Лекции по алгебре, III семестр, мех-мат МГУ

В. А. Артамонов

Содержание

Глава 1. Основы теории групп 5
1. Группы, подгруппы, порядки элементов 5
2. Смежные классы и теорема Лагранжа 7
3. Гомоморфизмы, нормальные подгруппы, факторгруппы 8
4. Действия групп на множествах 10
5. Теоремы Силова 12
6. Простые группы 14
7. Разрешимые группы 16
8. Прямые произведения групп 18

Глава 2. Конечно порожденные абелевы группы 21

Глава 3. Кристаллографические группы 27
1. Группы движений 27
2. Двумерный случай 28
3. Трехмерный случай 29

Глава 4. Элементы теории представлений групп 33
1. Основные понятия и примеры 33
2. Теорема Машке и ее приложения 34

Глава 5. Алгебры и поля 37
1. Кольца и алгебры 37
2. Теорема Фробениуса 41
3. Основы теории полей 43
4. Конечные поля 44
5. Алгебры Ли 45

Глава 6. Линейные группы и их алгебры Ли 47
1. Касательные пространства 47
2. Структура алгебры Ли на T_E 50
3. Представления групп Ли 54

ГЛАВА 1

Основы теории групп

В этой главе изучаются основные понятия теории групп.

1. Группы, подгруппы, порядки элементов

Напомним некоторые необходимые определения.

Определение 1.1. Множество G с бинарной операцией умножения xy называется *группой*, если

(1) умножение ассоциативно, т. е. $(xy)z = x(yz)$ для всех $x, y, z \in G$;
(2) существует такой элемент $1 \in G$, называемый *единицей* G, что $x1 = 1x = x$ для всех $x \in G$;
(3) для любого элемента $x \in G$ найдется такой элемент x^{-1}, называемый *обратным* к x, что $xx^{-1} = x^{-1}x = 1$.

Определение 1.2. *Порядком* группы G называется число $|G|$ элементов в G.

Упражнение 1.3. Пусть $\mathbb{F}_q$ – поле из q элементов. Доказать, что

$$|\operatorname{GL}(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Предложение 1.4. *Единичный элемент в группе единственен. Для каждого элемента $x \in G$ обратный элемент x^{-1} определен однозначно. Кроме того, если $x \in G$, то $(x^{-1})^{-1} = x$.*

Определение 1.5. Непустое подмножество H в группе G называется *подгруппой*, если вместе с любыми двумя его элементами оно содержит их произведение, и с каждым своим элементом H содержит его обратный.

Предложение 1.6. *Если H – подгруппа в группе G и 1 – единичный элемент G, то $1 \in H$.*

Упражнение 1.7. В произвольной группе произведение любого числа элементов не зависит от расстановки скобок.

Предложение 1.8. *Для непустого подмножества H в группе G следующие условия эквивалентны:*

(1) *H является подгруппой в G;*
(2) *если $x, y \in H$, то $xy^{-1} \in H$.*

Доказательство. Пусть выполнено условие (1), и $x, y \in H$. В силу определения 1.5 получаем $x, y^{-1} \in H$, откуда $xy^{-1} \in H$, т. е. выполнено условие (2).

Обратно, пусть выполнено условие (2), и $y \in H$. Тогда $y, y \in H$, откуда $1 = yy^{-1} \in H$ по (2). Далее $1, y \in H$, откуда $y^{-1} = 1y^{-1} \in H$ по (2). Наконец, если $x, y \in H$, то $x, y^{-1} \in H$ по доказанному выше. Отсюда $x(y^{-1})^{-1} = xy \in H$ по предложению 1.4. □

Примеры 1.9. Приведем примеры групп и их подгрупп:

(1) группа S_n содержит подгруппы A_n, S_{n-1};

(2) группа $\mathrm{SL}(n,\mathbb{C})$ содержит подгруппы

$$\mathrm{GL}(n,\mathbb{R}),\quad \mathrm{GL}(n,\mathbb{Q}),\quad \mathrm{SL}(n,\mathbb{C}),\quad \mathrm{SL}(n,\mathbb{R}),\quad \mathrm{O}(n,\mathbb{R}),$$
$$\mathrm{SO}(n,\mathbb{R}) = \mathrm{SL}(n,\mathbb{R}) \cap \mathrm{O}(n,\mathbb{R}),\quad \mathrm{U}(n,\mathbb{C}),$$
$$\mathrm{SU}(n,\mathbb{C}) = \mathrm{SL}(n,\mathbb{C}) \cap \mathrm{U}(n,\mathbb{C});$$

(3) группа * содержит подгруппы $U = \mathrm{U}(1,\mathbb{C})$, $U_n = \{z \in \mathbb{C} | z^n = 1\}$;
(4) группа диэдра $D_n, n \geq 3$, состоящая из всех движений $\mathbb{R}^2$, переводящих правильный n-угольник в себя.

Предложение 1.10. *Пусть правильный n-угольник расположен в $\mathbb{C} = \mathbb{R}^2$, причем его центр находится в нуле, вершины лежат на окружности радиуса 1, и одна из вершин в точке 1. Пусть*

$$a = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Тогда D_n состоит из элементов

$$1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}$$

и потому имеет порядок $2n$. Кроме того, $a^n = b^2 = (ba)^2 = 1$.

Упражнение 1.11. Пусть

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{C}).$$

Доказать, что

(1) $I^2 = J^2 = K^2 = -E$, $\quad IJ = K, JK = I, KI = J, JI = -K, KJ = -I, IK = -J$;
(2) 8 матриц $\pm E, \pm I, \pm J \pm K$ образуют подгруппу кватернионов Q_8 в группе $\mathrm{SL}(2,\mathbb{C})$.

Упражнение 1.12. Если $H_i, i \in I$ – подгруппы группы G, то $\cap_{i\in I} H_i$ – подгруппа группы G.

Определение 1.13. Пусть a – элемент группы G. Для произвольного целого числа n положим

$$a^n = \begin{cases} 1, & \text{если } n = 0; \\ \underbrace{a \cdots a}_{n \text{ множителей}}, & \text{если } n > 0; \\ (a^{-n})^{-1}, & \text{если } n < 0. \end{cases}$$

Предложение 1.14. *Пусть a – элемент некоторой группы и $n, m \in \mathbb{Z}$. Тогда*

$$a^{n+m} = a^n a^m, \quad (a^n)^m = a^{nm}.$$

Определение 1.15. Пусть a – элемент некоторой группы. *Порядком* $|a|$ (или $o(a)$) элемента a называется такое наименьшее натуральное число n, что $a^n = 1$. Если такого числа n нет, то говорят, что порядок a равен бесконечности.

Предложение 1.16. *Пусть $|a| = n < \infty$, и $m \in \mathbb{Z}$. Следующие условия эквивалентны:*

(1) $n|m$ $\quad$ *(n делит m);*
(2) $a^m = 1$.

Определение 1.17. Пусть $a \in G$. Через $\langle a \rangle$ обозначим множество $\{a^n | n \in Z\}$ всех степеней элемента a.

Упражнение 1.18. $\langle a \rangle$ является подгруппой в G.

Определение 1.19. Пусть $a \in G$. Подгруппа $\langle a \rangle$ называется *циклической* подгруппой в группе G, порожденной элементом a. Группа G называется *циклической* с *порождающим (образующим)* элементом a, если $\langle a \rangle = G$.

Примеры 1.20. Доказать, что

(1) группа $\mathbb{Z}$ является циклическая с порождающим элементом 1 (или -1);
(2) группа U_n комплексных корней n-ой степени из 1 является циклической группой с порождающим элементом

$$\exp \frac{2\pi i}{n} = \cos \frac{2\pi i}{n} + i \sin \frac{2\pi i}{n}.$$

Предложение 1.21. *Пусть a – элемент некоторой группы. Тогда $|\langle a \rangle| = |a|$.*

Доказательство. Если $a^r = a^m$ при некоторых $r < m$, то

$$a^{m-r} = 1, \text{ и } |a| = n < \infty.$$

В этом случае

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}.$$

□

Обозначение 1.22. Если $|a| = n$ в условии предложения 1.21, то циклическую группу, порожденную элементом a, мы будем обозначать $\langle a \rangle_n$.

Теорема 1.23. *Подгруппа циклической группы сама является циклической.*

Доказательство. Пусть H – подгруппа циклической группы $G = \langle a \rangle$. Если $H = 1$, то утверждение очевидно. Пусть H содержит неединичный элемент $a^m, m \neq 0$. Если $m < 0$, то H содержит и элемент $a^{-m}, -m > 0$. Выберем такое наименьшее натуральное число m, что $b = a^m \in H$. Если $a^r \in H, r \in \mathbb{Z}$, то, деля r с остатком на m, получаем $r = sm + q, 0 \leq q < m$. При этом по предложению 1.14

$$a^q = a^{r-sm} = a^r (a^m)^{-s} \in H,$$

что противоречит выбору m, если $q > 0$. □

Следствие 1.24. *Пусть $m_1, \ldots, m_n \in Z$, и d – чисел $m_1, \ldots, m_n$. Тогда существуют такие целые числа $u_1, \ldots, u_n \in Z$, что $m_1 u_1 + \cdots + m_n u_n = d$.*

Доказательство. Пусть $H = \mathbb{Z}m_1 + \cdots + \mathbb{Z}m_n$. Тогда H – подгруппа в $\mathbb{Z}$, и, следовательно, $H = \mathbb{Z}d$. Остается убедиться, что $d = (m_1, \ldots, m_n)$. □

Теорема 1.25. *Пусть $G = \langle a \rangle_n$ и H – подгруппа в G. Тогда существует и притом единственное такое число d, делящее n, что $H = \langle a^d \rangle_{\frac{n}{d}}$.*

Доказательство. По теореме 1.23 получаем $H = \langle a^k \rangle$ для некоторого $0 \leq k < n$. Положим $d = (n, k)$. Остается заметить, что $H = \langle a^d \rangle$. □

Упражнение 1.26. Описать все подгруппы в $\langle a \rangle_{12}$.

2. Смежные классы и теорема Лагранжа

Определение 1.27. Пусть H – подгруппа в группе G, и $g \in G$. *Левым смежным классом* gH называется подмножество $\{gh | h \in H\}$ в G.

Упражнение 1.28. Найти

(1) левые смежные классы $\mathrm{GL}(n, \mathbb{C})$ по $\mathrm{SL}(n, \mathbb{C})$;
(2) левые смежные классы $\mathbb{Z}$ по $n\mathbb{Z}$;
(3) левые и правые смежные классы S_n по S_{n-1}.

Упражнение 1.29. Пусть H – подгруппа в группе G и $x, y \in G$. Доказать, что следующие условия эквивалентны:

(1) $xH = yH$;
(2) $x^{-1}y \in H$.

Предложение 1.30. *Пусть H – подгруппа в группе G и $x \in G$. Тогда $|H| = |xH|$.*

Предложение 1.31. *Пусть H – подгруппа в группе G и $x, y \in G$, причем $y \in xH$. Тогда $xH = yH$.*

Доказательство. Ясно, что $yH \subseteq xH$. По условию $y = xh$ для некоторого $h \in H$. Следовательно, для любого $u \in H$ получаем $xu = y(h^{-1}u)$, где $h^{-1}u \in H$. Отсюда $xH \subseteq yH$, т. е. $xH = yH$. □

Следствие 1.32. *Пусть H – подгруппа в группе G. Тогда два левых (правых) смежных класса G по H либо совпадают, либо не пересекаются.*

Доказательство. Воспользоваться предложением 1.31. □

Теорема 1.33 (Теорема Лагранжа). *Пусть H – подгруппа в конечной группе G. Тогда $|G| = |H|j$, где j – число левых (правых) смежных класса G по H.*

Доказательство. Разобъем G на левые смежные классы по H. Тогда каждый элемент $x \in G$ лежит в некотором классе, именно, в xH. Остается воспользоваться следствием 1.32 и предложением 1.30. □

Следствие 1.34. *Порядок элемента конечной группы делит порядок группы.*

Следствие 1.35. *Группа простого порядка является циклической.*

3. Гомоморфизмы, нормальные подгруппы, факторгруппы

Определение 1.36. Отображение групп $f : G \to H$ называется *гомоморфизмом*, если $f(xy) = f(x)f(y)$ для всех $x, y \in G$. Инъективный гомоморфизм называется *мономорфизмом*. Сюръективный гомоморфизм называется *эпиморфизмом*. Биективный гомоморфизм называется *изоморфизмом*. Изоморфизм группы на себя называется *автоморфизмом*.

Примеры 1.37. Примеры гомоморфизмов:

(1) $\det : \mathrm{GL}(n, \mathbb{C}) \to C^*$;
(2) знак подстановки $\sigma : S_n \to \{\pm 1\}$.

Упражнение 1.38. Если g – фиксированный элемент группы G, то отображение $x \mapsto gag^{-1}$ является автоморфизмом группы G.

Определение 1.39. Автоморфизм из упражнения 1.38 называется *внутренним*. Он также называется *сопряжением с помощью g*.

Предложение 1.40. *Пусть $f : G \to H$ – гомоморфизмом. Тогда $f(1) = 1$ и $f(x^{-1}) = f(x)^{-1}$ для всех $x \in G$.*

Упражнение 1.41. Пусть $f : G \to H$ – гомоморфизм групп. Доказать, что

(1) если G_1 – подгруппа в G, то $f(G_1)$ является подгруппой в H;
(2) если $g : H \to F$ – гомоморфизм групп, то $gf : G \to F$ также является гомоморфизмом групп.

Определение 1.42. Подгруппа H в группе G называется *нормальной*, если $xHx^{-1} \subseteq H$ для любого $x \in G$. Если H –нормальная подгруппа в группе G, то пишут $H \triangleleft G$.

Предложение 1.43. *Пусть H – подгруппа в группе G. Тогда следующие условия эквивалентны:*

(1) *подгруппа H нормальна в G;*
(2) *$xHx^{-1} = H$ для любого $x \in G$;*
(3) *каждый левый смежный класс G по H является правым смежным классом;*
(4) *каждый правый смежный класс G по H является левым смежным классом.*

Доказательство. Пусть выполнено условие (1) и $x \in G$. Тогда

$$x^{-1}H(x^{-1})^{-1} = x^{-1}Hx \subseteq H,$$

откуда $H \subseteq xHx^{-1}$ и поэтому $xHx^{-1} = H$ в силу (1).

Пусть теперь выполнено (2). Тогда $xH = xHx^{-1}x = Hx$, т. е. выполнено (3).

Предположим теперь, что выполнено (3), и рассмотрим левый смежный класс xH. По условию он является правым смежным классом, содержащим x, т. е. $xH = Hx$ по предложению 1.31. Отсюда вытекает (2), и, следовательно, (1).

Итак, первые три условия эквивалентны. Аналогично показывается, что четвертое условие эквивалентно второму. □

Определение 1.44. Пусть $f : G \to H$ – гомоморфизм групп. *Ядром* $\ker f$ называется множество всех таких $x \in G$, что $f(x) = 1$.

Предложение 1.45. $\ker f \lhd G$.

Примеры 1.46. Доказать, что

(1) $A_n \lhd S_n$;
(2) $\mathrm{SL}(n, \mathbb{C}) \lhd \mathrm{GL}(n, \mathbb{C})$;
(3) $V_4 \lhd S_4$, $S_3 \not\lhd S_4$.

Упражнение 1.47. Пусть $f : G \to H$ – гомоморфизм групп. Доказать, что отображение f инъективно $\iff \ker f = 1$.

Предложение 1.48. *Пусть $f : G \to H$ – гомоморфизм групп и $x \in G$. Тогда $f^{-1}(f(x)) = x \ker f$.*

Доказательство. Заметим, что в силу упражнения 1.29

$$y \in f^{-1}(f(x)) \iff f(y) = f(x) \iff f(x^{-1}y) = 1$$
$$\iff x^{-1}y \in \ker f \iff x \ker f = y \ker f.$$

Отсюда вытекает утверждение □

Построение *факторгруппы* G/N, где $N \lhd G$. Построение *естественного гомоморфизма* $\pi : G \to G/N$.

Упражнение 1.49. Если $\pi : G \to G/N$ – естественный гомоморфизм, то $\ker \pi = N$.

Теорема 1.50 (Теорема о гомоморфизмах). *Пусть $f : G \to H$ – гомоморфизм групп. Тогда $G/\ker f \simeq f(G)$.*

Доказательство. Пусть $x \in G$. По предложению 1.48 получаем, что $f^{-1}(f(x)) = x \ker f$. Зададим теперь отображение $\zeta : f(G) \to G/\ker f$ по правилу

$$\zeta(f(x)) = f^{-1}(f(x)) = x \ker f.$$

Проверим, что ζ является гомоморфизмом групп. Пусть $x, y \in G$. Тогда $xy \in f^{-1}(f(xy))$, т. е.

$$\zeta(f(xy)) = xy(\ker f) = (x \ker f)(y \ker f) = \zeta(f(x))\zeta(f(y)).$$

Итак, ζ является гомоморфизмом.

Убедимся, что ζ инъективно. Пусть $g, h \in f(G)$ и $\zeta(g) = \zeta(h)$. По определению $g = f(x), h = f(y)$ для некоторых $x, y \in G$. Отсюда $x \ker f = y \ker f$, и поэтому $g = f(x) = f(y) = h$.

Убедимся, что ζ сюръективно. Если $x \in G$, то $x \ker f = \zeta(f(x))$. Итак, ζ – изоморфизм. □

Примеры 1.51. Доказать, что

(1) $\mathrm{GL}(n, \mathbb{C})/\mathrm{SL}(n, \mathbb{C}) \simeq \mathbb{C}^*$;
(2) $S_n/A_n \simeq \{\pm 1\}$;
(3) $\mathbb{Z}/n\mathbb{Z} \simeq U_n$.

4. Действия групп на множествах

Определение 1.52. Пусть G – группа и X – множество. Скажем, что G *действует* на X, если задано такое отображение

$$G \times X \to X, \quad (g, x) \mapsto gx \in X, \quad g \in G, x \in X,$$

что $1x = x, (gh)x = g(h(x))$ для всех $g, h \in G$ и $x \in X$. Другими словами, задан гомоморфизм группы G в группу перестановок множества X.

Примеры 1.53.

✠ Действие группы G сопряжениями на G.
♭ Пусть H – подгруппа в G. Тогда H действует умножениями слева на $X = G$.
♮ Группа $G = \mathrm{GL}(n, \mathbb{C})$ действует на n-мерном векторном комплексном пространстве $\mathbb{C}^n$.
♯ Группа S_n действует на кольце многочленов $\mathbb{C}[X_1, \ldots, X_n]$ по правилу

$$\sigma(f(X_1, \ldots, X_n)) = f(X_{\sigma 1}, \ldots, X_{\sigma n}).$$

Определение 1.54. Пусть задано действие группы G на множестве X, и $x \in X$. *Орбитой* Orb_x элемента x называется подмножество $\{gx | g \in G\}$. *Стабилизатором* St_x называется подмножество всех таких $g \in G$, что $gx = x$.

Предложение 1.55. *В случае действия ✠ орбита* Orb_x *совпадает с классом сопряженных элементом* $\{gxg^{-1} | g \in G\}$. *Стабилизатор* St_x *элемента* $x \in G$ *совпадает с централизатором* $C(x) = \{g \in G | gx = xg\}$.

В случае действия ♭ орбита Orb_x *совпадает с правым смежным классом* Hx. *Стабилизатор* St_x *элемента* $x \in G$ *равен 1.*

Предложение 1.56. *Разные орбиты не пересекаются.*

Предложение 1.57. *Пусть задано действие группы* G *на множестве* X, *и* $x \in X$. *Существует биекция между* Orb_x *и множеством левых смежных классов* G *по* St_x.

Доказательство. Пусть $g \in G$. Сопоставим элементу $gx \in \mathrm{Orb}_x$ класс gSt_x. □

Следствие 1.58. $|\mathrm{Orb}_x| = \dfrac{|G|}{|\mathrm{St}_x|}$.

Определение 1.59. Пусть задано действие группы G на множестве X, и $x \in X$. Скажем, что точка x *неподвижна* относительно этого действия, если $\mathrm{St}_x = G$, т. е. $\mathrm{Orb}_x = x$.

Замечание 1.60. В случае действия ♯ неподвижными элементами являются симметрические многочлены и только они. В случае действия ✠ неподвижными элементами являются элементы центра $Z(G) = \{x \in G | gx = xg \quad \forall g \in G\}$

Замечание 1.61.

Упражнение 1.62. Найти центры групп

$$\mathrm{GL}(n,k), \mathrm{SL}(n,k), \mathrm{O}(n,\mathbb{R}), \mathrm{U}(n,\mathbb{C}).$$

Теорема 1.63. *Каждая перестановка из S_n разлагается в произведение независимых циклов.*

Пусть $\sigma \in S_n$. Можно считать, что $\sigma \neq 1$. Возьмем произвольный элемент $k, 1 \leq k \leq n$, и предположим, что элементы $k_0 = k, k_1 = \sigma k, k_2 = \sigma^2 k, \ldots, k_l = \sigma^l k$ различны, но $\sigma^{l+1} k = \sigma^s k$, где $0 \leq s \leq l$.

Лемма 1.64. $s = 0$.

Доказательство. Доказательство. Если $s > 0$, то $\sigma(k_{s-1}) = \sigma(k_l)$, что невозможно, ибо σ действует инъективно на $X = \{1, \ldots, n\}$, но $k_{s-1} \neq k_l$ в силу выбора l. □

Итак, на множестве $\{k_0, k_1, \ldots, k_l\}$ подстановка σ действует как

$$\begin{pmatrix} k_0 & k_1 & \ldots & k_{l-1} & k_l \\ k_1 & k_2 & \ldots & k_l & k_0 \end{pmatrix}$$

Выберем теперь произвольное число $j, 1 \leq j \leq n$, причем $j \notin \{k_0, k_1, \ldots, k_l\}$. Как и выше строим множество $\{j_0, j_1, \ldots, j_t\}$, на котором подстановка σ действует как цикл

$$\begin{pmatrix} j_0 & j_1 & \ldots & j_{t-1} & j_t \\ j_1 & j_2 & \ldots & j_t & j_0 \end{pmatrix}$$

Лемма 1.65. *Все элементы $k_0, k_1, \ldots, k_l, j_0, j_1, \ldots, j_t$ различны.*

Доказательство. Пусть $j_r = k_q$. Тогда

$$j_0 = \sigma^{-r} j_r \in \{k_0, k_1, \ldots, k_l\},$$

что невозможно. □

Продолжая этот процесс, получаем подстановку

$$\tau = \begin{pmatrix} k_0 & k_1 & \ldots & k_{l-1} & k_l \\ k_1 & k_2 & \ldots & k_l & k_0 \end{pmatrix} \begin{pmatrix} j_0 & j_1 & \ldots & j_{t-1} & j_t \\ j_1 & j_2 & \ldots & j_t & j_0 \end{pmatrix} \cdots .$$

Непосредственная проверка показывает, что $\tau = \sigma$. □

Упражнение 1.66. Доказать, что

(1) если $\sigma = \sigma_1 \cdots \sigma_m$ – разложение перестановки $\sigma \in S_n$ в произведение независимых циклов, то $|\sigma|$ равен наибольшему общему делителю длин $\sigma_1, \ldots, \sigma_m$;
(2) два независимых цикла из S_n перестановочны.

Предложение 1.67. *Пусть $\pi \in S_n$ и $(i_1, \ldots, i_k)$ – цикл из S_n. Тогда*

$$\pi(i_1, \ldots, i_k)\pi^{-1} = (\pi(i_1), \ldots, \pi(i_k)).$$

Теорема 1.68. *Две перестановки из S_n сопряжены тогда и только тогда, когда они имеют одинаковое цикловое строение.*

Доказательство. Для доказательства необходимости нужно воспользоваться предложением 1.67. Обратно, пусть подстановки σ, τ имеют одинаковое цикловое строение, т. е.

$$\sigma = (k_0, k_1, \ldots, k_l)(j_0, j_1, \ldots, j_t) \cdots ,$$
$$\tau = (k'_0, k'_1, \ldots, k'_l)(j'_0, j'_1, \ldots, j'_t) \cdots .$$

По предложению 1.67 имеем $\pi\sigma\pi^{-1} = \tau$, где

$$\pi = \begin{pmatrix} k_0 & k_1 & \ldots & k_l & j_0 & j_1 & \ldots & j_t & \ldots \\ k'_0 & k'_1 & \ldots & k'_l & j'_0 & j'_1 & \ldots & j'_t & \ldots \end{pmatrix}.$$

□

Теорема 1.69. *Если $n \geq 3$, то $Z(S_n) = 1$.*

Доказательство. Пусть $\sigma \in Z(S_n) \setminus 1$, и

$$\sigma = (i_1, \ldots, i_k)(j_1, \ldots, j_t) \cdots$$

– разложение σ в произведение независимых циклов. Пусть в этом разложении встречаются два цикла длин $k, t \geq 2$. Положим $\pi = (i_1, j_1)$. Тогда $\pi^{-1} = \pi$, и по предложению 1.67

$$\pi\sigma\pi^{-1} = (j_1, i_2, \ldots, i_k)(i_1, j_2, \ldots, j_t) \cdots \neq \sigma,$$

что противоречит условию $\sigma \in Z(S_n)$.

Итак,

$$\sigma = (i_1, \ldots, i_k)$$

является циклом. Если его длина $k \geq 3$, то положим $\pi = (i_1, i_2)$. Тогда $\pi^{-1} = \pi$, и по предложению 1.67

$$\pi\sigma\pi^{-1} = (i_2, i_1, i_3, \ldots, i_k) \neq \sigma,$$

что противоречит условию $\sigma \in Z(S_n)$.

Итак, $\sigma = (i_1, i_2)$. Так как $n \geq 3$, то найдется индекс i_3, отличный от i_1, i_3. Положим $\pi = (i_1, i_3)$. Тогда по предложению 1.67

$$\pi\sigma\pi^{-1} = (i_3, i_2) \neq \sigma,$$

что противоречит условию $\sigma \in Z(S_n)$. □

Упражнение 1.70. Доказать, что две матрицы из $\mathrm{GL}(n, \mathbb{C})$ сопряжены (подобны) тогда и только тогда, когда они имеют одинаковые жордановы формы.

Определение 1.71. Пусть p – простое число. Группа порядка p^n называется *p-группой.*

Теорема 1.72. *Центр p-группы G нетривиален.*

Доказательство. Пусть $G = K_1 \cup \ldots \cup K_m$ – разложение G на непересекающиеся классы сопряженных элементов. Заметим, что $|K_i| = 1$ тогда и только тогда, когда $K_i = \{a_i\}$, где $a_i \in Z(G)$. Отсюда

$$G = Z(G) \cup K_r \cup \ldots \cup K_m, \quad |K_i| > 1. \tag{1}$$

По следствию 1.58 порядок $|K_i|$ делит порядок группы G, т. е. $|K_i| = p^{n_i}, n > n_i > 0$. Отсюда по (1) число p делит порядок $Z(G)$. □

5. Теоремы Силова

Теорема 1.73 (Первая теорема Силова). *Пусть G – конечная группа порядка $p^n m$, где p – простое число. Тогда в G существует подгруппа порядка p^n.*

Доказательство. Будем вести доказательство индукцией по порядку группы G. Случай $|G| = p^n$ очевиден.

Предположим сначала, что существует элемент $x \in G \setminus Z(G)$. Рассмотрим действие G сопряжениями на G. Тогда $1 < |\operatorname{Orb}_x| < |G|$ и $|G| = |\operatorname{Orb}_x||\operatorname{St}_x|$. Поэтому если p не делит $|\operatorname{Orb}_x|$, то p^n делит $|\operatorname{St}_x|$, причем $|\operatorname{St}_x| < |G|$. По индукции в St_x существует подгруппа порядка p^n, и теорема доказана.

Пусть p делит $|\operatorname{Orb}_x|$ для любого $x \in G \setminus Z(G)$. Тогда как и в (1) имеем

$$|G| = |Z(G)| + \sum_{x \in G \setminus Z(G)} |\operatorname{Orb}_x|.$$

Таким образом, p делит порядок $Z(G)$.

Лемма 1.74. *В $Z(G)$ существует элемент порядка p.*

Доказательство. Доказательство будем вести индукцией по порядку $|Z(G)|$. Если $|Z(G)| = p$, то утверждение очевидно. Пусть $|Z(G)| > p$, и $a \in Z(G) \setminus 1$. Предположим, что p не делит порядок a. Тогда $N = \langle a \rangle \triangleleft Z(G)$, причем

$$|Z(G)/N| = \frac{|Z(G)|}{|N|} < |Z(G)|.$$

По индукции в $Z(G)/N$ имеется элемент $bN, b \in Z(G)$, порядка p. предположим, что элемент b имеет порядок d. Тогда $b^d = 1$. При естественном гомоморфизме $\pi : Z(G) \to Z(G)/N$ получаем, что

$$(bN)^d = \pi(b)^d = \pi(b^d) = \pi(1) = N.$$

Поэтому в силу предложения 1.14 $p = |bN|$ делит d.

Итак, в $Z(G)$ всегда есть элемент b порядка d, делящегося на p. Тогда то $|b^{\frac{d}{p}}| = p$. □

Завершим доказательство теоремы. Пусть $a \in Z(G)$ имеет порядок p, и $N = \langle a \rangle \triangleleft G$. Тогда

$$|G/N| = \frac{|G|}{|N|} = \frac{|G|}{p}.$$

По индукции в G/N имеется подгруппа U порядка p^{n-1}. Пусть $H = \{y \in G | yN \in U\}$. Рассмотрим естественный гомоморфизм $\pi : H \to U, \pi(z) = zN$. По теореме о гомоморфизмах $U \simeq H/N$, и поэтому $|H| = |U||N| = p^n$. □

Определение 1.75. Пусть G – конечная группа порядка $p^n m$, где p – простое число, причем $(p, m) = 1$. Подгруппа порядка p^n в G называется *силовской* p-подгруппой.

Теорема 1.76 (Вторая теорема Силова). *Пусть G – конечная группа, и p – простое число. Тогда любая p-подгруппа в G содержится в некоторой силовской p-подгруппе. Любые две силовские p-подгруппы сопряжены в G.*

Доказательство. Пусть Γ произвольная p-подгруппа в G и P – силовская p-подгруппа в G. Рассмотрим множество $X = \{gP | g \in G\}$ левых смежных классов G по P. Группа Γ действует на X левыми сдвигами, т. е. если $y \in \Gamma$, то $y(gP) = (yg)P$. По следствию 1.58 порядок любой орбиты $|\operatorname{Orb}_{gP}|$ делит $|\Gamma| = p^k, k \leq n$. Следовательно, если $|G| = p^n m$, где $(p, m) = 1$, то

$$m = \frac{|G|}{|P|} = \sum_g |\operatorname{Orb}_{gP}| = \sum p^{k_i}.$$

Так как $(p, m) = 1$, то порядок некоторой орбиты Orb_{gP} равен 1, т. е. $\Gamma gP = gP$. Отсюда $g^{-1}\Gamma g \subseteq P$ и $\Gamma \subseteq gPg^{-1}$. Заметим, что $gPg^{-1} \simeq P$ является силовской p-подгруппой. В частности, если Γ – силовская p-подгруппа, то $\Gamma = gPg^{-1}$. □

Теорема 1.77 (Третья теорема Силова). *Пусть N_p – число силовских p-подгрупп в G. Тогда N_p делит порядок группы G и $N_p \equiv 1 \mod p$.*

Доказательство. Пусть S – множество всех силовских p-подгрупп группы G. Рассмотрим действие G на S сопряжениями. По второй теореме Силова S состоит из одной орбиты, причем по следствию 1.58 порядок этой орбиты, равный N_p, делит порядок группы G.

Пусть $S = \{P_0, \ldots, P_r\}$. Рассмотрим действие P_0 на S сопряжениями. Тогда S разбивается на непересекающиеся орбиты, длина каждой из которых равна степени p. Одна из орбит совпадает с P_0, и поэтому $r = p^{e_1} + \cdots + p^{e_s}$. Если $e_i > 0$ для всех $i > 0$, то $r = lp$, откуда $|S| = 1 + r \equiv 1 \mod p$.

Предположим, что, например, $e_1 = 0$, т. е. орбита P_1 также одноэлементна. Это означает, что $gP_1g^{-1} = P_1$ для всех $g \in P_0$. Но тогда P_0P_1 является p-подгруппой в G, содержащей как P_0, так и P_1, т. е. $P_0 = P_0P_1 = P_1$. □

6. Простые группы

Определение 1.78. Неабелева группа G называется *простой*, если в ней только две нормальные подгруппы G и 1.

Теорема 1.79. *Группа A_5 проста.*

Доказательство. Нам потребуется несколько лемм.

Лемма 1.80. *Знак цикла $(i_1, \dots, i_k) \in S_n$ равен $(-1)^{k-1}$.*

Доказательство. $(i_1, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_3)(i_1, i_2)$. □

Лемма 1.81. *Пусть $\sigma \in A_n$ и $\mathrm{Orb}_\sigma, \mathrm{Orb}'_\sigma$ – классы сопряженных элементов σ в S_n и A_n. Тогда либо $\mathrm{Orb}_\sigma = \mathrm{Orb}'_\sigma$, либо*

$$|\,\mathrm{Orb}'_\sigma\,| = \frac{|\,\mathrm{Orb}_\sigma\,|}{2}.$$

Доказательство. Пусть $\tau \in C(\sigma) \setminus A_n$, где $C(\sigma)$ – централизатор σ в S_n. Если $\gamma \in C(\sigma) \setminus A_n$, то $\tau^{-1}\gamma \in C(\sigma) \cap A_n$. Следовательно, получаем разбиение $C(\sigma)$ на два левых смежных класса

$$C(\sigma) = \tau[C(\sigma) \cap A_n] \cup [C(\sigma) \cap A_n]$$

по подгруппе $C(\sigma) \cap A_n$. Отсюда $|C(\sigma)| = 2|C(\sigma) \cap A_n|$, и поэтому

$$|\,\mathrm{Orb}_\sigma\,| = \frac{|S_n|}{|C(\sigma)|} = \frac{n!}{2|C(\sigma) \cap A_n|} = \frac{|A_n|}{|C(\sigma) \cap A_n|} = |\,\mathrm{Orb}'_\sigma\,|.$$

Если же $C(\sigma) \subseteq A_n$, то $C(\sigma) = C(\sigma) \cap A_n$, откуда

$$|\,\mathrm{Orb}_\sigma\,| = \frac{|S_n|}{|C(\sigma)|} = \frac{n!}{|C(\sigma) \cap A_n|} = \frac{2|A_n|}{|C(\sigma) \cap A_n|} = 2|\,\mathrm{Orb}'_\sigma\,|.$$

□

Лемма 1.82. *Все тройные циклы образуют один класс сопряженных элементов в $A_n, n \geq 5$.*

Доказательство. Рассмотрим класс сопряженных в A_n элементов, содержащий тройной цикл (i, j, k). Если $l \neq m \notin \{i, j, k\}$, то

$$(k, l, m)(i, j, k)(k, l, m)^{-1} = (i, j, l).$$

Отсюда вытекает утверждение леммы. □

Завершим доказательство теоремы. Все тройные циклы образуют один класс сопряженных элементов в A_5. Этот класс имеем порядок

$$2\binom{5}{3} = 2\frac{5!}{2!3!} = \frac{5!}{3!} = 20,$$

поскольку $(i, j, k), (j, i, k)$ – единственные циклы, построенные на трех элементах i, j, k. Далее

$$(j, k, l)(i, j)(k, l)(j, k, l)^{-1} = (i, k)(j, l);$$
$$(j, k, m)(i, j)(k, l)(j, k, m)^{-1} = (i, k)(j, m).$$

Следовательно, все произведения двойных циклов $\{(i, j)(k, l)\}$ образуют один класс из $3 \times 5 = 15$ элементов в A_5.

Рассмотрим класс $\{(1,2,3,4,5)\}$. Если $(1,2,3,4,5) = \pi(1,2,3,5,4)\pi^{-1}$, где $\pi \in S_n$, то π можно заменить на любой элемент $\pi(1,2,3,5,4)^m, m \geq 0$. Следовательно, можно считать, что $\pi(1) = 1$. Тогда по предложению 1.67 $(1,2,3,4,5) = (1,\pi(2),\pi(3),\pi(5),\pi(4))$, т. е. $\pi(2) = 2, \pi(3) = 3, \pi(5) = 4, \pi(4) = 5$. Итак, $\pi = (4,5) \notin A_5$. Таким образом, $(1,2,3,4,5), (1,2,3,5,4)$ лежат в разных классах сопряженных элементов в A_5. По лемме 1.81 имеется два класса сопряженных элементов, состоящих из циклов длины 5 в A_5. Оба класса содержат по

$$\frac{1}{2}\binom{5!}{5} = \frac{4!}{2} = \frac{24}{2} = 12$$

элементов. Действительно, при подсчете числа циклов $(i_1,\ldots,i_5)$ длины 5 можно предполагать, что $i_1 = 1$. Для i_2, i_3, i_4, i_5 остается 4! вариантов.

Итак, имеем разбиение на классы сопряженных элементов

$$A_5 = \{1\}_1 + \{(1,2,3)\}_{20} + \{(1,2)(3,4)\}_{15} + \{(1,2,3,4,5)\}_{12} + \{(1,2,3,5,4)\}_{12}.$$

Пусть $N \lhd A_5$. Тогда N содержит целиком некоторые классы сопряженных элементов. Поэтому

$$|N| = 1 + 20n_2 + 15n_3 + 12n_4 + 12n_5, \text{ где } n_i = 0, 1,$$

и $|N|$ делит $60 = |A_5|$. Единственные варианты: либо все $n_i = 0$, либо все $n_i = 1$. □

Изложим другое доказательство более общей теоремы.

Теорема 1.83. *Группы $A_n, n \geq 5$, просты*

Доказательство. Нам потребуется несколько лемм.

Лемма 1.84. *Группа A_n порождается тройными циклами.*

Доказательство. Если индексы i,j,k,l различны, то $(i,j)(k,l) = (i,j,k)(j,k,l)$, и $(i,j)(j,k) = (i,j,k)$. □

Лемма 1.85. *Пусть $N \lhd A_n$ содержит тройной цикл. Тогда $N = A_n$.*

Доказательство. Пусть $(i,j,k) \in N$ и $(a,b,c) \in A_n$. Так как $n \geq 5$, то существует такая подстановка

$$\sigma = \begin{pmatrix} i & j & k & u & v & \ldots \\ a & b & c & u' & v' & \ldots \end{pmatrix} \in A_n,$$

где $(u,v) = (u',v')$ или $(u,v) = (v',u')$, что $\sigma(i,j,k)\sigma^{-1} = (a,b,c)$. Остается воспользоваться предыдущей леммой. □

Лемма 1.86. *Пусть N содержит подстановку σ, в разложении которой на независимые циклы имеется цикл длины не меньше 4. Тогда $N = A_n$.*

Доказательство. Пусть $\sigma = (i,j,k,l,\ldots)\cdots$. Тогда N содержит элемент

$$\tau = (i,j,k)\sigma(i,j,k)^{-1}\sigma^{-1} = (i,j,l).$$

Остается воспользоваться предыдущей леммой. □

Лемма 1.87. *Пусть N содержит подстановку σ, в разложении которой на на независимые циклы имеются не менее двух циклов длины 3. Тогда $N = A_n$.*

Доказательство. Пусть $\sigma = (i,j,k)(a,b,c)\cdots$. Тогда в N содержится

$$\sigma' = (k,a,b)\sigma(k,a,b)^{-1}\sigma^{-1} = (i,c,k,a,b).$$

Отсюда $N = A_n$ по предыдущей лемме. □

Итак, можно считать, что N содержит подстановку σ, в разложение которой в независимые циклы не более одного цикла длины 3, причем остальные циклы имеют длину 2. Если имеется один тройной цикл, то $\sigma^2 \in N$ является тройным циклом, и тогда $N = A_n$.

Таким образом, можно считать, что σ является произведением четного числа независимых циклов длины 2.

Пусть $\sigma = (i,j)(a,b)$. Если $c \notin \{i,j,a,b\}$, то N содержит

$$(i,j,c)\sigma(i,j,c)^{-1}\sigma = (i,c,j),$$

откуда, как и выше $N = A_n$.

Пусть теперь $\sigma = (i,j)(a,b)(i',j')(a',b')\cdots$. Тогда N содержит и

$$(j,a)(b,i')\sigma(b,i')(j,a)\sigma = (i,i',b)(j,a,j').$$

Как и выше отсюда следует утверждение теоремы. □

7. Разрешимые группы

Определение 1.88. Пусть x, y – элементы группы G. *Коммутатором* элементов x, y называется элемент $[x,y] = xyx^{-1}y^{-1}$.

Упражнение 1.89. Доказать, что

$$[x,y]^{-1} = [y,x], \text{ и } z[x,y]z^{-1} = [zxz^{-1}, zyz^{-1}].$$

Примеры 1.90. Доказать, что

(1) в группе перестановок S_n $[(i,j),(j,k)] = (i,j,k)$, если индексы i,j,k различны;
(2) в группе матриц $\mathrm{GL}(n,k)$, где k – кольцо, $[1 + aE_{ik}, 1 + bE_{kj}] = 1 + abE_{ij}$, если индексы i,j,k различны.

Определение 1.91. *Коммутантом* $G' = [G,G]$ называется множество всех произведений коммутаторов в G.

Предложение 1.92. $G' \lhd G$.

Предложение 1.93. *Если $N \lhd G$, то следующие условия эквивалентны:*

(1) *группы G/N – абелева;*
(2) $N \supseteq G'$.

Теорема 1.94. $S_n' = A_n$.

Доказательство. Нужно воспользоваться леммой 1.84 и примером 1.90. □

Теорема 1.95. *Если $n \geq 3$, и k – поле, то* $\mathrm{GL}(n,k)' = \mathrm{SL}(n,k)' = \mathrm{SL}(n,k)$.

Упражнение 1.96. Доказать, что

(1) если поле k содержит не менее четырех элементов, то $\mathrm{GL}(2,k)' = \mathrm{SL}(2,k)$; именно, если существует такой элемент $q, q-1 \in k^*$, то

$$\left[\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & (q-1)^{-1}a \\ 0 & 1 \end{pmatrix}\right] = 1 + aE_{12};$$

(2) $\mathrm{GL}(2,\mathbb{F}_2) \simeq S_3$, и поэтому $\mathrm{GL}(2,\mathbb{F}_2)' \neq \mathrm{SL}(2,\mathbb{F}_2) = \mathrm{GL}(2,\mathbb{F}_2)$.

Упражнение 1.97. Вычислить $\mathrm{GL}(2,\mathbb{F}_3)'$.

Примеры 1.98. $A_4' = V_4$, и $A_n' = A_n$, если $n \geq 5$.

Определение 1.99. Если G – группа, то положим $G^{(1)} = G'$ и$G^{(k+1)} = [G^k, G^k]$. Группа G разрешима если существует такое натуральное число m, что $G^{(m)} = 1$.

Замечание 1.100. Для любых $m, n > 0$ верно равенство $(G^{(n)})^{(m)} = G^{(n+m)}$.

Предложение 1.101. *Пусть $f : G \to H$ – гомоморфизм групп. Тогда*

$$f(G^{(k)}) \subseteq H^{(k)}.$$

Если f – сюръективно, то $f(G^{(k)}) = H^{(k)}$.

Упражнение 1.102. Доказать, что

(1) если H – подгруппа в группе G, то $H^{(k)} \subseteq G^{(k)}$ для любого натурального числа k;
(2) $G^{(k)} \triangleleft G$ для любого натурального числа k.

Предложение 1.103. *Пусть $N \triangleleft G$. Следующие условия эквивалентны:*

(1) *группы G разрешима;*
(2) *группы G/N, и N разрешимы.*

Доказательство. Воспользоватьсяпредложением 1.101 □

Предложение 1.104. *Для группы G следующие условия эквивалентны:*

(1) *группы G разрешима;*
(2) *существует такой ряд подгруппы*

$$G = G_0 \supset G_1 \supset \cdots \supset G_{k-1} \supset G_k = 1,$$

что $G_{i+1} \triangleleft G_i$ и G_i/G_{i+1} – абелево для всех i.

Доказательство. Нужно воспользоваться предложением 1.103 и индукцией по k, убедившись, что группа G_1 разрешима. □

Следствие 1.105. *Пусть p-простое число. Тогда конечная p-группа разрешима.*

Доказательство. Нужно воспользоваться предложением 1.104 и теоремой 1.72. □

Предложение 1.106. *Пусть*

$$A, A' \in \mathrm{Mat}(t, k), \quad B, B' \in \mathrm{Mat}(t \times s, k), \quad C, C' \in \mathrm{Mat}(s, k).$$

Тогда

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \begin{pmatrix} A' & B' \\ 0 & C' \end{pmatrix} = \begin{pmatrix} AA' & AB' + BC' \\ 0 & CC' \end{pmatrix}$$

Определение 1.107. Группа *верхнетреугольных* матриц $T(n, k)$, k – поле. Группа *верхнеунитреугольных* матриц $UT(n, k)$, k – поле.

Следствие 1.108. *Рассмотрим отображение $\varphi : T(n, k) \to T(n-1, k)$ по правилу: если*

$$X = \left(\begin{array}{c|c} A & B \\ \hline 0 & c \end{array}\right) \in T(n, k), \text{ где } A \in T(n-1, k), B \in \mathrm{Mat}((n-1) \times 1, k), c \in k^*,$$

то $\varphi(X) = A$. Тогда φ является гомоморфизмом групп, причем

$$\varphi(UT(n, k)) = UT(n-1, k).$$

Предложение 1.109. $T(n, k)' \subset UT(n, k)$

Доказательство. Воспользоваться предложением 1.93. □

Теорема 1.110. *Группа $T(n, k)$ разрешима.*

Доказательство. По предложениям 1.109 и 1.103 достаточно показать, что группа $UT(n,k)$ разрешима. Будем вести доказательство индукцией по n. Если $n = 1$, то $UT(1,k) = 1$ и потому разрешима.

Пусть для $n-1$ теорема доказана. Рассмотрим гомоморфизм групп

$$\varphi : UT(n,k) \to UT(n-1,k)$$

из следствия 1.108. Заметим, что

$$\ker\varphi = \left\{ \left(\begin{array}{c|c} E & B \\ \hline 0 & 1 \end{array} \right) \in UT(n,k), \text{ где } B \in \mathrm{Mat}((n-1)\times 1, k) \right\}.$$

По предложению 1.106 получаем, что $\ker\varphi$ – абелева группа. Остается воспользоваться индукцией и следствием 1.103 с $N = \ker\varphi$. □

8. Прямые произведения групп

Определение 1.111. Группы G является *(внутренним) прямым произведением* своих подгрупп $G_1, \ldots, G_n$, (обозначение $G = G_1 \times \cdots \times G_n$) если:

- ♡ каждая подгруппа G_i нормальна в G;
- ♡ каждый элемент $g \in G$ имеет и притом единственное представление в виде произведения $g = g_1 \cdots g_n$, где $g_i \in G_i$.

Если G – группа относительно сложения, то говорят, что G является *прямой суммой* своих подгрупп $G_1, \ldots, G_n$, и пишут $G = G_1 \oplus \cdots \oplus G_n$.

Упражнение 1.112. Доказать, что $|G| = |G_1| \cdots |G_n|$.

Предложение 1.113. *Пусть $G = G_1 \times \cdots \times G_n$ и $g_i \in G_i, g_j \in G_j$, где $i \neq j$. Тогда $g_i g_j = g_j g_i$.*

Следствие 1.114. *Пусть $G = G_1 \times \cdots \times G_n$ и $g = g_1 \cdots g_n$, $h = h_1 \cdots h_n$, где $g_i, h_i \in G_i$ для всех i. Тогда*

$$gh = (g_1 h_1) \cdots (g_n h_n), \quad g^{-1} = g_1^{-1} \cdots g_n^{-1}.$$

Примеры 1.115. Имеются следующие прямые разложения:

(1) группа $\mathbb{C}^* \simeq U \times \mathbb{R}_+^*$;
(2) $\mathbb{R}^n = \mathbb{R}^k \oplus \mathbb{R}^{n-k}$.

Предложение 1.116. *Группа $\mathbb{Z}$ неразложима в прямую сумму.*

Предложение 1.117. *Пусть*

$$G = G_1 \times \cdots \times G_n \text{ и } g = g_1 \cdots g_n.$$

Тогда $|g| = (|g_1|, \ldots, |g_n|)$.

Теорема 1.118. *Пусть группа $G = G_1 \times \cdots \times G_n$ конечна. Следующие условия эквивалентны:*

- *группа G циклична;*
- *каждая группа G_i циклична и порядки групп $G_i, i = 1, \ldots, n$, попарно взаимно просты.*

Доказательство. Пусть группа G циклична, и $m_i = |G_i|$. Тогда каждая подгруппа $G_i, i = 1, \ldots, n$, циклична. Если, например, $(m_1, m_2) > 1$, то

$$(m_1, \ldots, m_n) < m_1 \cdots m_n.$$

Поэтому в силу предложения 1.117 в G нет элемента порядка $m_1 \cdots m_n = |G|$.

Обратно, пусть $G_i == \langle a_i \rangle_{m_i}$, причем все числа $m_1, \ldots, m_n$ попарно взаимно просты. Рассмотрим элемент $a = a_1 \cdots a_n \in G$. По предложению 1.117 его порядок равен

$$m_1 \cdots m_n = |G_1| \cdots |G_n| = |G|.$$

Следовательно, $G = \langle a \rangle$. □

Следствие 1.119. *Циклическая группа порядка d неразложима в прямое произведение тогда и только тогда, когда ее порядок является степенью простого числа.*

Пример 1.120. Прямое разложение циклической группа порядка 12.

Теорема 1.121. *Пусть $N_i \triangleleft G_i, i = 1, \ldots, m$. Тогда*

$$(N_1 \times \cdots \times N_m) \triangleleft (G_1 \times \cdots \times G_m)$$

и

$$(G_1 \times \cdots \times G_m)/(N_1 \times \cdots \times N_m) \simeq (G_1/N_1) \times \cdots \times (G_m/N_m).$$

Доказательство. Рассмотреть гомоморфизм групп

$$\pi : G \to (G_1/N_1) \times \cdots \times (G_m/N_m),$$

отображающий элемент

$$g = g_1 \cdots g_m \mapsto (g_1 N_1) \cdots (g_m N_m) \in (G_1/N_1) \times \cdots \times (G_m/N_m),$$

и воспользоваться теоремой о гомоморфизмах. □

Определение 1.122. Определение *внешнего прямого произведения* $G = G_1 \times \cdots \times G_m$.

Теорема 1.123. *Внешнее и внутреннее прямые произведения изоморфны.*

ГЛАВА 2

Конечно порожденные абелевы группы

В этой главе описывается строение конечно порожденных абелевых групп. Все абелевы группы будут предполагаться аддитивными.

Определение 2.1. Элементы $\mathbf{e} = (e_1, \ldots, e_n)$ являются *базисом* в абелевой группы A, если

- ♣ элементы из $\mathbf{e}$ *независимы*, т. е. из того, что
$$m_1 e_1 + \cdots + m_n e_n = 0, \text{ где } m_1, \ldots, m_n \in \mathbb{Z},$$
следует, что $m_1 = \cdots = m_n = 0$.
- ♠ элемент из $\mathbf{e}$ *порождают* группу A, т. е. каждый элемент $x \in A$ представим в виде $x = m_1 e_1 + \cdots + m_n e_n$.

Другими словами, каждый элемент $x \in A$ имеет и притом единственно представление в виде

$$x = m_1 e_1 + \cdots + m_n e_n, \quad m_i \in \mathbb{Z}. \tag{2}$$

Группа A *свободна*, если она обладает базисом. *Рангом* свободной абелевой группы A называется число векторов в базисе A.

Предложение 2.2. *Для абелевой группы A следующие условия эквивалентны:*

(1) *группа A обладает базисом $\mathbf{e} = (e_1, \ldots, e_n)$;*

(2) *группа*
$$A \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}.$$

Доказательство. Если $\mathbf{e}$ – базис A, то зададим
$$\psi : A \to \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}$$
по правилу: если $x \in A$ имеет представление (2), то $\psi(x) = (m_1, \ldots, m_n)$.

Обратно, группа
$$A = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}$$
обладает базисом $\mathbf{e} = (e_1, \ldots, e_n)$, где
$$e_i = (0, \ldots, \overset{i}{1}, 0, \ldots, 0), \quad i = 1, \ldots, n.$$

□

Предложение 2.3. *Число векторов в базисе свободной абелевой группы определено однозначно. Другими словами, ранг свободной абелевой группы определен однозначно.*

Доказательство. Пусть $(e_1, \ldots e_n)$ и $(f_1, \ldots, f_m)$ – два базиса в A. Предположим, что $m > n$. Тогда каждое f_j имеет представление
$$f_j = \sum_{i=1}^{n} a_{ji} e_i, \quad a_{ji} \in \mathbb{Z}.$$

Строки матрицы $(a_{ji}) \in \mathrm{Mat}(m \times n, \mathbb{Z})$ линейно зависимы над $\mathbb{Q}$. Следовательно, они линейно зависимы над $\mathbb{Z}$. Поэтому найдется такой ненулевой набор целых чисел $b_1, \ldots, b_m \in \mathbb{Z}$, что

$$(b_1, \quad \ldots, \quad b_m) \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} = 0.$$

Отсюда $b_1 f_1 + \cdots + b_m f_m = 0$, что противоречит независимости $f_1, \ldots, f_m$. □

Упражнение 2.4. Пусть A – свободная абелева группа с базисом $\mathbf{e} = (e_1, \ldots, e_n)$. Предположим, что $c_1, \ldots, c_n$ – элементы произвольной абелевой группы C. Тогда существует и притом единственный такой гомоморфизм $\psi : A \to C$, что $\psi(e_i) = c_i$, $1 \leq i \leq n$.

Следствие 2.5. *Пусть A – свободная абелева группа с базисом $\mathbf{e} = (e_1, \ldots, e_n)$. Тогда*

$$|\hom(A, \mathbb{Z}_2)| = 2^n.$$

В частности, ранг A определен однозначно.

Теорема 2.6. *Пусть A – свободная абелева группа ранга n. Если B – ненулевая подгруппа в A, то она свободна и ее ранг $\leq n$.*

Доказательство. Будет вести доказательство индукцией по n. Если $n = 1$, то $A \simeq \mathbb{Z}$. Тогда группа A циклична и, следовательно, по теореме 1.23 группа $B = \langle b \rangle$ циклична, причем $b \neq 0$. Тогда элемент b является базисом B.

Пусть для $n - 1$ теорема доказана, и $\mathbf{e} = (e_1, \ldots, e_n)$ – базис A. Положим

$$H = \{\sum_{i=1}^{n-1} a_i e_i | a_i \in \mathbb{Z}\}.$$

Тогда H – свободная абелева группа с базисом $(e_1, \ldots e_{n-1})$. По индукции $B \cap H$ – свободная абелева группа с базой $(f_1, \ldots, f_m)$, $\quad m \leq n - 1$. Следовательно, если $B \subseteq H$, то теорема доказана.

Пусть $B \nsubseteq H$. Рассмотрим такое наименьшее натуральное число d, что элемент

$$f = c_1 e_1 + \cdots + c_{n-1} e_{n-1} + d e_n \in H.$$

Покажем, что элементы $f_1, \ldots, f_m, f$ составляют базис H. Действительно, если

$$b = u_1 e_1 + \cdots + u_n e_n \in B, \quad u_i \in \mathbb{Z},$$

то $u_n = rd$ для некоторого $r \in \mathbb{Z}$. В самом деле, пусть $u_n = rd + l$, где $0 \leq l < d$. Тогда

$$b - rf = u'_1 e_1 + \cdots + u'_{n-1} e_{n-1} + l e_n \in H,$$

что противоречит выбору d, если $l \neq 0$. Итак, $u_n = rd$ и $b - rf \in B \cap H$. Поэтому

$$b - rf = a_1 f_1 + \cdots + a_m f_m, \quad a_i \in \mathbb{Z}.$$

Таким образом,

$$b = rf + a_1 f_1 + \cdots + a_m f_m, \quad r, a_i \in \mathbb{Z},$$

т. е. элементы

$$f, f_1, \ldots, f_m \tag{3}$$

порождают B.

Покажем, что элементы (3) независимы. Пусть

$$rf + a_1 f_1 + \cdots + a_m f_m = 0, \quad r, a_i \in \mathbb{Z}, \tag{4}$$

Коэффициент при e_n у элемента левой части (3) равен $rd = 0$, откуда $r = 0$, ибо $d \neq 0$. Таким образом, в (4) получаем, что

$$a_1 f_1 + \cdots + a_m f_m = 0,$$

откуда $a_1 = \cdots = a_m = 0$, ибо элементы $f_1, \ldots, f_m$ независимы. □

Определение 2.7. *Целочисленные элементарные преобразования строк (столбцов)* целочисленной матрицы состоят из двух типов преобразований:

- умножение слева (справа) на элементарные матрицы $E + aE_{ij}, a \in \mathbb{Z}$,
- умножение строки (столбца) на -1.

Упражнение 2.8. Совершая целочисленные элементарные преобразования строк (столбцов) можно переставить любые две строки (столбца).

Теорема 2.9. *Пусть* $A \in \mathrm{Mat}(n \times m, \mathbb{Z})$. *Целочисленными элементарными преобразованиями строк и столбцов можно* A *привести к диагональному виду* $\mathrm{diag}(d_1, d_2, \ldots), d_i \geq 0$.

Доказательство. Можно считать, что $A = (a_{ij}) \neq 0$. Пусть

$$\delta(A) = \min_{ij}\{|a_{ij}| \,|a_{ij} \neq 0\}.$$

Предположим, что матрицу A целочисленными элементарными преобразованиями строк и столбцов привели в такому виду, что далее $\delta(A)$ уменьшить нельзя. Переставляя строки и столбцы и умножая, если необходимо, на -1, можно считать, что $\delta(A) = a_{11}$.

Лемма 2.10. a_{11} *делит* a_{1j}, a_{i1} *для всех* i, j.

Доказательство. Пусть, например, a_{11} не делит a_{21}, т. е. $a_{21} = qa_{11} + r$, где $0 < r < a_{11}$. Вычитая из второй строки первую, умноженную на q, получаем на месте (21) элемент r, что противоречит выбору $\delta(A) = a_{11}$. □

По лемме 2.10 совершая элементарные преобразования строк и столбцов, можно добиться, чтобы $a_{1j} = a_{i1} = 0$ для всех $i, j > 1$. Доказательство теоремы завершается индукцией по размеру матрицы. □

Теорема 2.11 (Теорема о согласованном базисе). *Пусть* B *– ненулевая подгруппа в свободной абелевой группе ранга* n. *Тогда в* A *существует такой базис* $\mathbf{e} = (e_1, \ldots, e_n)$ *и такие натуральные числа* $d_1, d_2, \ldots d_k, k \leq n$, *что элементы* $d_1e_1, \ldots, d_ke_k$ *составляют базис* B.

Доказательство. Пусть $f_1 \ldots, f_n$ и $g_1, \ldots, g_k, k \leq n$, – произвольные базисы в A и в B (см. теорему 2.6). Тогда

$$g_i = \sum_{j=1}^{n} a_{ij} f_j, \quad a_{ij} \in \mathbb{Z}, \quad i = 1, \ldots, k.$$

Рассмотрим целочисленную матрицу $A = (a_{ij}) \in \mathrm{Mat}(k \times n, \mathbb{Z})$. Целочисленные элементарные преобразования строк A соответствуют элементарным преобразованиям базиса $g_1, \ldots, g_k$, а целочисленные элементарные преобразования столбцов A соответствуют элементарным преобразованиям базиса $f_1 \ldots, f_n$. По теореме теореме 2.9 изменяя оба базиса, можно считать, что $g_1 = d_1 f_1, \ldots, g_k = d_k f_k$. □

Определение 2.12. Абелева группа A *конечно порождена,* если существуют такие элементы $a_1, \ldots, a_n \in A$, что каждый элемент $x \in A$ имеет представление

$$x = c_1a_1 + \cdots + c_na_n, c_i \in \mathbb{Z}.$$

Определение 2.13. Циклическая группа *примарна,* если ее порядок является степенью простого числа.

Теорема 2.14 (Строение конечно порожденных абелевых групп). *Пусть* A *– конечно порожденная абелева группа. Тогда* A *разлагается в прямую сумму свободной абелевой группы и примарных циклических групп.*

Доказательство. Пусть $a_1, \ldots, a_n \in A$ из определения 2.12. Рассмотрим свободную абелеву группу F ранга n, например,

$$F = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}$$

Выберем в F базис $e_1, \ldots, e_n$ и зададим гомоморфизм $\xi : F \to A$, при котором

$$\xi(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} x_i a_i.$$

Нетрудно видеть, что ξ является эпиморфизмом. Пусть $B = \ker \xi$. По теореме 2.11 можно считать, что $d_1 e_1, \ldots, d_k e_k$ составляют базис B, где $d_1, \ldots, d_k$ – натуральные числа, $k \leq n$. Положим

$$N_i = \begin{cases} \mathbb{Z} d_i e_i, & \text{если } 1 \leq i \leq k; \\ 0, & \text{если } k < i \leq n. \end{cases}$$

По теореме 1.50 о гомоморфизмах и по теореме 1.121 получаем

$$A \simeq F/B \simeq (\mathbb{Z}e_1/N_1) \oplus \cdots \oplus (\mathbb{Z}e_n/N_n). \tag{5}$$

Если $1 \leq i \leq k$, то

$$\mathbb{Z}e_i/N_i = \mathbb{Z}e_i/\mathbb{Z}d_i e_i \simeq \mathbb{Z}/\mathbb{Z}d_i. \tag{6}$$

По теореме 1.118 группа (6) разлагается в прямую сумму примарных циклических групп.

Если $k < i \leq n$, то $N_i = 0$, и поэтому $\mathbb{Z}e_i/N_i \simeq \mathbb{Z}$. Итак, по (5) получаем, что

$$A \simeq (\oplus_i C_i) \oplus H,$$

где C_i – примарные циклические группы, и

$$H = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-k}.$$

По предложению 2.2 группа H свободна. □

Определение 2.15. Группа G *не имеет кручения*, если в ней нет нетривиальных, т. е. отличный от 1, элементов конечного порядка.

Следствие 2.16. *Конечно порожденная абелева группа без кручения свободна.*

Определение 2.17. Подгруппа $H \subseteq \mathbb{R}^n$ *дискретна*, если существует такая окрестность нуля U, что $U \cap H = 0$.

Теорема 2.18. *Дискретная подгруппа в $\mathbb{R}^n$ свободна.*

Доказательство. По следствию 2.16 достаточно показать, что группа H конечно порождена. Выберем в H максимальную линейно независимую систему векторов

$$f_1, \ldots, f_k, \quad k \leq n.$$

Положим

$$= \{\sum_{i=1}^{k} \alpha_i f_i | 0 \leq \alpha_i \leq 1\}.$$

Тогда является компактом, и, следовательно, $\cap H$ конечно. Остается заметить, что H порождается $\cap H, f_1, \ldots, f_k$. □

Теорема 2.19. *Пусть G – дискретная подгруппа в $\mathbb{R}^n$, и $\mathbf{e} = (e_1, \ldots, e_k)$ – ее базис. Тогда векторы из $\mathbf{e}$ независимы в $\mathbb{R}^n$.*

Доказательство. Пусть, например,

$$e_1 = \lambda_2 e_2 + \cdots + \lambda_k e_k, \quad \lambda_i \in \mathbb{R}.$$

Положим

$$S = \{\alpha_2 e_2 + \cdots + \alpha_k e_k | 0 \leq \alpha_j \leq 1, \quad j = 2, \ldots, k\}.$$

Тогда S является компактом, и, следовательно, как и в предыдущей теореме, $S \cap G$ конечно.

Для любого натурального числа d получаем

$$de_1 = [d\alpha_2]e_2 + \cdots + [d\alpha_k]e_k + (\beta_2 e_2 + \cdots + \beta_k e_k),$$

где $\beta_2 e_2 + \cdots + \beta_k e_k \in S \cap G$. Поэтому найдутся такие натуральные числа $d_1 > d_2$, что $d_1 e_1 - d_2 e_1$ лежит в подгруппе, порожденной $e_2, \ldots, e_k$, т. е.

$$(d_1 - d_2)e_1 = m_2 e_2 + \cdots + m_k e_k, \quad m_j \in \mathbb{Z}.$$

Это противоречит определению базиса в G. □

Упражнение 2.20. Пусть G – подгруппа в $\mathbb{R}$, порожденная $1, \sqrt{2}$. Будет ли она плотна в $\mathbb{R}$?

ГЛАВА 3

Кристаллографические группы

1. Группы движений

Определение 3.1. Преобразование Φ евклидова пространства E называется *движением*, если существует такой ортогональный линейный оператор ϕ и вектор b, что $\Phi(x) = \phi(x) + b$ для всех $x \in E$.

Упражнение 3.2. Все движений евклидова пространства E образуют - группу $G(E)$ относительно операции композиции отображений.

Упражнение 3.3. Доказать, что если Φ движение евклидова пространства E, то $\|\Phi(x) - \Phi(y)\| = \|x - y\|$ для всех $x, y \in E$.

Примерами движений являются *сдвиги* $\Phi(x) = x + b$ на фиксированный вектор $b \in E$ и ортогональные преобразования.

Теорема 3.4. *Множество N всех сдвигов образует нормальную подгруппу в $G(E)$, причем $G(E)/N \simeq O(E)$, где $O(E)$ - группа всех ортогональных преобразований в E. Кроме того, $N \simeq E$.*

Доказательство. Зададим отображение $\xi : G(E) \to O(E)$ по следующему правилу. Если $\Phi(x) = \phi(x) + b$ для всех $x \in E$, то положим $\xi(\Phi) = \phi$. Это определение корректно. Действительно, пусть $\Phi(x) = \phi(x) + b = \phi'(x) + b'$ для всех $x \in E$, где $b, b' \in E$ и $\phi, \phi' \in O(E)$. Тогда $\Phi(0) = b = b'$, откуда $\phi(x) = \phi'(x)$ для всех $x \in E$. Покажем теперь, что ξ явялется гомморфизмом групп. Пусть Φ как и выше, $\Psi(x) = \psi(x) + d$. Тогда $\Phi[\Psi(x)] = \phi[\psi(x)] + \phi(d) + b$, и поэтому $\xi(\Phi\Psi) = \phi\psi = \xi(\Phi)\xi(\Psi)$. Более того, $\ker\xi = N$. Поэтому $N \lhd G(E)$ и $G(E)/N \simeq O(E)$.

Сопоставляя $\psi \in N$ вектор $\psi(O)$ получаем изоморфизм $N \simeq E$. □

Определение 3.5. *Кристаллографической или пространственной* группой называется подгрупп Γ в группе движений $G(E)$ евлидова пространства E размерности n, причем

(1) при отождествлении N с E образ L подгруппы $\Gamma \cap N$ является дискретной подгруппой (или решеткой) в E ранга n;
(2) $\Gamma \cap N$ имеет конечный индекс в Γ.

Конечная группа $\Delta = \Gamma/(\Delta \cap N)$ называется *точечной* группой.

Упражнение 3.6. $\Gamma \cap N \lhd \Gamma$.

Обозначение 3.7. Положим $\Delta = \Gamma/(\Gamma \cap N) \subset O(E)$. Зафиксируем в соответствии с теоремой **??** базис $f_1, \ldots, f_n$ образа $\Gamma \cap N$ в E. Тогда L состоит из всех векторов $m_1 f_1 + \cdots + m_n f_n, \quad m_1, \ldots, m_n \in \mathbb{Z}$.

Предложение 3.8. *Пусть $\phi \in \Delta$ и $l \in L$. Тогда $\phi(l) \in L$.*

Доказательство. Пусть $\Phi(x) = \phi(x) + b$ и $\Psi(x) = x + l$ для всех $x \in E$, где $\Phi, \Psi \in \Gamma$. Тогда $\Phi^{-1}(x) = \phi^{-1}(x) - \phi^{-1}(b)$, откуда

$$(\Phi\Psi\Phi^{-1})(x) = \Phi(\Phi^{-1}(x) + l) = \phi(\phi^{-1}(x) - \phi^{-1}(b) + l) + b = x + \phi(l).$$

□

Следствие 3.9. *Существует такая матрица* $X \in GL(n, \mathbb{R})$, *что*

$$X\Delta X^{-1} \subseteq \mathrm{GL}(n, \mathbb{Z}).$$

В частности, если $A \in \Delta$, *то* $\operatorname{tr} A \in \mathbb{Z}$.

Теорема 3.10 (Жордан). *Существует такая функция* $\tau(n)$, *что для любой конечной подгруппы* G *в* $\mathrm{O}(n, \mathbb{R})$ *порядок* G *не превосходит* $\tau(n)$.

2. Двумерный случай

В этом разделе мы опишем кристаллографические группы в двумерном пространстве. Рассмотрим сначала строение конечных подгрупп Δ в группе $\mathrm{SO}(2, \mathbb{R})$. Гуппа $\mathrm{SO}(2, \mathbb{R})$ состоит из всех вращений двумерного евклидова пространства. В любом ортонормированном базисе этого пространства матрица оператора вращения имеет вид

$$g = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

Если $g \in \Delta$, то по следствию 3.9 $\operatorname{tr} g = 2\cos\alpha \in \mathbb{Z}$. Таким образом, $2\cos\alpha = 0, \pm 1, \pm 2$, откуда $\alpha = 0, \pm\dfrac{\pi}{3}, \pm\dfrac{\pi}{2}, \pm\dfrac{2\pi}{3}, \pi$. Итак, доказана

Теорема 3.11. *Подгруппа* Δ *в* $\mathrm{SO}(2, \mathbb{R})$ *является циклической группой порядка 1, 2, 3, 4, 6.*

Пусть теперь $\Delta \subset \mathrm{O}(2, \mathbb{R})$, но $\Delta \not\subset \mathrm{SO}(2, \mathbb{R})$. Тогда Δ содержит симметрию b относительно некоторой оси, причем $b^2 = 1$. Если $x \in \Delta \setminus \mathrm{SO}(2, \mathbb{R})$, то $bx \in \mathrm{SO}(2, \mathbb{R}) \cap \Delta$, причем bx – снова симметрия относительно некоторой оси, т. е. $(bx)^2 = 1$. По теореме 3.11 получаем $\mathrm{SO}(2, \mathbb{R}) \cap \Delta = \langle a \rangle_n, \quad n = 1, 2, 3, 4, 6$. Тогда $\mathrm{SO}(2, \mathbb{R}) \cap \Delta$ – подгруппа индекса 2 в Δ. Отсюда

$$\Delta = \{1, a, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\},$$

т. е. $\Delta = D_n$ – группа диэдра. Итак, доказана

Теорема 3.12. Δ – *одна из следующих групп:*

(1) *циклическая группа вращений порядка 1, 2, 3, 4, 6;*
(2) *группа диэдра* $D_n, \quad n = 1, 2, 3, 4, 6$.

По предложению 3.8 группа Δ действует как группа преобразований решетки L.

Теорема 3.13. *Возможны следующие варианты для решетки* $\Gamma \cap N$ *с базисом* f_1, f_2.

(1) *Длины* f_1, f_2 *различны и они не перпендикулярны. В этом случае опи порождают параллелограм. Тогда* Δ – *циклическая группа порядка 2, порождаемая центральной симметрией, или поворотом на* π.
(2) *Длины* f_1, f_2 *различны и они перпендикулярны. В этом случае опи порождают прямоугольник. Тогда* Δ – *группа* D_2 *порядка 4, порождаемая симметрией относительно прямой, проходящей через* f_1 *и поворотом на* π.
(3) *Длины* f_1, f_2 *одинаковы и они перпендикулярны. В этом случае опи порождают квадрат. Тогда* Δ – *группа* D_4.
(4) *Длины* f_1, f_2 *одинаковы и они не перпендикулярны. Кроме того, длина* $f_1 - f_2$ *отлична от длины* f_2. *В этом случае опи порождают ромб. Тогда* Δ – *группа* D_2, *порождаемая двумя симметриями относительно прямых, параллельных диагоналям ромба.*
(5) *Длины* f_1, f_2 *одинаковы и они не перпендикулярны. Кроме того, длина* $f_1 - f_2$ *равна длине* f_2. *В этом случае опи порождают ромб. Тогда* Δ – *группа* D_6, *порождаемая двумя симметрией относительно прямых, параллельных диагоналям ромба и поворотом на угол* $\dfrac{\pi}{3}$.

Кроме того, для каждой решетки допустимы подгруппы рассмотренных групп симметрий Δ, указанных выше.

3. Трехмерный случай

Рассмотрим теперь трехмерный случай. Как и выше рассмотрим строение конечных подгрупп в $\mathrm{SO}(3,\mathbb{R})$, затем в $\mathrm{O}(3,\mathbb{R})$ и, наконец, возможные решетки и их группы симметрий. Нам потребуется

ТЕОРЕМА 3.14. *Пусть $g \in \mathrm{O}(3,\mathbb{R})$, причем $hgh^{-1} \in GL(3,\mathbb{Z})$. Тогда существует такая матрица $u \in \mathrm{SO}(3,R)$, что*

$$ugu^{-1} = \begin{pmatrix} \det g & 0 & \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}, \tag{7}$$

где $\alpha = 0, \pm\dfrac{\pi}{3}, \pm\dfrac{2\pi}{3}, \pm\dfrac{\pi}{2}, \pi$.

ДОКАЗАТЕЛЬСТВО. Из курса алгебры известно, что матрица ортогонального оператора в некотором ортонормированном базисе имеет вид (7). Поэтому

$$\det g + 2\cos\alpha = \mathrm{tr}(ugu^{-1}) = \mathrm{tr}\, g = \mathrm{tr}(hgh^{-1}) \in \mathbb{Z}.$$

Так как $\det g = \pm 1$, то $2\cos\alpha \in \mathbb{Z}$. Отсюда как и выше получаем требуемое утверждение. □

ОБОЗНАЧЕНИЕ 3.15. Обозначим через S трехмерную сферу единичного радиуса в трехмерном пространстве с центром в нуле. Предположим, что Δ – конечная подгруппа в $\mathrm{SO}(3,\mathbb{R})$. Тогда каждый неединичный элемент из Δ является вращением относительно некоторой оси в перпендикулярной плоскости на угол из теоремы 3.14. Пересечение этой оси с S состоит из двух точек. Обозначим через X – множество всех таких точек из S для всех неединичных элементов из Δ.

ПРЕДЛОЖЕНИЕ 3.16. *Пусть $x \in X$ и $g \in \Delta$. Тогда $g(x) \in X$.*

ДОКАЗАТЕЛЬСТВО. Пусть l – неподвижная ось для $h \in \Delta \setminus 1$, и $x \in l \cap S$. Тогда $ghg^{-1}(g(l)) = g(l)$, т. е. $g(l)$ – неподвижная ось для $ghg^{-1} \in \Delta\setminus 1$, причем $g(x) \in g(l) \cap S$. □

ПРЕДЛОЖЕНИЕ 3.17. *Пусть $x \in X$ и Δ_x – стабилизатор x в Δ, т. е. множество всех таких $g \in \Delta$, что $g(x) = x$. Тогда H_x – циклическая группа порядка 1, 2, 3, 4, 6. При этом если $\Delta = \Delta_x \cup g_2\Delta_x \cup \ldots \cup g_m\Delta_x$ – разбиение Δ на левые смежные классы по Δ_x, то орбита x при действии Δ имеет порядок m и состоит из $x, g_2(x), \ldots, g_m(x)$. В частности, $|\Delta| = m|\Delta_x|$. Стабилизатор $g_i(x)$ равен $g_i\Delta_x g_i^{-1}$.*

ДОКАЗАТЕЛЬСТВО. Сопоставим $g_i\Delta_x$ элемент $g_i(x)$. □

ОБОЗНАЧЕНИЕ 3.18. Обозначим через M множество пар (x, g), где $g \in \Delta_x \setminus 1$.

Так как каждому $g \in \Delta\setminus 1$ соответствуют две точки из X, то $|M| = 2(|\Delta|-1)$. С другой стороны, X разбивается на орбиты $X_1, \ldots, X_k$ действия группы Δ. По предложению 3.17 число пар (x, g), где x пробегает одну орбиту X_i порядка m_i равно $m_i(|\Delta_i|-1)$, где $\Delta_i = \Delta_{x_i}$ для некоторого элемента $x_i \in X_i$. Кроме того, $m_i|\Delta_i| = |\Delta|$. Итак,

$$2(|\Delta| - 1) = m_1(|\Delta_1| - 1) + \cdots + m_k(|\Delta_k| - 1).$$

Деля на $|\Delta|$, получаем

$$2 - \frac{2}{|\Delta|} = (1 - \frac{1}{|\Delta_1|}) + \cdots + (1 - \frac{1}{|\Delta_k|}). \tag{8}$$

Так как $|\Delta_i| \geq 2$ для всех i, то $1 - \frac{1}{|\Delta_i|} \geq \frac{1}{2}$. Поэтому из (8) получаем $2(1 - \frac{1}{|\Delta|}) \geq \frac{k}{2}$, т. е. $k \leq 4 - \frac{4}{|\Delta|} < 4$. Случай $k = 1$ невозможен, поскольку

$$2(1 - \frac{1}{|\Delta|}) > 1 > 1 - \frac{1}{|\Delta_1|}.$$

Следовательно, $k = 2, 3$.

Пусть $k = 2$ и

$$2(1 - \frac{1}{|\Delta|}) = 2 - \frac{1}{|\Delta_1|} - \frac{1}{|\Delta_2|}$$

или,

$$\frac{2}{|\Delta|} = \frac{1}{|\Delta_1|} + \frac{1}{|\Delta_2|}$$

При этом $|\Delta_1|, |\Delta_2| \leq |\Delta|$. Отсюда $|\Delta_1| = |\Delta_2| = |\Delta|$. Это означает, что X состоит из двух точек, соответствующих одной оси. Поэтому Δ – циклическая группа вращений вокруг одной оси. Порядок Δ равен 1, 2, 3, 4, 6.

Пусть $k = 3$. Тогда из (8) вытекает

$$1 + \frac{2}{|\Delta|} = \frac{1}{|\Delta_1|} + \frac{1}{|\Delta_2|} + \frac{1}{|\Delta_3|}. \tag{9}$$

Можно считать, что $2 \leq |\Delta_1| \leq |\Delta_2| \leq |\Delta_3|$. Если $|\Delta_1| \geq 3$, то в равенстве (9) правая часть меньше 1, а левая больше. Следовательно, $|\Delta_1| = 2$ и

$$\frac{1}{2} + \frac{2}{|\Delta|} = \frac{1}{|\Delta_2|} + \frac{1}{|\Delta_3|}.$$

Непосредственный перебор показывает, что возможны лишь следующие случаи:

(1) $|\Delta_2| = 2, \quad |\Delta_3| = \frac{|\Delta|}{2}$;
(2) $|\Delta_2| = 3, \quad |\Delta_3| = 3 \quad |\Delta| = 12$;
(3) $|\Delta_2| = 3, \quad |\Delta_3| = 4 \quad |\Delta| = 24$;
(4) $|\Delta_2| = 3, \quad |\Delta_3| = 5 \quad |\Delta| = 60$.

Отсюда вытекает

ТЕОРЕМА 3.19. *Пусть Δ – конечная подгруппа в $\mathrm{SO}(3, \mathbb{R})$. Тогда Δ одна из следующих групп:*

(1) *циклическая группа порядка 1, 2, 3, 4, 6;*
(2) *группа диэдра D_n, где $n = 1, 2, 3, 4, 6$;*
(3) *группа вращений тетраэдра $T \simeq A_4$, см. Рисунок 3.1;*
(4) *группа вращений окраэдра $O \simeq S_4$, см. Рисунок 3.1;*
(5) *группа вращений икосаэдра $I \simeq A_5$, см. Рисунок 3.1.*

Отметим, что указанные группы действительно реализуются как группы симметрий некоторых молекул, см. Рисунок 3.2. Так группой симметрий молекулы $H_3C - CCl_3$ является циклическая группа порядка 3, группой симметрий молекулы C_{26} является группа диэдра D_3, группой симметрий молекулы метана CH_4 является группа тетраэдра T, группой симметрий молекулы гексафорид урана UF_6 является группа октаэдра O.

Для завершения рассмотрения опишем точечные группы, состоящие не только из вращения.

ОБОЗНАЧЕНИЕ 3.20. Обозначим через j центральную симметрию в трехмерном пространстве, т. е. $j(x) = -x$ для всех векторов x.

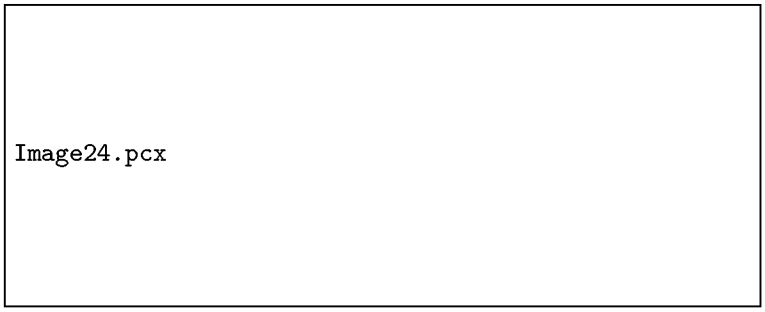

Рисунок 3.1

Рисунок 3.2

Упражнение 3.21. $j^2 = 1$ и $j \in \mathrm{O}(3,\mathbb{R}) \setminus \mathrm{SO}(3,\mathbb{R})$. Более того,

$$\mathrm{O}(3,\mathbb{R}) = \mathrm{SO}(3,\mathbb{R}) \times \langle j \rangle_2.$$

Предположим, что Δ – конечная подгруппа в $\mathrm{O}(3,\mathbb{R})$, не лежащая в $\mathrm{SO}(3,\mathbb{R})$. Тогда $A = \Delta \cap \mathrm{SO}(3,\mathbb{R})$ является подгруппой индекса 2 в Δ.

Предложение 3.22. *Если $j \in \Delta$, то $\Delta = A \times \langle j \rangle_2$.*

Предположим, что $j \notin \Delta$ и $\Delta \setminus A = jM$, где $M \subset \mathrm{SO}(3,\mathbb{R})$.

Предложение 3.23. *$AM = MA = M$, $M^2 = A^2 = A$. В частности, $G = A \cup M$ является подгруппой в $SO(3,\mathbb{R})$, причем A – подгруппа индекса 2 в G.*

Обозначение 3.24. Группа $\Delta = A \cup jM$ из предложения 3.23 обозначается через (G, A).

В силу теоремы 3.19 и предложения 3.23 справедлива

Теорема 3.25. *Пусть Δ – конечная подгруппа в $\mathrm{O}(3,\mathbb{R})$, не лежащая в $\mathrm{SO}(3,\mathbb{R})$. Тогда Δ – одна из следующих групп:*

(1) $\langle a \rangle_n \times \langle j \rangle_2$;
(2) $D_n \times \langle j \rangle_2$;
(3) $T \times \langle j \rangle_2$;
(4) $O \times \langle j \rangle_2$;
(5) $I \times \langle j \rangle_2$;
(6) $(\langle a \rangle_{2n}, \langle a^2 \rangle_n)$, $n = 2, 4, 6$;
(7) $(D_n, \langle a \rangle_n)$, $n = 2, 3, 6$;
(8) (D_{2n}, D_n), $n = 2, 3$;
(9) (O, T).

Всего 32 кристаллографических класса.

Имеются 72 различных неэквивалентных групп симметрий трехмерных решеток. Возможные многогранники, возникающие на репере f_1, f_2, f_3 указываются в Рисунок 3.3.

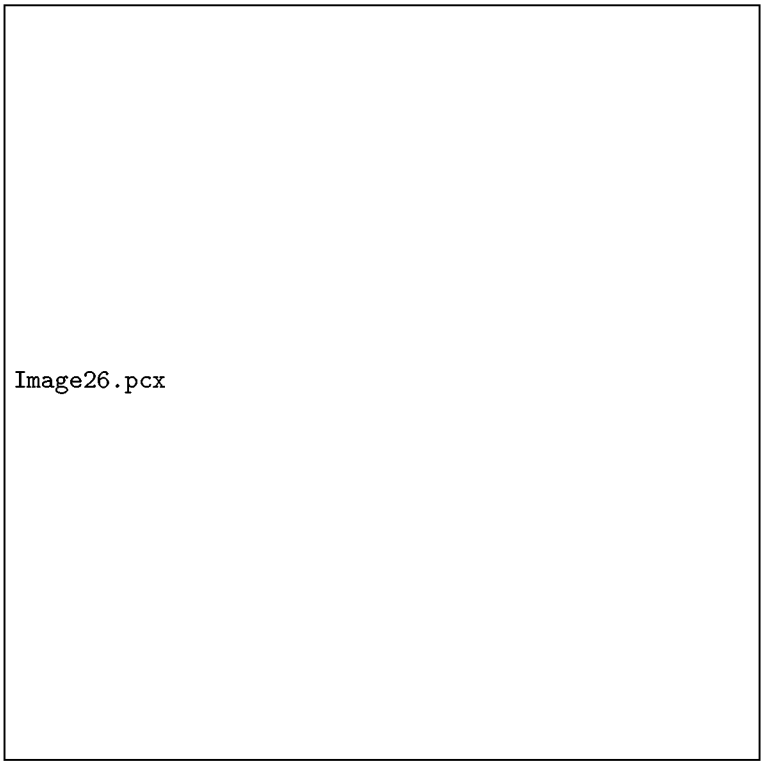

Рисунок 3.3

ГЛАВА 4

Элементы теории представлений групп

1. Основные понятия и примеры

Пусть V – векторное пространство над полем k. Через $\mathrm{GL}(V)$ обозначается множество всех обратимых линейных операторов на V, т. е. множество всех линейных операторов $\mathcal{A}$ в V, у которых есть такой (обратный) оператор $\mathcal{A}^{-1}$, что

$$\mathcal{A}\mathcal{A}^{-1} = \mathcal{A}^{-1}\mathcal{A} = \mathcal{E}.$$

Упражнение 4.1. $\mathrm{GL}(V)$ является группой относительно операции умножения операторов.

Определение 4.2. Пусть G – группа и V – векторное пространство над полем k. *Представлением* группы G в V называется гомоморфизм групп $\xi : G \to \mathrm{GL}(V)$.

Другими словами, каждому элементу $g \in G$ сопоставлен обратимый линейный оператор $\xi(g)$, причем $\xi(gh) = \xi(g)\xi(h)$ для всех $g, h \in G$. Если представление ξ фиксировано, то обычно действие оператора $\xi(g), g \in G$, на векторе $v \in V$ обозначается через gv. Тогда для всех $v, w \in V$ и $g, h \in G$ выполнены условия

$$g(\alpha v + \beta w) = \alpha(gv) + \beta(gw), \quad (gh)v = g(hv), \quad 1v = v. \tag{10}$$

Последние два равенства из (10) показывают, что группа G действует на множестве V.

Примеры 4.3. Укажем ряд представлений групп.

(1) Пусть $G = S_4$ и T – тетраэдр с вершинами, занумерованными числами 1,2,3,4. Предположим, что тетраэдр вложен в $\mathbb{R}^3$, причем его центр расположен в начале координат. Сопоставим каждой перестановке $\sigma \in S_4$ ортогональное преобразование $\mathbb{R}^3$, переводящее вершины 1,2,3,4 в $\sigma 1, \ldots, \sigma 4$. Такое преобразование существует, так как σ является произведением транспозиций, и для каждой транспозиции такое преобразование существует. Ясно, что возникает представление S_4.
(2) Группа S_n действует в $k[X_1, \ldots, X_n]$ с помощью перестановок переменных.
(3) Группы диэдра D_n и кватернионов Q_8 имеют естественное представление в $\mathbb{R}^2$ и в $\mathbb{C}^2$.

Определение 4.4. Пусть заданы два представления $\xi : G \to \mathrm{GL}(V), \phi : G \to \mathrm{GL}(W)$. Эти представления *эквивалентны (изоморфны)*, если существует такой изоморфизм векторных пространств $\zeta : V \to W$, что $\zeta[\xi(g)v] = \phi(g)[\zeta(v)]$ для всех $g \in V, v \in V$.

Переформулируем понятие представления и изоморфизм в матричных терминах. Пусть V – векторное пространство над полем k с базисом $\mathbf{e} = (e_1, \ldots, e_n)$. Если задано представление $\xi : G \to \mathrm{GL}(V)$, то каждому элементу $g \in G$ сопоставлена матрица $A_g = (a_{ij}(g)) \in \mathrm{GL}(n, k)$. Если $g, h \in G$, то $A_{gh} = A_g A_h$ и если $x = \sum_{i=1}^n x_i e_i \in V, x_i \in k$, то столбец из координат вектора $A_g x$ в базисе $\mathbf{e}$ равен

$$A_g \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Предположим, что $(f_1, \ldots, f_n)$ – базис пространства W, и $\zeta : V \to W$ – изоморфизм представления, причем

$$\zeta(e_i) = \sum_{j_1}^{n} f_j c_{ji}, \quad c_{ji} \in k, \quad i = 1, \ldots, n.$$

Положим $C = (c_{ji}) \in \mathrm{GL}(n, k)$, пусть при представлении $\phi : G \to \mathrm{GL}(W)$ элементу $g \in G$ соответствует матрица $B_g \in \mathrm{GL}(n, k)$. Тогда для любого $g \in G$ по определению 4.4 получаем

$$CA_g = B_g C \text{ или } B_g = CA_g C^{-1} \tag{11}$$

Теорема 4.5. *Каждое конечномерное представление конечной группы G над полем $\mathbb{R}$ (над $\mathbb{C}$) эквивалентно ортогональному (унитарному).*

Доказательство. Пусть задано представление $\psi : G \to \mathrm{GL}(V)$, где V – конечномерное вещественное пространство. В V существует структура евклидова пространства со скалярным произведением $(\ ,\ )$. Введем в V новое скалярное произведение

$$[x, y] = \frac{1}{|G|} \sum_{g \in G} (gx, gy).$$

Непосредственная проверка показывает, что $[\ ,\ ]$ является скалярным произведением, и $[gx, gy] = [x, y]$ для всех $x, y \in V$. □

Следствие 4.6. *Пусть $\psi : G \to \mathrm{GL}(V)$ – из теоремы 4.5. Если подпространство $U \subseteq V$ инвариантно относительно всех операторов $\psi(g), g \in G$, то $V = U \oplus W$, где подпространство W инвариантно относительно всех операторов $\psi(g), g \in G$.*

Следствие 4.7. *Пусть задан гомоморфизм $\psi : G \to \mathrm{GL}(n, \mathbb{R})$ конечной группы G, причем существует такое $1 < k < n$, что*

$$\psi(g) = \left(\begin{array}{c|c} B_g & C_g \\ \hline 0 & D_g \end{array}\right), \quad B_g \in \mathrm{GL}(k, \mathbb{R}), D_g \in \mathrm{GL}(n-k, \mathbb{R}), \quad C_g \in \mathrm{Mat}(k \times (n-k), \mathbb{R}),$$

для всех $g \in G$. Тогда существует такая матрица $F \in \mathrm{GL}(n, \mathbb{R})$, что

$$F \left(\begin{array}{c|c} B_g & C_g \\ \hline 0 & D_g \end{array}\right) F^{-1} = \left(\begin{array}{c|c} B'_g & 0 \\ \hline 0 & D'_g \end{array}\right), \quad B'_g \in \mathrm{GL}(k, \mathbb{R}), D'_g \in \mathrm{GL}(n-k, \mathbb{R}),$$

для всех $g \in G$.

Доказательство. Можно считать, что ψ ортогонально. Тогда $W = U^{\perp}$. □

2. Теорема Машке и ее приложения

Определение 4.8. *Подпредставление, прямая сумма* представлений, *неприводимое* представление, *вполне приводимое* представление.

Теорема 4.9. *Любое конечномерное вещественное представление конечной группы вполне приводимо.*

Доказательство. Индукция по размерности представления. □

Упражнение 4.10. Доказать, что

(1) естественные двумерные представления D_n, Q_8 неприводимы;
(2) представление S_4 из 4.3 неприводимо.

Теорема 4.11. *Все одномерные представления группы G сводятся к одномерным представлением G/G'.*

Доказательство. Нужно воспользоваться предложением 1.93. □

Теорема 4.12. *Любое неприводимое конечномерное комплексное абелевой группы одномерно.*

Доказательство. Пусть задано представление ψ абелевой группы G в пространстве V. Если $g \in G$, то оператор $\psi(g)$ имеет ненулевой собственный вектор с собственным значением λ_g. Следовательно, подпространство U в V, состоящее из нуля и всех собственных векторов для $\psi(g)$ с собственным значением λ_g отлично от нуля, причем в силу абелевости G оно инвариантно. Следовательно, $U = V$. Так как g – любой элемент из G, то для любых $g \in G, v \in V$ имеем $gv = \lambda_g v$. Отсюда вытекает утверждение. □

Следствие 4.13. *Описание неприводимых комплексных представлений конечных циклических и произвольных конечных групп.*

Предложение 4.14. *Пусть V – пространство размерности n над полем k нулевой характеристики с базисом $\mathbf{e} = (e_1, \ldots, e_n)$. Зададим представление S_n в V, полагая для $\sigma \in S_n$*

$$\sigma(e_i) = e_{\sigma i}, \quad i = 1, \ldots, n.$$

Пусть $U = k(e_1 + \cdots + e_m)$ и

$$W = \{x_1 e_1 + \cdots + x_n e_n | x_i \in k, \quad x_1 + \cdots + x_n = 0\}$$

Тогда U, W неприводимые подпредставления, причем $V = U \oplus W$.

Доказательство. Достаточно показать, что W неприводимо. Пусть $h = h_1 e_1 + \cdots + h_n e_n$ – ненулевой вектор из W. Переставляя e_i с помощью S_n можно считать, что $h_1 \neq 0$. Заметим, что случай $h_1 = h_2 = \cdots = h_n$ невозможен в силу нулевой характеристики поля. Переставляя $e_2, \ldots, e_n$ с помощью S_n можно считать, что $h_1 \neq h_2$. Тогда $h - (1,2)h = (h_1 - h_2)(e_1 - e_2)$. Следовательно, любое ненулевое инвариантное относительно S_n подпространство в W содержит вектор $(h_1 - h_2)^{-1}(h - (1,2)h) = e_1 - e_2$. Но тогда оно содержит и $(2,i)(e_1 - e_2) = e_1 - e_i$ для любого i. Поэтому это подпространство совпадает с W. □

ГЛАВА 5

Алгебры и поля

1. Кольца и алгебры

Определение 5.1. *Кольцо* (не обязательно ассоциативное). *Ассоциативные, коммутативные, антикоммутативные* кольца, *кольца Ли.*

Предложение 5.2. *В любом кольцо имеем* $0x = x0 = 0$.

Определение 5.3. *Поля, тела.*

Определение 5.4. *Алгебра* над полем (не обязательно ассоциативная). *Ассоциативные, коммутативные, антикоммутативные* алгебры, *алгебры Ли.*

Примеры 5.5. Укажем ряд алгебр.

- ♡ Ассоциативные алгебры – алгебры матриц $\mathrm{Mat}(n, k)$.
- ♡ Ассоциативно-коммутативные алгебры – алгебры многочленов $k[X_1, \ldots, X_n]$, алгебры рядов $k[[X]]$, алгебры непрерывных функций на топологическом пространстве.
- ♡ Если R – ассоциативная алгебра с 1, то алгебра матриц $\mathrm{Mat}(n, R)$ снова является ассоциативной алгеброй с 1.
- ♡ Алгебры Ли $A^{(-)}$ для ассоциативной алгебры A.

Определение 5.6. *Единичный* элемент, *делители нуля*, *обратимые* элементы алгебры. *Области, тела.*

Предложение 5.7. *Единичный элемент алгебры определен однозначно. Обратимые элементы ассоциативной алгебры образуют группу по умножению. Обратимый элемент ассоциативной алгебры не может быть делителем нуля.*

Следствие 5.8. *В теле и в поле нет делителей нуля.*

Примеры 5.9. Группы обратимых элементов в

(1) $k[X_1, \ldots, X_n]$ – это ненулевые константы;
(2) $k[[X]]$ – это ряды с ненулевым свободным членом;
(3) $\mathrm{Mat}(n, k)$ – это $\mathrm{GL}(n, k)$; делители нуля в $\mathrm{Mat}(n, k)$ – это вырожденные матрицы и только они.

Определение 5.10. Подалгебры, подалгебры с 1.

Предложение 5.11. *Пусть A – ассоциативная алгебры и $z \in A$. Положим*

$$k[z] = \{\sum a_i z_i | a_i \in k, \quad i \geq 0\}.$$

Тогда $k[z]$ – наименьшая подалгебра с 1 в A, содержащая z.

Определение 5.12. *Идеал* в кольце и в алгебре. Обозначение $I \triangleleft R$. Алгебра A *проста*, если в ней только два идеала A и 0.

Упражнение 5.13. Если идеал I кольца R с единицей содержит обратимый элемент, то $I = R$.

Следствие 5.14. *Любое тело просто.*

Предложение 5.15. *Пусть A – коммутативно-ассоциативная алгебра, и*

$$z_1, \dots, z_n \in A.$$

Тогда

$$(z_1, \dots, z_n) = \{\sum_{i=1}^{n} a_i z_i | a_i \in A\}$$

является идеалом в A.

Определение 5.16. Идеал

$$(z_1, \dots, z_n)$$

называется идеалом, *порожденным* множеством $z_1, \dots, z_n$. Идеал вида (z) в A называется *главным.*

Теорема 5.17. *Любой идеал в алгебра многочленов $k[X]$ является главным.*

Упражнение 5.18. Любой идеал в $\mathbb{Z}$ и в $\mathbb{Z}[i]$ является главным.

Теорема 5.19. *Пусть R – ассоциативная алгебра, и $A = \mathrm{Mat}(n, R)$. Предположим, что $I \lhd A$. Тогда существует и притом единственный такой идеал $J \lhd R$, что $I = \mathrm{Mat}(n, J)$.*

Доказательство. Положим

$$J = \{a \in R | aE_{11} \in I\}.$$

Пусть $X = (x_{ij}) \in I$, где $x_{ij} \in R$. Для любых $i, j = 1, \dots, n$ имеем

$$x_{ij}E_{11} = E_{1i}XE_{j1} \in I.$$

Следовательно, $x_{ij} \in J$, т. е. $I \subseteq \mathrm{Mat}(n, J)$.

Обратно, пусть $X = (x_{ij}) \in \mathrm{Mat}(n, J)$, т. е. $x_{ij} \in J$ для всех $i, j = 1, \dots, n$. В этом случае $x_{ij}E_{11} \in I$, откуда

$$X = \sum_{ij} x_{ij}E_{ij} = \sum_{ij} E_{i1}(x_{ij}E_{11})E_{1j} \in I.$$

□

Следствие 5.20. *Пусть D – тело. Тогда $\mathrm{Mat}(n, D)$ – простая алгебра.*

Определение 5.21. *Гомоморфизмы* колец и алгебр. *Изоморфизмы, автоморфизмы. Ядро* гомоморфизма $\ker \phi$.

Предложение 5.22. $\ker \phi$ *является идеалом кольца (алгебры).*

Следствие 5.23. *Пусть $\phi : k \to A$ – ненулевой гомоморфизм поля k в алгебре A. Тогда ϕ является мономорфизмом.*

Доказательство. Рассмотрим идеал $\ker \phi$. По следствию 5.14 либо $\ker \phi = k$, либо $\ker \phi = 0$. В первом случае $\phi = 0$, что противоречит предположению. Следовательно, $\ker \phi = 0$, и ϕ – мономорфизм по следствию 1.47. □

Следствие 5.24. *Пусть A – алгебра с единицей 1 над полем k. Тогда отображение $\phi : k \to A$, $\alpha \mapsto \alpha 1$ является вложением поля k в алгебру A.*

Определение 5.25. Пусть $I \lhd R$. Рассмотрим факторгруппу (относительно сложения) R/I. Для $a + I, b + I \in R/I$ и $\alpha \in k$ положим

$$(a + I)(b + I) = ab + I \in R/I, \quad \alpha(a + I) = \alpha a + I.$$

Получающаяся алгебра (кольцо) называется *факторалгеброй (факторкольцом)*

Предложение 5.26. *Определение факторалгебры (факторкольца) R/I корректно. Если R ассоциативно (коммутативно, кольцо или алгебра Ли), то этим же свойством обладает R/I.*

Доказательство. Пусть $a+I=a'+I, b+I=b'+I$. Тогда $a'=a+x, b'=b+y$, где $x,y\in I$. Поэтому

$$a'b'=ab+xb+ay+xy\in ab+I,$$

поскольку $xb+ay+xy\in I$ в силу определения идеала. Аналогично, если $\alpha\in k$, то

$$\alpha a'=\alpha a+\alpha x\in \alpha a+I.$$

Несложно проверяется и последнее утверждение. □

Определение 5.27. Рассмотрим гомоморфизм $\pi: R\to R/I$, $a\mapsto a+I$. Тогда π является гомоморфизмом колец (алгебр). Он называется *естественным* гомоморфизмом колец (алгебр).

Предложение 5.28. *Гомоморфизм $\pi: R\to R/I$ из определения 5.27 является гомоморфизмом колец (алгебр),* $\ker\pi=I$.

Теорема 5.29 (Теорема о гомоморфизмах). *Пусть $\phi: R\to R'$ – гомоморфизм колец (алгебр). Тогда* $\operatorname{Im}\phi\simeq R/\ker\phi$.

Доказательство. По теореме 1.50 отображение $\zeta: f(R)\to R/\ker\phi$, задаваемое по правилу

$$\zeta(\phi(x))=\phi^{-1}(\phi(x))=x+\ker\phi$$

является изоморфизмом аддитивных групп $\operatorname{Im}\phi$ и R/I. Остается показать, что $\zeta(ab)=\zeta(a)\zeta(b)$, и

$$\alpha\zeta(a)=\zeta(\alpha a) \tag{12}$$

для всех $a,b\in\operatorname{Im}\phi,\quad \alpha\in k$. Пусть $a=\phi(x),\quad b=\phi(y)$, где $x,y\in R$. Так как $\phi(x)\phi(y)=\phi(xy)$, то

$$\zeta(a)\zeta(b)=\phi^{-1}(\phi(x))\phi^{-1}(\phi(y))=\phi^{-1}\phi(xy)=\zeta(ab).$$

Аналогично проверяется (12). □

Примеры 5.30. Доказать, что

(1) $\mathbb{C}[X,Y]/(Y)\simeq\mathbb{C}[X]$;
(2) $\mathbb{R}[X]/(X^2+X+1)\simeq\mathbb{C}$.

В заключение этого раздела приведем важный пример простой алгебры. Напомним сначала, что для элементов x,y любой ассоциативной алгебре полагаем $[x,y]=xy-yx$.

Пусть $V=\mathbb{C}[X_1,\dots,X_n]$ – алгебра комплексных многочленов от $X_1,\dots,X_n$. Рассмотрим в V линейные операторы $p_1,\dots,p_n,q_1,\dots,q_n$, где для любого $f\in V$

$$p_i(f)=\frac{\partial f}{\partial X_i},\quad q_if=X_if. \tag{13}$$

Предложение 5.31. *Справедливы соотношения*

$$[p_i,p_j]=[q_i,q_j]=0,\quad [p_i,q_j]=\delta_{ij}$$

Доказательство. Достаточно проверить последнее соотношение. Если $f\in V$, то

$$[p_i,q_j]f=(p_iq_j-q_jp_i)f=\frac{\partial(X_jf)}{\partial X_i}-X_j\frac{\partial f}{\partial X_i}=$$
$$\frac{\partial X_j}{\partial X_i}f+X_j\frac{\partial f}{\partial X_i}-X_j\frac{\partial f}{\partial X_i}=\frac{\partial X_j}{\partial X_i}f=\delta_{ij}f. \tag{14}$$

□

Определение 5.32. *Алгеброй Вейля* $A_n(\mathbb{C})$ называется подалгебра с единицей в алгебре линейных операторов на V, порожденная всеми операторами p_i, q_j, $i,j = 1,\dots,n$.

В силу предложения 5.31 произвольный элемент из $A_n(\mathbb{C})$ является конечной линейной комбинацией одночленов

$$q_1^{m_1}\cdots q_n^{m_n}p_1^{s_1}\cdots p_n^{s_n}, \quad s_i, m_j \geq 0, \quad s_i, m_j \in \mathbb{Z}. \tag{15}$$

В частности, каждый элемент F из $A_n(\mathbb{C})$ можно представить в виде конечной суммы

$$F = \sum_i f_i(q_1,\dots,q_n)g_i(p_1,\dots,p_n). \tag{16}$$

Положим в этом случае

$$\frac{\partial F}{\partial p_j} = \textstyle\sum_i f_i(q_1,\dots,q_n)\dfrac{\partial g_i(p_1,\dots,p_n)}{\partial p_i};$$
$$\frac{\partial F}{\partial q_j} = \textstyle\sum_i \dfrac{\partial f_i(q_1,\dots,q_n)}{\partial q_j} g_i(p_1,\dots,p_n).$$

Предложение 5.33. *Если* $F \in A_n(\mathbb{C})$, *то для всех* $i = 1,\dots,n$

$$[p_i, F] = \frac{\partial F}{\partial q_i}, \quad [q_j, F] = -\frac{\partial F}{\partial p_j}.$$

Доказательство. Справедлива

Лемма 5.34. *В любой ассоциативной алгебре* A *выполнены равенства*

$$[x, yz] = [x,y]z + y[x,z], \quad [x,y] = -[y,x].$$

Доказательство. Непосредственное вычисление. □

Можно считать, что F является одночленом (15). В силу предложения 5.31 и леммы 5.34 получаем

$$[p_i, F] = q_1^{m_1}\cdots q_{i-1}^{m_{i-1}}[p_i, q_i^{m_i}]q_{i+1}^{m_{i+1}}\cdots q_n^{m_n}p_1^{s_1}\cdots p_n^{s_n}. \tag{17}$$

Остается показать, что

$$[p_i, q_i^m] = mq_i^{m-1}. \tag{18}$$

Если $m = 1$, то (18) вытекает из предложения 5.31. Пусть для m равенство (18) доказано. Тогда по лемме 5.34

$$[p_i, q_i^{m+1}] = [p_i, q_i]q_i^m + q_i[p_i, q_i^m] = q_i^m + q_i m q_i^{m-1} = (m+1)q_i^m.$$

□

Предложение 5.35. *Одночлены из* (15) *независимы.*

Доказательство. Пусть F – ненулевой элемент из (16). Представим F в виде $F = \sum_{i=0}^m u_i q_n^i$, где u_i – многочлены от $p_1,\dots,p_n,q_1,\dots,q_{n-1}$. По предложению 5.33 получаем, что

$$0 = [p_n, F] = \sum_{i=0}^m u_i i q_n^{i-1}.$$

Продолжая эти рассуждения, получаем в алгебре Вейля ненулевой многочлен сначала от $p_1,\dots,p_n,q_1,\dots,q_{n-1}$, и затем от $p_1,\dots,p_n$. Аналогично рассматривая $0 = [q_i, F]$ получаем противоречие. □

Теорема 5.36. *Алгебра* $A_n(\mathbb{C})$ *проста.*

Доказательство. Пусть $0 \neq I \lhd A_n(\mathbb{C})$. Предположим, что идеал I содержит ненулевой многочлен из доказательства предложения 5.35. Рассматривая $[p_i, F], [q_i, F] \in I$, как и в доказательстве предложения 5.35, получаем, что I содержит ненулевой элемент из поля $\mathbb{C}$. Этот элемент обратим в $A_n(\mathbb{C})$, и поэтому $I = A_n(\mathbb{C})$ в силу упражнения 5.13. □

2. Теорема Фробениуса

Опишем конечномерные тела над полем вещественных чисел.

Определение 5.37. Пусть $\mathbb{H}$ – множество всех комплексных матриц

$$z = \begin{pmatrix} a & -b \\ \overline{b} & \overline{a} \end{pmatrix} \tag{19}$$

Теорема 5.38. *$\mathbb{H}$ является подалгеброй в $\mathbb{R}$-алгебре всех комплексных матриц* $\mathrm{Mat}(2, \mathbb{C})$. *Более того, $\mathbb{H}$ является телом с центром $\mathbb{R}$.*

Доказательство. Для $z \in \mathbb{H}$ из (19) через $\|z\|$ обозначим $\sqrt{\det z} = \sqrt{|a|^2 + |b|^2}$. Тогда $\|z\| > 0$, если $z \neq 0$, $\|z_1 z_2\| = \|z_1\| \|z_2\|$.

Если z из (19), то положим

$$\overline{z} = \begin{pmatrix} \overline{a} & b \\ -\overline{b} & a \end{pmatrix}$$

Нетрудно видеть, что $z\overline{z} = \|z\|^2$. Таким образом, если $z \neq 0$, то $z^{-1} = \dfrac{\overline{z}}{\|z\|^2}$. Следовательно, $\mathbb{H}$ – тело. Оно некоммутативно, так как если

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \tag{20}$$

то $IJ = -JI$.

Найдем центр $\mathbb{H}$. Он состоит из всех матриц

$$w = \begin{pmatrix} u & -v \\ \overline{v} & \overline{u} \end{pmatrix},$$

что $wz = zw$ для всех матриц z из (19). Непосредственная проверка показывает, что $w = \lambda E$, $\lambda \in \mathbb{R}$. □

Упражнение 5.39. Доказать, что матрицы E, I, J, K, где I, J из (20) и

$$K = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix},$$

составляют базис $\mathbb{H}$ над $\mathbb{R}$, причем

$$IJ = K, \quad JK = I, \quad I^2 = J^2 = K^2 = -E.$$

Нам потребуется ряд утверждений.

Определение 5.40. Пусть A – ассоциативная k-алгебра с 1. Элемент $z \in A$ называется *алгебраическим* над k, если существует такой ненулевой многочлен $f \in k[X]$, что $f(z) = 0$. *Минимальным* многочленом алгебраического элемента z над k называется такой многочлен $f(X) \in k[X]$ минимальной степени со старшим коэффициентом 1, что $f(z) = 0$.

Упражнение 5.41. Пусть A – конечномерная ассоциативная алгебра над полем k с единицей. Доказать, что каждый элемент из A алгебраичен над k.

Упражнение 5.42. Доказать, что минимальный многочлен для заданного элемента определен однозначно.

Как показано в теореме 5.17 каждый идеал в алгебре многочленов $k[X]$ над полем k является главным.

Предложение 5.43. *Пусть $f \in k[X]$ имеет степень n. Тогда* $\dim_k (k[x]/(f)) = n$.

Доказательство. Убедимся, что элементы

$$1 + (f), X + (f), \ldots, X^{n-1} + (f) \tag{21}$$

составляют базис $k[x]/(f)$. □

Теорема 5.44. *Если k – поле, то $k[X]/(p)$ является полем тогда и только тогда, когда многочлен $p \in k[X]$ неприводим.*

Доказательство. Пусть $p = uv$, где $0 < \deg u, \deg v < n = \deg p$. По предложению 5.43 элементы $u + (p), v + (p) \neq 0$ в $k[X]/(p)$, но $(u + (p))(v + (p)) = 0$ в $k[X]/(p)$. Тогда в $k[X]/(p)$ имеются делители нуля, что противоречит следствию 5.8.

Обратно, если p – неприводим и $u \in k[X] \setminus (p)$, то $(u, p) = 1$. Следовательно, найдутся такие элементы $f, g \in k[X]$, что $1 = fu + gp$. Тогда $(u + (p))^{-1} = f + (p)$. □

Предложение 5.45. *Пусть A – область над полем k, и $z \in K$ – алгебраический элемент с минимальным многочленом $f(X)$. Тогда f неприводим. Положим*

$$k[z] = \{a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} | a_i \in k, n = \deg f\}.$$

Тогда $k[z]$ является подполем в K, содержащим k, и

$$k[z] \simeq k[X]/(f). \tag{22}$$

Предложение 5.46. *Пусть A конечномерное тело над $\mathbb{R}$, и $a \in A \setminus \mathbb{R}$. Тогда минимальный многочлен над a имеет степень два. Кроме того, $\mathbb{R}[a] \simeq \mathbb{C}$.*

Доказательство. Так как A конечномерно, все степени a зависимы. Следовательно, a алгебраично. Минимальный многочлен p для a неприводим и потому имеет степень не выше 2 в силу предложения 5.45. Так как $a \notin \mathbb{R}$, то степень p равна 2. Поэтому $a^2 + \alpha a + \beta = 0$, где $p = X^2 + \alpha X + \beta \in R[X]$. Положим

$$I = \frac{2a + \alpha}{\sqrt{4\beta - \alpha^2}}.$$

Тогда $I^2 = -1$, причем по предложению 5.45

$$\mathbb{R}[a] = \mathbb{R}[I] \simeq \mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}.$$

□

Теорема 5.47. *Пусть поле A является алгебраическим расширением поля $\mathbb{R}$. Тогда либо $A = \mathbb{R}$, либо $A = \mathbb{C}$.*

Доказательство. Заметим, что $A \supseteq \mathbb{R}1 = \mathbb{R}$. Можно считать, что $A \neq \mathbb{R}$. По предложению 5.46 $A \supseteq \mathbb{C}$. Итак, A является конечным расширением $\mathbb{C}$. Если $a \in A \setminus \mathbb{C}$, то минимальный многочлен $f \in \mathbb{C}[X]$ для a имеет комплексный корень λ. Отсюда $0 = f(a) = (a - \lambda)g(a)$, где $g \in \mathbb{C}[X]$. Так как в A нет делителей нуля, то $a - \lambda = 0$ и $a = \lambda \in \mathbb{C}$. □

Теорема 5.48 (Фробениус). *Пусть A – конечномерное тело над $\mathbb{R}$. Тогда A – одно из тел $\mathbb{R}, \mathbb{C}, \mathbb{H}$.*

Доказательство. Можно считать, что A не коммутативно. Как и в предыдущей теореме 5.47 $A \supseteq \mathbb{R}1 = \mathbb{R}$. Можно считать, что $A \neq \mathbb{R}$. По предложению 5.46 $A \supseteq \mathbb{C}$. Если $A = \mathbb{C}$, то теорема доказана. Пусть $A \neq \mathbb{C}$. В этом случае A является левым векторным пространством над $\mathbb{C}$. Рассмотрим в A линейный оператор $\mathcal{L}(x) = xi, \quad i \in \mathbb{C}$. Заметим, что $\mathcal{L}^4 = 1$. Поэтому получается комплексное конечномерное представление циклической группы G порядка 4. Следовательно, A разлагается в прямую сумму

$$A = A_1 \oplus A_{-1} \oplus A_i \oplus A_{-i}, \quad \text{где } A_j = \{x \in A | xi = jx\}.$$

Пусть $y \in A_1$. Тогда $yi = y$, откуда $y(i-1) = 0$, т. е. $y = 0$. Пусть $y \in A_{-1}$. Тогда $yi = -y$, откуда $y(i+1) = 0$, т. е. $y = 0$. Итак, $A_1 = A_{-1} = 0$, и

$$A = A_i \oplus A_{-i}, \quad \mathbb{C} \subseteq A_i.$$

Лемма 5.49. $A_i = \mathbb{C}$.

Доказательство. Пусть $a \in A_i$. Тогда $ai = ia$, т. е. поле $\mathbb{C}[a]$ является конечным расширением $\mathbb{C}$. По теореме 5.47 Получаем $A_i = \mathbb{C}$. □

Лемма 5.50. *Пусть* $y \in A_{\varepsilon i}, z \in A_{\tau i}$, *где* $\varepsilon, \tau = \pm 1$. *Тогда* $yz \in A_{\varepsilon\tau i}$.

Доказательство.

$$(yz)i = y(zi) = y(\tau ia) = \tau(yi)a = \tau\varepsilon i(ya).$$

□

Лемма 5.51. *Пусть* $y \in A_{\varepsilon i}$. *Тогда*

$$yA_{\varepsilon i} = A_i, \quad yA_{-\varepsilon i} = A_{-i}.$$

Доказательство. По лемме 5.50

$$yA_{\varepsilon i} \subseteq A_i, \quad yA_i \subseteq A_{\varepsilon i}.$$

Так как в A нет делителей нуля, то

$$\dim_{\mathbb{C}} A_{\varepsilon i} = \dim_{\mathbb{C}}(yA_{\varepsilon i}) \leq \dim_{\mathbb{C}} A_i = (yA_i) \leq \dim_{\mathbb{C}} A_{\varepsilon i}.$$

Отсюда следует утверждение. □

Следствие 5.52. $\dim_{\mathbb{C}} A_i = \dim_{\mathbb{C}} A_{-i} = 1$.

Завершим доказательство теоремы. Пусть $j \in A_{-i}$. По леммам 5.50, 5.49 $j^2 \in \mathbb{C}$. Тогда $ji = -ij$. По лемме 5.50 можно считать, что $j^2 = -1$. Положим $k = ij \in A_{-i}$. Тогда $ki = -ik$. Кроме того,

$$k^2 = ijij = i(-ij)j = -i^2j^2 = -1,$$

и

$$jk = j(ij) = (ji)j = -ij^2 = i, \quad kj = (ij)j = ij^2 = -i.$$

Итак, в силу следствия 5.52

$$A_i = \mathbb{C} = \mathbb{R}1 + \mathbb{R}i, \quad A_{-i} = \mathbb{C}j = \mathbb{R}j + \mathbb{R}k.$$

Отсюда $A \simeq \mathbb{H}$. □

3. Основы теории полей

Определение 5.53. *Подполя.*

Как показано в теореме 5.17 каждый идеал в алгебре многочленов $k[X]$ над полем k является главным. Пусть p – неприводимый многочлен из $k[X]$. Тогда $k[X]/(p)$ является полем.

Предложение 5.54. *Элемент* $x + (p) \in k[X]$ *является корнем* p *в поле* $k[X]/(p)$. *Минимальный элемент для* z *равен* p.

Определение 5.55. Пусть $f \in k[X]$. *Поле разложения* f – это такое расширение полей F/k, что

(1) в F многочлен f разлагается на линейные множители;
(2) в F нет меньшего подполя, содержащего k, в котором бы многочлен f разлагался на линейные множители.

ТЕОРЕМА 5.56. *Поле разложения F/k для заданного многочлена*

$$f \in k[X]$$

существует.

ДОКАЗАТЕЛЬСТВО. Индукция по степени $\deg f$. Разложим f в произведение неприводимых многочленов, и пусть p – неприводимый множитель f. Тогда в поле $K = k[X]/(p)$ многочлен p имеет корень $z = X + (p)$. Следовательно, в кольце $K[X]$ многочлен f представим в виде $f = g(X - z)$, где $g \in K[X]$ имеет степень $\deg f - 1$. По индукции для g существует поле разложения F/K. Остается заметить, что F/k – поле разложения для f. □

ТЕОРЕМА 5.57. *Пусть F_1/k и F_2/k – два поля для заданного многочлена $f \in k[X]$. Тогда существует такой изоморфизм полей $\phi : F_1 \to F_2$, что $\phi(x) = x$ для всех $x \in k$, т. е. ϕ является изоморфизмом k-алгебр.*

ДОКАЗАТЕЛЬСТВО. Индукция по степени $\deg f$. Разложим f в произведение неприводимых многочленов, и пусть p – неприводимый множитель f. Пусть $z_i \in F_i$ – корень p. По предложениям 5.54, 5.45 существует изоморфизм полей $\psi : k[z_1] \to k[z_2]$, тождественный на k. Без ограничения общности можно считать, что ψ тождественно, и $z_1 = z_2$. Нетрудно видеть, что F_i является полем разложения для $\dfrac{f}{X - z_1}$ – многочлена с коэффициентами из $k[z_i], i = 1, 2$. По индукции существует изоморфизм $F_1 \to F_2$, тождественный на $k[z_i]$. □

ОПРЕДЕЛЕНИЕ 5.58. *Характеристика* поля k – это порядок единицы в его аддитивной группе, если он отличен от нуля. В противном случае характеристика поля нулевая.

ПРЕДЛОЖЕНИЕ 5.59. *Если характеристика поля k равна $p > 0$, то k содержит поле вычетов $\mathbb{Z}/p\mathbb{Z}$. Если $\operatorname{char} k = 0$, то k содержит поле рациональных чисел $\mathbb{Q}$.*

4. Конечные поля

ПРЕДЛОЖЕНИЕ 5.60. *Пусть k – конечное поле. Тогда $\operatorname{char} k = p > 0$, и $|k| = p^n$.*

ПРЕДЛОЖЕНИЕ 5.61. *Пусть k – поле и $|k| = q$. Тогда $x^q = x$ для всех $x \in k$.*

ПРЕДЛОЖЕНИЕ 5.62. *Пусть k – поле характеристики $p > 0$. Если $x, y \in k$, то $(x + y)^p = x^p + y^p$.*

ПРЕДЛОЖЕНИЕ 5.63. *Пусть F – поле характеристики $p > 0$, в котором многочлен $f = X^q - X$ разлагается на линейные множители, где q – степень p. Тогда множество всех корней многочлена f является подполем в F, содержащим $\mathbb{Z}_p$. В частности, если F – поле разложения $f \in \mathbb{Z}_p[T]$, то F совпадает с множеством всех корней f.*

ДОКАЗАТЕЛЬСТВО. Пусть x, y – корни f, и $q = p^n$, то по предложению 5.62 $(x + y)^q = x^q + y^q = x + y$, т. е. $x + y$ является корнем f. Аналогично, $xy, x^{-1}, -x$ являются корнями f. Кроме того, по предложению 5.61 элементы из $\mathbb{Z}_p$ являются корнями f. □

ТЕОРЕМА 5.64. *Пусть q – степень простого числа p. Тогда существует и единственное поле порядка q. Оно обозначается $\mathbb{F}_q$. В частности, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.*

ДОКАЗАТЕЛЬСТВО. Пусть $k = \mathbb{Z}/pZ$ – поле вычетов характеристики p, и $f = T^q - T \in k[T]$. Пусть F – поле разложения f. По предложению 5.63 F/Z_p состоит из всех корней многочлена f. Остается показать, что у f нет кратных корней.

Пусть $c \in F$ – корень кратности $s > 1$ многочлена f. Тогда $f = T^q - T = (T - c)^s g(T)$, откуда

$$f' = qT^{q-1} - 1 = -1 = s(T - c)^{s-1} g(T) + (T - c)^s g(T)' = (T - c)^{s-1} h(T), \quad h(T) \in F[T],$$

что невозможно. Следовательно, $|F| = q$.

Итак, поле F разложения f – искомое. Его единственность вытекает из теоремы 5.57. □

Теорема 5.65. *Пусть k – поле и G – конечная подгруппа в k^*. Тогда группа G циклична.*

Доказательство. Пусть t – простой делитель порядка G и G_t – силовская t-подгруппа в G.

Лемма 5.66. *Группа G_t циклична.*

Доказательство. Пусть x – элемент наибольшего порядка t^s в G_t. Тогда G_t совпадает с множеством всех корней $X^{t^s} - 1$. □

Группа G разлагается в прямое произведение своих силовских циклических подгрупп G_t. Остается воспользоваться теоремой 1.118. □

Теорема 5.67. *Пусть p – простое число, и $q = p^n$. Тогда существует такой неприводимый многочлен $f \in \mathbb{F}_p[X]$ степени n, что $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(f)$.*

Доказательство. По теореме 5.65 группа k^* циклична с порождающим элементом a. В частности, $\mathbb{F}_p[a] = \mathbb{F}_q$. По предложению 5.45 получаем, что $\mathbb{F}_q = k[a] \simeq \mathbb{F}_p[X]/(f)$, где f – неприводимый многочлен из $\mathbb{F}_p[X]$. По предложению 5.43 степень f равна n. □

Теорема 5.68. *Группа автоморфизмов поля $\mathbb{F}_q$, где $q = p^n$ и p – характеристика поля $\mathbb{F}_1$, является циклической группой порядка n, порожденной элементом ϕ, где $\phi(x) = x^p$ для всех $x \in \mathbb{F}_q$.*

Доказательство. Пусть $\alpha \in \operatorname{Aut}\mathbb{F}_q$. Тогда α оставляет неподвижным элемент 1, и потому α тождественно на $\mathbb{Z}_p$. Пусть $\mathbb{F}_q = \mathbb{Z}_p[X]/(g)$, где $g \in \mathbb{Z}_p[X]$ – неприводимый многочлен степени n, корнем которого является элемент $a \in \mathbb{F}_q^*$, порождающий мультипликативную группу $\mathbb{F}_q^*$. Тогда g – минимальный многочлен для a. Следовательно,

$$0 = \alpha(g(a)) = g(\alpha(a)),$$

откуда $\alpha(a)$ – снова корень $g(a)$. Но число корней g в $\mathbb{F}_q$ не выше степени g, т. е. не больше n. Но α однозначно определяется своим значением на a. Следовательно, порядок $\operatorname{Aut}\mathbb{F}_q$ не больше n. Для доказательства теоремы достаточно проверить, что порядок ϕ равен n. Тогда $\operatorname{Aut}\mathbb{F}_q$ состоит из степеней ϕ.

Пусть $\phi^m = 1$, т, е. $x^{p^m} = x$ для всех $x \in \mathbb{F}_q$. Тогда каждый элемент F_q является корней $T^{p^m} - T$, что невозможно. □

5. Алгебры Ли

Определение 5.69. *Алгеброй Ли L* называется неассоциативная алгебра с умножением $[x, y]$, удовлетворяющая тождествам

$$[x, x] = [[x, y], z] + [[y, z], x] + [[z, x], y] = 0.$$

Пример 5.70. Алгебра $A^{(-)}$, алгебра $\mathbb{R}^3, [x, y] = x \times y$.

Упражнение 5.71. В алгебре Ли выполнено тождество антикоммутативности

$$[x, y] = -[y, x].$$

Определение 5.72. Пусть A – произвольная алгебра. Линейное оператор D на A называется *дифференцированием*, если $D(xy) = D(x)y + xD(y)$. Через $\operatorname{Der}(A)$ обозначается множество всех дифференцирований алгебры A.

Предложение 5.73. $\mathrm{Der}(A)$ *является подалгеброй Ли в алгебре Ли всех линейных операторов* $\mathfrak{L}(A)^{(-)}$ *на* A.

Упражнение 5.74. Пусть f – билинейная симметричная форма на n-мерном пространстве k^n, где k – поле. Через $o(n,f)$ – обозначается множество всех кососимметричных относительно f линейных операторов в k^n. т. е. множество всех таких линейных операторов $\mathcal{C}$ в k^n, что $f(\mathcal{C}x,y) = -f(x,\mathcal{C}y)$. Доказать, что $o(n,f)$ – подалгебра Ли в $\mathrm{Mat}(n,k)^{(-)}$.

Упражнение 5.75. Пусть f – полуторалинейная эрмитова форма на n-мерном комплексном пространстве $\mathbb{C}^n$. Через $su(n,f)$ обозначим множество всех кососимметричных относительно f линейных операторов в $\mathbb{C}^n$, т. е. множество всех таких линейных операторов $\mathcal{A}$ в $\mathbb{C}^n$, что $f(\mathcal{A}x,y) = -f(x,\mathcal{A}y)$. Доказать, что $su(n,f)$ – подалгебра Ли в $\mathrm{Mat}(2n,\mathbb{R})^{(-)}$.

Обозначение 5.76. Через $sl(n,k)$ обозначается множество всех матриц из $\mathrm{Mat}(n,k)$ со следом 0.

Упражнение 5.77. $sl(n,k)$ является подалгеброй Ли в $\mathrm{Mat}(n,k)^{(-)}$.

Предложение 5.78. *Пусть* k *– поле характеристики* $\neq 2$, *и*

$$H = E_{11} - E_{22}, \quad X = E_{12}, \quad Y = E_{21} \in \mathrm{Mat}(2,k).$$

Доказать, что

$$[X,Y] = H, \quad [H,X] = 2X, \quad [H,Y] = -2Y. \tag{23}$$

Теорема 5.79. *Алгебра* $sl(2,k)$ *проста, если* $\mathrm{char}\, k \neq 2$.

Доказательство. Пусть $0 \neq I \lhd sl(2,k)$, и

$$u = \alpha X + \beta Y + \gamma H \in I \setminus 0.$$

Тогда по (23)

$$[X,u] = \beta[X,Y] + \gamma[X,H] = \beta H - 2\gamma X \in I. \tag{24}$$

Кроме того,

$$[X,[X,u]] = \beta[H,X] = 2\beta X \in I.$$

Если $\beta \neq 0$, то $X \in I$, и тогда $I = sl(2,k)$ в силу (23).

Пусть $\beta = 0$. По (24) получаем, что $[X,u] = -2\gamma X \in I$. Если $\gamma \neq 0$, то $X \in I$, и поэтому $I = sl(2,k)$.

Пусть $\beta = \gamma = 0, quad\alpha \neq 0$. Тогда снова $X \in I$. □

Теорема 5.80. *Алгебра Ли* $(\mathbb{R}^3,\times)$ *проста.*

Доказательство. Убедимся сначала, что $(\mathbb{R}^3,\times)$ – алгебра Ли. Пусть e_1,e_2,e_3 – ортонормированный базис в $\mathbb{R}^3$. Тогда можно считать, что

$$[e_1,e_2] = e_3, \quad [e_2,e_3] = e_1, \quad [e_3,e_1] = e_2.$$

Непосредственная проверка показывает, что

$$[x,x] = J(e_1,e_2,e_3) = [[e_1,e_2],e_3] + [[e_2,e_3],e_1] + [[e_3,e_1],e_2] = 0.$$

Кроме того, Якобиан $J(x,y,z)$ кососимметричен. Отсюда выводится $(\mathbb{R}^3,\times)$ – алгебра Ли.

Пусть I – ненулевой идеал в $(\mathbb{R}^3,\times)$. Можно считать, что $e_1 \in I$. Тогда I содержит $e_3 = [e_1,e_2], e_2 = [e_3,e_1] \in I$. Следовательно, $I = (\mathbb{R}^3,\times)$. □

ГЛАВА 6

Линейные группы и их алгебры Ли

Всюду в этой работе под F понимается либо поле вещественных чисел $\mathbb{R}$, либо поле комплексных чисел $\mathbb{C}$.

1. Касательные пространства

Определение 6.1. Подгруппа G в полной линейной группе $\mathrm{GL}(n, F)$ называется *линейной*, если существует такая конечная система многочленов

$$f_s(X_{ij}) \in F[X_{ij} | 1 \leq i, j \leq n], \quad s = 1, \ldots, N, \tag{25}$$

что матрица $A = (a_{ij})$ принадлежит G тогда и только тогда, когда $f_s(a_{ij}) = 0$ для всех $s = 1, \ldots, N$.

Примеры 6.2. Подгруппы $\mathrm{O}(n, \mathbb{R})$, $\mathrm{SO}(n, \mathbb{R})$, $\mathrm{SL}(n, F)$ линейны.

Определение 6.3. Если G линейная группа, заданная системой уравнений (25), и $g \in G$, то *касательным пространством* T_g к G в точке g называется линейное пространство, состоящее из всех матриц $dX = (dx_{pq}) \in \mathrm{Mat}(n, F)$ с условием

$$\sum_{p,q} \frac{\partial f_i}{\partial x_{pq}}(g) dx_{pq} = 0, \quad i = 1, \ldots, r. \tag{26}$$

Рассмотрим пространство T_E для различных линейных групп.

Пример 6.4. Если $G = \mathrm{SL}(n, F)$, то G задается одним уравнением

$$f = \det X - 1 = 0.$$

Отсюда T_E задается одним уравнением

$$\frac{\partial f}{\partial x_{pq}} = \frac{\partial(\det X)}{\partial x_{pq}} = \frac{\partial(\sum_{i=1}^{n} A_{iq} x_{iq})}{\partial x_{pq}} = A_{pq}.$$

Таким образом,

$$\frac{\partial f}{\partial x_{pq}} = \delta_{pq},$$

откуда

$$\sum_{p.q} \frac{\partial f}{\partial x_{pq}} dx_{pq} = \sum_{p,q} \delta_{pq} dx_{pq} = \sum_{p} dx_{pp} = \mathrm{tr}(dX),$$

т. е. T_E задается уравнением $\mathrm{tr}(dX) = 0$.

Пример 6.5. Если $G = \mathrm{O}(n, \mathbb{R})$, то G задается одним уравнением ${}^t X \cdot X = E$. Это означает, что для $i, j = 1, \ldots, n$

$$\sum_{t=1}^{n} x_{ti} x_{tj} - \delta_{ij} = 0.$$

Таким образом,

$$\frac{\partial}{\partial x_{rs}}\left(\sum_{t=1}^{n} x_{ti}x_{tj} - \delta_{ij}\right) = \sum_{t=1}^{n}\left(\frac{\partial x_{ti}}{\partial x_{rs}}x_{tj} + x_{ti}\frac{\partial x_{tj}}{\partial x_{rs}}\right) = \sum_{t=1}^{n}(\delta_{tr}\delta_{is}x_{tj} + x_{ti}\delta_{tr}\delta_{js}).$$

Итак,

$$\frac{\partial}{\partial x_{rs}}\left(\sum_{t=1}^{n} x_{ti}x_{tj} - \delta_{ij}\right)|_E = \sum_{t=1}^{n}(\delta_{tr}\delta_{is}\delta_{tj} + \delta_{ti}\delta_{tr}\delta_{js}).$$

Отсюда вытекает, что T_E задается уравнениями

$$0 = \sum_{t,s,r=1}^{n}(\delta_{tr}\delta_{is}\delta_{tj} + \delta_{ti}\delta_{tr}\delta_{js})dx_{rs} = dx_{ji} + dx_{ij}.$$

Следовательно, T_E состоит из всех кососимметрических матриц $dX = (dx_{ij})$.

Зафиксируем элемент g линейной группы G. Отображение правого сдвига

$$R_g : G \to G, \quad x \mapsto xg,$$

является дифференцируемым отображением, поскольку умножение матриц задается линейными функциями от коэффициентов матрицы $x \in G$. Поэтому дифференциал dR_g этого отображения совпадает с матрицей g, т. е.

$$dR_g : T_x \to T_{xg}, \quad dR_g(dX) = (dX)g. \tag{27}$$

Но $R_{g_1g_2} = R_{g_1}R_{g_2}$. Следовательно, dR_g задает линейный изоморфизм T_E и T_g, т. е.

$$T_g = T_E g \tag{28}$$

для любого $g \in G$. В частности, справедливо

Предложение 6.6. $\dim T_E = \dim T_g$ *для любого* $g \in G$.

Определение 6.7. Пусть G – линейная группа. *Путем* из элемента E в элемент $g \in G$ называется такое дифференцируемое отображение $p : [0,1] \to G$, что $p(0) = E, p(1) = g$. *Связной компонентой* E в G называется множество всех элементов $g \in G$, обладающим путем из E в g. Группа G *связна*, если $G_E = G$.

Теорема 6.8. *Связная компонента* G_E *единичного элемента* E *является нормальной подгруппой в* G.

Доказательство. Пусть G_E – связная компонента E, и $g, h \in G_E$ с путями

$$x(t), y(t) : [0,1] \to G, \quad x(0) = y(0) = E, \quad x(1) = g, \quad y(1) = h.$$

Тогда $x(t)y(t)$ – дифференцируемый путь из E в gh. Кроме того, получаем дифференцированные пути

$$E \xrightarrow{x(t)^{-1}} X^{-1}, \qquad E \xrightarrow{Zx(t)Z^{-1}} ZXZ^{-1}.$$

□

Так как имеется локальная биекция G и T_E в окрестности E, то $T_E(G_E) = T_E(G)$.

Упражнение 6.9. Доказать, что

(1) G_E имеет конечный индекс в G;
(2) $\mathrm{O}(n, \mathbb{R})$ не связно, а $\mathrm{SO}(n, \mathbb{R})$ связно.

Упражнение 6.10. Будет ли группа $\mathrm{SL}(n, \mathbb{R})$ связна?

Предложение 6.11. *Пусть* $x : [0,1] \to G$ *– дифференцируемый путь в группе* G. *Если* $t_0 \in [0,1]$ *и* $g = x(t_0) \in G$, *то* $x'(t_0) \in T_g(G)$.

Доказательство. Пусть G задается системой алгебраических уравнений (25), и $x(t) = (x_{ij}(t))$. Тогда для любого $t \in [0,1]$

$$f_s(x_{ij}(t)) = 0, \quad i = 1, \dots, N.$$

Следовательно, используя правило дифференцирования сложной функции, для любого $s = 1, \dots, N$ получаем

$$\frac{\partial f_s}{\partial x_{pq}}(g) x'_{pq}(t_0) = 0.$$

Отсюда в силу определения 6.3 получаем требуемое утверждение. □

Теорема 6.12. *Пусть группа G связна. Тогда G определяется T_E.*

Доказательство. Пусть $X \in G$ и $x(t)$ – путь из E в X. Тогда

$$x(t)' \in T_{x(t)} = T_E x(t)$$

для всех $t \in [0,1]$ в силу (28). Итак,

$$x(t)' = A(t)x(t), \quad A(t) \in T_E \text{ для всех } t \in [0,1]. \tag{29}$$

Обратно, если $A \in T_E$, то рассмотрим дифференциальное уравнение (29), где $A(t) = A$ с начальным условием $x(0) = E$. Оно имеет и притом единственное решение.

Выберем в векторном пространстве $\mathrm{Mat}(n, F)$ такую новую систему координат $y_j, j = 1, \dots, n^2$, что T_E задается системой уравнений $y_i = 0$, где i пробегает первые d индексов. Тогда существует локальная биекция T_E и G. Поэтому решение (29) лежит в G.

Но это решение есть $\exp At$. Таким образом, $\exp : T_E \to G$ является локальной биекцией в окрестности U точки E. Так как отображение $x \mapsto x^{-1}$ непрерывно дифференцируемо, то можно считать, что $U^{-1} \subseteq U$. Обозначим через H множество всех произведений элементов из U. Если $x \in H$, то $xU \subseteq H$ является открытым подмножеством в G.

Пусть $G \setminus H$ непусто и $z \in G \setminus H$. Если $zU \cap H$ непусто, то $zu = u_1 \cdots u_t$, где $u, u_j \in U$. Отсюда $z = u_1 \cdots u_t u^{-1} \in H$, так как $u^{-1} \in U$. Следовательно, $zU \cap H$ пусто. Итак, G является объединением двух непересекающихся открытых подмножеств $G = H \cup (G \setminus H)$. Пусть $g \in G \setminus H$ и $x : [0,1] \to G$, где $x(o) = E, \quad x(1) = g$. Тогда отрезок $[0,1]$ является объединением двух непересекающихся открытых непустых подмножеств $x^{-1}(H), \quad x^{-1}(G \setminus H)$, что невозможно. □

Примеры 6.13. Рассмотрим экспоненциальное для ряда групп их порождающих элементов.

(1) Пусть $G = \mathrm{SL}(n, \mathbb{C})$. Тогда $T_E = sl(n, \mathbb{C})$. Базис $sl(n, \mathbb{C})$ составляют матрицы

$$E_{ij}, \quad 1 \le i \ne j \le n, \qquad E_{ii} - E_{jj}, \quad 1 \le i < j \le n.$$

При том

$$\exp(E_{ij}) = E + E_{ij}, \quad i \ne j,$$

$$\exp(E_{ii} - E_{jj}) = \mathrm{diag}(1, \dots, 1, \overset{i}{e}, 1, \dots, 1, \overset{j}{e}, 1 \dots, 1).$$

(2) Пусть $G = \mathrm{O}(2, \mathbb{R}), \quad T_E = o(2, \mathbb{R})$. Тогда

$$\exp \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} = \exp \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}^{-1} \begin{pmatrix} i\alpha & 0 \\ 0 & -i\alpha \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \right] =$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}^{-1} \begin{pmatrix} \exp(i\alpha) & 0 \\ 0 & \exp(-i\alpha) \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

2. Структура алгебры Ли на T_E

ТЕОРЕМА 6.14. *Пусть G – линейная группа, и $A, B \in T_E$. Тогда $[A, B] \in T_E$.*

ДОКАЗАТЕЛЬСТВО. Как и в доказательстве теоремы 6.12 $\exp(At), \exp(Bt) \in G$ для всех $t \in \mathbb{F}$. Следовательно,

$$[\exp(A\sqrt{t}), \exp(B\sqrt{t})] \in G \text{ для всех } t \in \mathbb{F}. \tag{30}$$

Вычислим касательный вектор к (30) в точке E. Имеем

$$\exp(A\sqrt{t}) = E + A\sqrt{t} + \frac{A^2 t}{2} + o(t);$$
$$\exp(B\sqrt{t}) = E + B\sqrt{t} + \frac{B^2 t}{2} + o(t);$$
$$\exp(A\sqrt{t})^{-1} = \exp(-A\sqrt{t}) = E - A\sqrt{t} + \frac{A^2 t}{2} + o(t);$$
$$\exp(B\sqrt{t})^{-1} = \exp(-B\sqrt{t}) = E - B\sqrt{t} + \frac{B^2 t}{2} + o(t);$$

Таким образом,

$$[\exp(A\sqrt{t}), \exp(B\sqrt{t})] = \exp(A\sqrt{t}) \exp(B\sqrt{t}) \exp(A\sqrt{t})^{-1} \exp(B\sqrt{t})^{-1} =$$
$$E + (A + B - A - B)\sqrt{t} +$$
$$\left(\frac{A^2}{2} + \frac{B^2}{2} + \frac{A^2}{2} + \frac{B^2}{2} + AB - A^2 - AB - BA - B^2 + AB\right) t + o(t) =$$
$$E + (AB - BA)t + o(t).$$

□

ОПРЕДЕЛЕНИЕ 6.15. Пусть

$$G_1 \subseteq \mathrm{GL}(n_1, F), \quad G_2 \subseteq \mathrm{GL}(n_2, F),$$

– линейные группы. Гомоморфизм групп $f : G_1 \to G_2$ называется *гомоморфизм линейных групп*, если существуют такие многочлены

$$f_{ij}(X_{rs}) \in F[X_{rs} | 1 \le r, s \le n_1], \quad 1 \le i, j \le n_2,$$

что для любого $g = (g_{rs}) \in G_1$ (i, j)-ый коэффициенты матрицы $f(g)$ равен $f_{ij}(g_{rs})$.

ТЕОРЕМА 6.16. *Если $f : G_1 \to G_2$ – гомоморфизм линейных групп, то $df\,|_E : T_E(G_1) \to T_E(G_2)$ является гомоморфизмом алгебр Ли.*

ДОКАЗАТЕЛЬСТВО. Пусть $A \in T_E(G_1)$. Тогда $df\,|_E\,(A) = J_E(f)A$, где $J_E(f)$ – значение Якобиана отображения f в точке E. Таким образом, отображение $df\,|_E$ линейно. Кроме того, $f(\exp(At)) = \exp(df\,|_E\,(A)t)$ для любого $t \in F$. Отсюда

$$f([\exp(A\sqrt{t}), \exp(B\sqrt{t})]) = [f(\exp(A\sqrt{t})), f(\exp(B\sqrt{t}))] =$$
$$[\exp(df\,|_E\,(A\sqrt{t})), \exp(df\,|_E\,(B\sqrt{t}))]. \tag{31}$$

Дифференцируя равенство (31) по t и полагая $t = 0$ получаем как и в доказательстве теоремы 6.14

$$df\,|_E\,([A, B]) = [df\,|_E\,(A), df\,|_E\,(B)].$$

□

СЛЕДСТВИЕ 6.17. *Пусть $f : G_1 \to G_2$ – гомоморфизм линейных групп, причем группа G_1 связна. Тогда $df\,|_E$ однозначно определяет f.*

ТЕОРЕМА 6.18. *Пусть A – конечномерная, не обязательно ассоциативная F-алгебра, G – группа ее автоморфизмов, и $\operatorname{Der} A$ – алгебра Ли ее дифференцирований. Тогда группа G линейна и $T_E = \operatorname{Der} A$ – ее алгебра Ли.*

ДОКАЗАТЕЛЬСТВО. Пусть $\mathbf{e} = (e_1, \dots, e_n)$ – произвольный базис в A. Тогда для любых $i, j = 1, \dots, n$

$$e_i e_j = \sum_{i,j,k=1}^{n} c_{ij}^k e_k, \quad c_{ij}^k \in F. \tag{32}$$

Если $\alpha \in G$ имеет в базисе $\mathbf{e}$ матрицу (a_{ij}), то

$$\alpha e_i = \sum_{k=1}^{n} e_k a_{ki}$$

Следовательно, для всех i, j

$$\begin{gathered}\alpha(e_i)\alpha(e_j) = \textstyle\sum_{t,s} e_s a_{si} e_t a_{tj} = \\ \textstyle\sum_{t,s} e_s e_t a_{si} a_{tj} = \sum_{t,s,k} c_{st}^k a_{si} a_{tj} e_k.\end{gathered} \tag{33}$$

С другой стороны,

$$\alpha(e_i e_j) = \sum_k c_{ij}^k \alpha(e_k) = \sum_{k,l} c_{ij}^k e_l a_{lk}.$$

Поэтому коэффициенты a_{ij} матрицы α удовлетворяют уравнениями

$$\sum_{k,l} c_{ij}^k e_l a_{lk} = \sum_{t,s,k} c_{st}^k a_{si} a_{tj},$$

и потому группа $G \subseteq \mathrm{GL}(n, F)$ линейна.

Найдем ее алгебру Ли. Элемент

$$D \in T_E \iff \exp(Dt) \in G = \operatorname{Aut} A \text{ для всех } t \in F.$$

Это означает, что для всех $a, b \in A$

$$\exp(Dt)(ab) = \exp(Dt)(a) \exp(Dt)(b).$$

Таким образом,

$$\begin{gathered}(E + \frac{Dt}{1!} + \frac{D^2t^2}{2!} + \cdots)(ab) = \\ (E + \frac{Dt}{1!} + \frac{D^2t^2}{2!} + \cdots)(a)(E + \frac{Dt}{1!} + \frac{D^2t^2}{2!} + \cdots)(b).\end{gathered} \tag{34}$$

Дифференцируя равенство (34) по t и полагая $t = 0$, получаем

$$D(ab) = D(a)b + aD(b).$$

Итак, $T_E \subseteq \operatorname{Der} A$.

Обратно, пусть $D \in \operatorname{Der} A$. Тогда $Dt \in \operatorname{Der} A$ для всех $t \in F$. Отсюда по формуле Лейбница

$$\exp(Dt)(ab) = (E + \frac{Dt}{1!} + \frac{D^2t^2}{2!} + \cdots)(ab) =$$
$$ab + (D(a)b + aD(b))t + \frac{1}{2!}(D^2(a)b + 2D(a)d(b) + aD^2(bt^n))t^2 + \cdots$$
$$+\frac{1}{n!}(\textstyle\sum_{i=0}^{n} \binom{n}{i} D^i(a)D^{n-i}(b)) + \cdots$$
$$(a + D(a)t + \frac{D^2(a)t^2}{2!} + \cdots)(b + D(b)t + \frac{D^2(b)t^2}{2!} + \cdots) =$$
$$\exp(Dt)(a)\exp(Dt)(b).$$

Итак, $\exp(Dt) \in G$. □

Рассмотрим подробнее свойства связных и несвязных групп Ли.

Теорема 6.19. *Группы*

$$\mathrm{SL}(n,\mathbb{C}), \quad \mathrm{GL}(n,\mathbb{C}), \quad \mathrm{SO}(n,\mathbb{R}), \quad \mathrm{U}(n,\mathbb{C}), \quad \mathrm{SU}(n,\mathbb{C})$$

связны. Группы $\mathrm{GL}(n,\mathbb{R}), \mathrm{O}(n,\mathbb{R})$ *несвязны.*

Теорема 6.20. *Любая компактная комплексная группа Ли изоморфна абелевой группе* $\mathbb{C}^n/\Gamma$, *где* Γ *– дискретная подгруппа ранга* $2n$ *в* $\mathbb{C}^n$.

Определение 6.21. Гомоморфизм групп Ли $f : G \to H$ называется *накрывающим*, если выполнено одно из эквивалентных условий:

(1) подгруппа $\ker f$ дискретна;
(2) $df : T_1(G) \to T_2(G)$ является изоморфизмом векторных пространств;
(3) f индуцирует диффеоморфизм окрестностей x и $f(x)$.

Пример 6.22. Гомоморфизм $f : \mathbb{R} \to \mathrm{U}(1,\mathbb{C})$, $f(x) = \exp(2\pi i)$. является накрытием.

Теорема 6.23. *Существует накрывающий гомоморфизм* $f : \mathrm{SL}(2,\mathbb{C}) \to \mathrm{SO}(3,\mathbb{C})$ *с ядром* $\ker f = \pm 1$. *При этом* $f(\mathrm{SU}(2,\mathbb{C})) = \mathrm{SO}(3,\mathbb{R})$.

Доказательство. Пусть $L = sl(2,\mathbb{C})$ – множество матриц со следом нуль, т. е.

$$sl(2,\mathbb{C}) = \{\begin{pmatrix} a & c \\ b & -a \end{pmatrix} | a,b,c \in \mathbb{C}\}.$$

Рассмотрим представление Ad группы $G = \mathrm{SL}(2,\mathbb{C})$ в L по правилу

$$(\operatorname{Ad} g)(x) = gxg^{-1}.$$

Заметим, что Ad сохраняет билинейную функцию

$$\begin{vmatrix} a & c \\ b & -a \end{vmatrix} = -a^2 - bc = (ia)^2 + \left[\frac{i(b-c)}{\sqrt{2}}\right]^2 + \left[\frac{i(b+c)}{\sqrt{2}}\right]^2.$$

Следовательно, $\operatorname{Ad} g \in \mathrm{SO}(3,\mathbb{C})$.

Ясно, что $\ker \operatorname{Ad} = \pm 1$. При этом $\operatorname{Im} \operatorname{Ad} = SO(3,\mathbb{C})$. □

Эта конструкция обобщается на произвольное $n \geq 2$. Именно, пусть C_n – алгебра Клиффорда от стандартной билинейной функции $(x,y) = \sum_{j=1}^{n} x_j y_j$ на n-мерном пространстве $\mathbb{C}^n$ со страндартным базисом $e_1, \ldots, e_n$. Тогда базис C_n составляют одночлены

$$e_{i_1} \cdots e_{i_m}, \quad 1 \leq i_1 < \ldots < i_m \leq n, \tag{35}$$

причем

$$e_k e_j = -e_j e_k, \text{ при } 1 \leq k \neq j \leq n, \quad e_j^2 = 1.$$

Поэтому $\dim C_n = 2^n$, и

$$C_n = C_n^0 \oplus C_n^1,$$

где базис C_n^k составляют одночлены (35), у которых $m \equiv k \mod 2$. В C_n имеется инволюция,

$$\overline{e_{i_1} \cdots e_{i_m}} = e_{i_m} \cdots e_{i_1}.$$

Положим $N(u) = u\overline{u}$ для любого $u \in C_n$.

Пусть C_n^* – группа обратимых элементов алгебры C_n. Через $\mathrm{Spin}(n, \mathbb{C})$ обозначим подгруппу всех таких

$$u \in (C_n^0)^*, \text{ что } N(u) = 1 \text{ и } u\mathbb{C}^n u^{-1} = \mathbb{C}^n, \tag{36}$$

где $\mathbb{C}^n$ – комплексная линейная оболочка векторов $e_1 \dots, e_n$.

Определение 6.24. Группа $\mathrm{Spin}(n, \mathbb{C})$ называется *комплексной спинорной группой.*

В силу (36) получается гомоморфизм

$$\pi : \mathrm{Spin}(n, \mathbb{C}) \to \mathrm{SO}(n, \mathbb{C}).$$

Можно показать, что гомоморфизм π сюръективен, и группа $\mathrm{Spin}(n, \mathbb{C})$ связна, $\ker \pi = \pm 1$.

Для описания элементов $\mathrm{Spin}(n, \mathbb{C})$ обозначим через Q^{n-1} все такие $y \in \mathbb{C}^n$, что $y = \sum y_j e_j$ и $\sum y_j^2 = 1$. В этом случае $y \in C_n^*$, и $\mathrm{Spin}(n, \mathbb{C})$ состоит из произведения четного числа элементов Q^{n-1}.

Пусть $n = 2l + 1$ – нечетно. Тогда алгебра

$$C_n^0 \simeq \mathrm{Mat}(2^l, \mathbb{C}).$$

Следовательно, в ней имеется простой левый идеал I размерности 2^l. Тем самым возникает неприводимое представление $\mathrm{Spin}(2l + 1, \mathbb{C})$, называется *спинорным представлением.*

Если $n = 2l$, то алгебра C_n проста, и поэтому имеется представление $\mathrm{Spin}(2l, \mathbb{C})$ в простом левом идеале J размерности 2^l. Снова возникает спинорное представление, но оно приводимо и разлагается в прямую сумму двух подпредставлений

$$J = (J \cap C_n^0) \oplus (J \cap C_n^1).$$

Определение 6.25. Группа Ли G *односвязна*, если в G любой путь стягивается в точку.

Теорема 6.26. *Любая связная группа Ли G имеет вид $G \simeq \tilde{G}/N$, где $\tilde{G}$ – односвязная группа Ли, и N – дискретный центральный нормальный делитель. Пара $\tilde{G}, N$ определена однозначно.*

Определение 6.27. Группа $\tilde{G}$ называется *односвязным накрытием G.*

Примеры 6.28. Следующие группы односвязны:

$$\mathrm{SL}(n, C), \quad \mathrm{SU}(n, \mathbb{C}), \quad \mathrm{Spin}(n, \mathbb{C}).$$

Имеются следующие односвязные накрытия:

(1) $\mathbb{R} \to \mathrm{U}(1, \mathbb{C})$;
(2) $\mathrm{SL}(2, \mathbb{C}) \to SO(3, \mathbb{C})$;
(3) $\mathrm{SU}(2, \mathbb{C}) \to SO(3, \mathbb{R})$;
(4) $\mathrm{SL}(2, \mathbb{C}) \times \mathrm{SL}(2, \mathbb{C}) \to \mathrm{SO}(4, \mathbb{C})$;
(5) $\mathrm{SL}(4, \mathbb{C}) \to \mathrm{SO}(6, \mathbb{C})$.

При этом в силу единственности накрытия

$$\mathrm{Spin}(3, \mathbb{C}) \simeq \mathrm{SL}(2, \mathbb{C}), \quad \mathrm{Spin}(4, \mathbb{C}) \simeq \mathrm{SL}(2, \mathbb{C}) \times \mathrm{SL}(2, \mathbb{C}),$$
$$\mathrm{Spin}(6, \mathbb{C}) \simeq SL(4, \mathbb{C}).$$

3. Представления групп Ли

Теорема 6.29. *Пусть G компактная группа Ли. Тогда на G существует и единственный такой интеграл $\int_G f(g)dg$ для каждой аналитической функции f на G, что он*

(1) *линеен относительно функции f;*
(2) $\int_G dg = 1$, $\int_G |f(g)|^2 dg > 0$, *если* $f \neq 0$;
(3) $\int_G f(g)dg = \int_G f(g^{-1})dg = \int_G f(gh)dg = \int_G f(hg)dg$, *если* $h \in G$.

Следствие 6.30. *Любое конечномерное представление компактной группы Ли вполне приводимо.*

Следствие 6.31. *Пусть задано представление $\phi : G \to \mathrm{GL}(V)$, где $\dim V < \infty$. В вводится скалярное произведение (x, y). Введем новое скалярное произведение*

$$\langle x, y\rangle = \int_G (\phi(g)x, \phi(g)y)dg.$$

В силу свойств интеграла каждый оператор $\phi(h), h \in G$, унитарен.

Теорема 6.32. *Любое неприводимое комплексное представление компактной группы Ли конечномерно.*

Теорема 6.33. *Группа всех унитарных матриц $\mathrm{U}(n, \mathbb{C})$ является максимальной компактной подгруппой в $\mathrm{GL}(n, \mathbb{C})$. Любая другая максимальная компактная подгруппа в $\mathrm{GL}(n, \mathbb{C})$ сопряжена с $\mathrm{U}(n, \mathbb{C})$. Группа всех ортогональных матриц $\mathrm{O}(n, \mathbb{R})$ является максимальной компактной подгруппой в $\mathrm{GL}(n, \mathbb{R})$. Любая другая максимальная компактная подгруппа в $\mathrm{GL}(n, \mathbb{R})$ сопряжена с $\mathrm{O}(n, \mathbb{R})$.*

Определение 6.34. Группа Ли *полупроста*, если в ней нет неединичных связных нормальных абелевых подгрупп.

Пример 6.35. Группы $\mathrm{SL}(n, \mathbb{C}), \mathrm{SU}(n, \mathbb{C}), \mathrm{SO}(3, \mathbb{R})$ полупросты.

Теорема 6.36. *Любая связная полупростая группа Ли допускает точное линейное представление.*

Определение 6.37. *Максимальным тором* в группе Ли G называется максимальная подгруппа Ли, являющаяся прямым произведением групп $\mathbb{C}^*$.

Примеры 6.38. Максимальный тор
в $\mathrm{GL}(n, \mathbb{C})$ – подгруппа диагональных матриц $D(n\mathbb{C})$,
в $\mathrm{SL}(n, \mathbb{C})$ – подгруппа диагональных матриц $D(n\mathbb{C}) \cap \mathrm{SL}(n, \mathbb{C})$,
в $\mathrm{SO}(n, \mathbb{C})$ – подгруппа диагональных матриц $D(n\mathbb{C}) \cap \mathrm{SO}(n, \mathbb{C})$.

Теорема 6.39. *В связной компактной группе Ли максимальный тор является максимальной связной коммутативной подгруппой Ли. Все такие подгруппы сопряжены.*

Определение 6.40. Максимальная связная разрешимая подгруппа Ли B^+ в группе Ли G называется *подгруппой Бореля.*

Заметим, что B^+ содержит максимальный тор H.

Теорема 6.41 (Морозов, Борель). *Все подгруппы Бореля B^+ связной комплексной группы Ли G сопряжены между собой в G.*

Примеры 6.42. Если $G = \mathrm{GL}(n, \mathbb{C})$, то $B^+ = T(n, \mathbb{C})$. Если G – одна из групп $\mathrm{SO}(n, \mathbb{C})$, $\mathrm{SL}(n, \mathbb{C})$, $\mathrm{SU}(n, \mathbb{C})$, то $B^+ = T(n, \mathbb{C}) \cap G$.

Определение 6.43. Пусть $\phi : G \to \mathrm{GL}(n, \mathbb{C})$ – комплексное представление группы Ли G. Для любого гомоморфизма $\chi : G \to \mathbb{C}^*$ через V_χ обозначим подпространство

$$V_\chi = \{v \in V | \phi(g)v = \chi(g)v \text{ для любого } g \in G\}.$$

Ненулевое подпространство V_χ называется *весовым*, ненулевые векторы из V_χ называются *весовыми*, а функция χ в этом случае называется *весом*.

Если H – максимальный тор в G, то H является компактной абелевой группой. Следовательно, все ее неприводимые представления одномерны. Поэтому если задано конечномерное представление $\phi : G \to GL(V)$ связной компактной группы Ли G с максимальным тором H, то

$$V = \oplus_{j=1}^{s} V_{\lambda_j}(H).$$

Определение 6.44. Весовой вектор $v \in V_j \setminus 0$ для H называется *старшим*, если для каждого элемента $g \in B^+$ найдется такое число $\chi_g \in \mathbb{C}$, что $\phi(g)v = \chi_g v$.

В частности, старший вес задает гомоморфизм $\chi : B^+ \to \mathbb{C}^*$.

Теорема 6.45. *Неприводимое конечномерное представление связной полупростой алгебраической группы G однозначно, с точностью до эквивалентности определяется своим старшим весом.*

Пример 6.46. Пусть $G = \mathrm{SL}(2, \mathbb{C})$. Тогда имеется естественное представление G в пространстве P_n однородных комплексных многочленов от X, Y степени n, именно,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ f(X, Y) = f(aX + bY, cX + dY).$$

Борелевская подгруппа B^+ состоит из всех верхнетреугольных матриц

$$B = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad a, d \in \mathbb{C}^*, \quad b \in \mathbb{C}.$$

Старший вектор этого представления – Y^n, так как $B \circ Y^n = a^{-n} Y^n$.

Легко видеть, что $-E$ действует при этом представлении тождественно, если n четно. Следовательно, при четном $n = 2k$ получается неприводимое представление

$$\mathrm{SO}(3, \mathbb{C}) \simeq \mathrm{SL}(2, \mathbb{C})/\{\pm E\}$$

степени $2k + 1$.

Пример 6.47. Пусть P_n как и выше. Заметим, что $\mathrm{SU}(2, \mathbb{C})$ состоит из всех матриц вида

$$\begin{pmatrix} a & -b \\ \overline{b} & \overline{a} \end{pmatrix}, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1.$$

Определим представление $\mathrm{SU}(2, \mathbb{C})$ в P_n как ограничение представления $\mathrm{SL}(2, \mathbb{C})$ из примера 6.46 на подгруппу $\mathrm{SU}(2, \mathbb{C})$. Получается неприводимое представление $\mathrm{SU}(2, \mathbb{C})$ со старшим вектором X^n. Действительно,

$$B^+ = \mathrm{SU}(2, \mathbb{C}) \cap T(2, \mathbb{C}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix} | a \in \mathbb{C}, \quad |a| = 1 \right\},$$

и поэтому

$$\begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix} \circ X^n = a^n X^n.$$

При четном $n = 2k$ получается неприводимое комплексное представление $\mathrm{SO}(3, \mathbb{R})$ степени $2k + 1$.

Представление из примера 6.47 можно описать по-другому. Пусть H_n – пространство всех однородных комплексных многочленов f степени n, удовлетворяющих дифференциальному уравнению

$$\Delta f = 0, \quad \Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}.$$

Действие $\mathrm{SO}(3, \mathbb{R})$ индуцировано естественным действием на координатах трехмерных векторов. Это представление имеет степень $2n + 1$ над $\mathbb{R}$, и оно эквивалентно представлению в P_n. Таким образом, получаются все неприводимые представления $\mathrm{SO}(3, \mathbb{R})$.