Н. Г. ЧЕБОТАРЁВ

ВВЕДЕНИЕ В ТЕОРИЮ АЛГЕБР

ОГИЗ
ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1949 ЛЕНИНГРАД

11-5-4

Редактор *А. Узков.* Техн. редактор *М. Д. Кислиновская.*

Подписано к печати 29/I 1949 г. 5,5 печ. л. 4,9 уч.-изд. л. 35 618 тип. зн. в печ. л. А-01585. Тираж 6 000 экз. Цена книги 3 руб. Заказ № 4380.

4-я типография им. Евг. Соколовой треста «Полиграфкнига» ОГИЗа при Совете Министров СССР, Ленинград, Измайловский пр., 29.

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ РЕДАКТОРА

Эта небольшая книжка издаётся по рукописи, оставшейся после безвременной кончины Николая Григорьевича Чеботарёва летом 1947 г.

Рукопись, по всей вероятности, должна была составить часть одной из глав давно задуманной Н. Г. Чеботарёвым третьей части его известной книги «Теория Галуа». Однако она представляет ценность и независимо от общего замысла книги, так как содержит достаточно законченный круг вопросов, а принятый автором способ изложения прельщает очень умеренными требованиями к первоначальной подготовке читателя: чтение почти всей книжки доступно уже при том небольшом знакомстве с теорией полей, которое предусмотрено программами первого курса университетов, и только заключительные параграфы требуют знания элементов теории Галуа. Эта особенность книжки, можно надеяться, будет сильно способствовать ознакомлению широких кругов математиков, не занимающихся алгеброй специально, с глубокой теорией гиперкомплексных систем, созданной в последние десятилетия.

К сожалению, из рукописи пришлось изъять теорию простых алгебр над p-адическими полями, так как её сохранение привело бы к необходимости коренной переработки начальной части рукописи.

А. Узков

§ 1. ОПРЕДЕЛЕНИЕ КОЛЬЦА

Совокупность некоторых объектов (элементов) называется *кольцом*, если относительно них соблюдаются следующие аксиомы:

1. Совокупность составляет абелеву группу относительно некоторой операции, которую мы будем называть (и обозначать) как *операцию сложения*.

II. Она составляет полугруппу (т. е. систему элементов, для которых определена операция с ассоциативным законом, но не обязательно с единицей и обратными элементами) относительно другой операции, которую мы будем называть (и обозначать) как *операцию умножения*.

III. Имеют место правый и левый дистрибутивные законы:

$$(a+b)\,c = ac + bc,$$
$$c\,(a+b) = ca + cb.$$

Кольцо называется *полем*, если выполнены следующие дополнительные требования:

1) Все элементы кроме нуля (т. е. единичного элемента группы по сложению) составляют группу относительно умножения.

2) Эта группа абелева.

Если выполняется только первое из этих требований, то совокупность называется *телом*.

В дальнейшем о всех рассматриваемых полях будет предполагаться, что они имеют характеристику нуль, т. е. что сложение любого числа единиц не можеть дать нуля.

§ 2. ОПРЕДЕЛЕНИЕ АЛГЕБРЫ

Пусть a произвольный элемент кольца A. Тогда в этом кольце будут также содержаться элементы

$$a + a = 2a = a2,$$
$$a + a + a = 3a = a3$$

и т. д., вообще элементы типа $na = an$, где n — целое рациональное число. Введём дополнительное предположение:

Кольцо A наряду с элементом a содержит также все элементы $\alpha \cdot a = a \cdot \alpha$, где α — произвольный элемент некоторого поля Ω. Кольца, удовлетворяющие этому предположению, мы будем называть *алгебрами* над полем Ω. Элементы поля Ω мы будем всегда считать перестановочными (относительно умножения) с элементами алгебры A.

Пусть в алгебре A содержится элемент a_1 и с ним все элементы $\alpha_1 a_1$, где α_1 пробегает поле Ω. Если алгебра A не исчерпывается элементами $\alpha_1 a_1$, то в ней найдётся элемент a_2, не представимый в форме $\alpha_1 a_1$. Тогда в A содержатся также элементы типа

$$\alpha_1 a_1 + \alpha_2 a_2, \tag{2.1}$$

где α_1, α_2 пробегают поле Ω. Различным α_1, α_2 соответствуют различные элементы алгебры A, так как из

$$\alpha_1 a_1 + \alpha_2 a_2 = \beta_1 a_1 + \beta_2 a_2$$

при $\alpha_1 \neq \beta_1$, $\alpha_2 \neq \beta_2$ мы получили бы

$$a_2 = \frac{\alpha_1 - \beta_1}{\beta_2 - \alpha_2} \cdot a_1,$$

что противоречило бы нашему предположению, что a_2 не представляется в форме $\alpha_1 \cdot a_1$.

Если элементами (2.1) алгебра A не исчерпывается, то в ней найдётся элемент a_3, не представимый в форме (2.1), а с ним элементы

$$\alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3,$$

где α_1, α_2, α_3 пробегают поле Ω, причём опять разным $\alpha_1, \alpha_2, \alpha_3$ соответствуют разные элементы алгебры A. Продолжая рассуждение, мы или исчерпаем всю алгебру A при помощи конечного числа элементов a_1, a_2, a_3, ... или не исчерпаем её, сколько бы ни находили элементов типа a_i. В первом случае будем называть алгебру A *алгеброй конечного порядка*, причём её *порядком* будем называть число n элементов $a_1, a_2, \ldots, a_n$ такого рода, что все элементы

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n \tag{2.2}$$

исчерпывают алгебру A и притом *независимы*, т. е. не допускают соотношений типа

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n = 0.$$

Совокупность элементов

$$[a_1, a_2, \ldots, a_n]$$

такого рода носит название *базиса* алгебры. Очевидно, что для каждой алгебры можно найти бесчисленное множество различных базисов; однако число n элементов, составляющих базис (т. е. порядок алгебры), останется одним и тем же. В самом деле, пусть $[a_1, a_2, \ldots, a_n]$ и $[b_1, b_2, \ldots, b_n]$ — базисы одной и той же алгебры A, причём пусть $m > n$. Выразим элементы b_i через первый базис:

$$\begin{aligned} b_1 &= \alpha_{11}a_1 + \alpha_{12}a_2 + \ldots + \alpha_{1n}a_n, \\ b_2 &= \alpha_{21}a_1 + \alpha_{22}a_2 + \ldots + \alpha_{2n}a_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ b_m &= \alpha_{m1}a_1 + \alpha_{m2}a_2 + \ldots + \alpha_{mn}a_n. \end{aligned} \tag{2.3}$$

Так как ранг матрицы

$$\left\| \begin{matrix} \alpha_{11}, & \alpha_{12}, & \ldots, & \alpha_{1n} \\ \alpha_{21}, & \alpha_{22}, & \ldots, & \alpha_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ \alpha_{m1}, & \alpha_{m2}, & \ldots, & \alpha_{mn} \end{matrix} \right\|$$

не превосходит n, т. е. меньше m, то найдутся отличные от нуля элементы $A_1, A_2, \ldots, A_m$ поля Ω, для которых будет иметь место

$$A_1\alpha_{1i} + A_2\alpha_{2i} + \ldots + A_m\alpha_{mi} = 0 \qquad (i = 1, 2, \ldots, n).$$

Умножая равенства (2.3) соответственно на $A_1, A_2, \ldots, A_m$ и складывая, мы получим

$$A_1 b_1 + A_2 b_2 + \ldots + A_m b_m = 0,$$

что противоречит независимости элементов второго базиса.

От одного базиса к другому всегда можно перейти при помощи линейной подстановки (2.3), где $m = n$ и определитель подстановки отличен от нуля. Обратно, всякая такая подстановка даёт новый базис. Таким образом, зная один базис алгебры A, мы без труда найдём её всевозможные базисы.

Если алгебра A содержит бесконечное число независимых элементов, то она называется *алгеброй бесконечного порядка*. Такого рода алгебрами мы не будем заниматься

в настоящем курсе. Говоря об алгебрах, мы будем разуметь алгебры конечного порядка, если не будем делать специальной оговорки.

От алгебр конечного порядка следует отличать *конечные* алгебры, состоящие из конечного числа элементов. Чтобы алгебра была конечной, необходимо, чтобы конечным было поле Ω. Если это условие соблюдается и если притом алгебра имеет конечный базис, то она должна быть конечной алгеброй.

§ 3. СТРУКТУРА АЛГЕБР

Пусть алгебра A задана базисом

$$[a_1, a_2, \ldots, a_n].$$

Чтобы полностью знать её свойства, мы должны уметь выражать в форме

(3.1) $$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n$$

всякий её элемент, получающийся в результате применения трёх первых арифметических действий над заданными элементами. Это мы будем знать, если будем иметь выражения для всех произведений $a_i a_j$ $(i, j = 1, 2, \ldots, n)$.
Пусть

(3.2) $$a_i a_j = \gamma_{ij}^1 a_1 + \gamma_{ij}^2 a_2 + \ldots + \gamma_{ij}^n a_n \qquad (i, j = 1, 2, \ldots, n),$$

или

(3.2′) $$a_i a_j = \sum_{\nu=1}^{n} \gamma_{ij}^{\nu} a_\nu. \qquad (i, j = 1, 2, \ldots, n).$$

Величины γ_{ij}^{ν} являются элементами поля Ω и называются *структурными константами* алгебры.

Пусть дано n^3 констант γ_{ij}^{ν} $(i, j, \nu = 1, 2, \ldots, n)$. Каким условиям они должны удовлетворять для того, чтобы составить систему структурных констант алгебры? Нетрудно убедиться, что при всякой системе таких констант все аксиомы для алгебр будут удовлетворены, за исключением того, что элементы алгебры составляют полугруппу относительно умножения (т. е. что для них имеет место ассоциативный закон). Таким образом для произвольных элементов a, b, c алгебры A должно иметь место

$$(ab)c = a(bc).$$

Выразим a, b, c через базис:

$$a = \sum_{i=1}^{n} \alpha^i a_i, \quad b = \sum_{j=1}^{n} \beta^j a_j, \quad c = \sum_{k=1}^{n} \gamma^k a_k,$$

и наша формула перепишется так:

$$\sum_{i,j,k=1}^{n} \alpha^i \beta^j \gamma^k (a_i a_j) a_k = \sum_{i,j,k=1}^{n} \alpha^i \beta^j \gamma^k a_i (a_j a_k).$$

Чтобы это равенство соблюдалось при всевозможных α^i, β^j, γ^k, необходимо и достаточно, чтобы имело место

$$(a_i a_j) a_k = a_i (a_j a_k).$$

Отсюда при помощи (3.2′) мы получим

$$\sum_{\nu=1}^{n} \gamma_{ij}^{\nu} a_\nu a_k = \sum_{\nu=1}^{n} a_i \gamma_{jk}^{\nu} a_\nu,$$

и далее

$$\sum_{\mu,\nu=1}^{n} \gamma_{ij}^{\nu} \gamma_{\nu k}^{\mu} a_\mu = \sum_{\mu,\nu=1}^{n} \gamma_{jk}^{\nu} \gamma_{i\nu}^{\mu} a_\mu.$$

Это соотношение в силу независимости элементов базиса даёт

$$\boxed{\sum_{\nu=1}^{n} \gamma_{ij}^{\nu} \gamma_{\nu k}^{\mu} = \sum_{\nu=1}^{n} \gamma_{jk}^{\nu} \gamma_{i\nu}^{\mu} \qquad (i, j, k, \mu = 1, 2, \ldots, n).} \tag{3.3}$$

Эти равенства являются необходимыми и достаточными условиями для того, чтобы константы γ_{ij}^{ν} составляли систему структурных констант алгебры.

Как будут меняться константы, если мы подвергнем базис линейному преобразованию? Пусть базисы $[a_1, a_2, \ldots, a_n]$ и $[b_1, b_2, \ldots, b_n]$ одной и той же алгебры A связаны линейной зависимостью

$$b_i = \sum_{\nu=1}^{n} \lambda_i^{\nu} a_\nu \qquad (i = 1, 2, \ldots, n), \tag{3.4}$$

определитель которой $|\lambda_i^{\nu}|$ отличен от нуля. Решая эту систему относительно a_i, получим

$$a_i = \sum_{\nu=1}^{n} \mu_i^{\nu} b_\nu \qquad (i = 1, 2, \ldots, n), \tag{3.5}$$

где между λ_i^ν и μ_i^ν имеют место зависимости

$$\sum_{\nu=1}^{n} \lambda_i^\nu \mu_\nu^j = \delta_i^j, \quad \sum_{\nu=1}^{n} \mu_i^\nu \lambda_\nu^j = \delta_i^j. \tag{3.6}$$

Здесь $\delta_i^i = 1$ и $\delta_i^j = 0$ при $i \neq j$. Подставляя в (3.2′), получим

$$\sum_{\alpha,\beta=1}^{n} \mu_i^\alpha \mu_j^\beta b_\alpha b_\beta = \sum_{s,\gamma=1}^{n} \gamma_{ij}^s \mu_s^\gamma b_\gamma.$$

Чтобы разрешить эту систему уравнений относительно b_α, b_β, умножим каждое из них на $\lambda_r^i \lambda_t^j$ и просуммируем по i и j. Тогда в силу (3.6) будем иметь

$$b_r b_t = \sum_{i,j,\gamma,s=1}^{n} \lambda_r^i \lambda_t^j \mu_s^\gamma \gamma_{ij}^s b_\gamma.$$

Если мы обозначим через $\overline{\gamma}_{rt}^\gamma$ структурные константы при новом базисе $[b_1, b_2, \ldots, b_n]$, то они выразятся через γ_{ij}^ν так:

$$\overline{\gamma}_{rt}^\gamma = \sum_{i,j,s=1}^{n} \gamma_{ij}^s \lambda_r^i \lambda_t^j \mu_s^\gamma. \tag{3.7}$$

Эти формулы показывают, что система структурных констант алгебры образует *тензор*, притом не произвольный, а удовлетворяющий соотношениям (3.3). Таким образом изучение свойств алгебры идёт параллельно с изучением свойств некоторого тензора третьего ранга.

В некоторых алгебрах существует элемент e, удовлетворяющий соотношениям

$$xe = ex = x$$

при всяком x из A. Элемент e носит название *главной единицы* алгебры A.

§ 4. ПРИМЕРЫ АЛГЕБР

1. Кватернионы. Это — исторически первый пример алгебр, предложенный свыше 100 лет тому назад Гамильтоном. Кватернионами называются элементы вида

$$\alpha + \beta i + \gamma j + \delta k, \tag{4.1}$$

где α, β, γ принадлежат некоторому полю Ω вещественных

чисел, а 1, i, j, k — система независимых элементов, составляющих базис алгебры (1 — главная единица) и удовлетворяющих уравнению

$$x^2+1=0 \qquad (x=i, j, k). \tag{4.2}$$

Таблица умножения для i, j, k такова:

$$\begin{aligned} &ij=k, \qquad jk=i, \qquad ki=j,\\ &ji=-k, \quad kj=-i, \quad ik=-j. \end{aligned} \tag{4.3}$$

Из этой таблицы видно, что умножение для кватернионов не коммутативно.

Покажем, что в случае вещественного поля Ω алгебра кватернионов есть тело, т. е. что для каждого кватерниона существует обратный элемент, дающий при умножении на данный кватернион главную единицу 1. Для этого введём понятие кватерниона, *сопряжённого* с кватернионом (4.1):

$$\alpha-\beta i-\gamma j-\delta k.$$

Нетрудно проверить, что произведение сопряжённых кватернионов равно $\alpha^2+\beta^2+\gamma^2+\delta^2$:

$$\begin{aligned} (\alpha+\beta i+\gamma j+\delta k)(\alpha-\beta i-\gamma j-\delta k)&=\\ =\alpha^2+\beta^2+\gamma^2+\delta^2.& \end{aligned} \tag{4.4}$$

Отсюда следует, что для каждого кватерниона (4.1) обратным ему является

$$\frac{\alpha-\beta i-\gamma j-\delta k}{\alpha^2+\beta^2+\gamma^2+\delta^2}.$$

В самом деле, знаменатель $\alpha^2+\beta^2+\gamma^2+\delta^2$ может в силу вещественности поля Ω быть равен нулю только при $\alpha=\beta=\gamma=\delta=0$.

II. Нулевая алгебра. Так называется алгебра, элементы базиса которой $a_1, a_2, \ldots, a_n$ (а с ними и все элементы алгебры) удовлетворяют соотношениям

$$a_i a_j=0 \quad (i, j=1, 2, \ldots, n). \tag{4.5}$$

III. Алгебра Грассмана. Пусть нам задано n элементов $e_1, e_2, \ldots, e_n$, удовлетворяющих соотношениям

$$e_i e_j=-e_j e_i, \quad e_i^2=0 \qquad (i, j=1, 2, \ldots, n). \tag{4.6}$$

Совокупность всевозможных произведений из $k \leqslant n$ различных e_i (если в произведение войдёт хоть одна единица два раза, то оно в силу (4.6) обратится в нуль) примем за базис алгебры, состоящий из

$$1 + C_n^1 + C_n^2 + \ldots + C_n^{n-1} + 1 = 2^n$$

членов. Отметим, что всякие две линейные комбинации элементов $e_1, e_2, \ldots, e_n$

$$a = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n, \quad b = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n$$

удовлетворяют условиям (4.6):

$$ab = -ba, \quad a^2 = 0.$$

При помощи алгебры Грассмана очень легко построить теорию определителей. Пусть нам даны n линейных форм:

(4.7) $a_i = \alpha_{1i} e_1 + \alpha_{2i} e_2 + \ldots + \alpha_{ni} e_n \quad (i = 1, 2, \ldots, n).$

Их произведение после раскрытия скобок будет содержать или нулевые члены или члены с $e_1 e_2 \ldots e_n$. Поэтому мы имеем право написать

(4.8) $$a_1 a_2 \ldots a_n = \Delta e_1 e_2 \ldots e_n.$$

Коэффициент Δ, зависящий от коэффициентов наших форм, мы будем называть *определителем* системы этих форм и записывать более подробно так:

(4.9) $$\Delta = \begin{vmatrix} \alpha_{11}, & \alpha_{12}, \ldots, & \alpha_{1n} \\ \alpha_{21}, & \alpha_{22}, \ldots, & \alpha_{2n} \\ \cdots & \cdots & \cdots \\ \alpha_{n1}, & \alpha_{n2}, \ldots, & \alpha_{nn} \end{vmatrix}.$$

Выведем из этого определения основные свойства определителей. Труднее всего здесь доказать неизменность определителя от замены строк столбцами. Для этого введём вторую систему элементов $f_1, f_2, \ldots, f_n$, каждый из которых пусть будет перестановочен с элементами e_i и удовлетворяет таким же соотношениям, как (4.6):

$$f_i f_j = -f_j f_i, \quad f_i^2 = 0 \qquad (i, j = 1, 2, \ldots, n).$$

Наряду с (4.7) введём обозначения

(4.10) $b_i = \alpha_{i1} f_1 + \alpha_{i2} f_2 + \ldots + \alpha_{in} f_n \qquad (i = 1, 2, \ldots, n).$

Умножая каждую из формул (4.7) на f_i и суммируя по i, получим в силу (4.10)

$$b_1 e_1 + b_2 e_2 + \ldots + b_n e_n = a_1 f_1 + a_2 f_2 + \ldots + a_n f_n.$$

Отметим, что произведения $b_i e_i$ перестановочны между собой и также произведения $a_i f_i$. Поэтому, возводя это равенство в n-ю степень, получим

$$(4.11)\quad n!\, b_1 b_2 \ldots b_n\; e_1 e_2 \ldots e_n = n!\; a_1 a_2 \ldots a_n\; f_1 f_2 \ldots f_n.$$

Вводя аналогично (4.8) обозначение

$$(4.12)\qquad b_1 b_2 \ldots b_n = \Delta_1 f_1 f_2 \ldots f_n,$$

где

$$(4.13)\qquad \Delta_1 = \begin{vmatrix} \alpha_{11}, & \alpha_{21}, \ldots, & \alpha_{n1} \\ \alpha_{12}, & \alpha_{22}, \ldots, & \alpha_{n2} \\ \cdots & \cdots & \cdots \\ \alpha_{1n}, & \alpha_{2n}, \ldots, & \alpha_{nn} \end{vmatrix}$$

и подставляя в (4.11) формулы (4.8) и (4.12), мы после сокращения будем иметь

$$\Delta_1 = \Delta$$

ч. и т. д.

Прибавление к строке определителя другой строки проводится в силу очевидного равенства

$$a_1 \ldots a_i \ldots a_j \ldots a_n = a_1 \ldots (a_i + \lambda a_j) \ldots a_j \ldots a_n.$$

Изменение знака при перестановке строк вытекает сразу из изменения знака при перестановке множителей в левой части формулы (4.8).

Для получения формулы Лапласа достаточно разбить произведение $a_1 a_2 \ldots a_n$ на два множителя и в каждом раскрыть скобки. Коэффициентом при каждом произведении единиц e_i будет минор. Беря произведение обоих множителей, получим выражение для определителя в виде суммы произведений миноров.

Для вывода теоремы об умножении определителей введём обозначения

$$a_i = \alpha_{1i} e_1 + \alpha_{2i} e_2 + \ldots + \alpha_{ni} e_n,$$
$$c_i = \beta_{1i} a_1 + \beta_{2i} a_2 + \ldots + \beta_{ni} a_n.$$

Так как элементы a_i подчиняются тем же законам, что и e_i, то имеет место

$$c_1 \cdot c_2 \ldots c_n = |\beta_{ij}| \cdot a_1 a_2 \ldots a_n,$$

откуда

$$c_1 \cdot c_2 \ldots c_n = |\beta_{ij}| \cdot |\alpha_{ij}| \cdot e_1 e_2 \ldots e_n.$$

Но, с другой стороны,

$$c_i = \sum_j \beta_{ji} \sum_\nu \alpha_{\nu j} e_\nu = \sum_\nu \gamma_{\nu i} e_\nu,$$

где

$$\gamma_{\nu i} = \sum_j \alpha_{\nu j} \beta_{ji},$$

откуда

$$c_1 \cdot c_2 \ldots c_n = |\gamma_{ij}| \cdot e_1 \cdot e_2 \ldots e_n,$$

т. е.

$$|\gamma_{ij}| = |\alpha_{ij}| \cdot |\beta_{ij}|,$$

ч. и т. д.

Для вывода формул Крамера умножим каждое из уравнений системы

$$\alpha_{i1} x_1 + \alpha_{i2} x_2 + \ldots + \alpha_{in} x_n = \beta_i$$

на e_i и просуммируем по i. Получим

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n + b, \tag{4.14}$$

где

$$b = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n.$$

Для получения выражения для x_i умножим (4.14) слева на $a_1 a_2 \ldots a_{i-1}$ и справа на $a_{i+1} \ldots a_n$. В левой части все члены, кроме i-го, обратятся в нуль, и мы получим

$$a_1 \ldots a_{i-1} a_i a_{i+1} \ldots a_n x_i = a_1 \ldots a_{i-1} b a_{i+1} \ldots a_n,$$

откуда нетрудно получить формулу Крамера.

IV. Полная матричная алгебра. Обозначая через e_{ij} матрицу n-го порядка, у которой на пересечении i-й строки и j-й колонны стоит единица, а на остальных местах нули, мы легко получим следующие соотношения:

$$e_{ij} e_{jk} = e_{ik}, \quad e_{ij} e_{ek} = 0 \ (j \neq e). \tag{4.15}$$

Рассмотрим алгебру, базис которой состоит из n^2 элементов

$$e_{ij} \qquad (i, j = 1, 2, \ldots, n),$$

для которых таблицей умножения служит (4.15). Нетрудно проверить для этой алгебры ассоциативный закон. Эта алгебра носит название *полной матричной алгебры*, так как произвольную матрицу n-го измерения $\|a_{ik}\|$ можно записать в виде

$$\|\alpha_{ik}\| = \sum_{i,\,k} \alpha_{ik} e_{ik}.$$

Нетрудно убедиться, что действия над элементами этой алгебры совпадают с обычными действиями над матрицами. Главной единицей в этой алгебре является

$$e_{11}+e_{22}+\ldots+e_{nn}.$$

V. Групповое кольцо. Пусть $s_1, s_2, \ldots, s_n$ — элементы некоторой конечной группы $\mathfrak{G}$. Возьмём какое-нибудь поле Ω и станем рассматривать выражения вида

$$\xi_1 s_1+\xi_2 s_2+\ldots+\xi_n s_n,$$

где ξ_i принимают всевозможные значения в поле Ω. Будем производить действия над такого рода элементами, считая элементы поля Ω перестановочными с s_i, для которых таблица умножения определяется структурой конечной группы:

$$s_i s_j = s_k.$$

Получается алгебра порядка n, называемая *групповым кольцом*. В ней главной единицей является единица группы.

УПРАЖНЕНИЯ

1) Чтобы система кватернионов над полем Ω (необязательно вещественным) образовала косое поле, необходимо и достаточно, чтобы неопределённое уравнение

$$x^2+y^2+u^2+v^2=0$$

не допускало внутри поля Ω решений, отличных от

$$x=y=u=v=0.$$

2) Всякая алгебра порядка 2 с главной единицей коммутативна.

3) Показать, что линейная система, составленная из матриц

$$\begin{Vmatrix}1&0\\0&1\end{Vmatrix},\quad \begin{Vmatrix}0&1\\-1&0\end{Vmatrix},\quad \begin{Vmatrix}-i&0\\0&1\end{Vmatrix},\quad \begin{Vmatrix}0&i\\i&0\end{Vmatrix},$$

есть алгебра. Составив для неё таблицу умножения, показать, что она изоморфна с алгеброй кватернионов.

§ 5. ПОДАЛГЕБРЫ

Если часть B элементов алгебры A сама составляет алгебру, то она называется подалгеброй алгебры A. Этот факт обозначается так:

$$B \subset A.$$

Порядок подалгебры B, если она не совпадает со всей алгеброй A, всегда меньше порядка алгебры A. Из способа нахо-

ждения элементов базиса (см. § 2) следует, что можно выбрать базис алгебры A так, чтобы часть его составляла базис подалгебры B. Для этого нужно взять базис $[b_1, b_2, \ldots, b_m]$ алгебры B и дополнить его независимыми элементами алгебры A, не выражающимися через этот базис.

Пусть $[b_1, b_2, \ldots, b_m; a_{m+1}, \ldots, a_n]$ есть базис алгебры A, в котором первые m элементов составляют базис подалгебры B. Выразим аналитически (т. е. через структурные константы) этот факт. То, что $[b_1, b_2, \ldots, b_m]$ составляет алгебру, выражается в том, что произведения $b_i b_j$ выражаются через одни b_i, т. е. что в выражениях

$$b_i b_j = \gamma_{ij}^1 b_1 + \ldots + \gamma_{ij}^m b_m + \gamma_{ij}^{m+1} a_{m+1} + \ldots + \gamma_{ij}^n a_n$$

константы

$$\gamma_{ij}^{m+1}, \ \gamma_{ij}^{m+2}, \ \ldots, \ \gamma_{ij}^n \qquad (i, j = 1, 2, \ldots, m)$$

равны нулю.

Введём понятие *линейной системы* в алгебре A, заданной базисом $[c_1, c_2, \ldots, c_k]$. Так называется совокупность элементов

$$\xi_1 c_1 + \xi_2 c_2 + \ldots + \xi_k c_k,$$

где $\xi_1, \xi_2, \ldots, \xi_k$ пробегают всевозможные элементы поля Ω. В частности, если произведения $c_i c_j$ линейно выражаются через c_i, линейная система составляет подалгебру.

Будем называть *произведением* линейных систем B и C, имеющих базисами $[b_1, b_2, \ldots, b_m]$ и $[c_1, c_2, \ldots, c_k]$, линейную систему, имеющую базисом

$$[\ldots b_i c_j \ldots] \qquad (i = 1, 2, \ldots, m; \ j = 1, 2, \ldots, k).$$

Другими словами, это — совокупность элементов bc, где b пробегает все элементы из B, c — все элементы из C.

Пользуясь этой символикой, мы можем записать условие того, чтобы линейная система B была подалгеброй, в таком виде:

(5.1) $$B.B \subset B, \quad \text{или} \quad B^2 \subset B.$$

Если подалгебра B обладает тем свойством, что элементы из B, умножаемые справа (слева) на элементы из A, дают опять элементы из B:

(5.2) $$BA \subset B \quad (AB \subset B),$$

то она называется *правым* (*левым*) *идеалом* алгебры A. Если же соблюдаются оба условия, то B называется *двусторонним идеалом*.

Аналитически условия того, что B есть идеал, легко вывести подобно предыдущему. Именно, условие для правого идеала B имеет вид

$$\gamma_{ij}^{\nu} = 0 \quad (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n;\ \nu = m+1, \ldots, n);$$

для левого идеала B

$$\gamma_{ij}^{\nu} = 0 \quad (i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, m;\ \nu = m+1, \ldots, n);$$

наконец, для двустороннего идеала B необходимо и достаточно соблюдение обоих этих условий.

Введём в рассмотрение одну весьма важную для дальнейшего подалгебру, называемую *центром* алгебры A. Так называется совокупность элементов алгебры A, перестановочных со всеми элементами алгебры A. Нетрудно видеть, что центр составляет алгебру. В самом деле, если при произвольном x из A имеет место

$$xa = ax, \quad xb = bx,$$

то также имеет место

$$x(a \pm b) = (a \pm b)x, \quad xab = abx, \quad xba = bax.$$

Из определения поля Ω следует, что Ω содержится в центре алгебры A. Центр, вообще говоря, не является идеалом.

Для нахождения центра положим

$$x = \xi_1 a_1 + \xi_2 a_2 + \ldots + \xi_n a_n, \quad \xi_i \subset \Omega$$

и решим систему линейных уравнений

$$\xi_1 (a_1 a_i - a_i a_1) + \xi_2 (a_2 a_i - a_i a_2) + \ldots + \xi_n (a_n a_i - a_i a_n) = 0 \quad (i = 1, 2, \ldots, n),$$

вытекающих из условий

$$xa_i = a_i x \qquad (i = 1, 2, \ldots, n).$$

Выражая произведения $a_j a_i$ при помощи формул (3.2) линейно через базис, получим систему однородных линейных уравнений

$$\sum_{\nu} \xi_\nu (\gamma_{\nu i}^{j} - \gamma_{i\nu}^{j}) = 0 \qquad (i, j = 1, 2, \ldots, n).$$

Если эта система имеет отличные от нуля решения $(\xi_1, \xi_2, \ldots, \xi_n)$, то каждое из таких решений определяет элемент центра

$$\xi_1 a_1 + \xi_2 a_2 + \ldots + \xi_n a_n.$$

УПРАЖНЕНИЯ

1) В нулевой алгебре любые независимые элементы составляют базис некоторой подалгебры, которая является двусторонним идеалом.

2) Порядок тела делится на порядок всякой своей подалгебры.

3) Все подалгебры алгебры кватернионов коммутативны.

4) Центром алгебры кватернионов является $\Omega \cdot e$, где e — её главная единица.

5) То же имеет место для полной матричной алгебры.

6) Центром группового кольца $[1, s_2, \ldots, s_m]$ является алгебра с базисом $[1, \sum s_i', \sum s_i'', \ldots]$, где суммы распространены на сопряжённые друг с другом элементы.

§ 6. ПРЕДСТАВЛЕНИЕ АЛГЕБР МАТРИЦАМИ

Покажем, что всякой алгебре соответствует *изоморфная* ей *алгебра матриц*, т. е. подалгебра полной матричной алгебры, описанной в § 4 (пример IV). Предварительно напомним понятия изоморфизма и гомоморфизма. Пусть нам даны две алгебры A и $\mathfrak{A}$ и пусть элементы обеих можно привести в такое взаимно однозначное соответствие:

$$a \longleftrightarrow \mathfrak{a},$$

причём из

$$a \longleftrightarrow \mathfrak{a}, \quad b \longleftrightarrow \mathfrak{b} \tag{6.1}$$

следует

$$a \pm b \longleftrightarrow \mathfrak{a} \pm \mathfrak{b}, \quad a \cdot b \longleftrightarrow \mathfrak{a} \cdot \mathfrak{b}, \tag{6.2}$$

то такое соответствие носит название *изоморфизма*, а алгебры A и $\mathfrak{A}$ *изоморфными* друг с другом.

Если при установленном соответствии (6.1) условия (6.2) выполняются, но соответствие не взаимно однозначное, то оно носит название *гомоморфизма*. Пусть над алгебрами A и $\mathfrak{A}$ установлено такого рода соответствие, причём каждому элементу алгебры A соответствует один единственный элемент алгебры $\mathfrak{A}$, но не обратно. Пусть, например, элементам a, b алгебры A соответствует один и тот же элемент $\mathfrak{a}$ алгебры $\mathfrak{A}$. Тогда в силу (6.2)

$$a - b \to 0,$$

т. е. не равным нулю элементам из A соответствует 0 в $\mathfrak{A}$. Обозначим через C совокупность элементов алгебры A, которым соответствует 0 в алгебре $\mathfrak{A}$. Нетрудно видеть, что C составляет алгебру. В самом деле, из

$$c_1 \to 0, \quad c_2 \to 0$$

следует

$$c_1 \pm c_2 \to 0, \quad c_1 \cdot c_2 \to 0,$$

т. е. из

$$c_1 \subset C, \quad c_2 \subset C$$

следует

$$c_1 \pm c_2 \subset C, \quad c_1 \cdot c_2 \subset C.$$

Более того, C составляет двусторонний идеал алгебры A. В самом деле, из

$$x \to \xi, \quad c \to 0$$

следует

$$xc \to 0, \quad cx \to 0,$$

т. е. при произвольном $x \subset A$ из

$$c \subset C$$

следует

$$xc \subset C, \quad cx \subset C.$$

Разобьём элементы алгебры A на *классы* по модулю двустороннего идеала C, говоря, что элементы a, b лежат в одном классе, если их разность $a - b$ лежит в C, и записывая это так:

$$a \equiv b \pmod{C}.$$

Такого рода сравнения мы, подобно обычным сравнениям, можем складывать, вычитать и перемножать, можем также умножать их справа или слева на произвольный элемент алгебры в силу того, что C есть двусторонний идеал.

Если мы формально приравняем друг другу все элементы алгебры A, лежащие в одном и том же классе по модулю C, то получим новую алгебру, которую называют *факторалгеброй* и обозначают так:

$$A/C.$$

Нетрудно убедиться, что порядок факторалгебры A/C равен разности $n - m$, где n — порядок алгебры A, а m — порядок алгебры C. В самом деле, если $[c_1, c_2, \ldots, c_m]$ есть базис

алгебры C, то обозначим через $[d_1, d_2, \ldots, d_r]$ базис алгебры A/C, т. е. систему независимых элементов алгебры A, между которыми не имеет места сравнение вида

$$\alpha_1 d_1 + \alpha_2 d_2 + \ldots + \alpha_r d_r \equiv 0 \pmod{C},$$

в то время как для всякого элемента алгебры A можно найти представление

$$a \equiv \beta_1 d_1 + \beta_2 d_2 + \ldots + \beta_r d_r \pmod{C}.$$

Тогда $[c_1, c_2, \ldots, c_m; d_1, d_2, \ldots, d_r]$ составит базис алгебры A, откуда и следует утверждение.

Приступим к построению алгебры матриц, изоморфной с данной алгеброй A. Чтобы найти матрицу n-го порядка, соответствующую элементу a алгебры A, выразим линейно через её базис $[a_1, a_2, \ldots, a_n]$ все произведения $a_1 a$, $a_2 a$, $\ldots$, $a_n a$. Пусть

$$a_i a = \alpha_{i1} a_1 + \alpha_{i2} a_2 + \ldots + \alpha_{in} a_n \qquad (i = 1, 2, \ldots, n).$$

Тогда сопоставим с элементом a матрицу

$$\| \alpha_{ij} \|.$$

Проверим гомоморфизм такого сопоставления. Пусть так же

$$a_i b = \beta_{i1} a_1 + \beta_{i2} a_2 + \ldots + \beta_{in} a_n.$$

Тогда

$$a_i (a \pm b) = (\alpha_{i1} \pm \beta_{i1}) a_1 + (\alpha_{i2} \pm \beta_{i2}) a_2 + \ldots + (\alpha_{in} \pm \beta_{in}) a_n,$$

$$a_i ab = \sum_{\nu} \alpha_{i\nu} a_\nu b = \sum_{\nu, \mu} \alpha_{i\nu} \beta_{\nu\mu} a_\mu = \sum_{\mu} \gamma_{i\mu} a_\mu,$$

где

$$\gamma_{i\mu} = \sum_{\nu} \alpha_{i\nu} \beta_{\nu\mu}.$$

Таким образом из

$$a \to \| \alpha_{ij} \|, \quad b \to \| \beta_{ij} \|$$

следует

$$a \pm b \to \| \alpha_{ij} \| \pm \| \beta_{ij} \|, \quad ab \to \| \alpha_{ij} \| \cdot \| \beta_{ij} \|,$$

а эти формулы как раз устанавливают гомоморфизм соответствия.

При таком сопоставлении изоморфизм не всегда имеет место. Например, для нулевой алгебры (см. § 4, пример II) каждому элементу соответствует нулевая матрица. Однако

изоморфизм имеет место в том важном случае, когда алгебра A содержит главную единицу. Беря её в качестве одного из элементов базиса, например a_1, мы для всякого элемента $a \neq 0$

$$a = \xi_1 a_1 + \xi_2 a_2 + \ldots + \xi_n a_n,$$

где не все $\xi_i = 0$, будем иметь

$$aa_1 = \xi_1 a_1 + \xi_2 a_2 + \ldots + \xi_n a_n,$$

а это показывает, что элементу a соответствует матрица, у которой первая строка такова:

$$\xi_1, \ \xi_2, \ \ldots, \ \xi_n,$$

т. е. не равна нулю. Таким образом ни одному не равному нулю элементу не может соответствовать нулевая матрица.

Если алгебра A не содержит главной единицы, то можно представить её как подалгебру другой алгебры $\overline{A}$ порядка $n+1$, если к элементам её базиса присоединить главную единицу a_0. Для полученной таким образом алгебры $\overline{A}$ надо проверить ассоциативный закон относительно умножения. Эту проверку достаточно произвести для элементов базиса, притом только для того случая, если среди них имеется a_0. Но для a_0 он сразу следует из соотношений

$$a_0 a_i = a_i a_0 = a_i \qquad (i = 1, \ 2, \ \ldots, \ n).$$

Таким образом алгебра $\overline{A} = [a_0, \ a_1, \ \ldots, \ a_n]$ содержит главную единицу, а потому для неё существует изоморфная с ней алгебра матриц $(n+1)$-го порядка. Беря в этой алгебре часть, соответствующую подалгебре A, получим и для A изоморфную с ней алгебру матриц $(n+1)$-го порядка.

Пример. Возьмём нулевую алгебру $A = [a_1, a_2, \ldots, a_n]$, где $a_i a_j = 0$. Рассмотрим алгебру $\overline{A} = [a_0, \ a_1, \ \ldots, \ a_n]$, где a_0 — главная единица. Имеет место

$$a_i a_0 = a_i, \quad a_i a_1 = 0, \ \ldots, \quad a_i a_n = 0,$$

откуда следует, что элементу a_i соответствует матрица e_{0i}.

Иногда алгебры допускают представление матрицами меньшего порядка. Это имеет место в том случае, если алгебра A имеет правый идеал. Пусть

$$[b_1 b_2, \ \ldots, \ b_m] \tag{6.3}$$

есть базис правого идеала B алгебры A. Чтобы представить элемент a алгебры A матрицей m-го порядка, умножим все

элементы b_i справа на a. В силу свойства правого идеала произведения $b_i \cdot a$ содержатся в B и потому выражаются через базис (6.3):

$$(6.4)\qquad \begin{cases} b_1 a = \alpha_{11} b_1 + \alpha_{12} b_2 + \ldots + \alpha_{1m} b_m, \\ b_2 a = \alpha_{21} b_1 + \alpha_{22} b_2 + \ldots + \alpha_{2m} b_m, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_m a = \alpha_{m1} b_1 + \alpha_{m2} b_2 + \ldots + \alpha_{mm} b_m. \end{cases}$$

Сопоставляя элементу a матрицу $\|\alpha_{ij}\|$, мы получим, вообще говоря, гомоморфное представление алгебры A матрицами m-го порядка.

Как изменится матрица A, сопоставленная с элементом a, если мы подвергнем базис линейному обратимому преобразованию S?

Пусть

$$S = \|\sigma_{ij}\|, \quad S^{-1} = \|\tau_{ij}\|,$$

где

$$\sum_\nu \sigma_{i\nu}\tau_{\nu j} = \delta_{ij}, \quad \sum_\nu \tau_{i\nu}\sigma_{\nu j} = \delta_{ij}.$$

Пусть далее $[b_1, b_2, \ldots, b_m]$ преобразуется в $[\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_m]$, где

$$(6.5)\qquad b_i = \sum_\nu \sigma_{i\nu}\bar{b}_\nu, \quad \bar{b}_i = \sum_\nu \tau_{i\nu} b_\nu.$$

Формулы (6.4) можно переписать так:

$$(6.4')\qquad b_i a = \sum_\mu \alpha_{i\mu} b_\mu,$$

или, подставляя (6.5):

$$\sum_\nu \sigma_{i\nu}\bar{b}_\nu a = \sum_\nu \left(\sum_\mu \alpha_{i\mu}\sigma_{\mu\nu}\right)\bar{b}_\nu,$$

где матрицей правой части служит произведение AS. Умножая каждую из этих формул на τ_{ki} и суммируя по i, получим:

$$(6.6)\qquad \bar{B}_k a = \sum_\nu \left(\sum_{i,\mu} \tau_{ki}\alpha_{i\mu}\sigma_{\mu\nu}\right)\bar{b}_\nu.$$

Из этих формул следует, что если при базисе $[b_1, b_2, \ldots, b_m]$ элементу a соответствовала матрица A, то при базисе $[\bar{b}_1, \ldots, \bar{b}_m]$ ему будет соответствовать матрица $S^{-1}AS$.

Такого рода преобразования, которые мы в дальнейшем будем часто проделывать, упрощаются благодаря особой символической записи. Станем рассматривать базис как матрицу из одной колонны:

$$\mathfrak{B} = \left\| \begin{matrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{matrix} \right\|.$$

Тогда формулы (6.5) можно в матричном исчислении переписать так:

$$\mathfrak{B} = S\overline{\mathfrak{B}}, \quad \overline{\mathfrak{B}} = S^{-1} \cdot \mathfrak{B}. \tag{6.5'}$$

Формулы (6.4) перепишутся так:

$$\mathfrak{B} \cdot a = A \cdot \mathfrak{B}. \tag{6.4''}$$

Подставляя сюда (6.5'), получим:

$$S\overline{\mathfrak{B}}a = A \cdot S\overline{\mathfrak{B}}^{-1}.$$

Умножая слева на S^{-1}, будем иметь

$$\overline{\mathfrak{B}} \cdot a = S^{-1}AS \cdot \overline{\mathfrak{B}}. \tag{6.6'}$$

Что получится в том частном случае, если первые k элементов базиса составляют сами базис правого идеала? Тогда в первых k формулах (6.4) не равными нулю будут только k первых членов и каждому элементу a будет соответствовать матрица вида

$$A = \left\| \begin{matrix} M & 0 \\ N & P \end{matrix} \right\|, \tag{6.7}$$

причём матрицы M сами будут давать представление. Представления типа (6.7) носят название *полуприведённых представлений* (в отличие от *вполне приведённых представлений*, которые имеют вид

$$A = \left\| \begin{matrix} M & 0 \\ 0 & P \end{matrix} \right\| \tag{6.8}$$

и которые, как мы увидим ниже, соответствуют правым идеалам, разлагаемым в *прямые суммы* правых идеалов).

Если относительно правого идеала B только известно, что он содержит правый подидеал, то это будет означать, что можно найти такую линейную подстановку S, что всякая матрица $S^{-1}AS$ нашего представления будет полуприведённой. В этом случае представление носит название полуприводимого представления, и мы приходим к теореме:

Теорема 1. *Чтобы представление алгебры матрицами было полуприводимо, необходимо и достаточно, чтобы правый идеал, при помощи которого оно получено, содержал отличный от него правый подидеал.*

Будем называть правый идеал, не содержащий отличных от него правых идеалов, *простым правым идеалом.* Тогда из теоремы 1 вытекает следствие:

Следствие. Чтобы правый идеал давал *неприводимое представление*, необходимо и достаточно, чтобы он был простым.

Представление алгебры матрицами можно также получить при помощи левого идеала. Для этого нужно умножить базис на представляемый элемент не справа, а *слева.* Пусть $\mathfrak{B}$ — базис левого идеала. Тогда

$$a \cdot \mathfrak{B} = A \cdot \mathfrak{B}.$$

Пусть также

$$b \cdot \mathfrak{B} = B \cdot \mathfrak{B}.$$

Отсюда

$$ab\mathfrak{B} = a \cdot B\mathfrak{B} = B \cdot a\mathfrak{B} = BA\mathfrak{B}.$$

Мы видим, что в этом случае из

$$a \to A, \quad b \to B$$

следует

$$ab \to BA,$$

т. е. что здесь матрицы перемножаются в порядке, противоположном порядку элементов. Такого рода гомоморфизм носит название *гомоморфизма 2-го рода.*

УПРАЖНЕНИЯ

1) Представить алгебру кватернионов матрицами четвёртого измерения.

2) Доказать, что каждая матрица, дающая представление 1-го рода данной алгебры, перестановочна с каждой матрицей, дающей представление 2-го рода той же алгебры.

§ 7. НИЛЬПОТЕНТНЫЕ АЛГЕБРЫ

Будем называть элемент a алгебры A ***нильпотентным***, если для него существует такой показатель α, при котором

$$a^{\alpha} = 0.$$

Если все элементы алгебры A нильпотентны, то самую алгебру мы будем называть *слабо нильпотентной*.

Если же для самой алгебры A существует такой показатель α, при котором

$$A^{\alpha} = 0,$$

то мы будем называть алгебру A ***нильпотентной***. В нильпотентной алгебре произведение её любых α элементов равно нулю, каковое свойство может служить определением нильпотентной алгебры.

Докажем, что в случае алгебры A конечного порядка понятия нильпотентности и слабой нильпотентности совпадают.

Теорема 2. *Всякая слабо нильпотентная алгебра конечного порядка нильпотентна.*

Доказательство. Допустим противное. Тогда алгебры

$$A,\ A^2,\ A^3,\ \ldots$$

не могут быть все время уменьшающихся порядков, так как порядок каждой конечен. Следовательно, найдётся такое k, что

$$A^{k+1} = A^k.$$

Вводя обозначение $B = A^k$, мы получим

$$B^2 = B. \tag{7.1}$$

Пусть $[b_1, b_2, \ldots, b_n]$ — базис алгебры B. Тогда, обозначая через C_i правый идеал b_iB, будем иметь

$$C_1 + C_2 + \ldots + C_s = B.$$

Это равенство означает, что всякий элемент алгебры B можно представить в виде суммы элементов идеалов $C_1, C_2, \ldots, C_s$.

Докажем, что хотя бы одна из алгебр C_i не нильпотентна. В противном случае, допустив, что имеет место

$$C_i^2 = 0 \quad (i = 1, 2, \ldots, S),$$

и разлагая выражение

$$B^{ps} = (C_1 + C_2 + \ldots + C_s)^{ps},$$

мы получим в каждом члене по крайней мере p одинаковых множителей C_i (для одного какого-нибудь i), и в силу

$$C_iC_j \subset C_i, \quad C_i^p = 0$$

этот член обратится в нуль. Отсюда

$$B^{ps} = 0,$$

что противоречит равенству (7.1).

Пусть C_1 — не нильпотентная алгебра. Тогда при некотором k_1 мы будем иметь

$$C_1^{k_1+1} = C_1^{k_1}.$$

Вводя обозначения $F = C_1^{k_1}$, мы получим

$$F^2 = F.$$

Внутри алгебры F опять выделим таким же способом подалгебру H, для которой будет иметь место

$$H^2 = H,$$

и т. д. Порядки получаемых таким образом алгебр

$$B,\ F,\ H, \ldots$$

не могут всё время убывать. Пусть для какой-нибудь из этих алгебр, например, W, дальнейшее построение не уменьшит порядка. Это означает, что, обозначая через $[w_1, w_2, \ldots, w]$ базис алгебры W, мы для какого-то значка i будем иметь

$$w_iW = W.$$

Это равенство показывает, что уравнение

$$w_ix = w_i$$

имеет решение

$$x \subset W.$$

Тогда для любого α мы будем иметь

$$w_ix^\alpha = w_ixx^{\alpha-1} = w_ix^{\alpha-1} = w_ix^{\alpha-2} = \ldots = w_ix = w_i,$$

а это показывает, что x не есть нильпотентный элемент, что противоречит нашему предположению относительно слабой нильпотентности алгебры A. Это доказывает теорему.

В связи с этой теоремой легко доказать следующую важную для дальнейшего теорему. Назовём *идемпотентом* элемент e, удовлетворяющий условию

$$e^2 = e. \tag{7.2}$$

Тогда имеет место

Теорема 3. *Если алгебра A не нильпотентна, то она содержит идемпотент.*

Доказательство. Пусть A — не нильпотентная алгебра. При доказательстве теоремы 2 мы видели, что она содержит подалгебру W, в которой существует элемент x, удовлетворяющий соотношению

$$wW = W. \tag{7.3}$$

Из этого, во-первых, следует, что W не содержит элемента $x \neq 0$, для которого бы имело место

$$wx = 0,$$

так как тогда, беря его в качестве первого элемента базиса

$$W = [x, w_2, \ldots, w_s],$$

мы бы имели

$$wW = [ww_2, \ldots, ww_s],$$

и порядок алгебры wW был бы меньше порядка алгебры W, что противоречит равенству (7.3).

Во-вторых, из (7.3) следует, что W содержит такой элемент e, что

$$we = w,$$

откуда

$$we^2 = we, \quad w(e^2 - e) = 0.$$

Но, в силу только что доказанного, элемент $e^2 - e$ должен быть нулём, и теорема доказана.

Найдём аналитические условия нильпотентности элемента, а также нильпотентности алгебры. Для этого мы воспользуемся изоморфным представлением алгебры матрицами.

Теорема 4. *Для того чтобы элемент a был нильпотентным, необходимо и достаточно, чтобы в матрице, соответствующей ему в изоморфном представлении, все характеристические корни были равны нулю.*

Доказательство. Условие достаточно, так как в этом случае характеристическое уравнение матрицы A имеет вид

$$u^n = 0.$$

Но, как известно, матрица есть символический корень своего характеристического уравнения, откуда

$$A^n = 0.$$

Но так как представление изоморфно, то должно иметь место равенство

$$a^n = 0,$$

что и нужно.

Условие необходимо. В самом деле, пусть

$$a^\alpha = 0;$$

тогда полином $\varphi(u)$ — наименьшей степени, для которого имеет место

$$\varphi(a) = 0,$$

должен быть делителем полинома u^α и потому имеет форму u^β. С другой стороны, известно, что его n-я степень делится на характеристический полином, который в силу этого должен иметь вид

$$u^n,$$

откуда следует, что все его корни — нули.

Следствие. *В алгебре порядка n наименьший показатель α, для которого имеет место $a^\alpha = 0$, не превышает $n+1$.*

Это следует из того, что алгебра порядка n имеет изоморфное представление матрицами порядка $n+1$.

Для вывода аналитических условий нильпотентности алгебры введём понятие *следа* элемента в каком-нибудь изоморфном представлении. *Следом* элемента a называется сумма диагональных элементов соответствующей ему матрицы. Иначе — это коэффициент при u^{n-1} в её характеристическом полиноме; ещё иначе — это сумма её характеристических корней. Для следа введён символ

$$S(a).$$

В силу линейности его выражения через элементы матрицы имеет место формула

$$S(a+b) = S(a) + S(b). \tag{7.4}$$

Чтобы получить выражение для следа элемента a_i базиса вспомним формулы (3.2′):

$$a_i a_j = \gamma_{ij}^{\nu} a_{\nu},$$

из которых получаем выражение для матрицы, соответствующей элементу a_j:

$$a_j \to \begin{Vmatrix} \gamma_{1j}^1, & \gamma_{1j}^2, & \dots, & \gamma_{1j}^n \\ \gamma_{2j}^1, & \gamma_{2j}^2, & \dots, & \gamma_{2j}^n \\ \dots & \dots & \dots & \dots \\ \gamma_{nj}^1, & \gamma_{nj}^2, & \dots, & \gamma_{nj}^n \end{Vmatrix},$$

откуда

$$S(a_j) = \sum_{\nu} \gamma_{\nu j}^{\nu}. \tag{7.5}$$

В силу (7.4) для элемента

$$a = \alpha^{\mu} a_{\mu}$$

имеет место

$$S(a) = \sum_{\mu, \nu} \alpha^{\mu} \gamma_{\nu\mu}^{\nu}. \tag{7.6}$$

Сформулируем условие нильпотентности алгебры:

Теорема 5. *Для того чтобы алгебра A была нильпотентна, необходимо и достаточно, чтобы для элементов её базиса $[a_1, a_2, \dots, a_n]$ имело место*

$$S(a_1) = 0, \quad S(a_2) = 0, \dots, S(a_n) = 0. \tag{7.7}$$

Доказательство. Условие необходимо, так как из нильпотентности алгебры следует нильпотентность элементов её базиса, для которых, таким образом, характеристические полиномы имеют вид u^n, и потому, в частности, имеет место $S(a_i) = 0$.

Условие достаточно. Чтобы убедиться в этом, выразим через базис степени произвольного элемента a алгебры, для которой имеет место (7.7). Тогда в силу (7.4) получим

$$S(a) = 0, \quad S(a^2) = 0, \dots, \quad S(a^n) = 0. \tag{7.8}$$

Но из теории матриц известно, что характеристический полином матрицы A^k имеет корнями k-е степени корней характеристического полинома матрицы A. Таким образом из равенств (7.8) следует, что все суммы степеней характеристических корней матрицы A равны нулю. Отсюда

следует, что равны нулю и коэффициенты её характеристического полинома, так как они выражаются через суммы степеней корней при помощи формул Ньютона. Отсюда в силу теоремы 4 следует, что элемент a нильпотентен, т. е. алгебра A слабо нильпотентна. Из теоремы же 2 вытекает нильпотентность алгебры A.

Примечание. Мы доказали теорему 2, предполагая алгебру A конечной. Для случая, когда алгебра бесконечна, можно привести пример слабо нильпотентной, но не нильпотентной алгебры. Пусть алгебра имеет бесконечный базис $[a_1, a_2, a_3, \ldots]$, элементы которого связаны соотношениями

$$a_i a_j = 0 \ (i \neq j), \quad a_n^n \neq 0, \quad a_n^{n+1} = 0.$$

Тогда всякий её элемент, выражаемый через конечное число элементов базиса:

$$a = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n,$$

нильпотентен: $a^{n+1} = 0$, в то время как не существует показателя α, для которого бы имело место $A^\alpha = 0$.

§ 8. РАДИКАЛЫ

Для дальнейшего нам понадобится

Теорема 6. *Следы элементов ab и ba равны:*

$$S(ab) = S(ba). \tag{8.1}$$

Доказательство. Не нарушая общности, можно принять a и b за элементы базиса, например, за a_1 и a_2 (этого нельзя сделать лишь тогда, если a и b зависимы; но тогда теорема очевидна в силу перестановочности a и b). Имеем

$$a_1 a_2 a_i = \gamma_{12}^{\nu} a_\nu a_i = \gamma_{12}^{\nu} \gamma_{\nu i}^{\mu} a_\mu,$$

откуда

$$S(a_1 a_2) = \gamma_{12}^{\nu} \gamma_{\nu\mu}^{\mu},$$

и точно так же

$$S(a_2 a_1) = \gamma_{21}^{\nu} \gamma_{\nu\mu}^{\mu}.$$

Но при помощи (3.3) мы получим

$$S(a_1 a_2) = \gamma_{12}^{\nu} \gamma_{\nu\mu}^{\mu} = \gamma_{2\mu}^{\nu} \gamma_{1\nu}^{\mu},$$

$$S(a_2 a_1) = \gamma_{21}^{\nu} \gamma_{\nu\mu}^{\mu} = \gamma_{1\mu}^{\nu} \gamma_{2\nu}^{\mu}.$$

Поменяв ролями значки ν и μ, мы придём к (8.1),

Назовём *собственно нильпотентными* элементы a, для которых элементы xa и ax при всяком x из A нильпотентны. Заметим, что из нильпотентности xa вытекает нильпотентность ax: если

$$(xa)^\alpha = 0,$$

то

$$(ax)^{\alpha+1} = a\,(xa)^\alpha x = 0.$$

Справедливо и обратное. Имеет место

Теорема 7. *Чтобы a был собственно нильпотентным, необходимо и достаточно соблюдение всех элементов a_i базиса равенств*

$$(8.2)\quad S(aa_i) = 0. \quad (i = 1, 2, \ldots, n).$$

Доказательство. Условие необходимо, так как для собственно нильпотентного a, в частности, нильпотентны все aa_i, и для них в силу теоремы 4 имеет место

$$S(aa_i) = 0.$$

Условие достаточно. Пусть, в самом деле, для какого-нибудь a имеет место (8.2). Тогда для каждого x имеет место

$$S(ax) = 0.$$

Но так как в форме ax можно представить каждый из элементов

$$ay, (ay)^2, \ldots, (ay)^n,$$

где y — произвольный элемент алгебры A, то отсюда

$$S(ay) = 0, \quad S((ay)^2) = 0, \ldots, \quad S((ay)^n) = 0$$

и в силу теоремы 4 ay нильпотентен. Точно так же

$$S(xa) = S(ax) = 0,$$

откуда, в частности,

$$S(ya) = 0, \quad S((ya)^2) = 0, \ldots, S((ya)^n) = 0,$$

а это показывает, что ya нильпотентен. Таким образом a собственно нильпотентен.

Теорема 8. *Совокупность собственно нильпотентных элементов алгебры A образует нильпотентную подалгебру, являющуюся двусторонним идеалом алгебры A.*

Доказательство. Если условия (8.2) соблюдаются для элементов a и b, то они также имеют место для $a \pm b$

и ab. Более того, они имеют место для ax и xa, где x — произвольный элемент алгебры A. В самом деле, пусть $xa_i = \xi_i^\nu a_\nu$. Тогда

$$S(axa_i) = \xi_i^\nu S(aa_\nu) = 0.$$

Точно так же, положив $a_i x = \eta_i^\nu a_\nu$, будем иметь

$$S(xaa_i) = S(a_i xa) = S(aa_i x) = \eta_i^\nu S(aa_\nu) = 0.$$

Отсюда следует, что совокупность собственно нильпотентных элементов алгебры A составляет её двусторонний идеал, ч. и т. д. Его нильпотентность следует из теоремы 2.

Этот идеал носит название *радикала* алгебры A. Будем обозначать его буквой R. Он содержит любой нильпотентный двусторонний идеал алгебры A, так как в таком идеале должен быть нильпотентен не только каждый его элемент a, но также все элементы ax, xa, где x — произвольный элемент алгебры A. Отсюда следует, что a собственно нильпотентен, т. е. входит в R.

Чтобы найти для данной алгебры A радикал, подчиним её элемент

$$a = \alpha^1 a_1 + \alpha^2 a_2 + \ldots + \alpha^n a_n$$

условиям (8.2). Получится система линейных уравнений

$$(8.3)\quad \begin{array}{l} S(a_1a_1)\alpha^1 + S(a_2a_1)\alpha^2 + \ldots + S(a_na_1)\alpha^n = 0, \\ S(a_1a_2)\alpha^1 + S(a_2a_2)\alpha^2 + \ldots + S(a_na_2)\alpha^n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S(a_1a_n)\alpha^1 + S(a_2a_n)\alpha^2 + \ldots + S(a_na_n)\alpha^n = 0, \end{array}$$

из которой определятся всевозможные системы решений, дающие собственно нильпотентные элементы a алгебры A. Эта система имеет отличные от нуля решения тогда и только тогда, если её определитель

$$(8.4)\qquad \Delta = \begin{vmatrix} S(a_1a_1), & S(a_2a_1), & \ldots, & S(a_na_1) \\ S(a_1a_2), & S(a_2a_2), & \ldots, & S(a_na_2) \\ \ldots & \ldots & \ldots & \ldots \\ S(a_1a_n), & S(a_2a_n), & \ldots, & S(a_na_n) \end{vmatrix}$$

равен нулю. Этот определитель носит название *дискриминанта* алгебры A. Всякий нильпотентный двусторонний и даже односторонний идеал B алгебры A содержится в её радикале R. В самом деле, если

$$b \subset B,$$

то и $bx \subset B$ при любом $x \subset A$, откуда следует, что при некотором α

$$(bx)^{\alpha} = 0.$$

Таким образом b есть собственно нильпотентный элемент алгебры A, т. е. $b \subset R$.

Если алгебра не содержит отличного от нуля радикала, то она называется *полупростой алгеброй*. Приведённые рассуждения позволяют сформулировать следующую теорему:

Теорема 9. *Чтобы алгебра была полупростой, необходимо и достаточно, чтобы её дискриминант был отличен от нуля.*

Форма уравнений (8.3) показывает справедливость следующей теоремы:

Теорема 10. *В полупростой алгебре можно всегда найти элемент a, для которого величины*

$$S(aa_1),\ S(aa_2),\ \ldots,\ S(aa_n)$$

принимают наперёд заданные значения из поля Ω. Этими значениями элемент a определяется однозначно. Докажем ещё следующую теорему:

Теорема 11. *Если R есть радикал алгебры A, то факторалгебра полупроста.*

Доказательство. Допустим противное. Тогда A должна содержать не лежащий в R элемент a такого рода, что некоторая степень элемента ax, где x — произвольный элемент алгебры A, лежит в R:

$$(ax)^{\alpha} \subset R.$$

Но так как все элементы радикала R нильпотентны, то существует такой показатель σ, при котором

$$(ax)^{\alpha\sigma} = 0.$$

Точно так же докажем существование показателей α', σ', при которых

$$(xa)^{\alpha'\sigma'} = 0.$$

Отсюда, в силу произвольности $x \subset A$, следует, что a собственно нильпотентен, т. е. входит в R, что противоречит допущению.

УПРАЖНЕНИЯ

1) Найти радикал алгебры, определяемой следующей таблицей умножения:

	e_1	e_2	u
e_1	e_1	0	u
e_2	0	e_2	0
u	0	u	0

Составить таблицу умножения для факторалгебры этой алгебры по радикалу.

2) Пусть e — какой-нибудь идемпотент алгебры A. Каждый элемент $a \subset A$ можно представить в виде

$$a = eae + e(a - ae) + (a - ea)e + (a - ea - ae + eae)$$

(двустороннее разложение Пирса). Если a пробегает алгебру A, то каждое из четырёх слагаемых пробегает линейную систему; обозначим их через eAe, eL_e, R_ee, C_e. Доказать, что каждая из этих линейных систем составляет алгебру.

3) Доказать, что радикал алгебры eAe есть eNe, т. е. пересечение радикала N алгебры A с eAe.

4) Доказать, что радикал алгебры C_e есть пересечение N с C_e.

5) Идемпотент e называется *принципальным*, если не существует другого идемпотента u, который был бы ортогонален к e (т. е. было бы $ue = eu = 0$). Доказать, что для принципальных и только для принципальных e алгебра C_e нильпотентна.

6) Если u — непринципальный идемпотент, то существует идемпотент $e = u + v$ такого рода, что

$$eu = ue = u, \quad ev = ve = v.$$

Тогда

$$C_e = C_u.$$

7) Всякая ненильпотентная алгебра содержит принципальный идемпотент.

8) Разность двух принципальных идемпотентов входит в радикал.

9) Идемпотент, не равный сумме взаимно ортогональных идемпотентов, называется примитивным. Доказать, что всякий идемпотент можно представить как сумму конечного числа взаимно ортогональных примитивных идемпотентов.

10) Если e идемпотент полупростой алгебры A, то алгебра eAe тоже полупроста. Если A проста (см. § 9), то проста и eAe.

11) Если алгебра A проста, то eAe является телом тогда и только тогда, когда e есть примитивный идемпотент.

§ 9. ПОЛУПРОСТЫЕ АЛГЕБРЫ

Теорема 12. *Полупростая алгебра A всегда содержит главную единицу.*

Доказательство. Пользуясь теоремой 10, найдём такой элемент e, для которого бы соблюдались равенства

$$S(ea_i) = S(a_i) \qquad (i = 1, 2, \ldots, n). \tag{9.1}$$

Отсюда следует

$$S(ea_i - a_i) = 0 \qquad (i = 1, 2, \ldots, n).$$

Взяв произвольный элемент

$$x = \xi^\nu a_\nu$$

алгебры A, мы отсюда получим

$$S(ex - x) = S(\xi^\nu (ea_\nu - a_\nu)) = \xi^\nu S(ea_\nu - a_\nu) = 0.$$

Беря в роли x последовательно

$$ya_1, ya_2, \ldots, ya_n,$$

мы будем иметь (y — опять произвольный элемент из A)

$$S((ey - y)a_i) = 0 \qquad (i = 1, 2, \ldots, n).$$

Но эти равенства, в силу теоремы 7, указывают, что элемент $ey - y$ собственно нильпотентен, т. е. что $ey - y = 0$:

$$ey = y. \tag{9.2}$$

Написав равенства (9.1) в форме

$$S(a_i e) = S(a_i) \qquad (i = 1, 2, \ldots, n),$$

мы аналогично получим отсюда

$$S(xe - x) = 0,$$
$$S(a_i(ye - y)) = 0 \qquad (i = 1, 2, \ldots, n),$$

откуда будем следовать

$$ye = y. \tag{9.3}$$

Равенства (9.2) и (9.3), в силу произвольности $y \subset A$, показывают, что e есть главная единица алгебры A, ч. и т. д.

Введём понятие *прямой суммы* двух (и более) подалгебр. Пусть A содержит два взаимно простых (т. е. не содержащих, кроме нуля, общих элемента) двусторонних идеала B и C. Тогда совокупность элементов $b + c$, где b пробегает B и c пробегает C, называется *прямой суммой* $B + C$. Докажем, что $B + C$ составляет алгебру. Всякое произведение bc, в силу двусторонности идеалов B, C, содержится и в B, и в C, а потому, в силу взаимной простоты последних, равно нулю. Точно так же и $cb = 0$. В силу этого произведение

$$(b + c)(b_1 + c_1) = bb_1 + cc_1$$

входит в $B+C$, так как

$$bb_1 \subset B, \quad cc_1 \subset C.$$

Теорема 13. *Если алгебра A содержит двусторонний идеал B, имеющий главную единицу, то A распадается в прямую сумму идеала B и некоторого другого двустороннего идеала.*

Доказательство. Выберем базис алгебры A так, чтобы его первые m членов составляли базис алгебры B:

$$[b_1, b_2, \ldots, b_m; c'_{m+1}, c'_{m+2}, \ldots, c'_n].$$

Покажем, что элементы C'_i можно нормировать так, чтобы они составляли базис другой алгебры. Именно, заменим их следующими:

$$c_i = c'_i - bc'_i - c'_ib + bc'_ib \qquad (i = m+1, \ldots, n),$$

где b — главная единица идеала B. В этом выражении три последних члена суть элементы алгебры B и потому выражаются через $b_1, b_2, \ldots, b_m$, так что наше преобразование обратимо, и система

$$[b_1, b_2, \ldots, b_m; c_{m+1}, c_{m+2}, \ldots, c_n]$$

тоже является базисом алгебры A.

Обозначим через C линейную систему элементов, имеющую базис $[c_{m+1}, c_{m+2}, \ldots, c_n]$. Если x — произвольный элемент алгебры B, то в силу того, что для B элемент b есть главная единица, имеем

$$xc_i = xc'_i - xc'_i - xc'_ib + xc'_ib = 0,$$
$$c_ix = c'_ix - bc'_ix - c'_ix + bc'_ix = 0,$$

откуда $BC = 0$, $CB = 0$.

Докажем, что C составляет алгебру. Элемент из C можно охарактеризовать тем, что он обращается в нуль при умножении на b. В самом деле, если

$$a = x + y, \quad x \subset B, \quad y \subset C,$$

то

$$ab = xb + yb = x,$$

так что

$$ab = 0$$

имеет место тогда и только тогда, если $x=0$, т. е. если $a \subset C$.

Если

$$x \subset C, \quad y \subset C,$$

то

$$xb=0, \quad yb=0,$$

откуда

$$(x+y)b=xb+yb=0,$$
$$(xy)b=x(yb)=0,$$

т. е.

$$x+y \subset C, \quad xy \subset C.$$

Алгебра C есть двусторонний идеал, так как

$$C \cdot A=C(B+C)=C \cdot B+C^2 \subset C,$$
$$A \cdot C=(B+C)C=B \cdot C+C^2 \subset C.$$

Это показывает, что A является прямой суммой двусторонних идеалов B и C.

Будем называть *простой алгеброй* алгебру, не содержащую отличных от самой себя двусторонних идеалов. Из этого определения следует, что простая алгебра может только тогда иметь отличный от нуля радикал, когда она с ним совпадает, т. е. когда она сама нильпотентна. В последнем случае, если α есть показатель, при котором

$$A^{\alpha-1} \neq 0, \quad A^{\alpha}=0,$$

то $A^{\alpha-1}$ составляет двусторонний идеал, так что алгебра A может быть простой только в случае $\alpha=2$, т. е. нулевой алгебры: $A=0$. Пусть $[a_1, a_2, \ldots, a_n]$ —базис нулевой алгебры. Линейная система с базисом $[a_1]$ составляет её двусторонний идеал, так что нулевая алгебра может быть простой только в случае $n=1$. Итак, мы приходим к теореме:

Теорема 14. *Всякая простая алгебра полупроста, за исключением нулевой алгебры порядка* 1.

В дальнейшем мы будем исключать из рассмотрения нулевые алгебры порядка 1.

Чтобы разложить полупростую алгебру в прямую сумму простых, докажем предварительно теорему.

Теорема 15. *Всякий двусторонний идеал полупростой алгебры есть тоже полупростая алгебра.*

Доказательство. Пусть двусторонний идеал B полупростой алгебры A содержит радикал S:

$$SB \subset S, \quad BS \subset S, \quad S^{\alpha} = 0.$$

Совокупность BSB есть, очевидно, двусторонний идеал в A:

$$ABSB \subset BSB, \quad BSB.A \subset BSB.$$

Вместе с тем

$$BSB \subset SB \subset S,$$

откуда следует, что BSB есть нильпотентный двусторонний идеал алгебры A и поэтому равен нулю:

$$BSB = 0.$$

Вместе с тем ASA есть двусторонний идеал алгебры A, не равный нулю, так как A содержит главную единицу e и потому

$$ASA \supset eSe = S.$$

С другой стороны,

$$ASA \subset ABA \subset B,$$
$$(ASA)^3 = ASA \cdot ASA \cdot ASA \subset BSB = 0,$$

т. е. двусторонний идеал ASA алгебры A нильпотентен, что противоречит полупростоте алгебры A.

Теперь нетрудно доказать основную теорему для полупростых алгебр.

Теорема 16. *Всякая полупростая алгебра A может быть разложена в прямую сумму простых алгебр.*

Доказательство. Если сама A не проста, то она содержит двусторонний идеал B, который в силу теоремы 15 является полупростой алгеброй и потому в силу теоремы 12 содержит главную единицу. Но тогда из теоремы 13 следует, что A разлагается в прямую сумму B и другого двустороннего идеала C:

$$A = B + C.$$

Если алгебры B и C не просты, то, повторяя с ним то же рассуждение, разобьём их опять в прямые суммы, у которых слагаемые в силу $BC = CB = 0$ тоже являются двусторонними идеалами алгебры A. Так как порядки получаемых

алгебр не могут безгранично убывать, то мы в конце концов придём к разложению

$$A = A_1 + A_2 + \ldots + A_m, \tag{9.4}$$

где $A_1, A_2, \ldots, A_m$ суть простые алгебры, для которых имеет место

$$A_i A_j = 0 \qquad (i \neq j). \tag{9.5}$$

Теорема 17. *Разложение полупростой алгебры в прямую сумму простых однозначно.*

Доказательство. Пусть наряду с (9.4) мы имеем

$$A = B_1 + B_2 + \ldots + B_s, \tag{9.6}$$

где также $B_1, B_2, \ldots, B_s$ — простые алгебры, для которых имеет место

$$B_i B_j = 0 \qquad (i \neq j). \tag{9.7}$$

Каждая алгебра $A_\lambda B_\mu A_\nu$ содержится и в A_λ и в A_ν, так как и A_λ и A_ν — двусторонние идеалы. Поэтому она отлична от нуля только в случае $\lambda = \nu$. Алгебра $A_\lambda B_\mu A_\nu$ входит и в A_λ, и в B_μ, и в силу их простоты должна или быть равной нулю, или совпадать с обеими алгебрами A_λ, B_μ. С другой стороны, A содержит главную единицу, в силу чего

$$AB_\mu A = B_\mu.$$

Отсюда

$$B_\mu = AB_\mu A = \sum_{\lambda, \nu} A_\lambda B_\mu A_\nu = \sum_{\lambda} A_\lambda B_\mu A_\lambda.$$

Это равенство показывает, что при данном μ не все $A_\lambda B_\mu A_\lambda$ обращаются в нуль, а следовательно, одна из A_λ совпадает с B_μ. Продолжая рассуждение, докажем полное совпадение обоих разложений.

Теорема 16 допускает следующее обращение.

Теорема 18. *Всякая прямая сумма простых алгебр, из которых ни одна не нильпотентна, полупроста.*

Доказательство. Допустим противное: пусть

$$A = A_1 + A_2 + \ldots + A_m$$

содержит радикал R. Произведение

$$R \cdot A_i$$

равно нулю, так как содержится и в R, и в A_i и является двусторонним идеалом для A_i. Поэтому

$$RA = RA_1 + RA_2 + \ldots + RA_m = 0. \tag{9.8}$$

Пусть $r \neq 0$ — элемент из R. Разложим его по A_i:

$$r = r_1 + r_2 + \ldots + r_m. \tag{9.9}$$

Пусть e_i — главная единица алгебры A_i. В силу $A_jA_i = 0$ $(i \neq j)$ имеет место $r_je_i = 0$ $(i \neq j)$. Умножая (9.9) справа на e_i, получим в левой части нуль в силу (9.8); справа же останется r_i. Итак,

$$r_i = 0 \qquad (i = 1, 2, \ldots, n),$$

а потому

$$r = 0,$$

в противоположность допущению.

Интересны компоненты главной единицы, содержащиеся в каждой из алгебр A_i. Пусть

$$e = e_1 + e_2 + \ldots + e_m,$$

где

$$e_i \subset A_i, \quad e_ie_j = 0 \qquad (i \neq j).$$

Из равенства

$$e^2 = e$$

вытекает

$$e_1^2 + e_2^2 + \ldots + e_m^2 = e_1 + e_2 + \ldots + e_m.$$

Но так как

$$e_i \subset A_i, \quad e_i^2 \subset A_i,$$

то в силу однозначности разложения в прямую сумму должно иметь место

$$e_i^2 = e_i \qquad (i = 1, 2, \ldots, m),$$

т. е. e_i являются идемпотентами.

Докажем, что e_i является главной единицей в алгебре A_i. В самом деле, пусть

$$x \subset A_i.$$

Тогда

$$xe_j = 0 \qquad (j \neq i),$$

Но $xe = ex = x$, откуда

$$x(e_1 + e_2 + \ldots + e_m) = xe_i = x,$$
$$(e_1 + e_2 + \ldots + e_m)\, x = e_i x = x,$$

что и нужно.

Интересна связь разложения полупростой алгебры A с разложением её центра Z. Разлагая произвольный элемент a алгебры A по A_i:

$$a = a_1 + a_2 + \ldots + a_m,$$

и обозначая через Z_i центр алгебры A_i, а через x_i — произвольный элемент из Z_i, мы будем иметь

$$ax_i = (a_1 + a_2 + \ldots + a_m)\, x_i = a_i z_i = x_i a_i =$$
$$= z_i (a_1 + a_2 + \ldots + a_m) = z_i a,$$

откуда следует, что z_i лежит в центре Z всей алгебры A, т. е. что

$$Z_i \subset Z \qquad (i = 1, 2, \ldots, m).$$

С другой стороны, разложим произвольный элемент z центра Z по A_i:

$$z = z_1 + z_2 + \ldots + z_m.$$

Обозначая через a_i произвольный элемент из A_i, мы из $a_i z = x a_i$ получим

$$a_i (z_1 + z_2 + \ldots + z_m) = (x_1 + x_2 + \ldots + x_m)\, a_i,$$

т. е.

$$a_i x_i = x_i a_i \qquad (i = 1, 2, \ldots, m),$$

откуда видно, что z_i лежит в центре Z_i алгебры A. Таким образом

$$Z = Z_1 + Z_2 + \ldots + Z_m.$$

Остаётся доказать, что алгебры $Z_1, Z_2, \ldots, Z_m$ просты. Докажем сначала, что они полупросты. Если бы, например, Z_1 содержала радикал, то она так же содержала бы двусторонний идеал C, для которого имело бы место

$$C^2 = 0.$$

Но тогда алгебра

$$C + A_1 C + C A_1 + A_1 C A_1 \neq 0$$

была бы двусторонним идеалом в алгебре A_1, для которого в силу перестановочности A_1 с C имело бы место

$$(C+A_1C+CA_1+A_1CA_1)^2=(C+A_1C)^2=$$
$$=C^2+CA_1C+A_1C^2+A_1CA_1C\subset C^2+C^2+C^2+C^2=0,$$

что бы противоречило полупростоте алгебры A_1.

Если бы Z_1 была не проста, т. е. если бы имело место

$$Z_1=Z'+Z'', \quad Z'Z''=Z''Z'=0,$$
$$Z_1Z'\subset Z', \quad Z'Z_1\subset Z', \quad Z_1Z''\subset Z'', \quad Z''Z_1\subset Z'',$$

то главная единица e_1 алгебры A_1 (которая, очевидно, входит в центр Z_1) разлагалась бы по Z' и Z'' так:

$$e_1=e'+e'', \quad e'e''=e''e'=0, \quad e'^2=e', \quad e''^2=e''.$$

Отсюда следует

$$A_1=A_1e_1=A_1e'+A_1e'',$$

причём $A_1e'=e'A_1$, $A_1e''=e''A_1$, так как e' и e'' входят в центр Z_1 алгебры A_1. Ввиду этого алгебры A_1e' и A_1e'' суть двусторонние идеалы, для которых

$$A_1e'\cdot A_1e''=A_1e'e''A_1=0.$$

Из того, что e' есть главная единица алгебры A_1e':

$$a_1e'\cdot e'=a_1e'^2=a_1e', \quad e'\cdot a_1e'=a_1e'^2=a_1e',$$

следует, что алгебры A_1e', A_1e'' взаимно просты. В самом деле, если $x\subset A_1e'$, $x\subset A_1e''$, то $xe'=x$, $xe'=0$, откуда $x=0$. Итак, алгебра A_1 распадается в прямую сумму двух алгебр, т. е. не проста, и мы приходим к теореме.

Теорема 19. *Если полупростая алгебра A разлагается в прямую сумму m простых алгебр, то её центр Z разлагается в прямую сумму m простых коммутативных алгебр, из которых каждая служит центром соответствующего компонента алгебры A.*

Теорема 20. *Простая коммутативная алгебра является полем.*

Доказательство. Допустим противное. Пусть элемент a коммутативной алгебры Z не имеет обратного элемента. Тогда алгебра Za не содержит главной единицы e алгебры Z и поэтому не исчерпывает всей алгебры Z. Вместе с тем она является левым, а в силу коммутативности дву-

сторонним, идеалом алгебры Z, что противоречит простоте последней.

Отсюда простым следствием является

Теорема 21. *Полупростая алгебра A проста тогда и только тогда, когда её центр является полем.*

§ 10. ПРОСТЫЕ АЛГЕБРЫ

Перейдём к исследованию простых алгебр. Важнейшим типом простых алгебр являются тела, т. е. алгебры, в которых все отличные от нуля элементы образуют группу относительно умножения.

Теорема 22. *Тело есть простая алгебра.*

Доказательство. Мы видим, что всякая непростая алгебра содержит или нильпотентные элементы, или идемпотенты e_i, e_j, для которых $e_ie_j = 0$; ясно, что такого рода элементы не имеют обратных элементов.

Другим примером простых алгебр является рассмотренная нами в § 4 (пример IV) полная матричная алгебра.

Теорема 23. *Полная матричная алгебра M есть простая алгебра.*

Доказательство. Допустим противное: пусть M содержит двусторонний идеал D и пусть в D содержится элемент

$$d = \sum_{i,j} \alpha^{ij} e_{ij},$$

где хоть один коэффициент, например, $\alpha^{\mu\nu}$, отличен от нуля. Тогда в D будет содержаться также элемент

$$\frac{1}{\alpha^{\mu\nu}} e_{k\mu} d e_{\nu s} = \frac{1}{\alpha^{\mu\nu}} e_{k\mu} \sum_{i,j} \alpha^{ij} e_{ij} \cdot e_{\nu s} = e_{ks},$$

где k и s — любые значки. Это показывает, что D совпадает с M. Таким образом M не содержит отличных от себя двусторонних идеалов, т. е. есть простая алгебра, ч. и т. д.

Вместе с тем формула

$$e_{11} \cdot e_{21} = 0$$

показывает, что M не есть тело.

Каждой строке матрицы соответствует правый идеал алгебры M:

$$R_i = [e_{i1}, e_{i2}, \ldots, e_{in}] \qquad (i = 1, 2, \ldots, n),$$

а каждому столбцу соответствует левый идеал. Эти идеалы простые, так как не содержат никаких подидеалов. В самом деле, пусть R_1 содержит идеал D, имеющий элемент

$$d = \sum_i \alpha^i e_{1i} \quad (\alpha^k \neq 0).$$

Тогда D содержит также элементы

$$d \cdot \frac{1}{\alpha^k} \cdot e_{ks} = e_{1s} \quad (s = 1, 2, \ldots, n),$$

т. е. все элементы идеала R_1.

Отметим, однако, что эти простые правые (левые) идеалы не единственны. Например, идеал

$$[e_{11} + e_{21}, e_{12} + e_{22}, \ldots, e_{1n} + e_{2n}]$$

тоже простой и имеет тот же порядок, что R_i.

В этом параграфе мы покажем, что изучение простых алгебр может быть приведено к изучению тел и полных матричных алгебр. Для этого необходимо ввести новое понятие *прямого произведения двух алгебр*. Пусть A и B — две алгебры. Будем рассматривать формальные произведения элементов A и элементов B, в которых множители будем считать перестановочными (из этого, конечно, не следует, что алгебры A и B коммутативны). Совокупность сумм произведений $a \cdot b$, где $a \subset A$, $b \subset B$, составляет алгебру, у которой закон композиции определяется законами композиции алгебр A и B. В самом деле,

$$ab \cdot a'b' = aa' \cdot bb'.$$

Эта алгебра называется *прямым произведением алгебр* A *и* B и обозначается так:

$$A \times B.$$

Если $[a_1, a_2, \ldots, a_m]$, $[b_1, b_2, \ldots, b_n]$ — базисы алгебр A, B, то базисом алгебры $A \times B$ служит система произведений

$$[\ldots a_i b_j \ldots] \quad (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n),$$

в силу чего порядок прямого произведения равен произведению порядков сомножителей.

Понятие прямого произведения может без труда быть перенесено на любое число сомножителей.

В частности, расширение поля Ω коэффициентов алгебры может быть истолковано как прямое умножение алгебры на расширенное поле.

Среди простых алгебр тела выделяются следующим критерием.

Теорема 24. *Простая алгебра является телом тогда и только тогда, когда она не содержит отличных от себя самой правых* (или левых) *идеалов.*

Доказательство. Если простая алгебра A содержит правый идеал B, т. е. если

$$BA \subset B, \quad B \neq A,$$

то, выбрав внутри B какой-нибудь элемент $b \neq 0$ и обозначив через $[a_1, a_2, \ldots, a_n]$ базис алгебры A, мы увидим, что элементы

$$ba_1, ba_2, \ldots, ba_n$$

содержатся в B и потому не независимы. Пусть

$$\lambda' ba_1 + \lambda^2 ba_2 + \ldots + \lambda^n ba_n = 0,$$

т. е.

$$b(\lambda' a_1 + \lambda^2 a_2 + \ldots + \lambda^n a_n) = 0,$$

а это равенство показывает, что внутри A не существует элемента, обратного к b.

Обратно, предположим, что A не является телом. Это означает, что A содержит элемент a, не имеющий обратного элемента. Поэтому правый идеал aA не содержит главной единицы алгебры A, т. е. не исчерпывает всей алгебры A. Таким образом A содержит отличный от A правый идеал. Аналогично можно доказать, что Aa является отличным от A левым идеалом.

Опишем способ разложения алгебры в сумму односторонних (например, правых) идеалов. Если R есть простой правый идеал алгебры A, то он в силу теоремы 3 или нильпотентен или содержит идемпотент. В первом случае R^2 есть отличный от R правый идеал, и в силу простоты R

$$R^2 = 0.$$

Но тогда алгебра A содержит двусторонний идеал $R + AR$, который нильпотентен в силу

$$(R + AR)^2 = R^2 + RAR + AR^2 + ARAR \subset$$
$$\subset R^2 + R \cdot R + AR^2 + AR \cdot R = 0.$$

Если алгебра A полупростая, то R содержит идемпотент e. Правый идеал eA содержится в R, и силу простоты последнего

$$eA = R.$$

Способ разложения состоит в представлении каждого элемента алгебры A в форме

$$a = ea + (a - ea). \tag{10.1}$$

Если заставить пробегать a всю алгебру A, то ea пробежит весь правый идеал R, а $(a - ea)$ — некоторый правый идеал, который взаимно прост с R. В самом деле, если

$$ex = y - ey,$$

то, умножая слева на e, мы получим

$$ex = ey - ey = 0.$$

Итак, мы пришли к разложению

$$A = R + R_1.$$

Если R_1 — непростой правый идеал, то в нём можно найти простой правый идеал алгебры A. Продолжая разложение, мы в конце концов получим:

$$A = R_1 + R_2 + \ldots + R_s, \tag{10.2}$$

где R_i — простые правые идеалы алгебры A. В этом разложении главная единица e представится так:

$$e = e_1 + e_2 + \ldots + e_s,$$

где

$$e_i \subset R_i \qquad (i = 1, 2, \ldots, s).$$

Возьмём $a_1 \subset R_1$. Тогда

$$a_1 = ea_1 = e_1a_1 + e_2a_1 + \ldots + e_sa_1,$$

но, с другой стороны,

$$a_1 = a_1 + 0 + \ldots + 0,$$

и в силу однозначности разложения

$$e_1a_1 = a_1, \quad e_2a_1 = 0, \quad \ldots, \quad e_sa_1 = 0.$$

В частности, беря $a_1 = e_1$, получим

$$e_1^2 = e_1, \quad e_2e_1 = 0, \quad \ldots, \quad e_se_1 = 0,$$

и вообще

$$e_i^2 = e_i, \quad e_i e_j = 0 \quad (i \neq j). \tag{10.3}$$

При этом в силу простоты идеала R_i

$$e_i R_i = R_i, \quad e_i R_j = 0 \quad (i \neq j),$$

откуда

$$e_i A = e_i (R_1 + R_2 + \ldots + R_s) = R_i.$$

Обратно, если главная единица разлагается на систему идемпотентов, удовлетворяющих равенствам (10.3), то, полагая $e_i A = R_i$, мы будем иметь

$$A = R_1 + R_2 + \ldots + R_s.$$

В самом деле, для любого a из A имеет место

$$a = ea = (e_1 + e_2 + \ldots + e_s)\, a = e_1 a + e_2 a + \ldots + e_s a.$$

Такое разложение однозначно, так как из

$$0 = b_1 + b_2 + \ldots + b_s, \quad b_i \subset e_i A,$$

умножая слева на e_i, мы получим

$$b_i = 0.$$

Пользуясь идемпотентами (10.3) и полагая

$$A e_i = L_i,$$

где L_i — левый идеал, мы точно таким же образом получим разложение

$$A = L_1 + L_2 + \ldots + L_s,$$

где L_i — тоже простые идеалы, так как в противном случае мы бы получили бо́льшее число идемпотентов (10.3) и, значит, разложение A на большее число правых идеалов.

Теперь приступим к доказательству основной теоремы этого параграфа.

Теорема 25. *Всякую простую алгебру можно представить как прямое произведение некоторого тела и полной матричной алгебры.*

Доказательство. Пусть

$$e = e_1 + e_2 + \ldots + e_s, \tag{10.4}$$

$$e_i A = R_i, \quad A e_i = L_i \quad (i = 1, 2, \ldots, s), \tag{10.5}$$

где R_i, L_i — простые идеалы простой алгебры A. Произведение L_iR_i есть двусторонний идеал, который содержит $e_i^2 = e_i$ и потому не равен нулю, в силу чего

$$L_iR_i = A.$$

Далее, полагая

$$R_iL_j = A_{ij} \qquad (i, j = 1, 2, \ldots, s) \tag{10.6}$$

и разлагая A так:

$$A = A^2 = (R_1 + R_2 + \ldots + R_s)(L_1 + L_2 + \ldots + L_s) = \sum_{i,j} R_iL_j = \sum_{i,j} A_{ij},$$

мы убедимся, что при этом разложении разложение элементов однозначно, так как из

$$0 = \sum_{i,j} a_{ij}, \quad a_{ij} \subset A_{ij},$$

умножая слева на e_μ, мы, в силу

$$e_\mu A_{ij} = e_\mu R_iL_i = e_\mu e_i A_{ej} = 0 \quad (\mu \neq i),$$

получим

$$0 = \sum_j a_{\mu j} \qquad (\mu = 1, 2, \ldots, s);$$

далее, умножая это равенство справа на e_ν, будем иметь

$$a_{\mu\nu} = 0 \qquad (\mu, \nu = 1, 2, \ldots, s).$$

В силу простоты R_i имеет место

$$A_{ij}R_j = R_iL_jR_j = R_iA = R_i.$$

Выберем из A_{ij} элемент $a_{ij} \neq 0$. Тогда

$$a_{ij}R_j \subset R_i$$

есть правый идеал, и в силу простоты идеала R_i

$$a_{ij}R_j = R_i.$$

Выберем в каждой из линейных систем A_{ij} по элементу e_{ij} следующим образом: в качестве e_{ii} возьмём идемпотенты e_i. Затем внутри

$$A_{12}, A_{13}, \ldots, A_{1s}$$

выберем $e_{12}, e_{13}, \ldots, e_{1s}$ произвольно, но так, чтобы

$$e_{1i}R_i = R_1 \qquad (i = 2, 3, \ldots, s). \tag{10.7}$$

Далее, определим e_{i1} из уравнений

$$e_{1i}e_{i1} = e_{11} \qquad (i = 2, 3, \ldots, s) \tag{10.8}$$

(это всегда выполнимо, так как, умножая (10.7) справа на L_1, мы будем иметь

$$e_{1i}A_{i1} = A_{11},$$

а потому уравнение (10.8) всегда имеет решение).
Наконец, определим e_{ij} при помощи формул

$$e_{ij} = e_{i1}e_{1j} \qquad (i, j = 2, 3, \ldots, s).$$

Тогда имеет место

$$e_{ij}e_{jk} = e_{i1}e_{1j}e_{j1}e_{1k} = e_{i1}e_1e_{1k} = e_{i1}e_{1k} = e_{ik}.$$
$(e_{i1}e_1 = e_{i1}$, так как e_{i1} лежит в $A_{i1} = R_iL_1 = e_iAe_1)$.
$$e_{ij}e_{rk} = e_{i1}e_{1j}e_{r1}e_{1k} = 0 \qquad (j \neq r),$$

так как $e_je_r = 0$.

Все элементы e_{ij} линейно независимы в силу однозначности разложения

$$A = \sum_{i,\ j} A_{ij} \tag{10.9}$$

и удовлетворяют равенствам, определяющим базис полной матричной алгебры. Обозначим алгебру с этим базисом через M_s.

Для выделения внутри A тела, элементы которого перестановочны с M_s, предварительно заметим, что алгебра A_{11} есть тело. В самом деле, в противном случае его главная единица e_1 распадалась бы на сумму идемпотентов, при помощи которых R_1 разлагался бы в сумму правых идеалов, что противоречит простоте R_1.

Построим новое тело, изоморфное с A_{11}, элементы которого были бы перестановочны с элементами алгебры M_s. Имеет место

$$A_{11} = R_1 \cdot L_1 = e_{11}Ae_{11}.$$

Приведём в соответствие с каждым элементом $e_{11}ae_{11}$ алгебры A_{11}, где a — произвольный элемент алгебры A, элемент

$$e_{11}ae_{11} + e_{21}ae_{12} + \ldots + e_{s1}ae_{1s}.$$

Это соответствие является изоморфизмом, так как сумме элементов $e_{11}ae_{11}$, $e_{11}be_{11}$ соответствует сумма

$$e_{11}(a+b)e_{11}+e_{21}(a+b)e_{12}+\ldots+e_{s1}(a+b)e_{1s},$$

а произведению $e_{11}ae_{11}\cdot e_{11}be_{11}$ — произведение

$$(e_{11}ae_{11}+e_{21}ae_{12}+\ldots+e_{s1}ae_{1s})(e_{11}be_{11}+e_{21}be_{12}+\ldots+$$
$$+e_{s1}be_{1s})=e_{11}ae_{11}\cdot e_{11}be_{11}+e_{21}(e_{11}ae_{11}\cdot e_{11}be_{11})e_{12}+\ldots+$$
$$+e_{s1}(e_{11}ae_{11}\cdot e_{11}be_{11})e_{1s}.$$

Каждый из образованных таким образом элементов перестановочен со всеми e_{ij}:

$$(e_{11}ae_{11}+e_{21}ae_{12}+\ldots+e_{s1}ae_{1s})e_{ij}=e_{i1}ae_{1j},$$
$$e_{ij}(e_{11}ae_{11}+e_{21}ae_{12}+\ldots+e_{s1}ae_{1s})=e_{i1}ae_{1j}.$$

Обратно, каждому такому элементу однозначно соответствует элемент из A_{11}, так как

$$e_{11}(e_{11}ae_{11}+e_{21}ae_{12}+\ldots+e_{s1}ae_{1s})e_{11}=e_{11}ae_{11}.$$

Обозначим полученное тело через K. Докажем, что прямое произведение $K\times M_s$ исчерпывает всю алгебру A. В самом деле,

$$e_{ij}(e_{11}ae_{11}+e_{21}ae_{12}+\ldots+e_{s1}ae_{1s})=e_{i1}ae_{1j}\subset A_{ij},$$

причём

$$e_{i1}Ae_{1j}=A_{ij},$$

так что в форме

$$e_{ij}\cdot k\quad(k\subset K)$$

можно представить всякий элемент алгебры A_{ij}. С другой стороны, из (10.9) следует, что всякий элемент алгебры A может быть представлен в форме

$$a=\sum_{i,\,j}e_{ij}k_{ij},\quad k_{ij}. \tag{10.10}$$

Это представление однозначно, так как из равенства

$$0=\sum_{ij}e_{ij}k_{ij},$$

умножая его слева на e_{1i} и справа на e_{j1}, мы получим

$$e_{11}k_{ij}=0;$$

если

$$k_{ij}=e_{11}ae_{11}+e_{21}ae_{12}+\ldots+e_{s1}ae_{1s},$$

то

$$e_{11}k_{ij} = e_{11}ae_{11} = 0,$$

и далее

$$e_{\nu 1}(e_{11}k_{ij})\,e_{1\nu} = e_{\nu 1}k_{ij}e_{1\nu} = 0 \qquad (\nu = 1,\ 2,\ \ldots,\ s),$$

так что

$$k_{ij} = 0 + 0 + \ldots + 0 = 0.$$

Теорема доказана.

Имеет место также обратная теорема.

Теорема 26. *Всякое прямое произведение полной матричной алгебры на тело есть простая алгебра.*

Доказательство. Допустим противное: пусть это произведение имеет двусторонний идеал D и пусть

$$\sum_{i,\ j} e_{ij}k_{ij} \subset D,$$

причём пусть $k_{ij} \neq 0$. Отсюда

$$e_{\mu i}\Big(\sum_{i,\ j} e_{ij}k_{ij}\Big)e_{j\nu} = e_{\mu\nu}k_{ij} \subset D \qquad (\mu,\ \nu = 1,\ 2,\ \ldots,\ s);$$

умножая на элемент, обратный к k_{ij}, получим

$$e_{\mu\nu} \subset D \qquad (\mu,\ \nu = 1,\ 2,\ \ldots,\ s),$$
$$e_{\mu\nu}k_{\mu\nu} \subset D \qquad (\mu,\ \nu = 1,\ 2,\ \ldots,\ s)$$

при любом $k_{\mu\nu} \subset K$, откуда следует, что любой элемент алгебры A содержится в D, ч. и т. д.

Теорему 25 можно ещё формулировать так:

Всякий элемент простой алгебры может быть представлен как матрица с элементами из некоторого косого поля.

УПРАЖНЕНИЯ

1) Если алгебра A содержит полную матричную алгебру M и главные единицы этих алгебр совпадают, то $A = M \times C$, где алгебра C есть совокупность элементов, перестановочных с каждым элементом из M (принято обозначение $C = A^M$).

2) *Нормальной* называется алгебра, центр которой совпадает с Ω. Если $A = B \times C$, где B — нормальная алгебра, то $C = A^B$. Таким образом задание одного множителя B (если он нормальный) вполне определяет другой множитель C.

3) Если $A = B \times C$ нормальна, то нормальны B и C.

4) Если $A = B \times C$ проста, то просты B и C.

§ 11. ПОЛЯ РАЗЛОЖЕНИЯ

Дальнейшее изучение тел встречает трудности арифметического характера. Основным инструментом в дальнейших исследованиях является расширение центра изучаемого тела.

Предварительно докажем следующую вспомогательную теорему.

Теорема 27. *Произведение нескольких полных матричных алгебр*

$$M_{s_1},\ M_{s_2},\ \ldots,\ M_{s_k}$$

есть полная матричная алгебра

$$M_{s_1 s_2 \cdots s_k}.$$

Доказательство. Достаточно доказать теорему для случая двух алгебр. Пусть

$$M_s = [\ldots a_{ij} \ldots] \qquad (i,\ j = 1,\ 2,\ \ldots,\ s)$$
$$M_t = [\ldots b_{ij} \ldots] \qquad (i,\ j = 1,\ 2,\ \ldots,\ t)$$

две полные матричные алгебры измерений s, t, так что

$$a_{ij}a_{jk} = a_{ik}, \quad a_{ij}a_{rk} = 0 \quad (j \neq r),$$
$$b_{ij}b_{jk} = b_{ik}, \quad b_{ij}b_{rk} = 0 \quad (j \neq r);$$

кроме того, пусть элементы a_{ij} перестановочны с элементами b_{ij}. Положим

$$e_{\mu+s(\nu-1),\ \rho+s(\sigma-1)} = a_{\mu\rho}b_{\nu\sigma} \qquad (\mu,\ \rho = 1,\ 2,\ \ldots,\ s;\ \nu,\ \sigma = 1,\ 2,\ \ldots,\ t).$$

Нетрудно понять, что всякое целое положительное число $p \leqslant st$ можно, и притом однозначно, представить в форме $\mu + s(\nu - 1)$. Составим произведение

$$e_{\mu+s(\nu-1),\ \rho+s(\sigma-1)} \cdot e_{\alpha+s(\beta-1),\ \gamma+s(\delta-1)} = a_{\mu\rho}b_{\nu\sigma}a_{\alpha\gamma}b_{\beta\delta} = a_{\mu\rho}a_{\alpha\gamma}b_{\nu\sigma}b_{\beta\delta}.$$

Если хоть одно из равенств

$$\rho = \alpha,\ \sigma = \beta$$

не выполняется, то это произведение равно нулю. Если же оба они выполняются, то оно равно

$$a_{\mu\gamma}b_{\nu\delta} = e_{\mu+s(\nu-1),\ \gamma+s(\delta-1)},$$

откуда

$$e_{pq}e_{uv} = 0 \quad (q \neq u), \quad e_{pq}e_{qv} = e_{pv}$$
$$(p, q, u, v = 1, 2, \ldots, st).$$

Эти равенства показывают, что

$$M_s \times M_t = M_{st}.$$

Применяя этот результат постепенно к произведению первых двух множителей, затем к полученному произведению и третьему множителю и т. д., мы докажем теорему в полном объёме.

Пусть D — тело порядка n над полем Ω. D может быть задано базисом

$$[a_1, a_2, \ldots, a_n]$$

и константами γ_{ij}^{s}, где

$$a_i a_j = \sum_{s=1}^{n} \gamma_{ij}^{s} a_s. \tag{11.1}$$

Будем предполагать, что центр этого тела состоит только из элементов

$$\xi \cdot e,$$

где e — главная единица алгебры D, а ξ пробегает поле Ω. В этом случае алгебра D называется *нормальной*.

Теперь рассмотрим прямое произведение

$$\Omega_1 \times D,$$

где $\Omega_1 \supset \Omega$ — новое коммутативное поле. Элементы этого произведения могут быть представлены так:

$$\alpha^1 a_1 + \alpha^2 a_2 + \ldots + \alpha^n a_n,$$

где α^i пробегают поле Ω_1. Константы γ_{ij}^{s} остаются теми же. Из соотношений (11.1), которым вполне определяется тело D, нельзя вывести линейных соотношений между a_i над полем Ω_1, так что мы имеем право предположить линейную независимость элементов базиса a_i и в алгебре $\Omega_1 \times D$ и её порядок будет попрежнему равен n.

Докажем, что в алгебре $\Omega_1 \times D$ центром является $\Omega_1 \times e$. Положим $a_1 = e$ и поставим требование, чтобы элемент

$$y = \eta^1 a_1 + \eta^2 a_2 + \ldots + \eta^n a_n$$

был перестановочен с любым элементом

$$x = \xi^1 a_1 + \xi^2 a_2 + \ldots + \xi^n a_n$$

алгебры $\Omega_1 \times D$: $xy = yx$. Полагая $x = a_i$, получим

$$\eta^1 (a_1 a_i - a_i a_1) + \eta^2 (a_2 a_i - a_i a_2) + \ldots + \eta^n (a_n a_i - a_i a_n) = 0 \quad (i = 1, 2, \ldots, n).$$

Из нашего условия относительно D следует, что эта система уравнений (которые можно представить как линейные уравнения относительно η^i) не имеет в поле Ω других решений, кроме

$$\eta_2 = \eta_3 = \ldots = \eta_n = 0$$

(неизвестная η^1 в них не входит, так как в силу $a_1 = e$ имеем при всяком i $a_1 a_i - a_i a_1 = 0$). Если бы в поле эта система имела другое решение, то из неё вытекали бы линейные соотношения между a_i над полем Ω_1, чего мы не предполагаем. Отсюда

$$y = \eta^1 \cdot e,$$

что и требовалось доказать.

Алгебра $\Omega_1 \times D$ полупроста. Это следует из того, что условие полупростоты

$$|S(a_i a_j)| \neq 0,$$

предполагаемое для алгебры D, сохраняет силу и в $\Omega_1 \times D$.

Алгебра $\Omega_1 \times D$ проста, как это следует из теоремы 21 и из того, что центр алгебры $\Omega_1 \times D$ есть поле $\Omega_1 e$.

Исследуем вопрос, является ли алгебра $\Omega_1 \times D$ телом. Это имеет место не всегда. Обратно, мы покажем, что для каждого тела D существует поле Ω_1, для которого алгебра $\Omega_1 \times D$ является полной матричной алгеброй над Ω_1. В этом случае поле Ω_1 носит название *поля разложения* тела D.

Теорема 28. *Каждое тело D имеет поле разложения.*

Доказательство. Возьмём произвольный элемент a*) тела D и составим ряд его степеней:

$$e = a^0, \ a, \ a^2, \ \ldots, \ a^n.$$

---

*) Предположим, что a не входит в центр алгебры D,

Их число $n+1$, а потому между ними должна иметь место линейная зависимость. Таким образом a удовлетворяет уравнению

$$f(a)\cdot e=0,$$

где

$$f(x)=x^n+p_1x^{n-1}+\ldots+p^n$$

и все коэффициенты p_i лежат в Ω. Пусть корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ этого полинома образуют поле Ω_1. Тогда имеет место равенство

$$f(a)\cdot e=(a-\alpha_1 e)(a-\alpha_2 e)\ldots(a-\alpha_n e)=0,$$

где ни один элемент $a-\alpha_i e$ поля $\Omega_1\times D$ не может быть равен нулю, так как в этом случае a было бы перестановочно со всеми элементами алгебры $\Omega_1\times D$. Поэтому

$$\Omega_1\times D=D_1\times M_{s_1},$$

где D_1 — тело меньшего порядка, чем n, а M_{s_1} — полная матричная алгебра измерения s_1.

Продолжая такое же приведение для тела D_1, затем для вновь полученного тела и т. д., мы в конце концов придём к такому полю $\overline{\Omega}$, что

$$\overline{\Omega}\times D=M_{s_1}\times M_{s_2}\times\ldots\times M_{s_k},$$

или, в силу теоремы 27,

$$\overline{\Omega}\times D=M_{s_1 s_2\ldots s_k}. \tag{11.2}$$

Эта формула показывает, что $\overline{\Omega}$ есть искомое поле разложения.

В формуле (11.2) порядок алгебры в левой части равен n, а в правой $(s_1\cdot s_2\ldots s_k)^2$. Отсюда следует

Теорема 29. *Порядок всякого нормального тела* (скажем общее: всякой нормальной простой алгебры) *равен квадрату целого рационального числа.* Введём новое понятие *степени* простой алгебры, т. е. степень полинома наименьшей степени, который обращается в нуль, если вместо переменной x мы подставим произвольный элемент

$$a=\xi^1a_1+\xi^2a_2+\ldots+\xi^na_n$$

алгебры. (Мы должны считать ξ^i не элементами поля Ω, а переменными, которые должны также войти в коэффициенты

полинома.) При доказательстве теоремы 28 мы видели, что степень не может быть выше порядка алгебры.

Теорема 30. *Если $f(x)$ — полином наименьшей степени, для которого имеет место $f(a) \cdot e = 0$, то всякий другой полином $F(x)$, для которого имеет место $F(a)\, e = 0$, делится на $f(x)$.*

Доказательство. Пусть при делении $F(x)$ на $f(x)$ мы получили остаток $r(x)$, степень которого ниже, чем степень $f(x)$. Подставляя в тождество

$$F(x) = f(x) \cdot q(x) + r(x)$$

$x = a$, получим

$$F(a)\, e = f(a) \cdot q(a) \cdot e + r(a)\, e = 0,$$

т. е.

$$r(a)\, e = 0,$$

что противоречит определению $f(x)$.

Будем для краткости называть полиномом $f(x)$ наименьшей степени, для которого

$$f(a) \cdot e = 0,$$

главным полиномом для a.

Определим степень нормальной простой алгебры A порядка m^2. Имеет место

Теорема 31. *Степень нормальной простой алгебры A порядка m^2 равна m.*

Доказательство. Пусть $\bar{\Omega}$ есть поле разложения алгебры A. Тогда имеет место

$$\bar{\Omega} \times A = M_m.$$

Из теории матриц известно, что всякая матрица m-го измерения удовлетворяет уравнению степени m (характеристическое уравнение) и что это уравнение совпадает с главным, если выбрать матрицу так, чтобы её характеристические корни были различны. Если мы выберем в качестве базиса алгебры $\bar{\Omega} \times A$ базис алгебры A, то для

$$a = \xi' a_1 + \xi^2 a_2 + \ldots + \xi^{m^2} a_{m^2}$$

получим тоже полином наименьшей степени m. Если при этом считать ξ^i входящими в поле Ω (или же считать их независимыми

переменными), то коэффициенты этого полинома тоже будут лежать в поле Ω, так как степени

$$e,\ a,\ a^2,\ \ldots,a^m,$$

линейно выраженные через базис, должны быть линейно зависимы, и эта зависимость выразится через ξ^i и γ_{ij}^s (последние по условию лежат в Ω). Таким образом степень нормальной простой алгебры m^2-го порядка равна m.

Пример. Разобранное в примере I § 4 тело кватернионов имеет базис

$$[1,\ i,\ j,\ k],$$

где

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i,$$
$$ki = -ik = j.$$

Здесь $m^2 = 4$, следовательно, $m = 2$. В самом деле, элемент

$$a = \alpha + \frac{\beta i}{2} + \frac{\gamma}{2} j + \frac{\delta}{2} k \tag{11.3}$$

удовлетворял уравнению

$$a^2 - 2\alpha \cdot a + \left(\alpha^2 + \frac{\beta^2}{4} + \frac{\gamma^2}{4} + \frac{\delta^2}{4}\right) = 0. \tag{11.4}$$

Чтобы найти для этого тела поле разложения, достаточно найти поле, в котором существует правый идеал. Мы видели, что для последнего достаточно, чтобы алгебра содержала идемпотент, отличный от главной единицы (см. теорему 24 и разложение (10.1). Но чтобы элемент a был идемпотентом, т. е. удовлетворял уравнению

$$a^2 - a = 0,$$

необходимо положить в уравнении (11.4)

$$2\alpha = 1, \quad \beta^2 + \gamma^2 + \delta^2 = -1. \tag{11.5}$$

Итак, чтобы Ω_1 было полем разложения, необходимо, чтобы в нём -1 представлялась как сумма трёх квадратов. Но это и достаточно, так как в этом случае $\Omega_1 \times A$ будет содержать полную матричную алгебру 2-го измерения и поэтому будет с ней совпадать.

Нетрудно видеть, что полем разложения является $\mathfrak{Q}(\sqrt{-1})$, так как уравнения (11.5) имеют решение

$$\alpha=\frac{1}{2},\quad \beta=\sqrt{-1},\quad \gamma=\delta=0,$$

и искомый идемпотент таков:

$$\frac{1}{2}+i\cdot\sqrt{-1}.$$

Известно, что существуют (мнимые) циклические поля сколь угодно высокой степени, в которых -1 разлагается в сумму трёх (и даже двух) квадратов. Такие поля являются полями разложения для алгебры кватернионов, притом *минимальными* в том смысле, что всякое подполе такого поля уже не является полем разложения для алгебры кватернионов. В самом деле, в циклических полях каждое подполе вполне определяется своей степенью и, в частности, входит в вещественное поле, степень которого вдвое меньше степени заданного поля. Но в вещественных полях -1 не может быть представлена как сумма квадратов.

УПРАЖНЕНИЯ

1) Чтобы элемент алгебры был регулярным (т. е. имел обратный), необходимо и достаточно, чтобы его главный полином имел отличный от нуля свободный член.

2) В любом поле главный полином для каждого элемента неприводим.

3) Всякую алгебру порядка n с главной единицей можно рассматривать как подалгебру полной матричной алгебры измерения n (т. е. порядка n^2): $A\subset M_n$ (представление первого рода). Тогда её представления второго рода образуют тоже алгебру A^{-1} порядка n, поэлементно перестановочную с A. Имеет место

$$A^{-1}=M_n^A.$$

Кроме того, $A\times A^{-1}=M_n$.

4) Если алгебра A содержит нормальную простую подалгебру B и главные единицы у A и B совпадают, то $A=B\times C$, где $C=A^B$.

5) Если A — простая алгебра и $A=M_t\times D=M_s\times C$, где D — тело, то t делится на S.

6) Если B и D — некоторые тела, а их прямое произведение есть полная матричная алгебра, то $B=D^{-1}$,

§ 12. АВТОМОРФИЗМЫ ПРОСТЫХ АЛГЕБР

В теории простых алгебр имеет большое значение изучение *автоморфизмов*, т. е. изоморфных отображений алгебр самих на себя. Среди них особую роль играют *внутренние автоморфизмы*, т. е. автоморфизмы, получаемые при помощи преобразования всех элементов алгебры каким-либо одним элементом той же алгебры. Именно, пусть s — элемент алгебры A, имеющий обратный. Тогда, если мы установим соответствие

$$a \to s^{-1}as,$$
$$b \to s^{-1}bs$$

для всех элементов алгебры A, то, очевидно, будет иметь место

$$a \pm b \to s^{-1}(a \pm b)s = s^{-1}as \pm s^{-1}bs,$$
$$ab \to s^{-1}(ab)s = s^{-1}as \cdot s^{-1}bs.$$

Для простых нормальных алгебр можно установить весьма простой факт.

Теорема 32. *Все автоморфизмы нормальной простой алгебры суть внутренние автоморфизмы.*

Доказательство. 1° Сначала докажем теорему для полной матричной алгебры M_n. Пусть S — автоморфизм, переводящий каждую e_{ij} в f_{ij}:

$$e_{ij}^S = f_{ij} \quad (i, j = 1, 2, \ldots, n),$$

и пусть

$$f_{ij} = \sum_{\nu} d_{ij}e_{ij} \quad (i, j = 1, 2, \ldots, n;\ (d_{ij} \subset \Omega)).$$

Пусть $d_{pq} \neq 0$. Введём элементы

$$a = d_{pq}^{-1}e_{1p}f_{11}, \quad b = f_{11}e_{q1}.$$

Между e_{ij}, а также между f_{ij} имеют место обычные матричные соотношения и, в частности, $f_{11}^2 = f_{11}$, а потому

$$ab = d_{pq}^{-1}e_{1p}f_{11}e_{q1} = d_{pq}^{-1}e_{1p}\sum_{i,j} d_{ij}e_{ij}e_{q1} = d_{pq}^{-1}d_{pq}e_{11} = e_{11}.$$

С другой стороны,

$$ba = f_{11}d_{pq}^{-1}e_{qp}f_{11},$$

так что, если

$$e_{qp} = \sum_{i,j} u_{ij} f_{ij},$$

то

$$ba = d_{pq}^{-1} u_{11} \cdot f_{11}.$$

Но $(ba)^2 = b(ab)\, a = f_{11} e_{q1} e_{11} d_{pq}^{-1} e_{1p} f_{11} = d_{pq}^{-1} f_{11} e_{qp} f_{11} = ba$,

т. е. ba есть идемпотент. Отсюда

$$(d_{pq}^{-1} u_{11} f_{11})^2 = (d_{pq} u_{11} f_{11}),$$

т. е.

$$(d_{pq}^{-1} u_{11}) = 1, \quad ba = f_{11}.$$

Введём элементы

$$h = \sum_i e_{i1} a f_{1i}, \quad g = \sum_j f_{j1} b e_{1j}.$$

Имеем

$$hg = \sum_i e_{i1} a f_{1i} f_{i1} b e_{1i} = \sum_i e_{i1} a f_{11} b e_{1i} = \sum_i e_{ii} = 1,$$

откуда

$$h = g^{-1}.$$

Нетрудно убедиться, что наш автоморфизм осуществляется преобразованием $g(\ldots)g^{-1}$. В самом деле,

$$ge_{\mu\nu}g^{-1} = ge_{\mu\nu}h = \sum_{j,i} f_{j1} b e_{1j} e_{i1} a f_{1i} =$$
$$= f_{\mu 1} b e_{11} a f_{1\nu} = f_{\mu 1} f_{11} f_{1\nu} = f_{\mu\nu} = e_{\mu\nu}^{\mathcal{B}}.$$

Преобразованием же базиса определяется весь автоморфизм.

2° Докажем теорему в общем случае. Пусть нормальная простая алгебра A имеет поле разложения k, так что

$$A_k = M_n.$$

Распространим заданный автоморфизм S на A_k, считая, что элементы поля k инвариантны относительно автоморфизма S. Тогда, как мы уже доказали, в алгебре $A_k = M_n$ существует элемент g такого рода, что автоморфизм S осуществляется преобразованием $g(\ldots)g^{-1}$. Докажем, что и в алгебре A можно найти такого рода элемент. Пусть

$$[u_1, u_2, \ldots, u_{n^2}]$$

—базис алгебры A и пусть

$$g = \sum_i \xi_i u_i, \quad \xi_i \subset k.$$

Тогда

$$u_i^g = g u_i g^{-1} \qquad (i = 1, 2, \ldots, n^2),$$

откуда

$$u_i^g \sum_\nu \xi_\nu u_\nu = \sum_\nu \xi_\nu u_\nu \cdot u_i \; (i = 1, 2, \ldots, n^2).$$

Зная выражения u_i^g через u_i и пользуясь таблицей умножения алгебры A, мы получим систему линейных однородных уравнений относительно ξ_ν, коэффициенты которых лежат в Ω. Эта система, как мы знаем, имеет решение в поле k такого рода, что $g = \sum_\nu \xi_\nu u_\nu$ есть регулярный элемент, т. е. определитель, соответствующий ему в представлении матрицы, отличен от нуля. Это значит, что если мы выразим переменные ξ_ν при помощи линейных уравнений через систему независимых и затем подставим эти выражения в выражение определителя, то получим однородный полином с коэффициентами из Ω, не равный тождественно нулю. Если мы теперь выберем для переменных ξ_ν значения из Ω, не обращающие этот полином в нуль, то соответствующий этим значениям элемент $g = \sum_\nu \xi_\nu u_\nu$ регулярен, и преобразование $g(\ldots)g^{-1}$ осуществляет заданный автоморфизм S. Итак все автоморфизмы нормальной простой алгебры A внутренние, ч. и т. д.

§ 13. ТЕЛА КАК СКРЕЩЕННЫЕ ПРОИЗВЕДЕНИЯ

Целью настоящего параграфа является сведение тел к особой форме алгебр, которые Э. Нётер назвала *скрещенными произведениями*. Для этого предварительно нужно доказать несколько теорем.

Теорема 33. *Пусть D — тело порядка m^2, Z — его поле разложения. Тогда степень поля Z делится на m:*

$$n = rm. \tag{13.1}$$

Доказательство. Алгебра

$$M = Z \times D$$

есть полная алгебра матриц m-го порядка.

Пусть

$$e_{ik} \qquad (i,\ k = 1,\ 2,\ \ldots,\ m)$$

система её матричных единиц. Рассмотрим её правый идеал

$$R = e_{11}M = e_{11}v_1 + e_{12}v_2 + \ldots + e_{1m}v_m,$$

где v_1, v_2, ..., v_m пробегают поле Z. Определим двояким путём порядок этой алгебры. С одной стороны, в R можно выделить D-базис, т. е. систему элементов

$$[u_1,\ u_2,\ \ldots,\ u_r],$$

между которыми не существует соотношений

$$u_1\xi_1 + u_2\xi_2 + \ldots + u_r\xi_r = 0$$

и таких, что в форме $u_1\xi_1 + u_2\xi_2 + \ldots + u_r\xi_r$ может быть представлен всякий элемент алгебры R.

В самом деле, пусть $u_1 \subset R$. Тогда в силу того, что R есть правый идеал алгебры M, при всяком $\xi_1 \subset D$ имеет место $u_1\xi_1 \subset R$. Если произведениями $u_1\xi_1$ идеал R не исчерпывается, возьмём в R элемент u_2, не представляемый в форме $u_1\xi_1$. Тогда при всяких $\xi_1 \subset D$, $\xi_2 \subset D$ имеет место $u_1\xi_1 + u_2\xi_2 \subset R$. Если в этой форме идеал R не исчерпывается, возьмём непредставимый в этой форме элемент u_3 и будем продолжать процесс до исчерпания идеала R. Полученная система $[u_1,\ u_2,\ \ldots,\ u_r]$ является D-базисом идеала R. В самом деле, если бы какой-нибудь элемент идеала R мог быть представлен через эту систему двумя различными способами, то имело бы место

$$u_1\xi_1 + u_2\xi_2 + \ldots + u_r\xi_r = 0, \quad \xi_i \subset D,$$

где не все ξ_i равны нулю. Если ξ_k — последний не равный нулю элемент, то, разделив справа соотношение на ξ_k^{-1} (ведь D — косое поле), получим

$$u_k = -u_1\xi_1\xi_k^{-1} - u_2\xi_2\xi_k^{-1} - \ldots - u_{k-1}\xi_{k-1}\xi_k^{-1},$$

что противоречит способу выбора элемента u_k.

Если r есть порядок D-базиса алгебры R, то порядок R относительно Ω есть rm^2. С другой стороны, алгебра R имеет порядок m относительно поля Z, а потому её порядок относительно поля Ω равен mn.

Итак,

$$rm^2 = mn,$$

откуда следует (13.1).

Теорема 34. *Пусть тело D порядка m^2 имеет поле разложения Z степени $n = rm$. Тогда алгебра*

$$A = D \times M_r,$$

где M_r — полная матричная алгебра измерения r, содержит поле (притом максимальное), *изоморфное с Z.*

Доказательство. Рассмотрим опять D-базис $[u_1, u_2, \ldots, u_r]$ алгебры $R = e_{11}M$, где $M = Z \times D$. Представляя при помощи этого базиса элементы поля Z:

$$zu_i = u_i z = u_1\alpha_{i1} + u_2\alpha_{i2} + \ldots + u_r\alpha_{ir} \qquad (i = 1, 2, \ldots, r),$$

где

$$z \subset Z, \qquad \alpha_{ik} \subset D,$$

мы получим представление поля Z матрицами измерения r с коэффициентами из D. Это представление изоморфно, так как из

$$u_i z = 0 \qquad (i = 1, 2, \ldots, r)$$

вытекает

$$e_{11}z = 0, \quad e_{12}z = 0, \ldots, e_{1r}z = 0,$$

и если

$$z = \sum_{i,k} \beta_{ik} e_{ik},$$

то

$$\sum_k \beta_{1k}e_{1k} = 0, \quad \sum_k \beta_{2k}e_{1k} = 0, \ldots, \quad \sum_k \beta_{rk}e_{1k} = 0,$$

откуда

$$\beta_{ik} = 0 \qquad (i, k = 1, 2, \ldots, r),$$

т. е.

$$z = 0.$$

Но поскольку A состоит из *всех* матриц измерения r с коэффициентами из D, A содержит поле, изоморфное с этим представлением поля Z, т. е. изоморфное с полем Z. Это поле максимально, так как алгебра A имеет порядок $m^2 \cdot r^2$ и потому не может содержать полей порядка выше $m \cdot r$.

Пусть A — нормальная простая алгебра порядка $n^2 = m^2 \cdot r^2$ (степень m наибольшего содержащегося в ней тела мы будем называть *индексом* алгебры A) и пусть Z — её

максимальное поле степени $m \cdot r$. Предположим, что Z нормально (в смысле теории Галуа). Это существенно не ограничивает исследования. В самом деле, если Z не нормально, то существует нормальное поле $Z_1 \supset Z$ степени $n_1 = m \cdot r \cdot r_1$. Тогда алгебра

$$A \times M_{r_1} = D \times M_r \times M_{r_1} = D \times M_{rr_1},$$

в силу теоремы 35, содержит поле, изоморфное с нормальным полем Z_1. Алгебра же A составляет подалгебру алгебры $A \times M_{r_1}$.

Пусть z — примитивный элемент поля Z. Его характеристический полином не имеет кратных корней. Элемент z^S (т. е. элемент z, над которым произведён автоморфизм S группы Galois $\mathfrak{G}$ поля Z/Ω) удовлетворяет тому же характеристическому уравнению, что и z, а потому в алгебре A существует такой элемент u_S, что

$$z^S = u_S^{-1} z u_S. \tag{13.2}$$

Пусть группа Galois поля Z/Ω

$$\mathfrak{G} = \mathfrak{e} + S_2 + \ldots + S_n.$$

Определим для каждого автоморфизма этой группы по элементу u_S, удовлетворяющему условию (13.2). Заметим, что выбор u_S не зависит от выбора z внутри Z, так как из (13.2) следует

$$\varphi(z^S) = u_S^{-1} \varphi(z) u_S.$$

Пусть

$$[z_1, z_2, \ldots, z_n]$$

есть Ω — базис поля Z. Докажем, что система

$$[\ldots u_{Si} \cdot z_j \ldots] \qquad [i, j = 1, 2, \ldots, n)$$

составляет Ω-базис алгебры A или что

$$[u_\mathfrak{e}, u_{S_2}, \ldots, u_{S_n}]$$

составляет Z-базис алгебры A. Прежде всего мы заключаем, что элемент

$$u_S u_T u_{ST}^{-1}$$

перестановочен с z:

$$u_S u_T u_{ST}^{-1} \cdot z = u_S u_T z^{ST} u_{ST}^{-1} = u_S z^{(ST)^{T^{-1}}} u_T u_{ST}^{-1} =$$
$$= z^{(ST)T^{-1}S^{-1}} u_S u_T u_{ST}^{-1} = z u_S u_T u_{ST}^{-1},$$

а потому, в силу максимальности поля Z, он содержится в Z. Обозначая его через $a_{S,T}$, будем иметь

$$u_S u_T = u_{ST} \cdot a_{S,T}, \quad a_{S,T} \subset Z. \tag{13.3}$$

Формулы (13.3) и (13.2), которые мы будем писать так:

$$z u_S = u_S z^S, \tag{13.4}$$

составляют таблицу умножения для алгебры, определяемой нашим базисом. В самом деле, пусть

$$a = \sum_S u_S x_S, \quad b = \sum_S u_S \cdot y_S, \tag{13.5}$$
$$x_S \subset Z, \quad y_S \subset Z.$$

Тогда

$$a \cdot b = \sum_{S,T} u_S x_S u_T y_T = \sum_{S,T} u_S u_T x_S^T y_T =$$
$$= \sum_{S,T} u_{ST} \cdot a_{S,T} x_S^T \cdot y^T,$$
$$a_{S,T} x_S^T y_T \subset Z,$$

т. е. ab тоже представилось в форме (13.5).

Докажем, что построенная нами алгебра исчерпывает всю алгебру A. Для этого достаточно доказать независимость элементов u_S Z-базиса, так как этим мы покажем, что порядок этой алгебры есть n^2, т. е. равен порядку алгебры A.

Допустим существование линейной зависимости

$$\sum_S u_S y_S = 0, \quad y_S \subset Z. \tag{13.6}$$

Умножим эту зависимость слева на примитивный элемент z поля Z, затем справа на z^T, где T — один из автоморфизмов группы $\mathfrak{G}$, такой, что $y_T \neq 0$, и вычтем друг из друга оба полученные равенства:

$$\sum_S u_S y_S (z^S - z^T) = 0. \tag{13.7}$$

Если при каком-нибудь u_S в (13.6) коэффициент не был равен нулю, то он не будет нулём и в (13.7), за исключением коэффициента при u_T, который в (13.7) равен нулю. Постепенно изгоняя из равенства таким путём все члены, мы в конце концов придём к соотношению с одним заранее указанным членом. Значит, в нём $y_S = 0$, и так с каждым членом.

Всё доказанное можно формулировать в виде следующей теоремы:

Теорема 35. *Всякая нормальная простая алгебра является подалгеброй некоторой алгебры, называемой скрещенным произведением, которая задаётся нормальным полем Z степени n, а также n независимыми элементами u_S, соответствующими автоморфизмам S группы* Galois *поля Z, удовлетворяющими соотношениям*

$$zu_S = u_S z^S, \tag{13.8}$$

$$u_S u_T = u_{ST} a_{S,T}, \quad a_{S,T} \subset Z. \tag{13.9}$$

Скрещенное произведение, заданное полем Z и константами $a_{S,T}$, принято обозначать так:

$$(a, Z).$$

Теорема 36. *Всякое скрещенное произведение*

$$A = (a, Z)$$

есть нормальная простая алгебра.

Доказательство. Докажем прежде всего, что Z есть максимальное поле алгебры A. Если

$$a = \sum_S u_S y_S$$

перестановочно со всеми z, т. е. если

$$az = za,$$

то

$$\sum_S u_S y_S (z - z^S) = 0.$$

Но если z — примитивный элемент поля Z, то $z - z^S = 0$ только для $S = \varepsilon$. Отсюда в силу независимости элементов u_S

$$y_S (z - z^S) = 0,$$

или

$$y_S = 0 \quad \text{при} \quad S \neq \mathfrak{e},$$

т. е.

$$a = u_{\mathfrak{e}} y_{\mathfrak{e}}.$$

Поле, образованное такого рода элементами, изоморфно с Z.

Теперь предположим, что a лежит в центре. Тогда $a = y_{\mathfrak{e}}$ и, кроме того,

$$u_S \cdot y_{\mathfrak{e}} = y_{\mathfrak{e}} \cdot u_S,$$

т. е.

$$u_S \cdot y_{\mathfrak{e}} = u_S \cdot y_{\mathfrak{e}}^S,$$

откуда

$$y_{\mathfrak{e}}^S = y_{\mathfrak{e}}.$$

Но так как под S мы можем разуметь любой автоморфизм группы $\mathfrak{G}$, то $y_{\mathfrak{e}} \subset \Omega$, откуда следует, что алгебра A нормальна.

Наконец, докажем, что алгебра A проста. Пусть B — её двусторонний идеал и пусть

$$b = \sum_S u_S y_S \subset B.$$

Тогда в B будут также содержаться элементы

$$zb = \sum_S z u_S y_S = \sum_S u_S z^S y_S,$$

$$b\bar{z} = \sum_S u_S y_S \bar{z},$$

а также

$$b_1 = zb - b\bar{z} = \sum_S u_S y_S (z^S - \bar{z}).$$

Беря в качестве z примитивный элемент поля Z и полагая $\bar{z} = z^T$, где T — любой автоморфизм группы $\mathfrak{G}$, мы получим элемент из B, у которого коэффициент при u_T равен нулю. Продолжая процесс, получим из B элемент типа

$$u_R y_R a_R, \quad a_R \neq 0,$$

т. е. элемент u_R. Из

$$u_R \subset B$$

следует для всякого $S \subset \mathfrak{G}$:

$$u_S = u_R \cdot u_{R,S}^{-1} \cdot a_{R,R}^{-1} {}^{-1}{}_S \subset B,$$

т. е. все элементы базиса $[u_e, u_{S_2}, \ldots, u_{S_n}]$ входят в B. Отсюда

$$B = A,$$

и A есть простая алгебра.

Теорема 37. *Пусть A — нормальная простая алгебра, Z — её максимальное поле. Тогда наименьшее нормальное поле Z^*, содержащее Z, есть поле разложения алгебры A.*

Доказательство. Образуем алгебру A^*, содержащую A, которая являлась бы скрещенным произведением (a, Z^*). Пусть

$$[u_e, u_{S_2}, \ldots, u_{S_n}]$$

есть Z^*-базис алгебры A^*. Найдём при его помощи представление алгебры A^* матрицами n-го измерения:

$$[u_e, u_{S_2}, \ldots, u_{S_n}]\, a = A\, [u_e, u_{S_2}, \ldots, u_{S_n}].$$

Коэффициенты матриц A лежат в Z. Это представление истинное, так как алгебра A^* проста. Но так как порядок алгебры A^* равен n^2, т. е. порядку полной матричной алгебры измерения n, то отсюда следует, что, присоединяя к полученной алгебре матриц поле Z^*, мы получим все матричные единицы измерения n, т. е. полную матричную алгебру M_n. Это показывает, что Z^* является полем разложения алгебры A^*, а с нею подавно и алгебры A.

§ 14. ЭЛЕМЕНТАРНЫЕ СВОЙСТВА СКРЕЩЕННЫХ ПРОИЗВЕДЕНИЙ

Константы $a_{S,T}$ скрещенных произведений играют большую роль при изучении структуры алгебр, а потому мы изучим их подробнее.

Можно, имея нормальное поле Z, задать совершенно произвольно константы $a_{S,T}$ для построения скрещенного произведения? Оказывается, что нет. В самом деле, из ассоциативного закона

$$(u_S u_T)\, u_V = u_S (u_T u_V)$$

мы имеем

$$u_{ST} a_{S,T} a_V = u_S u_{TV} a_{T,V},$$

$$u_{S,TV} a_{ST,V} a^V_{S,T} = u_{STV} a_{S,TV} a_{T,V},$$

откуда

$$a^V_{S,T} = \frac{a_{S,TV}\, a_{T,V}}{a_{ST,V}}. \tag{14.1}$$

Если это условие соблюдается, то скрещенное произведение, определяемое формулами

$$zu_S = u_S z^S, \tag{14.2}$$

$$u_S u_T = u_{ST} a_{S,T}, \tag{14.3}$$

удовлетворяет, как нетрудно убедиться, всем законам, которым должна подчиняться алгебра.

Как простая алгебра (a, Z) должна иметь главную единицу. Станем подыскивать её в форме

$$e = \sum_S u_S y_S,$$

подчиняя её условиям

$$eu_T = u_T e = u_T,$$

т. е.

$$\sum_S u_{ST} a_{S,T} y_S^T = \sum_S u_{TS} a_{T,S} y_S = u_T,$$

откуда в силу независимости Z-базиса

$$y_S = 0 \quad \text{при} \quad S \neq \varepsilon,$$

$$a_{\varepsilon,T} y_\varepsilon^T = 1, \quad a_{T,\varepsilon} y_\varepsilon = 1.$$

В частности,

$$y_\varepsilon = a^{-1}_{\varepsilon,\varepsilon},$$

и остаётся проверить, что

$$a_{T,\varepsilon} = a_{\varepsilon,\varepsilon},$$

$$a^T_{\varepsilon,\varepsilon} = a_{\varepsilon,T}.$$

Первую формулу мы получим, полагая в (14.1) $T = V = \varepsilon$:

$$a_{S,\varepsilon} = \frac{a_{S,\varepsilon}\, a_{\varepsilon,\varepsilon}}{a_{S,\varepsilon}} = a_{\varepsilon,\varepsilon}.$$

Вторая формула получается, если положить в (14.1) $S = T = \varepsilon$:

$$a^V_{\varepsilon,\varepsilon} = \frac{a_{\varepsilon,V} \cdot a_{\varepsilon,V}}{a_{\varepsilon,V}} = a_{\varepsilon,V}.$$

Таким образом главная единица алгебры (a, Z) есть

$$e = u_\varepsilon \cdot a_{\varepsilon,\varepsilon}^{-1}. \tag{14.4}$$

Мы не придём к противоречию, если положим

$$e = 1,$$

т. е.

$$u_\varepsilon = a_{\varepsilon,\varepsilon}. \tag{14.5}$$

Когда мы определяли из условия

$$zu_S = u_S z^S$$

матрицу u_S, то у нас в распоряжении оставался произвольный множитель — элемент поля Z. И в самом деле, если

$$u_S^{-1} z u_S = z^S,$$

то

$$(u_S c_S)^{-1} z\,(u_S c_S) = c_S^{-1}(u_S^{-1} z u_S)\, c_S = c_S^{-1} z^S c_S = z^S.$$

Обратно, из

$$u_S^{-1} z u_S = z^S, \quad \bar{u}_S^{-1} z \bar{u}_S = z^S$$

вытекает, что элемент $u_S^{-1}\bar{u}_S$ перестановочен с элементами поля Z и потому входит в Z, откуда

$$\bar{u}_S = u_S c_S, \quad c_S \subset Z. \tag{14.6}$$

Как изменятся константы $a_{S,T}$, если мы проделаем над Z-базисом преобразование (14.6). Если наряду с (14.2), (14.3) мы будем иметь

$$z\bar{u}_S = \bar{u}_S \cdot z^S, \quad \bar{u}_S \bar{u}_T = \bar{u}_{ST} \cdot \bar{a}_{S,T},$$

то отсюда при помощи (14.6) мы получим

$$u_S c_S u_T c_T = u_{ST} c_{ST} \cdot \bar{a}_{S,T},$$

т. е.

$$u_{ST} a_{S,T} c_S^T c_T = u_{ST} c_{ST} \cdot \bar{a}_{S,T},$$

откуда

$$\bar{a}_{S,T} = a_{S,T} \cdot \frac{c_S^T c_T}{c_{ST}}. \tag{14.7}$$

Обратно, если две системы констант (a) и $(\bar{a})$ связаны соотношениями (14.7), где c_S^T — произвольные элементы поля Z, то, производя обратное рассуждение, мы убедимся, что скрещенные произведения (a, Z) и $(\bar{a}, Z)$ совпадают.

Будем отмечать существование между двумя системами констант (a), $(\bar{a})$ соотношений (14.7) символом

$$(\bar{a}) \sim (a) \tag{14.8}$$

и говорить, что обе системы констант *эквивалентны*. Тогда в силу доказанного имеет место

Теорема 38. *Для того чтобы две системы констант* (a), $(\bar{a})$ *образовали одно и то же скрещенное произведение*:

$$(a, Z) = (\bar{a}, Z),$$

необходимо и достаточно, чтобы они были эквивалентны;

$$(a) \sim (\bar{a}).$$

В частности, если система констант (a) эквивалентна системе констант, состоящих из единиц, т. е. если эти константы можно выразить так:

$$a_{S,T} = \frac{c_S^T c_T}{c_{ST}}, \tag{14.9}$$

то мы будем отмечать этот факт символом

$$(a) \sim 1.$$

Имеет место

Теорема 39. *Если*

$$(a) \sim 1,$$

то

$$(a, Z) \sim 1,$$

т. е. скрещенное произведение (a, Z) *есть полная матричная алгебра.*

Доказательство. Не нарушая общности, можно предположить, что для всех S, T имеет место

$$a_{S,T} = 1$$

(этого можно добиться преобразованием базиса). Это означает, что

$$u_S u_T = u_{ST}. \tag{14.10}$$

Произведём преобразование базиса

$$[u_e, u_{S_2}, \ldots, u_{S_n}],$$

заменив его базисом

$$[v_1, v_2, \ldots, v_n],$$

где

$$v_i = \sum_S u_S z_i^S \qquad (i = 1,2,\ldots,n), \tag{14.11}$$

где $[z_1, z_2, \ldots, z_n]$ — Ω-базис поля Z. Это преобразование обратимо, так как его определитель, равный квадратному корню из дискриминанта базиса $[z_1, z_2, \ldots, z_n]$, отличен от нуля.

Образуем при помощи базиса $[v_1, v_2, \ldots, v_n]$ представление алгебры (a, Z) матрицами. В общем случае коэффициенты этих матриц лежат в поле Z. Докажем, что в силу (14.10) они лежат в поле Ω. Достаточно доказать это для матриц, соответствующих элементам z и u_R. Имеем

$$z \cdot v_i = \sum_S z u_S z_i^S = \sum_S u_S z^S z_i^S \qquad (i = 1, 2, \ldots, n). \tag{14.12}$$

Пусть элементы zz_i выражаются через базис $[z_1, z_2, \ldots, z_n]$ так:

$$zz_i = \alpha_{1i} z_1 + \alpha_{2i} z_2 + \ldots + \alpha_{ni} z_n \qquad (i = 1, 2, \ldots, n),$$

где $\alpha_{ji} \subset \Omega$. Тогда

$$z^S z_i^S = \alpha_{1i} z_1^S + \alpha_{2i} z_i^S + \ldots + \alpha_{ni} z_n^S \qquad (i = 1, 2, \ldots, n).$$

Подставляя в (14.12), получим

$$zv_i = \sum_S u_S \sum_j \alpha_{ji} z_j^S = \sum_j \alpha_{ji} \sum_S u_S z_j^S = \sum_j \alpha_{ji} v_j.$$

Таким образом элементу z соответствует матрица $\|\alpha_{ij}\|$ с коэффициентами из поля Ω.

Далее, пользуясь (14.10), будем иметь

$$u_T v_i = \sum_S u_{TS} z_i^S = \sum_S u_S z_i^{T^{-1}S} \qquad (i = 1, 2, \ldots, n). \tag{14.13}$$

Выразим элементы $z_i^{T^{-1}}$ через базис $[z_1, z_2, \ldots, z_n]$:

$$z_i^{T^{-1}} = \beta_{1i} z_1 + \beta_{2i} z_2 + \ldots + \beta_{ni} z_n \qquad (i = 1, 2, \ldots, n),$$

откуда получим

$$z_i^{T^{-1}S} = \beta_{1i} z_1^S + \beta_{2i} z_2^S + \ldots + \beta_{ni} z_n^S \qquad (i = 1, 2, \ldots, n).$$

Подставляя в (14.13), будем иметь

$$u_T v_i = \sum_S u_S \sum_j \beta_{ji} z_j^S = \sum_j \beta_{ji} \sum_S u_S z_j^S = \sum_j \beta_{ji} v_j,$$

так что элементу u_T соответствует матрица $\|\beta_{ij}\|$ с коэффициентами из поля Ω. Таким образом мы получили для элементов алгебры (a, Z) изоморфное представление матрицами n-го измерения с коэффициентами из поля Ω. Это показывает, что (a, Z) есть полная матричная алгебра с коэффициентами из поля Ω, что и нужно.

Теорема 40. *Если алгебра*

$$A = (a, Z)$$

имеет индекс m, *то имеет место*

$$(a^m) \sim 1. \tag{14.14}$$

Доказательство. Пусть

$$A = D \times M_r,$$

где D — косое поле порядка m^2 и M_r — полная матричная алгебра измерения r, так что A — алгебра порядка n^2, где $n = mr$. Алгебра $e_{11}M_r$ есть правый идеал алгебры M_r порядка r, а потому алгебра

$$R = e_{11}M_r \times D$$

есть правый идеал алгебры A порядка $m^2 r$. Но $R = e_{11}A$, а её подалгебра $e_{11}Z$ остаётся того же порядка $n = mr$, что и Z, так как Z, будучи полем, не имеет внутри A делителей нуля (все его элементы обратимы). В силу этого для алгебры R можно найти $\frac{m^2 r}{mr} = m$-членный Z-базис

$$[v_1, v_2, \ldots, v_m],$$

через который каждый элемент алгебры R выражается так:

$$v_1 y_1 + v_2 y_2 + \ldots + v_m y_m, \quad y_i \subset Z.$$

Из того, что R есть правый идеал алгебры A, следует, что произведения $v_i u_S$ лежат в R, т. е. что имеет место

$$v_i u_S = v_1 \alpha_{i1} + v_2 \alpha_{i2} + \ldots + v_m \alpha_{im} \qquad (i = 1, 2, \ldots, m),$$

где

$$\alpha_{ij} \subset Z.$$

Запишем эти равенства так:

$$[v_1, v_2, \ldots, v_m]\, u_S = [v_1, v_2, \ldots, v_m] \cdot U_S, \tag{14.15}$$

где $U_S = \|\alpha_{ij}\|$ — матрица с коэффициентами из поля Z. Заметим, что получаемое таким образом представление алгебры A не удовлетворяет условиям изоморфизма, как мы в этом сейчас убедимся. Такое представление носит название *полулинейного*.

Умножая (14.15) на u_T, получим

$$\begin{aligned}[v_1, v_2, \ldots, v_m]\, u_S u_T &= [v_1, v_2, \ldots, v_m] \cdot U_S \cdot u_T = \\ &= [v_1, v_2, \ldots, v_m] \cdot u_T \cdot U_S^T = [v_1, v_2, \ldots, v_m]\, U_T \cdot U_S^T.\end{aligned} \tag{14.16}$$

Итак, вместо изоморфизма полулинейное представление состоит в следующем сопоставлении элементов алгебры и матриц.

Если

$$u_S \longrightarrow U_S, \quad u_T \longrightarrow U_T, \tag{14.17}$$

то

$$u_S u_T \longrightarrow U_T \cdot U_S^T. \tag{14.18}$$

Заметим, что определители $|U_S|$ всех матриц U_S отличны от нуля, так как все элементы u_S имеют обратные элементы, в силу чего $R \cdot u_S = R$.

Сопоставляя (14.16) с

$$[v_1, v_2, \ldots, v_m]\, u_{ST} = [v_1, v_2, \ldots, v_m]\, U_{ST},$$

будем иметь

$$U_T \cdot U_S^T = U_{ST} \cdot a_{S,T}. \tag{14.19}$$

Беря в обеих частях этого матричного равенства определители и вводя обозначение

$$|U_S| = c_S,$$

получим

$$c_T \cdot c_S^T = c_{ST} \cdot a_{S,T}^m,$$

т. е.

$$a^m_{S,T} = \frac{c_T \cdot c^T_S}{c_{ST}}, \tag{14.20}$$

откуда в силу (14.9)

$$(a^m) \sim 1, \tag{14.21}$$

ч. и т. д.

§ 15. КОМПОЗИЦИЯ КЛАССОВ АЛГЕБР

Будем называть две простые алгебры A и B *эквивалентными*:

$$A \sim B,$$

если содержащиеся в них как компоненты тела изоморфны, т. е. если

$$A = D \times M_1, \quad B = D \times M_2,$$

где M_1, M_2 — полные матричные алгебры. Ясно, что из $A \sim B$, $B \sim C$ следует $A \sim C$. Будем также говорить, что эквивалентные простые алгебры находятся в одном и том же *классе алгебр*.

Введённый нами в предыдущем параграфе символ

$$A \sim 1$$

обозначает в соответствии с принятым теперь условием, что $A = M_r$.

Даны две нормальные простые алгебры (a, Z), (b, Z), построенные при помощи одного и того же нормального поля Z. Рассмотрим прямое произведение

$$(a, Z) \times (b, Z).$$

Оказывается, что оно содержит скрещенное произведение (ab, Z), константы которого образованы почленным перемножением констант a и b. Имеет место

Теорема 41. *Прямое произведение* $(a, Z) \times (b, Z)$ *эквивалентно алгебре* (ab, Z):

$$(a, Z) \times (b, Z) \sim (ab \times Z). \tag{15.1}$$

Доказательство. Будем обозначать изоморфные поля Z в алгебрах (a, Z) и (b, Z) различно: например,

вместо (b, Z) будем писать $(b\widetilde{Z})$. Алгебра $(a, Z) \times (b, \overline{Z})$ содержит коммутативную подалгебру $Z \times \overline{Z}$ порядка n^2 и степени n. Как полупростая алгебра она разлагается в прямую сумму простых алгебр, которые в силу коммутативности должны быть полями. Пусть $\widetilde{Z}$ — одно из таких полей, e — его главная единица. Тогда

$$\widetilde{Z} = e(Z \times \overline{Z}).$$

Но $\widetilde{Z}$ содержит поля eZ и $e\overline{Z}$, каждое из которых изоморфно с Z. Отсюда

$$\widetilde{Z} = e(Z \times \overline{Z}) = eZ = e\overline{Z}.$$

Действительно, поля eZ и $e\overline{Z}$ как изоморфные должны быть сопряжёнными. Но, будучи оба нормальными, они должны совпадать.

Поскольку каждый простой прямой компонент алгебры

$$Z \times \overline{Z}$$

имеет порядок n, алгебра $Z \times \overline{Z}$ разлагается в прямую сумму и простых компонентов:

$$Z \times \overline{Z} = e_1 Z + e_2 Z + \ldots + e_n Z,$$

где идемпотенты e_i связаны условиями ортогональности:

$$e_i^2 = e_i; \quad e_i e_j = 0 \quad (i \neq j).$$

Будем обозначать через S автоморфизмы поля $Z \times \overline{Z}$, которые производят над элементами поля Z соответствующие автоморфизмы S, а элементы поля $\overline{Z}$ оставляют неизменными. Тогда

$$(e_i^S)^2 = e_i^S, \quad e_i^S e_j^S = 0 \qquad (i \neq j).$$

Все идемпотенты

$$e, e^{S_2}, \ldots, e^{S_n}$$

отличны друг от друга, так как в противном случае мы бы имели $e^S = e$ $(S \neq \varepsilon)$, откуда отдельные элементы алгебры

$$e\overline{Z} = eZ$$

оставались бы неизменными, что противоречит определению автоморфизма S. Отсюда в силу однозначности разложения $Z \times \bar{Z}$ в прямую сумму следует:

$$Z \times \bar{Z} = eZ + e^{S_2}Z + \ldots + e^{S_n}Z.$$

Таким образом всякий элемент z^* алгебры $Z \times \bar{Z}$ может быть однозначно представлен в форме

$$z^* = ez + e^{S_2}z_{S_2} + \ldots + e^{S_n}z_{S_n}.$$

В частности, для элементов поля $\bar{z}$ в силу $\bar{z}^S = \bar{z}$ имеет место

$$e^S z^S + e^{S_2 S} z^S_{S_2} + \ldots + e^{S_n S} z^S_{S_n} = ez + e^{S_2}z_{S_2} + \ldots + e^{S_n}z_{S_n},$$

откуда в силу однозначности разложения

$$z_S = z^S,$$

т. е.

$$\bar{z} = ez + e^{S_2}z^{S_2} + \ldots + e^{S_n}z^{S_n}. \tag{15.2}$$

Определим при помощи формулы (15.2) автоморфизм $\bar{S}$ поля $\bar{Z}$, соответствующий автоморфизму S поля Z. Пусть

$$\bar{z}^{\bar{S}} = ez^S + e^{S_2}z^{S_2 S} + \ldots + e^{S_n}z^{S_n S} = \sum_i e^{S_i}z^{S_i S}.$$

Будем также считать, что автоморфизм $\bar{S}$ оставляет неизменными элементы поля Z. Тогда перепишем нашу формулу так:

$$\bar{z}^{\bar{S}} = \sum_i e^{S_i S^{-1}} \cdot z^{S_i},$$

откуда следует

$$e^{S_i \bar{S}} = e^{S_i S^{-1}} \tag{15.3}$$

и, в частности,

$$e^{\bar{S}} = e^{S^{-1}}. \tag{15.4}$$

Эта формула означает, что если элемент e выражен через элементы полей Z и $\bar{Z}$:

$$e = \psi(z, \bar{z}),$$

то

$$\psi(z^S, \bar{z}) = \psi(z, \bar{z}^{\bar{S}^-}).$$

Кроме того, из определения автоморфизма S и $\bar{T}$ следует, что они перестановочны.

Если u_S, $\bar{u}_{\bar{S}}$ — элементы скрещенных произведений (a, Z), $(b, \bar{Z})$, для которых

$$z u_S = u_S z^S, \quad \bar{z}\,\bar{u}_{\bar{S}} = \bar{u}_{\bar{S}} \bar{z}^{\bar{S}},$$

то

$$e^T u_S = u_S e^{TS}, \quad e^T \bar{u}_{\bar{S}} = \bar{u}_S e^{T\bar{S}} = \bar{u}_{\bar{S}} e^{T S^{-1}}.$$

Если мы введём обозначения

$$e_{S,T} = u_{S^{-1}} u_T e^T,$$
$$e_{S,S} = e^S,$$

то в силу ортогональности элементов e^S

$$\begin{aligned} e_{S,T} e_{V,W} &= u_{S^{-1}} u_T e^T u_{V^{-1}} u_W e^W = \\ &= u_{S^{-1}} u_T e^T e^V u_{V^{-1}} u_W, \\ &= 0 \quad (T \neq V), \\ &= u_{S^{-1}} u_T e^T u_{T^{-1}} u_W = u_{S^{-1}} u_W e^W = e_{S,W} \,(T = V), \end{aligned}$$

откуда видно, что $e_{S,T}$ представляют собой систему n^2 матричных единиц, дающих полную матричную алгебру n-го измерения M_n.

Далее мы должны доказать, что алгебра $(a, Z) \times (b, \bar{Z})$ содержит алгебру, элементы которой перестановочны с элементами алгебры M_n и которая изоморфна с $e(a, Z) \times \times (b, \bar{Z})\, e$. Доказательство ничем не отличается от доказательства теоремы 25. Поэтому мы остановимся на структуре алгебры $e(a, Z) \times (b, \bar{Z})\, e$. Её элементы можно представить в форме

$$\sum_{S,T} e u_S y_S \bar{u}_T \bar{y}_T e = \sum_{S,T} u_S y_S e^S e^{\bar{T}^{-1}} \bar{u}_{\bar{T}} \bar{y}_{\bar{T}} =$$
$$= \sum_{S,T} u_S y_S e^S e^T \bar{u}_{\bar{T}} \bar{y}_{\bar{T}},$$

В силу ортогональности e^S, e^T стоящий под знаком суммы член только тогда отличен от нуля, если $S = T$. Отсюда общий член нашей алгебры представляется так:

$$\sum_S u_S y_S e^S \bar{u}_{\bar{S}} \bar{y}_{\bar{S}} = \sum_S e u_S \bar{u}_{\bar{S}} y_S \bar{y}_{\bar{S}} e .$$

Эта формула показывает, что базис нашей алгебры относительно $Z \times \bar{Z}$ есть

$$[u_e \bar{u}_{\bar{e}},\ u_{S_2} \bar{u}_{\bar{S}_2},\ \ldots,\ u_{S_n} \bar{u}_{\bar{S}_n}] .$$

Соответствующие этому базису множители выводятся из формул

$$u_S u_T = u_{ST} a_{S,T}, \quad \bar{u}_{\bar{S}} \bar{u}_{\bar{T}} = \bar{u}_{\bar{S}\bar{T}} b_{\bar{S},\bar{T}} .$$

Именно, имеет место

$$u_S \bar{u}_{\bar{S}} u_T \bar{u}_{\bar{T}} = u_{ST} \bar{u}_{\bar{S}\bar{T}} \cdot a_{S,T} b_{\bar{S},\bar{T}} .$$

Итак, множители алгебры $e(a, Z) \times (b, \bar{Z}) e$ получаются путём почленного перемножения множителей алгебр (a, Z) и $(b, \bar{Z})$, что доказывает справедливость формулы (15.1).

Введём понятие *умножения классов алгебр*. Под произведением двух классов нормальных простых алгебр A и B мы будем разуметь класс алгебр, эквивалентных с прямым произведением $A \times B$. Если A и B мы возьмём в форме скрещенных произведений (a, Z), (b, Z), то в качестве их произведения можно взять (ab, Z).

Все эти классы алгебр (с общим полем разложения Z) образуют абелеву группу. Как мы только что видели, вместо классов алгебр мы можем перемножать их множители:

$$(a) \cdot (b) \sim (ab).$$

Назовём *показателем* алгебры A наименьшее целое положительное число l, при котором

$$A^l \sim 1.$$

Тогда имеет место

Теорема 42. *Показатель l алгебры A делит её индекс n и вместе с тем содержит все простые множители числа n.*

Доказательство. В самом деле, если $A \sim (a, Z)$, то из теоремы 42 следует, что

$$A^m \sim (a^m, Z).$$

Но из теоремы 41

$$(a^m) \sim 1$$

и теоремы 40 вытекает

$$A^m \sim 1.$$

Если бы m не делилось на l, то

$$m = lq + r, \quad 0 < r < l.$$

Тогда

$$A^m = (A^l)^q \times A^r \sim A^r \sim 1.$$

Но это в силу $0 < r < l$ противоречит определению показателя l.

С другой стороны, пусть Z — нормальное поле разложения алгебры A, $n = rm$ — его степень, p — одно из простых чисел, входящих в m. Пусть Σ — подполе поля Z, принадлежащее к силовской подгруппе группы $\mathfrak{G}$ поля Z, имеющей порядок p^λ. Σ не есть поле разложения алгебры A, так как его степень не делится на p и, следовательно, на m, вопреки теореме 34. Алгебра $\Sigma \times A$ имеет полем разложения поле Z, степень которого над полем Σ равна p^λ. Отсюда следует, что её индекс есть степень p, не превышающая p^λ; поэтому и показатель её есть p^μ, где $0 < \mu \leqslant \lambda$ (в случае $\mu = 0$ имело бы место $\Sigma \times A \sim 1$). Итак,

$$(\Sigma \times A)^{p^{\mu-1}} \not\sim 1, \quad (\Sigma \times A)^{p^\mu} \sim 1.$$

Но из

$$A^l \sim 1$$

следует

$$(\Sigma \times A)^l \sim 1,$$

откуда видно, что l делится на p^μ, ч. и т. д.

Р. Брауэр показал на примере, что при данном $m = p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k}$ показатель l может принимать все значения, делящиеся на $p_1 p_2 \ldots p_k$ и входящие делителем в m. В его примере поле Ω — функциональное. Для числовых же полей, как мы увидим ниже, всегда $l = m$.

Теорема 43. *Всякое нормальное тело можно разложить в прямое произведение тел, порядок каждого из которых есть степень простого числа.*

Доказательство. Пусть нормальное тело D имеет степень $m = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_k^{\lambda_k}$ и показатель $l = p_1^{\mu_1} p_2^{\mu_2} \dots p_k^{\mu_k}$ $(1 \leqslant \mu_i \leqslant \lambda_i)$. Пусть $q_i = \dfrac{l}{p_i^{\mu_i}}$. Решим в целых *положительных* числах неопределённое уравнение

$$1 + l\xi = q_1 x_1 + q_2 x_2 + \dots + q_k x_k.$$

Тогда

$$D \sim D^{1+l\xi} \sim D^{q_1 x_1} \times D^{q_2 x_2} \times \dots \times D^{q_k x_k}.$$

Каждое косое поле

$$D_i \sim D^{q_i x_i}$$

имеет показатель $p_i^{\mu_i}$, так как, с одной стороны,

$$D_i^{p_i^{\mu_i}} \sim D^{q_i x_i p_i^{\mu_i}} = D^{l x_i} \sim 1;$$

с другой стороны, если бы имело место

$$D_i^{p_i^{\nu_i}} \sim 1, \quad \nu_i < \mu_i,$$

то

$$D^{l_i p_i^{\mu_i - \nu_i}} \sim \Pi D_i^{p_i^{\nu_i} q_i} \sim 1,$$

что противоречит определению показателя l.

Пусть

$$D_1 \times D_2 \times \dots \times D_k = D \times M_r, \tag{15.5}$$

где M_r — полная матричная алгебра измерения r. Так как степень алгебры D_i есть степень p_i и, с другой стороны, делитель степени m алгебры D, то она равна $p_i^{\nu_i}$ $(\nu_i \leqslant \lambda_i)$. Тогда сравнение степеней алгебр в обеих частях равенства (15.5) даёт

$$p_1^{\nu_1} p_2^{\nu_2} \dots p_k^{\nu_k} = p_1^{\nu_1} p_2^{\lambda_2} \dots p_k^{\lambda_k} \cdot r,$$

откуда

$$\nu_i = \lambda_i \qquad (i = 1, 2, \dots, k), \quad r = 1,$$

и равенство (15.5) перепишется так:

$$D = D_1 \times D_2 \times \ldots \times D_k, \tag{15.6}$$

где D_i имеет степень $p_i^{\lambda_i}$ и показатель $p_i^{\mu_i}$, ч. и т. д.

Исследуем, что произойдёт со скрещенным произведением

$$A = (a, Z),$$

если мы присоединим к нему произвольное поле φ. Имеет место

Теорема 44. *Прямое произведение*

$$\varphi \times A = \varphi \times (a, Z)$$

эквивалентно скрещенному произведению

$$(a_\varphi, Z_\varphi),$$

где (a_φ) *— часть системы констант* (a)*, соответствующая автоморфизмам, оставляющим поле* φ *инвариантным, а* Z_φ *— композит полей* Z *и* φ.

Доказательство. Сначала рассмотрим алгебру

$$\varphi \times Z,$$

входящую в $\varphi \times A$. Она является полупростой коммутативной алгеброй и поэтому может быть представлена как прямая сумма нескольких полей. Если обозначить через $\overline{Z}$ одно из таких полей и через e его главную единицу, то

$$\overline{Z} = eZ_\varphi = e(\varphi \times Z).$$

Если мы обозначим через F пересечение полей φ и Z и через H подгруппу группы Галуа $\mathfrak{G}$ поля Z, к которой оно принадлежит, то степень поля F равна k, где

$$n = h \cdot k$$

и h — порядок группы H. Группа H изоморфна с группой Galois поля Z, если к области рациональности K присоединить φ, так что её порядок равен степени композита Z_φ относительно φ. С другой стороны, порядок алгебры $\varphi \times Z$ равен n, так как порядок алгебры не меняется при присоединении к области рациональности новых элементов. Отсюда следует, что $\varphi \times Z$ есть прямая сумма k полей, изоморфных с $\overline{Z}$. Каждому из этих полей соответствует идемпотент, и

система получаемых таким образом k ортогональных идемпотентов даёт начало полной матричной алгебре M_k k-го измерения, содержащейся внутри $\varphi \times A$.

Как обычно, докажем, что $\varphi \times A$ есть прямое произведение алгебры M_k и алгебры порядка h^2, изоморфной с

$$e(\varphi \times A)\, e.$$

Эту последнюю алгебру мы и изучим подробнее.

Каждый автоморфизм S группы $\mathfrak{G}$ переводит идемпотент e в другой идемпотент e^S. Какие из них оставляют e неизменными? S переводит поле $\overline{Z}$, входящее как прямое слагаемое алгебры $\varphi \times Z$ в другое, вообще говоря, поле $e^S(\varphi \times Z)$. Если же $e^S = e$, то

$$e^S(\varphi \times Z) = e(\varphi \times Z).$$

Но это показывает, что S является автоморфизмом поля $\overline{Z}$, который оставляет неизменными элементы области рациональности φ и, в частности, F. Значит, S входит в подгруппу H. Обратно, если $S \subset H$, т. е. если $\overline{Z}^S = \overline{Z}$, то его главная единица e остаётся на месте. Если мы разложим $\mathfrak{G}$ на смежные классы по подгруппе H:

$$\mathfrak{G} = H + HS_2 + \ldots + HS_k,$$

то получим k различных идемпотентов

$$e, e^{S_2}, \ldots, e^{S_k}.$$

Внутри $e(\varphi \times A)\, e$ элементы u_s имеют те же свойства, что и внутри A (ведь элементы из φ перестановочны с u_S), и потому, в частности,

$$e^R u_S = u_S e^{RS}.$$

Элементы алгебры $\varphi \times A$ могут быть однозначно представлены в виде

$$a^* = \sum_s u_s z_s^* \quad (z_s^* \subset \varphi \times Z),$$

а потому элементы алгебры

$$\overline{A} = e(\varphi \times A)\, e$$

представляются в виде

$$\overline{a} = \sum_S e u_S \cdot z_S^* e = \sum_S u_S e^S e z_S^*.$$

Если при этом S не лежит в H, то $e^S e = 0$, а потому

$$\bar{a} = \sum_{S \subset H} u_S e z_S^* = \sum_{S \subset H} u_S \bar{z}_S \quad (\bar{z}_S \subset Z).$$

Эта формула показывает, что

$$u_S \, (S \subset H)$$

образуют $\bar{Z}$-базис алгебры $\bar{A}$. Этот базис является частью Z-базиса

$$[u_\varepsilon, \; u_{S_2}, \; \ldots, \; u_{S_n}]$$

алгебры A, соответствующей подгруппе H. Его константы $a_{S,\,T}^{\varphi}$ являются частью констант $a_{S,\,T}$. Поэтому

$$A = (a^{\varphi}, \; \bar{Z})$$

и

$$\varphi \times A \sim (a^{\varphi}, Z_{\varphi}),$$

где $Z_{\varphi} = \bar{Z}$ есть композит полей φ и Z.

В частности, если $\varphi = Z$, то $H = 1$, $(a^{\varphi}) \sim 1$, откуда $\varphi \times A \sim 1$. Таким образом мы опять получаем известный ранее результат, что Z есть поле разложения алгебры $A = (a, Z)$.

§ 16. ЦИКЛИЧЕСКИЕ АЛГЕБРЫ

Рассмотрим подробнее структуру *циклических* алгебр, т. е. таких скрещенных произведений, у которых группа Галуа $\mathfrak{G}$ поля Z циклическая. Пусть Z — циклическое поле относительно Ω и пусть

$$\mathfrak{G} = \varepsilon + S + S^2 + \ldots + S^{n-1}$$

его группа Галуа. Элементы u_{S^λ} удовлетворяют соотношениям

$$u_{S^\lambda} \; u_{S^\mu} = u_{S^{\lambda+\mu}} \; a_{S^\lambda,\, S^\mu},$$

в силу чего элементы

$$1, \quad u_S, \quad (u_S)^2, \; \ldots, \quad (u_S)^{n-1}$$

тоже составляют Z-базис алгебры $A = (a, Z)$, и $(u_S)^\lambda$ играют ту же роль, что и $u s^\lambda$:

$$Z \, (u_S)^\lambda = (u_S)^\lambda Z^{S^\lambda},$$

в силу чего мы можем принять

$$u_{S^\lambda} = (u_S)^\lambda \qquad (\lambda = 1,\ 2,\ \ldots,\ n-1),$$

так что

$$u_{S^\lambda} \cdot u_{S^\mu} = u_{S^{\lambda+\mu}} \qquad (\lambda + \mu \leqq n-1),$$

т. е.

$$a_{S^\lambda,\, S^\mu} = 1 \qquad (\lambda + \mu \leqq n-1).$$

Положим

$$(u_S)^n = \alpha, \quad \alpha \subset Z.$$

Тогда

$$u_{S^\lambda} \cdot u_{S^\mu} = u_{S^{\lambda+\mu}} \cdot \alpha \qquad (\lambda + \mu \leqq n).$$

Имеет место

Теорема 45. *α есть элемент поля Ω.*

Доказательство. Из формулы (14.1)

$$a^V_{S,\,T} = \frac{a_{S,\,TV}\, a_{T,\,V}}{a_{ST,\,V}}; \tag{16.1}$$

полагая $T = S^{n-1}$, $V = S$, мы имеем

$$a^S_{S,\,S^{n-1}} = \frac{a_{S,\,\varepsilon} \cdot a_{S^{n-1},S}}{a_{\varepsilon,\,S}} = a_{S^{n-1},\,S},$$

т. е.

$$\alpha^S = \alpha,$$

откуда следует, что α остаётся инвариантным при всех автоморфизмах группы $\mathfrak{S}$ и потому входит в Ω.

Теорема 46. $(\alpha, Z) \sim 1$ *имеет место тогда и только тогда, когда α может быть представлен как норма элемента поля Z.*

Доказательство. $(\alpha, Z) \sim 1$ равносильно условиям

$$a_{S^\mu,\,S^\nu} = \frac{c_{S^\nu} \cdot c^{S^\nu}_{S^\mu}}{c_{S^{\mu+\nu}}},$$

Беря $\mu = 1$, а $\nu = 1, 2, \ldots, n-1$, будем иметь

$$1 = \frac{c_S \cdot c_S^S}{c_{S^2}},$$

$$1 = \frac{c_{S^2} \cdot c_S^{S^2}}{c_{S^3}},$$

$$\cdots\cdots\cdots$$

$$1 = \frac{c_{S^{n-2}} \cdot c_S^{S^{n-2}}}{c_{S^{n-1}}},$$

$$\alpha = \frac{c_{S^{n-1}} \cdot c_S^{S^{n-1}}}{c_e}.$$

Перемножая, получим

$$\alpha = \frac{c_S \cdot c_S^S \cdot c_S^{S^2} \ldots c_S^{S^{n-1}} \cdot c_{S^2} \cdot c_{S^3} \ldots c_{S^{n-1}}}{c_{S^2} \cdot c_{S^3} \ldots c_{S^{n-1}}} = N(c_S).$$

Обратно, если $\alpha = N(c)$, то, полагая

$$c_{S^\mu} = c \cdot c^S \cdot c^{S^2} \ldots c^{S^{\mu-1}},$$

мы будем в случае $\mu + \nu \leqq n-1$ иметь

$$\frac{c_{S^\nu} \cdot c_{S^\mu}^{S^\nu}}{c_{S^{\mu+\nu}}} = \frac{c \cdot c^S \cdot c^{S^2} \ldots c^{S^{\nu-1}} \cdot c^{S^\nu} \cdot c^{S^{\nu+1}} \ldots c^{S^{\nu+\mu-1}}}{c \cdot c^S \cdot c^{S^2} \ldots c^{S^{\nu+\mu-1}}} = 1;$$

если же $\mu + \nu = n$, то

$$\frac{c_{S^\nu} \cdot c_{S^\mu}^{S^\nu}}{c_{S^{\mu+\nu}}} = c_{S^\nu} \cdot c_{S^\mu}^{S^\nu} = c \cdot c^S \ldots c^{S^{\nu+\mu-1}} = N(c) = \alpha,$$

и мы получим для a_{S^μ, S^ν} выражение

$$\frac{c_{S^\nu} \cdot c_{S^\mu}^{S^\nu}}{c_{S^{\mu+\nu}}},$$

откуда

$$(a) \sim 1,$$

что и нужно.

Будем обозначать циклическую алгебру, заданную полем Z, автоморфизмом S и величиной α, символом (α, Z, S). Имеет место

Теорема 47. *Циклическая алгебра* $A = (\alpha, Z, S)$ *степени* n *является телом, если* n *есть самая низшая положительная степень числа* α, *являющаяся нормой числа из* Z.

Доказательство. При сделанных предположениях допустим противное, именно допустим, что A не есть тело. Тогда A содержит полную матричную алгебру M_r, где

$$n = r \cdot m, \quad r > 1.$$

Если e_{11} — один из идемпотентов алгебры M_r, то A содержит правый идеал $e_{11} A$ порядка

$$\frac{n^2}{r} = n \cdot m.$$

Пусть

$$[w_1, w_2, \ldots, w_n]$$

будет Z-базис идеала $e_{11} A$. При его помощи можно получить полулинейное представление алгебры A. Пусть, в самом деле,

$$[w_1, w_2, \ldots, w_m]\, u = [w_1, w_2, \ldots, w_m]\, U,$$

где u — элемент из A и U — матрица m-го измерения с коэффициентами из Z. Беря в качестве u элемент u_S и пользуясь формулой

$$z u_S = u_S z^S, \quad z \subset Z,$$

получим

$$[w_1, w_2, \ldots, w_m]\, u^2 = [w_1, w_2, \ldots, w_m]\, U \cdot u =$$
$$= [w_1, w_2, \ldots, w_m] \cdot u \cdot U^S = [w_1, w_2, \ldots, w_m] \cdot U \cdot U^S,$$
$$[w_1, w_2, \ldots, w_m]\, u^3 = [w_1, w_2, \ldots, w_m]\, U\, U^S U^{S^2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$[w_1, w_2, \ldots, w_m]\, u^n =$$
$$= [w_1, w_2, \ldots, w_m]\, U \cdot U^S \cdot U^{S^2} \ldots U^{S^{n-1}}.$$

Но из $u^n = \alpha$ следует

$$U \cdot U^S \cdot U^{S^2} \ldots U^{S^{n-1}} = \begin{Vmatrix} \alpha & \ldots & 0 \\ \cdot & \cdot & \cdot \\ 0 & \ldots & \alpha \end{Vmatrix}.$$

Обозначая через β определитель матрицы U и беря от обеих частей этого равенства определители, получим

$$\beta \cdot \beta^{S} \cdot \beta^{S^2} \dots \beta^{S^{n-1}} = \alpha^m,$$

т. е.

$$\alpha^m = N(\beta), \quad \beta \subset Z,$$

что в силу $m < n$ противоречит предположениям теоремы. Итак, A есть тело.