е. мы получаем

$$m^3(m^3 + q^3)^2 - (m^3 + q^3)q^6 + m^6q^3 + 3m^3q^3(m^3 + q^3) = 1,$$

или, если мы положим $m^2q = \lambda$, $m^3 - q^3 = \mu$, уравнение

$$9\lambda^3 + \mu^3 = 1, \tag{11}$$

т. е. опять уравиеиие нашего же типа, но специально для $a = 9$. Прямая положительная основная единица кольца $Q(\sqrt[3]{9})$ есть $\sqrt[3]{9} - 2$, т. е. она двухчленна. Уравнение (11) имеет поэтому, в силу теорем I и II, только нетривиальное решение $\lambda = 1$, $\mu = -2$ и еще тривиальное решение $\lambda = 0$, $\mu = 1$. Но случай $\lambda = 1$, $\mu = -2$ дает, в силу $m^3 - q^3 = \mu$, $m = -1$, $q = 1$, и, следовательно, $\delta = 0$, т. е. $M = P = 0$, $Q = 1$, а случай $\lambda = 0$, $\mu = 1$ дает либо $m = 0$, $q = -1$, либо $m = 1$, $q = 0$, т. е. дает $M = Q = 0$, $P = 1$, $a = 1$ или $P = Q = 0$, $M = 1$, $a = 1$.

7. Доказательство основной теоремы. Мы сейчас показали, что квадрат и куб единицы ие могут быть решениями; если бы мы хотели это же доказать для пятой степеии, то иадо было бы показать, что нет таких целых рациональных чисел M, P, Q, a, из которых первые два не равны нулю одно-

временно и последнее $a>1$, которые удовлетворяют одновременно уравнениям

$$M^3a^2+P^3a+Q^3-3MPQa=1$$

и

$$5M^4Qa^2+10M^3P^3a^2+30M^2PQ^2a+20MP^2Qa+5MQ^4+P^5a+10P^2Q^3=0.$$

Это уравнения уже довольно сложные, и не видно, как это сделать. Однако, если использовать все доказанные теоремы, то следующий метод ведет к цели даже в случае любой степени единицы и дает полное решение уравнения (1).

Пусть $A(\sqrt[3]{a})^3+B\sqrt[3]{a}+C$ — единица кольца $O(\sqrt[3]{a})$ и $[A(\sqrt[3]{a})^2+B\sqrt[3]{a}+C]^m=M(\sqrt[3]{a})^2+P\sqrt[3]{a}+Q$; тогда легко видеть, что

$$3(\sqrt[3]{a})^2\cdot M=[A(\sqrt[3]{a})^3+B\sqrt[3]{a}+C]^m+\zeta\cdot[A\zeta^2(\sqrt[3]{a})^2+B\zeta\sqrt[3]{a}+C]^m+$$
$$+\zeta^2[A\zeta(\sqrt[3]{a})^2+B\zeta^2\sqrt[3]{a}+C]^m,$$

где ζ, как и раньше, есть $\sqrt[3]{1}=e^{\frac{2\pi i}{3}}$.

Пусть $M=0$. Рассмотрим отдельно случаи $m=3\gamma+2$ и $m=3\gamma+1$. Случая $m=3\gamma$, в силу теоремы IV, нам рассматривать не надо.

Итак, пусть $m=3\gamma+2$ и $M=0$; мы имеем тогда равенство

$$[A\zeta(\sqrt[3]{a})^2+B\sqrt[3]{a}+C\zeta^2]^m+[A\zeta^2(\sqrt[3]{a})^2+B\sqrt[3]{a}+C\zeta]^m=$$
$$=-[A(\sqrt[3]{a})^2+B\sqrt[3]{a}+C]^m.$$

В силу теоремы III можно считать, что m нечетное, в таком случае $[\zeta^2A(\sqrt[3]{a})^2+B\sqrt[3]{a}+\zeta C]+[\zeta A(\sqrt[3]{a})^2+B\sqrt[3]{a}+\zeta^2C]$ делитель $[A(\sqrt[3]{a})^2+B\sqrt[3]{a}+C]^m$, т. е. алгебранческая единица, т. е. $-A(\sqrt[3]{a})^2+2B\sqrt[3]{a}-C$ есть единица, и мы имеем $-A^3a^2+8B^3a-C^3-6ABCa=\pm1$.

С другой же стороны, мы имеем

$$A^3a^2+B^3a+C^3-3ABCa=1,$$

откуда получаем сложением

$$9aB(B^2-AC)=2 \text{ или } 0,$$

т. е. либо $B^2-AC=0$, либо $B=0$; но B^2-AC есть (см. (2)) коэффициент „обратной“ единицы, и, следовательно, он по теореме I не равен нулю, т. е. получается $B=0$, т. е. сама возводимая в степень единица имеет вид $A(\sqrt[3]{a})^2+C$, и никакая ее степень выше 1-й, по теореме II, не может быть двухчленной единицей. Но мы рассматриваем случай $m=3\gamma+2$, т. е. $m>1$, и, следовательно, в этом случае равенство $M=0$ вообще невозможно. Если $m=3\gamma+1$ и $M=0$, то мы имеем

$$[A(\sqrt[3]{a})^2+\zeta B\sqrt[3]{a}+\zeta^2C]^m+[A(\sqrt[3]{a})^2+\zeta^2B\sqrt[3]{a}+\zeta C]^m=$$
$$=-[A(\sqrt[3]{a})^2+B\sqrt[3]{a}+C]^m,$$

откуда, совсем аналогично, получаем, что $2A(\sqrt[3]{a})^2-B\sqrt[3]{a}-C$ — единица, и если мы тогда аналогично сравним равенства

$$8A^3a^2-B^3a-C^3-6ABCa=\pm1 \text{ и } A^3a^2+B^3a+C^3-3ABCa=1,$$

то получим $9aA(A^2a-BC)=2$ или 0. Но тут опять A^2a-BC — коэффициент обратной единицы, который не равен нулю; мы получаем, таким образом, теперь $A=0$; иначе говоря, возводимая в степень единица имеет вид $B\sqrt[3]{a}+C$, т. е. сама двухчленна, и, следовательно, никакая ее степень выше 1-й, по теореме II, не может быть двухчленной единицей. Мы тут рассматри-

ваем случай $m = 3\gamma + 1$; в этом случае равенство $M = 0$ возможно, но, как мы видим, лишь при $m = 1$. Приняв во внимание теорему I, мы получаем, таким образом, что нетривиальным решеннем уравнения (1) может быть только сама положительная прямая основная единица кольца $O(\sqrt[3]{a})$, если она двухчленная. В результате получается следующая основная теорема об уравнении (1), дающая полное его решение:

Теорема V. *Неопределенное уравнение* $aX^3 + Y^3 = 1$, *где* a — *целое рациональное число, которое не есть полный куб, кроме тривиального решения* $X = 0$, $Y = 1$, *всегда имеющегося, может иметь еще одно и только одно нетривиальное решение в целых числах* X, Y; *это нетривиальное решение будет иметься тогда и только тогда, когда положительная прямая основная единица кольца* $O(\sqrt[3]{a})$ — *двухчленная, т. е. она имеет вид* $B_0\sqrt[3]{a} + C_0$, *причем решением этим будет тогда* $X = B_0$, $Y = C_0$.

§ 72. Обобщение метода § 71 на уравнение $I(X, Y) = 27$

Метод, примененный к решению уравнений, рассмотренных в предыдущем параграфе, может быть применен для решения довольно обширного класса неопределенных уравнений третьей степени и даже к некоторым неопределенным уравнениям четвертой степени.

Впервые метод § 71 был обобщен норвежским математиком Нагелем, который решил до конца неопределенные уравнения $aX^3 + bY^3 = c$ при c равном 1 или 3. Дальнейшее обобщение принадлежит Д. К. Фаддееву. Мы не будем рассматривать отдельно уравнения типа Нагеля, они войдут, как частный случай, в более обширный класс уравнений, который мы рассмотрим в следующем параграфе.

Сейчас мы займемся задачей об отыскании единиц кубического поля отрицательного дискриминанта, лежащих на плоскости нулевого следа.

Эта задача равносильна решению неопределенного уравнения

$$I(X, Y) = 27,$$

где $I(X, Y)$ — кубический ковариант индексформы максимального кольца поля.

Действительно, пусть

$$f(X, Y) = aX^3 + bX^2Y + cXY + eY^3$$

— индексформа максимального кольца. За базис этого кольца можно принять $[1, \omega_1, \omega_2]$, где ω_1 и ω_2 суть корни уравнений

$$\omega_1^3 = b\omega_1^2 - ac\omega_1 + a^2e, \quad \omega_2^3 = c\omega_2^2 - be\omega_2 + ae^2.$$

Кубический ковариант

$$I(X, Y) = (27a^2e - 9abc + 2b^3)X^3 + (27abe - 18ac^2 + 3b^2c)X^2Y + \\ + (-27ace + 18b^2e - 3bc^2)XY^2 + (-27ae^2 + 9bce - 2c^3)Y^3$$

может быть представлен в виде

$$N[(3\omega_1 - b)X - (3\omega_2 - c)Y],$$

откуда следует, что каждое решение уравнения $I(X, Y) = 27$ определяет единицу ε максимального кольца, удовлетворяющую соотношению

$$\varepsilon + \varepsilon' + \varepsilon'' = 0,$$

т. е. лежащую на плоскости нулевого следа.

Действительно, если $I(X, Y)=N[(3\omega_1-b)X-(3\omega_2-c)Y]=27$, то $bX+cY$ делится на 3, и целое число

$$\varepsilon=\frac{1}{3}[(3\omega_1-b)X-(3\omega_2-c)Y]$$

является единицей максимального кольца, которая, очевидно, лежит на плоскости нулевого следа.

Обратно, если единица $\varepsilon=Z+X\omega_1-Y\omega_2$ лежит на плоскости нулевого следа, то X, Y, Z удовлетворяют соотношению $3Z+bX-cY=0$, откуда следует, что

$$3\varepsilon=(3\omega_1-b)X-(3\omega_2-c)Y,$$

и, следовательно, X, Y дают решение уравнения

$$I(X, Y)=27.$$

Необходимо заметить, что решение уравнения $I(X, Y)=27$, если $I(X, Y)$ есть кубический ковариант любой кубической двойничной формы (не обязательно индексформы максимального кольца), также приводится к задаче об отыскании единиц на плоскости нулевого следа, по тем же соображениям.

Перейдем к решению задачи.

Попрежнему единицу ε кубического кольца отрицательного дискриминанта с положительной нормой мы будем называть прямой, если $0<\varepsilon<1$, и обратной, если $\varepsilon>1$.

Лемма 1. *За исключением единицы* ε, *заданной уравнением* $\varepsilon^3=\varepsilon+1$, *не существует обратных единиц, лежащих на плоскости нулевого следа.*

Доказательство. Каждая единица, лежащая на плоскости нулевого следа, является корнем уравнения

$$\varepsilon^3=-q\varepsilon+1.$$

Это уравнение имеет отрицательный дискриминант при $q\geqslant -1$. При $q=-1$ ε будет обратной единицей, при $q=0$ уравнение приводимо и, наконец, при $q\geqslant 1$ ε будет прямой единицей, так как $\varphi(0)=-1$, $\varphi(1)=q$, где $\varphi(z)=z^3+qz-1$, имеют разные знаки, и, следовательно, корень ε уравнения $\varphi(z)=0$ лежит между 0 и 1. Лемма доказана.

Лемма 2. *Единица, являющаяся кубом другой единицы, не может лежать на плоскости нулевого следа.*

Доказательство. Пусть $\varepsilon=\eta^3$, и η является корнем уравнения $\eta^3=s\eta^2-q\eta+1$. Тогда $\varepsilon+\varepsilon'+\varepsilon''=s^3-3sq+3$. Очевидно, что целое рациональное число $\varepsilon+\varepsilon'+\varepsilon''=s^3-3sq+3$ не может делиться на 9 и, следовательно, не может равняться нулю. Лемма доказана.

Лемма 3. *Единица, являющаяся четвертой степенью другой единицы, не может находиться на плоскости нулевого следа, за единственным исключением единицы* ε, *заданной уравнением* $\varepsilon^3=-1040\varepsilon+1$, *которая равна* η^4, *где* $\eta^3=2\eta^2-6\eta+1$.

Доказательство. Пусть $\varepsilon=\eta^4$, η *удовлетворяет уравнению* $\eta^3=s\eta^2-q\eta+1$. *Тогда*

$$\varepsilon+\varepsilon'+\varepsilon''=s^4-4s^2q+4s+2q^2.$$

Если ε лежит на плоскости нулевого следа, то

$$s^4-4s^2q+4s+2q^2=0.$$

Из этого равенства следует, что s и q должны делиться на 2. Положив $s=2s_1$, $q=2q_1$, получим

$$2s_1^4-4s_1^2q+s_1+q_1^2=0,$$

откуда

$$q_1 = 2s_1^2 \pm \sqrt{2s_1^4 - s_1}.$$

Для того чтобы последнее равенство было возможно, необходимо, чтобы $s_1(2s_1^3 - 1)$ было полным квадратом и, следовательно, чтобы $2s_1^3 - 1 = \pm v^2$.

Легко видеть, что уравнение $2s_1^3 - 1 = v^2$ имеет единственное решение $s_1 = 1$, которому соответствует $q_1 = 1$ или $q_1 = 3$. Уравнение $2s_1^3 - 1 = -v^2$ имеет единственное решение $s_1 = 0$, которому соответствует $q_1 = 0$.

Итак, если $\varepsilon = \eta^4$ лежит на плоскости нулевого следа, то η должно удовлетворять одному из уравнений

$$\eta^3 = 2\eta^2 - 6\eta + 1, \quad \eta^3 = 2\eta^2 - 2\eta + 1.$$

Второе уравнение приводимо, первое дает единственное исключение, оговоренное в условии леммы. Лемма доказана.

Лемма 4. *Положительная степень числа, лежащего на плоскости нулевого следа, не может находиться на плоскости нулевого следа, за исключениями степеней чисел, заданных уравнениями:*

$$\eta^3 = -\eta + 1; \quad \eta^3 = -6\eta + 12; \quad \eta^3 = -4\eta + 4;$$
$$\eta^3 = -30\eta + 60; \quad \eta^3 = -2\eta + 2; \quad \eta^3 = -3\eta + 9;$$
$$\eta^3 = -3\eta + 3; \quad \eta^3 = -5\eta + 5; \quad \eta^3 = -30\eta + 30.$$

Доказательство. Пусть η — число плоскости нулевого следа, и $\eta^3 = -q\eta + n$ — уравнение, корнем которого является η.

Обозначим $\eta^m + \eta'^m + \eta''^m$ через s_m. По известной формуле Варинга для степенных сумм, s_m представляется в виде

$$s_m = \sum_{2\alpha + 3\beta = m} \frac{m}{(\alpha + \beta)} \cdot \frac{(\alpha + \beta)!}{\alpha!\beta!} (-q)^\alpha n^\beta.$$

Суммирование распространено на все целые неотрицательные α, β, для которых

$$2\alpha + 3\beta = m.$$

Выпишем s_m, расположив правую часть по возрастающим степеням n. При этом нам придется отдельно рассмотреть случаи четного и нечетного m. В первом случае положим $m = 2l$, во втором $m = 2l + 3$. Получим

$$s_{2l} = \sum_{s=0}^{\left[\frac{l}{3}\right]} \frac{2l}{l-s} \cdot \frac{(l-s)!}{(2s)!\,(l-3s)!} (-q)^{l-3s} n^{2s} =$$
$$= 2 \cdot (-q)^l + \frac{2l\,(l-2)}{1 \cdot 2} (-q)^{l-3} \cdot n^2 +$$
$$+ \frac{2l\,(l-3)\,(l-4)\,(l-5)}{1 \cdot 2 \cdot 3 \cdot 4} (-q)^{l-6} \cdot n^4 + \ldots$$

$$s_{2l+3} = \sum_{s=0}^{\left[\frac{l}{3}\right]} \frac{2l+3}{l-s+1} \cdot \frac{(l-s+1)!}{(2s+1)!\,(l-3s)!} (-q)^{l-3s} \cdot n^{2s+1} =$$
$$= \frac{2l+3}{1} (-q)^l n + \frac{(2l+3)\,(l-1)\,(l-2)}{1 \cdot 2 \cdot 3} (-q)^{l-3} \cdot n^3 + \ldots$$

Приравняем s_m нулю, введя обозначения $q^3 = q_1\delta$, $n^2 = n_1\delta$, где δ — общий наибольший делитель чисел q^3 и n^2.

После очевидных сокращений получим:

$$2q_1^{l_1} - \frac{2l(l-2)}{1\cdot 2} q_1^{l_1-1} n_1 + \frac{2l(l-3)(l-4)(l-5)}{1\cdot 2\cdot 3\cdot 4} q_1^{l_1-2} n_1^2 - \ldots = 0 \qquad (\alpha)$$

$$\left(\text{при } m = 2l; \qquad l_1 = \left[\frac{l}{3}\right]\right)$$

$$\frac{2l+3}{1} q_1^{l_1} - \frac{(2l+3)(l-1)(l-2)}{1\cdot 2\cdot 3} q_1^{l_1-1} n_1 + \ldots = 0 \qquad (\beta)$$

$$\left(\text{при } m = 2l+3; \quad l_1 = \left[\frac{l}{3}\right]\right)$$

Равенство (α), очевидно, невозможно при n_1, отличном от 1 и 2, так как при выполнении этого равенства n_1 должно быть делителем $2q_1^{l_1}$, а q_1 и n_1 взаимно просты. Далее, при $n_1 = 2$ равенство (α) невозможно при четном l, так как в этом случае все слагаемые левой части, кроме первого, делятся на 4, а первое не делится на 4. Если же l нечетное, то все слагаемые, начиная с третьего, делятся на 8. Положив $n_1 = 2$, придем к сравненню

$$2q_1^{l_1-1}[q_1 + 1 - (l-1)^2] \equiv 0 \pmod 8,$$

откуда $q_1 \equiv 3 \pmod 4$.

Итак, равенство (α) возможно только при $n_1 = 1$ и при $n_1 = 2$. Во втором случае должно быть $q_1 \equiv 3 \pmod 4$.

Обратимся теперь к исследованию равеиства (β).

Оно, очевидно, невозможно при четном n_1, так как n_1 должно быть делителем $2l+3$. Оно невозможно также при n_1, делящемся на любое простое число большее 3, и при n_1, делящемся на 3^2, так как в этих случаях первое слагаемое делится на меньшую степень рассматриваемого простого числа, чем все остальные слагаемые. В этом легко убедиться простым подсчетом.

Следовательно, равеиство (β) возможно только при $n_1 = 1$ и $n_1 = 3$, причем последний случай возможен только при $m = 2l+3$, делящемся на 3.

Расположим теперь s_m по возрастающим степеням q. При этом нам придется различать три случая, в зависнмости от класса по модулю 3, которому принадлежит m. Для этих трех случаев будем писать m в виде $3k$, $3k+2$, $3k+4$.

$$s_{3k} = \sum_{s=0}^{\left[\frac{k}{2}\right]} \frac{3k}{k+s} \cdot \frac{(k+s)!}{(3s)!\,(k-2s)!} (-q)^{3s} \cdot n^{k-2s} = 3n^k - \frac{3k\cdot k(k-1)}{1\cdot 2\cdot 3} q^3 n^{k-2} + \\ + \frac{3k(k+1)k(k-1)(k-2)(k-3)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} q^6 n^{k-4} - \ldots$$

$$s_{3k+2} = \sum_{s=0}^{\left[\frac{k}{2}\right]} \frac{3k+2}{k+s+1} \cdot \frac{(k+s+1)!}{(3s+1)!\,(k-2s)!} (-q)^{3s+1} \cdot n^{k-2s} = -\frac{3k+2}{1} qn^k + \\ + \frac{(3k+2)(k+1)k(k-1)}{1\cdot 2\cdot 3\cdot 4} q^4 n^{k-2} - \ldots$$

$$s_{3k+4} = \sum_{s=0}^{\left[\frac{k}{2}\right]} \frac{3k+4}{k+s+2} \cdot \frac{(k+s+2)!}{(3s+2)!\,(k-2s)!} (-q)^{3s+2} \cdot n^{k-2s} = \frac{(3k+4)(k+1)}{1\cdot 2} q^2 n^k - \\ - \frac{(3k+4)(k+2)(k+1)k(k-1)}{1\cdot 2\cdot 3\cdot 4\cdot 5} q^5 n^{k-2} + \ldots$$

Приравняем s_m нулю, введя прежние обозначения:

$$q_1 = \frac{q^3}{\delta}, \quad n_1 = \frac{n^2}{\delta}, \quad \delta = (q^3, n^2).$$

После сокращений придем к равенствам

$$3n_1^{k_1} - \frac{3k \cdot k(k-1)}{1 \cdot 2 \cdot 3} n_1^{k_1-1} q_1 + \\ + \frac{3k(k+1) \cdot k(k-1)(k-2)(k-3)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} n^{k_1-2} q_1^2 - \ldots = 0 \qquad (\gamma)$$

$$\left(\text{при } m = 3k, \qquad k_1 = \left[\frac{k}{2}\right]\right),$$

$$\frac{3k+2}{1} n_1^{k_1} - \frac{(3k+2)(k+1)k(k-1)}{1 \cdot 2 \cdot 3 \cdot 4} n_1^{k_1-1} q_1 + \ldots = 0 \qquad (\delta)$$

$$\left(\text{при } m = 3k+2, \; k_1 = \left[\frac{k}{2}\right]\right),$$

$$\frac{(3k+4)(k+1)}{1 \cdot 2} n_1^{k_1} - \frac{(3k+4)(k+2)(k+1)k(k-1)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} n_1^{k_1-1} q_1 + \ldots = 0 \qquad (\varepsilon)$$

Заметим, что в равенстве (γ) n_1 может равняться 1, 2, 3, а в равенствах (δ) и (ε) n_1 может равняться только 1 и 2.

Равенство (γ), очевидно, невозможно при q_1, отличном от 1 и 3.

Равенство (δ) возможно только при $q_1 = 1$, 2 и 4, так как в случае, если q_1 делится на простое число $p \geqslant 3$ или на 2^3, то все слагаемые левой части, кроме первого, делятся на более высокую степень простого числа p (или 2), чем первое слагаемое.

Пусть в равенстве (δ) $q_1 = 4$. Тогда n_1 может быть равно только 1. Легко видеть, что все слагаемые левой части равенства (δ), начиная с третьего, делятся в этом случае на 16. Следовательно, должно иметь место сравненне

$$3k + 2 - \frac{(3k+2)(k+1)k(k-1)}{6} \equiv 0 \pmod{16}.$$

Это возможно только при четном k. Положив $k = 2k_1$, получим

$$9k_1 + 3 - (3k_1 + 1)k_1(4k_1^2 - 1) \equiv 0 \pmod 8.$$

Это сравнение, в свою очередь, возможно только при нечетном k_1. В этом случае $4k_1^2 \equiv 4 \pmod 8$, и последнее сравнение равносильно сравнению

$$(3k_1 + 1)(1 - k_1) \equiv 0 \pmod 8,$$

откуда $k_1 = 1 \pmod 4$ и $m = 6k_1 + 2 \equiv 0 \pmod 8$.

Равенство (ε) невозможно при q_1, делящемся на простое число $p > 5$, и при q_1, делящемся на 3^2, 2^2 и 5^2, так как при этом первое слагаемое делится на меньшую степень этого простого числа, чем все остальные.

Положив $q_1 = 3n$ и соединив первые два слагаемые, придем к заключению, что равенство (ε) возможно только при $n_1 \equiv n \pmod 3$. Наконец, положив $q_1 = 5n$ и соединив первые два слагаемые, придем к заключению, что равенство (ε) возможно при $n_1 \equiv n \pmod 5$, $m \equiv 1 \pmod 5$ и при $n_1 \equiv -n \pmod 5$, $m \equiv 0 \pmod 5$.

Соединяя все вместе, получим, что s_m может равняться нулю только при следующих значениях n_1, q_1 и m:

n_1	3	2	2	1	1	1	1	1	1
q_1	1	3	15	4	2	3	5	30	1
m	$\equiv 0(3)$	$\equiv 0(6)$	$\equiv 0(10)$	$\equiv 0(8)$					

Эти случаи как раз и были упомянуты в качестве исключений в условии леммы.

Замечание. Для комбинаций $n_1 = 2$, $q_1 = 3$ m должно делиться на 6. Однако уже $s_6 = 0$, и уравнение, которому удовлетворяет η^6, где $\eta^3 = -6n + 12$, не находится в числе исключений. Следовательно, среди степеней числа η на плоскости нулевого следа находится только η^6. Подобным образом среди степеней чисел, заданных уравнениями

$$\eta^3 = -30\eta + 60 \quad (n_1 = 2, q_1 = 15), \quad \eta^3 = -4\eta + 4 \quad (n_1 = 1, q_1 = 4)$$

на плоскости нулевого следа находятся только η^{10} (для первого уравнения) и η^8 (для второго). Более тонкое исследование равенства (3) показывает, что при $n_1 = 3$, $q_1 = 1$, m должно делиться на 9. Но η^9, где $\eta^3 = -3\eta + 9$, находится на плоскости нулевого следа; следовательно, кроме η^9, не существует степеней η, лежащих на плоскости нулевого следа.

Исследование остальных пяти исключений сводится, как мы увидим в следующем параграфе, к решению некоторых совершенно конкретных неопределенных уравнений, которые могут быть решены методом алгорифма повышения, который будет рассмотрен в § 75. Это исследование дает, что на плоскости нулевого следа лежат η^{11} для $n_1 = q_1 = 1$ и η^{13} для $n_1 = 1$, $q_1 = 2$.

Таким образом, мы имеем окончательно только шесть исключений. На плоскости нулевого следа лежат

η^6, где $\eta^3 = -6\eta + 12$; η^8, где $\eta^3 = -4\eta + 4$; η^{10}, где $\eta^3 = -30\eta + 6$;
η^9, где $\eta^3 = -3\eta + 9$; η^{11}, где $\eta^3 = -\eta + 1$; η^{13}, где $\eta^3 = -2\eta + 2$.

В этом параграфе лемма 4 будет нужна только для единиц, т. е. для $n = 1$. В следующем она нам будет нужна для $n_1 = 1$. Мы дали лемму в более общей формулировке, так как она представляет некоторый интерес сама по себе.

Теорема. *На плоскости нулевого следа может находиться только прямая основная единица области или ее квадрат, за исключениями:*

$$\begin{aligned} &\varepsilon_0^{-1}, \text{ где } \varepsilon_0^3 = -\varepsilon_0^2 + 1, \\ &\varepsilon_0^4, \text{ где } \varepsilon_0^3 = 2\varepsilon_0^2 - 6\varepsilon_0 + 1, \\ &\varepsilon_0^{11}, \text{ где } \varepsilon_0^3 = -\varepsilon_0 + 1. \end{aligned}$$

Доказательство. Пусть ε_0 — прямая основная единица области, и пусть $\varepsilon = \varepsilon_0^m$ лежит на плоскости нулевого следа

$$\varepsilon_0^m + \varepsilon_0'^m + \varepsilon_0''^m = 0.$$

m не может быть отрицательным, за одним единственным исключением в силу леммы 1, и в силу леммы 3 не может делиться на 4, за одним единственным исключением. Пусть m делится на нечетное простое число p. Обозначим $\varepsilon_0^{\frac{m}{p}} = \eta$. Тогда

$$\eta^p + \eta'^p + \eta''^p = 0.$$

Из этого соотношения следует, что число $\eta' + \eta''$ представляет собой единицу. Пусть $\eta^3 = s\eta^2 - q\eta + 1$ — уравнение, корнем которого является η. Из того, что $\eta' + \eta''$ — единица, следует что $N(\eta' + \eta'') = N(s - \eta) = qs - 1 = \pm 1$. Следовательно, или $qs = 2$ или $qs = 0$.

Равенство $qs = 2$ приводит к четырем уравнениям для η, из которых только одно $\eta^3 = \eta^2 - 2\eta + 1$ имеет отрицательный дискриминант и имеет вещественный корень между 0 и 1.

Если же $qs = 0$, то или $q = 0$, или $s = 0$.

Если $s = 0$, то, в силу леммы 4, $q = 1$ и $p = 11$.

Если $q = 0$, то η — прямая единица только при $s = -1$.

Этот случай нужно исследовать отдельно.

Оба исключения, нуждающиеся в дополнительных исследованиях, приводятся к отысканию единиц на плоскости нулевого следа в области, с дискриминантом равным -23.

Соответствующее неопределенное уравнение

$$x^3+2x^2y+9xy^2+25y^3=1$$

имеет единственное решение $x=1$, $y=0$, в чем можно убедиться посредством „алгорифма повышения". Этому решению соответствует единственная единица этой области η^{-1}, где $\eta^3=-\eta^2+1$, лежащая на плоскости нулевого следа. Тем самым теорема доказана полностью.

Из доказанной теоремы непосредственно следует, что для того чтобы решить уравнение $I(x,y)=27$, нужно найти основную прямую единицу ε_0 области, которой принадлежат корни формы

$$f(x,y)=ax^3+bx^2y+cxy^2+ey^3.$$

Затем, если эта единица или ее квадрат лежит на плоскости нулевого следа и принадлежит кольцу, порожденному корнями формы $f(x,y)$, то $I(x,y)=27$ имеет единственное решение (за исключением $D=-31$), которое находится посредством представления 3ε, где ε — единица плоскости нулевого следа, в виде $(3\omega_1-b)x-(3\omega_2-c)y$.

В противном случае (за двумя исключениями) уравнение $I(x,y)=27$ не имеет решений.

§ 73. Дальнейшее обобщение метода § 71

Решим теперь тем же методом еще более широкий класс неопределенных уравнений. Определению этого класса мы должны предпослать одну лемму, касающуюся самого общего неопределенного уравнения третьей степени вида $f(x,y)=1$, где $f(x,y)$ — кубическая форма.

Лемма 1. *Для того чтобы уравнение $f(x,y)=1$ имело решение, необходимо (но не достаточно), чтобы форма $f(x,y)$ была примитивна (т. е. чтобы коэффициенты формы не имели общего делителя, отличного от 1) и представлялась в виде нормы линейной функции с коэффициентами из кольца, заданного формой* (доказательство см. пункт 1, § 76).

Заметим, между прочим, что для представления формы $f(x,y)$ в виде нормы линейной функции с коэффициентами из кольца O, соответствующего форме $f(x,y)$, необходимо и достаточно, чтобы $O^*=O$, где O^* — решетка, полярная решетке, изображающей кольцо O.

Итак, среди уравнений $f(x,y)=1$ есть смысл рассматривать только те, для которых $f(x,y)=N(\lambda x+\mu y)$, где λ, μ — числа, принадлежащие кольцу, соответствующему форме $f(x,y)$. Решение таких уравнений равносильно отысканию единиц кольца, имеющих вид $\lambda x+\mu y$. В геометрической трактовке решение уравнения $f(x,y)$ равносильно отысканию единиц на плоскости $\lambda x+\mu y$, проходящей через начало координат.

Пусть $\varepsilon=\lambda x+\mu y$ — единица, дающая решение уравнения $f(x,y)=1$. Введем в рассмотрение сопряженные числа $\varepsilon'=\lambda' x+\mu' y$, $\varepsilon''=\lambda'' x+\mu'' y$. Между единицами ε, ε', ε'', очевидно, выполняется соотношение

$$\varphi\cdot\varepsilon+\varphi'\cdot\varepsilon'+\varphi''\cdot\varepsilon''=0,$$

где $\varphi=\lambda'\mu''-\lambda''\mu'$; $\varphi'=\lambda''\mu-\lambda\mu''$; $\varphi''=\lambda\mu'-\lambda'\mu$.

Числа φ, φ', φ'' зависят только от вида уравнения $f(x,y)$, но не от выбранного решения.

Мы дадим решение уравнения $f(x,y)=1$, для которых числа φ, φ', φ'' ассоциированны, т. е. отличаются множителями, которые суть единицы, и форма $f(x,y)$ имеет отрицательный дискриминант.

Для выяснения вопроса о том, какие уравнения могут быть причислены к рассматриваемому классу, докажем следующую лемму.

Лемма 2. *Если* $f(x, y)=N(\lambda x+\mu y)$ *примитивна и разлагается на множители с целыми алгебраическими коэффициентами (сколь угодно высокого порядка)*

$$f(x, y)=(\alpha_1 x+\beta_1 y)(\alpha_2 x+\beta_2 y)(\alpha_3 x+\beta_3 y)$$

так, что числа $\alpha_1\beta_2-\alpha_2\beta_1$, $\alpha_2\beta_3-\alpha_3\beta_2$, $\alpha_3\beta_1-\alpha_1\beta_3$ *ассоциированы, то числа* φ, φ', φ'' *также ассоциированы.*

Доказательство. Сопоставим два разложения формы $f(x, y)$ на множители: $f(x, y)=(\lambda x+\mu y)(\lambda' x+\mu' y)(\lambda'' x+\mu'' y)=(\alpha_1 x+\beta_1 y)(\alpha_2 x+\beta_2 y)(\alpha_3 x+\beta_3 y)$. Эти два разложения могут отличаться одно от другого только постоянными множителями. Следовательно,

$$\lambda=\varepsilon_1\alpha_1;\quad \lambda'=\varepsilon_2\alpha_2;\quad \lambda''=\varepsilon_3\alpha_3;$$
$$\mu=\varepsilon_1\beta_1;\quad \mu'=\varepsilon_2\beta_2;\quad \mu''=\varepsilon_3\beta_3.$$

Форма $f(x, y)$ примитивна. Следовательно, числа α_1, β_1 взаимно просты, и можно подобрать такие целые алгебраические числа γ, δ, что $\alpha_1\gamma+\beta_1\delta=1$.

Следовательно, $\varepsilon_1=\lambda\gamma+\mu\delta$ представляет собою целое алгебраическое число, как результат действий сложения и умножения над целыми числами. Из тех же соображений докажем, что $\frac{1}{\varepsilon_1}$, ε_2, $\frac{1}{\varepsilon_2}$, ε_3, $\frac{1}{\varepsilon_3}$ суть целые алгебраические числа, и, следовательно, ε_1, ε_2, ε_3 — единицы.

Числа φ, φ', φ'' лишь множителями $\varepsilon_2\varepsilon_3$, $\varepsilon_3\varepsilon_1$, $\varepsilon_1\varepsilon_2$, представляющими собой единицы, отличаются от чисел $\alpha_2\beta_2-\alpha_3\beta_2$, $\alpha_3\beta_1-\alpha_1\beta_3$, $\alpha_1\beta_2-\alpha_2\beta_1$. Следовательно, если эти последние ассоциированы, то и φ, φ', φ'' ассоциированы,— что и требовалось доказать.

Теперь мы легко покажем, что к рассматриваемому нами классу неопределенных уравнений относятся уравнения вида $ax^3+by^3=1$. Действительно,

$$ax^3+by^3=(x\sqrt[3]{a}+y\sqrt[3]{b})(x\sqrt[3]{a}+y\sqrt[3]{b}\,\zeta)(x\sqrt[3]{a}+y\sqrt[3]{b}\,\zeta^2),$$

где $\zeta=e^{\frac{2\pi i}{3}}$. Определители $\alpha_2\beta_3-\alpha_3\beta_2$, $\alpha_3\beta_1-\alpha_1\beta_3$, $\alpha_1\beta_2-\alpha_2\beta_1$ равны соответственно $\sqrt[3]{ab}\,(\zeta^2-\zeta)$, $\sqrt[3]{ab}\,(1-\zeta^2)$, $\sqrt[3]{ab}\,(\zeta-1)$ и, очевидно, ассоциированы.

Подобным же образом убедимся в том, что уравнения $ax^3+by^3=3$ [при $a\not\equiv\pm b \pmod 9$] и $I(x, y)=27$ приводятся к уравнениям того же типа. Уравнения $ax^3+y^3=1$, являясь частным случаем уравнений $ax^3+by^3=1$, также относятся к рассматриваемому классу. Правда, мы увидим, что уравнения $ax^3+y^3=1$ и $I(x, y)=27$ занимают особое положение и нуждаются в отдельном исследовании, которое уже изложено в предыдущих параграфах.

Перехожу к решению уравнений нашего класса.

Итак, пусть форма $f(x, y)$ примитивна и представляется в виде $N(\lambda x+\mu y)$, причем числа $\varphi=\lambda'\mu''-\lambda''\mu'$, $\varphi=\lambda''\mu-\lambda\mu''$, $\varphi''=\lambda\mu'-\lambda'\mu$ ассоциированы. Как мы видели, решение уравнения $f(x, y)=1$ равносильно решению задачи об отыскании единиц „на плоскости“

$$\varphi\cdot\varepsilon+\varphi'\cdot\varepsilon'+\varphi''\cdot\varepsilon''=0. \qquad (*)$$

Число φ не принадлежит кубическому полю, которому принадлежит корень формы f, однако числа φ^2 и $\varphi'\varphi''$ принадлежат этому полю. Умножив равенство (*) на $\varphi\varphi'\varphi''$, получим

$$\nu\varepsilon+\nu'\varepsilon'+\nu''\varepsilon''=0,$$

где $\nu=\varphi^2\varphi'\varphi''$ принадлежит кубическому полю и ν' и ν'' сопряжены с ν. Обозначим через l норму числа ν. Очевидно, что ν, ν' и ν'' ассоциированы между

собой и, следовательно, ассоциированы с $\sqrt[3]{l}$. Таким образом, решение неопределенных уравнений рассматриваемого класса приводится к следующей задаче:

Среди чисел ω, принадлежащих данному кубическому полю и лежащих на плоскости нулевого следа

$$\omega + \omega' + \omega'' = 0,$$

найти все числа, ассоциированные, вместе с сопряженными, с $\sqrt[3]{l}$, где l — данное целое рациональное число.

Заметим, что для уравнения $ax^3 + by^3 = 1$ число $l = ab$. Без нарушения общности можно считать, что число l положительно и свободно от кубических множителей. Положим $l = fg^2$, считая f и g свободными от квадратов.

Обозначим через L совокупность всех чисел рассматриваемого кубического поля, делящихся, вместе с сопряженными, на $\sqrt[3]{l}$. Через $\bar{L}$ обозначим совокупность чисел, делящихся, вместе с сопряженными, на $\sqrt[3]{\bar{l}}$, где $\bar{l} = f^2g$. Совокупности L и $\bar{L}$, очевидно, идеалы. Далее, через L_0 и $\bar{L}_0$ обозначим совокупность чисел нулевого следа, принадлежащих соответственно идеалам L и $\bar{L}$. Совокупности L_0 и $\bar{L}_0$ имеют, очевидно, двухчленные базисы. Обозначим их соответственно $[\nu_1, \nu_2]$ и $[\bar{\nu}_1, \bar{\nu}_2]$.

Легко видеть, что каждое число, принадлежащее идеалу L, может быть представлено в виде $\frac{x\nu_1 + y\nu_2 + z}{3}$, где x, y, z — целые рациональные числа, причем z делится на fg. Действительно, пусть ν — какое-либо число, принадлежащее идеалу L. Обозначим $\nu + \nu' + \nu'' = z$. Целое рациональное число z делится на $\sqrt[3]{l}$ и, следовательно, на fg. Далее, число $3\nu - z$ принадлежит, очевидно, совокупности L_0. Следовательно, $3\nu - z = x\nu_1 + y\nu_2$ с целыми рациональными x и y. Поэтому ν действительно равно $\frac{x\nu_1 + y\nu_2 + z}{3}$. Аналогично, каждое число, принадлежащее идеалу $\bar{L}$, представляется в виде $\frac{x\bar{\nu}_1 + y\bar{\nu}_2 + z}{3}$.

Пусть $\omega = x\nu_1 + y\nu_2$ — число плоскости нулевого следа, дающее решение задачи, т. е. ассоциированное с $\sqrt[3]{l}$. Число $\eta = \frac{\omega}{\sqrt[3]{l}}$ является единицей поля, получающегося в результате соединения кубических полей $\Omega(\omega)$ и $\Omega(\sqrt[3]{l})$. Это поле будет, вообще говоря, полем девятого порядка, и η будет алгебраическим числом девятого порядка. Число η может принадлежать полю $\Omega(\omega)$ только в двух случаях: если $l = 1$ или если $\Omega(\omega)$ совпадает с $\Omega(\sqrt[3]{l})$.

Оба эти случая уже были рассмотрены. Действительно, если $l = 1$, то задача приводится к отысканию единиц на плоскости нулевого следа. Если $\Omega(\omega)$ совпадает с $\Omega(\sqrt[3]{l})$, то задача приводится к решению уравнения $x^3 + ly^3 = 1$. Действительно, базис плоскости нулевого следа для поля $\Omega(\sqrt[3]{l})$ образован числами $\sqrt[3]{l}$ и $\sqrt[3]{\bar{l}}$, следовательно, совокупность L_0 образована числами вида $x\sqrt[3]{l} + y\sqrt[3]{\bar{l}}$, делящимися на $\sqrt[3]{l}$. Такими числами будут все числа $x\sqrt[3]{l} + y\sqrt[3]{l^2}$. Из них ассоциированными с $\sqrt[3]{l}$ будут, очевидно, те, для которых

$$N(x + y\sqrt[3]{l}) = x^3 + ly^3 = 1.$$

Мы исключим из рассмотрения эти два случая.

Введем теперь в рассмотрение единицу

$$\varepsilon = \eta^3 = \frac{\omega^3}{l}.$$

Эта единица уже принадлежит основному кубическому полю, и она не является кубом единицы того же поля (конечно, если случан $l=1$ и $\Omega(\omega)=\Omega(\sqrt[3]{l})$ исключены).

Единицы внда $\frac{\omega^3}{l}$, где ω — число плоскости нулевого следа, мы будем называть искомыми единицами.

Докажем теперь несколько теорем относительно этих единиц, из которых затем легко получим полное решение задачи, поставленной в этом параграфе.

Теорема 1. *Единица $\varepsilon=\frac{\omega^3}{l}$, где ω — число плоскости нулевого следа, не может быть обратной, за конечным числом исключений.*

Доказательство. Обозначим через $\eta=\sqrt[3]{\varepsilon}=\frac{\omega}{\sqrt[3]{l}}$, $\eta'=\frac{\omega'}{\sqrt[3]{l}}$, $\eta''=\frac{\omega''}{\sqrt[3]{l}}$. Числа η, η', η'' являются корнями уравнения вида

$$\eta^3=-q\sqrt[3]{l}\,\eta+1,$$

где q — целое рациональное число. Это уравнение имеет один вещественный корень η и два сопряженных комплексных η' и η'', н, следовательно, дискриминант этого уравнения отрицателен:

$$-4lq^3-27<0.$$

Это возможно только прн $q>0$, за исключениямн $q=-1$, $l=1,2,3,4,5,6$.

Но, если $q>0$, то вещественный корень η уравнения $\eta^3=-q\sqrt[3]{l}\,\eta+1$ удовлетворяет неравенству $0<\eta<1$. Следовательно, также $0<\varepsilon<1$, что и требовалось доказать.

Теорема 2. *Положительная степень единицы вида $\frac{\omega}{\sqrt[3]{l}}$, где ω — число нулевого следа, не может быть ни единицей такого же вида, ни единицей вида $\frac{\omega}{\sqrt[3]{l}}$, за исключениями η^8, где $\eta=\frac{\omega}{\sqrt[3]{4}}$, $\omega^3=-4\omega+4$, и η^{13}, где $\eta=\frac{\omega}{\sqrt[3]{2}}$, $\omega^3=-2\omega+2$.*

Доказательство. Если $\left(\frac{\omega}{\sqrt[3]{l}}\right)^n=\frac{\omega_1}{\sqrt[3]{l}}$ или $\frac{\omega_1}{\sqrt[3]{l}}$, то ω^n представляет собой число плоскости нулевого следа. Но мы знаем нз леммы 4 предыдущего параграфа, что степень числа, лежащего на плоскости нулевого следа, не может быть числом нулевого следа, за шестью исключениямн. В виду того, что ω обладает тем свойством, что $\frac{\omega}{\sqrt[3]{l}}$ есть единица, ω должно быть корнем уравнения $\omega^3=-q\omega+n$, где $n=l$, q делится на $\sqrt[3]{l^2}$, и, следовательно, q^3 делится на n^2. Кроме того, $l\neq 1$. Этим требованиям удовлетворяют только те два исключения из шестн, которые упомянуты в условии теоремы.

Теорема 3. *Единица вида $\frac{\omega^3}{l}$, где ω — число плоскости нулевого следа, не может быть нечетной степенью другой единицы, за конечным числом исключений.*

Доказательство. Пусть $\frac{\omega^3}{l}=\frac{(xv_1+yv_2)^3}{l}=\varepsilon^p$, где ε — единица поля $\delta(\omega)$, и пусть это поле не принадлежит к числу исключенй нз теорем 1 н 2.

Здесь p обозначает нечетное число. Число p не может делиться на 3, и, следовательно, $p \equiv \pm 1 \pmod 6$.

Рассмотрим подробно случай $p \equiv 1 \pmod 6$. Положим $p = 6k + 1$.

Единица ε должна быть прямой основной единицей. Введем в рассмотрение единицу $\varepsilon^{\frac{1}{3}} = \sqrt[3]{\varepsilon^p} \cdot \varepsilon^{-2k} = \frac{\omega\varepsilon^{-2k}}{\sqrt[3]{l}}$. Число $\omega_1' = \omega\varepsilon^{-2k}$, очевидно, принадлежит идеалу L и, следовательно, представляется в виде $\frac{x_1\nu_1 + y_1\nu_2 + z_1}{3}$ при z, делящемся на fg.

Итак,

$$\eta = \varepsilon^{\frac{1}{3}} = \frac{x_1\nu_1 + y_1\nu_2 + z_1}{3\sqrt[3]{l}} = \frac{\omega_1}{\sqrt[3]{l}},$$

$$\eta^p = \varepsilon^{\frac{p}{3}} = \frac{\omega}{\sqrt[3]{l}}.$$

Введем в рассмотрение числа $\eta' = \frac{\omega_1'}{\sqrt[3]{l}}$, $\eta'' = \frac{\omega_1''}{\sqrt[3]{l}}$.

Для них имеет место равенство

$$\eta^p + \eta'^p + \eta''^p = 0,$$

откуда следует, что $\eta' + \eta'' = \frac{z_1 - \omega_1}{\sqrt[3]{l}}$ представляет собой алгебраическую единицу и, следовательно, $z_1 - \omega_1$ ассоциировано с $\sqrt[3]{l}$.

С другой стороны, ω_1 является корнем уравнения

$$\omega_1^3 = z_1\omega_1^2 - q\omega_1 + l,$$

причем z_1 делится на fg, q делится на l.

Вследствие того, что $N(z_1 - \omega_1) = \pm l$, между коэффициентами z_1 и q выполнено соотношение

$$N(z_1 - \omega_1) = z_1^3 - z_1^3 + qz_1 - l = \pm l,$$

откуда

$$qz_1 = 2l,$$

или

$$qz_1 = 0.$$

Первое равенство возможно лишь для конечного числа значений q, z_1, l. Второе возможно при $q = 0$, или при $z_1 = 0$.

Если $q = 0$, то $\frac{1}{\omega_1} + \frac{1}{\omega_1'} + \frac{1}{\omega_1''} = 0$, и следовательно $\bar{\omega}_1 + \bar{\omega}_1' + \bar{\omega}_1'' = 0$, где $\bar{\omega}_1 = \frac{fg}{\omega_1} = \sqrt[3]{l}\,\eta^{-1}$ — целое алгебраическое число, ассоциированное с $\sqrt[3]{l}$ и лежащее на плоскости нулевого следа. Это невозможно, за конечным числом исключений, так как обратная единица $\frac{1}{\varepsilon} = \frac{1}{\eta^3}$ не может иметь вид $\frac{\bar{\omega}_1^3}{l}$ при $\bar{\omega}_1$, лежащем на плоскости нулевого следа.

Если же $z_1 = 0$, то $\omega_1 + \omega_1' + \omega_1'' = 0$ и, следовательно, ω_1 лежит на плоскости нулевого следа и

$$\left(\frac{\omega_1}{\sqrt[3]{l}}\right)^p = \frac{\omega}{\sqrt[3]{l}}.$$

Это невозможно в силу теоремы 2, за конечным числом исключений. Тем самым теорема доказана для $p \equiv 1 \pmod 6$.

Для второго случая $p \equiv -1 \pmod 6$ теорема доказывается посредством аналогичных рассуждений. Мы их опускаем.

Из всего сказанного выше следует, что единицами искомого вида $\frac{(xv_1+yv_2)^3}{l}$ могут быть только единицы ε_0^{2k}, где ε_0 — прямая основная единица поля. Следовательно, такая единица в данном поле может быть только одна, так как если бы их обнаружилось две, то одна из них была бы степенью другой, что невозможно.

Докажем теперь, что эту единицу, если она существует, можно найти в конечном числе действий или убедиться в ее несуществовании.

Для этого докажем следующие теоремы.

Теорема 4. *Неопределенное уравнение*

$$m^2u^6 - 2^sn^2v^6 = 1$$

при данных нечетных m *и* n *не имеет решений* u, v, *если* $s \geqslant 8k+4$.

Здесь k обозначает число различных нечетных простых делителей числа n.

Доказательство. От каждого решения уравнения

$$m^2u^6 - 2^sn^2v^6 = 1$$

можно „спуститься" к решению другого уравнения такого же вида.

Действительно, уравнение

$$m^2u^6 - 2^sn^2v^6 = 1$$

можно переписать в виде

$$\frac{mu^3+1}{2} \cdot \frac{mu^3-1}{2} = 2^{s-2}n^2v^6,$$

откуда вытекает, вследствие взаимной простоты чисел $\frac{mu^3+1}{2}$ и $\frac{mu^3-1}{2}$, что

$$\frac{mu^3 \pm 1}{2} = 2^{s-2}n_1^2v_1^6; \quad \frac{mu^3 \mp 1}{2} = m_1^2u_1^6,$$

где $(m_1, 2n_1) = 1$, $m_1n_1 = n$, $u_1v_1 = v$.

Отсюда следует, что

$$m_1^2u_1^6 - 2^{s-2}n_1^2v_1^6 = \mp 1.$$

Знак (—) в правой части, очевидно, невозможен при $s \geqslant 4$. Следовательно, мы действительно „спустились" к новому уравнению

$$m_1^2u_1^6 - 2^{s_1}n_1^2v_1^6 = 1$$

такого же вида, как исходное, причем v_1 является делителем v, $m_1n_1 = n$, $(m_1, 2n_1) = 1$ и $s_1 = s-2$. От этого уравнения можно спуститься к следующему и т. д. до тех пор, пока показатель при двойке не станет меньше двух.

Такой спуск может быть двух родов.

Спуском первого рода мы будем называть спуск, при котором $m_1 = 1$, тогда $n_1 = n$.

Спуском второго рода будем называть спуск, при котором $m_1 > 1$. Тогда n_1 будет содержать меньше простых делителей, чем n, в виду того, что m_1 и n_1 взаимно просты и $n_1 = \frac{n}{m_1}$.

Покажем теперь, что невозможны *четыре* спуска первого рода под ряд.

Действительно, если бы имели место один за другим четыре спуска первого рода, то следующие пять уравнений имели бы решения:

$$m^2u^6 - 2^s n^2 v^6 = 1,$$
$$u_1^6 - 2^{s-2} n^2 v_1^6 = 1,$$
$$u_2^6 - 2^{s-4} n^2 v_2^6 = 1,$$
$$u_3^6 - 2^{s-6} n^2 v_3^6 = 1,$$
$$u_4^6 - 2^{s-8} n^2 v_4^6 = 1.$$

Однако, это невозможно. В самом деле, решение второго и пятого уравнений можно рассматривать как решение уравнения

$$x^3 - Ay^3 = 1 \quad (A = 2^{s-8} n^2)$$

при $x = u_2^2$, $y = 4v_1^2$ для второго уравнения и при $x = u_4^2$, $y = v_4^2$ для пятого.

Эти решения уравнения $x^3 - Ay^3 = 1$ различны, так как v_4 является делителем v_1. Но мы знаем, что уравнение $x^3 - Ay^3 = 1$ может иметь не более одного решения с $xy \neq 0$.

Итак, предположение, что возможны под ряд четыре спуска первого рода, привело нас к противоречию, и поэтому на каждые четыре спуска приходится по крайней мере один спуск второго рода. Следовательно, после каждых четырех спусков число n теряет по крайней мере один нечетный простой множитель. После $4k$ спусков n потеряет все нечетные простые множители, и мы придем к уравнению

$$m_{4k}^2 u_{4k}^6 - 2^t v_{4k}^6 = 1,$$

где $t = s - 4k \geqslant 4$.

Сделав спуск еще один раз, мы придем к уравнению

$$u_{4k+1}^6 - 2^{t-2} v_{4k+1}^6 = 1.$$

Это уравнение, очевидно, не имеет решений, ибо $t - 2 \geqslant 2$, а уравнеиия

$$x^3 - 4y^3 = 1, \quad x^3 - 8y^3 = 1 \text{ и } x^3 - 16y^3 = 1$$

решений с $xy \neq 0$ не имеют. Тем самым теорема доказана.

Спуск, примененный в этом доказательстве, придуман Nagell'ем.

Теорема 5. *Единицы искомого вида* $\varepsilon = \frac{(xv_1 + yv_2)^3}{l}$ *могут находиться только среди степеней*

$$\varepsilon_0^{4^s} \text{ или } \varepsilon_0^{2 \cdot 4^s}$$

при $s \leqslant \frac{4k+8}{3}$, *где* k *обозначает число различных простых делителей числа* l.

Доказательство. Прежде всего отметим, что для существования единицы $\varepsilon = \frac{(xv_1 + yv_2)^3}{l}$ необходимо, чтобы основная прямая единица ε_0, или её квадрат ε_0^2, имела вид $\frac{\omega_1^3}{l}$, где ω_1 — число основной кубической области, ассоциированное с $\sqrt[3]{l}$. Действительно, пусть $\frac{(xv_1 + yv_2)^3}{l} = \varepsilon_0^{2^k}$. Очевидно, что $2^k \equiv 1 \pmod 3$ при четном k и $2^k \equiv 2 \pmod 3$ при нечетном k. Положив $2^k = 3t + \sigma$, $\sigma = 1$ или 2, получим

$$\varepsilon_0^{\frac{\sigma}{3}} = \frac{(xv_1 + yv_2)\,\varepsilon_0^{-t}}{\sqrt[3]{l}} = \frac{\omega_1}{\sqrt[3]{l}}.$$

Обозначим $\varepsilon_0^{\frac{\sigma}{3}} = \eta_0$, $\varepsilon^{\frac{1}{3}} = \eta$. Из нашего рассуждения следует, что

$$\eta = \eta_0^{4^s}.$$

Введем в рассмотрение уравнения, корнями которых являются

$$\eta_0,\ \eta_1 = \eta_0^4,\ \eta_2 = \eta_0^{16}, \ldots,\ \eta_s = \eta_0^{4^s}, \ldots$$

Эти уравнения имеют вид:

$$\eta_0^3 = a_0 \sqrt[3]{l}\ \eta_0^2 - b_0 \sqrt[3]{l}\ \eta_0 + 1,$$
$$\eta_1^3 = a_1 \sqrt[3]{l}\ \eta_1^2 - b_1 \sqrt[3]{l}\ \eta_1 + 1$$

и т. д.

Между коэффициентами этих уравнений выполнены соотношения

$$a_{s+1} = a_s^4 f^2 g - 4a_s^2 b_s f g + 2b_s^2 g + 4a_s,$$
$$b_{s+1} = b_s^4 f g^2 - 4b_s^2 a_s f g + 2a_s^2 f + 4b_s.$$

Для единиц искомого вида $a_s = 0$.

Покажем теперь, что a_s и b_s при $s \geqslant 1$ делятся на 2^{2s-1} или, если этого нет, то решений задачи не существует. Для этого рассмотрим несколько случаев.

Пусть $l = fg^2$ — нечетное число и a_0 — нечетное. Тогда, очевидно, все a_s — нечетные, и равенство $a_s = 0$ невозможно. Пусть теперь $l = fg^2$ нечетное число, a_0 — четное, но b_0 — нечетное. В этом случае все b_s — нечетные и все $a_s \equiv 2 \pmod 4$. Следовательно, и в этом случае равенство $a_s = 0$ невозможно. Если же a_0 и b_0 — оба четные, то a_1, b_1 делятся на 8, a_2, b_2 делятся на 32 и т. д.

Наконец, если $l = fg^2$ — четное число, то a_1, b_1 — оба четные, a_2, b_2 делятся на 8 и т. д., a_s, b_s — оба делятся на 2^{2s-1}.

Допустим теперь, что $a_{s+1} = 0$ при $s + 1 > \frac{4k+8}{3}$

Это приводит нас к неопределенному уравнению

$$a_s^4 f^2 g - 4a_s^2 b_s f g + 2b_s g + 4a_s = 0.$$

Из этого уравнения следует, что $4a_s$ делится на g. Так как кроме того a_s делится на 2^{2s-1}, то можно быть уверенным в том, что a_s делится на $2^{2s-2}g$. Положим $a_s = 2^{2s-2} g\alpha$. После подстановки и сокращения на $2g$ придем к уравнению

$$2^{8s-9} l^2 \alpha^4 - 2^{4s-3} \alpha^2 l b_s + b_s^2 + 2^{2s-1} \alpha = 0,$$

откуда

$$(b_s - 2^{4s-4} \alpha^2 l)^2 = 2^{2s-1} \alpha (2^{6s-8} l^2 \alpha^3 - 1).$$

Числа $2^{2s-1}\alpha$ и $2^{6s-8} l^2 \alpha^3 - 1$ взаимно просты и их произведение равно полному квадрату. Следовательно,

$$\alpha = \pm 2u^2,$$
$$2^{6s-8} l^2 \alpha^3 - 1 = \pm v^2.$$

Знаки здесь находятся в соответствии. Верхний знак, очевидно, нужно отбросить. Подставив $\alpha = -2u^2$ во второе равенство, получим

$$2^{6s-5} l^2 u^6 = v^2 - 1,$$

откуда

$$\frac{v-1}{2} \cdot \frac{v+1}{2} = 2^{6s-7} l^2 u^6.$$

Числа $\frac{v-1}{2}$ и $\frac{v+1}{2}$ взаимно просты. Следовательно,

$$\frac{v\pm 1}{2} = m^2 u_1^6; \quad \frac{v\mp 1}{2} = 2^{6s-7} n^2 v_1^6,$$

где $mn = l$, $u_1 v_1 = u$.
Вычитая, получим

$$m^2 u_1^6 - 2^{6s-7} n^2 v_1^6 = \pm 1.$$

Знак (—) в правой части, очевидно, нужно отбросить.

Но последнее уравнение не имеет решений в силу теоремы 4.

Действительно, $s+1 > \frac{4k+8}{3}$, $6s-7 > 8k+3$ и, следовательно,

$$6s-7 \geqslant 8k+4.$$

Число n содержит не больше нечетных простых делителей, чем число l. Таким образом, уравнение

$$m^2 u_1^6 - 2^{6s-7} n^2 v_1^6 = 1$$

удовлетворяет условиям теоремы 4 и потому не имеет решений.

§ 74. Обобщение метода § 71 на уравнение $x^4 - Ay^4 = \pm 1$

Эти уравнения были впервые решены проф. В. А. Тартаковским в работе «Auflösung der Gleichung $x^4 - py^4 = 1$». (Изв. А. Н., 1926) посредством метода, существенно отличного от того, к изложению которого мы сейчас приступаем.

1°. Уравнение

$$x^4 - Ay^4 = \pm 1 \tag{1}$$

можно преобразовать к виду

$$(x^2 + xy\sqrt[4]{-4A} + y^2\sqrt{-A})(x^2 - xy\sqrt[4]{-4a} + y^2\sqrt{-A}) = \pm 1. \tag{2}$$

Число $x^2 + xy\sqrt[4]{-4A} + y^2\sqrt{-A}$ принадлежит кольцу $O(\sqrt[4]{-4A})$ с базисом $\left[1, \sqrt[4]{-4A}, \sqrt{-A}, \sqrt{-A}\cdot\sqrt[4]{-4A}\right]$ поля $\Omega\sqrt[4]{-4A}$ и является в силу (2) единицей этого кольца, причем единицей специального вида — в ней отсутствует член, содержащий $\sqrt{-A}\sqrt[4]{-4A}$.

Таким образом, всякое решение уравнения (1) определяет трехчленную единицу вида $a + b\sqrt[4]{-4A} + c\sqrt{-A}$ кольца $O(\sqrt[4]{-4A})$. Нетрудно видеть, что обратно всякая трехчленная единица этого вида определяет решение уравнения (1).

В самом деле, пусть $\varepsilon = a + b\sqrt[4]{-4A} + c\sqrt{-A}$ есть единица.
Тогда ее норма

$$N(\varepsilon) = \varepsilon\,\varepsilon'\,\varepsilon''\,\varepsilon''' = (a^2 - Ac^2)^2 + 4A(ac - b^2)^2$$

должна равняться 1. Для этого нужно, чтобы

$$ac - b^2 = 0, \tag{3}$$
$$a^2 - Ac^2 = \pm 1. \tag{4}$$

Из (4) мы видим, что $(a, c) = 1$, и, следовательно, из (3)

$$a = \pm x^2, \quad b = \pm xy, \quad c = \pm y^2.$$

Подставляя в (4), получим

$$x^4 - Ay^4 = \pm 1.$$

Итак, задача отыскания трехчленных единиц кольца $O(\sqrt[4]{-4A})$ равносильна задаче о решении уравнения (1).

2°. Изучим ближе свойства единиц кольца $O(\sqrt[4]{-4A})$.

Прежде всего отметим, что поле $\Omega(\sqrt[4]{-4A})$, а следовательно и кольцо $O(\sqrt[4]{-4A})$, по теореме Дирихле, имеют одну основную единицу, степени которой, с целым положительным или отрицательным показателем, дают все единицы.

Пусть $\varepsilon = a + b\sqrt[4]{-4A} + c\sqrt{-A} + d\sqrt{-A}\sqrt[4]{-4A}$ — какая-либо единица кольца $O(\sqrt[4]{-4A})$.

Сопряженные с ней числа суть

$$\varepsilon' = a + bi\sqrt[4]{-4A} + c\sqrt{-A} + di\sqrt{-A}\sqrt[4]{-4A},$$
$$\varepsilon'' = a - b\sqrt[4]{-4A} + c\sqrt{-A} - d\sqrt{-A}\sqrt[4]{-4A},$$
$$\varepsilon''' = a - bi\sqrt[4]{-4A} + c\sqrt{-A} + di\sqrt{-A}\sqrt[4]{-4A}.$$

Ее норма

$$(N(\varepsilon) = (a^2 - Ac^2 + 4Abd)^2 + 4A(ac - b^2 + Ad^2)^2 = 1.$$

Следовательно,

$$a^2 - Ac^2 + 4Abd = \pm 1, \tag{5}$$
$$ac - b^2 + Ad^2 = 0. \tag{6}$$

Вторая сопряженная ε'' принадлежит тому же кольцу, что и ε. Легко видеть, что

$$\varepsilon\varepsilon'' = (a^2 - Ac^2 + 4Abd) + 2\sqrt{-A}(ac - b^2 - Ad^2) = \pm 1.$$

Следовательно,

$$\varepsilon'' = \pm\frac{1}{\varepsilon}. \tag{7}$$

Будем единицу ε называть прямой, если $|\varepsilon| > 1$, и обратной, если $|\varepsilon| < 1$. Из (7) следует, что если прямая единица ε трехчленна, то обратная $\frac{1}{\varepsilon}$ также трехчленна, и наоборот. Таким образом, достаточно искать трехчленные единицы среди положительных степеней основной прямой единицы.

Отметим следующее неравенство:

Если ε — прямая единица, то $|\varepsilon| > 2\sqrt[4]{4A} - 1$.

В самом деле

$$\varepsilon - \varepsilon'' = 2\sqrt[4]{-4A}(b + d\sqrt{-A})$$

и, следовательно,

$$|\varepsilon - \varepsilon''| = 2\sqrt[4]{4A}\sqrt{b^2 + Ad^2}.$$

Так как ε — прямая единица, то $|\varepsilon''| = \left|\frac{1}{\varepsilon}\right| < 1$ и, следовательно,

$$|\varepsilon| \geqslant |\varepsilon - \varepsilon''| - |\varepsilon''| > 2\sqrt[4]{4A} - 1.$$

3°. Теорема 1. *Нечетная степень трехчленной единицы вида*

$$a + b\sqrt[4]{-4A} + c\sqrt{-A}$$

не может быть трехчленной того же вида.

Доказательство. Пусть $\varepsilon = a + b\sqrt[4]{-4A} + c\sqrt{-A}$. Тогда

$$\varepsilon'' = a - b\sqrt[4]{-4A} + c\sqrt{-A}$$

$$\varepsilon^2 = \varepsilon(\varepsilon'' + 2b\sqrt[4]{-4A}) = \pm 1 + 2b\varepsilon\sqrt[4]{-4A}.$$

Следовательно,

$$(\pm 1)^n\varepsilon^{2n} = (1 \pm 2b\varepsilon\sqrt[4]{-4A})^n = 1 \pm \frac{n}{1}\cdot 2b\varepsilon\sqrt[4]{-4A} +$$

$$+ \frac{n(n-1)}{1\cdot 2}\cdot 8b^2\varepsilon^2\sqrt{-A} \pm \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}\cdot 16b^3\varepsilon^3\sqrt{-A}\sqrt[4]{-4A} + \ldots$$

$$+ \frac{n(n-1)\ldots(n-k+1)}{k!}\,2^k b^k\left(\sqrt[4]{-4A}\right)^k\cdot\varepsilon^k + \ldots$$

Умножая обе части равенства на ε'', получим

$$(\pm 1)^{n+1}\varepsilon^{2n-1} = \varepsilon'' + n\cdot 2b\sqrt[4]{-4A} \pm \frac{n(n-1)}{1\cdot 2}\,8b^2\varepsilon\sqrt{-A} +$$

$$+ \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}\,16b^3\varepsilon^2\sqrt{-A}\sqrt[4]{-4A} \pm \ldots \pm$$

$$\pm \frac{n(n-1)\ldots(n-k+1)}{k!}\cdot 2^k b^k(\sqrt[4]{-4A})^k\varepsilon^{k-1} + \ldots =$$

$$= a - b\sqrt[4]{-4A} + c\sqrt{-A} + n\cdot 2b\sqrt[4]{-4A} +$$

$$+ n(n-1)\cdot 4b^2\sqrt{-A}\,(a + b\sqrt[4]{-4A} + c\sqrt{-A}) \pm$$

$$\pm \frac{n(n-1)(n-2)}{3}\cdot 8b^3\sqrt{-A}\sqrt[4]{-4A}\,(\pm 1 + 2ab\sqrt[4]{-4A} +$$

$$+ 4b^2\sqrt{-A} + 2bc\sqrt{-A}\sqrt[4]{-4A}) + \ldots \pm$$

$$\pm \frac{n(n-1)\ldots(n-k+1)}{k!}\cdot 2^k b^k(\sqrt[4]{-4A})^k\varepsilon^{k-1} + \ldots$$

Для того, чтобы ε^{2n-1} была трехчленной, нужно, чтобы коэффициент при $\sqrt{-A}\sqrt[4]{-4A}$ в правой части предыдущего равенства равнялся нулю, т. е.

$$n(n-1)\cdot 4b^3 + \frac{n(n-1)(n-2)}{3}\cdot 8b^3 + \ldots +$$

$$+ \frac{n(n-1)\ldots(n-k+1)}{k!}\,2^k b^k H_k + \ldots = 0. \qquad (8)$$

Здесь через H_k обозначен коэффициент при $\sqrt{-A}\sqrt[4]{-4A}$ в $(\sqrt[4]{-4A})^k\varepsilon^{k-1}$. Очевидно, что H_k делится на 4 для $k \geqslant 4$.

Сократим равенство (8) на $4b^3$ и введем обозначение $G_k = \frac{H_k}{4}b^{k-3}$. Получим

$$n(n-1) + \frac{n(n-1)(n-2)}{3}\cdot 2 + \ldots +$$

$$+ \frac{n(n-1)\ldots(n-k+1)}{k!}\,2^k G_k + \ldots = 0. \qquad (9)$$

Равенство (9), очевидно, невозможно. В самом деле, пусть 2^σ — наибольшая степень 2, входящая в $n(n-1)$. Тогда во 2-е слагаемое $\frac{n(n-1)(n-2)}{3}\cdot 2$ входит 2 с показателем, не меньшим, чем $\sigma + 1$, так же как и во все остальные слагаемые, ибо, как известно, 2 входит в $k!$ самое большее с показателем $k-1$. Следовательно, левая часть равенства (9) не делится на $2^{\sigma+1}$ и не может равняться нулю.

Таким образом, приравняв нулю коэффициент при $\sqrt{-A}\sqrt[4]{-4A}$ в $(\pm 1)^{n+1}\varepsilon^{2n-1}$, мы пришли к противоречию. Тем самым теорема 1 доказана.

Теорема 2. *Нечетная степень трехчленной единицы вида*

$$a+c\sqrt{-A}+d\sqrt{-A}\sqrt[4]{-4A}$$

не может быть трехчленной вида $a'+b'\sqrt[4]{-4A}+c'\sqrt{-A}$.

Доказательство. Пусть

$$\varepsilon=a+c\sqrt{-A}+d\sqrt{-A}\sqrt[4]{-4A}.$$

Тогда

$$\varepsilon''=a+c\sqrt{-A}-d\sqrt{-A}\sqrt[4]{-4A}$$

и

$$\varepsilon^2=\pm 1+2d\sqrt{-A}\sqrt[4]{-4A}\cdot\varepsilon.$$

Далее

$$\begin{aligned}(\pm 1)^n\varepsilon^{2n}&=(1\pm 2d\sqrt{-A}\sqrt[4]{-4A}\varepsilon)^n=\\&=1\pm 2nd\sqrt{-A}\sqrt[4]{-4A}\,\varepsilon+\\&+\frac{n(n-1)}{1\cdot 2}\cdot 4d^2\cdot(-A)\sqrt{-4A}\,\varepsilon^2\pm\ldots\pm\\&\pm\frac{n(n-1)\ldots(n-k+1)}{k!}2^kd^k(\sqrt{-A}\sqrt[4]{-4A}\varepsilon)^k+\ldots\end{aligned}$$

Откуда, умножая на ε'', получим

$$\begin{aligned}(\pm 1)^{n+1}\varepsilon^{2n-1}&=\varepsilon''+2nd\sqrt{-A}\sqrt[4]{-4A}\pm\\&\pm\frac{n(n-1)}{1\cdot 2}\cdot 8d^2(-A)\sqrt{-A}\varepsilon\pm\ldots\pm\\&\pm\frac{n(n-1)\ldots(n-k+1)}{k!}2^kd^k(\sqrt{-A}\sqrt[4]{-4A})^k\varepsilon^{k-1}+\ldots=\\&=a+c\sqrt{-A}+d\sqrt{-A}\sqrt[4]{-4A}+2nd\sqrt{-A}\sqrt[4]{-4A}\pm\\&\pm\frac{n(n-1)}{1\cdot 2}8d^2(-A)\sqrt{-A}(a+c\sqrt{-A}+d\sqrt{-A}\sqrt[4]{-4A})\pm\\&\pm\ldots\pm\frac{n(n-1)\ldots(n-k+1)}{k!}2^kd^k(\sqrt{-A}\sqrt[4]{-4A})^k\varepsilon^{k-1}+\ldots\end{aligned}$$

Приравниваем нулю коэффициент при $\sqrt{-A}\sqrt[4]{-4A}$. Получим

$$\begin{aligned}&(2n+1)d+\frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}\cdot 8d^3H_3+\ldots\pm\\&\pm\frac{n(n-1)\ldots(n-k+1)}{k!}2^kd^kH_k+\ldots=0.\end{aligned}\qquad(10)$$

Через H_k мы обозначаем коэффициент при

$$\sqrt{-A}\sqrt[4]{-4A}\quad\text{в}\quad(\sqrt{-A}\sqrt[4]{-4A})^k\cdot\varepsilon^{k-1}.$$

Сокращая равенство (10) на d, придем к равенству

$$\begin{aligned}&(2n+1)+\frac{n(n-1)(n-2)}{3}4d^2H_3+\ldots\\&\pm\frac{n(n-1)\ldots(n-k+1)}{k!}2^kd^{k-1}H_k+\ldots=0,\end{aligned}$$

которое, очевидно, невозможно, ибо в левой части первое слагаемое $(2n+1)$ не делится на 2, а все остальные делятся.

Теорема 3. *Уравнение* $x^4 - 2y^4 = -1$ *имеет единственное решение* $x = \pm 1$, $y = \pm 1$. *Уравнение* $x^4 - 2y^4 = +1$ *не имеет решений, отличных от тривиального* $x = \pm 1$, $y = 0$.

Доказательство. Решение уравнений $x^4 - 2y^4 = \pm 1$ сводится к отысканию трехчленных единиц в $O(\sqrt[4]{-8})$.

Легко установить, что $\varepsilon_0 = 1 + \sqrt[4]{-8} + \sqrt{-2}$ является единицей $O(\sqrt[4]{-8})$.

Эта единица определяет решение $x = \pm 1$, $y = \pm 1$ уравнения

$$x^4 - 2y^4 = -1.$$

Докажем, что ε_0 — основная единица $O(\sqrt[4]{-8})$. В самом деле,

$$|\varepsilon_0| \approx 3.40,$$

а из 2^0 мы видим, что модуль любой единицы должен быть больше

$$2\sqrt[4]{8} - 1 \approx 2.36.$$

Отсюда следует, что ε_0 не может быть степенью какой-либо единицы, т. е. является единицей основной. Так как ε_0 — трехчленная единица, то среди ее нечетных степеней не может быть трехчленных единиц. Теорема будет доказана, если доказать, что среди четных степеней ε_0 не найдется ни одной трехчленной единицы.

Имеем

$$\varepsilon_0^2 = -1 + 2\sqrt[4]{-8}\cdot\varepsilon_0$$

и

$$\varepsilon_0^{2n}(-1)^n = 1 - 2n\sqrt[4]{-8}\,\varepsilon_0 + \frac{n(n-1)}{1\cdot 2}\cdot 8\sqrt{-2}\,\varepsilon_0^2 - \ldots$$

$$\pm\frac{n(n-1)\ldots(n-k+1)}{k!}\,2^k(\sqrt[4]{-8})^k\varepsilon_0^k + \ldots =$$

$$= 1 - 2n\sqrt[4]{-8}\,(1 + \sqrt[4]{-8} + \sqrt{-2}) +$$

$$+\frac{n(n-1)}{1\cdot 2}\cdot 8\sqrt{-2}\,(1 + 2\sqrt[4]{-8} + 4\sqrt{-2} + 2\sqrt{-2}\sqrt[4]{-8}) + \ldots$$

$$\pm\frac{n(n-1)\ldots(n-k+1)}{k!}\cdot 2^k(\sqrt[4]{-8})^k\varepsilon_0^k + \ldots$$

Приравнивая нулю коэффициент при $\sqrt{-2}\sqrt[4]{-8}$ и сокращая на 2, получим

$$-n + 4n(n-1) + \ldots \pm\frac{n(n-1)\ldots(n-k+1)}{k!}\cdot 2^{k-1}H_k + \ldots = 0, \quad (11)$$

где H_k — коэффициент при $\sqrt{-2}\sqrt[4]{-8}$ в $(\sqrt[4]{-8})^k\varepsilon^k$.

Очевидно, что для $k \geqslant 3$ H_k делится на 2. Если n делится на 2^σ, то $4n(n-1)$ делится на $2^{\sigma+2}$, и все остальные слагаемые левой части равенства (11) делятся, по крайней мере, на $2^{\sigma+1}$, ибо n делится на 2^σ, $k!$ делится, самое большее, на 2^{k-1}, H_k делится на 2. Следовательно, равенство невозможно, и теорема доказана.

4°. Теорема 4. *Квадрат единицы* $O(\sqrt[4]{-4A})$ *не может быть трехчленной единицей.*

Доказательство. Допустим обратное. Пусть

$$\varepsilon = a + b\sqrt[4]{-4A} + c\sqrt{-A} + d\sqrt{-A}\sqrt[4]{-4A}$$

— единица из $O(\sqrt[4]{-4A})$, и пусть $\varepsilon^2 = a' + b'\sqrt[4]{-4A} + c'\sqrt{-A}$.

Но

$$\varepsilon^2 = a^2 - Ac^2 - 4bdA + 2(ab - cdA)\sqrt[4]{-4A} + \\ + 2(b^2 - Ad^2 + ac)\sqrt{-A} + 2(ad + bc)\sqrt{-A}\sqrt[4]{-4A}.$$

Следовательно,

$$ad + bc = 0,$$

или

$$\frac{a}{b} = \frac{c}{-d},$$

откуда

$$\left.\begin{aligned} a &= km, \quad c = kn, \\ b &= lm, \quad d = -ln. \end{aligned}\right\} \tag{12}$$

С другой стороны, так как ε — единица, то

$$a^2 - Ac^2 + 4Abd = \pm 1, \tag{5}$$
$$ac - b^2 + Ad^2 = 0. \tag{6}$$

Подставив из (12) значения a, b, c, d в (5) и (6), получим

$$k^2m^2 - Ak^2n^2 - 4Al^2mn = \pm 1, \tag{5'}$$
$$k^2mn - l^2m^2 + Al^2n^2 = 0. \tag{6'}$$

Из (5') видим, что

$$(k, l) = 1; \quad (m, n) = 1; \quad (k, A) = 1; \quad (m, A) = 1.$$

Из (6') видим, что Al^2n^2 делится на m, l^2m^2 делится на n, следовательно, l^2 делится на m, ия n и на их произведение mn, ибо $(m, n) = 1$. С другой стороны, k^2mn делится на l^2, следовательно, mn делится на l^2, откуда

$$mn = \pm l^2.$$

Следовательно,

$$m = \sigma_1u^2; \quad n = \sigma_2v^2; \quad l = uv,$$

где

$$\sigma_1 = \pm 1, \quad \sigma_2 = \pm 1.$$

Подставив в (5') и (6'), получим

$$k^2(u^4 - Av^4) - 4A\sigma_1\sigma_2u^4v^4 = \pm 1, \tag{5''}$$
$$k^2\sigma_1\sigma_2u^2v^2 - u^2v^2(u^4 - Av^4) = 0. \tag{6''}$$

Из (6'') находим

$$k^2 = \sigma_1\sigma_2(u^4 - Av^4). \tag{13}$$

Подставив в (5''), получим

$$(u^4 - Av^4)^2 - 4Au^4v^4 = \pm 1,$$

или

$$u^8 - 6Au^4v^4 + A^2v^4 = \pm 1,$$

откуда

$$Av^4 = 3u^4 \pm \sqrt{8u^8 \pm 1}, \tag{14}$$

и, следовательно,

$$8u^8 \pm 1 = t^2. \tag{15}$$

Знак минус в левой части (15), очевидно, отпадает, так как квадрат нечетного числа не может иметь вид $8N-1$.

Следовательно,

$$8u^8 = (t-1)(t+1),$$

откуда

$$t \mp 1 = 2p^8; \quad t \pm 1 = 4q^8; \quad u = pq. \tag{16}$$

Из равенств (16) получаем

$$p^8 - 2q^8 = \mp 1. \tag{17}$$

Уравнения (17), в силу теоремы 3, допускают решения

$$p = 1, \quad q = 0,$$
$$p = 1, \quad q = 1$$

и других не имеют.

Первое решенне дает $u = 0$, что, очевидно, невозможно. Второе дает $u = 1$ и из (14) $Av^4 = 6$ или 0. Решение $Av^4 = 0$ дает $a = \pm 1$;

$$b = c = d = 0$$

из $\varepsilon_0 = \pm 1$; $Av^4 = 6$ дает, после подстановки в (13), невозможное равенство

$$k^2 = -5\sigma_1\sigma_2.$$

Теорема доказана.

Теорема 5. *Никакая нечетная степень основной единицы, кроме первой, не может быть трехчленной.*

Доказательство. Допустим обратное, что

$$\varepsilon_0^n = a' + b'\sqrt[4]{-4A} + c'\sqrt{-A},$$

где n — нечетное число.

Рассмотрим отдельно случан

$$n = 4m+1,$$
$$n = 4m-1.$$

Пусть

$$n = 4m+1$$

и

$$\varepsilon_0 = a + b\sqrt[4]{-4A} + c\sqrt{-A} + d\sqrt{-A}\sqrt[4]{-4A};$$

тогда

$$\varepsilon_0^{4m+1} = a' + b'\sqrt[4]{-4A} + c'\sqrt{-A}, \tag{18}$$

$$(\varepsilon_0''')^{4m+1} = a' - b'i\sqrt[4]{-4A} - c'\sqrt{-A}. \tag{19}$$

Умножим равенство (19) на i и вычтем из (18). Получим

$$\varepsilon_0^{4m+1} - i(\varepsilon_0''')^{4m+1} = a'(1-i) + c'(1+i)\sqrt{-A} =$$
$$= (1-i)(a' + ic'\sqrt{-A}) = (1-i)(a' - c'\sqrt{A}). \tag{20}$$

Левая часть равеиства (20)

$$\varepsilon_0^{4m+1} - i(\varepsilon_0''')^{4m+1} = \varepsilon_0^{4m+1} - (i\varepsilon_0''')^{4m+1}$$

делится на число

$$\lambda=\varepsilon_0-i\varepsilon_0''=$$
$$=a+b\sqrt[4]{-4A}+c\sqrt{-A}+$$
$$+d\sqrt{-A}\sqrt[4]{-4A}-i(a-bi\sqrt[4]{-4A}-c\sqrt{-A}+di\sqrt{-A}\sqrt[4]{-4A})=$$
$$=a(1-i)+c(1+i)\sqrt{-A}+2d\sqrt{-A}\sqrt[4]{-4A}=$$
$$=(1-i)(a+ci\sqrt{-A}+d\cdot(1+i)\cdot\sqrt{2}\sqrt[4]{A^3}e^{\frac{2\pi l}{4}})=$$
$$=(1-i)(a-c\sqrt{A}-2d\sqrt[4]{A^3}).$$

Следовательно, $a'-c'\sqrt{A}$ делится на $a-c\sqrt{A}-2d\sqrt[4]{A^3}$. Легко видеть, что $a'-c'\sqrt{A}$ является единицей поля $\Omega(\sqrt{A})$, ибо, как мы видели в 1^0, $a'=\pm x^2$, $c'=\pm y^2$, где x и y — решение уравнения

$$x^4-Ay^4=\pm 1,$$

которое можно записать в виде

$$(x^2-y^2\sqrt{A})(x^2+y^2\sqrt{A})=\pm 1.$$

Следовательно, число $\lambda=a-c\sqrt{A}-2d\sqrt[4]{A^3}$ является единицей поля $\Omega(\sqrt[4]{A})$, и его норма должна быть равна ± 1:

$$N(\lambda)=(a^2+Ac^2)^2-4A(ac+2Ad^2)^2=\pm 1. \tag{21}$$

С другой стороны,

$$a^2-Ac^2+4Abd=\pm 1, \tag{5}$$
$$ac-b^2+Ad^2=0. \tag{6}$$

Исключив b из равенства (5) и (6), получим

$$(a^2-Ac^2)^2\mp 2(a^2-Ac^2)+1-16A^2d^2(ac+Ad^2)=0. \tag{22}$$

Вычитая равенство (22) из (21), получим

$$\pm 2(a^2-Ac^2)-1=\pm 1,$$

откуда

$$a^2-Ac^2=0, \quad \text{или} \quad \pm 1.$$

Подставляя в (5), получим

$$4Abd=\pm 2, \quad \pm 1, \quad 0,$$

откуда или $b=0$, или $d=0$, так как равенства

$$4Abd=\pm 2, \quad \pm 1,$$

очевидно, невозможны.

Аналогичным образом для $n=4m+3$ мы придем к тому, что и в этом случае или $b=0$ или $d=0$, но это невозможно, так как мы знаем из теорем 1 и 2, что среди нечетных степеней единиц вида

$$a+b\sqrt[4]{-4A}+c\sqrt{-A}$$

и

$$a+c\sqrt{-A}+d\sqrt{-A}\sqrt[4]{-4A}$$

не может быть трехчленных единиц вида

$$a' + b' \sqrt[4]{-4A} + c' \sqrt{-A}.$$

Теорема доказана.

5°. Соединяя вместе результаты 4°, мы видим, что трехчленной единицей $O(\sqrt[4]{-4A})$ может быть только основная единица. Следовательно, уравнение $x^4 - Ay^4 = \pm 1$ может иметь только одно решение, отличное от тривиального, и его дает основная единица $O\sqrt[4]{-4A}$, если она имеет трехчленный вид.

Этот же метод обобщается на уравнении

$$ax^4 - by^4 = 1,\ 2,\ 4,\ 8$$

подобно тому, как метод решения уравнений $ax^3 + y^3 = 1$ обобщается на уравнениях, разобранных нами в § 3, среди которых, в частности, содержатся уравнения $ax^3 + by^3 = 1,\ 3$, решенные ранее Нагелем.

§ 75. О числе решений неопределенного уравнения $AX^3 + BX^2Y + CXY^2 + EY^3 = \sigma$, где форма (A, B, C, E) неприводима и имеет отрицательный дискриминант

1. Сведение задачи на случай, когда $\sigma = 1$. Если $\sigma \neq 1$, то, как это показал еще Лагранж („Nouvelle méthode pour résoudre les problèmes indeterminées en nombres entiers", Mémoires de Berlin, t. XXIV, 1770), решение уравнения $AX^3 + BX^2Y + CXY^2 + EY^3 = \sigma$ может быть приведено к решению ряда уравнений вида $A_iX^3 + B_iX^2Y + C_iXY^2 + E_iY^3 = 1$, где $i = 1, 2, \ldots, k$ и k не больше, чем σ.

Действительно, пусть задано уравнение

$$AX^3 + BX^2Y + CXY^2 + EY^3 = \sigma. \tag{1}$$

Лагранж замечает, что можно предположить, что X и σ — взаимно простые, так как, если бы $X = X'\delta$, $\sigma = \sigma'\delta$, где δ — какой-нибудь простой множитель σ, то либо Y делится на него, но тогда мы могли бы все сократить на δ^3, или же E делится на δ, тогда, наложив $E = E'\delta$ и сократив все на δ, мы пришли бы к представлению числа σ' формой $(A\delta^2, B\delta, C, E')$.

Далее, Лагранж говорит: пусть X, Y — какое-нибудь решение, тогда, в виду того, что X и σ — взаимно простые, можно найти числа $\bar{Y}$ и θ такие, что $\sigma\bar{Y} + \theta \cdot X = Y$ и что $-\frac{\sigma}{2} < \theta \leqslant \frac{\sigma}{2}$. Подставив это Y в уравнение (1), мы получаем уравнение

$$(A + B\theta + C\theta^2 + E\theta^3)X^3 + (B + 2C\theta + 3E\theta^2)\sigma X^2Y + (C + 3E)\sigma^2XY^2 + E\sigma^3Y^3 = \sigma$$

все члены которого делятся на σ, кроме $(A + B\theta + C\theta^2 + E\theta^3)X^3$; но X — взаимно простое с σ, и, следовательно, $A + B\theta + C\theta^2 + E\theta^3$ должно делиться на σ; значит, надо брать только такие θ, которые удовлетворяли бы сравнению $A + B\theta + C\theta^2 + E\theta^3 \equiv 0 \pmod{\sigma}$, и для каждого из корней θ_i этого сравнения получается, после сокращения на σ, уравнение вида

$$A_iX^3 + B_iX^2\bar{Y} + C_iX\bar{Y}^2 + E_i\bar{Y}^3 = 1, \tag{2}$$

где

$$A_i = \frac{A + B\theta_i + C\theta_i^2 + E\theta_i^3}{\sigma}; \quad B_i = B + 2C\theta_i + 3E\theta_i^2;$$
$$C_i = (C + 3E\theta_i)\sigma; \quad E_i = E\sigma^2.$$

Найдя все решения $X\bar{Y}$ всех этих уравнений (2_i), мы найдем все решения X, Y уравнения (1), у которых X взаимно простое с σ, полагая $Y = \sigma\bar{Y} + \theta_i X$, и все решения, у которых X не взаимно простое с σ, сокращая, как указано в начале, на σ, из решений сокращенных уравнений, в которых уже сокращенное X — взаимно простое с сокращенным σ, причем эти уравнения мы опять сведем на уравнения типа (2_i).

2. Сведение вопроса о числе представлений на представление единицы целой формой. Итак, вопрос о нахождении всех представлений кубической двойничной формой (A, B, C, E) заданного числа σ сводится на вопрос о нахождении всех представлений числа 1 конечным числом таких же форм, а следовательно, и вопрос о числе представлений σ исходной формой также сводится к вопросу о числах представлений 1 этими формами. Пусть (A, B, C, E) одна из таких форм. Одно из двух: либо она не представляет 1, и тогда число представлений числа 1 равно нулю, либо она число 1 представляет, т. е. существуют такие значения $x = \beta$, $y = \delta$, что $A\beta^3 + B\beta^2\delta + C\beta\delta^2 + E\delta^3 = 1$, но тогда β и δ взаимно просты, и можно подобрать такие также целые рациональные числа α, γ, чтобы было $\alpha\delta - \beta\gamma = 1$; если теперь преобразовать форму (A, B, C, E) целочисленной унимодулярной подстановкой $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, то последний коэффициент преобразованной формы будет равен $A\beta^3 + B\beta^2\delta + C\beta\delta^2 + E\beta^3$, т. е. будет равен 1. Преобразованную форму мы будем писать так: $(n, -q, s, 1)$. Форму, у которой один из крайних коэффициентов (мы будем всегда предполагать, что четвертый) равен 1, мы будем называть „целой“. Итак, если форма (A, B, C, E) имеет представления числа 1, то она эквивалентна некоторой целой форме, причем число представлений ею числа 1 равно числу представлений числа 1 этой целой формой. Вопрос о числе представлений любого числа кубической двойничной формой мы, таким образом, свели на вопрос о числе представлений 1 целой формой. Мы не говорим здесь, что если форма (A, B, C, E) дана, то мы можем найти форму $(n, -q, s, 1)$, а только, что если форма (A, B, C, E) имеет представления 1, то целая форма $(n, -q, s, 1)$, ей эквивалентная, существует.

3. Сведение вопроса о числе представлений на разыскание двухчленных единиц. Из тождества

$$X^3 n - X^2 Y q + XY^2 s + Y^3 = (X\rho + Y)(X\rho' + Y)(X\rho'' + Y),$$

где ρ, ρ', ρ'' — корни кубического уравнения $\rho^3 = s\rho^2 + q\rho + n$, мы видим, что каждому решению уравнения

$$nX^3 - qX^2Y + sXY^2 + Y^3 = 1 \qquad (3,)$$

соответствует в кольце $O(\rho) = [\rho^2, \rho, 1]$ положительная, т. е. с нормой $+1$, единица, имеющая вид $X\rho + Y$, т. е. двухчленная положительная единица, и обратно.

В случае, когда $D = s^2q^2 - 18sqn + 4q^3 - 4s^3n - 27n^2 < 0$, который мы единственно будем дальше рассматривать, т. е. когда один корень ρ вещественен, а два других ρ', ρ'' — комплексно сопряженные, все положительные единицы кольца $O(\rho)$ суть степени с целыми рациональными показателями одной так называемой основной единицы этого кольца. Мы будем, как и раньше, называть положительной прямой основной единицей ту основную единицу ε_0,

которая удовлетворяет неравенствам $0<\varepsilon_0<1$. (В табл. стр. 230 даны как раз эти положительные прямые основные единицы всех колец $O(\rho)$ с отрицательными дискриминантами D, по абсолютной величиие не бо́льшими 379.) В таком случае все положнтельные единицы ε кольца $O(\rho)$ суть степени с положительными целыми рациональными показателями m этой прямой основиой единицы ε_0 и ей обратной $\eta_0=\varepsilon_0^{-1}$, т. е. всякая такая единица есть лнбо ε_0^m, либо η_0^m. В случае $D<0$ весь вопрос о числе представлений сводится, таким образом, к разысканию всех тех целых положительных показателей m, при которых лнбо ε_0^m, либо η_0^m — двухчленная в ρ еднница, т. е. имеет вид $P\rho+Q$.

Мы будем называть решением формы систему целых рациональных зиачений X, Y, которые, будучи подставлены в форму, делают ее равною 1, но для краткости будем также называть решением ту двухчленную еднннцу, которая дает решение.

4. Об обратных решениях. В этом пункте мы рассмотрим степени η_0^m обратной единицы с целыми положительными m.

Теорема. *Среди степеней обратной основной единицы с положительными целыми рациональными показателями m может быть лишь конечное число двухчленных единиц, и они все могут быть найдены.* Случаю $D<0$, т. е. когда одиа пара комплексных корней, соответствует сигнатурное пространство $(x, y, z)R_{2.1}$, т. е. положительные единицы решетки $[\rho^2, \rho, 1]$ лежат в нем иа поверхности $(x^2+y^2)z=1$. Двухчленные числа $X\rho+Y$ лежат в плоскости $x+Hy+z=0$, где, как легко вычислить, $H=\frac{1}{\sqrt{|D|}}[2(3q+s^2)\rho+sq+9n]$. Как легко подсчитать, единичная поверхность $(x^2+y^2)z=1$ не имеет с двухчленной плоскостью общих точек, у которых $z>\sqrt[3]{H^2+1}$. В ряду степеней η_0^m могут быть, следовательно, двухчленные единицы только для показателей m, не больших чем $l=\frac{\lg\sqrt[3]{H^2+1}}{\lg\eta_0}$. После того как вычислена основная едиинца ε_0 кольца $O(\rho)$, мы можем найти число l, затем вычислнть все η_0^m для $m\leqslant l$, и так найти все обратные решения уравнения $(n, -q, s, 1)=1$, либо показать, что таковых нет.

Замечание. Можно, не вычисляя единицы, указать граиицу снизу для велнчины обратной основной едиицы $\eta_0=\varepsilon_0^{-1}$ в зависимости от величины дискриминанта D кольца, если только $|D|>27$, так как поверхность, иа которой лежат все точки данного дискриминанта, имеет уравненне $((x+z)^2+y^2)y=\frac{\pm\sqrt{|D|}}{2}$ и, как легко видеть, не пересекается при $|D|>27$ с единичной поверхностью $(x^2+y^2)z=1$ при $z=1$, а только ниже и выше, и, например, уже при $|D|>54$ наименьшее z верхнего сечения >2. При больших $|D|$, z растет как $\sqrt[3]{\frac{|D|}{4}}$. Это ограничение η_0 снизу годится для всех колец, кроме одного, так как только кольцо, определяемое уравнением $\rho^3=-\rho^2+1$, имеет дискриминант —23, по абсолютной величине меньший, чем 27. Истинные значения единиц η_0 несколько больше этой границы. Приводим табличку уравнений, которым удовлетворяют самые малые обратные основные единицы η_0, приближенные с недостатком велнчины этих единиц, и их дискриминанты.

$z^3=z+1$	1.3	— 23
$z^3=z^2+1$	1.4	— 31
$z^3=z^2+z+1$	1.8	— 44
$z^3=2z^2+1$	2.2	— 59
$z^3=3z^2-z+1$	2.7	— 76
$z^3=2z^2+2z+1$	2.8	— 83
$z^3=3z^2+1$	3.1	—135
$z^3=3z^2+z+1$	3.3	—176
$z^3=4z^2-2z+1$	3.5	—107
$z^3=3z^2+2z+1$	3.6	—175
$z^3=4z^2-z+1$	3.8	—199
$z^3=3z^2+3z+1$	3.8	—108
.....	....	.....

Для разыскания прямых решений эти геометрические соображения нам иичего не дают, так как единичная поверхность пересекается с двухчленной

плоскостью для $z<1$ по бесконечной линии, и совершенно не видно, почему бы на ней не могло лежать даже бесконечного числа точек параллелепипедальной системы $O(\rho)$. Причины невозможности такого обстоятельства, до сих пор найденные, — чисто арифметической природы.

5. О решениях эквивалентных целых форм. Пусть $(n, -q, s, 1)$ и $(\bar{n}, -\bar{q}, \bar{s}, 1)$ — две эквивалентные целые формы и $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ — подстановка, преобразующая первую форму во вторую. В таком случае β, δ — решение первой формы, т. е. $n\beta^3 - q\beta^2\delta + s\beta\delta^2 + \delta^3 = 1$, и α и γ — два таких целых рациональных числа, что $\alpha\delta - \beta\gamma = 1$. Легко видеть, что если взять другие числа α', γ', удовлетворяющие этому уравнению, то получится форма $(\bar{n}', -\bar{q}', \bar{s}', 1)$, параллельная форме $(\bar{n}, -\bar{q}, \bar{s}, 1)$, т. е. получается из этой формы подстановкой $\begin{pmatrix}1 & 0\\ r & 1\end{pmatrix}$. Мы будем говорить, что целая форма $(\bar{n}, -\bar{q}, \bar{s}, 1)$, или, скорее, параллель ей параллельных форм, получается из целой формы $(n, -q, s, 1)$ при помощи ее решения β, δ.

Пусть $X=\beta_1$, $Y=\delta_1$; $X=\beta_2$, $Y=\delta_2$; ...; $X=\beta_l$, $Y=\delta_l$ ... все последовательные решения целой формы $(n, -q, s, 1)$, соответствующие степеням $\varepsilon_0^{m_1}, \varepsilon_0^{m_2}, \ldots, \varepsilon_0^{m_l}, \ldots$ положительной прямой основной единицы, причем $m_1 < m_2 < \ldots < m_l < \ldots$ и нет решений с промежуточными значениями показателей. В силу теоремы п. 4, ряд этих показателей имеет первый член m_1, который отрицателен, если есть обратные решения, и нуль — если нет обратных решений; что же касается вопроса, имеет ли он последний член, то этот вопрос совпадает с вопросом о конечности числа решений. Если предполагать известной теорему Туэ, то можно считать известным, что этот ряд конечный. Но мы строим теорию, независимую от теоремы Туэ, и потому пока тут этого утверждать еще не можем. Пусть β_k, δ_k — одно из решений. Тогда эквивалентная целая форма $(\bar{n}, -\bar{q}, \bar{s}, 1) = (n - q, s, 1)\begin{pmatrix}\alpha_k & \beta_k\\ \gamma_k & \delta_k\end{pmatrix}$ имеет решения $X = \delta_k\beta_l - \beta_k\delta_l$, $Y = -\gamma_k\beta_l + \alpha_k\delta_l$ (где $l = 1, 2 \ldots$). Если ρ и $\bar{\rho}$ — корни уравнений $\rho^3 = s\rho^2 + q\rho + n$ и $\bar{\rho}^3 = \bar{s}\bar{\rho}^2 + \bar{q}\bar{\rho} + \bar{n}$ то, мы имеем $\bar{\rho} = \frac{\alpha_k\rho + \gamma_k}{\beta_k\rho + \delta_k}$; решениями второй формы, следовательно, будут

$$(\delta_k\beta_l - \beta_k\delta_l)\bar{\rho} + (-\gamma_k\beta_l + \alpha_k\delta_l) = \frac{(\alpha_k\delta_k - \beta_k\gamma_k)(\beta_l\rho + \delta_l)}{\beta_k\rho + \delta_k} = \frac{\beta_l\rho + \delta_l}{\beta_k\rho + \delta_k}.$$

Мы получаем таким образом теорему:

Теорема. *Если преобразовать целую форму в эквивалентную целую форму при помощи решения $\varepsilon_0^{m_k}$ первой формы, то решения второй целой формы получаются из решений $\varepsilon_0^{m_1}, \varepsilon_0^{m_2}, \ldots, \varepsilon_0^{m_l}$ первой целой формы, если их разделить на $\varepsilon_0^{m_k}$, т. е. они будут $\varepsilon_0^{m_1 - m_k}, \varepsilon_0^{m_2 - m_k}, \ldots, \varepsilon_0^{m_l - m_k} \ldots$*

6. О сведении к целой форме, которая не имеет обратных решений. Пользуясь предыдущими теоремами, можно преобразовывать любую целую форму, имеющую обратные решения, в эквивалентную ей целую форму, которая не имеет обратных решений. Для этого достаточно вычислить основную единицу ε_0, затем способом, указанным в п. 4, найти обратное решение $\varepsilon_0^{m_1}$ с наибольшим по абсолютной величине (отрицательным) показателем m_1 и преобразовать затем заданную форму при помощи этого решения.

Мы будем дальше везде предполагать, что это преобразование сделано, и, следовательно, форма не имеет обратных решений.

7. О степенях двухчленной единицы.

Теорема. *Никакая степень единицы вида* $b\rho + c$, *где* $b \neq \pm 1$, *не может быть двухчленной единицей.*

То-есть, надо показать, что при возвышении в степень единиц вида $b\rho + c$, где $b \neq \pm 1$, получаются такие единицы $M\rho^2 + P\rho + Q$, у которых $M \neq 0$.

Действительно, если $(b\rho + c)^m$ дает $M = 0$, то мы получаем уравнение:

$$\frac{m(m-1)}{1\cdot 2} c^{m-2} + \frac{m(m-1)(m-2)}{1\cdot 2\cdot 3} bc^{m-3}s + \\ + \frac{m(m-1)(m-2)(m-3)}{1\cdot 2\cdot 3\cdot 4} b^2c^{m-4}(q + s^2) + \ldots = 0.$$

В виду того, что $b\rho + c$ — единица, числа b и c взаимно простые. Предположим сначала, что b имеет простого делителя π, большего трех, и пусть $\frac{m(m-1)}{1\cdot 2}$ делится точно на π^k. Оставим в числителе каждого из следующих биномиальных коэффициентов нетронутыми два первых множителя, т. е. $m(m-1)$, а в знаменателе два последних, и сократим все остальные множители с оставшимися множителями числителя. Первый член делится точно на π^k, а в остальных степень π, которая может быть утеряна, вследствие того, что π может содержаться в произведении двух последних множителей знаменателя, меньше, чем та степень π, которая будет приобретена из степени b, так как даже для $\pi = 5$ мы имеем $\pi > 3$, $\pi^2 > 4$, $\pi^3 > 5$ и т. д., да еще π может содержаться в целом числе, получающемся в результате сокращения остальных множителей знаменателя и числителя, и в множителе, состоящем из коэффициентов n, q, s формы, который есть в каждом члене. Все следующие члены, следовательно, делятся по крайней мере на π^{k+1}, а первый только на π^k; написанное равенство, следовательно, невозможно.

Остается еще случай, когда b состоит только из множителя 2 и 3. В случае, если b делится на 3^2 и $\frac{m(m-1)}{1\cdot 2}$ точно делится на 3^k, следующие члены делятся, по крайней мере, на 3^{k+1}, так как $3^2 > 3$, $3^4 > 4$, $3^6 > 5$ и т. д. Если b делится на 2 и $\frac{m(m-1)}{1\cdot 2}$ точно делится на 2^k, то $\frac{m(m-1)(m-2)}{1\cdot 2\cdot 3} bc^{m-3}s$ и $\frac{m(m-1)(m-2)(m-3)}{1\cdot 2\cdot 3\cdot 4} b^2c^{m-4}(q + s^2)$ делятся, по крайней мере, на 2^{k+1}, так как одно из чисел $m-2$ или $m-3$ четное, все же следующие члены также делятся по крайней мере на 2^{k+1}, так как $2^3 > 5$, $2^4 > 6$ и т. д.

Остается только еще случай $|b| = 3$. В этом случае мы получаем из $c^3 + sc^3b - qcb^2 + nb^3 = 1$, что $c^3 \equiv c \equiv 1 \pmod 3$, т. е. $c = 3\gamma + 1$; если подставить это c и $b = \pm 3$, мы получаем $s \equiv 0 \pmod 3$. Мы видим, следовательно, что если $\frac{m(m-1)}{1\cdot 2}$ точно делится на 3^k, то $\frac{m(m-1)(m-2)}{1\cdot 2\cdot 3} bc^{m-3}s$ делится по крайней мере на 3^{k+1}, а остальные члены также делятся по крайней мере на 3^{k+1}, так как $3^2 > 4$, $3^3 > 5$ и т. д.

Замечание. В случае, когда $b = \pm 1$, степень двухчленной единицы $b\rho + c$ может быть опять двухчленной, как это показывают примеры.

8. Алгорифмы повышения. Мы переходим теперь к изложению особого способа, который мы называем алгорифмом повышения. Пусть $\varepsilon_0 = a\rho^2 + b\rho + c$ и пусть $\varepsilon_0^{m_i} = P_i\rho + a_i$ все решения уравнения $(n, -q, s, 1) = 1$, причем мы здесь еще не знаем, конечное их число или бесконечное. Если написать уравнения $\varepsilon_0'^{m_i} = P_i\rho' + Q_i$ и $\varepsilon_0''^{m_i} = P_i\rho'' + Q_i$ для сопряженных корней ρ' и ρ'' и вычесть друг из друга, мы получим $\varepsilon_0'^{m_i} - \varepsilon_0''^{m_i} =$

$= P_i(\rho' - \rho'')$, откуда мы видим, что P_i всех решений делятся на число $\frac{\varepsilon_0' - \varepsilon_0''}{\rho' - \rho''} = -a\rho + b + as$; а именно мы имеем:

$$P_i = (-a\rho + b + as) \cdot (\varepsilon_0'^{m_i - 1} + \varepsilon_0'^{m_i - 2}\varepsilon_0'' + \ldots + \varepsilon_0' \varepsilon_0''^{m_i - 2} + \varepsilon_0''^{m_i - 1}),$$

или, так как второй множитель правой части — целая симметрическая фуикция от ρ' и ρ'' с целыми рациоиальными коэффициентами, то

$$P_i = (-a\rho + b + as) \cdot (A_i\rho^2 + B_i\rho + C_i),$$

где числа A_i, B_i, C_i — целые рациональные. Мы получаем отсюда:

$$A_i b - B_i a = 0; \quad -A_i aq + B_i(b + as) - C_i a = 0; \quad -A_i an + (b + as) C_i = P_i,$$

откуда

$$A_i = \frac{a^2 P_i}{N(-a\rho + b + as)}; \quad B_i = \frac{abPi}{N(-a\rho + b + as)}; \quad C_i = \frac{(b^2 + abs + a^2 q)\, Pi}{N(-a\rho + b + as)}.$$

Но общий иаибольший делитель $(a^2, ab, b^2 + abs + a^2 q)$ равеи $(a, b)^2$, поэтому, если мы обозначим $(a, b) = \delta$, т. е. $a = a_1\delta$; $b = b_1\delta$, то все P_i всех решений делятся на число $\varkappa$, где $\varkappa = |\delta \cdot N(-a_1\rho + b_1 + a_1 s)|$. Если $\varkappa > 1$, то это значит, что все решения имеют вид $\bar{P}_i\bar{\rho} + Q$, где $\bar{\rho} = \varkappa\rho$ и $\bar{P}_i = \frac{P_i}{\varkappa}$; все они, следовательно, лежат в „повышенном“ кольце $O(\bar{\rho}) = O(\varkappa\rho)$. Основная едииица $\bar{\varepsilon}_0$ кольца $O(\bar{\rho})$ есть первая такая степень ε_0^{μ} осиовной единицы ε_0 кольца $O(\rho)$, которая лежит в кольце $O(\bar{\rho})$, т. е. у которой коэффициенты при ρ^2 и ρ делятся иа $\varkappa^2$ и $\varkappa$. Если $\varkappa$ взаимно простое с индексом числа ρ в Ω_ρ, то μ — делитель $\varphi(\varkappa^2)$, где φ — эйлерова фуикция в $\Omega\rho$, так как на основании леммы Ферма в Ω_ρ мы имеем $\varepsilon_0^{\varphi(\varkappa^2)} \equiv 1 \pmod{\varkappa^2}$, т. е. $\varepsilon_0^{\varphi(\varkappa^2)}$ имеет вид $\varkappa^2(t_1\rho^2 + t_2\rho + t_3) + 1$. Если $\varkappa$ — взаимно простое с индексом ρ, то можно предположить, что t_1, t_2, t_3 — целые, т. е. в этом случае $\varepsilon_0^{\varphi(\varkappa^2)}$ лежит уже в $O(\bar{\rho})$. В случае, когда $\varkappa$ не взаимно простое с индексом ρ, можно также без труда иайти показатель μ. Все приводится, таким образом, теперь к задаче: найти среди степеней ε_0 все те, которые двухчленны в $\bar{\rho}$, т. е. имеют вид $P_i\bar{\rho} + Q_i$. Если повторять это рассуждение, мы будем переходить в кольца $O(\bar{\bar{\rho}})$, $O(\bar{\bar{\bar{\rho}}})$ и т. д. Мы можем так все время повышать то кольцо, в котором нам надо искать решения, до тех пор, пока, наконец, какое-нибудь $\varkappa^*$ не станет равно 1, что может случиться, только если соответствеиное число $-a^*\rho^* + b^* + a^*s^*$ будет либо рациональной, либо алгебраической единицей.

Замечание. Может случиться, что у самой основной единицы кольца $O(\rho)$ коэффициенты при ρ^2 и ρ соответственно делятся иа ν^2 и $\nu \neq 1$, так что ε_0 сама уже лежит в повышеином отиосительно $O(\rho)$ кольце $O(\nu\rho)$. В таком случае мы сразу перейдем в кольцо $O(\nu\rho)$, присоединив множитель ν к ρ. Это же может случиться на любом шаге алгорифма при вычислении основной единицы в некотором уже повышением кольце. В таком случае мы поступим так же. Таким образом, получается, что иногда, кроме повышающих миожителей $\varkappa$, получаются еще эти „добавочные“ множители ν, которые только еще сильнее повышают кольцо.

9. Теорема. — *$a\rho + b + as$ не может быть алгебраической единицей в повышенном кольце.*

Алгорифм повышеиия может остановиться тогда и только тогда, когда иа каком-иибудь его шаге число — $a\rho + b + as$ — обыкиовенная рациональная или алгебраическая единица. (Хотя рассматриваемое кольцо здесь может быть не заданное, а уже повышенное, мы для простоты опускаем значок * иад буквами.) Покажем, что — $a\rho + b + as$ алгебраической едииицей может быть только до первого повышеиия, т. е. у исходного кольца. Для этого будем все время предполагать, что форма так преобразована, что оиа ие имеет обратных решений.

В таком случае, если $-a\rho+b+as$ — алгебраическая единица, то она, как двухчленная, есть $\pm$ степень с положительным целым рациональным показателем μ положительной прямой основной единицы соответственного кольца $O(\rho)$, т. е. $\pm\varepsilon_0^{\mu}$, причем $\mu>1$, так как, если $\varepsilon_0=a\rho^2+b\rho+c$ и было бы $-a\rho+b+as=\pm(a\rho^2+b\rho+c)$, то мы получили бы $a=b=c=0$, что невозможно.

Пусть теперь $\eta_0=\varepsilon_0^{-1}$. Легкое вычисление дает $\pm\eta_0^{\mu}=\frac{1}{-a\rho+b+as}=$ $=a\varepsilon_0+a'$, где $a'=abs+b^2-a^2q-ac$. Мы получаем отсюда $\pm\eta_0^{\mu+1}=$ $=a'\eta_0+a$. Если теперь предположить, что кольцо $O(\rho)$ повышенное, т. е. что $\rho=k\rho_0+r$, где $k>1$, r — целые рациональные и ρ_0 — целое алгебраическое число, то мы получаем

$$\eta_0=\varepsilon_0^{-1}=a'\rho^2+b'\rho+c'=k\cdot\vartheta+c'',$$

где ϑ — целое алгебранческое, а c'' — целое рациональное. Следовательно, $\eta_0^{\mu+1}=(k\vartheta+c'')^{\mu+1}$. Мы получаем, таким образом, $\pm(k\vartheta+c'')^{\mu+1}=a'\eta_0+a=$ $=a'k\vartheta+(a'c''+a)$, что на основании теоремы п. 7 невозможно.

Замечание. Мы предположим сначала, что у исходной целой формы число $-a\rho+b+as$ не есть ни обыкновенная рациональная, ни алгебраическая единица, в таком случае по крайней мере первый шаг алгорифма повышения сделать можно. Посмотрим, как в этом случае может протекать дальше алгорифм повышения и какие из этого можно сделать следствия.

10. Первый случай. $-a^*\rho^*+b^*+a^*s^*$ ни на каком шаге алгорифма не станет единицей. Если $-a^*\rho^*+b^*+a^*s^*$ каждый раз не единица, то P_i всех решений должны делиться на χ, $\chi\chi$, $\chi\chi\chi$, $\chi\chi\chi\chi$ и т. д., т. е. всякое P_i превосходит любую наперед заданную величину, уравнение $(n, -q, s, 1)=1$ не имеет, следовательно, в этом случае ни одного решения.

11. Второй случай. $-a^*\rho^*+b^*+a^*s^*$ станет на известном шаге единицей, в силу теоремы п. 9 и того, что мы предположили, что первый шаг алгорифма повышения можно было сделать; в этом случае одна будет обыкновенной единицей: $+1$ или -1. Если $-a^*\rho^*+b^*+a^*s^*=\pm1$, то мы имеем $a^*=0$, $b^*=\pm1$. Все решения суть, следовательно, двухчленные единицы кольца $O(\rho^*)$, которое имеет основную единицу $\xi_0^*=a^*\rho^{*2}+b^*\rho^*+$ $+c^*$, т. е. $\pm\rho^*+c^*$. Но в виду того, что мы предполагаем, что наша форма была преобразована, как указано в п. 6, иначе говоря, что она не имеет обратных решений, то все решения должны быть степенями с целыми положительными показателями m этой прямой положительной основной единицы ε_0^* кольца $O(\rho^*)$, и именно такими степенями, которые двухчленны, т. е. имеют вид $P^*\rho^*+Q$. Пусть $\rho^*=k\rho$, где k — произведение всех повышающих и дополнительных множителей χ и ν, причем в рассматриваемом нами случае $k>1$. Мы получаем $(\pm k\rho+c^*)^m=P_k^*\rho+Q$, что на основании теоремы п. 7 невозможно ни для какого $m>1$. В рассматриваемом случае поэтому уравнение $(n, -q, s, 1)=1$ имеет сверх тривиального $X=0$, $Y=1$ еще одно решение $\pm k\rho+c^*$ и никаких других решений.

12. Случай, когда у исходного уравнения $-a\rho+b+as$ есть единица. Если $-a\rho+b+as$ — обыкновенная единица, т. е. $-a\rho+$ $+b+as=\pm1$, то $a=0$, $b=\pm1$, и основная прямая положительная единица кольца $O(\rho)$ $\varepsilon_0=a\rho^2+b\rho+c=\pm\rho+c$. Но в таком случае заданная целая форма параллельна целой форме, корнем которой является ε_0. Пусть эта форма есть $(1, -t, r, 1)$, т. е. ε_0 — корень уравнения $z^3=rz^2+tz+1$. Форма эта имеет оба крайние коэффициента равные 1. Такую форму, оба крайние коэффициента которой равны 1, мы будем называть обратимой. Мы рассмотрим теорию таких обратимых форм в пп. 13—23.

Предположим теперь, что $-a\rho+b+as=\varepsilon$ — алгебраическая единица. Представим прямую основную положительную единицу $\varepsilon_0=a\rho^2+b\rho+c$ кольца $O(\rho)$ в дробнолинейной форме (см. § 12) через ρ, $\varepsilon_0=\frac{\alpha\rho+\beta}{\gamma\rho+\delta}$; тогда можно, как легко вычислить, взять $\alpha=\pm(abs+b^2-a^2q-ac)$; $\beta=\pm(acs+bc-a^2n)$; $\gamma=\pm(-a)$; $\delta=\pm(b+as)$. Мы выбираем еще здесь так знак $\pm$, чтобы $N(\gamma\rho+\delta)=\pm N(\varepsilon)=+1$. Если опять $z^3=rz^2+tz+1$ — уравнение, которому удовлетворяет ε_0, то форма

$$(1,\ -t,\ r,\ 1)=(X\varepsilon_0+Y)(X\varepsilon_0'+Y)(X\varepsilon_0''+Y)=$$
$$=N\left(X\frac{\alpha\rho+\beta}{\gamma\rho+\delta}+Y\right)=N(X(\alpha\rho+\beta)+Y(\gamma\rho+\delta))\cdot\frac{1}{N(\gamma\rho+\delta)}=$$
$$=N[(X\alpha+Y\gamma)\rho+(X\beta+Y\delta)]=$$
$$=(\bar{X}\rho+\bar{Y})(\bar{X}\rho'+\bar{Y})(\bar{X}\rho''+\bar{Y})=(n,\ -q,\ s,\ 1),$$

если положить

$$\bar{X}=\alpha X+\gamma Y;\quad \bar{Y}=\beta X+\delta Y \quad\text{и если}\quad z^3=sz^2+qz+n$$

есть уравнение, которому удовлетворяет ρ.

Мы видим, таким образом, что $(1,-t,r,1)=(n,-q,s,1)\begin{pmatrix}\alpha & 1\\ \beta & \delta\end{pmatrix}$, но так как $\alpha\delta-\beta\gamma=\pm 1$, то форма $(n,-q,s,1)$ эквивалентна обратимой форме $(1,-t,r,1)$.

Итак, в случае, когда у исходного уравнения $-a\rho+b+as$ — рациональная или алгебраическая единица, т. е. нельзя сделать даже первого шага алгорифма повышения, оно эквивалентно обратимому уравнению.

13. О приведении обратимого уравнения к основному обратимому. Если заданное уравнение обратимое, т. е. если $n=1$, ρ — алгебраическая единица, однако ρ может быть не основной единицей кольца $O(\rho)$. Так, например, корень ε уравнения $z^3=z^2-2z+1$ — единица, но не основная единица кольца $O(\varepsilon)$; основная единица кольца $O(\varepsilon)$ есть $\varepsilon_0=\varepsilon^2-\varepsilon+1$, и мы имеем $\varepsilon=\varepsilon_0^2$. Из того, что ε_0 заключается в $O(\varepsilon)$, следует $D'_{\varepsilon_0}\geqslant D_\varepsilon$, а из того, что ε — степень ε_0, следует аналогично, что $D_\varepsilon\geqslant D_{\varepsilon_0}$, т. е. $D_{\varepsilon_0}=D_\varepsilon$. Если мы, следовательно, повторим рассуждения предыдущего пункта, то мы покажем, что, если $z^3=rz^2+tz+1$ — уравнение, которому удовлетворяет ε_0, то формы $(1,\ -t,\ r,\ 1)$ и $(1,\ -q,\ s,\ 1)$ эквивалентны, и найдем подстановку $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ для перехода от одной из них к другой, т. е. от заданного обратимого уравнения к эквивалентному ему основному обратимому уравнению.

14. О решениях обратимой формы с четными показателями. Пусть $(1,\ -q,\ s,\ 1)$ — основная, прямая (т. е. такая, что корень уравнения $z^3=sz^2+qz+1$ — прямая основная единица кольца, соответствующего этой форме) обратимая форма. Все ее решения будут степенями с целыми положительными показателями положительной прямой основной единицы ε и ей обратной единицы η, причем ε — корень уравнения $z^3=sz^2+qz+1$. Мы рассмотрим отдельно четные и нечетные показатели. Начнем с четных показателей. Если мы будем искать решения вида $(\varepsilon^2)^{m_i}$, то мы получим (совсем аналогично тому, как в п. 8), что все P_t этих решений будут делиться на

$$\frac{\varepsilon'^2-\varepsilon''^2}{\varepsilon'-\varepsilon''}=\varepsilon'+\varepsilon''.$$

Если $N(\varepsilon'+\varepsilon'')\neq\pm 1$, мы получим число $\varkappa$, отличное от 1, на которое должны делиться все P_t всех этих решений; совершенно аналогично, все P_t всех решений $(\eta_i^2)^{m_i}$ должны делиться на

$$\frac{\eta_i'^2-\eta_i''^2}{\varepsilon'-\varepsilon''},$$

но мы имеем

$$\frac{\eta'^2-\eta''^2}{\varepsilon'-\varepsilon''}=\frac{\frac{1}{\varepsilon'^2}-\frac{1}{\varepsilon''^2}}{\varepsilon'-\varepsilon''}=-\frac{\varepsilon'^2-\varepsilon''^2}{(\varepsilon'\varepsilon'')^2(\varepsilon'-\varepsilon'')},$$

т. е.

$$N\left(\frac{\eta'^2-\eta''^2}{\varepsilon'-\varepsilon''}\right)=N(\varepsilon'+\varepsilon'')$$

и поэтому все эти P_i также должны делиться на $\varkappa$. Таким образом, все прямые и обратные решения с четными показателями суть двухчленные единицы повышенного кольца $O(\varkappa\varepsilon)$. Наоборот, всякая двухчленная единица кольца $O(\varkappa\varepsilon)$ есть решение рассматриваемого обратимого уравнения.

15. Об обращенной форме. Всякая обратимая форма имеет всегда, кроме тривиального решения 1, еще решение ε. Если мы преобразуем обратимую форму при помощи решения ε, т. е. подстановкой $\begin{pmatrix}\alpha & 1\\ \gamma & 0\end{pmatrix}$, где мы возьмем $\alpha=0$, $\gamma=-1$, то мы получим по п. 5 „обращенную“ форму $(1, s, -q, 1)$, иначе говоря, форму, получаемую из заданной обратимой, если написать ее коэффициенты в обратном порядке.

16. О решениях обратимой формы с нечетными показателями. Для того, чтобы исследовать решения $P_i\varepsilon+Q_i$, соответствующие нечетным показателям m_i, мы перейдем к обращенной форме. В силу п. 5, все решения заданной формы с нечетными показателями будут соответствовать решениям обращенной формы с четными показателями, и обратно. Эти решения суть

$$\frac{1}{\varepsilon}(P_i\varepsilon+Q_i)=Q_i\eta+P_i.$$

Все Q_i всех тех из решений, которые прямые, должны делиться на $\frac{\varepsilon'^2-\varepsilon''^2}{\eta'-\eta''}$; но мы имеем

$$N\left(\frac{\varepsilon'^2-\varepsilon''^2}{\eta'-\eta''}\right)=N(\varepsilon'+\varepsilon''),$$

и, следовательно, если $N(\varepsilon'+\varepsilon'')\neq\pm1$, то все эти Q_i должны делиться на $\varkappa>1$. Совершенно аналогично все Q_i всех обратных решений должны делиться на $\frac{\eta'^2-\eta''^2}{\eta'-\eta''}$; но мы имеем

$$N\left(\frac{\eta'^2-\eta''^2}{\eta'-\eta''}\right)=N(\varepsilon'+\varepsilon''),$$

и, следовательно, все Q_i всех этих решений должны делиться на то же самое число $\varkappa$. Мы видим, таким образом, что все решения заданной обратимой формы с нечетными показателями, как прямые так и обратные, суть двухчленные единицы в кольце $O(\varkappa\eta)$. Наоборот, всякая двухчленная единица кольца $O(\varkappa\eta)$ есть решение заданного обратимого уравнения, надо только поменять местами P_i и Q_i.

17. О неэквивалентности тех двух форм, на которые сводится обратимая форма в том случае, когда $N(\varepsilon'+\varepsilon'')\neq\pm1$. Если $N(\varepsilon'+\varepsilon'')\neq\pm1$, то решение обратимого уравнения $(1, -q, s, 1)=1$ сводится, таким образом, на решение таких двух повышенных уравнений:

$$(\varkappa^3, -q\varkappa^2, s\varkappa, 1)=1 \quad\text{и}\quad (\varkappa^3, s\varkappa^2, -q\varkappa, 1)=1.$$

Легко видеть, что эти формы неэквивалентны друг другу. Действительно, если бы это имело место, корни $\varkappa\varepsilon$ и $\varkappa\eta$ этих форм должны были бы выражаться цело друг через друга, но это невозможно, так как $\varepsilon=\eta^2+q\eta+s$ и $\varkappa\varepsilon=$

$= \varkappa\eta^2 + \varkappa q\eta + \varkappa s$; но невозможно найти такие три целые рациональные числа A, B, C, чтобы было $A\varkappa^2\eta^2 + B\varkappa\eta + C = \varkappa\eta^2 + \varkappa q\eta + \varkappa s$.

18. О случаях, когда $N(\varepsilon' + \varepsilon'') = \pm 1$. Мы имеем таким образом возможность, в случае обратимого уравнения, свести задачу на разрешение „повышенных" уравнений, для которых уже можно применять алгорифмы повышения. Но остались еще исключительные случаи, когда мы этого сделать не можем, а именно случаи, когда $N(\varepsilon' + \varepsilon'') = \pm 1$. Мы имеем $N(\varepsilon' + \varepsilon'') = N(s - \varepsilon) = sq + 1$ и $sq + 1 = +1$, если $s = 0$ или $q = 0$. Эти случаи мы рассмотрим в двух следующих пунктах. $sq + 1 = -1$ тогда и только тогда, когда $sq = -2$, т. е. в случаях $s = 1, q = -2$; $s = -1, q = 2$; $s = 2, q = -1$; $s = -2, q = 1$, что дает уравнения с дискриминантами $-23, +49, -23, +49$. Тут получается только два уравнения с отрицательным определителем, но оба они эквивалентны уравнению $z^3 = -z^2 + 1$, которое опять типа $q = 0$. Остается, следовательно, рассмотреть обратимые уравнения с $s = 0$ или $q = 0$.

19. Степень корня уравнения $z^3 = qz + 1$, если $|q| \neq 1$. Пусть у нас имеется обратимое уравнение $z^3 = qz + 1$ и ε его корень, мы исследуем его решения вида ε^m, где m положительно. Если коэффициент M при ε^2 в ε^m равен нулю, то мы имеем, как легко видеть, одно из следующих равенств:

(1) если $m = 3\gamma + 2$:

$$1 + q^3\frac{(\gamma-1)\gamma(\gamma+1)}{1\cdot2\cdot3} + q^6\frac{(\gamma-3)(\gamma-2)(\gamma-1)(\gamma+1)(\gamma+2)}{1\cdot2\cdot3\cdot4\cdot5\cdot6} + \ldots = 0;$$

(2) если $m = 3\gamma + 1$:

$$\gamma + q^3\frac{(\gamma-2)(\gamma-1)\gamma(\gamma+1)}{1\cdot2\cdot3\cdot4} + q^6\frac{(\gamma-4)(\gamma-3)(\gamma-2)(\gamma-1)\gamma(\gamma+1)(\gamma+2)}{1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7} + \ldots = 0;$$

(3) если $m = 3\gamma$:

$$\frac{\gamma(\gamma-1)}{1\cdot2} + q^3\frac{(\gamma-3)(\gamma-2)(\gamma-1)\gamma(\gamma+1)}{1\cdot2\cdot3\cdot4\cdot5} + q^6\frac{(\gamma-5)(\gamma-4)(\gamma-3)(\gamma-2)(\gamma-1)\gamma(\gamma+1)(\gamma+2)}{1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8} + \ldots = 0.$$

Очевидно, что если $|q| \neq 1$, случай $m = 3\gamma + 2$ невозможен. Что же касается двух других случаев, то заметим, что простое число p входит в $m!$ не выше чем с показателем $\frac{m-1}{p-1}$; если мы обозначим $\frac{p^m}{m!} = \bar{p}^m$, то мы увидим, что дробь $\bar{p}^m$ после сокращения на возможно более высокую степень p будет иметь в числителе p с показателем, равным, по крайней мере,

$$\left[m - \frac{m-1}{p-1}\right],$$

где [] обозначает, как всегда, наибольшую целую часть. Второе и третье из предыдущих равенств мы перепишем так:

$$\bar{q}\cdot\gamma + \bar{q}^4(\gamma+1)\ldots(\gamma-2) + \bar{q}^7(\gamma+2)\ldots(\gamma-4) + \ldots = 0;$$
$$\bar{q}^2\gamma(\gamma-1) + \bar{q}^5(\gamma+1)\ldots(\gamma-3) + \bar{q}^8(\gamma+2)\ldots(\gamma-5) + \ldots = 0.$$

Предположим сначала, что $|q|$ простое число p, большее трех. В таком случае здесь каждый следующий член делится на более высокую степень p, чем первый, так как

$$\left[4 - \frac{3}{p-1}\right] > \left[4 - \frac{3}{3}\right] = 3$$

и

$$\left[m-\frac{m-1}{p-1}\right]$$

не уменьшается при увеличении m; первое равенство, следовательно, невозможно;

$$\left[5-\frac{4}{p-1}\right]\geqslant\left[5-\frac{4}{4}\right]=4,$$

т. е. и второе равенство также невозможно.

Если $|q|=3$ и γ делится точно на 3^k, то в первом равенстве первый член делится на 3^{k+1}, а второй, по крайней мере, на $3^{k+\left[4-\frac{3}{2}\right]}=3^{k+2}$, следующие же, в виду того, что

$$\left[m-\frac{m-1}{2}\right]$$

при увеличении m не уменьшается, также, по крайней мере, на 3^{k+2}; таким образом, и для $|q|=3$ первое равенство невозможно. Во втором равенстве, если $|q|=3$ и $\gamma(\gamma-1)$ точно делится на 3^k, первый член делится точно на 3^{k+2}, второй, по крайней мере, на 3^{k+4}, третий, по крайней мере, на $3^{k+\left[8-\frac{7}{2}\right]}=3^{k+4}$, а все следующие также, по крайней мере, на 3^{k+4}; второе равенство также невозможно при $|q|=3$. Пусть, наконец, $|q|=2$ и γ точно делится на 2^k; тогда первый член первого равенства делится точно на 2^{k+1}, а все следующие на более высокие степени 2, так как после сокращения $\overline{2^m}$, 2 не останется в знаменателе, а во втором и третьем членах в числителе, кроме множителей $\gamma(\gamma-1)$, есть по крайней мере еще два последовательных множителя, т. е. по крайней мере еще один множитель 2. То же самое для второго равенства. Если $|q|$ не простое число, то мы можем из $|q|$ выделить простого делителя p и провести все предыдущее рассуждение для этого p. Если после этого выделения p в $|q|p^{-1}$ еще входит, то всякий следующий член будет тем более делиться на более высокую степень p, чем первый. Мы видим, таким образом, что среди степеней ε^m, где ε — корень уравнения $z^3=qz+1$, $|q|\neq 1$ и $m>1$, кроме степени ε^3, которая равна $q\varepsilon+1$, нет других двухчленных единиц.

20. Решение прямого основного обратимого уравнения в случае $s=0$, $q\neq -1$. Если $z^3=qz+1$ прямое обратимое уравнение, то из $D=4q^3-27<0$ мы получаем $q=1$, 0 или <0. Но $q=1$ дает обратное уравнение, $q=0$ приводимое. Уравнение $z^3=-z+1$ мы рассмотрим в п. 21. Остаются, следовательно, только случаи $q<-1$. Все прямые решения суть степени ε с положительными показателями m. По предыдущему пункту таких решений только два: ε и $\varepsilon^3=q\varepsilon+1$. Все обратные решения суть степени с положительными показателями обратной основной единицы $\eta=\varepsilon^{-1}=\varepsilon^2-q$, которые двухчленны в ε. Мы можем для исследования этих решений применить результат п. 4, а именно, мы покажем, что уже $\eta>\sqrt[3]{H^2+1}$, т. е. что нет обратных решений. Действительно, неравенство $\eta>\sqrt[3]{H^2+1}$ удовлетворяется, так как его можно написать так:

$$\varepsilon^2-q>\sqrt[3]{\left[\frac{3}{\sqrt{|D|}}(2q\varepsilon+3)\right]^2+1},$$

или

$$\varepsilon^6+3|q|\varepsilon^4+3|q|^2\varepsilon^2+|q|^3-1>\frac{9}{|D|}(4|q|^2\varepsilon^2-12|q|\varepsilon+9),$$

или

$$|q|^2\varepsilon^2+|q|\varepsilon+|q|^3>\frac{36}{|D|}q^2\varepsilon^2-\frac{108}{|D|}|q|\varepsilon+\frac{81}{|D|}.$$

Но это неравенство имеет место, так как для $q<-1$, $|D|\geqslant 59$, а следовательно,

$$|q|^2\varepsilon^2>\frac{36}{|D|}|q|^2\varepsilon^2;$$

далее

$$|q|\varepsilon>-\frac{108}{|D|}|q|\varepsilon \quad \text{и} \quad |q|^3>\frac{81}{|D|}.$$

m	M_m	P_m	Q_m
[1]	0	1	0
2	1	0	0
[3]	0	−1	1
4	−1	1	0
5	1	1	−1
6	1	−2	1
7	−2	0	1
[8]	0	3	−2
....	.....	.....	.....

Мы видим, таким образом, что прямое основное уравнение вида $z^3=qz+1$, если $q\neq -1$, не имеет никаких решенний, кроме трех следующих: тривиального решения 1 и двух очевидиых решений ε и $\varepsilon^3=q\varepsilon+1$.

21. Решение уравнения $(1, 1, 0, 1)=1$. Пусть $\varepsilon^m=M_m\varepsilon^2+P_m\varepsilon+Q_m$. Вычислим небольшую табличку степеней ε^m. Мы видим, что, кроме первой степени и куба, двухчленна еще восьмая степень. Мы докажем, что дальше, до бесконечности, уже нет таких степеней, которые двухчленны. Действительно, предположим, что дальше были бы такие степени, напр. $\varepsilon^m=P_m\varepsilon+Q_m$, тогда m имело бы один из восьми видов $m=8\gamma+r$, где $r=0, 1, 2, 3, 4, 5, 6, 7$, т. е. ε^m была бы вида $(3\varepsilon-2)^\gamma\cdot\varepsilon^r$. Но мы имеем: $(3\varepsilon-2)^\gamma=(-2)^\gamma+\gamma(-2)^{\gamma-1}\cdot 3\varepsilon+$

$$+\frac{\gamma(\gamma-1)}{1\cdot 2}(-2)^{\gamma-2}\cdot 3^2\varepsilon^2+\frac{\gamma(\gamma-1)(\gamma-2)}{1\cdot 2\cdot 3}(-2)^{\gamma-3}3^3\varepsilon^3+\ldots$$

и поэтому M_m имело бы для соответственного r вид:

$$r=0;\quad \frac{\gamma(\gamma-1)}{1\cdot 2}(-2)^{\gamma-2}\cdot 3^2+\frac{\gamma(\gamma-1)(\gamma-2)}{1\cdot 2\cdot 3}(-2)^{\gamma-3}3^3M_3+$$
$$+\frac{\gamma(\gamma-1)(\gamma-2)(\gamma-3)}{1\cdot 2\cdot 3\cdot 4}(-2)^{\gamma-4}3^4M_4+\ldots$$

$$r=1;\quad \gamma(-2)^{\gamma-1}\cdot 3+\frac{\gamma(\gamma-1)}{1\cdot 2}(-2)^{\gamma-2}\cdot 3^2M_3+$$
$$+\frac{\gamma(\gamma-1)(\gamma-2)}{1\cdot 2\cdot 3}(-2)^{\gamma-3}3^3M_4+\ldots \qquad \text{и т. д.}$$

Во всех этих случаях $M_m=0$ невозможно, что легко видеть, если исследовать делимость последовательных членов на степени числа 3, так же как мы это делали в пп. 7 и 19, и если принять во внимание, что M_4, M_5, M_6, M_7 не делятся на 3, а $M_8=0$. Уравнение $(1, 1, 0, 1)=1$ не имеет, следовательно, прямых решений, кроме ε, ε^3, ε^8. Что же касается обратных решений, то применение метода п. 4 показывает, что таковых нет. Все решения уравнения $(1, 1, 0, 1)=1$, таким образом, следующие: $\varepsilon^0=1$, $\varepsilon^1=\varepsilon$, $\varepsilon^3=-\varepsilon+1$, $\varepsilon^8=3\varepsilon-2$.

22. Случай $q=0$. Уравнение $z^3=sz^2+1$ может быть прямым, т. е. его корень прямой единицей (т. е. единицей, удовлетворяющей неравенству $\varepsilon<1$), только если $s<0$, но дискриминант его равен $-4s^3-27$ и может быть <0 только, если $s>-2$. Случай $q=0$ приводит, следовательно, только к одному уравнению $s=-1$, т. е. к уравнению $(1, 0, -1, 1)=1$.

23. Решение уравнения $(1, 0, -1, 1)=1$. Мы начнем опять с вычисления таблички степеней $\varepsilon^m=M_m\varepsilon^2+P_m\varepsilon+Q_m$. Мы продолжали это вычислением до $m=120$ (так, например, $\varepsilon^{120}=11275550\cdot\varepsilon^2+9734175\cdot\varepsilon-$

— 13773374), но за решением ε^{14} мы не нашли никакого дальнейшего решения. Мы покажем, что дальше, до бесконечности, уже и нет решений. Действительно, если бы дальше чем ε^{14} было решение, оно имело бы вид $(4\varepsilon-3)^\gamma\cdot\varepsilon^r$, где r — одно из чисел 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 12, 13. Мы имеем уравнение:

$$(4\varepsilon-3)^\gamma=(-3)^\gamma+\gamma(-3)^{\gamma-1}\cdot 4\varepsilon+\frac{\gamma(\gamma-1)}{1\cdot 2}(-3)^{\gamma-2}\cdot 4^2\varepsilon^2+\ldots$$

Если мы помножим его на ε^r, то получим, что коэффициент при ε^2 равен

$$M_r(-3)^\gamma+M_{r+1}\gamma(-3)^{\gamma-1}\cdot 4+M_{r+2}\frac{\gamma(\gamma-1)}{1\cdot 2}\cdot\cdot(-3)^{\gamma-2}4^2+\ldots=M_m. \qquad (1)$$

Очевидно, что этот коэффициент не равен нулю в случае, когда $r=2, 3, 4, 6, 7, 8, 9, 10, 11, 13$, так как в этих случаях, как это видно из таблички, M_r не делится на 4. В случаях $r=1$ и $r=5$ мы имеем $M_r=0$, а M_{r+1} равно 1 и -1; действительно, если γ точно делится на 2^k, то первый следующий отличный от нуля член $M_{r+1}\cdot\gamma(-3)^{\gamma-1}\cdot 4$ делится на 2^{k+2}, а все следующие, как это легко видеть при помощи метода п. 7, делятся на еще более высокие степени двойки. Случай $r=0$ дает

m	M_m	P_m	Q_m
1	0	1	0
2	1	0	0
3	−1	0	1
4	1	1	−1
5	0	−1	1
6	−1	1	0
7	2	0	−1
8	−2	−1	2
9	1	2	−2
10	1	−2	1
11	−3	1	1
12	4	1	−3
13	−3	−3	4
14	0	4	−3

$$\frac{\gamma(\gamma-1)}{1\cdot 2}(-3)^{\gamma-2}\cdot 4^2+M_3\frac{\gamma(\gamma-1)(\gamma-2)}{1\cdot 2\cdot 3}\cdot(-3)^{\gamma-3}\cdot 4^3+\ldots,$$

что, по совершенно аналогичной причине, не может быть нулем. Остается еще только один случай $r=12$. Тут непосредственное исследование коэффициентов равенства (1) ничего нам не дает, так как $M_{12}=4$, а $M_{13}=-3$, и поэтому оба первые члена могут делиться на одну и ту же степень двойки. Однако мы можем в этом случае записать ε^m также и так: $(4\varepsilon-3)^\gamma\varepsilon^{-2}$, где $\varepsilon^{-2}=\varepsilon+1$, и мы получаем тогда, что коэффициент при ε^2 в ε^m равен:

$$\gamma\cdot 4(-3)^{\gamma-1}+M_3\frac{\gamma(\gamma-1)}{1\cdot 2}\cdot 4^2(-3)^{\gamma-2}+M_4\frac{\gamma(\gamma-1)(\gamma-2)}{1\cdot 2\cdot 3}4^3(-3)^{\gamma-3}+\ldots$$
$$+\frac{\gamma(\gamma-1)}{1\cdot 2}\cdot 4^2(-3)^{\gamma-2}+M_3\frac{\gamma(\gamma-1)(\gamma-2)}{1\cdot 2\cdot 3}4^3(-3)^{\gamma-3}+\ldots$$

Пусть γ точно делится на 2^k; тогда первый член точно делится на 2^{k+2}, а все следующие, по крайней мере, на 2^{k+3}; этот коэффициент также не может, следовательно, равняться нулю. Прямых решений с $m>14$, следовательно, нет. Применение метода п. 4 показывает, что есть только одно обратное решение $\varepsilon^{-2}=\varepsilon+1$. Все решения уравнения $(1, 0, -1, 1)=1$ суть, следовательно, следующие пять:

$$\varepsilon^{-2}=\varepsilon+1;\quad \varepsilon^0=1;\quad \varepsilon^1=\varepsilon;\quad \varepsilon^5=-\varepsilon+1;\quad \varepsilon^{14}=4\varepsilon-3.$$

24. Сводка полученных результатов. Из всего полученного в пп. 1—23 следует, что:

1°. Число решений общего уравнения $(A, B, C, E)=1$, если это число больше нуля, равно числу решений некоторого „целого“ эквивалентного ему уравнения $(n, -q, s, 1)=1$, которое мы, однако, вообще говоря, не умеем найти по уравнению

$$(A, B, C, E)=1.$$

2^0. Для всякого целого уравнения $(n, -q, s, 1)=1$ можно узнать, эквивалентно ли оно „обратимому“ уравнению $(1, -t, r, 1)=1$. Для этого достаточно вычислить основную единицу соответствующего ему кольца.

3^0. Если уравнение $(n, -q, s, 1)=1$ не эквивалентно обратимому, то алгорифм повышения можно начать, и он либо не кончится, тогда оно имеет только одно „тривиальное“ решение (0, 1), или же кончится, *но как далеко, неизвестно*, и тогда уравнение имеет два решения, это тривиальное и еще одно, которое мы узнали бы, если бы провели алгорифм повышения до его окончания.

4^0. Если уравнение эквивалентно обратимому, то это обратимое можно свести на два повышенных, каждое из которых уже не эквивалентно обратимому, и решать уже их.

5^0. Этого нельзя сделать лишь в некоторых особых случаях, в которых, однако, уравнения нами решены до конца, причем все эти особые уравнения имеют не больше, чем 4 решения (включая и тривиальное).

6^0. Только одно из них имеет 5 решений.

7^0. Бесконечно много уравнений, а именно, например, уравнения $(1, -q, 0, 1)=1$ при $|q|>1$ имеют по 3 решения.

Заметим еще, что вопрос о том, эквивалентно ли *заданное* общее уравнение $(A, B, C, E)=1$ обратимому $(1, -t, r, 1)=1$, можно также всегда решить, так как кольцо, соответствующее форме (A, B, C, E), то же самое, что и кольцо, соответствующее форме $(1, -t, r, 1)$, так как формы эти эквивалентны и, следовательно, если вычислим основную единицу ε кольца, соответствующего форме (A, B, C, E), и ее дискриминант не равен дискриминанту формы (A, B, C, E), то форма эта не эквивалентна обратимой; если же он равен, то эта форма эквивалентна обратимой, а именно той, корнем которой является эта единица ε.

В результате получается следующая основная теорема:

Теорема. *Число решений в целых числах X, Y неопределенного уравнения $(A, B, C, E)=1$, где (A, B, C, E), неприводимая, целочисленная кубическая двойничная форма отрицательного дискриминанта, вообще говоря, не больше двух, и только если форма эквивалентна обратимой, оно может быть равно трем и четырем. Только в случае единственного класса с дискриминантом -23 оно равно пяти. Никакое такое уравнение не имеет больше пяти решений.*

После того как при помощи алгорифма повышения мы свели вопрос на исследование обратимых форм, мы исследовали эти последние опять-таки алгорифмом повышения, разбивая решения на решения с четными и решения с нечетными показателями. Нагель для рассмотрения *обратимых* уравнений предложил иной, весьма остроумный и по существу дела геометрический способ, который показывает, что такое уравнение не может иметь, за исключением трех случаев, больше чем три решения, что еще несколько улучшает нашу предыдущую теорему, в которой оставалось неясным, может ли быть у бесконечно многих различных неэквивалентных обратимых уравнений по четыре решения. Перейдем к рассмотрению этого дополнения Нагеля, причем изложим его геометрически.

25. *О двухчленных в ε степенях прямой основной в $O(\varepsilon)$ единицы ε.* Начнем с теоремы:

Если ε — прямая основная единица кольца $O(\varepsilon)$, то двухчленных в ε обратных единиц нет, кроме одного случая, а именно, когда $D=-23$. Действительно, при данном дискриминанте D_ε двухчленная плоскость, построенная на $1, \varepsilon$, имеет общие точки с единичной поверхностью $(x^2+y^2)z=1$, не более как на высоте H_ε, которую легко вычислить. Для существования двухчленных в ε обратных единиц необходимо, чтобы H_ε была $\geqslant H_D$, где H_D — высота наинизшей точки пересечения дискриминантной поверхности D_ε с верхней частью единичной поверхности. Но для того, чтобы было $H_\varepsilon \geqslant H_D$, необходимо, как

легко видеть, чтобы ε лежала на линии пересечения единичной поверхности и поверхности D_ε достаточно далеко от начала, т. е. чтобы ε было достаточно мало, но, как показывает вычисление, в таком случае, например, начиная с $D=-59$, получается, что даже уже ε^{-1} больше, чем H_ε. Таким образом, двухчленных в ε обратных единиц при $|D_\varepsilon|\geqslant 59$ нет. Случаи $D_\varepsilon=-44$, -31, -23 можно легко исследовать, каждый в отдельности, при помощи способа п. 4, и получается, что обратная двухчленная в ε единица, где ε — прямая основная единица кольца $O(\varepsilon)$, имеется только одна для $D_\varepsilon=-23$, а именно единица ε, удовлетворяющая уравнению $\varepsilon^3=-\varepsilon^2+1$, есть прямая основная единица кольца $O(\varepsilon)$, и $\varepsilon^{-2}=\varepsilon+1$.

Теорема. *Если* $|D_\varepsilon|>44$, *то среди степеней* ε^m *с целыми неотрицательными показателями прямой основной единицы* ε *кольца* $O(\varepsilon)$, *кроме тривиальных двухчленных в* ε *единиц* $\varepsilon^0=1$ *и* $\varepsilon^1=\varepsilon$, *может быть только еще одна двухчленная в* ε *единица.* Действительно, пусть $\varepsilon^\mu=b\varepsilon+c$, причем μ наименьший показатель, больший 1, при котором ε^m двухчленна в ε, и пусть еще $\varepsilon^{\mu'}=B\varepsilon+C$ тоже двухчленна в ε, где $\mu'>\mu$. Тогда $\mu'=\mu\cdot\nu+\tau$, где ν и τ — целые рациональные и $0\leqslant\tau\leqslant\mu-1$. Покажем, что если $|D_\varepsilon|>59$, то $\tau\geqslant 2$. Действительно, если бы $\tau=0$, то было бы $(b\varepsilon+c)^\nu=B\varepsilon+C$ и по лемме п. 7 было бы $b=\pm 1$, т. е. $0<\pm\varepsilon+c<1$. Но $0<\varepsilon<1$ и, следовательно, было бы $c=1$ и $b\varepsilon+c=-\varepsilon+1$.

Однако, если $-\varepsilon+1$ положительная единица, то, если $\varepsilon^3=r\varepsilon^2+t\varepsilon+1$, $\varepsilon-1$ удовлетворяет уравнению

$$(x+1)^3=r(x+1)^2+t(x+1)+1$$

и, следовательно,

$$-N(\varepsilon-1)=N(-\varepsilon+1)=-1=r+t+1-1,$$

т. е. $r+t=-1$ и

$$D_\varepsilon=r^4-6r^3+7r^2+6r-31;$$

но это D_ε отрицательно лишь для $r=-1, 0, 1, 2, 3, 4$, и тогда соответственно $D_\varepsilon=-23, -31, -23, -23, -31, -23$.

Предположим, что теперь $\tau=1$. Тогда мы имели бы $(b\varepsilon+c)^\nu\cdot\varepsilon=A\varepsilon+B$. Так как тут коэффициент при ε^2 должен равняться нулю, то, если $\varepsilon^3=r\varepsilon^2+t\varepsilon+1$, мы имеем

$$\nu bc^{\nu-1}+\frac{\nu(\nu-1)}{1\cdot 2}b^2c^{\nu-2}r+\sum_{k\geqslant 3}\binom{\nu}{k}b^kc^{\nu-k}\lambda_k=0,$$

где λ_k — целые рациональные. Сократив это равенство на νb, мы получаем равенство

$$c^{\nu-1}+\frac{1}{2}(\nu-1)bc^{\nu-2}r+\sum_{k\geqslant 3}\binom{\nu-1}{k-1}\frac{b^{k-1}}{k}\cdot c^{\nu-k}\cdot\lambda_k=0.$$

Пусть b делится на нечетное простое число π. Тогда сумма Σ также делится на π, так как $\pi^{k-1}\geqslant 3^{k-1}>k$ для всех $k\geqslant 3$. Второй член $\frac{1}{2}(\nu-1)bc^{\nu-2}r$ также делится на π, т. е. и c должно было бы делиться на π, но это невозможно, так как b и c взаимно простые, потому что $b\varepsilon+c$ единица. Если b четное, то сумма Σ делится на 2, так как $2^{k-1}>k$, если $k\geqslant 3$. Второй член также четный, если либо b делится на 4, либо r четное, и в таком случае и c было бы четное, что невозможно. Остается только один возможный случай $|b|=2$ и r нечетное, так как b делиться на нечетное простое число π, как мы показали, не может. Но если $|b|=2$, то $\varepsilon^m=b\varepsilon+c=\pm 2\varepsilon+c$, откуда, так как $0<\varepsilon<1$ и $0<\varepsilon^\mu<1$, получается $|c|<3$, т. е. только и возможно, что $b\varepsilon+c=\pm(2\varepsilon-1)$. Посмотрим, для каких дискриминантов D_ε возможно

вообще, чтобы $2\varepsilon - 1$ было единицей. Мы имеем $N(2\varepsilon - 1) = 2r + 4t + 7$, откуда, если наложить $N(2\varepsilon - 1) = -1$, мы получаем $r = -2t - 4$, т. е. r четное, а нам надо, чтобы оно было нечетное. Если же положим $N(2\varepsilon - 1) = 1$, то получаем $r = -2t - 3$. В этом случае мы имеем, что дискриминант $D_\varepsilon = 4t^3 + t^2(2t+3)^2 + 4(2t+3)^3 + 18t(2t+3) - 27$, и он отрицателен только для $t = -1, -2, -3, -4, -5$. Но случай $t = -3$ дает приводимое уравнение, а случаи $t = -4, -5$ дают $1 < \varepsilon$, мы же предполагаем единицу прямой основной единицей. Случай $t = -2$ дает уравнение $\varepsilon^3 = \varepsilon^2 - 2\varepsilon + 1$, т. е. ε хотя и положительная прямая, но не основная единица кольца $O(\varepsilon)$; ε есть квадрат основной единицы этого кольца. Остается только один случай $t = -1$, дающий уравнение $\varepsilon^3 = -\varepsilon^2 - \varepsilon + 1$ с дискриминантом -44, которое имеет 4 решения: $\varepsilon^0 = 1$, $\varepsilon^1 = \varepsilon$, $\varepsilon^4 = 2\varepsilon - 1$, $\varepsilon^{17} = -103\varepsilon + 56$, причем *по основной теореме* это и все его решения.

Итак, если положить $\varepsilon^\tau = u\varepsilon^2 + v\varepsilon + w$, то тут $u \neq 0$, так как $\tau > 1$ и $< \mu$, а ε^μ наинизшая степень ε с $\mu > 1$, которая двухчленна в ε. Мы имеем, следовательно,

$$(b\varepsilon + c)^\nu \cdot (u\varepsilon^2 + v\varepsilon + w) = B\varepsilon + C,$$

причем $u \neq 0$. Возведя слева в степень по биному, перемножив и положив, что коэффициент при ε^2 равен нулю, мы получим:

$$u[c^\nu + \nu c^{\nu-1} br + \ldots] + v\left[\nu c^{\nu-1} b + \frac{\nu(\nu-1)}{1\cdot 2} c^{\nu-2} b^2 r + \ldots\right] +$$
$$+ w\left[\frac{\nu(\nu-1)}{1\cdot 2} c^{\nu-2} b^2 + \frac{\nu(\nu-1)(\nu-2)}{1\cdot 2\cdot 3} c^{\nu-3} b^3 r + \ldots\right] = 0,$$

откуда мы получаем, что $uc^\nu \equiv 0 \pmod{b}$. Но так как $b\varepsilon + c$ единица, b и c взаимно простые, то, следовательно, мы имеем, что u делится на b, т. е. что имеет место неравенство

$$|u| \geqslant |b|. \tag{1}$$

Покажем еще, что $\tau = \mu - 1$ тоже невозможно. Действительно, если бы это было, мы имели бы

$$u\varepsilon^2 + v\varepsilon + w = \varepsilon^{\mu-1} = \frac{\varepsilon^\mu}{\varepsilon} = \frac{b\varepsilon + c}{\varepsilon},$$

или

$$u\varepsilon^3 + v\varepsilon^2 + w\varepsilon = b\varepsilon + c,$$

т. е.

$$(ur + v)\varepsilon^2 + (ut + w)\varepsilon + u = b\varepsilon + c,$$

откуда

$$u = c$$

и, следовательно, так как $u \equiv 0 \pmod{b}$ и b и c взаимно просты, b получается равным ± 1, но, как мы видели, если $|D_\varepsilon| > 31$, то $b \neq \pm 1$. Итак, мы имеем еще неравенство

$$\tau \leqslant \mu - 2. \tag{2}$$

Неравенства (1) и (2), как это легко видеть из следующего геометрического рассмотрения, при $|D_\varepsilon| > 44$ несовместимы. Действительно, в виду того, что $\tau \leqslant \mu - 2$, а расстояния точек от оси z при их перемножении перемножаются, мы должны иметь, если будем обозначать через $\{\ \}$ расстояние от точки до оси z, следующее неравенство:

$$\{u\varepsilon^2 + v\varepsilon + w\} \leqslant \frac{\{b\varepsilon + c\}}{\{\varepsilon^2\}}. \tag{3}$$

Пусть теперь координаты x, y проекции ε на плоскость X, Y параллельно рациональному направлению суть (α, β), а координаты проекции $\varepsilon^2 - (\gamma, \delta)$. В таком случае проекция точки $M\varepsilon^2 + P\varepsilon + Q$ имеет координаты $(M\gamma + P\alpha, M\delta + P\beta)$, так как прибавление Q лишь переносит точку параллельно рациональному направлению. В виду того, что расстояние от точки до оси z отличается от расстояния от такой ее проекции не больше чем на z точки, мы можем неравенство (3) заменить следующим более сильным:

$$\{u\gamma + v\alpha,\ u\delta + v\beta\} - \varepsilon^{\tau} \leqslant \frac{|b|\{\alpha, \beta\} + \varepsilon^{\mu}}{\{\alpha, \beta\}^2 - \varepsilon^2}. \tag{4}$$

Заменим еще в $\{u\gamma + v\alpha,\ u\delta + v\beta\}$ v тем v^*, при котором это расстояние будет наименьшим, т. е. заменим это расстояние расстоянием h от начала до прямой $x = u\gamma + v^*\alpha$, $y = u\delta + v^*\beta$, где v^* переменный параметр; обычное уравнение этой прямой имеет вид $x\beta + y\alpha + (\alpha\delta - \beta\gamma)u = 0$, т. е.

$$h = \left|\frac{u(\alpha\delta - \beta\gamma)}{\sqrt{\alpha^2 + \beta^2}}\right|;$$

тогда получится из (4) еще более сильное неравенство:

$$\frac{|u| \cdot |\alpha\delta - \beta\gamma|}{\sqrt{\alpha^2 + \beta^2}} - \varepsilon^{\tau} \leqslant \frac{|b|\sqrt{\alpha^2 + \beta^2} + \varepsilon^{\mu}}{\alpha^2 + \beta^2 - \varepsilon^2},$$

или, так как в силу неравенства (1) $|u| \geqslant |b|$, а $|\alpha\delta - \beta\gamma|$, как легко видеть, равно объему основного параллелепипеда решетки $[\varepsilon^2, \varepsilon, 1]$, т. е. равно $\frac{1}{2}\sqrt{|D_\varepsilon|}$, и принимая во внимание, что τ и μ больше 2, мы получаем неравенство

$$u\varepsilon^2 < \alpha^2 + \beta^2$$

и

$$\sqrt{|D_\varepsilon|} \leqslant \left(2(1 + \varepsilon^2)\sqrt{\alpha^2 + \beta^2} + \frac{\varepsilon^2}{\sqrt{\alpha^2 + \beta^2} - 1}\right),$$

откуда легко получается

$$|D_\varepsilon| < 44.$$

Соединяя обе сейчас доказанные нами теоремы, мы видим, что обратимое уравнение $(1, r, -t, 1) = 1$ может иметь максимум три решения, если его дискриминант $|D| > 44$. Заметим, что три решения могут быть в бесконечно многих случаях, а именно, например, уравнения $(1, 0, -t, 1) = 1$, рассмотренные в п. 20, всегда имеют три решения. Что же касается уравнений с дискриминантами -44, -31, -23, то два последние были нами вполне решены в пп. 21, 23 и оказались имеющими четыре и пять решений. Уравнение же с $D = -44$, как было указано выше, имеет четыре решения: ε^0, ε^1, ε^4, ε^{17}, и так как по основной теореме оно не может иметь больше четырех решений, то это все его решения.

Собирая все сказанное, мы получаем следующую окончательную теорему:

Теорема. *Число решений в целых числах X, Y неопределенного уравнения $(A, B, C, E) = 1$, где (A, B, C, E) неприводимая, целочисленная, кубическая двойничная форма отрицательного дискриминанта, вообще говоря, не больше двух и только, если форма эквивалентна обратимой, оно может быть равно трем, причем в этом случае оно равно двум или трем, и при этом трем для бесконечного числа классов. Только в случае двух единственных классов форм с дискриминантами -44 и -31 оно равно четырем и только в случае единственного класса с дискриминантом -23 оно равно пяти. Никакое такое уравнение не может иметь больше пяти решений.*

Получается такая табличка числа решений:

если форма не эквивалентна обратимой	0
	1
	2 } если форма эквивалентна обратимой
	3 }
	4 если $D=-44$ и -31
	5 если $D=-23$.

§ 76. Дальнейшие исследования об алгорифме повышения

При доказательстве предыдущей основной теоремы о числе представлений числа кубической двойничной формой отрицательного дискриминанта был рассмотрен своеобразный вычислительный процесс, который мы называли алгорифмом повышения. Этот алгорифм был разобран лишь для целой формы, т. е. такой, у которой один из крайних коэффициентов равен 1. Для вопроса о числе решений этого достаточно, так как если рассматриваемая форма не эквивалентна целой форме, то число представлений ею числа 1 равно нулю и, значит, достаточно рассматривать лишь целые формы. Для получения же самих решений этого недостаточно, так как у нас нет способа узнать, эквивалентна ли заданная форма целой форме. Поэтому, если рассматривать алгорифм повышения как способ для получения самих решений в общем случае кубической двойничной формы отрицательного определителя, то надо построить этот алгорифм и для нецелой формы. Оказывается, это можно сделать. Самый алгорифм повышения можно рассматривать как способ последовательного приближения к решению. Полное решение было бы получено, если бы мы имели способ узнавать на некотором, заранее ограниченном по номеру, шаге алгорифма повышения, наступит такое положение, что дальше вычислять не надо, так как дальше алгорифм заведомо не оборвется и, следовательно, дальше решений нет. Два такие „критериума остановки" мы предлагаем ниже, причем критерии эти во всех нами вычисленных примерах наступали обычно на одном из первых шагов повышения; однако, мы пока не умеем указать границу для номера того шага, на котором тот или иной из этих критериумов должен появиться.

1. Об одном необходимом условии для того, чтобы неопределенное уравнение $(A, B, C, E)=1$ имело решение. Пусть $AX^3+BX^2Y+CXY^2+EY^3=(A, B, C, E)=\Phi(X, Y)$ некоторая заданная кубическая двойничная форма и ω_1 и ω_2 корни уравнений $\omega_1^3-B\omega_1^2+AC\omega_1-A^2E=0$ и $\omega_2^3-C\omega_2^2+B\omega_2-AE^2=0$, причем $\omega_1\omega_2=AE$. Модуль $[\omega_1, \omega_2, 1]$, как это показано в § 15, представляет собою кольцо. Мы будем обозначать это кольцо $O(\Phi)$ или $O[\omega_1, \omega_2, 1]$. Дискриминант этого кольца равен дискриминанту Ф. Эквивалентным формам соответствует одно и то же кольцо. Как легко видеть, не всякая форма Ф может быть представлена как норма (в поле $\Omega(\omega_1)$) числа вида $\lambda X+\mu Y$, где λ и μ — целые числа поля $\Omega(\omega_1)$, так как, если, например, форма Ф примитивна, т. е. ее коэффициенты A, B, C, E не имеют общего делителя, то и λ и μ не должны были бы иметь общего делителя, но $\rho=\frac{\lambda}{\mu}$ есть корень уравнения $N(\rho-Y)=A-BY+CY^2-EY^3=0$, т. е. $\frac{\lambda}{\mu}$ самое общее кубическое дробное число. Но если в поле $\Omega(\omega_1)$ не один класс идеалов, то можно в нем всегда найти сколько-угодно дробных чисел, которые, если их представить несократимой в поле дробью, то все же числитель и знаменатель этой дроби будут иметь общего идеального делителя и, следовательно, не будут взаимно простыми. В том же случае, когда форма Ф может представлять число 1, она эквивалентна „целой" форме, т. е. такой, у которой $E=1$, например, $(A, B, C, E)=(n, -q, s, 1)\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, и, если ρ корень уравнения $\rho^3=s\rho^2+q\rho+n$,

то мы получаем $(A, B, C, E) = N_{\mathfrak{Q}}(\lambda X + \mu Y)$, где $\lambda = \alpha\rho + \gamma$, $\mu = \beta\rho + \delta$, т. е. в этом случае Φ имеет такое „целое" разложение в своем кольце $O(\Phi) = O[\rho^2, \rho, 1]$. Если Φ примитивна, что мы будем всегда дальше предполагать, то числа λ и μ взаимно простые. Мы имеем $\frac{\lambda}{\mu} = \frac{\omega_2}{E}$ и, следовательно, мы получаем $E = \mu j$; $\omega_2 = \lambda j$, где j число из $\mathfrak{Q}(\omega_1)$. Число $\alpha E - \beta\omega_2$ кольца $O(\Phi)$ равно $(\alpha\mu - \beta\lambda)\cdot j = j$, так как $\alpha\mu - \beta\lambda = 1$, т. е. число j есть число кольца $O(\Phi)$. Идеал (ω_2, E) кольца $O(\Phi)$ должен, следовательно, быть главным идеалом и притом числом кольца $O(\Phi)$. Если форма Φ задана, то можно при помощи методов, рассмотренных в гл. II и IV, узнать, главный ли идеал (ω_2, E) в $\mathfrak{Q}(\omega_1)$ и, в случае, когда это так, можно найти соответствующее целое алгебраическое число j кольца, если таковое существует. А именно, если (ω_2, E) главный идеал $\mathfrak{Q}(\omega_1)$ и равен целому числу I из $\mathfrak{Q}(\omega_1)$, то число j, если таковое существует, равно $I\cdot\varepsilon$, где ε — некоторая единица из $\mathfrak{Q}(\omega_1)$. Пусть дискриминант формы Φ отрицательный. Тогда все единицы $\mathfrak{Q}(\omega_1)$ суть степени одной основной I_0; пусть I_0^{μ} первая степень I_0, которая лежит в кольце $O(\Phi)$, т. е. $I_0^{\mu} = \varepsilon_0$, где ε_0 основная единица кольца $O(\Phi)$. Тогда, если среди чисел I, II_0, II_0^2 .. $II_0^{\mu-1}$ нет числа, лежащего в $O(\Phi)$, то искомого числа j нет. Если же такое есть, то мы его найдем среди этих μ чисел.

Если j найдено, то $\lambda = \frac{\omega_2}{j}$; $\mu = \frac{E}{j}$ или же отличаются от этих чисел на один и тот же множитель, который есть единица ε в кольце $O(\Phi)$, так как, если $\lambda\varepsilon$ и $\mu\varepsilon$ лежат в кольце $O(\Phi)$, то и $\alpha\mu\varepsilon - \beta\lambda\varepsilon$ тоже лежит в кольце.

Для возможности существования решения уравнения $\Phi(X, Y) = 1$, *таким образом, необходимо существование такого разложения* Φ *в собственном кольце.*

Примеры показывают, что это условие, однако, не достаточно.

2. О двух сравнениях, которым должны удовлетворять все решения P, Q уравнения $\Phi(X, Y) = 1$ в случае, когда Φ неприводимая целочисленная двойничная кубическая форма отрицательного дискриминанта. Предположим, что выведенное выше необходимое условие выполнено, и пусть $\lambda = r\omega_1 + s\omega_2 + t$; $\mu = u\omega_1 + v\omega_2 + w$. Если мы имеем $\Phi(P, Q) = 1$, то $\lambda P + \mu Q$ положительная единица кольца $O(\Phi)$. Если определитель формы Φ отрицательный, то кольцо $O(\Phi)$ имеет только одну независимую основную единицу. Пусть $\varepsilon_0 = a\omega_1 + b\omega_2 + c$ прямая, положительная основная единица, т. е. основная единица, удовлетворяющая неравенствам $0 < \varepsilon_0 < 1$. Девять целых рациональных чисел a, b, c; r, s, t; u, v, w могут быть вычислены при помощи способов, указанных в гл. II и IV. Мы имеем $\lambda P + \mu Q = \varepsilon_0^m$. В виду того, что двухчленная плоскость $\lambda X + \mu Y$ пересекает верхнюю часть единичной поверхности по конечному куску кривой, мы можем, подобно тому, как это было указано в п. 4 § 75, найти все такие решения с $m < 0$; если наивысшее такое решение есть ε_0^{-k}, то, взяв вместо λ и μ $\lambda\varepsilon_0^{-k}$ и $\mu\varepsilon^{-k}$, что всегда можно сделать, мы перейдем к такому новому целому разложению рассматриваемой формы Φ, при котором она заведомо не имеет решений с отрицательными показателями m. Для любого решения P, Q мы будем тогда иметь

$$\lambda P + \mu Q = (rP + uQ)\,\omega_1 + (sP + vQ)\,\omega_2 + (tP + wQ) = \\ = F\omega_1 + G\omega_2 + H = \varepsilon = \varepsilon_0^m = (a\omega_1 + b\omega_2 + c)^m,$$

где $m > 0$. Если написать это же уравнение для сопряженных колец и вычесть, получается

$$F(\omega_1' - \omega_1'') + G(\omega_2' - \omega_2'') = \varepsilon_0'^m - \varepsilon_0''^m = (\varepsilon_0' - \varepsilon_0'')(U\omega_1 + V\omega_2 + W) = \\ = [a(\omega_1' - \omega_1'') + b(\omega_2' - \omega_2'')](U\omega_1 + V\omega_2 + W),$$

где U, V, W — тоже целые рациональные числа. Мы имеем

$$\omega_1' - \omega_1'' = \frac{AE(\omega_2'' - \omega_2')}{\omega_2' \cdot \omega_2''} = \frac{AE\omega_2(\omega_2'' - \omega_2')}{AE^2} = -\frac{\omega_2}{E}(\omega_2' - \omega_2''),$$

поэтому, после соответственных сокращений, мы получаем

$$-F\omega_2 + EG = (-a\omega_2 + Eb)(U\omega_1 + V\omega_2 + W).$$

Сравнение коэффициентов дает три уравнения, решая которые, мы получим: $\Delta \cdot U = a(bF - aG)$; $\Delta \cdot V = b(bF - aG)$; $\Delta \cdot W = b(aC - bE)G + a(aA - bB)F$, где $\Delta = a^3A - a^2bB + ab^2C - b^3E$. Пусть $\delta = (a, b)$ и $a = a_1\delta$, $b = b_1\delta$, и обозначим $\frac{\Delta}{\delta^3} = \chi$, тогда мы имеем:

$$\chi \cdot \delta \cdot U = a_1(b_1F - a_1G);$$
$$\chi \cdot \delta \cdot V = b_1(b_1F - a_1G);$$
$$\chi \cdot \delta \cdot W = b_1(a_1C - b_1E)G + a_1(a_1A - b_1B)F.$$

Из первых двух из этих уравнений, в виду того, что $(a_1, b_1) = 1$, мы получаем

$$b_1F - a_1G \equiv 0 \pmod{\chi\delta},$$

или

$$P \cdot K + QL \equiv 0 \pmod{\chi\delta}, \tag{1}$$

где $K = \begin{vmatrix} a_1 & b_1 \\ r & s \end{vmatrix}$; $L = \begin{vmatrix} a_1 & b_1 \\ u & v \end{vmatrix}$, а из третьего

$$P \cdot \mathrm{K} + Q\mathrm{L} \equiv 0 \pmod{\chi\delta}, \tag{2}$$

где $\mathrm{K} = \begin{vmatrix} Ca_1b_1 - Eb_1^2, & Ba_1b_1 - Aa_1^2 \\ r & s \end{vmatrix}$; $\mathrm{L} = \begin{vmatrix} Ca_1b_1 - Eb_1^2, & Ba_1b_1 - Aa_1^2 \\ u & v \end{vmatrix}$.

Этим сравнениям (1) и (2) должны удовлетворять все решения P, Q уравнения $\Phi(x, y) = 1$.

3. О случае, когда сравнения (1) и (2) удовлетворяются тождественно. Пусть λ, μ—разложение Φ в $O(\Phi)$, тогда $\lambda_k = \lambda\varepsilon_0^k$; $\mu_k = \mu\varepsilon_0^k$ тоже такое разложение. Если мы обозначим числа K, L, K, L для этого разложения через K_k, L_k, K_k, L_k, то, как легко вычислить, $K_1 = Kc + \delta\mathrm{K}$; $L_1 = Lc + \delta\mathrm{L}$ и $\mathrm{K}_1 \equiv \mathrm{K}c + \delta \cdot K \cdot \varphi$; $\mathrm{L}_1 \equiv \mathrm{L}c + \delta L\varphi$ по модулю $\chi\delta$, где $\varphi = -ACa_1^2 + (AE + BC)a_1b_1 - BEb_1^2$. Если сравнения (1) и (2) удовлетворяются тождественно, т. е. $K \equiv L \equiv \mathrm{K} \equiv \mathrm{L} \equiv 0 \pmod{\chi\delta}$, то, следовательно, сравнения (1_k) и (2_k) также удовлетворяются тождественно. Пусть σ — какой-нибудь общий делитель K и L, тогда σ — также делитель $\begin{vmatrix} r & s \\ u & v \end{vmatrix}$, так как a_1 и b_1 — взаимно простые. Число $\begin{vmatrix} r & s \\ u & v \end{vmatrix}$ есть индекс модуля $[\lambda, \mu, 1]$ по отношению к модулю $[\omega_1, \omega_2, 1]$.

Предположим, что уравнение $\Phi(x, y) = 1$ имеет решение. В таком случае $\lambda = (\alpha\rho + \gamma) \cdot \varepsilon$; $\mu = (\beta\rho + \delta) \cdot \varepsilon$, где ε — единица, и притом единица кольца $[\omega_1, \omega_2, 1] = [\rho^2, \rho, 1]$, так как $\alpha\mu - \beta\lambda = \varepsilon$. Пусть $\varepsilon = A\rho^2 + B\rho + \Gamma$. Мы имеем тогда:

$$\begin{vmatrix} r & s \\ u & v \end{vmatrix} = \begin{vmatrix} A\alpha s + B\alpha + A\gamma, & A\alpha q + \Gamma\alpha + B\gamma \\ A\beta s + B\beta + A\delta, & A\beta q + \Gamma\beta + B\delta \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \begin{vmatrix} As + B, & A \\ Aq + \Gamma, & B \end{vmatrix} =$$
$$= ABs + B^2 - A^2q - A\Gamma = A',$$

где A' — коэффициент при ρ^2 обратной положительной единицы $\eta = \varepsilon^{-1}$. Всякий общий делитель K и L есть, следовательно, делитель этого A'. Если, следовательно, $K \equiv L \equiv 0 \pmod{\varkappa\delta}$ и σ — произведение всех различных простых чисел, которые входят множителями в $\varkappa$, то A' должно делиться на $\sigma \cdot \delta$. Число $N[A'(s-\rho)+B']$ есть индекс единицы, η по отношению к кольцу $O(\rho)$, и так как η — степень ε_0^{-1} с целым положительным показателем, оно должно делиться на индекс $\varkappa\delta^3$ единицы ε_0 по отношению к $O(\rho)$. Но, как легко видеть, A' и B' имеют δ своим общим делителем, т. е. $A' = A_1' \cdot \delta$; $B' = B_1' \cdot \delta$, и, следовательно, число $N[A_1'(s-\rho)+B_1']$ должно делиться на $\varkappa$. Но так как $A_1' \equiv 0 \pmod{\varkappa}$, то $B_1'^3 \equiv 0 \pmod{\varkappa}$, и, стало быть, $B_1' \equiv 0 \pmod{\sigma}$. Если, следовательно, сравнение (1) удовлетворяется тождественно, то σ есть делитель A_1' и B_1'.

Перейдем теперь к сравнениям (1_1) и (2_1); они должны также удовлетворяться тождественно, если удовлетворяются тождественно сравнения (1) и (2). Если мы, следовательно, положим $\varepsilon\varepsilon_0 = A''\rho^2 + B''\rho + \Gamma''$ и $\varepsilon_0 = \bar{a}\rho^2 + \bar{b}\rho + \bar{c}$, то A_1'' и B_1'' должны также делиться на σ. Если мы теперь выразим A_1'' и B_1'' через A', B', Γ' и $\bar{a}$, $\bar{b}$, $\bar{c}$, то мы получим (если положить $\bar{a} = \bar{a}_1\delta$; $\bar{b} = \bar{b}_1\delta$), что $\bar{a}_1\Gamma$ и $\bar{b}_1\Gamma$ делятся на σ. Но $(\bar{a}_1, \bar{b}_1) = 1$, так как, как легко видеть, общий наибольший делитель $\bar{a}$ и $\bar{b}$ — тот же самый, как у a и b (т. е. δ), а Γ не может делиться на σ, если $\sigma > 1$, т. е. $\sigma = 1$. Отсюда получается, что $\varkappa = \pm 1$. Число $u = a_1\omega_1 + b_1\omega_2$ из $O(\Phi)$ имеет, таким образом, по отношению к $O(\Phi)$ индекс ± 1 и, следовательно, форма $(\bar{n}, -\bar{q}, \bar{s}, 1)$, корнем которой является $\bar{\rho}$, есть целая форма, эквивалентная форме Φ.

Таким образом, найдено одно решение уравнения $\Phi = 1$. Мы сейчас покажем, что одновременно найдено и некоторое еще второе решение.

Действительно, из $K \equiv L \equiv \mathrm{K} \equiv \mathrm{L} \equiv 0 \pmod{\varkappa\delta}$ мы получаем легко, что $r \equiv s \equiv u \equiv v \equiv 0 \pmod{\varkappa\delta}$; так, например, $K \cdot (Ba_1b_1 - Aa_1^2) - \mathrm{K}b_1 = (-Aa_1^3 + Ba_1^2b_1 - Ca_1b_1^2 + Eb_1^3) \cdot s = -\varkappa s$, т. е., если K и K делятся на $\varkappa\delta$, то s делится на δ. Таким образом, в этом случае $A' = \begin{vmatrix} r & s \\ u & v \end{vmatrix} \equiv 0 \,[\mathrm{mod}\ \delta^2]$. Единица η, а следовательно и единица ε, лежит в этом случае в кольце $O(\delta\rho)$. Пусть $\varepsilon = \varepsilon_0^{\tau}$, т. е. $\varepsilon = A_1\delta^2\rho^2 + B_1\delta\rho + \Gamma = (\bar{a}_1\delta\rho^2 + \bar{b}_1\delta\rho + \bar{c})^{\tau}$. Сравнивая коэффициенты при ρ^2, мы получаем отсюда $\tau\bar{a}_1\,\delta\bar{c}^{\tau-1} \equiv 0 \pmod{\delta^2}$. Но $(\bar{c}, \delta) = 1$, и можно предположить, что $(\tau, \delta) = 1$, так как от λ, μ можно всегда перейти к $\lambda\varepsilon_0^k$, $\mu\varepsilon_0^k$ так, чтобы вместо τ было $\tau - k$, причем k можно всегда взять такое, чтобы было $(\tau - k, \delta) = 1$. Поэтому $\bar{a}_1 \equiv 0 \pmod{\delta}$, и, следовательно, сама единица ε_0 лежит в рассматриваемом случае в кольце $O(\delta\rho)$. Индекс ε_0 по отношению к $O(\rho)$ равен $\pm\delta^3$, так как $\varkappa = \pm 1$. Единица ε_0 есть, следовательно, единица кольца $O(\delta\rho)$, имеющая по отношению к этому кольцу индекс ± 1. Форма $(\delta^3 n, -\delta^2 q, \delta s, 1)$, соответствующая кольцу $O(\delta\rho)$, таким образом, эквивалентна некоторой обратимой форме $(1, -q', s', 1)$. Уравнение $(\delta^3 n, -\delta^2 q, \delta s, 1) = 1$ имеет, следовательно, два решения: $(0, 1)$ и (X_1, Y_1), а потому уравнение $(n, -q, s, 1) = 1$ имеет два решения: $(0, 1)$ и $(\delta X_1, Y_1)$, и уравнение $(A, B, C, E) = 1$ также имеет в этом случае два решения, так как $(A, B, C, E) \sim (n, -q, s, 1)$. Мы получаем, следовательно, теорему:

Теорема. *Если сравнения* (1) и (2) *удовлетворяются тождественно, и* $\varkappa \neq \pm 1$, *уравнение* $\Phi(X, Y) = 1$ *не имеет решений; если же* $\varkappa = \pm 1$, *то оно имеет два решения, которые можно оба найти, причем решение уравнения* $\Phi(X, Y) = 1$ *сводится на решение обратимого уравнения* $(1, -q', s', 1) = 1$, *которое может быть найдено.*

4. Алгорифм повышения. Пусть сравнения (1) и (2) не удовлетворяются оба тождественно. Пусть, например, сравнение (1) не удовлетворяется тождественно. Обозначим через d общий наибольший делитель K, L и $\varkappa\delta$, и пусть $K=d\cdot K'$; $L=dL'$; $\varkappa\delta=d\varkappa'$; тогда мы будем иметь $PK'+QL'\equiv 0 \pmod{\varkappa'}$. Если теперь $(K', L')=d'$ и $K'=K''d'$; $L'=L''\cdot d'$, то мы будем иметь $(d'\varkappa')=1$ и, следовательно, $PK''+QL''\equiv 0 \pmod{\varkappa'}$, где уже $(K'', L'')=1$. Если перейти от формы (A, B, C, E) к форме (A', B', C', E') при помощи подстановки $\begin{pmatrix}\alpha, & -L''\\ \gamma, & K''\end{pmatrix}$, где $\alpha K''+\gamma L''=1$, то мы получим $A'P'^3+B'P'^2Q'+C'P'Q'^2+E'Q'^3=1$, где $P'\equiv 0 \pmod{\varkappa'}$, так как $P'=PK''+QL''$.

Положим $P'=\overline{P}\cdot\varkappa'$ и $\overline{A}=A'\cdot\varkappa'^3$; $\overline{B}=B'\cdot\varkappa'^2$; $\overline{C}=C'\cdot\varkappa'$; $\overline{E}=E$, тогда мы получим уравнение $(\overline{A}, \overline{B}, \overline{C}, \overline{E})=1$, на решение которого сводится решение заданного уравнения $(A, B, C, E)=1$. Форма $(\overline{A}, \overline{B}, \overline{C}, \overline{E})$ имеет в $\varkappa'^6$ раз больший дискриминант, чем форма (A, B, C, E), и $\varkappa'\neq\pm 1$, так как мы предположили, что сравнение (1) не удовлетворяется тождественно. От формы $(\overline{A}, \overline{B}, \overline{C}, \overline{E})$ мы аналогично перейдем к форме $(\overline{\overline{A}}, \overline{\overline{B}}, \overline{\overline{C}}, \overline{\overline{E}})$ и т. д. Этот процесс может оборваться, только если либо на каком-нибудь шагу соответственная форма не будет иметь целого разложения в собственном кольце, и в этом случае уравнение $(A, B, C, E)=1$ не имеет решений, или если на каком-нибудь шагу сравнения (1) и (2) окажутся удовлетворяющимися тождественно, в этом случае уравнение $(A, B, C, E)=1$ либо вовсе не имеет решений, либо оно имеет два решения, которые мы и найдем на этом шагу алгорифма.

5. Первый случай, когда уравнение $\Phi(X, Y)=1$ имеет одно и только одно решение. В этом случае, который встречается очень часто, в силу теоремы п. 3 алгорифм повышения нигде не кончится. Дальнейшее изучение этого весьма замечательного обстоятельства мы здесь производить не будем.

6. Второй случай, когда уравнение $\Phi(X, Y)=1$ имеет по крайней мере два решения. В этом случае, как это будет ясно из геометрического соображения, которое мы разберем в следующем пункте, на некотором шаге алгорифма повышения сравнения (1) и (2) удовлетворятся тождественно.

7. Приближение к решениям при помощи алгорифма повышения. Пусть X, Y — все пары целых рациональных чисел. Рассмотрим их как точки по отношению к некоторой зафиксированной координатной системе; тогда они составят параллелограмматическую решетку точек. Те из этих точек (P, Q), целые координаты которых удовлетворяют сравнению $PK''+QL''\equiv 0 \pmod{\varkappa'}$, т. е. удовлетворяют неопределенному уравнению $PK''+QL''=t\varkappa'$, где t — целое рациональное число, образуют, очевидно, подрешетку этой решетки. Всякий шаг повышения при помощи нашего алгорифма ведет каждый раз к подрешетке предыдущей решетки, основной параллелограмм которой имеет, по крайней мере, в два раза бо́льшую площадь и которая имеет с предыдущей общую точку (0, 0). Если имеется одно решение (P_1, Q_1), то весь этот процесс сводится к выбрасыванию из решетки X, Y каждый раз рядов точек, параллельных ряду $(0, 0)$ $(P_1, Q)_1$. Этот процесс может итти без конца, как это и будет, как мы это показали, в случае, когда есть одно и только одно решение. Если же есть два решения: (P_1, Q_1) и (P_2, Q_2), то площадь основного параллелограмма получаемых решеток не может превзойти площади параллелограмма, построенного на точках $(0, 0)$, (P_1, Q_1), (P_2, Q_2), так как эти точки будут лежать во всех этих решетках, и поэтому алгорифм должен кончиться. Если мы будем в каждой подрешетке находить ближайшую к $(0, 0)$ ее точку, то, если решение только одно, оно встретится в ряду этих минимумов.

8. Вычисление чисел λ и μ для повышенных форм. Пусть λ и μ уже вычислены для заданной формы $\Phi(X, Y)$ тем способом, который

был указан в п. 1, а также вычислена ε_0. Если, в соответствии с п. 4, мы перейдем от формы Φ к форме $\bar{\Phi}$ при помощи подстановки $\begin{pmatrix} \alpha, & -L'' \\ \gamma, & K'' \end{pmatrix}$, то $\gamma' = \alpha\lambda + \gamma\mu$; $\mu' = \mu K'' - \lambda L''$.

Пусть это уже сделано, т. е. $\lambda' = \lambda$, $\mu' = \mu$. В таком случае

$$(A, B, C, E) = N(\lambda x + \mu y);$$
$$(\bar{A}, \bar{B}, \bar{C}, \bar{E}) = N(\lambda\chi' X + \mu Y) = (A\chi'^3, B\chi'^2, C\chi', E).$$

Базис, соответствующий этой повышенной форме, есть $\omega_1 = \chi'^2\omega_1$; $\bar{\omega}_2 = \chi'\omega_2$. Разложение $\bar{\Phi}$ в $O(\Phi)$ есть $\lambda\chi'$, μ, но $\bar{\Phi}$ должна иметь разложение $\bar{\lambda}$, $\bar{\mu}$ в своем собственном кольце $O(\bar{\Phi})$ и, следовательно, $\bar{\lambda} = \lambda\chi'\varepsilon_0^\tau$; $\bar{\mu} = \mu\varepsilon_0^\tau$, где τ — целый положительный показатель $< \nu$, если ε_0^ν — первая степень ε_0, лежащая в $O(\bar{\Phi})$.

9. Критериумы остановки. Может быть, что уравнение $\Phi(X, Y) = 1$ вовсе не имеет решений. Надо поэтому найти обстоятельство, которое после наперед заданного числа шагов алгорифма повышения показывало бы, что дальше вычислять не надо, так как дальше заведомо решений нет. Если бы мы нашли такой критерий, то вся задача была бы решена. Мы не нашли до сих пор такого критериума. Мы можем указать, однако, на два следующих критериума, которые во всех численных примерах, нами рассмотренных, обыкновенно появлялись на одном из первых шагов повышения, хотя мы и не можем наперед ограничить номер того шага, раньше которого такой критериум осуществится. Во-первых, может случиться, что на каком-нибудь шаге повышенная форма не будет иметь разложения в собственном кольце, в чем можно будет всегда убедиться при помощи метода п. 8. Во-вторых, может случиться, что на некотором шаге сравнения (1) и (2) будут несовместимы, что будет, как легко видеть, тогда и только тогда, когда $\begin{vmatrix} r, & s \\ u, & v \end{vmatrix}$ не делится на δ.

10. Два примера. Пусть форма (2, 0, 3, 2), $D = -648$; тогда $\omega_1^3 + 6\omega_1 - 8 = 0$; $\omega_2^3 - 3\omega_2 - 8 = 0$; $\omega_1 - 1 = \varepsilon$ единица, числа λ и μ кольца $O(2, 0, 3, 2)$ должны иметь норму 2; однако, если употребить известные методы, рассмотренные, например, в § 22, можно показать, что в кольце $O(2, 0, 3, 2)$ нет чисел с нормой 2. Форма (2, 0, 3, 2), следовательно, не имеет разложения в собственном своем кольце. Тут имеет место первый критериум остановки, и уравнение $(2, 0, 3, 2) = 1$ не имеет решений. Пусть теперь дана форма (3, 3, 4, 2), $D = -516$; тут $\omega_1^3 - 3\omega_1^2 + 12\omega_1 - 18 = 0$; $\omega_2^3 - 4\omega_2^2 + 6\omega_2 - 12 = 0$; вычислим числа λ и μ; они суть: $\lambda = -3 + \omega_2$; $\mu = 2 - \omega_1$; основная единица кольца $O(3, 3, 4, 2)$ есть $\varepsilon_0 = 23 - 7\omega_2$; $\delta = 7$; $\begin{vmatrix} r & s \\ u & v \end{vmatrix} = 1$ и не делится на 7; следовательно, сравнения (1) и (2) несовместимы. Тут имеет, таким образом, место второй критериум остановки. Уравнение $(3, 3, 4, 2) = 1$ не имеет решений. (Между прочим, это форма с наименьшим по абсолютной величине отрицательным дискриминантом, которая не представляет числа 1 по нетривиальной причине, т. е. не потому, что она неприметивна, и не потому, что она имеет два крайних коэффициента четные, а оба средних нечетные, т. е. форма, все числа представляемые которой имеют общим делителем двойку, иначе говоря, что кольцо имеет общего делителя всех индексов его чисел.)

11. Алгорифм повышения для случая целой формы. Если форма Φ „целая“, т. е. один из ее крайних коэффициентов равен 1, например $\Phi = (n, -q, s, 1)$, то мы имеем [если основная единица кольца $O(\Phi)$ есть $a\rho^2 + b\rho + c$, где $\rho^3 = s\rho^2 + q\rho + n$ и $a = a_1\delta$; $b = b_1\delta$ и $(a_1, b_1) = 1$] $K = a_1$; $L = 0$; $\mathrm{K} = a_1 b_1 s - b_1^2$; $\mathrm{L} = 0$, и, следовательно, в виду того, что $(a_1, b_1) = 1$,

оба сравнения (1) и (2) сводятся к одному $P \equiv 0 \pmod{\varkappa\delta}$, и получается тот же алгорнфм повышення, который был рассмотрен в § 75.

12. Критериум остановки для случая целой формы. В этом случае критериумы п. 9 никогда не имеют места, однако здесь существует другой критерий. Если a и b основной единицы $\varepsilon_0 = a\rho^2 + b\rho + c$ делятся соответственно на k^2 и k, где k — целое рациональное число, то можно ρ сразу заменить на $\rho \cdot k$ и нскать двухчленные не в ρ, а в $\rho \cdot k$ единнцы. Единицу, у которой нет такого k, мы будем поэтому называть „приведенной". Докажем теорему:

Никакая степень ε_0^m с целым положительным показателем m не может быть двухчленной в ρ, если ε_0 приведенная и если имеется нечетное простое число π, на которое делится a и b.

Действительно, пусть $a = a_1\pi$; $b = b_1\pi$, ио $a_1 \not\equiv 0 \pmod{\pi}$, тогда коэффициент при ρ^2 в ε_0^m равен

$$m \cdot c^{m-1} \cdot \pi \cdot a_1 + \frac{m(m-1)}{1 \cdot 2} c^{m-2} \cdot \pi^2 \cdot A_2 + \frac{m(m-1)(m-2)}{1 \cdot 2 \cdot 3} c^{m-3}\pi^3 A_3 + \ldots,$$

где A_2, $A_3 \ldots$ — целые рациональные числа. Этот коэффициент не может равняться нулю, так как $(a_1, \pi) = 1$ н $(c, \pi) = 1$, и следовательно, если m точно делится на π^τ, то мы имеем (если $\pi > 2$) $\pi^2 > 3$, $\pi^3 > 4$ н т. д. Мы будем называть всякий общий делитель a и b единицы „делителем" этой единицы.

Пусть ε_0^μ — низшая степень основной единицы ε_0, которая имеет делителя π. Могут тогда быть два случая: или коэффициент при ρ^2 у ε_0^μ делится только на π, или, по крайней мере, на π^2. В первом случае мы будем называть π „первого", а во втором „второго" рода по отношению к ε_0. Легко видеть, что если ε_0^m имеет делителя π, то ε_0^m — степень ε_0^μ. Отсюда ясно, что: *если на некотором шаге алгорифма повышения (не непременно на первом шаге) встретится повышающий множитель π, который есть простое число первого рода по отношению к исходной основной единице, то решений с положительными m нет, и можно прекратить вычисление.* Во всех случаях, когда мы использовали этот способ, мы натыкались на повышающий множитель 1-го рода на одном из первых шагов, на первом или втором шаге обыкновенно, и потому этот способ всегда давал полное решение уравнения. До сих пор, однако, мы не нашли доказательства того, что если нет решений вообще, появится повышающий множитель первого рода хотя бы на каком бы то ни было шаге алгорифма.

В внду того, что при больших π очень сложно непосредственно вычислять ε_0^μ по модулю π^2, мы использовали в таких случаях следующие два определителя, которые облегчают это вычисление. Мы прнведем здесь для сокращения эти определители без вывода. Мы будем предполагать, что π — не делитель дискримннанта числа ρ. В таком случае повышающее простое число π может быть в $\Omega(\rho)$ только лнбо произведением трех различных простых идеалов 1-го порядка $\pi = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, либо произведением идеала 2-го порядка $\mathfrak{q}$ на идеал 1-го порядка $\mathfrak{p}$ $\pi = \mathfrak{q} \cdot \mathfrak{p}$, но не может быть само простым идеалом, так как оно есть делитель нормы двухчленного числа $-a\rho + b + as$.

Необходимое и достаточное условне того, чтобы π было второго рода по отношению к ε, если $\pi = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, есть $\Delta \equiv 0 \pmod{\pi}$, а в случае $\pi = \mathfrak{q} \cdot \mathfrak{p}$ есть $\nabla \equiv 0 \pmod{\pi}$, где определители Δ и ∇ суть:

$$\Delta = \begin{vmatrix} \sigma_1 + \dfrac{\psi(x_1)(2ax_1 + b)}{\varepsilon_1 \cdot f'(x_1)}, & x_1, & 1 \\ \sigma_2 + \dfrac{\psi(x_2)(2ax_2 + b)}{\varepsilon_2 \cdot f'(x_2)}, & x_2, & 1 \\ \sigma_3 + \dfrac{\psi(x_3)(2ax_3 + b)}{\varepsilon_3 \cdot f'(x_3)}, & x_3, & 1 \end{vmatrix}$$

[тут

$$f(x)=x^3-sx^2-qx-n=(x-x_1)(x-x_2)(x-x_3)+\pi\psi(x);\ \sigma_i=\frac{\varepsilon_1^{\pi-1}-1}{\pi};$$

$$\varepsilon_i=ax_i^2+bx_i+c \text{ (где } x_i=x_1,\ x_2,\ x_3);\ f'(x)=3x^2-2sx-q].$$

$$\nabla=\begin{vmatrix} \frac{\varepsilon_1^{\pi-1}-1}{\pi}+\frac{\psi(x_1)(2ax_1+b)}{\varepsilon_1 f'(x_1)}, & x_1, & 1 \\ \frac{(A-B\theta)^{\pi+1}-\nu}{\nu\pi}+\frac{\psi(\beta')(2a\beta'+b)}{(A+B\theta)\cdot f'(\beta')}, & \beta', & 1 \\ \frac{(A+B\theta)^{\pi+1}-\nu}{\nu\pi}+\frac{\psi(\beta'')(2a\beta''+b)}{(A-B\theta)\cdot f'(\beta'')}, & \beta'', & 1 \end{vmatrix}$$

где

$$f(x)=(x-x_1)(x^2+hx+k)+\pi\cdot\psi(x);\quad -\pi<h<\pi;\quad h=2h_1;$$

$$\theta=\sqrt{h_1^2-k};\ \beta'=-h_1+\theta;\ \beta''=-h_1-\theta;\ a\beta'^2+b\beta'+c=A+B\theta;$$

$$\nu=A^2-B^2(h_1^2-k);\ \varepsilon_1=ax_1^2+bx_1+c;\quad f'(x)=3x^2-2sx-q.$$

13. Пример. Форма $(2, 6, 3, 1)=1$, $D=-216$. (Об этом уравненни существует целая маленькая литература, оно связано с уравнением $U^3-V^2=-2$; в 25 томе Math. Zeitschr. A. Brauer дал решение этого уравнення, показав, что если в уравнении $U^3-V^2=-k$, $k=2$, то его можно решить одним специальным методом. Однако еще в 1920 г. при помощи алгорифма повышения нами были вполне решены все уравнения вида $(A, B, C, E)=1$, например с $D<0$ и $|D|<300$, а следовательно и это уравнение.) Форма $(2, 6, 3, 1)\backsim(2, 3, 0, 1)$; $\rho^3=-3\rho+2$; $\varepsilon_0=-\rho^2-\rho+1$; $-a\rho+b+as=\rho-1$; $\varkappa=2$, $\delta=1$, поэтому первый повышающий множитель $\pi=2$. Надо перейти в кольцо $O(\bar{\rho})$, где $\bar{\rho}=2\rho$. Мы получаем $\varepsilon_0^2=-\bar{\rho}^2-3\bar{\rho}+5$; $-\bar{a}\bar{\rho}+\bar{b}+\bar{as}=\bar{\rho}-3$, и поэтому второй повышающий множитель $\bar{\pi}=47$. Так как 47 довольно велико, мы используем приведенные определители. $47=\mathfrak{q}\cdot\mathfrak{p}$, мы должны, следовательно, вычислить $\nabla\cdot x^3+3x-2=(x-25)(x^2-22x+111)+47(x^2-14x+59)$, т. е. $x_1=25$; $\varepsilon_1=649$; $\sigma=\frac{649^{46}-1}{47}\equiv 34\pmod{47}$; $\beta'=11+\theta$, где $\theta=\sqrt{10}$; $A+B\theta=-141-23\theta$; $\nu\equiv 872\pmod{47^2}$; число

$$872^{-1}\cdot 47^{-1}[(-141+23\theta)^{48}-872]\equiv 10\theta-2\pmod{47}.$$

Мы получаем, следовательно, $\nabla\equiv 18\theta\not\equiv 0\pmod{47}$. Простое число 47, поэтому, первого рода по отношению к $\varepsilon_0=-\rho^2-\rho+1$, и, следовательно, уравнение $(2, 6, 3, 1)=1$ не имеет решений. (Надо заметить, что из всех уравнений с $|D|<300$ это уравнение ведет к самым неприятным вычислениям, для всех остальных не приходится прибегать к вычислению Δ или ∇.)

§ 77. О целых кубических уравнениях с данным дискриминаитом

Мы называем кубическое уравненне $z^3=sz^2+qz+n$ целым, если его коэффициенты s, q, n целые рациональные.

Задача — *найти все целые кубические уравнения или, что все равно, все целые кубические иррациональности с данным дискриминантом D,* — очевидно, эквивалентна задаче о представлении чисел кубическими двойничными формами, так как, если найти все максимальные кольца, дискриминанты которых суть делители D, отличающиеся от D на квадратные множители Δ^2, то задача сводится к представлению чисел Δ индексформами соответственных колец.

Если $z^3 = sz^2 + qz + n$ целое уравнение с данным дискриминантом D, то все ему „параллельные“ целые уравнения, т. е. уравнения, получаемые из этого уравнения преобразованием z на $z + r$, где r — любое целое рациональное число, также, очевидно, имеют тот же дискриминант. Каждому решению индекс-форма $= \Delta$ будет соответствовать вся параллель таких уравнений, так как если $[1, \omega_1, \omega_2]$ базис соответственно кольца и $r + x\omega_1 + y\omega_2$ общее число кольца, то переменными в индекс-форме будут только x и y, и они найдутся, а r останется неопределенным. Из всякой параллели таких уравнений можно выбрать представителем уравнение с наименьшим по абсолютной величине s, т. е. такое единственное в данной параллели, у которого $s = -1, 0$ или 1.

В виду того, что для всех $-300 < D < 0$ мы нашли (см. стр. 317) (при помощи алгорифма повышения) все решения уравнений $f(x, y) = 1$, мы можем дать и соответственную табличку представителей всех параллелей всех целых кубических уравнений с этими дискриминантами. На стр. 318 дано начало такой таблицы. Любопытно заметить, как уже „велико“ даже „наименьшее“ из уравнений в 4-й параллели, соответствующей дискриминанту -44.

§ 78. Об уравнении $U^3 - V^2 = k$

Весьма замечательно, что основная наша задача о представлении числа кубической двойничной формой теснейшим образом связана с вопросом о взаимном распределении кубов и квадратов в натуральном ряде чисел, а именно, она оказывается просто равносильной задаче о нахождении кубов и квадратов, разность между которыми есть заданное число k, т. е. задаче о решении в целых числах U, V неопределенного уравнения

$$U^3 - V^2 = k, \tag{1}$$

где k — заданное целое число.

Действительно, мы сейчас покажем (в п. 1), что если найдены все решения всех уравнений $f_i(x, y) = 1$, где f_i — представители всех классов кубических двойничных форм, дискриминанты которых $108k$ (а этих представителей легко найти способом § 30), то мы сможем найти все решения уравнения (1); отсюда, между прочим, также получится, что уравнение (1) *имеет лишь ограниченное число решений.*

С другой стороны, мы покажем (в п. 2), что для того, чтобы найти все решения уравнения

$$f(x, y) = 1, \tag{2}$$

где f — кубическая двойничная форма, определитель которой равен D, достаточно найти все решения уравнения (1) для $k = 3D$.

1. Умножим обе части уравнения (1) на 108; мы получим тогда уравнение $4(3U)^3 - 27(2V)^2 = 108k$. Пусть U, V какое-нибудь решение уравнения (1); сопоставим ему кубическую двойничную форму $x^3 - 3Ux y^2 - 2Vy^3 = (1, 0, -3U, -2V)$, определитель которой равен $108k$; задача о решении уравнения (1), очевидно, равносильна задаче о разыскании всех форм вида $(1, 0, -3U, 2V)$, где U, V — целые рациональные, имеющие определитель $108k$. Найдем представителей всех классов кубических двойничных форм определителя $108k$. Если $f(x, y)$ какая-нибудь из этих форм и в ее классе есть форма вида $(1, 0, -3U, -2V)$, причем $(1, 0, -3U, -2V) = f(x, y)\binom{\alpha\ \beta}{\gamma\ \delta}$, то $f(\alpha, \gamma) = 1$, т. е. $x = \alpha$, $y = \gamma$ — решение уравнения $f(x, y) = 1$. Обратно, если $x = \alpha$, $y = \gamma$ — решение, то, подобрав так β и δ, что $\alpha\delta - \beta\gamma = 1$, мы можем перейти от формы f к эквивалентной ей форме, имеющей равный единице коэффициент при x^3. Очевидно, что при данных α и γ выбор β и δ

неоднозначен, именно, если β_0, δ_0—какие-либо подходящие значения β и δ, то все остальные имеют вид

$$\beta = \beta_0 + t\alpha, \quad \delta = \delta_0 + t\gamma$$

при целом t, откуда следует, что

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta_0 \\ \gamma & \delta_0 \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

Поэтому формы, получающиеся из формы $f(x, y)$ посредством подстановок $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, при определенных α, γ и различных β, δ будут все „параллельны" между собою, т. е. будут получаться одна из другой посредством подстановки $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

Таким образом, каждому решению α, γ уравнения $f(x, y) = 1$ соответствует совокупность параллельных между собою форм, эквивалентных $f(x, y)$ и имеющих равный 1 коэффициент при x^3. В каждой такой совокупности может быть, как легко видеть, не больше одной формы с равным нулю коэффициентом при x^2y. Таким образом, для того чтобы решить уравнение (1), достаточно:

α) Найти по одному представителю $f(x, y)$ из каждого из классов форм определителя 108 k. Эта задача решается в конечном числе действий. Заметим, что при этом необходимо найти не только неприводимые формы, но и приводимые.

β) Решить уравнения $f(x, y) = 1$. Эта задача в случае $D < 0$, т. е. $k < 0$, во многих случаях может быть решена посредством „алгорифма повышения". (Повидимому, всегда, но это не доказано.) В случае приводимой f она решается легко.

γ) Исходя из каждого решения (α, γ), подобрав числа β, δ так, чтобы $\alpha\delta - \beta\gamma = 1$, преобразовать формы $f(x, y)$ к формам, имеющим равный 1 коэффициент при x^3.

δ) Для каждой из этих форм найти параллельную форму вида $x^3 + qxy^2 - ny^3$, если это возможно, или убедиться, что такой формы нет.

ε) Из получившихся форм выбрать те, для которых

$$q \equiv 0 \pmod 3,$$
$$n \equiv 0 \pmod 2,$$

тогда $U = -\frac{q}{3}$, $V = \frac{n}{2}$ будет решением уравнения (1). Этим способом получатся все решения.

Если форма $f(x, y)$ приводима, то она либо не эквивалентна форме вида $x^3 + qxy^2 - ny^3$, либо если эквивалентна такой форме, то ее можно заменить этой формой и искать уже решения уравнения $x^3 + qxy^2 - ny^3 = 1$, но если форма f приводима, то и эта форма приводима, и тогда она имеет вид $(x + ry)(x^2 + gxy + ty^2)$, и, следовательно, все сводится к тому, чтобы найти такие целые x, y, что либо одновременно

$$\left.\begin{aligned} x + ry &= 1, \\ x^2 + gxy + ty^2 &= 1, \end{aligned}\right\}$$

либо

$$\left.\begin{aligned} x + ry &= -1, \\ x^2 + gxy + ty^2 &= -1. \end{aligned}\right\}$$

Таким образом, решений будет в этом случае всего не больше чем 4. Если форма $f(x, y)$ неприводима и $k < 0$, т. е. $D < 0$, то по основной теореме

§ 75 число решений уравнения $f(x, y)=1$ не более трех, так как

$$D=108k\neq -23,\ -31,\ -44.$$

В случае же $k>0$, т. е. $D>0$, мы имеем по Зигелю (см. § 70, с дополнением Фаддеева) только, что число решений не больше, чем 15, поэтому мы получаем, что число решений уравнения (1) в случае $k<0$ не больше, чем $4h$, а в случае $k>0$ не больше, чем $15h$, где h число классов кубических двойничных форм определителя $108k$.

2. Посмотрим теперь, наоборот, как сводится решение уравнения (2) на решение уравнения (1). Мы имеем тождество Кэлн между ковариантами кубической двойничной формы

$$4H^3-Q^2=27Df^2.$$

Оно непосредственно вытекает из выражений ковариантов, данных в лемме II, § 32. Из него следует, что если уравнение $f(x, y)=1$ имеет решение (x_0, y_0), то уравнение $U^3-V^2=16\cdot 27D$ имеет решение $U=4H(x_0, y_0)$, $V=4Q(x_0, y_0)$.

Если, следовательно, найти все решения U, V уравнения $U^3-V^2=16\cdot 27\cdot D$, то решение уравнения $f(x, y)=1$ приводится к отысканию всех целых решений системы $\left.\begin{matrix}4H(x, y)=U\\ f(x, y)=1\end{matrix}\right\}$. Эта же задача решается тривиально.

Приложим еще небольшую табличку всех решений уравнений

$$U^3-V^2=k, \quad \text{для} \quad k=-1,\ -2,\ -3,\ -4,\ -5 \text{ и } -6.$$

-1	-2	-3	-4	-5	-6
$-1, 0$ $0, 1$ $2, 3$	$-1, 1$	$1, 2$	$0, 2$	$-1, 2$	Нет решений

Уравнение $U^3-V^2=-8$ имеет всего 4 решения:

$$U=-2,\ 2,\ 46,\ 1,$$
$$V=\ 0,\ 4,\ 312,\ 3;$$

первое решение соответствует приводимому классу, второе и третье — одному из неприводимых классов, четвертое — другому неприводимому классу.

Уравнение $U^3-V^2=-17$ ведет к дискриминанту $D=-108\cdot 17=-1836$. Такой дискриминант имеет, например, кольцо, образованное уравнением $\rho^3=-6\rho+6$, и мы получаем сразу одно решение $U=-2$, $V=3$; основная единица этого кольца есть $\varepsilon_0=-\rho+1$, соответственно этой двучленной единице мы получаем второе решение $U=8$, $V=23$; четвертая степень основной единицы $\varepsilon_0^4=26\rho-23$ опять двучленная единица, соответствующее ей решение есть $U=5234$, $V=378661$, и мы получаем те близкие куб и квадрат 143 384 152 904 и 143 384 152 921, которые одним эвристическим способом нашел впервые, повидимому, Веребрюссов (см. Матем. сб., т. XXVI), причем надо отметить, что давшая их двухчленная единица имеет совсем небольшие коэффициенты: 26 и -23.

ТАБЛИЦА ВСЕХ ПРЕДСТАВЛЕНИЙ ЧИСЛА 1 ВСЕМИ КУБИЧЕСКИМИ ДВОЙНИЧНЫМИ ФОРМАМИ ОТРИЦАТЕЛЬНЫХ ДИСКРИМИНАНТОВ, ДИСКРИМИНАНТЫ КОТОРЫХ НЕ ПРЕВОСХОДЯТ 300 ПО АБСОЛЮТНОЙ ВЕЛИЧИНЕ

[Таблица вычислена Б. Делоне (13)]

$-D$	Основное ур-ние	Основная единица	Δ	Решения	ч. р.
23	$\varepsilon^3 = -\varepsilon^2 + 1$	ε	1	$\varepsilon^{-2} = \varepsilon + 1;\ \varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;$ $\varepsilon^5 = -\varepsilon + 1;\ \varepsilon^{14} = 4\varepsilon - 3$	5
31	$\varepsilon^3 = -\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;\ \varepsilon^2 = -\varepsilon + 1;$ $\varepsilon^8 = 3\varepsilon - 2$	4
44	$\varepsilon^3 = -\varepsilon^2 - \varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;\ \varepsilon^4 = 2\varepsilon - 1;$ $\varepsilon^{17} = -103\varepsilon + 56$	4
59	$\varepsilon^3 = -2\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;\ \varepsilon^3 = -2\varepsilon + 1$	3
76	$\varepsilon^3 = \varepsilon^2 - 3\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;\ \varepsilon^8 = -36\varepsilon + 13$	3
83	$\varepsilon^3 = -2\varepsilon^2 - 2\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
87	$\varepsilon^3 = -\varepsilon^2 - 2\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
104	$\rho^3 = \rho + 2$	$-\rho^2 + \rho + 1$	2	$\varepsilon^0 = 1;\ \varepsilon^2 = 2\rho - 3$	2
107	$\varepsilon^3 = 2\varepsilon^2 - 4\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;\ \varepsilon^4 = -7\varepsilon + 2$	3
108	$\rho^3 = 2$	$\rho - 1$	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \rho - 1$	2
116	$\rho^3 = \rho^2 + 2$	$\rho^2 - \rho - 1$	2	$\varepsilon^0 = 1$	1
135	$\varepsilon^3 = -3\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;\ \varepsilon^3 = -3\varepsilon + 1$	3
139	$\varepsilon^3 = 4\varepsilon^2 - 6\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
140	$\varepsilon^3 = 3\varepsilon^2 - 5\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
152	$\rho^3 = \rho^2 + 2\rho + 2$	$-\rho^2 + \rho + 3$	2	$\varepsilon^0 = 1$	1
172	$\rho^3 = 2\rho^2 + 2$	$-\rho^2 + 2\rho + 1$	2	$\varepsilon^0 = 1$	1
175	$\varepsilon^3 = -2\varepsilon^2 - 3\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
176	$\varepsilon^3 = -\varepsilon^2 - 3\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
199	$\varepsilon^3 = \varepsilon^2 - 4\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
200	$\rho^3 = 2\rho^2 - 3\rho + 4$	$\rho^2 - \rho - 1$	2	$\varepsilon^0 = 1$	1
204	$\rho^3 = \rho^2 - \rho + 3$	$-\rho^2 + \rho + 1$	3	$\varepsilon^0 = 1$	1
211	$\varepsilon^3 = 6\varepsilon^2 - 10\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
212	$\rho^3 = \rho^2 - 4\rho + 2$	$2\rho - 1$	8	$\varepsilon^0 = 1;\ \varepsilon^1 = 2\rho - 1$	2
216	$\rho^3 = -3\rho + 2$	$-\rho^2 - \rho + 1$	2	$\varepsilon^0 = 1$	1
231	$\varepsilon^3 = -4\varepsilon^2 - 5\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
236	$\rho^3 = 2\rho^2 + \rho + 2$	$\rho^2 - 3\rho + 1$	4	$\varepsilon^0 = 1$	1
239	$\rho^3 = \rho + 3$	$\rho^2 - \rho - 1$	3	$\varepsilon^0 = 1;\ \varepsilon^2 = 3\rho - 5$	2
243	$\varepsilon^3 = -\varepsilon^2 - 12\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
244	$\rho^3 = 5\rho^2 - 4\rho + 2$	$-2\rho^2 + 10\rho - 7$	16	$\varepsilon^0 = 1$	1
247	$\varepsilon^3 = -3\varepsilon^2 - 4\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
255	$\varepsilon^3 = 5\varepsilon^2 - 8\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
268	$\varepsilon^3 = 7\varepsilon^2 - 13\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon$	2
279	$\varepsilon^3 = 2\varepsilon^2 - 5\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = 2$	2
283	$\varepsilon^3 = -4\varepsilon + 1$	ε	1	$\varepsilon^0 = 1;\ \varepsilon^1 = \varepsilon;\ \varepsilon^3 = -4\varepsilon + 1$	3
300	$\rho^3 = 4\rho^2 - 2\rho + 2$	$-\rho^2 + 5\rho - 5$	9	$\varepsilon^0 = 1$	1

ТАБЛИЦА ВСЕХ НЕПАРАЛЛЕЛЬНЫХ ДРУГ ДРУГУ КУБИЧЕСКИХ УРАВНЕНИЙ ОТРИЦАТЕЛЬНЫХ ДИСКРИМИНАНТОВ, НЕ ПРЕВОСХОДЯЩИХ 172 ПО АБСОЛЮТНОЙ ВЕЛИЧИНЕ, ИМЕЮЩИХ НАИМЕНЬШИЕ s.

[Таблица вычислена Б. Делоне (13)]

D	s	q	n	D	s	q	n
	1	−2	1	−87	−1	−2	1
	−1	0	1		−1	2	3
−23	0	1	1				
	−1	4	5	−104	0	1	2
	0	55	157		1	46	106
	0	−1	1		1	−3	2
	1	0	1	−107	1	3	2
−31	1	2	1		−1	157	812
	0	17	27				
				−108	0	0	2
	−1	−1	1		0	6	6
	1	1	1	−116	1	0	2
−44	1	11	11				
	−1	31281	2139919		0	−3	1
				−135	0	3	3
					0	33	73
−59	0	−2	1				
	−1	1	2	−139	−1	−1	2
	1	9	8		0	8	9
				−140	0	−2	2
−76	1	−3	1		−1	5	7
	0	2	2				
	1	3077	64681	−152	1	2	2
−83	1	−1	2	−172	2	0	2
	−1	3	4				

Б. РЕШЕНИЕ НЕОПРЕДЕЛЕННЫХ УРАВНЕНИЙ 3-й СТЕПЕНИ С ДВУМЯ НЕИЗВЕСТНЫМИ В ДРОБНЫХ ЧИСЛАХ

§ 79. О рациональных точках на кривых 3-го порядка

В главе V и в предыдущих параграфах этой главы мы занимались неопределенными уравнениями высших степеней с двумя неизвестными, интересуясь их решением в целых числах. В геометрической трактовке решение таких уравнений равносильно отысканию точек с целыми координатами на алгебраической кривой. При этом мы главным образом занимались уравнениями третьего порядка. Решения таких уравнений вида $f(x, y)=1$, где $f(x, y)$ форма, мы искали среди алгебраических единиц, т. е. среди решений уравнения

$$N(x_1, x_2, x_3)=1,$$

где N — форма Дирихле, все решения которого можно найти, пользуясь некоторыми периодическими алгорифмами. Трудность решения состояла в том, чтобы среди известного, но бесконечного множества решений найти решения некоторого определенного „выродившегося“ вида.

В настоящем параграфе мы займемся решением двойничных кубических уравнений в рациональных числах. Эта задача оказывается существенно отлич-

ной от предыдущей. Для весьма широкого класса таких уравнений форма общего решения, если только решение существует, несколько напоминает форму решения уравнения

$$N(x_1, x_2, x_3) = 1$$

(N — форма Дирихле), решение которого определяется единицами области. Именно, все решения получаются из некоторых „основных решений" посредством операций, напоминающих возведение в степень и перемножение основных единиц. Исключения из этого правила представляют также весьма широкий класс уравнений.

Решение двойничных уравнений $\Phi(u, v) = 0$, где $\Phi(u, v)$, вообще говоря, неоднородный многочлен от u и v, в рациональных числах u, v, очевидно, равносильно решению некоторых тройничных однородных уравнений в целых числах.

Действительно, положив в решении уравнения $\Phi(u, v) = 0$

$$u = \frac{x}{z}, \quad v = \frac{y}{z},$$

где z — общий знаменатель u и v, и умножая на z^s, получим, что x, y, z являются решениями в целых числах однородного тройничного уравнения

$$z^s \Phi\left(\frac{x}{z}, \frac{y}{z}\right) = F(x, y, z) = 0.$$

Обратно, каждому решению в целых числах уравнения $F(x, y, z) = 0$ при $z \neq 0$ соответствует решение в рациональных числах двойничного уравнения

$$\Phi(u, v) = F(u, v, 1) = 0.$$

При этом пропорциональным решениям уравнения $F(x, y, z) = 0$ соответствует одно и то же решение уравнения $f(u, v) = 0$, и, обратно, каждому решению второго уравнения соответствует бесконечно много пропорциональных решений первого.

Решению уравнения $F(x, y, z) = 0$ при $z = 0$ не соответствует реально существующее решение уравнения $\Phi(u, v) = 0$. Однако для большей простоты и для того, чтобы не было необходимости вводить специальные оговорки, целесообразно рассматривать „рациональные решения" уравнения $\Phi(u, v) = 0$ также и вида $\left(\frac{x}{0}, \frac{y}{0}\right)$, понимая под каждым таким решением не более как факт существования решения $(x, y, 0)$ для уравнения $F(x, y, z) = 0$.

Такие решения мы будем называть бесконечно далекими. Только тривиальному решению $(0, 0, 0)$ уравнения $F(x, y, z) = 0$ мы не сопоставляем никакого решения уравнения $\Phi(u, v) = 0$.

В геометрической трактовке решение уравнения $\Phi(u, v) = 0$ в рациональных числах выглядит как задача об отыскании точек с рациональными координатами на кривых. Бесконечно далеким решениям уравнения $f(u, v) = 0$ соответствуют бесконечно далекие точки с рациональными координатами, т. е. рациональные направления бесконечных ветвей кривой. В дальнейшем изложении мы будем придерживаться геометрической терминологии.

Характер распределения рациональных точек на алгебраической кривой существенно зависит от рода кривой, который определяется как $\frac{m-1}{2}$, где m — число связности *комплексной* кривой (точнее, поверхности Римана) $\Phi(u, v) = 0$, которая представляет собой двухмерное многообразие в четырехмерном пространстве.

Род нераспадающейся кривой определяется по известной формуле

$$p = \frac{(n-1)(n-2)}{2} - d,$$

где p — род, n — степень кривой, d — число двойных точек кривой (причем ν-кратная точка принимается за $\frac{\nu(\nu-1)}{2}$ двойных точек по вполне понятным геометрическим соображениям).

Кривая третьего порядка может быть или нулевого, или первого рода, в зависимости от того, имеет ли она двойную точку, или нет. Нераспадающаяся кривая третьего порядка, очевидно, не может иметь больше одной двойной точки.

Кривые нулевого рода называются также уникурсальными кривыми.

Прежде всего решим задачу о распределении рациональных точек на уникурсальных кривых третьего порядка, именно — докажем, что уникурсальная кривая третьего порядка, уравнение которой имеет рациональные коэффициенты, содержит бесконечно много рациональных точек, и укажем способ для их разыскания.

Действительно, пусть кривая третьего порядка

$$\Phi(u,\ v)=0$$

уникурсальна, т. е. имеет двойную точку.

Координаты двойной точки, как известно, удовлетворяют уравнениям:

$$\left.\begin{aligned}\Phi(u,\ v)&=0,\\ \Phi'_u(u,\ v)&=0,\\ \Phi'_v(u,\ v)&=0.\end{aligned}\right\}\qquad (*)$$

Все эти уравнения имеют рациональные коэффициенты. Поэтому координаты $(u,\ v)$ могут быть только алгебраическими. Пусть $R(u,\ v)$ — поле, получающееся присоединением чисел u и v к полю рациональных чисел. В виду того, что уравнения (*) имеют рациональные коэффициенты, они будут удовлетворяться вместе с числами u, v также и сопряженными числами $(u',\ v')$ и т. д. Отсюда заключаем, что если бы поле $R(u,\ v)$ было отлично от поля рациональных чисел, то кривая $\Phi(u,\ v)=0$ имела бы больше одной двойной точки, что невозможно. Следовательно, поле $R(u,\ v)$ совпадает с полем рациональных чисел и потому u, v оба рациональны.

Итак, мы доказали, что двойная точка уникурсальной кривой третьего порядка с рациональными коэффициентами имеет рациональные координаты.

Рассмотрим пучок прямых

$$v-v_0=t(u-u_0),$$

проходящих через двойную точку кривой третьего порядка с рациональными угловыми коэффициентами t.

Каждая прямая этого пучка будет пересекаться с кривой $\Phi(u,\ v)=0$ в одной точке, кроме двойной, и эта точка будет иметь рациональные координаты. Действительно, уравнение третьей степени с рациональными коэффициентами

$$\Phi(u,\ v_0+t(u-u_0))=0,$$

к решению которого приводит совместное решение уравнений кривой и прямой, будет иметь двойной рациональный корень u_0, следовательно, третий корень этого уравнения будет также рационален.

Таким образом каждому рациональному значению параметра t в уравнении пучка прямых соответствует рациональная точка на кривой $\Phi(u,\ v)=0$.

Очевидно и обратное, что каждая рациональная точка на кривой $f(u,\ v)=0$ соответствует рациональному значению параметра t, ибо угловой коэффициент прямой, соединяющей любую рациональную точку на кривой с рациональной же двойной точкой, будет рационален.

Таким образом мы получим все рациональные точки, решив совместно уравнения

$$\Phi(u, v) = 0 \quad \text{и} \quad v - v_0 = t(u - u_0)$$

в общем виде и придавая затем параметру t все рациональные значения.

Итак, задача о рациональных точках на уникурсальных кривых третьего порядка решена до конца, и в дальнейшем мы будем исключительно заниматься более интересным случаем кривых 1-го рода, не имеющих двойной точки.

Прежде всего отметим два предложения почти очевидных, но чрезвычайно важных для дальнейшего.

Теорема 1. *Касательная к кривой третьего порядка, проведенная в рациональной точке, пересекает кривую в рациональной точке.*

Теорема 2. *Секущая, соединяющая две рациональных точки кривой, пересекает кривую в третьей рациональной точке.*

Доказательство. Пусть $v - v_0 = t(u - u_0)$ уравнение секущей, соединяющей две рациональных точки кривой $f(u, v) = 0$, или касательной, проведенной в рациональной точке. В обоих случаях это уравнение, очевидно, имеет рациональные коэффициенты. Уравненне 3-й степени

$$\Phi(u, v_0 + t(u - u_0)) = 0,$$

к решению которого приводится совместное решение уравнений кривой и прямой, также имеет рациональные коэффицненты. Это уравнение имеет два известных рациональных корня, если прямая есть секущая, и один двойной рациональный корень, если прямая — касательная. Следовательно, 3-й корень u этого уравнения, являющийся абсциссой, интересующей нас точки пересечения, тоже рационален.

Ордината v также рациональна в виду того, что v рационально выражается через u. Обе теоремы доказаны.

А. Пуанкаре высказал предположение, что все рациональные точки на кривой третьего порядка могут быть получены из конечного числа некоторых основных точек посредством операций проведения секущих и касательных. Предположение А. Пуанкаре было впервые доказано Морделлем в 1922 г. Доказательство Морделля было несколько упрощено и значительно обобщено А. Вейлем в нескольких работах, посвященных этому вопросу.

Мы здесь докажем теорему Морделля, используя доказательство А. Вейля, но оставив в стороне его обобщения. Для доказательства нам будут нужны некоторые вспомогательные преобразования, к изложению которых мы и перейдем в следующем параграфе.

§ 80. Бирациональное преобразование

Две алгебраические кривые $f(u, v) = 0$ и $f_1(u_1, v_1) = 0$ называются связанными посредством бирационального преобразования, если координаты всех точек первой кривой рационально выражаются через координаты точек второй кривой, и, обратно, координаты точек второй кривой рационально выражаются через координаты точек первой кривой. Очевидно, что задачи об отыскании рациональных точек на кривых, связанных бирациональным преобразованием, равносильны, в случае если коэффициенты в выражении координат точек одной кривой через координаты точек другой в обе стороны рациональны.

Покажем, что от любой кривой третьего порядка, уравнение которой имеет рациональные коэффициенты, можно перейти к некоторой кривой специального канонического вида, связанной с исходной посредством бирационального преобразования с рациональными коэффициентами, если только исходная кривая содержит хотя бы одну рациональную точку.

Действительно, пусть кривая
$f(u, v) = Au^3 + Bu^2v + Cuv^2 + Dv^3 + Eu^2 + Fuv + Gv^2 + Hu + Kv + M = 0$
имеет рациональную точку (u_0, v_0).

Перенесем начало координат в точку пересечения (u_1, v_1) касательной к кривой $f(u, v) = 0$ в точке (u_0, v_0) с самой кривой и затем повернем оси координат так, чтобы новая ось Ou совпадала с касательной в точке (u_0, v_0). При подходящем выборе масштаба в новых осях это преобразование будет бирациональным с рациональными коэффициентами. Уравнение кривой после этого преобразования примет вид:

$$A'u^3 + B'u^2v + C'uv^2 + D'v^3 + E'u^2 + F'uv + G'v^2 + H'u + K'v = 0.$$

Свободный член будет отсутствовать.

Затем проведем через новое начало координат пучок прямых линий. Каждая прямая этого пучка будет встречать кривую в начале координат и еще в двух точках, координаты которых получаются посредством решения некоторого квадратного уравнения.

Действительно, положив $v = tu$, получим:

$$(A' + B't + C't^2 + D't^3)\,u^3 + (E' + F't + G't^2)\,u^2 + (H' + K't)\,u = 0,$$

откуда

$$u = 0,$$

или

$$u = \frac{-E' - F't - G't^2 \pm \sqrt{(E' + F't + G't^2)^2 - 4(H' + K't)(A' + B't + C't^2 + D't^3)}}{2(A' + B't + C't^2 + D't^3)}.$$

Обозначив $\pm\sqrt{(E' + F't + G't^2)^2 - 4(H' + K't)(A' + B't + C't^2 + D't^3)}$ через s, получим, что исходная кривая бирациональным преобразованием с рациональными коэффициентами связана с кривой 4-го порядка

$$s^2 = (E' + F't + G't^2)^2 - 4(H' + K't)(A' + B't + C't^2 + D't^3).$$

Действительно,

$$u = \frac{-E' - F't - G't^2 + s}{2(A' + B't + C't^2 + D't^3)},$$
$$v = tu$$

и обратно,

$$t = \frac{v}{u},$$

$$s = E' + F't + G't^2 + 2u(A' + B't + C't^2 + D't^3).$$

То обстоятельство, что ось Ou является касательной к исходной кривой, говорит о том, что квадратное уравнение для определения u должно иметь двойной корень при $t = 0$. Это возможно в том и только в том случае, если

$$E'^2 - 4A'H' = 0.$$

Таким образом свободный член в правой части уравнения кривой 4-го порядка

$$s^2 = (E' + F't + G't^2)^2 - 4(A' + B't + C't^2 + D't^3)(H' + K't)$$

равен 0.

Запишем это уравнение в более простой форме, введя обозначения для коэффициентов в правой части:

$$s^2 = at + bt^2 + ct^3 + dt^4.$$

Умножим теперь обе части уравнения на $\frac{4a^2}{t^4}$ и обозначим

$$\frac{2as}{t^2}=\eta';\quad \frac{a}{t}+\frac{b}{3a}=\xi'.$$

Заданное этими равенствами преобразование, очевидно, бирационально. После этого преобразования наша кривая преобразуется в кривую

$$\eta'^2=4\xi'^3-g_2'\xi'-g_3',$$

где g_2' и g_3' — рациональные постоянные, просто выражающиеся через a, b, c, d. Сделав, наконец, бирациональное преобразование

$$\eta'=\alpha^3\eta,\quad \xi'=\alpha^2\xi,$$

где α — подходящим образом подобранное рациональное число, преобразуем уравнение к виду

$$\eta^2=4\xi^3-g_2\xi-g_3,$$

где g_2 и g_3 — целые рациональные числа, не делящиеся соответственно на четвертую и шестую степень одного и того же числа, отличного от 1.

Кривая

$$\eta^2=4\xi^3-g_2\xi-g_3$$

связана посредством бирациональиого преобразования с исходной кривой

$$f(u, v)=0.$$

Кривая вида

$$\eta^2=4\xi^3-g_2\xi-g_3$$

иосит название иормальной формы Вейерштрасса кривой 3-го порядка.

Правая часть уравнения кривой в нормальиой форме Вейерштрасса не должна иметь кратного корня, если мы исходили из кривой первого рода, ибо в противном случае нормальная кривая, а следовательно и исходная имели бы двойную точку.

Это преобразование в случае, если точка пересечения касательной с кривой будет бесконечно далекой точкой, надо несколько изменить, так как перемещение начала координат в бесконечно далекую точку бессмысленно. Однако преобразование все же возможно, что очевидно вследствие возможности введения однородных координат.

Преобразование кривой 3-го порядка без двойной точки к нормальной форме позволяет ввести весьма удобный аналитический аппарат для изучения кривой.

Именно, кривая

$$\eta^2=4\xi^3-g_2\xi-g_3$$

униформизируется посредством эллиптических функций Вейерштрасса

$$\xi=\wp(t),$$
$$\eta=\wp'(t).$$

Бесконечно далекая точка кривой соответствует значению параметра $t=0$.

Известно далее, что для значений t_1, t_2, t_3 параметра, соответствующих трем точкам, лежащим на одной прямой, выполняются соотношения

$$t_1+t_2+t_3\equiv 0 \pmod{\omega_1, \omega_2},$$

где ω_1, ω_2 — периоды эллиптической функции $\gamma(t)$. Благодаря этому операции построения рациональных точек посредством проведения секущих и касательных через другие точки соответствуют операциям сложения и удвоения значений аргумента эллиптической функции (с изменением знака результата на обратный).

В виду того, что действие сложения ассоциативно, операция построения новых точек посредством построения секущих тоже в некотором смысле ассоциативна. Именно, пусть T_1, T_2, T_3 — три точки на кривой, которым соответствуют значения параметров t_1, t_2, t_3.

Точку T, соответствующую значению параметра $-t_1-t_2-t_3$, можно построить несколькими способами.

Так, способ построения точки T, основанный на представлении $-t_1-t_2-t_3$ в виде $-(t_1+t_2)-t_3$, состоит в следующем.

1. Через точки T_1 и T_2 проводится секущая. Третья точка N' пересечения этой секущей с кривой соответствует значению параметра $-t_1-t_2$.

2. Строится точка N, симметричная с точкой N' относительно оси $O\xi$. Точка N соответствует значению параметра t_1+t_2.

3. Через точки N и T_3 проводится секущая. Третья точка пересечения этой секущей с кривой и будет искомой точкой T.

Представив $-t_1-t_2-t_3$ в виде $-t_1-(t_2+t_3)$, получим другой способ построения точки T.

1. Находится точка M' пересечения кривой с секущей T_2T_3.

2. Находится симметричная с M' точка M.

3. Находится точка T пересечения кривой с секущей MT_1.

Оба эти способа должны дать одну и ту же точку, что непосредственно не является очевидным.

Однако ассоциативность операции построения точек посредством проведения секущих может быть доказана и без введения эллиптических функций.

В дальнейшем мы будем называть построение точки T, симметричной с точкой пересечения кривой с секущей T_1T_2, сложением точек T_1 и T_2; построение точки, симметричной с точкой пересечения кривой с касательной в точке T_1,— удвоением точки T_1 и т. д.

Повторяем, что переместительность сложения точек геометрически очевидна, ассоциативность сложения точек можно установить посредством введения эллиптических функций, но она может быть доказана и иначе, например непосредственным вычислением.

Все дальнейшие рассуждения мы имеем возможность провести не пользуясь эллиптическими функциями, но только используя переместительность и ассоциативность сложения точек. Однако в тех случаях, где это будет облегчать формулировку, мы все же будем обращаться к эллиптическим функциям.

§ 81. Доказательство теоремы Морделя, данное А. Вейлем

Переходим к доказательству основной теоремы этой теории о том, что все рациональные точки на кривой третьего порядка могут быть получены из конечного числа основных точек посредством проведения секущих и касательных, т. е. посредством действия сложения значений аргумента эллиптических функций, соответствующих рациональным точкам. Достаточно доказать эту теорему для кривых, заданных в нормальной форме. Для нас будет удобно остановиться на нормальной форме, несколько отличной от формы Вейерштрасса, именно на форме

$$u^2 = v^3 - h_2 v - h_3,$$

которая получается из формы

$$\eta^2 = 4\xi^3 - g_2\xi - g_3$$

подстановкой $\eta = \frac{u}{4}$, $\xi = \frac{v}{4}$.

Числа h_2 и h_3 можно считать целыми и не делящимися соответственно на квадрат и куб одного и того же целого числа, отличного от 1.

Правая часть нормальной формы уравнения

$$v^3 - h_2 v - h_3$$

не имеет кратных корней. Следовательно, уравнение

$$v^3 - h_2 v - h_3 = 0$$

определяет некоторую кубическую область, приводимую или неприводимую. Корни уравнения $v^3 - h_2 v - h_3 = 0$ обозначим через ρ, ρ' ρ''.

Уравнение

$$u^2 = v^3 - h_2 v - h_3$$

можно представить в виде

$$N(v - \rho) = u^2.$$

Решение этого уравнения равносильно решению задачи о выборе из всех целых и дробных чисел кубической области, нормы которых являются полными квадратами чисел специального *двухчленного* вида $v - \rho$.

Среди чисел, нормы которых являются полными квадратами, находятся все квадраты чисел области и кроме того многие другие числа.

Разбиваем все такие числа на классы, объединяя в одном классе все числа, отличающиеся одно от другого множителем, равным квадрату числа области. Квадраты всех чисел области попадают в один класс, который мы будем называть главным. Всего классов в данной кубической области бесконечно много. Классы можно перемножать, так как произведение двух чисел, взятых из данных классов, принадлежит вполне определенному классу. Главный класс играет роль единицы в этом умножении. Квадрат каждого класса дает главный класс. Как мы уже говорили, в каждой кубической области существует бесконечно много классов чисел, нормы которых являются полными квадратами. Однако имеет место следующая теорема.

Теорема 1. Двухчленные числа $v - \rho$, *нормы которых являются квадратами, могут принадлежать лишь* конечному *числу классов.*

Доказательство. Пусть $N(v - \rho) = u^2$.

Представим рациональное число v в виде несократимой дроби $\frac{a}{b}$ и докажем прежде всего, что знаменатель b этой дроби должен быть полным квадратом. Действительно, $(a, b) = 1$, и, следовательно, $N(a - b\rho)$ и b — взаимно просты. Очевидно, имеет место равенство $N(a - b\rho) = b^3 u^2$ и, следовательно,

$$bN(a - b\rho) = (b^2 u)^2.$$

Произведение двух целых взаимно простых чисел равно полному квадрату. Следовательно, каждый из множителей представляет собой полный квадрат

$$b = c^2 \qquad (a, c) = 1$$
$$N(a - c^2\rho) = n^2.$$

Числа $v - \rho$ и $a - c^2\rho$ принадлежат, очевидно, к одному классу чисел с квадратными нормами, поэтому нам достаточно доказать конечность числа классов для чисел вида $a - c^2\rho$.

Разложим целое число $a - c^2\rho$ на простые идеалы и выделим в этом разложении полный квадрат

$$a - c^2\rho = \mathfrak{a}\mathfrak{b}^2.$$

Здесь идеал $\mathfrak{a}$ не делится ни на один квадрат простого идеала.

Введем в рассмотрение число $\lambda = (a - c^2\rho')(a - c^2\rho'')$. В виду того, что $\lambda(a - c^2\rho)$ представляет собою квадрат целого рационального числа, число λ должно делиться на идеал $\mathfrak{a}$.

Сопоставляя сравнения

$$a - c^2\rho \equiv 0 \pmod{\mathfrak{a}},$$

$$\lambda = (a - c^2\rho')(a - c^2\rho'') \equiv 0 \pmod{\mathfrak{a}},$$

легко получаем, что

$$c^4(\rho - \rho')(\rho - \rho'') \equiv 0 \pmod{\mathfrak{a}}.$$

Но c и $\mathfrak{a}$, очевидно, взаимно просты. Следовательно, $\mathfrak{a}$ является делителем дифференты $(\rho - \rho')(\rho - \rho'')$ числа ρ, и, следовательно, для идеала $\mathfrak{a}$ имеется лишь конечное число возможностей. Очевидно далее, что для чисел $\mathfrak{a}\mathfrak{b}^2$, принадлежащих одному классу, идеалы $\mathfrak{a}$ одинаковы, а идеалы $\mathfrak{b}$ эквивалентны. Обратно, числа $\mathfrak{a}\mathfrak{b}^2$, для которых идеалы $\mathfrak{a}$ одинаковы и идеалы $\mathfrak{b}$ эквивалентны, могут отличаться друг от друга множителем, состоящим из квадрата числа области и единицы. Следовательно, числа $\mathfrak{a}\mathfrak{b}^2$ при данном идеале $\mathfrak{a}$ и при данном классе для $\mathfrak{b}$ могут распределиться на два класса для областей отрицательного дискриминанта и на четыре класса для областей с положительным дискриминантом.

Теорема доказана, так как для двухчленных чисел число возможностей для идеала $\mathfrak{a}$ конечно, число возможностей для класса, которому принадлежит идеал $\mathfrak{b}$ тоже конечно, и, наконец, числа вида $\mathfrak{a}\mathfrak{b}^2$ с одинаковыми идеалами $\mathfrak{a}$ и эквивалентными идеалами $\mathfrak{b}$ распределяются самое большое по четырем классам.

Итак, хотя все числа с квадратными нормами распределяются в бесконечное множество классов, двухчленные числа $v - \rho$ с квадратными нормами распределяются в конечное число классов. Все классы образуют группу относительно умножения. Мы не можем этого утверждать для двухчленных чисел $v - \rho$, так как произведение двухчленных чисел не является двухчленным. Однако мы имеем возможность составлять по двум двухчленным числам с квадратной нормой третье другим способом. Каждое двухчленное число $v - \rho$ с квадратной нормой u^2 соответствует точке (u, v) с рациональными координатами на кривой

$$u^2 = v^3 - h_2 v - h_3.$$

Такие точки мы умеем „складывать", точнее, складывать значения аргументов эллиптических функций, соответствующих этим точкам.

Теорема 2. *При „сложении" точек* (u_1, v_1) и (u_2, v_2) *кривой* $u^2 = v^3 - h_2 v - h_3$ *классы, которым принадлежат числа* $v_1 - \rho$ и $v_2 - \rho$, *перемножаются.*

Доказательство. „Суммой" двух точек (u_1, v_1) и (u_2, v_2), как мы уже знаем, является точка, симметричная с точкой пересечения кривой с секущей, соединяющей точки (u_1, v_1) и (u_2, v_2). Абсцисса v „суммы" точек (u_1, v_1) и (u_2, v_2) совпадает с абсциссой точки пересечения кривой и секущей.

Для определения числа v исключаем u из уравнения кривой $u^2 = v^3 - h_2 v - h_3$ и из уравнения секущей

$$u - u_1 = \frac{u_2 - u_1}{v_2 - v_1}(v - v_1).$$

Для определения v получаем кубическое уравнение

$$v^3 - h_2 v - h_3 = \left[u_1 + \frac{u_2 - u_1}{v_2 - v_1}(v - v_1)\right]^2,$$

корнями которого, кроме v, будут также v_1 и v_2.

Заменим $v-\rho=\lambda$; $v_1-\rho=\lambda_1$; $v_2-\rho=\lambda_2$.
Уравнение преобразуется в следующее:

$$\lambda^3+H_1\lambda^2+H_2\lambda=\left[u_1+\frac{u_2-u_1}{\lambda_2-\lambda_1}(\lambda-\lambda_1)\right]^2.$$

Свободного члена в левой части уравнения не будет, так как $v^3-h_2v-h_3$ делится на $v-\rho$. Корнями этого уравнения будут $v-\rho$; $v_1-\rho$; $v_2-\rho$. В виду того, что произведение корней уравнения равно свободному члену с обратным знаком,

$$(v-\rho)(v_1-\rho)(v_2-\rho)=\left[u_1-\lambda_1\frac{u_2-u_1}{\lambda_2-\lambda_1}\right]^2=\left[\frac{u_1\lambda_2-u_2\lambda_1}{v_2-v_1}\right]^2,$$

откуда

$$v-\rho=(v_1-\rho)(v_2-\rho)\cdot\left[\frac{u_2-u_1}{\lambda_2-\lambda_1}\right]^2.$$

Из этого равенства справедливость теоремы вытекает непосредственно.

Теорема 3. *Число $v_2-\rho$, соответствующее точке (u_2, v_2), полученной удвоением другой точки (u_1, v_1), принадлежит главному классу (т. е. является полным квадратом числа рассматриваемой кубической области).*

Доказательство. Уравненне

$$v^3-h_2v-h_3=\left[u_1+\frac{3v_1^2-h_2}{2u_1}(v-v_1)\right]^2,$$

получающееся в результате исключения u из уравнений кривой и касательной в точке (u_1, v_1); имеет двойной корень v_1 и простой v_2.

Положив $v-\rho=\lambda$; $v_1-\rho=\lambda_1$, получим уравнение относительно λ, имеющее двойной корень λ_1 и простой $v_2-\rho$.

$$\lambda^3+H_1\lambda^2+H_2\lambda=\left[u_1+\frac{3v_1^2-h_2}{2u_1}(\lambda-\lambda_1)\right]^2.$$

Отсюда следует, что

$$(v_2-\rho)\lambda_1^2=\left[u_1-\frac{3v_1^2-h_2}{2u_1}\lambda_1\right]^2$$

и, наконец,

$$v_2-\rho=\left[\frac{u_1}{\lambda_1}-\frac{3v_1^2-h_2}{2u_1}\right]^2,$$

откуда справедливость теоремы вытекает непосредственно.

Теорема 4 *(обратная теореме 3). Если число $v_2-\rho$, соответствующее рациональной точке (u_2, v_2), принадлежит главному классу чисел с квадратной нормой, то точка (u_2, v_2) может быть получена удвоением некоторой другой рациональной точки (u_1, v_1).*

Доказательство. Пусть $v_2-\rho=(A+B\rho+C\rho^2)^2$, где A, B и C — рациональные числа. Приравнивая коэффициенты при 1, ρ и ρ^2 в обеих частях равенства (что надо сделать не только в случае неприводимой области, но и в случае приводимой), получим

$$\begin{aligned}A^2+2BCh_3&=v_2,\\2AB+2BCh_2+C^2h_3&=-1,\\B^2+2AC+C^2h_2&=0.\end{aligned}$$

Исключая A из второго и третьего равенств, получим

$$B^3 - h_2BC^2 - h_3C^3 = C,$$

или, поделив на C^3,

$$\left(\frac{1}{C}\right)^2 = \left(\frac{B}{C}\right)^3 - h_2\left(\frac{B}{C}\right) - h_3.$$

Мы видим, что $\left(\frac{1}{C}, \frac{B}{C}\right)$ представляет собой рациональную точку на кривой

$$u^2 = v^3 - h_2v - h_3.$$

Обозначив $\frac{1}{C} = u_1$, $\frac{B}{C} = v_1$, получим после простых вычислений, что

$$v_2 - \rho = \left[\frac{u_1}{v_1 - \rho} - \frac{3v_1^2 - h_2}{2u_1}\right]^2,$$

откуда следует справедливость теоремы.

Теорема 5. *В результате „сложения" двух точек, для которых соответствующие числа $v - \rho$ принадлежат к одному классу, получается точка, которую можно получить удвоением некоторой другой точки.* Теорема непосредственно следует из теорем 2 и 4.

Теорема 6. *Все рациональные точки на кривой $u^2 = v^3 - h_2v - h_3$ могут быть получены действием сложения над конечным числом некоторых основных рациональных точек.*

Доказательство. Рассмотрим все рациональные точки на кривой $u^2 = v^3 - h_2v - h_3$ и распределим их по классам, объединяя в один класс те точки, для которых числа $v - \rho$ принадлежат к одному классу. Таких классов, как мы уже знаем, будет конечное число. Из каждого класса выберем по одному представителю. Пусть (u_1, v_1), (u_2, v_2), ..., (u_k, v_k) совокупность таких представителей. Над каждой другой рациональной точкой (u, v) мы имеем возможность сделать следующую операцию, которую будем называть спуском. Найдем среди представителей всех классов точку (u_i, v_i), принадлежащую тому же классу, что и (u, v). Затем сложим точку (u_i, v_i) с точкой (u, v). Получим новую точку, которая, в силу теоремы 5, будет удвоением некоторой точки (u', v').

Над точкой (u', v') можно в свою очередь произвести операцию спуска и перейти к новой точке (u'', v'') и т. д. Нам удастся показать, что от любой рациональной точки можно „спуститься" в конечном числе шагов к одной из точек заведомо конечного множества точек. Обозначив через $t_1, t_2, \ldots, t_k$ аргументы представителей всех классов, через $t'_1, t'_2, \ldots, t'_s$ аргументы конечного множества точек, к которым приводит спуск, и, наконец, через t аргумент исходной точки, мы будем иметь

$$t = -t_{i_1} + 2[-t_{i_2} + \ldots + 2[-t_{i_m} + 2t'_j]\ldots],$$

откуда следует, что t представляется в виде линейной формы с целыми рациональными коэффициентами через аргументы $t_1, t_2, \ldots, t_k, t'_1, t'_2, \ldots, t'_s$ конечного множества точек, что нам и требуется доказать.

Итак, нам нужно доказать только то, что операция спуска, будучи произведена достаточное число раз, приводит в конце концов к точке, принадлежащей некоторому конечному множеству точек.

Для этого произведем некоторые оценки.

Перейдем от рассмотрения рациональных чисел u, v к рассмотрению целых чисел x, y, z, положив, как при доказательстве теоремы 1, $v = \frac{x}{z^2}$ при вза-

имно простых x, z. Тогда $u=\frac{y}{z^3}$, причем y, x, z будут удовлетворять уравнению

$$y^2=x^3-h_2xz^4-h_3z^6.$$

Назовем *высотой* рациональной точки бо́льшее из чисел x, z^2. Очевидно, что может быть лишь конечное число точек, имеющих высоту, меньшую данного числа.

Докажем прежде всего, что если L — высота точки (u_2, v_2) главного класса, то высота точки (u_1, v_1), удвоением которой получается (u_2, v_2), будет меньше $cL^{\frac{1}{3}}$, где c — постоянная, зависящая только от h_2 и h_3.

Действительно, формула удвоения аргумента дает

$$v_2-\rho=\left[\frac{u_1}{v_1-\rho}-\frac{3v_1^2-h_2}{2u_1}\right]^2.$$

Положив

$$v_2=\frac{x_2}{z_2^2};\qquad u_1=\frac{y_1}{z_1^3};\qquad v_1=\frac{x_1}{z_1^2};$$

$$x_1-z_1^2\rho=\lambda_1;\qquad x_1-z_1^2\rho'=\lambda_1';\qquad x_1-z_1^2\rho''=\lambda_1'',$$

мы получим после несложных вычислений

$$\frac{x_2}{z_2^2}-\rho=\frac{(\lambda_1\lambda_1'+\lambda_1\lambda_1''-\lambda_1'\lambda_1'')^2}{4y_1^2z_1^2},$$

$$\frac{x_2}{z_2^2}-\rho'=\frac{(\lambda_1'\lambda_1''+\lambda_1'\lambda_1-\lambda_1''\lambda_1)^2}{4y_1^2z_1^2},$$

$$\frac{x_2}{z_2^2}-\rho''=\frac{(\lambda_1''\lambda_1+\lambda_1''\lambda_1'-\lambda\lambda_1')^2}{4y_1^2z_1^2},$$

откуда следует, что

$$z_2=\frac{1}{k}\cdot 2y_1z_1,$$

где k — натуральное число, входящее делителем в числа $\lambda_1\lambda_1'+\lambda_1\lambda_1''-\lambda_1'\lambda_1''$; $\lambda_1'\lambda_1''+\lambda_1'\lambda_1-\lambda_1''\lambda_1$; $\lambda_1''\lambda_1+\lambda_1''\lambda_1'-\lambda\lambda_1'$. Очевидно, что $(k, z_1)=1$, так как

$$\lambda_1\lambda_1'+\lambda_1\lambda_1''-\lambda_1'\lambda_1''\equiv x_1^2 \pmod{z_1},$$

а x_1 и z_1 взаимно просты. Далее k, очевидно, входит делителем в $2\lambda_1\lambda_1'$; $2\lambda_1'\lambda_1''$; $2\lambda_1''\lambda_1'$ и, следовательно, в

$$2\lambda_1\lambda_1'(\lambda_1-\lambda_1')+2\lambda_1'\lambda_1''(\lambda_1'-\lambda_1'')+2\lambda_1''\lambda_1(\lambda_1''-\lambda_1)=$$
$$=-2(\lambda_1-\lambda_1')(\lambda_1'-\lambda_1'')(\lambda_1''-\lambda_1)=-2z_1^6\sqrt{\Delta},$$

где Δ — дискриминант числа ρ. В виду того, что $(k, z_1)=1$, k входит делителем в $2\sqrt{\Delta}$. Следовательно, k ограничено сверху постоянной, зависящей только от h_2 и h_3.

Итак,

$$z_2^2=\frac{4}{k^2}y_1^2z_1^2=\frac{4}{k^2}z_1^2\lambda_1\lambda_1'\lambda_1'',$$

$$\left.\begin{aligned}\lambda_2 &= x_2 - z_2^2\rho = \frac{1}{k^2}(\lambda_1\lambda_1' + \lambda_1\lambda_1'' - \lambda_1'\lambda_1'')^2,\\ \lambda_2' &= x_2 - z_2^2\rho' = \frac{1}{k^2}(\lambda_1'\lambda_1'' + \lambda_1'\lambda_1 - \lambda_1''\lambda_1)^2,\\ \lambda_2'' &= x_2 - z_2^2\rho'' = \frac{1}{k^2}(\lambda_1''\lambda_1 + \lambda_1''\lambda_1' - \lambda_1\lambda_1')^2.\end{aligned}\right\} \quad (*)$$

Допустим сначала, что z_1 — маленькое число, именно что $z_1^2 < L^{\frac{1}{6}}$.

Допустив теперь, что $|x_1| > cL^{\frac{1}{3}}$, мы сейчас же получим противоречие, если только взять c достаточно большим. Действительно, если $|x_1| > c_1L^{\frac{1}{3}}$, то

$$|x_1 - z_1^2\rho_1| > c_2L^{\frac{1}{3}};\quad |x_1 - z_1^2\rho_1'| > c_2L^{\frac{1}{3}};\quad |x_1 - z_1^2\rho_1'| > c_2L^{\frac{1}{3}}$$

и, следовательно,

$$z_2^2 = \frac{4}{k^3}z_1^2(x_1 - z_1^2\rho_1)(x_1 - z_1^2\rho_1')(x_1 - z_1^2\rho_1'') > \frac{4}{k^3}c_2^3L,$$

что невозможно при достаточно большом c_2.

Допустим теперь, что $z_1^2 > L^{\frac{1}{6}}$. В этом случае произведем оценку другим способом.

Из соотношений (*) следует, что

$$\lambda_1'\lambda_1'' = \frac{k}{2}\left(\sqrt{x_2 - z_2^2\rho'} + \sqrt{x_2 - z_2^2\rho''}\right),$$

откуда следует, что

$$\lambda_1 = \frac{k^2}{4}\cdot\frac{z_2^2}{z_1^2}\cdot\frac{1}{\lambda_1'\lambda_1''} = \frac{k}{2}\cdot\frac{z_2^2}{z_1^2\left(\sqrt{x_2 - z_2^2\rho'} + \sqrt{x_2 - z_2^2\rho''}\right)} =$$

$$= \frac{k}{2}\cdot\frac{\sqrt{x_2 - z_2^2\rho'} - \sqrt{x_2 - z_2^2\rho''}}{z_1^2(\rho'' - \rho')}$$

и, следовательно,

$$|\lambda_1| < c\frac{L^{\frac{1}{2}}}{z_1^2} < cL^{\frac{1}{3}},$$

где c — постоянная, зависящая только от h_2 и h_3. Таким же образом получим, что $|\lambda_1'| < cL^{\frac{1}{3}}$, откуда непосредственно вытекает справедливость таких же оценок для x_1 и z_1^2.

Выясним теперь, насколько увеличивается высота точки при сложении ее с другой.

Пусть высота точки (u_1, v_1) есть M. Высота точки (u_2, v_2) есть L.

По формуле сложения после несложных преобразований получим

$$\frac{x}{z^2} - \rho = \frac{[y_2z_1(x_1 - z_1^2\rho) - y_1z_2(x_2 - z_2^2\rho)]^2}{(x_2z_1^2 - x_1z_2^2)^2(x_1 - z_1^2\rho)(x_2 - z_2^2\rho)},$$

откуда следует, что

$$z \leqslant x_2z_1^2 - x_1z_2^2,$$

так как числитель, очевидно, делится на $(x_1 - z_1^2\rho)(x_2 - z_2^2\rho)$. Отсюда следует, что высота точки (u, v), получающейся сложением точек (u_1, v_1) и (u_2, v_2), не превосходит cM^2L^2, где c — постоянная.

Приложим эти результаты к оценке высоты результата при спуске.

Пусть M_0 наибольшая высота выбранных представителей всех классов точек. Пусть L высота исходной точки. Складывая исходную точку с одной из точек представителей, получим точку с высотой, не превышающей $cM_0^2L^2$. Эта точка будет удвоенной для точки (u', v'), высота которой будет меньше $c'M_0^{\frac{2}{3}}L^{\frac{2}{3}}$. Эта высота будет, вообще говоря, мевьше высоты L исходной точки. Однако в конечном числе шагов уменьшение высоты точки при спуске должно прекратиться, ибо иначе существовало бы бесконечно много точек с высотой, меньшей L. Высота точки при спуске не будет уменьшаться только, если $c'M_0^{\frac{2}{3}}L^{\frac{2}{3}} \geqslant L$, что может быть только при $L \leqslant c'^3M_0^2$.

Итак, от любой точки можно в конечном числе действий спуститься к точке, высота которой $\leqslant c'^3M_0^2$. Таких же точек может быть лишь конечное число. Тем самым теорема доказана.

§ 82. Об уравнении $x^3+y^3=Az^3$

Уравнение, указанное в заглавии этого параграфа, является частным случаем уравнений, рассмотренных в предыдущих параграфах. Однако для него очень удобно провести самостоятельное исследование, основанное на той же идее спуска, но посредством деления аргумента на 3, а не на 2, как в предыдущем параграфе. При этом нам удастся получить довольно точные оценки числа основных решений уравнения.

Переходим к изложению.

1°. Рассмотрим кривую

$$x^3+y^3=A \tag{1}$$

и ее параметрическое представление

$$x=x(t)=\frac{9A+\wp'(t)}{6\wp(t)},$$

$$y=y(t)=\frac{9A-\wp'(t)}{6\wp(t)}.$$

Известно, что функция $\wp(t)$, а следовательно, также $x(t)$ и $y(t)$ имеют действительный период ω и комплексный $\omega'=\omega\cdot e^{\frac{2\pi i}{3}}$.

Точка (x, y) пробегает кривую (1), когда t проходит вещественные значения от 0 до ω. Значению $t=0$ соответствует бесконечно далекая точка кривой, $t=\frac{1}{2}\omega$ соответствует точка $P\left(\sqrt[3]{\frac{A}{2}}, \sqrt[3]{\frac{A}{2}}\right)$, $t=\frac{1}{3}\omega$ и $t=\frac{2}{3}\omega$ соответствуют точки перегиба кривой $Q_1\left(\sqrt[3]{A}, 0\right)$ и $Q_2\left(0, \sqrt[3]{A}\right)$. Точка P рациональна только для $A=2k^3$, точки Q — только для $A=k^3$. При всех остальных значениях A значения аргумента, дающие рациональные точки, несоизмеримы с периодом.

Простейшим алгебраическим действиям над аргументом t соответствуют простые геометрические операции над точками кривой. Именно:

1) Если аргументу t соответствует точка $M(x, y)$, то аргументу $-t$ соответствует точка $M(y, x)$.

2) Если t_1 соответствует точке $M_1(x_1, y_1)$, t_2 соответствует точке $M_2(x_2, y_2)$, то $-t_1-t_2$ соответствует точке M_3 пересечения секущей M_1M_2 с кривой.

3) Если t соответствует M, то $-2t$ соответствует точка пересечения N кривой с касательной в точке M.

Исходя из этого, легко дать формулы для вычисления новых решений уравнения $x^3+y^3=A$ по уже известным.

I. Если аргументу t соответствует решение (x, y, z), то $-t$ соответствует решению (y, x, z).

II. Если t_1 соответствует (x_1, y_1, z_1) и t_2 соответствует (x_2, y_2, z_2), то $-t_1-t_2$ соответствует X, Y, Z, где

$$\left.\begin{aligned} X &= Az_1z_2(x_2z_1-x_1z_2)+y_1y_2(x_1y_2-x_2y_1),\\ Y &= Az_1z_2(y_2z_1-y_1z_2)+x_1x_2(y_1x_2-y_2x_1),\\ Z &= x_1x_2(x_2z_1-x_1z_2)+y_1y_2(y_2z_1-y_1z_2). \end{aligned}\right\} \tag{2}$$

(„формулы сложения").

Если $t_1=t_2$, то формулы сложения теряют смысл; для этого случая вводим „формулы удвоения".

III. Если t_1 соответствует (x_1, y_1, z_1), то $-2t_1$ соответствует X_2, Y_2, Z_2, где

$$\left.\begin{aligned} X_2 &= -x_1(x_1^3+2y_1^3),\\ Y_2 &= y_1(2x_1^3+y_1^3),\\ Z_2 &= z_1(y_1^3-x_1^3). \end{aligned}\right\} \tag{3}$$

Кроме того, для дальнейшего нам нужны „формулы утроения".

IV. Если t_1 соответствует (x_1, y_1, z_1), то $3t_1$ соответствует X_3, Y_3, Z_3, где

$$\left.\begin{aligned} X_3 &= x_1^9+6x_1^6y_1^3+3x_1^3y_1^6-y_1^9,\\ Y_3 &= y_1^9+6y_1^6x_1^3+3y_1^3x_1^6-x_1^9,\\ Z_3 &= 3x_1y_1z_1(x_1^6+x_1^3y_1^3+y_1^6). \end{aligned}\right\} \tag{4}$$

Не трудно проверить справедливость следующих соотношений:

$$3(x_1+y_1)(x_1-z_1\rho)(y_1-z_1\rho)=(x_1+y_1-z_1\rho)^3, \tag{1'}$$

$$3(x_1-z_1\rho)(x_2-z_2\rho)(X-Z\rho)=[y_1(x_2-z_2\rho)-y_2(x_1-z_1\rho)]^3, \tag{2'}$$

$$3(x_1+y_1)(x_2+y_2)(X+Z)=A[z_2(x_1+y_1)-z_1(x_2+y_2)]^3, \tag{2''}$$

$$3(x_1\zeta+y_1\zeta^2)(x_2\zeta+y_2\zeta^2)(X\zeta+Y\zeta^2)=A[z_2(x_1\zeta+y_1\zeta^2)-z_1(x_2\zeta+y_2\zeta^2)]^3, \tag{2'''}$$

$$X_2-Z_2\rho=(x_1-z_1\rho)(x_1+z_1\rho)^3, \tag{3'}$$

$$X_2+Y_2=(x_1+y_1)(y_1-x_1)^3, \tag{3''}$$

$$X_2\zeta+Y_2\zeta^2=(x_1\zeta+y_1\zeta^2)(y_1\zeta^2-x_1\zeta)^3, \tag{3'''}$$

$$X_3-Z_3\rho=(-y^2x+x^2z\rho-yz^2\rho^2)^3, \tag{4'}$$

$$X_3+Y_3=9Ax_1^3y_1^3z_1^3, \tag{4''}$$

$$X_3\zeta+Y_3\zeta^2=\zeta(1-\zeta)(x_1^3-y_1^3\zeta^2)^3. \tag{4'''}$$

В формулах $(1')-(4''')$ $\rho=\sqrt[3]{A}$, $\zeta=e^{\frac{2\pi i}{3}}$; остальные обозначения те же, что в формулах (2), (3), (4).

2^0. В дальнейшем мы будем пользоваться следующими результатами из теории поля $\Omega(\sqrt[3]{A})$.

Если A свободно от кубических множителей и $A=fg^2$, где f — произведение простых множителей, входящих в A в первой степени, g — произведение простых множителей A, входящих в квадрате, то базисом целых чисел

поля $\Omega(\sqrt[3]{A})$ является или $[1, \rho, \bar{\rho}]$, если

$$A \not\equiv \pm 1 \pmod 9, \quad \text{или} \quad \left[1, \rho, \frac{1 \pm \rho \pm \bar{\rho}}{3}\right],$$

если $A \equiv \pm 1 \pmod 9$, через ρ мы обозначаем $\sqrt[3]{A}$; $\bar{\rho} = \sqrt[3]{\bar{A}}$, где $\bar{A} = f^2 \cdot g$.

В первом случае $\Omega(\sqrt[3]{A})$ называется полем первого рода, во втором — полем второго рода. В полях первого рода $3 = \pi_3^3$, в полях второго рода $3 = \pi_3^2\pi_1$, где π_3, π_1 — простые идеалы из $\Omega(\rho)$.

В дальнейшем будем считать, что A свободно от кубических множителей.

Уравнение $x^3+y^3=Az^3$ можно записать в виде

$$N(x - z\rho) = -y^3.$$

Отсюда следует, что если двучленное число $x - z\rho$ является кубом какого-нибудь числа λ из $\Omega(\rho)$, то $(x, y = -N(\lambda), z)$ дают решение уравнения

$$x^3+y^3=Az^3.$$

Докажем следующую теорему:

Теорема 1. *Если* $X - Z\rho = \lambda^3$, *где* λ *число поля* $\Omega(\rho)$ *и* X *взаимно просто с* A, *то решение* $(X, Y = -N(\lambda), Z)$ *может быть получено утроением аргумента некоторого другого решения* (x_1, y_1, z_1).

Доказательство. Без нарушения общности можно считать, что

$$\lambda = a + b\rho + c\bar{\rho},$$

где a, b, c — целые числа, не имеющие общего делителя.

Тогда

$$\begin{aligned} X - Z\rho &= (a + b\rho + c\bar{\rho})^3 = \\ &= a^3 + Ab^3 + \bar{A}c^3 + 6fgabc + 3\rho(a^2b + fgb^2c + fc^2a) + \\ &+ 3\bar{\rho}(gab^2 + fgbc^2 + ca^2), \qquad (5) \\ Y &= -N(a + b\rho + c\bar{\rho}) = -a^3 - Ab^3 - \bar{A}c^3 + 3fgabc. \end{aligned}$$

Откуда

$$X = a^3 + Ab^3 + \bar{A}c^3 + 6fgabc, \qquad (5')$$

$$Y = -a^3 - \bar{A}b^3 - Ac^3 + 3fgabc, \qquad (5'')$$

$$Z = 3(a^2b + fgb^2c + fc^2a), \qquad (5''')$$

$$gab^2 + fgbc^2 + ca^2 = 0. \qquad (6)$$

Из (5′) заключаем, что $(a, A) = 1$, из (6) — что ca^2 делится на g.

Следовательно, c делится на g, так что $c = gc_1$.

Подставляя в (6) и сокращая на g, получим

$$ab^2 + Abc_1^2 + c_1a^2 = 0. \qquad (6')$$

Обозначим $(b, c_1) = d$, $b = db_1$, $c_1 = dc_2$.

Тогда $(a, d) = 1$, $(b_1, c_2) = 1$.

Подставив в (6′), получим

$$ab_1^2d + b_1c_2^2d^2A + c_2a^2 = 0, \qquad (6'')$$

откуда следует, что $c_2 = dc_3$. Подставив в (6″), имеем

$$ab_1^2 + b_1c_3^2d^3A + a^2c_3 = 0. \qquad (6''')$$

Из (6''') следует, что $a = c_3^2 a_1$ и

$$a_1 b_1^2 + b_1 A d^3 + a_1^2 c_3^3 = 0, \qquad (6'''')$$

и, наконец, $b_1 = a_1^2 b_2$, откуда

$$a_1^3 b_2^2 + A b_2 d^3 + c_3^3 = 0. \qquad (7)$$

Из (7) видим, что c_3^3 делится на b_2. С другой стороны $(c_3, b_2) = 1$.

Следовательно, $b_2 = e = \pm 1$.

Равенство (7) перепишем в виде

$$a_1^3 + c_3^3 = A(-ed)^3, \qquad (7')$$

откуда следует, что $(a_1, c_3, -ed)$ есть решение уравнения $x^3 + y^3 = Az^3$. Обозначив $a_1 = x_1$; $c_3 = y_1$; $-ed = z_1$, получим

$$a = x_1 y_1^2; \quad b = -x_1^2 z_1; \quad c = g z_1^2 y_1$$

и из (5'), (5''), (5''') получим

$$\left.\begin{aligned} X &= -(x_1^9 + 6x_1^6 y_1^3 + 3x_1^3 y_1^6 - z_1^9), \\ Y &= -(y_1^9 + 6y_1^6 x_1^3 + 3y_1^3 x_1^6 - x_1^9), \\ Z &= -3x_1 y_1 z_1 (x_1^6 + x_1^3 y_1^3 + y_1^6). \end{aligned}\right\} \qquad (8)$$

Сопоставляя (8) с (6), непосредственно устанавливаем справедливость теоремы 1.*

Теорема 2. *Для того чтобы аргумент решения (X, Y, Z) был утроенным аргументом некоторого решения (x_1, y_1, z_1), необходимо и достаточно, чтобы $9(X+Y)^2(X - Z\rho)$ было кубом числа из $\Omega(\rho)$.*

Доказательство. Необходимость высказанного условия непосредственно следует из соотношений (4') и (4'').

Для доказательства достаточности покажем, что найдутся X_1, Y_1, Z_1, пропорциональные X, Y, Z, такие, что $X_1 - Z_1\rho = \lambda^3$ и X_1 взаимно просто с A.

Итак, пусть

$$9(X+Y)^2(X - Z\rho) = \lambda^3. \qquad (9)$$

Без нарушения общности можно считать X и Y взаимно простыми.

Так как $X^3 + Y^3 = AZ^3$ и A не содержит кубических множителей, то если только $(X, Y) = 1$, также и $(X, AZ) = 1$ и $(Y, AZ) = 1$.

Имеем

$$\begin{aligned} 9(X+Y)^2(X - Z\rho) &= (a + b\rho + c\bar{\rho})^3 = \\ &= a^3 + Ab^3 + \bar{A}c^3 + 6fgabc + 3\rho(a^2 b + fgb^2 c + fc^2 a) + \\ &+ 3\bar{\rho}(a^2 c + gb^2 a + fgc^2 b) \end{aligned}$$

и

$$N[9(X+Y)^2(X - Z\rho)] = -9^3 (X+Y)^6 \cdot Y^3 = [a^3 + Ab^3 + \bar{A}c^3 - 3fgabc]^3.$$

Откуда

$$\begin{aligned} 9X(X+Y)^2 &= a^3 + Ab^3 + \bar{A}c^3 + 6fgabc, \\ 9Y(X+Y)^2 &= -a^3 - Ab^3 - \bar{A}c^3 + 3fgabc. \end{aligned}$$

Складывая, получим

$$(X+Y)^3 = fgabc.$$

Отсюда следует, что $X+Y$ делится на fg. С другой стороны, уравнение $X^3 + Y^3 = AZ^3$ можно переписать в виде

$$(X+Y)[(X+Y)^2 - 3XY] = fg^2 Z^3. \qquad (10)$$

---

* Теорема 1 была доказана Б. Делоне в работах, посвященных уравнению $ax^3 + y^3 = 1$ еще в 1916 г.

Пусть A не делится на 3. Так как в этом случае $3XY$ взаимно просто с A, а $(X+Y)^2$ делится на всех простых делителей A, то выражение $(X+Y)^2-3XY$ с A взаимно просто. Следовательно, $X+Y$ делится на A.

Очевидно, что $X+Y$ и $(X+Y)^2-3XY$ или взаимно просты, или имеют общего делителя 3. Следовательно, или $X+Y=Av^3$, или $X+Y=9Av^3$.

В первом случае, из (9), $9(X-Z\rho)=\lambda_1^3$ и решение $(9X, 9Y, 9Z)$ удовлетворяет условиям теоремы 1.

Во втором случае $X-\rho Y=\lambda_1^3$, и, следовательно, само решение (X, Y, Z) удовлетворяет условиям теоремы 1.

Пусть A делится на 3, $A=3^\sigma f_1 g_1^2$, где $\sigma=1$ или 2. В этом случае $X+Y=3^{\sigma-1}f_1g_1^2v^3$ [из (10)], и, следовательно, из (9) $X-Z\rho=\lambda_1^3$, т. е. снова для решения (X, Y, Z) выполнены условия теоремы 1.

Замечание. Не трудно видеть, что если A не делится на 3, то равенства

$$(X+Y)^2(X-Z\rho)=\lambda^3 \quad \text{и} \quad 3(X+Y)^2(X-Z\rho)=\lambda^3$$

невозможны.

Теорема 3. *Для того чтобы аргументы решений* (x_1, y_1, z_1) *и* (x_2, y_2, z_2) *отличались на утроенный аргумент некоторого третьего решения* (x_3, y_3, z_3), *необходимо и достаточно, чтобы*

$$\frac{(x_1+y_1)^2(x_1-z_1\rho)}{(x_2+y_2)^2(x_2-z_2\rho)}=\lambda^3, \tag{11}$$

где λ — *целое или дробное число поля* $\Omega(\rho)$.

Доказательство. Докажем достаточность условия. Для этого составим решение (X, Y, Z), аргумент которого равен разности аргументов решений

$$(x_1, y_1, z_1) \quad \text{и} \quad (x_2, y_2, z_2).$$

Решение X, Y, Z получим по формулам сложения из (y_1, x_1, z_1) и (x_2, y_2, z_2). Следовательно, из соотношений (2′) и (2″)

$$3(y_1-z_1\rho)(x_2-z_2\rho)(X-Z\rho)=\alpha^3, \qquad 3(x_1+y_1)(x_2+y_2)(X+Y)=\beta^3,$$

откуда

$$27(x_1+y_1)^2(y_1-z_1\rho)(x_2+y_2)^2(x_2-z_2\rho)(X+Y)^2(X-Z\rho)=(\alpha\beta)^3. \tag{12}$$

Из (1′)

$$3(x_1+y_1)^4(x_1-z_1\rho)(y_1-z_1\rho)=\nu^3. \tag{13}$$

Поделив (12) на (13), получим

$$9(X+Y)^2(X-Z\rho)\cdot\frac{(x_2+y_2)^2(x_2-z_2\rho)}{(x_1+y_1)^2(x_1-z_1\rho)}=\left(\frac{\alpha\beta}{\nu}\right)^3,$$

откуда, принимая во внимание условие (11),

$$9(X+Y)^2(X-Z\rho)=\left(\frac{\alpha\beta\lambda}{\nu}\right)^3=\mu^3.$$

Тем самым, на основании теоремы 2, достаточность условия (11) доказана.

Для доказательства необходимости нужно те же самые преобразования произвести в обратном порядке.

Замечание. Не трудно, принимая во внимание замечание к теореме 2, установить, что в случае, если A не делится на 3, равенства

$$\frac{(x_1+y_1)^2(x_1-z_1\rho)}{(x_2+y_2)^2(x_2-z_2\rho)}=3^\sigma\lambda^3,$$

где $\sigma=1$ или 2, невозможны.

3°. Представим уравнение $X^3+Y^3=AZ^3$ в виде

$$3(X+Y)(X-Z\rho)(Y-Z\rho)=(X+Y-Z\rho)^3. \qquad (1')$$

Если X, Y, Z взаимно просты, то $X+Y$; $X-Z\rho$; $Y-Z\rho$ также взаимно просты (попарно).

В случае если $\Omega(\rho)$ 1-го рода, на основании (1') и того, что 3 является кубом идеала, заключаем, что $X+Y$; $X-Z\rho$; $Y-Z\rho$ являются кубами идеалов и, следовательно, $9(X+Y)^2(X-Z\rho)$ также является кубом идеала.

Таким же образом, в случае если $\Omega(\rho)$ — область 2-го рода, то

$$9(X+Y)^2(X-Z\rho)=j^3 \text{ или } 3j^3, \text{ или } 9j^3,$$

где j — идеал поля $\Omega(\rho)$.

Из соображений теории групп следует, что число классов идеалов, кубы которых дают главный класс, $s=3^k$.

Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s$ — представители всех таких классов. Обозначим числа, соответствующие их кубам, $\mu_1, \mu_2, \ldots, \mu_s$. Тогда всякое число, являющееся кубом идеала, будет отличаться лишь кубом целого или дробиого числа поля $\Omega(\rho)$ от одного из $3s$ чисел ряда

$$\mu_1, \mu_1\varepsilon, \mu_1\varepsilon^2; \mu_2, \mu_2\varepsilon, \mu_2\varepsilon^2, \ldots, \mu_s, \mu_s\varepsilon, \mu_s\varepsilon^2, \qquad (A)$$

где через ε обозначена основная единица поля $\Omega(\rho)$. Следовательно, числа $9(X+Y)^3(X-Z\rho)$ будут лишь на кубы чисел из $\Omega(\rho)$ отличаться от чисел ряда (A), в случае если $\Omega(\rho)$ — 1-го рода, или от чисел ряда (B):

$$\mu_1, \mu_1\varepsilon, \mu_1\varepsilon^2; 3\mu_1, 3\mu_1\varepsilon, 3\mu_1\varepsilon^2; 9\mu_1, 9\mu_1\varepsilon, 9\mu_1\varepsilon^2; \ldots, \qquad (B)$$

в случае если $\Omega(\rho)$ — поле 2-го рода.

Будем называть решения уравнения $X^3+Y^3=AZ^3$ эквивалентными, если соответствующие им числа $9(X+Y)^2(X-Z\rho)$ отличаются на куб числа из $\Omega(\rho)$. Эквивалентные решения объединяем в классы. Соотиошения (2'), (2''), (3') и (3'') показывают, что классы решений образуют группу, которая, очевидно, является подгруппой групп (A) или (B). Следовательно, число классов решений равно 3^m, где

$$m\leqslant k+1 \text{ в случае } \Omega(\rho) \text{ 1-го рода}$$
$$m\leqslant k+2 \quad \text{„} \quad \Omega(\rho) \text{ 2-го рода}$$

Не трудно показать, используя замечание к теореме 3, что

$$m\leqslant k \quad \text{в случае } \Omega(\rho) \text{ 1-го рода, } (A, 3)=1.$$
$$m\leqslant k+1 \quad \text{„} \quad \Omega(\rho) \text{ 2-го рода}$$

Мы знаем, что система значений аргумента t, дающих решения уравиеиия $x^3+y^3=Az^3$, имеет конечный базис.

Мы знаем, что если исключить из рассмотрения $A=1$, $A=2$, то интересующие нас значения аргумента t несоизмеримы с периодом ω. В таком случае, как легко видеть, можно установить существование такого базиса $t_1, t_2, \ldots, t_p$, для которого соотношение $r_1t_1+r_2t_2+\ldots+r_pt_p=n\omega$ невозможно ни при каких целых значениях $r_1, r_2, \ldots, r_p, n$.

Докажем, что $p=m$, где 3^m — число классов решений уравнения $x^3+y^3=Az^3$.

В самом деле, решения, соответствующие 3^p зиачениям аргумента

$$t=a_1t_1+a_2t_2+\ldots+a_pt_p \qquad (a_i=0, 1, 2)$$

не могут быть эквивалентны, ибо в противном случае, в силу теоремы 3, разность двух таких аргументов была бы, с точностью до периода, утроенным аргументом некоторого третьего решения

$$(\alpha_1'-\alpha_1'')t_1+(\alpha_2'-\alpha_2'')t_2+\ldots+(\alpha_p'-\alpha_p'')t_p=3\beta_1t_1+3\beta_2t_2+\ldots+3\beta_pt_p+n\omega,$$

что, очевидно, невозможно.

Обратно, аргумент любого решения $t=\gamma_1t_1+\gamma_2t_2+\ldots+\gamma_pt_p$ может быть представлен в виде $t=\alpha_1t_1+\alpha_2t_2+\ldots+\alpha_pt_p+3(\beta_1t_1+\beta_2t_2+\ldots+\beta_pt_p)$, где $\alpha_i=0,\ 1,\ 2$, откуда следует, в силу теоремы 3, что любое решение эквивалентно одному из 3^p решений, соответствующих значениям аргумента $\alpha_1t_1+\alpha_2t_2+\ldots+\alpha_pt_p$. Итак, $3^p=3^m$, и, следовательно, $p=m$.

Хотя нам уже известно, что основных решений существует конечное число, представляет некоторый интерес вопрос о том, насколько быстро уменьшается величина решений при спуске, основанном на делении аргумента на три.

Пусть

$$(x_1, y_1, z_1),\ (x_2, y_2, z_2),\ \ldots,\ (x_s, y_s, z_s) \qquad (C)$$

— представители всех возможных классов решений уравнения $x^3+y^3=Az^3$, и пусть $t_1, t_2, \ldots, t_s$ — соответствующие им значения аргумента. Обозначим L — верхнюю границу чисел $|x_i|, |y_i|, |z_i|$ $(i=1, 2, \ldots, s)$. Пусть (X, Y, Z) какое-нибудь решение уравнения, отличное от решений (C). Соответствующее ему значение аргумента обозначим T. Среди решений (C) найдется решение (x_i, y_i, z_i), эквивалентное взятому решению (X, Y, Z). Тогда решение (X_3, Y_3, Z_3), соответствующее аргументу $T-t_i$, будет утроенным для некоторого решения (x, y, z).

X_3, Y_3, Z_3 определим по формулам:

$$\begin{aligned}X_3&=AZz_i(x_iZ-z_iY)+Xy_i(Yy_i-Xx_i),\\ Y_3&=AZz_i(y_iZ-z_iY)+Yx_i(Xx_i-Yy_i),\\ Z_3&=x_iY\ (x_iZ-z_iY)+y_iX(y_iZ-z_iX).\end{aligned}$$

Откуда

$$|Z_3|<2L^2\cdot[|X|+|Y|]^2. \qquad (14)$$

Не нарушая справедливости неравенства (14), можно считать X_3, Y_3, Z_3 взаимно простыми, ибо сокращение их на общего делителя может только уменьшить их абсолютную величину.

Но решение (X_3, Y_3, Z_3) есть утроенное для некоторого решения (x, y, z). Следовательно, или X_3, Y_3, Z_3, или $9X_3$, $9Y_3$, $9Z_3$ получаются из (x, y, z) по формулам утроения (4)

$$\begin{aligned}3^3X_3&=x^9+6x^6y^3+3x^3y^6-y^9,\\ 3^3Y_3&=y^9+6y^6x^3+3y^3x^6-x^9,\\ 3^3Z_3&=3xyz(x^6+x^3y^3+y^6),\end{aligned}$$

откуда

$$|xyz|\cdot(x^6+x^3y^3+y^6)<3Z_3.$$

Далее, $x^6+x^3y^3+y^6\geqslant\frac{3}{4}x^6$, и так как $x^3=Az^3-y^3$, то имеем

$$|Az^3|+|y|^3\geqslant|x|^3,$$

откуда

$$(A+1)|yz|^3>|x^3|\ \text{ и }\ |yz|>\frac{|x|}{\sqrt[3]{A+1}}>\frac{|x|}{2\sqrt[3]{A}}.$$

Следовательно,

$$\frac{3}{8\sqrt[3]{A}}|x|^3<3|Z_3|;\ |x|^3<8A^{\frac{1}{3}}|Z_3|<16A^{\frac{1}{3}}L^2[|X|+|Y|]^2,$$

откуда

$$|x|<2^{\frac{1}{2}}A^{\frac{1}{24}}L^{\frac{1}{4}}[|X|+|Y|]^{\frac{1}{4}}.$$

Таким же образом

$$|y|<2^{\frac{1}{2}}A^{\frac{1}{24}}L^{\frac{1}{4}}[|X|+|Y|]^{\frac{1}{4}} \quad \text{и} \quad |x|+|y|<2^{\frac{2}{3}}A^{\frac{1}{24}}L^{\frac{1}{4}}[|X|+|Y|]^{\frac{1}{4}}.$$

Итак, сумма абсолютных величин x и y для нового решения, вообще говоря, меньше такой же суммы для взятого решения (X, Y, Z). Повторив ту же операцию над (x, y, z), мы придем к еще меньшему решению и т. д., до тех пор, пока мы не придем к одному из решений (x_i, y_i, z_i) или к решению, для которого указанная операция уже не будет сопровождаться уменьшением величины $|x|+|y|$.

Это будет, когда $|x|+|y|$ станет меньше, чем $M=(2^{\frac{3}{2}}A^{\frac{1}{24}}L^{\frac{1}{4}})^{\frac{4}{3}}=$ $=4A^{\frac{1}{18}}L^{\frac{1}{3}}$.

Итак, посредством спуска можно перейти от любого решения к такому, для которого $|x|+|y|<4A^{\frac{1}{18}}L^{\frac{1}{3}}$.

Резюмируем полученные результаты.

Число m основных решений уравнения $x^3+y^3=Az^3$ конечно. Именно:

$m\leqslant k+1$, если A делится на 3 или $A\equiv\pm 1 \pmod 9$,
$m\leqslant k$ „ $A\equiv\pm 2, \pm 4 \pmod 9$,

где $3^k=s$ — числo классов идеалов поля $\Omega(\sqrt[3]{A})$, кубы которых дают главный класс.

4°. В случае, если A — простое число или квадрат простого числа, методом, аналогичным предыдущему, можно получить более точные оценки числа основных решений, именно число основных решений не более двух. Мы ограничимся рассмотрением A простого, $A\neq 2$, $A\neq 3$.

Теорема 4. *Для того чтобы решение (X, Y, Z) было утроенным для некоторого другого решения (x, y, z), необходимо и достаточно, чтобы $(X+Y)^2$ $(X\zeta+Y\zeta^2)$ было произведением A^2 на куб целого числа поля $\Omega(\zeta)$, где $\zeta=e^{\frac{2\pi i}{3}}$.*

Доказательство. Необходимость непосредственно следует из соотношений $(4'')$ и $(4''')$. Докажем достаточность.

Пусть

$$(X+Y)^2(X\zeta+Y\zeta^2)=A^2(a+b\zeta)^3. \tag{15}$$

Без нарушения общности можно считать X, Y, Z попарно взаимно простыми.

Из $(15)'$ следует, что

$$X(X+Y)^2=A^2(-a^3+3a^2b-b^3), \qquad Y(X+Y)^2=A^2(-a^3+3ab^2-b^3),$$

откуда

$$(X+Y)^3=A^2(-2a^3+3a^2b+3ab^2-2b^3),$$

и, следовательно, $X+Y$ делится на A.

С другой стороны, $(X+Y)(X\zeta+Y\zeta^2)(X\zeta^2+Y\zeta)=AZ^3$.

Числа $X+Y$, $X\zeta+Y\zeta^2$, $X\zeta^2+Y\zeta$ или взаимно просты, или имеют общим делителем $\eta=1-\zeta$, причем в последнем случае $X\zeta+Y\zeta^2$ и $X\zeta^2+Y\zeta$ делятся на η, но не делятся на $3=-\zeta^2\eta^2$.

Следовательно, $X+Y=3^\sigma Av^3$, где $\sigma=0$ или 2.

Подставляя в (15), получим

$$3^{\sigma_1}(X\zeta+Y\zeta^2)=(a_1+b_1\zeta)^3, \text{ где } \sigma_1=0 \text{ или } 1,$$

откуда

$$3^{\sigma_1}X=-a_1^3+3a_1^2b_1-b_1^3, \qquad 3^{\sigma_1}Y=-a_1^3+3a_1b^2-b_1^3. \tag{16}$$

Так как X и Y взаимно просты, то $(a_1, b_1)=1$.

Складывая равенства (16), получим

$$3^{\sigma_1}(X+Y)=-2a_1^3+3a_1^2b_1+3a_1b_1^2-2b_1^3=(2b_1-a_1)(2a_1-b_1)(a_1+b_1).$$

Но $3^{\sigma_1}(X+Y)=3^{\sigma+\sigma_1}Av^3=A(3^{\sigma_1}v)^3$.

Итак

$$(a_1-2b_1)(b_1-2a_1)(a_1+b_1)=A(3^{\sigma_1}v)^3. \tag{17}$$

Числа a_1-2b_1, b_1-2a_1, a_1+b_1 или попарно взаимно просты, или имеют общего делителя 3. Одно из них делится на A, так как A простое.

Обозначим его через t, а остальные — через p, q. Очевидно, что

$$t+p+q=0.$$

С другой стороны, $p=\delta x_1^3$, $q=\delta y_1^3$, $t=-A\delta z_1^3$, где $\delta=1$ или 3 на основании (17).

Следовательно, $x_1^3+y_1^3=Az_1^3$.

Не трудно проверить, что во всех возможных комбинациях t, p, q решение (X, Y, Z) получается по формулам утроения из (x_1, y_1, z_1).

Теорема 5. *Для того чтобы аргументы решений* (x_1, y_1, z_1) *и* (x_2, y_2, z_2) *отличались на утроенный аргумент некоторого третьего решения, необходимо и достаточно, чтобы*

$$\frac{(x_1+y_1)^2(x_1\zeta+y_1\zeta^2)}{(x_2+y_2)^2(x_2\zeta+y_2\zeta^2)}=\lambda^3,$$

где λ *— целое или дробное число поля* $\Omega(\zeta)$.

Доказательство основано на соотношении (3′) и теореме 4 и аналогично доказательству теоремы 3.

5°. Пусть A — простое число вида $6n-1$. Тогда A — простое число в поле $\Omega(\zeta)$, и $x\zeta+y\zeta^2$, если $(x, y)=1$, взаимно просто с A.

Из равенства $(x+y)(x\zeta+y\zeta^2)(x\zeta^2+y\zeta)=Az^3$ заключаем, что для чисел $x+y$ и $x\zeta+y\zeta^2$ имеется 6 возможностей:

$$\begin{aligned}
x+y&=Av^2, & x\zeta+y\zeta^2&=(a+b\zeta)^3,\\
x+y&=Av^2, & x\zeta+y\zeta^2&=\zeta(a+b\zeta)^3,\\
x+y&=Av^2, & x\zeta+y\zeta^2&=\zeta^2(a+b\zeta)^3,\\
x+y&=9Av^2, & x\zeta+y\zeta^2&=\eta(a+b\zeta)^3,\\
x+y&=9Av^2, & x\zeta+y\zeta^2&=\zeta\eta(a+b\zeta)^3,\\
x+y&=9Av^2, & x\zeta+y\zeta^2&=\zeta^2\eta(a+b\zeta)^3,
\end{aligned}$$

и, соответственно, для числа $(x+y)^2(x\zeta+y\zeta^2)$ — три возможности:

$$\begin{aligned}
(x+y)^2(x\zeta+y\zeta^2)&=A^2(a_1+b_1\zeta)^3,\\
(x+y)^2(x\zeta+y\zeta^2)&=A^2\zeta(a_1+a_1\zeta)^3,\\
(x+y)^2(x\zeta+y\zeta^2)&=A^2\zeta^2(a_1+b_1\zeta)^3.
\end{aligned}$$

Отсюда легко получить, аналогично 3°, что уравнение $X^3+Y^3=AZ^3$ может иметь не более одного основного решения.

Если A — простое число вида $6n+1$, то в поле $\Omega(\zeta)$ A разлагается на два простых множителя: $A=\pi_1\pi_2$.

В этом случае для числа $(x+y)^2\,(x\zeta+y\zeta^2)$ имеется 9 возможностей:

$$(x+y)^2(x\zeta+y\zeta^2) = A^2\ (a+b\zeta)^3, = \pi_1\ (a+b\zeta)^3, = \pi_2\ (a+b\zeta)^3,$$
$$= A^2\zeta\,(a+b\zeta)^3, = \pi_1\zeta\ (a+b\zeta)^3, = \pi_2\zeta\ (a+b\zeta)^3,$$
$$= A^2\zeta^2(a+b\zeta)^3, = \pi_1\zeta^2(a+b\zeta)^3, = \pi_2\zeta^2(a+b\zeta)^3,$$

и, соответственно, уравнение $X^3+Y^3=AZ^3$ может иметь не более двух основных решений.

Можно еще уточнить оценки числа основных решений следующим образом.

В случае, если $(x+y)^2(x\zeta+y\zeta^2)=A^2\zeta\,(a+b\zeta)^3$, число $x\zeta+y\zeta^2$ имеет вид $\zeta(a_1+b_1\zeta)^3$, или тот же вид имеет число $3(x\zeta+y\zeta^2)$; соответственно $x+y=Av^3$ или $9Av^3$.

Но тогда

$$3^{\sigma_1}x = a_1^3 - 3a_1b_1^2 + b_1^3, \qquad 3^{\sigma_1}y = 3a_1^2b_1 - 3a_1b_1^2,$$

откуда

$$3^{\sigma_1}(x+y) = a_1^3 + 3a_1^2b_1 - 6a_1b_1^2 + b_1^3 \text{ и } a_1^3 + 3a_1^2b_1 - 6ab_1^2 + b_1^3 = A(3^{\sigma_1}v)^3.$$

Форма $a_1^3+3a_1^2b_1-6ab_1^2+b_1^3$ может иметь только таких простых делителей, которые разлагаются на идеалы в действительном подполе поля $\Omega\left(e^{\frac{2\pi i}{9}}\right)$, т. е. простых делителей вида $18n\pm1$.

Следовательно, если $A\not\equiv\pm1\pmod{18}$, то рассмотренная возможность отпадает, и число основных решений уравнения $x^3+y^3=Az^3$ понижается на единицу.

Итак, для простых $A\neq2, \neq3$ уравнение $x^3+y^3=Az^3$ имеет

при $A=18n+1$ не более двух основных решений,

„ $A=18n+7$, „ $A=18n+13$, „ $A=18n+17$ } не более одного основного решения,

„ $A=18n+5$, „ $A=18n+11$ } не имеет решений.

Для $A=A_1^2$, где A_1 — простое число, верны те же оценки числа основных решений.

ТАБЛИЦА ОСНОВНЫХ РЕШЕНИЙ УРАВНЕНИЙ

$x^3+y^3=Az^3$ для $A\leqslant50$

	Число основных решений	Осиовные решения		Число основных решеиий	Осиовные решения
6	1	(37, 17, 21)	28	1*	(3, 1, 1)
7	1	(2,—1, 1)	30	2	(289, — 19, 93);
9	1	(2, 1, 1)			(163, 107, 57)
12	1	(89, 19, 39)	31	1	(137, — 65, 42)
13	1	(7, 2, 3)	33	1	(1853, 523, 582)
15	1	(397, 683, 294)	34	1	(631, — 359, 182)
17	1	(18, — 1, 7)	35	1*	(3, 2, 1)
19	2	(8, 1, 3); (5, 3, 2)	37	2	(4, — 3, 1) и (19, 18, 7)
20	1	(19, 1, 7)	42	1*	(449, — 71, 129)
22	1	(25469, 17299, 9954)	43	1	(7, 1, 2)
26	1*	(3, —1, 1)	49	1	(11, — 2, 3)
			50	1	(23417, —11267, 6111).

* Для $A=26, 28, 35, 42$ применение результатов 3^0 дает, что число осиовных решений $\leqslant2$; но легко доказать рассуждением, аналогичным 4^0, что оно $\leqslant1$. Для всех остальных $A\leqslant50$ известно, что уравнение $x^3+y^3=Az^3$ не имеет решений, кроме тривиальных.