ВАН-ДЕР-ВАРДЕН

СОВРЕМЕННАЯ АЛГЕБРА

ВТОРАЯ ЧАСТЬ

ОНТИ • НКТП • СССР • 1937

Б. Л. ВАН-ДЕР-ВАРДЕН
ПРОФЕССОР УНИВЕРСИТЕТА В ГРОНИНГЕНЕ

СОВРЕМЕННАЯ АЛГЕБРА

ВТОРАЯ ЧАСТЬ

Перевод с немецкого Л. Я. Окунева

Цена 3 р. Перепл. 1 р.

ОБЪЕДИНЕННОЕ
НАУЧНО-ТЕХНИЧЕСКОЕ ИЗДАТЕЛЬСТВО НКТП СССР
ГЛАВНАЯ РЕДАКЦИЯ ОБЩЕТЕХНИЧЕСКОЙ ТЕХНО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1937 ЛЕНИНГРАД

MODERNE AIGEBRA

VON
DR. B. L. VAN DER WAERDEN
O. PROFESSOR AN DER UNIVERSITÄT
GRONINGEN

unter Benutzung von Vorlesungen
von
E. ARTIN und E. NOETHER

ZWEITER TEIL

BERLIN
VERLAG VON JULIUS SPRINGER
1931

Редакция *Л. Я. Окунева.* Оформление *В. Ф. Зазулькой.*

Изд. № 96. Тираж 7 000. Сдано в набор 19/X-35 г. Подп. в печ. 26/I-37 г. Формат бумаги 62 × 94. Уч.-авт. лист. 14,84. Бумажных листов $6^5/_8$. Печатн. знак. в бумажн. листе 101 000. Заказ № 1657. Уполном. Главл. № В-46044. Выход в свет февраль 1937 г.

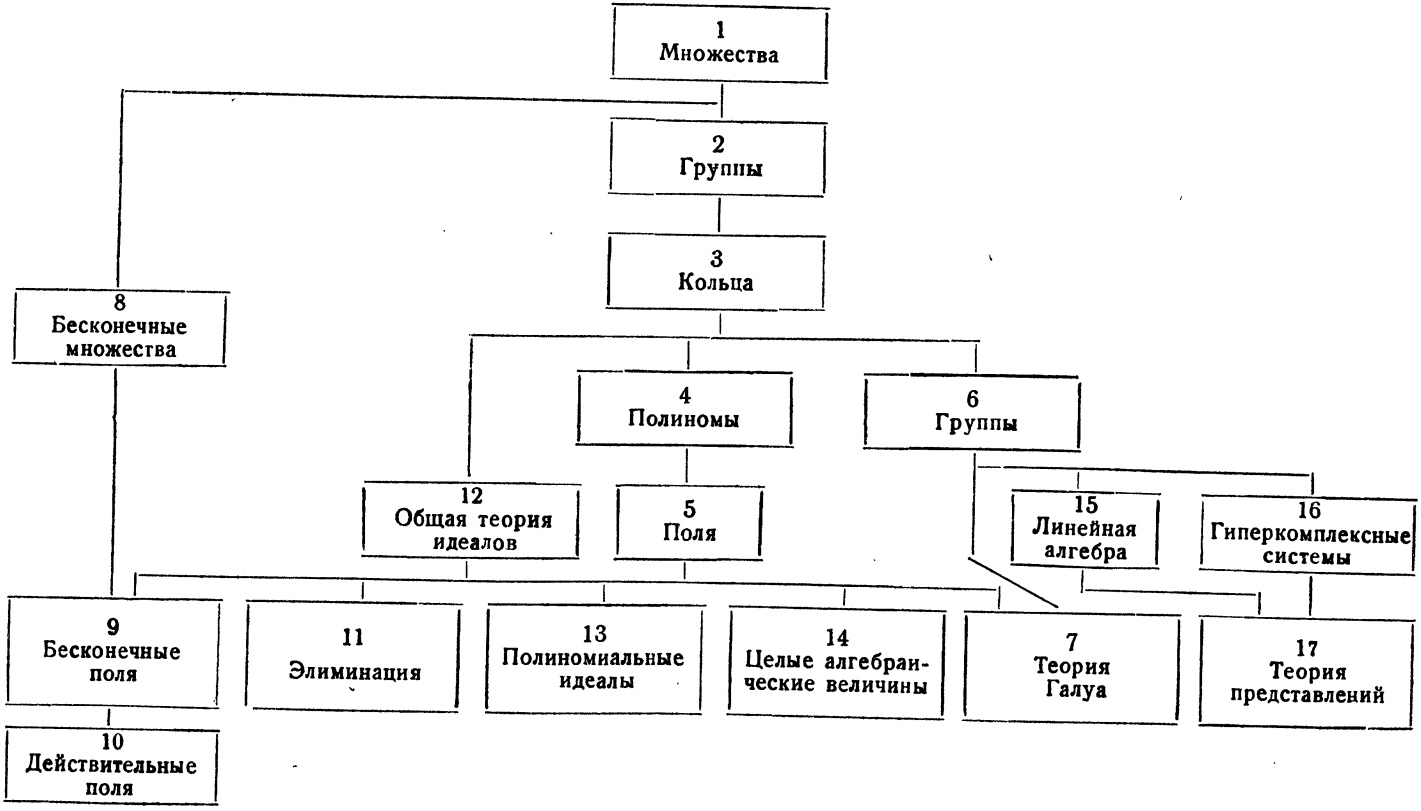
3-я тип. ОНТИ. Ленинград, ул. Моисеенко, 10.

ПРЕДИСЛОВИЕ

За последние десять лет особенно сильное развитие получили такие отделы абстрактной алгебры, как общая теория идеалов коммутативного кольца, теория полиномиальных идеалов, теория гиперкомплексных систем и т. д. Настоящая книга как раз содержит подробное изложение этих отделов современной алгебры.

Схематический чертеж.

Логическая зависимость между отдельными главами.



ОГЛАВЛЕНИЕ

Глава одиннадцатая

Теория исключения

Глава двенадцатая

Общая теорема идеалов коммутативного кольца

Глава тринадцатая

Теория полиномиальных идеалов

Глава четырнадцатая

Целые алгебраические величины

Глава пятнадцатая

ЛИНЕЙНАЯ АЛГЕБРА

Глава шестнадцатая

ТЕОРИЯ ГИПЕРКОМПЛЕКСНЫХ ВЕЛИЧИН

Глава семнадцатая

ТЕОРИЯ ПРЕДСТАВЛЕНИЯ ГРУПП И ГИПЕРКОМПЛЕКСНЫХ СИСТЕМ

ГЛАВА ОДИННАДЦАТАЯ

ТЕОРИЯ ИСКЛЮЧЕНИЯ

Теория исключения исследует системы алгебраических уравнений со многими неизвестными и ищет условия их разрешимости, а также формулы для вычисления их решений в различных случаях. Мы будем предполагать известной ту часть теории, которая рассматривает линейные уравнения (т. е. теорию определителей). Далее будет предполагаться известным, что одно уравнение высшей степени с одним неизвестным разрешимо или, точнее, что если уравнение в данном поле еще неразрешимо, то можно построить такое поле расширения, в котором оно уже будет разрешимо, и даже такое, в котором наше уравнение разлагается целиком (ч. I, глава V). В дальнейшем всегда под „решениями уравнения" или „корнями полинома" будут подразумеваться именно такие решения в соответствующем поле расширения основного коммутативного поля K.

§ 71. РЕЗУЛЬТАНТ ДВУХ ПОЛИНОМОВ

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n,$$

$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$$

два полинома в $\mathsf{K}[x]$. Так как для нас важен также случай, когда a_ν, b_ν зависят от других переменных, и для некоторых значений этих переменных a_ν и b_ν могут оказаться равными нулю, то мы не будем исключать из рассмотрения случаи $a_0 = 0$ и $b_0 = 0$. Если полином $f(x)$ записан в указанной форме, начиная с члена a_0x^n, то мы n назовем формальной степенью полинома и a_0 — формальным начальным коэфициентом. Предположим пока, что по крайней мере один из начальных коэфициентов a_0, b_0 не исчезает.

Условие существования общего решения уравнений $f = 0$, $g = 0$ состоит в том, что оба полинома f, g должны иметь общий непостоянный множитель $\varphi(x)$. Покажем прежде всего, что это условие имеет место тогда и только тогда, если

$$h(x)f(x) = k(x)g(x), \tag{1}$$

где $h(x)$ степени не выше, чем $m-1$, а $k(x)$ степени не выше, чем $n-1$, и по крайней мере один из полиномов h, k не исчезает тождественно.

А именно, если (1) выполнено, то, разлагая обе части равенства на простые множители, получим слева и справа одни и те же множители.

Мы можем предположить, что $f(x)$ имеет действительно степень $n\,(a_0 \neq 0)$, так как в противном случае мы бы поменяли ролями $f(x)$ и $g(x)$. Все простые множители $f(x)$ в правой части (1) должны встречаться по меньшей мере столько раз, сколько они встречаются в $f(x)$. Но в $k(x)$ все эти множители с указанной кратностью входить не могут, так как степень $k(x)$ меньше или равна $n-1$ и $k(x)$ не исчезает тождественно. Отсюда должен существовать простой множитель $f(x)$, входящий также и в $g(x)$, что и требовалось показать.

Если, обратно, $\varphi(x)$ — непостоянный общий множитель $f(x)$ и $g(x)$, то

$$f(x) = \varphi(x)\,k(x),$$
$$g(x) = \varphi(x)\,h(x)$$

и тогда равенство (1) удовлетворится.

Для дальнейшего исследования равенства (1) положим

$$h(x) = c_0x^{m-1} + c_1x^{m-2} + \ldots + c_{m-1},$$
$$k(x) = d_0x^{n-1} + d_1x^{n-2} + \ldots + d_{n-1}.$$

Подставляя в (1) и сравнивая слева и справа коэфициенты при степенях x^{n+m-1}, x^{n+m-2}, $\ldots$, x, 1, получим следующую систему линейных уравнений относительно коэфициентов c_i и d_j:

$$\left.\begin{array}{rcl}
c_0a_0 & = & d_0b_0,\\
c_0a_1 + c_1a_0 & = & d_0b_1 + d_1b_0,\\
c_0a_2 + c_1a_1 + c_2a_0 & = & d_0b_2 + d_1b_1 + d_2b_0,\\
\cdots\cdots\cdots\cdots & & \\
c_{m-2}a_n + c_{m-1}a_{n-1} & = & d_{n-2}b_m + d_{n-1}b_{m-1},\\
c_{m-1}a_n & = & d_{n-1}b_m.
\end{array}\right\} \qquad (2)$$

Всего получилось $n+m$ однородных линейных уравнений для $n+m$ неизвестных c_i, d_j. Потребуем, чтобы не все неизвестные были равны нулю. Для этого необходимо, чтобы детерминант равнялся нулю. Опуская минусы в детерминанте и переставляя соответствующим образом строки и столбцы, получим окончательно:

$$R = \left|\begin{array}{c}
a_0\ a_1 \ldots a_n \\
\quad a_0\ a_1 \ldots a_n \\
\quad\cdots\cdots \\
\quad\quad a_0\ a_1 \ldots a_n \\
b_0\ b_1 \ldots b_m \\
\quad b_0\ b_1 \ldots b_m \\
\quad\cdots\cdots \\
\quad\quad b_0\ b_1 \ldots b_m
\end{array}\right| \qquad \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} m \text{ строк} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} n \text{ строк} \end{array} \qquad (3)$$

(Там, где ничего не написано, подразумеваются нули.)

Определитель R называется *результантом* полиномов $f(x)$, $g(x)$. Заметим, что он однороден относительно a_i и степени m; точно так же R — однородный полином степени n относительно b_j. Далее легко

видеть, что R содержит „главный член“ $a_0^m b_0^n$ и исчезает не только тогда, когда полиномы f, g имеют общий множитель, но и тогда, когда $a_0 = b_0 = 0$. Итак:

Результант двух полиномов $f(x)$, $g(x)$ есть целая рациональная функция коэфициентов вида (3). *Если результант равен нулю, то полиномы f, g либо имеют общий непостоянный множитель, либо их начальные коэфициенты равны нулю, и обратно.*

Приведенный метод исключения принадлежит Эйлеру; вид (3) результанта известен под названием результанта Сильвестера.

Исключительный случай $a_0 = b_0 = 0$ при формулировке теоремы можно опустить, для чего либо заранее полагается $a_0 = 1$, что мы в дальнейшем иногда будем делать, либо рассматриваются две однородные формы с двумя переменными:

$$F(x) = a_0 x_1^n + a_1 x_1^{n-1} x_2 + \ldots + a_n x_2^n,$$
$$G(x) = b_0 x_1^m + b_1 x_1^{m-1} x_2 + \ldots + b_m x_2^m$$

вместо полиномов одного переменного. Таким образом первоначальные многочлены f, g и числа n, m определяют однозначно формы F, G, и обратно. Разложению f на множители:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n =$$
$$= (p_0 x^r + \ldots + p_r)(q_0 x^s + \ldots + q_s)$$

соответствует разложение F:

$$F(x) = a_0 x_1^n + \ldots + a_n x_2^n =$$
$$= (p_0 x_1^r + \ldots + p_r x_2^r)(q_0 x_1^s + \ldots + q_s x_2^s),$$

и аналогично для g и G. Точно так же общему множителю f и g соответствует общий множитель F и G. Но если $a_0 = b_0 = 0$, то F, G имеют общим множителем x_2; таким образом два случая, сформулированные в теореме, можно выразить одной фразой: „F и G имеют общий множитель“. Из решения $\{\xi_1, \xi_2\}$ уравнений $F = 0$, $G = 0$ получается, если только $\xi_2 \neq 0$, решение $\xi = \xi_1 : \xi_2$ первоначальных уравнений $f = 0$, $g = 0$. Но если $\xi_2 = 0$ и $\xi_1 \neq 0$, то $a_0 = b_0 = 0$. Тривиальное решение $\xi_1 = \xi_2 = 0$ не принимается в расчет.

Вернемся снова к неоднородным полиномам f и g; примем их коэфициенты за неизвестные и рассмотрим

$$\begin{aligned}
x^{m-1} f(x) &= a_0 x^{n+m-1} + a_1 x^{n+m-2} + \ldots + a_n x^{m-1},\\
x^{m-2} f(x) &= \quad a_0 x^{n+m-2} + \ldots\ldots + a_n x^{m-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
f(x) &= \quad a_0 x^n + \ldots\ldots\ldots + a_n,\\
x^{n-1} g(x) &= b_0 x^{n+m-1} + b_1 x^{n+m-2} + \ldots + b_m x^{n-1},\\
x^{n-2} g(x) &= \quad b_0 x^{n+m-2} + \ldots\ldots + b_m x^{n-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
g(x) &= \quad b_0 x^m + \ldots\ldots\ldots + b_m.
\end{aligned}$$

Детерминант правой части этой системы уравнений как раз есть R,

Если справа исключить $x^{n+m-1}, \ldots, x$, умножив на миноры последнего столбца и складывая, то слева получится полином вида

$$Af + Bg,$$

где A и B — полиномы относительно x и a_μ, b_ν, а справа будет R. *Следовательно,*

$$R \equiv 0\,(f, g)\ ^{1})$$

в целочисленной области полиномов x, a_μ, b_ν ²).

§ 72. РЕЗУЛЬТАНТ КАК СИММЕТРИЧЕСКАЯ ФУНКЦИЯ КОРНЕЙ

Если вынести за знак определителя R множитель $a_0^m\, b_0^n$, то получится полином R^* относительно $\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}, \frac{b_1}{b_0}, \ldots, \frac{b_m}{b_0}$. Эти дроби равны $-s_1, s_2, \ldots, (-1)^n s_n; -\sigma_1, \sigma_2, \ldots, (-1)^m \sigma_m$, где s и σ — элементарные симметрические функции корней $\xi_1, \ldots, \xi_n$ полинома f и корней $\eta_1, \ldots, \eta_m$ полинома g. R^*, рассматриваемое как функция ξ и η, исчезает при $\xi_i = \eta_k$ и потому делится на $\xi_i - \eta_k$ (§ 19); таким образом R^* должно делиться на произведение

$$\prod_i \prod_k (\xi_i - \eta_k).$$

Отсюда само R будет делиться на

$$S = a_0^m\ b_0^n \prod_i \prod_k (\xi_i - \eta_k). \tag{1}$$

Это произведение можно преобразовать двояким образом. **Во-первых,** из

$$g(x) = b_0 \prod_k (x - \eta_k)$$

следует при $x = \xi_i$:

$$\prod_i g(\xi_i) = b_0^n \prod_i \prod_k (\xi_i - \eta_k),$$

откуда

$$S = a_0^m \prod_i g(\xi_i). \tag{2}$$

Во-вторых, из

$$f(x) = a_0 \prod_i (x - \xi_i) = (-1)^n a_0 \prod_i (\xi_i - x)$$

подобным же образом следует, что

$$S = (-1)^{nm}\ b_0^n \prod_k f(\eta_k). \tag{3}$$

---

¹) Это сокращенная запись сравнения $R \equiv 0 \pmod{(f, g)}$.

²) Для форм F, G получается, что $x_2^{n+m-1}\, R \equiv 0\,(F, G)$.

Из (2) видно, что S — целая однородная функция степени n относительно b, а из (3), что S — целая однородная функция степени m относительно a. Но те же степени имеет и R, и R делится на S; следовательно, R должно совпадать с S с точностью до целого множителя. Сравнивая справа и слева члены с наивысшими степенями b_0, получаем как в R, так и в S член $+a_0^m b_0^n$, откуда целый множитель должен быть равен единице; следовательно,

$$R = S.$$

Таким образом мы установили для R три представления (1), (2), (3).

Отсюда также легко получается неразложимость результанта как полинома неизвестных $a_0, \ldots, b_m$, а именно не только неразложимость в целочисленной области полиномов, но даже *абсолютная неразложимость*, т. е. R оказывается неразложимым в области полиномов тех же неизвестных с коэфициентами из любого поля. В самом деле, если бы R распадалось на два (очевидно однородных) множителя A, B, то A и B снова были бы симметрическими функциями корней. Так как R делится на $\xi_1 - \eta_1$, то на $\xi_1 - \eta_1$ должно делиться A или B; пусть это будет, например, A. Тогда A как симметрическая функция должна делиться также на все остальные $\xi_i - \eta_k$ и тем самым на их произведение

$$\prod_i \prod_k (\xi_i - \eta_k).$$

В силу равенства

$$R = a_0^m b_0^n \prod \prod (\xi_i - \eta_k)$$

для множителя B остается предположить, что $B = \text{const.}\, a_0^p b_0^q$. Но R, как полином от a и b, не делится ни на a_0, ни на b_0; поэтому $B = \text{const.}$, что доказывает неприводимость R.

Другое доказательство можно найти у F. S. Macaulay, Algebraic Theory of Modular Systems, § 3, Cambridge 1916.

Задачи. 1. Указать в форме детерминанта критерий того, что $f(x)$ и $g(x)$ имеют общий множитель по меньшей мере степени k.

2. Для двух полиномов второй степени

$$4R = (2a_0b_2 - a_1b_1 + 2a_2b_0)^2 - (4a_0a_2 - a_1^2)(4b_0b_2 - b_1^2).$$

3. Результант полинома $f(x) = x^n + \ldots$ и его производной $f'(x)$ равен дискриминанту $f(x)$ (§ 24).

4. Результант изобарен и веса mn относительно a, b (см. § 24).

§ 73. СИСТЕМА РЕЗУЛЬТАНТОВ ДЛЯ НЕСКОЛЬКИХ ПОЛИНОМОВ ОДНОГО ПЕРЕМЕННОГО

Теорема. *Для r полиномов $f_1, \ldots, f_r$ одного переменного с неопределенными коэфициентами существует система $D_1, \ldots, D_h$ целочисленных полиномов коэфициентов, обладающих тем свойством, что при частных значениях коэфициентов из поля K условия $D_1 = 0, \ldots, D_h = 0$ необходимы и достаточны для того, чтобы либо уравнения $f_1 = 0, \ldots,$*

$f_r = 0$ *были разрешимы в подходяще подобранном поле расширения, либо чтобы формальные начальные коэфициенты всех полиномов* $f_1, \ldots, f_r$ *были равны нулю.*

Доказательство будет приведено на основании *кронекеровского метода исключения.*

Прежде всего преобразуем полиномы $f_1, \ldots, f_r$ в полиномы одинаковой степени; для этого, если n — наибольшая из (формальных) степеней, умножим каждый полином более низкой степени n_i на x^{n-ni} и на $(x-1)^{n-ni}$; таким образом из f_i мы получим два полинома формальной степени n, общие корни которых при некотором частном выборе коэфициентов совпадают с корнями f_i. Кроме того, их начальные коэфициенты совпадают с начальным коэфициентом f_i. В результате получим систему многочленов одинаковой степени, которая состоит из несколько большего числа полиномов, чем система $f_1, \ldots, f_r$, но имеет те же общие корни. Мы ее обозначим через $g_1, \ldots, g_s$.

Составим теперь из $g_1, \ldots, g_s$ линейные комбинации

$$g_u = u_1 g_1 + \ldots + u_s g_s, \quad g_v = v_1 g_1 + \ldots + v_s g_s$$

с неопределенными u, v, которые присоединим к полю K. Если при некоторых значениях коэфициентов $g_1, \ldots, g_s$ g_u и g_v имеют общий множитель, то этот множитель выражается рационально через u и v (§ 16). Но рационально зависящих от v множителей полинома g_u не может быть, так как g_u от v не зависит. Следовательно, всякий общий множитель g_u и g_v не зависит ни от v, ни от u, а потому он должен войти в $g_1, \ldots, g_s$. Обратно, если $g_1, \ldots, g_s$ имеют общий множитель, то он должен также быть общим множителем g_u и g_v.

Необходимым и достаточным условием того, что g_u и g_v имеют общий множитель или что их начальные коэфициенты равны нулю, есть равенство нулю их результанта R:

$$R = 0 \text{ тождественно относительно } u, v. \tag{1}$$

Если R расположить по произведениям степеней u и v и обозначить коэфициенты через $D_1, \ldots, D_h$, то (1) будет эквивалентно

$$D_1 = 0, \quad D_2 = 0, \quad \ldots, \quad D_h = 0.$$

Но D_i — целочисленные полиномы от неопределенных коэфициентов полиномов $f_1, f_2, \ldots, f_r$. Тем самым теорема полностью доказана.

Система $D_1, \ldots, D_h$ называется *системой результантов* многочленов $f_1, \ldots, f_r$.

Из § 71 следует, что

$$\begin{aligned} R &\equiv 0 \ (g_u, g_v) \\ &\equiv 0 \ (g_1, \ldots, g_s) \\ &\equiv 0 \ (f_1, f_2, \ldots, f_r), \end{aligned}$$

а отсюда, если обе части расположить по произведениям степеней u_i и v_i, имеем:

$$(D_1, \ldots, D_h) \equiv 0 \, (f_1, \ldots, f_r), \tag{2}$$

Замечания. 1. Если заранее известно относительно некоторого многочлена f_v, например f_1, что его формальный начальный коэфициент не

равен нулю, то указанные выше операции преобразования f_ν в полиномы одинаковой степени становятся лишними. Кроме того, можно в данном случае несколько упростить вычисление, рассматривая вместо g_u и g_v результант от f_1 и $v_2 f_2 + \ldots + v_r f_r$.

2. Очевидно, что и здесь, как в § 71, можно формально обойти случай исчезания всех начальных коэфициентов, переходя к однородным формам x_1 и x_2. В этом случае, чтобы получить g_i из f_i, следует умножить их на $x_1^{n-n_i}$ и $x_2^{n-n_i}$ (вместо x^{n-n_i} и $(x-1)^{n-n_i}$).

3. В случае одного полинома указанные преобразования приводят к системе результантов, состоящей только из нуля.

§ 74. ОБЩАЯ ТЕОРИЯ ИСКЛЮЧЕНИЯ

Здесь и ниже символ $\{\xi_1, \ldots, \xi_n\}$ будет обозначать последовательность из n занумерованных элементов подходяще выбранного расширения основного поля K. Если $f(\xi_1, \ldots, \xi_n) = 0$, где f — полином, то последовательность $\{\xi_1, \ldots, \xi_n\}$, или коротко ξ, называется *корнем* f. Задача общей теории исключения состоит в том, чтобы по крайней мере теоретически определить все решения произвольной системы алгебраических уравнений

$$f_1(\xi) = 0, \quad f_2(\xi) = 0, \quad \ldots, \quad f_r(\xi) = 0,$$

т. е. все общие корни полиномов $f_1, \ldots, f_r$ из $K[x_1, \ldots, x_n]$ [1]).

Мы приведем здесь метод „последовательного исключения" всех неизвестных с помощью системы результантов предыдущего параграфа. При этом целесообразно предположить, что в систему $f_1, \ldots, f_r$ входит полином степени α, у которого коэфициент при x_1^α есть постоянная, отличная от нуля. Если это обстоятельство не имеет места, то мы поступаем следующим образом: *либо* все полиномы $f_1, \ldots, f_r$ исчезают тождественно; тогда решением будет всякая система значений $\{\xi_1, \ldots, \xi_n\}$. *Либо* существует f_i, например f_1, не исчезающее тождественно. В этом случае вводим новые переменные $x_1', \ldots, x_n'$ с помощью подстановки

$$\left.\begin{aligned} x_1 &= u_1 x_1', \\ x_2 &= x_2' + u_2 x_1', \\ &\cdots\cdots\cdots \\ x_n &= x_n' + u_n x_1', \end{aligned}\right\} \qquad (1)$$

где $u_1, \ldots, u_n$ — неизвестные, которые мы присоединяем к полю K. Подставляя (1) в $f_1, \ldots, f_r$, получим новые полиномы $f_1', \ldots, f_r'$ [2]) от переменных $x_1', \ldots, x_n'$, у которых коэфициент при наивысшей степени x_1' является теперь не исчезающим полиномом от $u_1, \ldots, u_n$. А именно, если α есть степень f_1, то

$$f_1' = f_1(u_1 x_1', x_2' + u_2 x_1', \ldots, x_n' + u_n x_1'),$$

---

[1]) Практически указанный метод вычисления корней непомерно громоздок.

[2]) Очевидно, что это не производные.

и в этом выражении коэфициентом при $x_1'^{\alpha}$ будет $f_1^*(u_1, \ldots, u_n)$, где f_1^* — составная часть f_1 наивысшей (α-й) степени [1]).

Теперь можно исключить x_1' и найти систему результантов

$$d_1, \ldots, d_l,$$

зависящих исключительно от $x_2', \ldots, x_n'$. Корень $\{\xi_2', \ldots, \xi_n'\}$ этой системы результантов определяет (так как неисчезание начальных коэфициентов было заранее обеспечено) по крайней мере один корень $\{\xi_1', \ldots, \xi_n'\}$ полиномов $f_1, \ldots, f_n$, и таким образом получаются все корни. Недостающее неизвестное ξ_1' можно определить из системы уравнений, общий наибольший делитель которых отличен от постоянной, т. е. всякий раз мы будем иметь для ξ_1' алгебраическое уравнение по крайней мере первой степени. Если $d_1, \ldots, d_l$ не исчезают тождественно, то мы продолжим подобным же образом преобразования (вводим $x_2'', \ldots, x_n''$ вместо $x_2', \ldots, x_n'$) и исключение и т. д. Процесс заканчивается на s-м шагу, если после исключения $x_1', x_2'', \ldots, x_s^{(s)}$ мы придем к тождественно исчезающей системе полиномов от $x_{s+1}^{(s)}, \ldots, x_n^{(s)}$. Если же это не имеет места, то процесс продолжается до тех пор, пока не исключатся все неизвестные. При этом если полученные результанты (равные постоянным) не равны нулю, то наша система уравнений, очевидно, неразрешима. В первом же случае, когда после s преобразований результанты равны нулю, можно $x_{s+1}^{(s)}, \ldots, x_n^{(s)}$ заменить произвольными значениями $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ и затем последовательно (в обратном порядке) определить $\xi_1', \xi_2'', \ldots, \xi_s^{(s)}$. Для всякой системы значений $\{\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}\}$ найдется конечное число систем значений $\{\xi_1', \xi_2'', \ldots, \xi_s^{(s)}\}$, из которых с помощью подстановки (1) получаются системы $\{\xi_1, \xi_2, \ldots, \xi_n\}$, удовлетворяющие первоначальным уравнениям.

Можно также $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ заменить неизвестными и найти затем $\xi_1', \ldots, \xi_n^{(s)}$ в виде одной или нескольких систем алгебраических функций этих неизвестных; однако заметим, что могут существовать частные решения $\{\xi_1, \ldots, \xi_n\}$, которые нельзя получить из общего решения, как это видно из следующего примера.

Пусть

$$f_1 = x_1^2 + x_1 x_2,$$
$$f_2 = x_1 x_2 + x_2^2 + x_1 + x_2.$$

Преобразование (1) здесь бесполезно, так как f_1 содержит член x_1^2. Результант по x_1 должен тождественно исчезать, ибо при всяком значении x_2 f_1 и f_2 имеют общим множителем $x_1 + x_2$. Отсюда для неизвестного ξ_2 получаем $\xi_1 = -\xi_2$. Но если возьмем частное решение $\xi_2 = -1$, то f_2 станет равным нулю, и для ξ_1 кроме значения $+1$ найдется

[1]) Замечание: вместо неизвестных u_ν можно использовать частные значения u_ν в основном поле или (если это поле конечно) частные значения из подходяще выбранного поля расширения, которые подбираются так, чтобы для них $f^*(u_1, \ldots, u_n)$ не исчезало.

еще значение 0. Но систему значений $\{0, -1\}$ никак нельзя получить из общего решения $\xi_1 = -\xi_2$.

Как в этом примере, так и в общем случае „алгебраическое многообразие" общих корней $f_1, \ldots, f_r$ распадается на „неразложимые многообразия" разных „измерений", допускающие „параметрическое представление" с помощью алгебраических функций. Соответствующее доказательство (которое не зависит от теории исключения) см. в главе 13. Точное вычисление этих многообразий и параметрических представлений можно провести с помощью теории исключения, но мы на этом не будем останавливаться [1]).

Из сравнения (2) предыдущего параграфа следует сравнение

$$(d_1, \ldots, d_l) \equiv 0 \ (f_1', \ldots, f_r'), \tag{2}$$

имеющее место в области полиномов $\mathsf{K}(u)[x_1', \ldots, x_n']$.

Отсюда получается интересный результат для случая, когда исключение приводит к результантам, состоящим из не равных нулю постоянных. А именно, в этом случае

$$1 \equiv 0 \ (f_1, \ldots, f_r).$$

В более подробной формулировке: *если полиномы* $f_1, \ldots, f_r$ *из* $\mathsf{K}[x_1, \ldots, x_n]$ *в любом алгебраическом поле над* K *не имеют общих корней, то в* $\mathsf{K}[x_1, \ldots, x_n]$ *удовлетворяется равенство*

$$1 = A_1 f_1 + \ldots + A_r f_r.$$

Доказательство (методом полной индукции по числу переменных). Для постоянных f_i или для полиномов одного переменного все ясно. Пусть теорема верна для полиномов от $n-1$ переменных. Для n переменных первые результанты $d_1, \ldots, d_l$ будут полиномами от $n-1$ переменных; эти полиномы также не имеют общих корней. Поэтому в $\mathsf{K}(u)[x_2', \ldots, x_n']$

$$1 = B_1 d_1 + \ldots + B_l d_l.$$

Отсюда в силу (2) следует, что

$$1 = A_1' f_1' + \ldots + A_r' f_r'.$$

Заменим здесь x_i' их значениями из (1); тогда f_i' перейдут в f_i. Выражение справа рационально относительно u; если умножим обе части равенства на знаменатель $g(u)$, то получим:

$$g(u) = A_1(u) \cdot f_1 + \ldots + A_r(u) \cdot f_r.$$

Сравним коэфициенты какого-нибудь произведения степеней u, у которого коэфициент слева отличен от нуля; тогда будем иметь:

$$1 = A_1 f_1 + \ldots + A_r f_r.$$

Задача. Если степени f_i ограничены, то ограничены также степени полиномов $A_1, \ldots, A_r$.

---

[1]) См., например, книжку F. S. Macaulay, Algebraic Theory of Modular Systems, Cambridge Tracts. № 19, Cambridge 1916.

§ 75. ТЕОРЕМА ГИЛЬБЕРТА О КОРНЯХ

Обобщением теоремы, доказанной в конце предыдущего параграфа, является следующая *теорема Гильберта о корнях.*

Если f — полином $\mathsf{K}[x_1, \ldots, x_n]$, равный нулю для всех значений, обращающих в нуль полиномы $f_1, \ldots, f_r$, то

$$f^\rho \equiv 0 \ (f_1, \ldots, f_r)$$

для некоторого натурального числа ρ (и обратно).

Доказательство [1]). Для $f = 0$ утверждение очевидно. В случае $f \neq 0$ присоединим новое переменное z. Тогда полиномы

$$f_1, \ldots, f_r, \ 1 - zf$$

из $\mathsf{K}[x_1, \ldots, x_n, z]$ не имеют общих корней, так как общий корень $f_1, \ldots, f_r$ является корнем f, но не $1 - zf$. Поэтому в силу теоремы предыдущего параграфа

$$1 = A_1 f_1 + \ldots + A_r f_r + A(1 - zf).$$

Подставим в это тождество $z = \frac{1}{f}$ и умножим затем, чтобы освободиться от дроби, обе части на некоторую степень f^ρ. Тогда получится:

$$f^\rho = B_1 f_1 + \ldots + B_r f_r,$$

что и требовалось доказать.

Обратное очевидно.

Из этого доказательства и задачи § 74 следует, что существует верхняя граница ρ, которая определяется степенями $f_1, \ldots, f_r$ и f. Но на самом деле оказывается, что верхняя граница ρ зависит *только* от $f_1, \ldots, f_r$, как это будет показано в § 91.

Обобщение теоремы о корнях. *Если полиномы $h_1, \ldots, h_k$ обращаются в нуль для всех общих корней полиномов $f_1, \ldots, f_r$, то*

$$(h_1, \ldots, h_k)^\sigma \equiv 0 \ (f_1, \ldots, f_r)$$

или: любое произведение степеней h_i с суммой показателей, равной σ принадлежит идеалу $(f_1, \ldots, f_r)$ (и обратно).

Доказательство. Имеем, что

$$h_i^{\rho_i} \equiv 0 \ (f_1, \ldots, f_r).$$

Положим

$$\sigma = (\rho_1 - 1) + (\rho_2 - 1) + \ldots + (\rho_k - 1) + 1.$$

Произведение $h_1^{l_1} \ldots h_k^{l_k}$ при $l_1 + \ldots + l_k = \sigma$ содержит по крайней мере один множитель $h_i^{\rho_i}$, так как в противном случае сумма $l_1 + \ldots + l_k$ была бы меньше или равна $(\rho_1 - 1) + \ldots + (\rho_k - 1) = \sigma - 1$. Отсюда следует справедливость теоремы.

Обратное очевидно.

---

[1]) См. A. Rabinowitsch, Math. Ann., т. 102, стр. 518, 1929.

§ 76. КРИТЕРИЙ РАЗРЕШИМОСТИ ОДНОРОДНОЙ СИСТЕМЫ УРАВНЕНИЙ

В § 74 был указан метод, с помощью которого можно узнать, имеет или не имеет решения рассматриваемая система алгебраических уравнений. Но это еще не *„алгебраический критерий"* разрешимости, когда мы имеем систему целых рациональных функций коэфициентов, и обращение в нуль этой системы является необходимым и достаточным условием разрешимости (как, например, результант § 71 и система результантов § 73 в случае одного неизвестного или определитель системы линейных *однородных* уравнений). Такого критерия вообще не существует [1]), за исключением, например, случая однородных уравнений.

Если $f_1, \ldots, f_r$ — однородные полиномы $x_1, \ldots, x_n$ $(n > 1)$ и ни один из них не является постоянной, то мы прежде всего будем всегда иметь „тривиальный" корень $\{0, \ldots, 0\}$. Постараемся установить критерий существования нетривиального корня $\{\eta_1, \ldots, \eta_n\}$; тем самым в силу однородности будет существовать целый *„луч"* корней $\{\lambda\eta_1, \ldots, \lambda\eta_n\}$ [2]).

Нижеследующий вывод принадлежит Г. Капфереру [3]). Он исходит из кронекеровского метода последовательных исключений, рассматривая формы $f_1, \ldots, f_r$ как полиномы x_1 и составляя систему результантов $D_1, \ldots, D_h$ [но без подготовительного преобразования (1) § 74]. Тогда оказывается, что если $f_1, \ldots, f_r$ имеют общий нетривиальный корень, то $D_1, \ldots, D_h$ как полиномы $x_2, \ldots, x_n$ имеют также нетривиальный общий корень, и обратно.

При доказательстве следует различать два случая.

Случай 1. Существует по крайней мере один полином f_λ, содержащий член вида cx_1^m (c — постоянная). В этом случае из нетривиального корня $\{\xi_2, \ldots, \xi_n\}$ системы $D_1, \ldots, D_h$ получается согласно определению системы результантов по крайней мере один корень $\{\xi_1, \ldots, \xi_n\}$ полиномов $f_1, \ldots, f_r$, который не может быть, очевидно, тривиальным, и обратно, из каждого такого корня $\{\xi_1, \ldots, \xi_n\}$ получается также нетривиальный корень $\{\xi_2, \ldots, \xi_n\}$ D_ν; в самом деле, если бы $\xi_2, \ldots, \xi_n$ были равны нулю, то из $f_\lambda = c\xi_1^m + \ldots = 0$ сразу следовало бы $\xi_1 = 0$.

---

[1]) Это видно из следующего примера: уравнения

$$\left.\begin{aligned} a_1x_1 + a_2x_2 + a_3 &= 0, \\ b_1x_1 + b_2x_2 + b_3 &= 0 \end{aligned}\right\}$$

„в общем", т. е. при $a_1b_2 - a_2b_1 \neq 0$, разрешимы. Если бы условие

$$D_1(a, b) = 0, \ldots, D_h(a, b) = 0$$

было необходимым и достаточным для разрешимости, то D должны были исчезать при неопределенных a, b, т. е. тождественно исчезать. Тем самым уравнения были бы всегда разрешимы, что неверно. (Неравенство $a_1b_2 - a_2b_1 \neq 0$ также не является необходимым и достаточным.)

[2]) Корни $\{\lambda\eta_1, \ldots, \lambda\eta_n\}$ образуют при постоянном η и переменном λ прямую пространства R_n, исходящую из начала $\{0, \ldots, 0\}$ и потому называемую „лучом". Луч можно также рассматривать как „точку проективного пространства" P_{n-1}, однородные координаты которой суть η (см. § 87).

[3]) Kapferer H.: Über Resultanten und Resultantensysteme. Sitzungsber. Bayer. Akad. München 1929, стр. 179—200.

Случай 2. Полиномы не содержат членов вида cx_1^m. Тогда согласно § 73 будут тождественно равны нулю $D_1, \ldots, D_h$; таким образом будет также существовать нетривиальное решение, например $\{1,1, \ldots, 1\}$, системы $D_1, \ldots, D_h$. Но в этом случае $f_1, \ldots, f_r$ наверное имеют нетривиальный корень, а именно $\{1,0, \ldots, 0\}$, так как член с наивысшей степенью x_1 всюду отсутствует.

Итак, приведенное выше утверждение доказано. Так как $D_1, \ldots, D_h$ однородны относительно $x_2, \ldots, x_n$, то можно исключение продолжить и исключить x_2 и т. д., пока, наконец, не получится система форм одного лишь x_n:

$$b_1 x_n^{s_1},\ b_2 x_n^{s_2}, \ldots, b_k x_n^{s_k}. \tag{1}$$

Для существования нетривиального корня этих форм необходимо и достаточно, чтобы исчезали все коэфициенты $b_1, \ldots, b_k$.

Но величины $b_1, \ldots, b_k$ были получены из коэфициентов первоначальных форм определенным целым рациональным процессом, зависящим только от степеней $f_1, \ldots, f_r$; поэтому $b_1, \ldots, b_k$ суть целочисленные полиномы коэфициентов $f_1, \ldots, f_r$.

Система многочленов $b_1, \ldots, b_k$ (или любая система, равенство нулю которой указывает на существование корня) называется также *системой результантов* форм $f_1, \ldots, f_r$.

Если доказанное выше сравнение

$$(D_1, \ldots, D_h) \equiv 0 \ (f_1, \ldots, f_r) \tag{2}$$

записывать на каждом этапе последовательных исключений, то из всех этих сравнений в итоге получится

$$x_n^{s_\nu} b_\nu \equiv 0 \ (f_1, \ldots, f_r). \qquad (\nu = 1, \ldots, k) \tag{3}$$

Далее, из закона образования $b_1, \ldots, b_k$ легко следует, что они суть однородные формы коэфициентов каждого отдельного f_i. В самом деле, $D_1, \ldots, D_h$ получаются из результанта R, содержащего коэфициенты a_ν полиномов f_i только в комбинации $a_\nu u_i$ и $a_\nu v_i$. Таким образом всякий член R относительно a_ν имеет ту же степень, что и по отношению к u_i и v_i, взятых вместе; если R расположить по произведениям степеней u и v, то коэфициент D_j такого произведения будет однородным полиномом a_ν определенной степени. Рассуждая подобным образом на втором, третьем и т. д. этапах исключения, получим наше утверждение.

Резюмируем результаты этого параграфа:

r форм $f_1, \ldots, f_r$ с неопределенными коэфициентами обладают системой результантов, состоящей из целочисленных полиномов b_ν от этих коэфициентов; для частных значений коэфициентов в каком-нибудь поле K условие равенства нулю всех результантов является необходимым и достаточным для существования решения уравнений $f_1 = 0, \ldots, f_r = 0$, отличного от нуля. b_ν однородны относительно коэфициентов каждой отдельной формы f_i и удовлетворяют сравнению (3).

Задачи. 1. Как будет выглядеть система результантов для случая системы линейных форм?

2. Если $\varphi_1(t_1, t_2), \ldots, \varphi_n(t_1, t_2)$ n однородных форм, не имеющих общего множителя, и рассматривается совокупность всех точек ξ

проективного пространства, отношения координат которых определяются из уравнений:

$$\xi_1 : \xi_2 : \ldots : \xi_n = \varphi_1(\tau_1, \tau_2) : \varphi_2(\tau_1, \tau_2) : \ldots : \varphi_n(\tau_1, \tau_2) \qquad (4)$$

для нетривиальных значений τ, то эта совокупность, включая систему значений $\{0, \ldots, 0\}$, характеризуется также однородным уравнением $F(\xi_1, \ldots, \xi_n) = 0$ [прежде всего следует пропорцию (4) свести к однородным уравнениям относительно ξ и τ].

3. Если система однородных уравнений $f_1(x_1, \ldots, x_n) = 0, \ldots,$ в которые, кроме x, рационально входят еще неопределенные параметры, разрешима при неопределенных значениях параметров, то она разрешима и при всяком частном значении параметров.

4. Существует алгебраический критерий разрешимости системы уравнений относительно нескольких последовательностей $x_1, \ldots, x_n; y_1, \ldots, y_m; \ldots$ неизвестных, причем данные уравнения однородны относительно каждой из этих последовательностей.

Методы отыскания решений однородных уравнений см. еще у F. Mertens: Sitzgsber. Wiener Akad. Wiss., т. 108, (1889), стр. 1174; см. также § 79 настоящей книги.

§ 77. ИНЕРТНЫЕ ФОРМЫ

В предыдущих параграфах мы рассматривали систему результантов произвольного числа однородных форм; теперь оказывается, что для n форм n переменных надо исходить из одного результанта, а для числа форм $m < n$ никакое условие разрешимости не является вообще необходимым. Чтобы это показать, придется доказать ряд теорем, относящихся к так называемым „инертным формам".

Пусть

$$\begin{aligned} f_1 &= a_1 x_1^{\alpha} + a_2 x_1^{\alpha-1} x_2 + \ldots + a_\omega x_n^{\alpha}, \\ f_2 &= b_1 x_1^{\beta} + b_2 x_1^{\beta-1} x_2 + \ldots + b_\omega x_n^{\beta}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ f_r &= e_1 x_1^{\varepsilon} + e_2 x_1^{\varepsilon-1} x_2 + \ldots + e_\omega x_n^{\varepsilon} \end{aligned}$$

r форм соответственно степеней $l_1 = \alpha$, $l_2 = \beta$, $\ldots$, $l_r = \varepsilon$. Эти формы состоят из всевозможных членов указанной степени с неопределенными коэфициентами. Последние коэфициенты (т. е. коэфициенты при $x_n^{\alpha}, x_n^{\beta}, \ldots, x_n^{\varepsilon}$) обозначены через $a_\omega, b_\omega, \ldots, e_\omega$. Все дальнейшие рассуждения будут относиться к целочисленным полиномам от неизвестных $x_1, \ldots, x_n, a, \ldots, e_\omega$.

Уже в § 76 мы встретились с полиномами T от коэфициентов $a_1, \ldots, e_\omega$, обладающими свойством

$$x_i^{\tau} T \equiv 0 (f_1, \ldots, f_r) \qquad (1)$$

для некоторого i и τ. Такой полином T называется по Гурвицу *инертной формой*. Вся система результантов § 76 состоит из инертных форм.

Можно инертные формы определить еще иначе. А именно, положим

$$\begin{aligned} f_1 &= f_1^* + a_\omega x_n^{\alpha}, \\ &\ldots\ldots\ldots \\ f_r &= f_r^* + e_\omega x_n^{\varepsilon}. \end{aligned}$$

Тогда, производя подстановку

$$\left.\begin{aligned} a_\omega &= -\frac{f_1^*}{x_n^\alpha}, \\ &\cdots\cdots \\ e_\omega &= -\frac{f_r^*}{x_n^\varepsilon}, \end{aligned}\right\} \tag{2}$$

мы достигнем того, что $f_1, \ldots, f_r$ в (1) станут равными нулю. Тогда в сравнении (1) исчезнет левая часть; но так как x_i подстановкой не затрагиваются, то T после подстановки должно обратиться в нуль:

$$T\left(a_1, \ldots, -\frac{f_1^*}{x_n^\alpha}; \ldots; e_1, \ldots, -\frac{f_r^*}{x_n^\varepsilon}\right) = 0. \tag{3}$$

Мы видим, что если сравнение (1) удовлетворяется хотя бы для *одного* x_i, то тем самым имеет место (3).

Обратно, если какой-нибудь полином $T(a_1, \ldots, a_\omega, \ldots, e_1, \ldots, e_\omega)$ удовлетворяет (3), то, располагая T по степеням $a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\varepsilon}$, легко видим из (3), что член, не зависимый от этих величин, исчезает; таким образом получается:

$$T \equiv 0\left(a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\varepsilon}\right)$$

в области дробей со знаменателем вида x_n^λ. Если умножить на знаменатель наивысшей степени, то все дроби станут целыми, и получится

$$x_n^\tau T \equiv 0\,(f_1, \ldots, f_r).$$

Итак: если (1) имеет место для какого-нибудь x_i, то удовлетворяется (3), а если удовлетворяется (3), то выполняется (1) для x_n. Отсюда прежде всего вытекает, что если (1) справедливо для некоторого x_i, то оно верно и для x_n; поэтому, так как индекс n особой роли не играет, получается, что (1) справедливо для любого x_j и (1) равносильно (3): *уравнение* (3) *так же характеризует инертную форму, как и* (1).

Сумма или разность двух инертных форм, очевидно, также является инертной; подобный же вывод можно сделать относительно кратных инертной формы. Таким образом инертные формы T образуют идеал $\mathfrak{T}$.

Легко видеть, что идеал $\mathfrak{T}$ простой. А именно, если произведение $T_1 T_2$ обладает свойством (3), то этим свойством должен обладать один из сомножителей.

Инертные формы играют роль, аналогичную роли системы результантов § 76. А именно, если формы $f_1, \ldots, f_r$ допускают (нетривиальный) общий корень, то после подстановки этого корня в (1) правая часть обратится в нуль, и, так как не все x_i нули, получается, что $T = 0$ для каждой инертной формы. Обратно, если для данной системы $f_1, \ldots, f_r$ обращаются в нуль *все* инертные формы, то будет также равна нулю и система результантов; поэтому должен существовать

общий корень. Отсюда следует, что если найден какой-нибудь базис идеала $\mathfrak{T}$ инертных форм, то можно применять его в качестве системы результантов.

Докажем теперь следующую теорему:

Если число r форм f_i меньше числа n переменных, то все инертные формы равны нулю. Если же $r = n$, то все инертные формы, независимые от e_ω, равны нулю.

Из первой половины этой теоремы следует, что система результантов m форм ($m < n$) тождественно обращается в нуль, т. е. в этом случае всегда существует общий корень.

Доказательство. Пусть сперва $r < n$. Если бы инертная форма T была отлична от нуля, то из (3) следовало бы, что

$$-\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_r^*}{x_n^\varepsilon}$$

алгебраически зависимы относительно области полиномов величин $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$. Можно положить $x_n = 1$; это не изменит справедливости нашего утверждения.

Точно так же в случае $r = n$, если бы теорема была неверна, следовало бы, что

$$-\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_{n-1}^*}{x_n^\delta}$$

(где δ — степень формы f_{n-1}) алгебраически зависимы (f_n^* не входит, так как T должно быть независимым от e_ω). И здесь можно положить $x_n = 1$.

В том и в другом случаях последовательность полиномов

$$\left[-f_1^*\right]_{x_n=1}, \ldots, \left[-f_s^*\right]_{x_n=1} \quad (s < n)$$

была бы алгебраически зависима относительно области полиномов $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$. Но мы имеем следующую лемму.

Лемма. *Если последовательность полиномов $f_1, \ldots, f_s$ от переменных $a_1, \ldots, a_p, x_1, \ldots, x_q$ алгебраически зависима относительно $\mathsf{K}[a_1, \ldots, a_t]$, где K — область целостности, то эта зависимость остается в силе при всяком частном значении $a_p = \alpha$ ($\alpha \in \mathsf{K}$).*

Доказательство леммы. По предположению

$$F(a_1, \ldots, a_p, f_1, \ldots, f_s) = 0, \tag{4}$$

причем F — полином и для неизвестных $z_1, \ldots, z_s$

$$F(a_1, \ldots, a_p, z_1, \ldots, z_s) \not\equiv 0. \tag{5}$$

Можно допустить, что полином $F(a, z)$ не содержит множителем $a_p - \alpha$, так как в противном случае мы бы (4) и (5) сократили на этот множитель. Тогда F также не будет обращаться в нуль при $a_p = \alpha$:

$$F(a_1, \ldots, a_{p-1}, \alpha, z_1, \ldots, z_s) \not\equiv 0.$$

Но (4) остается в силе и при $a_p = \alpha$, откуда и следует справедливость леммы.

Применяя лемму несколько раз, получим, что алгебраическая зависимость сохраняется при частном значении некоторых или всех неизвестных a.

Теперь легко можно закончить прерванное доказательство. Выберем частные значения величин $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$ так, чтобы формы $f_1^*, \ldots, f_s^*$ перешли в $x_1^\alpha, \ldots, x_s^\delta$. В силу $s < n$ эти выражения при $x_n = 1$ не изменятся. Так как алгебраическая зависимость сохраняется и при частных значениях, то выражения $x_1^\alpha, \ldots, x_s^\delta$ должны быть алгебраически зависимыми. Но это, очевидно, невозможно, а потому наше предположение неверно, и теорема доказана.

Что верно для $r < n$, то уже неверно для $r = n$. Оказывается, что при $r = n$ *существует инертная форма* D_e, *не обращающаяся в нуль. Она однородна относительно* $a_1, \ldots, a_\omega, b_1, \ldots, b_\omega$ *и т. д. и имеет степень* $L_n = l_1 l_2 \ldots l_{n-1}$ *относительно* $e_1, \ldots, e_\omega$.

Доказательство. Положим

$$\sum_1^n (l_i - 1) = l - 1.$$

Совокупность всех произведений x_i степени l можно упорядочить следующим образом:

Сперва идут все произведения степеней, содержащие $x_1^{l_1}$; *затем* идут произведения, содержащие $x_2^{l_2}$, но не $x_1^{l_1}$, и т. д. *Наконец,* идут произведения, содержащие $x_n^{l_n}$, но не $x_1^{l_1}, x_2^{l_2}$ и т. д.

В результате мы переберем все произведения степени l, так как не учтенными оказываются только такие произведения, которые содержат x_1 не выше чем в $l_1 - 1$-й степени и т. д., наконец, x_n не выше чем в $l_n - 1$-й степени, а степень этих произведений не выше $\Sigma(l_i - 1)$, т. е. никак не равна l. Обозначим теперь учтенные произведения через

$$H_{l-l_1}^{(\nu)} x_1^{l_1}, \quad H_{l-l_2}^{(\nu)} x_2^{l_2}, \ldots, \quad H_{l-l_n}^{(\nu)} x_n^{l_n}, \tag{6}$$

где $H_{l-l_i}^{(\nu)}$ — произведение степени $l - l_i$. В частности к последней категории H_{l-l_n} принадлежат только произведения степени $< l_1$ относительно $x_1, \ldots,$ степени $< l_{n-1}$ относительно x_{n-1}, а степень x_n определяется тем требованием, что общая степень произведения H_{l-l_n} должна быть равна $l - l_n$. Таким образом последняя категория состоит из $l_1 l_2 \ldots l_{n-1}$ произведений степеней.

Теперь берем формы вида:

$$H_{l-l_i}^{(\nu)} f_i; \tag{7}$$

число этих форм, очевидно, равно числу произведений (6) степени l. Матрица коэфициентов форм (7) является квадратной; ее определитель D_e при $f_i = x_i^{l_i}$ равен единице. Таким образом D_e не исчезает тождественно. Кроме того D_e — инертная форма, так как, если умножить равенства

$$H_{l-l_i}^{(\nu)} f_i = \sum a_{\nu\mu} H_l^{(\mu)}$$

на алгебраические дополнения какого-нибудь столбца D_e и сложить, то

слева получится линейная комбинация от f_i, а справа $D_e \cdot H_l^{(\mu)}$. Если в частности положить $H_l^{(\mu)} = x_i^l$, то будем иметь:

$$D_e x_i^l \equiv 0 (f_1, \ldots, f_r).$$

Наконец, D_e однородно относительно коэфициентов каждой отдельной формы f_i, а относительно коэфициентов f_n она будет степени $L_n = l_1 l_2 \ldots l_{n-1}$. Тем самым теорема доказана.

У A. Hurwitz, Über die Trägheitsformen eines algebraischen Moduls, Annali di Matematica (3a), 20, 1913, читатель найдет дальнейшие свойства инертных форм.

§ 78. РЕЗУЛЬТАНТ n ФОРМ n ПЕРЕМЕННЫХ

Возьмем n общих форм (т. е. форм с неизвестными или неопределенными коэфициентами) $f_1, \ldots, f_n$ от переменных $x_1, \ldots, x_n$ и рассмотрим идеал $\mathfrak{T}$ инертных форм. Станем искать в $\mathfrak{T}$ полином наиболее низкой степени относительно e_ω. Такой полином обязательно должен существовать, и его степень относительно e_ω не равна нулю, так как, кроме нуля, не имеется другой инертной формы, независимой от e_ω. Если разложим этот полином на неразложимые множители, то по крайней мере один из сомножителей должен принадлежать $\mathfrak{T}$, так как $\mathfrak{T}$ — простой идеал. Кроме того, этот множитель имеет ту же степень относительно e_ω, что и весь полином, так как в $\mathfrak{T}$ больше нет многочлена более низкой степени. Обозначим наш множитель через R и докажем такую теорему:

Всякий полином идеала $\mathfrak{T}$ делится на R.

Доказательство. Расположим R по нисходящим степеням e_ω:

$$R = S e_\omega^\lambda + \ldots \quad (\lambda > 0,\ S \not\equiv 0).$$

Пусть теперь T — полином из $\mathfrak{T}$. Так как T относительно e_ω имеет степень не ниже чем λ, то мы можем T умножить на S и затем понизить степень e_ω, вычитая кратное R. Продолжая этот процесс до тех пор, пока не получится степень, которая меньше λ, придем к уравнению вида:

$$S^j T - QR = T'.$$

T' также принадлежит $\mathfrak{T}$, и его степень относительно e_ω меньше λ; поэтому T' должно быть равно нулю. Таким образом $S^j T$ делится на R. Но R неразложимо и S не делится на R (не делится, так как S от e_ω не зависит); поэтому T делится на R, что и требовалось доказать.

Итак, $\mathfrak{T}$ — главный идеал с базисом R. При этом R определяется однозначно до постоянного множителя. Назовем R *результантом* форм $f_1, \ldots, f_n$. Целесообразность этого названия сразу оправдывается. А именно, если R обращается в нуль для частных значений коэфициентов форм $f_1, \ldots, f_n$, то исчезают все формы идеала $\mathfrak{T}$, в частности обращаются в нуль все формы системы результантов $f_1, \ldots, f_n$; отсюда $f_1, \ldots, f_n$ имеют нетривиальный общий корень. Обратно, если $f_1, \ldots, f_n$ имеют нетривиальный общий корень, то, подставляя этот корень в тождество

$$x_i^\lambda R = A_1 f_1 + \ldots + A_n f_n$$

мы обратим в нуль правую часть, а потому будет равна нулю и левая

часть тождества; но по крайней мере существует одно x_i, не равное нулю, откуда $R=0$. Согласно замечанию в предыдущем параграфе, мы действительно имеем право назвать R *результантом* форм $f_1, \ldots, f_n$: *равенство нулю R необходимо и достаточно для существования нетривиального решения.*

Теперь докажем еще несколько формальных теорем относительно результанта, которые необходимы для определения степени R.

Если $f_1 = g \cdot h$, где g и h — общие формы степеней μ, ν $(\mu + \nu = l_1)$, то R *делится на произведение*

$$R_g \cdot R_h = R(g, f_2, \ldots, f_n) \cdot R(h, f_2, \ldots, f_n).$$

Доказательство. Из

$$x_n^j R = A_1 f_1 + \ldots + A_n f_n$$

следует при $f_1 = g \cdot h$:

$$x_n^j \cdot R(gh, f_2, \ldots, f_n) = A_1 gh + A_2 f_2 + \ldots + A_n f_n;$$

таким образом $R(gh, f_2, \ldots, f_n)$ принадлежит как идеалу $\mathfrak{T}_g$, порожденному формами $g, f_2, \ldots, f_n$, так и идеалу $\mathfrak{T}_h$, порожденному $h, f_2, \ldots, f_n$.

Следовательно, $R(gh, f_2, \ldots, f_n)$ делится как на R_g, так и на R_h, а потому делится на их произведение $R_g R_h$ (так как R_g и R_h неразложимы и различны), что и требовалось доказать.

Если теперь подобрать $f_1, \ldots, f_{n-1}$ так, чтобы каждое из них было равно произведению линейных форм, то, применяя несколько раз только что доказанную теорему, получим, что R делится на произведение $L_n = l_1 l_2 \ldots l_{n-1}$ частичных результантов; каждый из них содержит e_i. Таким образом произведение имеет по меньшей мере степень L_n относительно e_i. С другой стороны, мы видели, что степень R относительно e_i не выше L_n, откуда следует, что степень в точности равна L_n.

Совершенно так же, как D_e (§ 77), мы можем образовать $D_a, D_b, \ldots$, располагая формы $f_1, \ldots, f_n$ так, чтобы f_1 или f_2 или f_3 и т. д. всякий раз оказывались в конце. Тогда окажется, что степень D_a относительно a_i равна $L_1 = l_2 l_3 \ldots l_n$, степень D_b относительно b_i равна $L_2 = l_1 l_3 \ldots l_n$ и т. д.; все $D_a, D_b, \ldots, D_e$ делятся на R, и R имеет относительно a_i степень L_1, относительно b_i — степень L_2 и т. д. Определение R как элемента базиса идеала $\mathfrak{T}$ не зависит от порядка следования форм $f_1, \ldots, f_n$. Вместе с тем можно убедиться, что степень R равна наивысшей степени, которую вообще может иметь общий делитель $D_a, D_b, \ldots, D_e$; следовательно: R есть *общий наибольший делитель полиномов* $D_a, D_b, \ldots, D_e$.

При $f_i = x_i^{l_i}$ $(i = 1, \ldots, n)$ D_e равно единице, а R есть делитель D_e; таким образом, при $f_i = x_i^{l_i}$, $R = \pm 1$, т. е. вообще R содержит член

$$\pm a_1^{L_1} \ldots e_\omega^{L_n}.$$

Нормируем R так, чтобы этот „главный член“ входил со знаком плюс.

Прежняя формулировка: „R делится на $R_g R_h$ при $f_1 = g \cdot h$“ теперь уточняется следующим образом:

$$R_{gh} = R_g \cdot R_h.$$

Это следует из сравнения степеней и главных членов.

Объединяя все вместе, имеем:

n общих форм n переменных обладают результантом R, который является неразложимым целочисленным полиномом относительно коэфициентов форм, и этот результант можно определить как базис идеала инертных форм. Обращение в нуль результанта для частных $f_1, \ldots, f_n$ *с коэфициентами из некоторого поля является необходимым и достаточным условием существования отличного от нуля решения системы уравнений* $f_1 = 0, \ldots, f_n = 0$. *Результант есть однородный многочлен степени* $L_1 = l_2 l_3 \ldots l_n$ *относительно коэфициентов* f_1 *и т. д. Он содержит главный член* $a_1^{L_1} \ldots e_\omega^{L_n}$ *и при* $f_i = x_i^{l_i}$ *равен единице. При* $f_1 = g \cdot h$ R *равно произведению* $R_g \cdot R_h$. *Наконец, R общий наибольший делитель n вполне известных определителей* $D_a, D_b, \ldots, D_e$.

Задачи. 1. Для двух форм с двумя переменными результант совпадает с результантом Сильвестера (§ 71).

2. Для формы f степени l и $n-1$ линейных форм

$$\sum b_i x_i, \ \ldots, \ \sum e_i x_i$$

результант равен

$$f(X_1, \ldots, X_n),$$

где $X_1, \ldots, X_n$ — миноры $n-1$-го порядка матрицы

$$\begin{pmatrix} b_1, \ldots, b_n \\ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \\ e_1 \ \ldots \ e_n \end{pmatrix}$$

3. Результант абсолютно неразложим.

4. Если ввести в формы $f_1, \ldots, f_n$ новые переменные с помощью линейной подстановки

$$x_i = \sum a_{ik} x_k'$$

с неисчезающим определителем, то результант преобразованных форм (от переменных $x_1', \ldots, x_n'$) с точностью до постоянного множителя, не зависящего от a_{ik}, равен результанту $f_1, \ldots, f_n$.

Дальнейшие свойства результанта читатель найдет в цитированной выше (§ 72 и § 74) книжке F. S. Macaulay: Modular Systems, а также у E. Fischer: Über die Cayleysche Eliminationsmethode, Math. Zeitschr., т. 26, стр. 497—550, 1927.

§ 79. *u*-РЕЗУЛЬТАНТ И ТЕОРЕМА БЕЗУ

Под *лучом решений* (см. § 76) однородной системы уравнений подразумевается совокупность всех решений вида $\{\lambda\xi_1, \ldots, \lambda\xi_n\}$, пропорциональных нетривиальному решению $\{\xi_1, \ldots, \xi_n\}$. Предположим, что система уравнений

$$f_1 = 0, \ \ldots, \ f_r = 0, \tag{1}$$

допускает только конечное число лучей $\{\xi_1^{(\alpha)}, \ldots, \xi_n^{(\alpha)}\}$ $(\alpha = 1, \ldots, q)$, и найдем эти лучи.

Присоединим к полиномам $f_1, \ldots, f_r$ линейную форму

$$l = u_1 x_1 + \ldots + u_n x_n$$

с неопределенными коэфициентами и построим систему результантов $b_1(u), \ldots, b_t(u)$ форм $f_1, \ldots, f_r, l$. Эта система результантов при частных значениях $u_1, \ldots, u_n$ обращается в нуль тогда и только тогда, если решение $\{\xi^{(\alpha)}\}$ уравнений (1) удовлетворяет также уравнению

$$l_\alpha = u_1 \xi_1^{(\alpha)} + \ldots + u_n \xi_n^{(\alpha)} = 0.$$

Другими словами: общие корни форм $b_1(u), \ldots, b_t(u)$ (рассматриваемых относительно u) являются также корнями произведения $\Pi_\alpha l_\alpha$.

Отсюда следует согласно теореме Гильберта о корнях (§ 75), с одной стороны,

$$\left(b_i(u)\right)^{\tau_i} \equiv 0 \left(\Pi_\alpha l_\alpha\right) \qquad (i = 1, \ldots, t), \tag{2}$$

а с другой стороны,

$$\left(\Pi_\alpha l_\alpha\right)^{\tau} \equiv 0 \left(b_1(u), \ldots, b_t(u)\right). \tag{3}$$

l_α линейные формы u, а потому они неразложимы. Согласно (2) $b_i(u)$ и тем самым их общий наибольший делитель $D(u)$ делятся на все линейные множители l_α. Но из (3) следует:

$$\left(\Pi_\alpha l_\alpha\right)^{\tau} \equiv 0 \left(D(u)\right).$$

Поэтому $D(u)$ других линейных множителей, кроме l_α, не содержит, откуда

$$D(u) = \Pi l_\alpha^{\rho_\alpha}, \quad \rho_\alpha > 0, \tag{4}$$

т. е. *линейные формы, определяющие лучи решений* (1), *найдутся при разложении формы* $D(u)$ *на множители.* Форма $D(u)$, общий наибольший делитель системы результантов $f_1, \ldots, f_r$ и l, называется *u-результантом* $f_1, \ldots, f_r$.

Рассмотрим в частности случай $n-1$ однородных уравнений n переменных, обладающих конечным числом лучей решений. Присоединяя линейную форму l, получим n форм, которые имеют единственный результант $R(u)$; он, очевидно, будет также u-результантом и в силу (4) разлагается. Решения встречаются с известной *кратностью* ρ_α. Сумма ρ_α равна степени $R(u)$, откуда она равна произведению степеней форм $f_1, \ldots, f_{n-1}$ (см. § 78). Это доказывает теорему Безу:

Если $n-1$ *однородных уравнений с* n *неизвестными имеют только конечное число лучей решений, то сумма кратностей* ρ_α *этих лучей решений* [*см. равенство* (4)] *равна произведению степеней уравнений.*

Для $n = 3$ и $n = 4$ это приводит к такой геометрической теореме: сумма кратностей точек пересечения двух алгебраических кривых в проективной плоскости и соответственно трех алгебраических поверхностей в проективном пространстве равна произведению степеней этих кривых (поверхностей). Кратности могут принимать целые положительные значения, которые определяются показателями линейных множителей $R(u)$.

Задача. Как будет выглядеть первая теорема этого параграфа для однородных уравнений с двумя рядами $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_m)$ неизвестных, если линейную форму l заменить через $\sum\sum u_{ik}x_iy_k$?

См. еще B. L. v. d. Waerden, Der Multiplizitätsbegriff der algebraischen Geometrie, Math. Ann., т. 97, стр. 756, 1927; H. Kapferer, Axiomatische Begründung des Bézoutschen Satzes, Sitzungsber. Heidelberger Akademie, 1927, 8. Abhandlung, стр. 33—59.

ГЛАВА ДВЕНАДЦАТАЯ

ОБЩАЯ ТЕОРИЯ ИДЕАЛОВ КОММУТАТИВНОГО КОЛЬЦА

§ 80. ТЕОРЕМЫ О БАЗИСЕ И ЦЕПЯХ ДЕЛИТЕЛЕЙ

В этой главе мы исследуем свойства делимости идеалов коммутативного кольца и посмотрим, как далеко могут быть распространены простые законы, имеющие место в области целых чисел, на случай общего кольца. При этом ради простоты целесообразно ограничиться кольцом, в котором любой идеал обладает конечным базисом; мы увидим, что и при таком ограничении будет охвачено весьма много важных случаев.

Мы говорим, что в кольце $\mathfrak{o}$ *справедлива теорема о базисе*, если любой идеал $\mathfrak{o}$ обладает конечным базисом.

Теорема о базисе верна для всякого поля, так как в поле существуют только идеалы (0) и (1). Она верна также для кольца целых чисел и вообще для любого кольца главных идеалов. Затем теорема справедлива для конечного кольца. Позднее мы увидим, что теорема о базисе верна для кольца вычетов $\mathfrak{o}/\mathfrak{a}$, как только она верна для $\mathfrak{o}$. Наконец, имеет место следующее важное предложение, принадлежащее Гильберту:

Если теорема о базисе верна для $\mathfrak{o}$ *и в* $\mathfrak{o}$ *существует единица, то теорема справедлива также для кольца полиномов* $\mathfrak{o}[x]$.

Доказательство. Пусть $\mathfrak{A}$ — идеал кольца $\mathfrak{o}[x]$. Коэфициенты при наивысшей степени x полиномов идеала $\mathfrak{A}$ образуют, включая и нуль, идеал из $\mathfrak{o}$; в самом деле, если α и β — старшие коэфициенты полиномов a и b:

$$a = \alpha x^n + \ldots,$$
$$b = \beta x^m + \ldots,$$

то, предполагая $n \geqslant m$, получим снова полином из $\mathfrak{A}$:

$$a - bx^{n-m} = (\alpha x^n + \ldots) - (\beta x^n + \ldots) = (\alpha - \beta)x^n + \ldots$$

и его старшим коэфициентом будет $\alpha - \beta$ или нуль; точно так же, если α — старший коэфициент a, $\lambda\alpha$ или нуль будет старшим коэфициентом полинома λa.

Этот идеал $\mathfrak{a}$ старших коэфициентов по предположению обладает базисом $(\alpha_1, \ldots, \alpha_r)$; пусть, например, α_i — старший коэфициент полинома

$$a_i = \alpha_i x^{n_i} + \ldots$$

степени n_i, и пусть n будет наибольшее из конечного множества чисел n_i.

Положим полиномы a_i в основание образуемого базиса $\mathfrak{A}$. Посмотрим, какие новые полиномы будут необходимы для полноты базиса.

Если

$$f = \alpha x^N + \dots$$

есть полином $\mathfrak{A}$ степени $N \geqslant n$, то α должно принадлежать идеалу $\mathfrak{a}$:

$$\alpha = \sum \lambda_i \alpha_i.$$

Построим теперь полином

$$f_1 = f - \sum \left(\lambda_i x^{N-n_i}\right) a_i.$$

В этом полиноме коэфициент при x^N равен

$$\alpha - \sum \lambda_i \alpha_i = 0;$$

таким образом, степень f_1 меньше N. Следовательно, можно полином f заменить по модулю $(a_1, \dots, a_r)$ полиномом более низкой степени. Продолжая подобным образом далее, мы дойдем до степени, меньшей n. Поэтому достаточно ограничиться полиномами со степенями, не превосходящими $n-1$.

Коэфициенты при x^{n-1} полиномов из $\mathfrak{A}$, степень которых меньше или равна $n-1$, образуют, включая нуль, идеал $\mathfrak{a}_{n-1}$; пусть

$$(\alpha_{r+1}, \dots, \alpha_s)$$

будет базис этого идеала.

Пусть α_{r+i} будет старший коэфициент полинома

$$a_{r+i} = \alpha_{r+i} x^{n-1} + \dots$$

Включим теперь и полиномы $a_{r+1}, \dots, a_s$ в базис. Любой полином, степень которого меньше или равна $n-1$, может быть заменен по модулю $(a_{r+1}, \dots, a_s)$ полиномом степени $\leqslant n-2$; для этого стоит только, как и выше, вычесть подходяще подобранную линейную комбинацию

$$\sum \lambda_{r+i} a_{r+i}.$$

Подобным образом мы продолжаем дальше. Коэфициенты при x^{n-2} полиномов степени $\leqslant n-2$ образуют вместе с нулем идеал $\mathfrak{a}_{n-2}$, элементы базиса $\alpha_{s+1}, \dots, \alpha_t$ которого пусть соответствуют полиномам $a_{s+1}, \dots, a_t$. Эти полиномы снова включим в базис. Таким путем мы придем наконец к идеалу $\mathfrak{a}_0$, состоящему из постоянных, лежащих в $\mathfrak{A}$; пусть базису $(\alpha_{v+1}, \dots, \alpha_w)$ идеала $\mathfrak{a}_0$ будут соответствовать полиномы $a_{v+1}, \dots, a_w$. В конечном счете любой полином $\mathfrak{A}$ должен привестись к нулю по модулю

$$(a_1, \dots, a_r, a_{r+1}, \dots, a_s, \dots, a_{v+1}, \dots, a_w).$$

Таким образом многочлены $a_1, \dots, a_w$ образуют базис идеала, что доказывает теорему о базисе.

Из этой теоремы после ее n-кратного применения непосредственно вытекает следующее обобщение:

Если для кольца $\mathfrak{o}$ *с единицей верна теорема о базисе, то она также верна и для кольца полиномов* $\mathfrak{o}[x_1, \ldots, x_n]$ *с конечным числом неизвестных* $x_1, \ldots, x_n$.

Наиболее важными частными случаями являются целочисленная область полиномов $C[x_1, \ldots, x_n]$ и любое кольцо полиномов $\mathsf{K}[x_1, \ldots, x_n]$ с коэфициентами из поля K. Во всех этих областях идеал обладает конечным базисом.

Гильберт высказал свою теорему для этих случаев в несколько более общей на вид формулировке, а именно:

Во всяком подмножестве $\mathfrak{M}$ *кольца* $\mathfrak{o}$ (*а не только во всяком идеале*) *существует конечное множество таких элементов* $m_1, \ldots, m_r$, *что любой элемент* m *из* $\mathfrak{M}$ *может быть записан в виде*:

$$\lambda_1 m_1 + \ldots + \lambda_r m_r$$

(λ_i *содержится в* $\mathfrak{o}$).

Но эта теорема является непосредственным следствием теоремы о базисе идеала. Действительно, если $\mathfrak{A}$ есть идеал, порожденный подмножеством $\mathfrak{M}$, то прежде всего $\mathfrak{A}$ обладает базисом:

$$\mathfrak{A} = (a_1, \ldots, a_s).$$

Элемент a_i зависит (как элемент идеала, порожденного $\mathfrak{M}$) от конечного числа величин $\mathfrak{M}$:

$$a_i = \sum_k \lambda_{ik} m_{ik},$$

откуда все элементы идеала $\mathfrak{A}$ зависят линейно от конечного числа m_{ik}; в частности это справедливо для элементов из $\mathfrak{M}$.

Важнее то, что теорема о базисе также эквивалентна следующей „теореме о цепях делителей“ [1]).

Первая формулировка теоремы о цепях делителей

Если дана последовательность идеалов $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ *кольца* $\mathfrak{o}$ *и всякий* $\mathfrak{a}_{i+1}$ *есть собственный делитель* $\mathfrak{a}_i$:

$$\mathfrak{a}_i \subset \mathfrak{a}_{i+1},$$

то последовательность состоит из конечного числа членов.

Или, что одно и то же:

Вторая формулировка теоремы о цепях делителей

Если дана бесконечная последовательность делителей

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots,$$

то, начиная с некоторого n, *все члены должны быть равны*:

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$$

Что теорема о цепи делителей вытекает из теоремы о базисе, доказывается следующим образом.

---

[1]) Пожалуй, точнее было бы употребить выражение „постулат о цепях делителей“ или „условие о цепях делителей“.

Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ — бесконечная последовательность, причем всегда $\mathfrak{a}_i \subset \mathfrak{a}_{i+1}$. Объединение $\mathfrak{v}$ всех идеалов $\mathfrak{a}_i$ является идеалом. В самом деле, если a и b лежат в $\mathfrak{v}$, например a лежит в $\mathfrak{a}_n$, а b в $\mathfrak{a}_m$, то a и b лежат в $\mathfrak{a}_N$, где N — наибольшее из чисел n и m; таким образом $a - b$ также лежит в $\mathfrak{a}_N$, т. е. в $\mathfrak{v}$. А если a лежит в $\mathfrak{v}$, например в $\mathfrak{a}_n$, то λa лежит также в $\mathfrak{a}_n$, а потому λa содержится в $\mathfrak{v}$.

По предположению этот идеал $\mathfrak{v}$ обладает базисом $(a_1, \ldots, a_r)$. Любое a_i лежит в некотором идеале $\mathfrak{a}_{n_i}$. Если n — наибольшее из числа n_i, то $a_1, \ldots, a_r$ будут лежать в $\mathfrak{a}_n$. Так как элементы идеала $\mathfrak{v}$ линейно зависят от $a_1, \ldots, a_r$, то все элементы из $\mathfrak{v}$ лежат в $\mathfrak{a}_n$, а отсюда следует:

$$\mathfrak{v} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \ldots$$

Обратно, теорема о базисе вытекает, как следствие из теоремы о цепях делителей (предположив еще справедливость постулата выбора). А именно: на основании постулата выбора (§ 58) в каждом не пустом подмножестве $\mathfrak{o}$ можно выделить некоторый элемент. Пусть $\mathfrak{a}$ — идеал, a_1 — элемент, выделенный из $\mathfrak{a}$. Если a_1 еще не порождает $\mathfrak{a}$, то в $\mathfrak{a}$ существуют элементы, не лежащие в (a_1); пусть a_2 — элемент, выделенный из множества этих элементов. Тогда

$$(a_1) \subset (a_1, a_2).$$

Если a_1 и a_2 не порождают всего идеала $\mathfrak{a}$, то подобным же образом находим третий элемент a_3 в $\mathfrak{a}$, не лежащий в (a_1, a_2), и т. д. Таким образом получится последовательность делителей:

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots,$$

которая должна состоять из конечного числа (например r) членов. Отсюда следует:

$$(a_1, a_2, \ldots, a_r) = \mathfrak{a},$$

т. е. $\mathfrak{a}$ обладает конечным базисом.

Если теорема о цепях делителей верна в кольце $\mathfrak{o}$, то она верна во всяком кольце вычетов $\frac{\mathfrak{o}}{\mathfrak{a}}$.

Доказательство. В $\frac{\mathfrak{o}}{\mathfrak{a}}$ идеал $\bar{\mathfrak{b}}$ есть некоторое множество классов вычетов. Если возьмем множество всех элементов этих классов вычетов, то получится идеал $\mathfrak{b}$ в кольце $\mathfrak{o}$. Обратно, $\mathfrak{b}$ определяет однозначно $\bar{\mathfrak{b}}$ в силу равенства

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

Поэтому последовательности идеалов $\bar{\mathfrak{b}}_1 \subset \bar{\mathfrak{b}}_2 \subset \bar{\mathfrak{b}}_3 \subset \ldots$ в $\frac{\mathfrak{o}}{\mathfrak{a}}$ соответствует последовательность идеалов $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \ldots$ кольца $\mathfrak{o}$, а так как последняя состоит из конечного числа членов, то это же обстоятельство должно иметь место и для первой последовательности.

Тем самым доказано, что из теоремы о базисе $\mathfrak{o}$ следует теорема о базисе $\frac{\mathfrak{o}}{\mathfrak{a}}$ (см. начало параграфа).

Теорема о делителях допускает еще две формулировки, которые в приложениях часто оказываются предпочтительнее.

Третья формулировка теоремы о цепях делителей: условие максимальности

Если в $\mathfrak{o}$ имеет место теорема о делителях, то во всяком не пустом множестве идеалов существует максимальный идеал, т. е. такой, который не содержится в остальных идеалах множества.

Доказательство. Пусть из не пустого множества идеалов выделен идеал. Допустим теперь, что в множестве $\mathfrak{M}$ идеалов не существует максимального идеала. Тогда любой идеал множества содержался бы в другом идеале того же множества. Выделим из $\mathfrak{M}$ идеал $\mathfrak{a}_1$, затем из множества идеалов, содержащих $\mathfrak{a}_1$, но не равных $\mathfrak{a}_1$, выделим $\mathfrak{a}_2$ и т. д.; получим бесконечную последовательность:

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \ldots,$$

что по предположению невозможно.

Четвертая формулировка теоремы о цепях делителей: принцип индукции

Пусть в $\mathfrak{o}$ выполняется постулат о цепях делителей. Если идеал $\mathfrak{a}$ обладает свойством E, коль скоро обладают этим свойством все собственные делители $\mathfrak{a}$ (и в частности единичный идеал), то свойство E справедливо для всех идеалов кольца $\mathfrak{o}$.

Доказательство. Допустим, что идеал не обладает свойством E. Тогда в силу третьей формулировки теоремы о делителях, существует максимальный идеал $\mathfrak{a}$, не обладающий свойством E. В силу максимальности все собственные делители $\mathfrak{a}$ имеют свойство E, откуда $\mathfrak{a}$ также должно иметь свойство E, что ведет к противоречию.

§ 81. ПРОИЗВЕДЕНИЕ И ОТНОШЕНИЕ ИДЕАЛОВ

Так же, как и в § 15, под *общим наибольшим делителем* или *суммой* идеалов $\mathfrak{a}, \mathfrak{b}, \ldots$ мы подразумеваем идеал $(\mathfrak{a}, \mathfrak{b}, \ldots)$, порожденный объединением их множеств, точно так же под *общим наименьшим кратным* мы подразумеваем пересечение $[\mathfrak{a}, \mathfrak{b}, \ldots] = \mathfrak{a} \cap \mathfrak{b} \cap \ldots$ Те же обозначения, что и для суммы идеалов, употребляются также для образующих, состоящих из элементов и идеалов, например:

$$(\mathfrak{a}, b) = \big(\mathfrak{a}, (b)\big).$$

Само собой очевидно, что $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a})$, $\big((\mathfrak{a}, \mathfrak{b}), \mathfrak{c}\big) = \big(\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})\big) = (\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ и т. д. Затем:

$$[(a_1, a_2, \ldots), (b_1, b_2, \ldots)] = (a_1, a_2, \ldots, b_1, b_2, \cdots),$$

т. е. *если друг за другом написать базисы отдельных идеалов, то получится базис общего наибольшего делителя.*

Если элементы идеала $\mathfrak{a}$ перемножить с элементами идеала $\mathfrak{b}$, то произведения ab (в противоположность суммам) вообще не образуют идеал [1]). *Произведением* же идеалов $\mathfrak{a}$, $\mathfrak{b}$ называется идеал, порожденный этими произведениями; он обозначается через $\mathfrak{a} \cdot \mathfrak{b}$ или $\mathfrak{ab}$. Он состоит из всех сумм вида $\sum a_i b_i$ (a_i содержатся в $\mathfrak{a}$, b_i — в $\mathfrak{b}$).

[1]) Пример: если в области полиномов $\mathfrak{a} = (x, y)$ и $\mathfrak{b} = (x^2, y)$, то x^3 и y^3 суть произведения вида $a \cdot b$, но $x^3 - y^2$ уже нельзя представить в таком виде.

Очевидно, что

$$\mathfrak{a}\cdot\mathfrak{b}=\mathfrak{b}\cdot\mathfrak{a},$$
$$(\mathfrak{a}\cdot\mathfrak{b})\cdot\mathfrak{c}=\mathfrak{a}\cdot(\mathfrak{b}\cdot\mathfrak{c});$$

таким образом с произведениями идеалов можно обращаться, как с обычными произведениями. В частности имеет смысл говорить о *степенях* $\mathfrak{a}^\rho$ идеала; они определяются на основании равенств:

$$\mathfrak{a}^1=\mathfrak{a};\quad \mathfrak{a}^{\rho+1}=\mathfrak{a}\cdot\mathfrak{a}^\rho.$$

Если $\mathfrak{a}=(a_1,\ \ldots,\ a_n)$ и $\mathfrak{b}=(b_1,\ \ldots,\ b_m)$, то, очевидно, произведение $\mathfrak{ab}$ порождается произведениями a_ib_k. *Итак, базис произведения получается при умножении всех элементов базиса одного сомножителя на все элементы базиса другого.*

В частности для главных идеалов имеет место

$$(a)\cdot(b)=(ab);$$

таким образом здесь в области элементов $\mathfrak{o}$ произведение совпадает с обычным.

Произведение $\mathfrak{a}\cdot(b)$ произвольного идеала на главный идеал состоит из всех произведений вида ab, где a лежит в $\mathfrak{a}$. Поэтому просто пишется $\mathfrak{a}b$ или $b\mathfrak{a}$.

Далее имеет место „дистрибутивный закон для идеалов".

$$\mathfrak{a}\cdot(\mathfrak{b},\ \mathfrak{c})=(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c}), \tag{1}$$

так как $\mathfrak{a}\cdot(\mathfrak{b},\ \mathfrak{c})$ порождается произведениями $a(b+c)$, которые в силу

$$a(b+c)=ab+ac$$

все лежат в $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$; обратно, $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$ порождается произведениями ab и ac, лежащими в $\mathfrak{a}\cdot(\mathfrak{b},\ \mathfrak{c})$.

То же правило (1) справедливо и тогда, когда в скобке вместо $\mathfrak{b}$, $\mathfrak{c}$ стоит несколько или даже бесконечное число идеалов.

Так как все произведения ab лежат в $\mathfrak{a}$, то

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{a}$$

и точно так же

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{b}.$$

Отсюда следует, что

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq[\mathfrak{a},\ \mathfrak{b}]$$

или: *произведение делится на общее наименьшее кратное.*

В кольце целых чисел произведение общего наименьшего кратного на общий наибольший делитель двух идеалов $\mathfrak{a}$, $\mathfrak{b}$ равно $\mathfrak{ab}$. Это, однако, не верно для произвольного кольца; имеет только место

$$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\ \mathfrak{b})\equiv 0\ \ (\mathfrak{a}\cdot\mathfrak{b}). \tag{2}$$

Доказательство.

$$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\ \mathfrak{b})=([\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{a},\ [\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{b})\subseteq(\mathfrak{b}\cdot\mathfrak{a},\ \mathfrak{a}\cdot\mathfrak{b})=\mathfrak{a}\cdot\mathfrak{b}.$$

Идеал $\mathfrak{o}$, состоящий из всех элементов рассматриваемого кольца, называется согласно § 14 *единичным идеалом*. Очевидно, что

$$\mathfrak{a}\cdot\mathfrak{o}\subseteq\mathfrak{a}.$$

Но если $\mathfrak{o}$ содержит единицу e, то также обратно

$$\mathfrak{a} = \mathfrak{a} \cdot e \subseteq \mathfrak{a} \cdot \mathfrak{o},$$

откуда

$$\mathfrak{a} \cdot \mathfrak{o} = \mathfrak{a}.$$

Поэтому в данном случае идеал $\mathfrak{o}$ играет роль единицы умножения и порождается единицей. Всегда

$$(\mathfrak{a}, \mathfrak{o}) = \mathfrak{o}; \quad \mathfrak{a} \cap \mathfrak{o} = \mathfrak{a}.$$

Под *отношением* $\mathfrak{a} : \mathfrak{b}$ идеала, где $\mathfrak{a}$ — идеал, мы подразумеваем совокупность таких элементов γ из $\mathfrak{o}$, для которых

$$\gamma b \equiv 0 (\mathfrak{a}) \text{ для всех } b \text{ из } \mathfrak{b}. \tag{3}$$

Эта совокупность является идеалом, так как если γ и δ удовлетворяют (3), то $\gamma - \delta$ и $r\gamma$ также удовлетворяют (3). При этом предполагается, что $\mathfrak{a}$ — идеал; $\mathfrak{b}$ может и не быть идеалом.

Если $\mathfrak{a}$ и $\mathfrak{b} \neq$ идеалы, то по определению

$$\mathfrak{b} \cdot (\mathfrak{a} : \mathfrak{b}) \equiv 0 (\mathfrak{a}).$$

В кольце целых чисел, чтобы получить отношение двух главных идеалов (a), $(b) \neq 0$, достаточно в разложении числа a на множители удалить множители b; например:

$$\begin{aligned} (12) : (2) &= (6), \\ (12) : (4) &= (3), \\ (12) : (8) &= (3), \\ (12) : (5) &= (12). \end{aligned}$$

Иными словами, надо разделить a в обычном смысле на общий наибольший делитель (a, b).

В общем кольце оказывается верным соответствующее правило:

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a} : (\mathfrak{a}, \mathfrak{b}),$$

которое легко доказать.

Очевидно, что $\mathfrak{a} \equiv 0 \ (\mathfrak{a} : \mathfrak{b})$, так как любой элемент $\mathfrak{a}$ обладает свойством (3). Могут встретиться два предельных случая:

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{o} \quad \text{и} \quad \mathfrak{a} : \mathfrak{b} = \mathfrak{a}.$$

Первый случай получается тогда, если $\mathfrak{b} \subseteq \mathfrak{a}$, так как здесь для всякого γ

$$\gamma \mathfrak{b} \equiv 0 (\mathfrak{b}) \equiv 0 (\mathfrak{a}).$$

Второй случай означает, что из $\gamma \mathfrak{b} \equiv 0 (\mathfrak{a})$ следует $\gamma \equiv 0 (\mathfrak{a})$, т. е. сравнение можно сократить на $\mathfrak{b}$. В этом случае $\mathfrak{b}$ называется взаимно *простым с* $\mathfrak{a}$; однако мы будем редко пользоваться этим легко вводящим в заблуждение термином и большей частью будем прямо писать равенство $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$. В случае целых чисел a и b (оба не равны нулю), критерий: „из $\gamma b \equiv 0 (a)$ следует $\gamma \equiv 0 (a)$“ выполняется только тогда, когда a и b не имеют общего простого множителя. Но в более общих случаях термин „взаимно простое с ...“ *не является симметричным*; например,

если $\mathfrak{a}$ — простой идеал и $\mathfrak{b}$ — собственный простой делитель идеала $\mathfrak{a}$, отличный от $\mathfrak{o}$, то

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a}, \text{ т. е. } \mathfrak{b} \text{ взаимно просто с } \mathfrak{a},$$

в то время как

$$\mathfrak{b} : \mathfrak{a} = \mathfrak{o}, \text{ т. е. } \mathfrak{a} \text{ не взаимно просто с } \mathfrak{b}.$$

Например,

$$(0) : (2) = (0),$$
$$(2) : (0) = (1).$$

Важно следующее правило:

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_r] : \mathfrak{b} = [\mathfrak{a}_1 : \mathfrak{b}, \ldots, \mathfrak{a}_r : \mathfrak{b}]. \tag{4}$$

Доказательство. Из

$$\gamma\mathfrak{b} \subseteq [\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$$

следует:

$$\gamma\mathfrak{b} \subseteq \mathfrak{a}_i \text{ для } i = 1, 2, \ldots, r,$$

и обратно.

Задачи. 1. Доказать, что

$$(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{b}\mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b},$$
$$\mathfrak{a} : (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c}).$$

2. Показать эквивалентность трех соотношений:

a) $\mathfrak{a} : \mathfrak{b}_1 = \mathfrak{a}$ и $\mathfrak{a} : \mathfrak{b}_2 = \mathfrak{a}$;
b) $\mathfrak{a} : [\mathfrak{b}_1 \cap \mathfrak{b}_2] = \mathfrak{a}$;
c) $\mathfrak{a} : \mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{a}$.

§ 82. ПРОСТЫЕ И ПРИМАРНЫЕ ИДЕАЛЫ

Простой идеал мы определили как идеал, кольцо вычетов которого не содержит делителей нуля.

В области целых чисел всякое целое число $a > 0$ есть произведение степеней простых чисел:

$$a = p_1^{\rho_1} \ldots p_r^{\rho_r}, \tag{1}$$

а потому любой идеал (a) равен произведению степеней простых идеалов:

$$(a) = (p_1)^{\rho_1} \ldots (p_r)^{\rho_r}.$$

Однако в более общих кольцах закон разложения идеалов может оказаться не столь простым. Например, в целочисленной области полиномов одного неизвестного x не простой идеал $(4, x)$, кроме $\mathfrak{o}$, имеет простым делителем только $(2, x)$, и однако идеал $(4, x)$ нельзя представить степенью $(2, x)$. Таким образом в общем случае идеал $\mathfrak{a}$ нельзя разложить на произведение простых составных частей; но оказывается, что $\mathfrak{a}$ можно представить в виде общего наименьшего кратного (пересечения) простых составных частей, как, например, это имеет место для (a) в области целых чисел:

$$(a) = [(p_1^{\rho_1}), \ldots, (p_r^{\rho_r})].$$

Идеал $(p_k^{\rho_k})$ обладает следующим характеризующим его свойством: если произведение ab делится на $p_k^{\rho_k}$, в то время как a не делится на $p_k^{\rho_k}$, то другой множитель b содержит по крайней мере делитель числ $p_k^{\rho_k}$. Иными словами, некоторая степень b^ρ должна делиться на $p_k^{\rho_k}$. Итаак, из

$$ab \equiv 0\,(p_k^{\rho_k}), \quad a \not\equiv 0\,(p_k^{\rho_k})$$

следует:

$$b^\rho \equiv 0\,(p_k^{\rho_k}).$$

Идеал с таким свойством будет называться *примарным*.

Идеал $\mathfrak{q}$ *называется примарным, если из*

$$ab \equiv 0\,(\mathfrak{q}), \quad a \not\equiv 0\,(\mathfrak{q})$$

следует, что существует такое ρ, *что*

$$b^\rho \equiv 0\,(\mathfrak{q}).$$

Можно определение сформулировать еще так:

Если в кольце вычетов по $\mathfrak{q}$ $\bar{a}\bar{b} = 0$ *и* $\bar{a} \neq 0$, *то некоторая степень* $\bar{b}^\rho$ *должна равняться нулю.*

Если $\bar{a}\bar{b} = 0$ и $\bar{a} \neq 0$, то это означает не что иное, как то, что $\bar{b}$ есть делитель нуля. Если степень $\bar{b}^\rho$ элемента $\bar{b}$ кольца равна нулю, то элемент называется *нильпотентным*. Поэтому можно также выразиться следующим образом:

Идеал называется примарным, если в его кольце вычетов любой делитель нуля является нильпотентным.

Как видно, определение это представляет лишь видоизменение определения простого идеала; в кольце вычетов по простому идеалу любой делитель нуля должен быть не только нильпотентным, но и сам исчезать.

Мы увидим, что примарные идеалы в общих кольцах играют такую же роль, как степени простых чисел в области целых чисел, а именно, что при весьма общих предположениях любой идеал представляется в виде пересечения примарных идеалов, и в этом представлении находят свое выражение существеннейшие структурные свойства идеалов.

Примарные идеалы не обязательно должны быть степенями простых идеалов; так, уже упомянутый вначале идеал $(4, x)$ оказывается примарным. Но обратное также не имеет места; в самом деле в кольце тех же целочисленных полиномов $a_0 + a_1x + \ldots + a_nx^n$, для которых a_1 делится на 3, $\mathfrak{p} = (3x, x^2)$ есть простой идеал, но $\mathfrak{p}^2 = (9x^2, 3x^3, x^4)$ не примарно, потому что

$$9 \cdot x^2 \equiv 0\,(\mathfrak{p}^2), \quad x^2 \not\equiv 0\,(\mathfrak{p}^2), \quad 9^\rho \not\equiv 0\,(\mathfrak{p}^2)$$

для всякого ρ.

Свойства примарных идеалов, независимые от постулата о цепи делителей

I *Примарному идеалу* $\mathfrak{q}$ *соответствует простой идеал* $\mathfrak{p}$, *который определяется следующим образом:* $\mathfrak{p}$ *есть совокупность элементов* b, *степень которых* b^ρ *лежит в* $\mathfrak{q}$.

Доказательство. Во-первых, $\mathfrak{p}$ есть идеал, так как из $b^\rho \equiv 0\,(\mathfrak{q})$ следует $(rb)^\rho \equiv 0\,(\mathfrak{q})$ и из $b^\rho \equiv 0\,(\mathfrak{q})$ и $c^\sigma \equiv 0\,(\mathfrak{q})$ следует $(b-c)^{\rho+\sigma-1} \equiv 0\,(\mathfrak{q})$, так как в каждое слагаемое $(b-c)^{\rho+\sigma-1}$ входит либо b^ρ, либо c^σ.

Во-вторых, $\mathfrak{p}$ есть простой идеал, ибо из

$$ab \equiv 0\,(\mathfrak{p}),$$

$$a \not\equiv 0\,(\mathfrak{p})$$

следует, что существует ρ, для которого

$$a^\rho b^\rho \equiv 0\,(\mathfrak{q})$$

и, кроме того,

$$a^\rho \not\equiv 0\,(\mathfrak{q}),$$

а потому существует такое σ, что

$$b^{\rho\sigma} \equiv 0\,(\mathfrak{q});$$

отсюда следует

$$b \equiv 0\,(\mathfrak{p}).$$

В-третьих, $\mathfrak{p}$ есть делитель $\mathfrak{q}$:

$$\mathfrak{q} \equiv 0\,(\mathfrak{p}),$$

так как элементы $\mathfrak{q}$ наверное обладают тем свойством, что их степени лежат в $\mathfrak{q}$.

$\mathfrak{p}$ называется простым идеалом, *принадлежащим* или *соответствующим* $\mathfrak{q}$, а $\mathfrak{q}$ — примарным идеалом, *принадлежащим* $\mathfrak{p}$. В силу определения примарного идеала имеем:

II. *Из* $ab \equiv 0\,(\mathfrak{q})$ *и* $a \not\equiv 0\,(\mathfrak{q})$ *следует* $b \equiv 0\,(\mathfrak{p})$.

До некоторой степени обращением этой теоремы является следующее предложение:

III. *Если* $\mathfrak{q} \neq \mathfrak{o}$ *есть идеал и* $\mathfrak{p}$ *— совокупность элементов кольца* $\mathfrak{o}$, *обладающие тем свойством, что*

1) *из* $ab \equiv 0\,(\mathfrak{q})$ *и* $a \not\equiv 0\,(\mathfrak{q})$ *следует* $b \equiv 0\,(\mathfrak{p})$,

2) *из* $b \equiv 0\,(\mathfrak{p})$ *следует* $b^\rho \equiv 0\,(\mathfrak{q})$,

то $\mathfrak{q}$ *примарно и* $\mathfrak{p}$ *— простой идеал, принадлежащий* $\mathfrak{q}$.

Доказательство. Из $ab \equiv 0\,(\mathfrak{q})$ и $a \not\equiv 0\,(\mathfrak{q})$ следует (согласно 1 и 2) $b^\rho \equiv 0\,(\mathfrak{q})$. Таким образом $\mathfrak{q}$ примарно. Остается показать, что $\mathfrak{p}$ состоит из элементов b кольца $\mathfrak{o}$, степени которых b^ρ лежат в $\mathfrak{q}$. Предположим сперва, что $b \not\equiv 0\,(\mathfrak{q})$ и ρ — наименьшее натуральное число, для которого $b^\rho \equiv 0\,(\mathfrak{q})$. Тогда $b \cdot b^{\rho-1} \equiv 0\,(\mathfrak{q})$, $b^{\rho-1} \not\equiv 0\,(\mathfrak{q})$, откуда согласно 1 $b \equiv 0\,(\mathfrak{p})$. Пусть теперь $b \equiv 0\,(\mathfrak{q})$. Очевидно, что для всякого r из $\mathfrak{o}$, которое можно выбрать так, чтобы $r \not\equiv 0\,(\mathfrak{q})$, произведение $rb \equiv 0\ (\mathfrak{q})$, откуда согласно 1 $b \equiv 0\,(\mathfrak{p})$.

Таким образом $\mathfrak{p} \supset \mathfrak{q}$. Обратно, из 2 следует, что всякому элементу b идеала $\mathfrak{p}$ соответствует ρ, дающее $b^\rho \equiv 0\,(\mathfrak{q})$ [1]).

---

[1]) Мы здесь отступили от немецкого текста, выбросив лишнее для $\mathfrak{q} \neq \mathfrak{o}$ требование $\mathfrak{q} \equiv 0\,(\mathfrak{p})$ (см. стр. 33 немецкого издания). В связи с этим пришлось несколько изменить доказательство теоремы. Из нашего доказательства вид-

С помощью этой теоремы можно выяснить, будет ли данный идеал примарен, и найти простой идеал, принадлежащий примарному идеалу.

Свойство II справедливо также и тогда, если вместо a и b фигурируют идеалы $\mathfrak{a}$ и $\mathfrak{b}$:

IV. *Из* $\mathfrak{ab} \equiv 0\,(\mathfrak{q})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ *следует* $\mathfrak{b} \equiv 0\,(\mathfrak{p})$. Действительно, если бы $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$, то в $\mathfrak{b}$ существовал бы элемент b, не лежащий в $\mathfrak{p}$, и точно так же элемент a из $\mathfrak{a}$, не лежащий в $\mathfrak{q}$. Но произведение ab должно лежать в $\mathfrak{q}$, что противоречит ранее доказанному.

Подобным же образом доказывается соответствующая теорема для простого идеала:

Из $\mathfrak{ab} \equiv 0\,(\mathfrak{p})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{p})$ *следует* $\mathfrak{b} \equiv 0\,(\mathfrak{p})$.

Одним из следствий этого является тот факт, что *из* $\mathfrak{a}^h \equiv 0\,(\mathfrak{p})$ *следует* $\mathfrak{a} \equiv 0\,(\mathfrak{p})$ (здесь мы $h-1$ раз применяем теорему).

Можно IV сформулировать еще так:

IV′. *Из* $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$ *следует* $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$.

В кольце вычетов $\frac{\mathfrak{o}}{\mathfrak{q}}$ лежит (в силу $\mathfrak{p} \supseteq \mathfrak{q}$) идеал $\frac{\mathfrak{p}}{\mathfrak{q}}$. Он состоит из всех нильпотентных элементов, т. е. в случае $\mathfrak{q} \neq \mathfrak{o}$ из всех делителей нуля.

Свойства примарных идеалов, вытекающие из постулата о цепи делителей

Если $\mathfrak{p}$ — простой идеал, принадлежащий $\mathfrak{q}$, то некоторая степень любого элемента $\mathfrak{p}$ лежит в $\mathfrak{q}$. При этом показатели степени, вообще говоря, могут зависеть от выбираемого элемента и неограниченно увеличиваться. Но если в кольце $\mathfrak{o}$ имеет место постулат о цепи делителей, то показатели степени уже не могут неограниченно возрастать в силу следующих теорем:

V. *Степень* $\mathfrak{p}^\rho$ *делится на* $\mathfrak{q}$:

$$\mathfrak{p}^\rho \equiv 0\,(\mathfrak{q}).$$

Доказательство. Пусть $(p_1, \ldots, p_r)$ — базис $\mathfrak{p}$ и $p_1^{\rho_1}, \ldots, p_r^{\rho_r}$ лежат в $\mathfrak{q}$.

Положим

$$\rho = \sum_1^r (\rho_i - 1) + 1.$$

Тогда $\mathfrak{p}^\rho$ порождается всевозможными произведениями из ρ сомножителей p_i; сомножитель p_i в каждом из таких произведений должен встречаться более чем $\rho_i - 1$ раз, т. е. по меньшей мере ρ_i раз; таким образом выходит, что все образующие $\mathfrak{p}^\rho$ лежат в $\mathfrak{q}$, откуда и следует теорема.

но, что $\mathfrak{q} \equiv 0\,(\mathfrak{p})$ есть простое следствие требования 1. Что касается единичного идеала $\mathfrak{o}$, то его принято считать примарным идеалом, принадлежащим самому себе. *Прим. перев.*

Поэтому между примарным идеалом $\mathfrak{q}$ и соответствующим простым идеалом $\mathfrak{p}$ существует такая зависимость:

$$\left.\begin{aligned} \mathfrak{q} &\equiv 0\ (\mathfrak{p}), \\ \mathfrak{p}^{\rho} &\equiv 0\ (\mathfrak{q}). \end{aligned}\right\} \tag{2}$$

Наименьшее число ρ, для которого еще верны эти соотношения, называется *показателем* $\mathfrak{q}$. В частности, показатель равен верхней границе показателей степеней, в которые надо возвысить элементы $\mathfrak{p}$, чтобы получить элементы $\mathfrak{q}$.

Если $\mathfrak{q}$ примарно, то сравнения вполне характеризуют соответствующий простой идеал $\mathfrak{p}$. В самом деле, предположив, что существует второй простой идеал $\mathfrak{p}'$ с показателем ρ', также удовлетворяющий (2), получим:

$$\mathfrak{p}^{\rho} \subseteq \mathfrak{q} \subseteq \mathfrak{p}', \text{ откуда } \mathfrak{p} \subseteq \mathfrak{p}';$$
$$\mathfrak{p}'^{\rho'} \subseteq \mathfrak{q} \subseteq \mathfrak{p}, \text{ откуда } \mathfrak{p}' \subseteq \mathfrak{p};$$

следовательно, $\mathfrak{p}' = \mathfrak{p}$. Но (2), однако, не характеризует примарный идеал: (2) может выполняться и для не примарного $\mathfrak{q}$ (см. приведенную ниже задачу 1).

VI. *Из* $\mathfrak{a}\mathfrak{b} \equiv 0\ (\mathfrak{q})$ *и* $\mathfrak{a} \not\equiv 0\ (\mathfrak{q})$ *следует, что некоторая степень* $\mathfrak{b}^{\sigma} \equiv 0\ (\mathfrak{q})$.

Доказательство. Достаточно выбрать $\sigma = \rho$. А именно, из $\mathfrak{a}\mathfrak{b} \equiv 0\ (\mathfrak{q})$ и $\mathfrak{a} \not\equiv 0\ (\mathfrak{q})$ следует согласно доказанному выше, что $\mathfrak{b} \equiv 0\ (\mathfrak{p})$, а отсюда

$$\mathfrak{b}^{\rho} \equiv 0\ (\mathfrak{p}^{\rho}) \equiv 0\ (\mathfrak{q}).$$

Идеал $\mathfrak{q}$, обладающий этим свойством, называется *сильным примарным идеалом*, в отличие от ранее определенных *слабых примарных идеалов* или просто примарных. Но если имеет место постулат о цепях делителей, то оба эти понятия совпадают, так как мы уже видели, что в этом случае примарные идеалы являются также сильными, а обратное просто следует при $\mathfrak{a} = (a), \mathfrak{b} = (b)$. Если же постулат о цепях делителей не осуществляется, то всякий сильный примарный идеал является также слабым, но обратное уже не верно.

Пример. В области полиномов бесконечного числа неизвестных $x_1, x_2, x_3, \ldots$ идеал

$$\mathfrak{q} = (x_1, x_2^2, x_3^3, \ldots)$$

примарен и

$$\mathfrak{p} = (x_1, x_2, x_3, \ldots)$$

есть соответствующий ему простой идеал. Это легче всего выводится из теоремы III. $\mathfrak{q}$ состоит из полиномов без постоянного члена, причем в каждом члене по крайней мере существует одно x_ν степени ν, в то время как $\mathfrak{p}$ состоит из всех полиномов без постоянного члена. Теперь, если $a \not\equiv 0\ (\mathfrak{q})$ и $b \not\equiv 0\ (\mathfrak{p})$, то b содержит постоянный член $b_0 \neq 0$, а a — член, в котором каждое x_ν имеет степень $< \nu$. Среди этих членов a возьмем член наинизшей степени; при умножении на постоянную b_0 получится член наинизшей степени, входящий в ab, в котором опять всякое x_ν имеет степень $< \nu$. Таким образом получается, что $ab \not\equiv 0\ (\mathfrak{q})$. Тем самым предположение 1 теоремы III доказано. Если далее $b \equiv 0\ (\mathfrak{p})$, то b не должно содержать постоянного члена; если x_ω — последнее из неизвестных $x_1, x_2, \ldots$, входящих в полином b (b содержит только конечное число x_ν), то в b^{ω^2} все члены будут по крайней мере степени ω^2. Таким образом в каждый член войдет по меньшей мере одно x_ν степени ω; поэтому b^{ω^2} лежит в $\mathfrak{q}$, и все предположения теоремы III выполнены.

Однако $\mathfrak{p}^\rho \not\equiv 0\ (\mathfrak{q})$, какое бы большое ρ мы ни взяли, так как $\mathfrak{p}^\rho$ содержит элемент x^ρ_{p+1}, не лежащий в $\mathfrak{q}$.

Задачи. 1. Идеал $\mathfrak{a} = (x^2, 2x)$ в целочисленной области полиномов одного переменного x не примарен. Однако $(x)^2 \equiv 0\ (\mathfrak{a}) \equiv 0\ (x)$ и (x) — простой идеал.

2. Пусть $\mathfrak{o}$ — кольцо с единицей. Если $\mathfrak{p}$ — простой идеал, свободный от делителей (§ 15), и $\mathfrak{p}^\rho \equiv 0\ (\mathfrak{a}) \equiv 0\ (\mathfrak{p})$, то $\mathfrak{a}$ — примарный идеал, принадлежащий простому идеалу $\mathfrak{p}$ [1]).

3. Если $\mathfrak{o}$ имеет единицу, то само $\mathfrak{o}$ является единственным примарным идеалом, принадлежащим простому идеалу $\mathfrak{o}$.

4. Если $\mathfrak{o}^*$ — подкольцо $\mathfrak{q}$ и $\mathfrak{q}$ — примарный идеал в $\mathfrak{o}$, принадлежащий простому идеалу $\mathfrak{p}$, то $\mathfrak{q} \cap \mathfrak{o}^*$ — примарный идеал в $\mathfrak{o}^*$, принадлежащий простому идеалу $\mathfrak{p} \cap \mathfrak{o}^*$.

§ 83. ОБЩАЯ ТЕОРЕМА РАЗЛОЖЕНИЯ

Пусть в кольце $\mathfrak{o}$ выполняется постулат о цепи делителей: всякая последовательность идеалов, из которых каждый делится на следующий, обрывается. Отсюда получается (положив еще в основу постулат выбора) „принцип индукции по делителям".

Идеал $\mathfrak{m}$ называется *приводимым*, если он является пересечением двух своих собственных делителей:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b},\ \mathfrak{a} \supset \mathfrak{m},\ \mathfrak{b} \supset \mathfrak{m}.$$

Если такое представление невозможно, то идеал называется *неприводимым*.

Примером неприводимого идеала могут служить простые идеалы, так как, если бы

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b},\ \mathfrak{a} \supset \mathfrak{p},\ \mathfrak{b} \supset \mathfrak{p},$$

то

$$\mathfrak{ab} \equiv 0\ (\mathfrak{a} \cap \mathfrak{b}) \equiv 0\ (\mathfrak{p}),\ \mathfrak{a} \not\equiv 0\ (\mathfrak{p}),\ \mathfrak{b} \not\equiv 0\ (\mathfrak{p}),$$

что противоречит свойству простоты.

Имеет место следующая *первая теорема разложения*:

Всякий идеал есть пересечение конечного числа неприводимых идеалов.

Доказательство. Для неприводимого идеала теорема верна. Поэтому пусть $\mathfrak{m}$ приводимо:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b},\ \mathfrak{a} \supset \mathfrak{m},\ \mathfrak{b} \supset \mathfrak{m}.$$

[1]) В немецком издании эта задача сформулирована неверно, так как упущено из виду существование единицы. Можно показать, что в кольце без единицы идеал $\mathfrak{a}$ может оказаться и не примарным. Например, в кольце всех четных чисел идеал $(2p)$, p — нечетное простое число, является простым идеалом, свободным от делителей. Если положить $\mathfrak{a} = (2^2 \cdot p)$, то все требования задачи будут удовлетворены, и тем не менее идеал $\mathfrak{a}$ оказывается не примарным. В самом деле, легко видеть, что $2p \cdot 2 = 0\ (\mathfrak{a})$, $2p \not\equiv 0\ (\mathfrak{a})$ и $2^k \not\equiv 0\ (\mathfrak{a})$ для любого натурального k ***Прим. перев.***

Если предположить теорему доказанной для всех собственных делителей $\mathfrak{m}$, то она будет в частности справедливой для $\mathfrak{a}$ и $\mathfrak{b}$; таким образом

$$\mathfrak{a} = [i_1, \ldots, i_s], \quad \mathfrak{b} = [i_{s+1}, \ldots, i_r].$$

Но отсюда следует, что

$$\mathfrak{m} = [i_1, \ldots, i_s, i_{s+1}, \ldots, i_r],$$

т. е. теорема также верна и для $\mathfrak{m}$. Так как она верна для единичного идеала (всегда неприводимого), то она согласно „принципу индукции по делителям" вообще верна.

Теперь в силу следующей теоремы пересечение неприводимых идеалов сводится к пересечению примарных идеалов.

Теорема. *Неприводимый идеал примарен.*

Доказательство. Пусть $\mathfrak{m}$ не примарно. Надо доказать, что $\mathfrak{m}$ приводимо.

Так как $\mathfrak{m}$ не примарно, то существуют два элемента a, b, для которых

$$ab \equiv 0\,(\mathfrak{m}),$$
$$a \not\equiv 0\,(\mathfrak{m}),$$
$$b^\rho \not\equiv 0\,(\mathfrak{m}) \text{ для какого бы то ни было } \rho.$$

Согласно постулату о цепях делителей последовательность отношений

$$\mathfrak{m} : b, \ \mathfrak{m} : b^2, \ \ldots$$

должна содержать конечное число различных членов, т. е. для некоторого k

$$\mathfrak{m} : b^k = \mathfrak{m} : b^{k+1}.$$

Мы теперь утверждаем, что

$$\mathfrak{m} = (\mathfrak{m}, \ a) \cap (\mathfrak{m}, \ \mathfrak{o}b^k). \tag{1}$$

Оба идеала справа делят $\mathfrak{m}$, и притом являются собственными делителями, так как первый содержит a, а второй идеал содержит b^{k+1}. Покажем, что всякий общий элемент этих идеалов необходимо принадлежит $\mathfrak{m}$. Такой элемент c, будучи элементом идеала $(\mathfrak{m}, \ \mathfrak{o}b^k)$, имеет вид:

$$c = m + rb^k;$$

с другой стороны, c как элемент $(\mathfrak{m}, \ a)$ удовлетворяет сравнению:

$$cb \equiv 0\,(\mathfrak{m}b, \ ab) \equiv 0\,(\mathfrak{m}).$$

Отсюда следует:

$$mb + rb^{k+1} = cb \equiv 0\,(\mathfrak{m}), \quad rb^{k+1} \equiv 0\,(\mathfrak{m}),$$

откуда в силу

$$\mathfrak{m} : b^{k+1} = \mathfrak{m} : b^k$$

имеем:

$$rb^k \equiv 0\,(\mathfrak{m}), \quad c = m + rb^k \equiv 0\,(\mathfrak{m}).$$

Тем самым (1) доказано; $\mathfrak{m}$ действительно приводимо.

Так как любой идеал можно представить в виде пересечения конечного числа неприводимых идеалов и неприводимый идеал примарен, то отсюда следует, что *любой идеал есть пересечение конечного числа примарных идеалов.* Эту теорему можно еще уточнить.

Прежде всего в представлении

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

можно выбросить все лишние идеалы $\mathfrak{q}_i$, т. е. все такие идеалы, которые содержат пересечение остальных. Тогда получится *несократимое* представление, т. е. такое, в котором уже не существует компонентов $\mathfrak{q}_i$, содержащих пересечение остальных. В таком представлении может еще оказаться, что некоторые примарные компоненты приводятся к одному примарному идеалу, т. е. что их пересечение также примарно. Следующие теоремы показывают, когда это имеет место:

1. *Пересечение конечного числа примарных идеалов, принадлежащих к одному и тому же простому идеалу, также примарно и обладает тем же простым идеалом.*

2. *Несократимое представление не примарно, если не все примарные компоненты принадлежат одному и тому же простому идеалу.*

Эти теоремы справедливы независимо от постулата о цепях делителей.

Доказательство 1. Пусть

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r],$$

где $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ все принадлежат $\mathfrak{p}$. Мы обращаемся к теореме III (§ 82). Из

$$ab \equiv 0 \,(\mathfrak{m}), \quad a \not\equiv 0 \,(\mathfrak{m})$$

следует:

$$ab \equiv 0 \,(\mathfrak{q}_\nu)$$

для всех ν и

$$a \not\equiv 0 \,(\mathfrak{q}_\nu)$$

по крайней мере для одного ν, а отсюда $b \equiv 0 \,(\mathfrak{p})$.

Если, с другой стороны, $b \equiv 0 \,(\mathfrak{p})$, то

$$b^{\rho_\nu} \equiv 0 \,(\mathfrak{q}_\nu) \text{ для всех } \nu;$$

таким образом, если $\rho = \max \rho_\nu$, то

$$b^\rho \equiv 0 \,(\mathfrak{q}_\nu) \text{ для всех } \nu, \quad b^\rho \equiv 0 \,(\mathfrak{m}).$$

Тем самым доказаны два свойства, упомянутые в теореме III. Таким образом, $\mathfrak{m}$ примарно и $\mathfrak{p}$ — соответствующий простой идеал.

Доказательство 2. Пусть дано несократимое представление

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] \qquad (r \geqslant 2),$$

в котором по крайней мере два соответствующих простых идеала $\mathfrak{p}$

различны. Пусть каждая группа примарных идеалов, принадлежащих одному и тому же простому идеалу, сведена к примарному идеалу. Представление тогда останется несократимым.

Среди конечного числа простых идеалов $\mathfrak{p}_\nu$ существует минимальный, т. е. такой, который не содержит ни один из остальных. Пусть это, например, $\mathfrak{p}_1$. Так как $\mathfrak{p}_1$ не содержит идеалов $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, то существуют такие элементы a_ν, что

$$\left.\begin{aligned} a_\nu &\not\equiv 0\ (\mathfrak{p}_1), \\ a_\nu &\equiv 0\ (\mathfrak{p}_\nu) \end{aligned}\right\} \qquad (\nu = 2, 3, \ldots, r);$$

следовательно, для достаточно большого ρ

$$a_\nu^\rho \equiv 0\ (\mathfrak{q}_\nu).$$

Если бы имело место $\mathfrak{q}_1 = \mathfrak{m}$, то представление $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ было бы сократимым (а именно $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$ были бы лишними). Поэтому в $\mathfrak{q}_1$ имеется элемент q_1, для которого

$$q_1 \not\equiv 0\ (\mathfrak{m}).$$

Произведение

$$q_1 (a_2 \ldots a_r)^\rho$$

лежит как в $\mathfrak{q}_1$, так и в $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$; следовательно, оно лежит в $\mathfrak{m}$. Но q_1 не лежит в $\mathfrak{m}$. Если бы $\mathfrak{m}$ было примарным, то отсюда следовало бы:

$$(a_2 \ldots a_r)^{\rho\sigma} \equiv 0\ (\mathfrak{m}),$$

$$(a_2 \ldots a_r)^{\rho\sigma} \equiv 0\ (\mathfrak{p}_1),$$

откуда, так как $\mathfrak{p}_1$ простое,

$$a_\nu \equiv 0\ (\mathfrak{p}_1)$$

по крайней мере для одного ν, что невозможно.

Если в несократимом представлении

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

все соответствующие простые идеалы $\mathfrak{p}_\nu$ различны, так что два или большее число идеалов пересечения нельзя заменить одним примарным идеалом, то говорят о *пересечении максимальных примарных идеалов*.

Эти максимальные примарные идеалы также называются *примарными компонентами* $\mathfrak{m}$.

Заменим примарные идеалы представления $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$, принадлежащие одному и тому же простому идеалу, их пересечениями. В результате получится пересечение максимальных примарных идеалов. Таким образом имеем *вторую теорему о разложении*:

Всякий идеал есть пересечение конечного множества максимальных примарных компонентов. Простые идеалы, принадлежащие этим примарным компонентам, все различны.

Эта вторая теорема о разложении, доказанная для области полиномов Э. Ласкером, а для общего случая Э. Нетер, представляет существеннейший результат теории идеалов. Приложения теоремы будут даны на всем

протяжении тринадцатой главы. В ближайшем параграфе мы увидим, как эта теорема увязывается с единственностью примарных компонентов.

Задачи. 1. Разложить идеал $(9, 3x+3)$ в целочисленной области полиномов одного неизвестного на примарные компоненты.

2. Для любого идеала $\mathfrak{a}$ существует такое произведение степеней простых идеалов $\mathfrak{p}_1^{\rho_1} \cdot \mathfrak{p}_2^{\rho_2} \cdot \ldots \mathfrak{p}_h^{\rho_h}$, делящееся на $\mathfrak{a}$, что всякое $\mathfrak{p}_\nu$ делит $\mathfrak{a}$.

3. Если кольцо $\mathfrak{o}$ обладает единицей, то идеал $\mathfrak{a}$, отличный от $\mathfrak{o}$, делится по крайней мере на один простой идеал, отличный от $\mathfrak{o}$.

4. Идеал $(4, 2x, x^2)$ в целочисленной области полиномов одного переменного, хотя и примарен, но приводим. [Разложение таково: $(4, 2x, x^2) = (4, x) \cap (2, x^2)$.]

§ 84. ТЕОРЕМЫ ОДНОЗНАЧНОСТИ

Разложение идеала на максимальные примарные компоненты не однозначно.

Пример: идеал

$$\mathfrak{m} = (x^2, xy)$$

в области полиномов $\mathsf{K}[x, y]$ состоит из полиномов, которые делятся на x и не содержат линейных членов. Множество всех полиномов, делящихся на x, образует простой идеал

$$\mathfrak{q}_1 = (x);$$

множество всех полиномов, не содержащих линейного и постоянного члена, образует примарный идеал

$$\mathfrak{q}_2 = (x^2, xy, y^2).$$

Таким образом

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_2].$$

Это представление несократимо. $\mathfrak{q}_1$ и $\mathfrak{q}_2$ — максимальные примарные идеалы, так как простые идеалы (x) и (x, y), принадлежащие соответственно $\mathfrak{q}_1$ и $\mathfrak{q}_2$, различны.

Но существует еще другое представление

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_3],$$

где

$$\mathfrak{q}_3 = (x^2, y),$$

так как если полином делится на x и не содержит члена с неизвестным x в первой степени, то полином лежит в $\mathfrak{m}$.

Если поле K бесконечно, то существует даже бесконечное число представлений

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}^{(\lambda)}], \quad \mathfrak{q}^{(\lambda)} = (x^2, y + \lambda x).$$

Но во всех приведенных представлениях $\mathfrak{m}$ имеется нечто общее, а именно, *число* примарных компонентов и соответствующих простых идеалов

$$(x), (x, y)$$

одно и то же. Вообще имеет место следующая теорема.

Первая теорема однозначности. Если $\mathfrak{m}$ *допускает несколько несократимых разложений на максимальные примарные компоненты, то число компонентов во всех разложениях одно и то же, причем все эти представления* $\mathfrak{m}$ *обладают одними и теми же простыми идеалами.*

Доказательство. Для примарного идеала теорема тривиальна. Поэтому воспользуемся методом индукции по числу примарных компонентов, входящих по крайней мере в одно представление рассматриваемого идеала.

Пусть

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}]. \tag{1}$$

Из всех простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_l, \mathfrak{p}'_1, \ldots, \mathfrak{p}'_{l'}$ возьмем максимальный, т. е. такой, который не делится на остальные. Пусть это будет $\mathfrak{p}_1$. Тогда $\mathfrak{p}_1$ должно войти справа, так как в противном случае

$$[\mathfrak{q}_1 : \mathfrak{q}_1, \ldots, \mathfrak{q}_l : \mathfrak{q}_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1, \ldots, \mathfrak{q}'_{l'} : \mathfrak{q}_1].$$

Но $\mathfrak{q}_1 \not\equiv 0 (\mathfrak{p}_\nu)$ (для всех $\nu > 1$), потому что иначе было бы $\mathfrak{p}_1 \equiv 0 (\mathfrak{p}_\nu)$, что противоречит максимальности $\mathfrak{p}_1$. Точно так же для всех ν следует, что $\mathfrak{q}_1 \not\equiv 0 (\mathfrak{p}'_\nu)$. По теореме IV′ (§ 82)

$$\mathfrak{q}_\nu : \mathfrak{q}_1 = \mathfrak{q}_\nu \ (\nu = 2, \ldots, l),$$
$$\mathfrak{q}'_\nu : \mathfrak{q}_1 = \mathfrak{q}'_\nu \ (\nu = 1, \ldots, l').$$

Но из $\mathfrak{q}_1 : \mathfrak{q}_1 = \mathfrak{o}$ получается, что

$$[\mathfrak{o}, \mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}].$$

Направо стоит $\mathfrak{m}$; следовательно, должно также и слева стоять $\mathfrak{m}$; $\mathfrak{o}$ может быть опущено; таким образом

$$\mathfrak{m} = [\mathfrak{q}_2, \ldots, \mathfrak{q}_l].$$

Но тогда первое из двух представлений (1) было бы сократимо, что противоречит предположению.

Итак, максимальный простой идеал входит в *обе* части.

Теперь пусть, например, $l \leqslant l'$. Докажем, что $l = l'$ и (при соответственном расположении) $\mathfrak{p}'_\nu = \mathfrak{p}_\nu$. Пусть для идеала, число примарных компонентов которого меньше l, все доказано. Расположим $\mathfrak{q}$ и $\mathfrak{q}'$ так, чтобы $\mathfrak{p}_1 = \mathfrak{p}'_1$ было максимальным идеалом, принадлежащим $\mathfrak{q}_1$ и $\mathfrak{q}'_1$.

Возьмем от обеих частей (1) отношения по произведению $\mathfrak{q}_1\mathfrak{q}'_1$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}'_1, \ldots, \mathfrak{q}_l : \mathfrak{q}_1\mathfrak{q}'_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'} : \mathfrak{q}_1\mathfrak{q}'_1].$$

Тогда из тех же соображений, что и выше, мы получим:

$$\left.\begin{aligned} \mathfrak{q}_\nu : \mathfrak{q}_1\mathfrak{q}'_1 &= \mathfrak{q}_\nu, \\ \mathfrak{q}'_\nu : \mathfrak{q}_1\mathfrak{q}'_1 &= \mathfrak{q}'_\nu \end{aligned}\right\} \quad (\nu > 1).$$

Далее, так как $q_1 q_1'$ делится на q_1 и на q_1', имеет место:

$$q_1 : q_1 q_1' = \mathfrak{o},$$
$$q_1' : q_1 q_1' = \mathfrak{o};$$

таким образом

$$[q_2, \ldots, q_l] = [q_2', \ldots, q_{l'}'].$$

Согласно индуктивному предположению должно быть $l' - 1 = l - 1$, т. е. $l' = l$, так как слева и справа стоит несократимое пересечение максимальных примарных компонентов. Кроме того, при соответственном расположении должно быть $\mathfrak{p}_\nu = \mathfrak{p}_\nu'$ для всех $\nu > 1$. Так как $\mathfrak{p}_1' = \mathfrak{p}_1$, то все доказано.

Идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$, которые по только что доказанной теореме определяются однозначно, называются *простыми идеалами, принадлежащими идеалу* $\mathfrak{m}$. Они обладают следующим важным свойством:

Если идеал $\mathfrak{a}$ *не делится на простые идеалы, принадлежащие идеалу* $\mathfrak{b}$, *то* $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$, *и обратно.*

Доказательство. Пусть $\mathfrak{b} = [q_1, \ldots, q_l]$ — несократимое представление. Пусть $\mathfrak{a} \not\equiv 0 \, (\mathfrak{p}_i)$ для $i = 1, \ldots, l$, где $\mathfrak{p}_i$ принадлежит q_i. Отсюда следует, что

$$q_i : \mathfrak{a} = q_i,$$
$$\mathfrak{b} : \mathfrak{a} = [q_1, \ldots, q_l] : \mathfrak{a} =$$
$$= [q_1 : \mathfrak{a}, \ldots, q_l : \mathfrak{a}] =$$
$$= [q_1, \ldots, q_l] = \mathfrak{b}.$$

Обратно, пусть $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$. Если бы имело место $\mathfrak{a} \equiv 0 \, (\mathfrak{p}_i)$ для некоторого i, например $\mathfrak{a} \equiv 0 \, (\mathfrak{p}_1)$, то отсюда вытекало бы $\mathfrak{a}^\varrho \equiv 0 \, (q_1)$; поэтому

$$\mathfrak{a}^\varrho \cdot [q_2, \ldots, q_l] \equiv 0 \, ([q_1, q_2, \ldots, q_l]) \equiv 0 \, (\mathfrak{b}),$$

откуда, так как сравнение (по модулю $\mathfrak{b}$) можно сократить на $\mathfrak{a}$ и тем самым также на $\mathfrak{a}^\varrho$,

$$[q_2, \ldots, q_l] \equiv 0 \, (\mathfrak{b}),$$

что противоречит несократимости представления.

Одним из важнейших частных случаев является тот случай, когда $\mathfrak{a}$ есть главный идеал (a):

Если элемент a *не делится ни на какой простой идеал, принадлежащий идеалу* $\mathfrak{b}$, *то* $\mathfrak{b} : a = \mathfrak{b}$, *т. е. из* $ac \equiv 0 \, (\mathfrak{b})$ *всегда следует* $c \equiv 0 \, (\mathfrak{b})$.

Можно еще иначе сформулировать общую теорему, представив $\mathfrak{a}$ в виде пересечения $[q_1', \ldots, q_{l'}']$ примарных идеалов, $\mathfrak{a}$ тогда и только тогда делится на $\mathfrak{p}_i$, если на $\mathfrak{p}_i$ делится одно из q_j' [1]) или, что одно и то же, одно из $\mathfrak{p}_j'$. Таким образом:

Если ни один простой идеал, принадлежащий $\mathfrak{a}$, *не делится на простой идеал, принадлежащий* $\mathfrak{b}$, *то* $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$, *и обратно.*

---

[1]) В самом деле, очевидно, что если q_j' делится на $\mathfrak{p}_i$, то $\mathfrak{a}$ также делится на $\mathfrak{p}_i$, а из $\mathfrak{a} \equiv 0 \, (\mathfrak{p}_i)$ следует $q_1' \ldots q_{l'}' \equiv 0 \, ([q_1', \ldots, q_{l'}']) \equiv 0 \, (\mathfrak{p}_i)$, откуда q_j' делится на $\mathfrak{p}_i$.

Именно в такой формулировке и будет использовано предложение при доказательстве второй теоремы однозначности, однозначности „изолированных компонентов".

Под *компонентом* идеала $\mathfrak{a}$ будет подразумеваться любое пересечение примарных идеалов, входящих в какое-нибудь несократимое представление $\mathfrak{a}$ через максимальные примарные идеалы.

Пусть таким образом

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$$

будет несократимое представление, причем

$$\mathfrak{a}_1 = [\mathfrak{q}_1, \ldots, \mathfrak{q}_k] \quad \text{или} \quad = \mathfrak{o}, \text{ если } k = 0$$
$$\mathfrak{a}_2 = [\mathfrak{q}_{k+1}, \ldots, \mathfrak{q}_l] \text{ или } = \mathfrak{o}, \text{ если } k = l.$$

Тогда

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2,$$

и $\mathfrak{a}_1$ есть компонент $\mathfrak{a}$.

Компонент $\mathfrak{a}_1$ называется *изолированным*, если ни один простой идеал $\mathfrak{p}_{k+i}$, принадлежащий $\mathfrak{a}_2$, не делится на идеал $\mathfrak{p}_i$, принадлежащий $\mathfrak{a}_1$.

Назовем принадлежащий к $\mathfrak{a}$ простой идеал окутанным, если он является делителем другого простого идеала, принадлежащего к $\mathfrak{a}$. Тогда можно определить изолированный компонент идеала $\mathfrak{a}$ как такой, у которого множество принадлежащих к нему простых идеалов или вовсе не содержит окутанных простых идеалов, или, содержа окутанные простые идеалы, содержит также все окутывающие их простые идеалы.

Вторая теорема однозначности: подмножеством простых идеалов, принадлежащих $\mathfrak{a}$, *изолированный компонент идеала* $\mathfrak{a}$ *определяется однозначно.*

Доказательство. Пусть даны два представления

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1' \cap \mathfrak{a}_2', \tag{2}$$

причем $\mathfrak{a}_1'$ имеет те же соответствующие простые идеалы, что и $\mathfrak{a}_1$. Кроме того, пусть $\mathfrak{a}_1$ и $\mathfrak{a}_1'$ — изолированные компоненты. Тогда из доказанной выше теоремы следует:

$$\mathfrak{a}_1 : \mathfrak{a}_2 = \mathfrak{a}_1,$$
$$\mathfrak{a}_1' : \mathfrak{a}_2 = \mathfrak{a}_1'.$$

Таким образом, составляя в (2) отношения по $\mathfrak{a}_2$, получим:

$$\mathfrak{a} : \mathfrak{a}_2 = \mathfrak{a}_1 = \mathfrak{a}_1' \cap (\mathfrak{a}_2' : \mathfrak{a}_2),$$
$$\mathfrak{a}_1 \subset \mathfrak{a}_1'.$$

Точно так же следует, что

$$\mathfrak{a}_1' \subseteq \mathfrak{a}_1,$$

откуда

$$\mathfrak{a}_1 = \mathfrak{a}_1',$$

что и требовалось доказать.

В частности *изолированные примарные компоненты* некоторого идеала определяются однозначно.

§ 85. ТЕОРИЯ ВЗАИМНО ПРОСТЫХ ИДЕАЛОВ

Здесь и ниже мы будем предполагать, что кольцо $\mathfrak{o}$ обладает единицей. Эта единица порождает единичный идеал $\mathfrak{o}$:

$$\mathfrak{o} = (1)\ ^{1}).$$

Два идеала $\mathfrak{a}$, $\mathfrak{b}$ называются *взаимно простыми*, если они не имеют, кроме $\mathfrak{o}$, общего наибольшего делителя, или если их общий наибольший делитель равен $\mathfrak{o}$:

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}.$$

Это равенство означает, что любой элемент $\mathfrak{o}$ равен сумме из элементов идеала $\mathfrak{a}$ и идеала $\mathfrak{b}$; очевидно, что $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ тогда и только тогда, если

$$1 = a + b \tag{1}$$

(a лежит в $\mathfrak{a}$, а b — в $\mathfrak{b}$). Но тогда

$$\left.\begin{aligned} a &\equiv 1\ (\mathfrak{b}), \quad b \equiv 0\ (\mathfrak{b}), \\ a &\equiv 0\ (\mathfrak{a}), \quad b \equiv 1\ (\mathfrak{a}). \end{aligned}\right\} \tag{2}$$

Если два примарных идеала $\mathfrak{q}_1$, $\mathfrak{q}_2$ взаимно просты, то и подавно взаимно просты соответствующие простые идеалы $\mathfrak{p}_1$, $\mathfrak{p}_2$ (общий делитель $\mathfrak{p}_1$ и $\mathfrak{p}_2$ должен быть общим делителем $\mathfrak{q}_1$, $\mathfrak{q}_2$). Но верно также и обратное: *если* $\mathfrak{p}_1$, $\mathfrak{p}_2$ *взаимно просты, то и* $\mathfrak{q}_1$, $\mathfrak{q}_2$ *взаимно просты*. Действительно, из

$$1 = p_1 + p_2$$

следует при возвышении в $(\rho + \sigma - 1)$-ю степень:

$$1 = p_1^{\rho+\sigma-1} + \ldots + p_2^{\rho+\sigma-1};$$

если возьмем затем ρ и σ настолько большими, чтобы p_1^{ρ} лежало в $\mathfrak{q}_1$ и p_2^{σ} — в $\mathfrak{q}_2$, то направо каждый член суммы будет лежать в $\mathfrak{q}_1$ или в $\mathfrak{q}_2$, откуда

$$1 = q_1 + q_2.$$

Если два идеала $\mathfrak{a}$, $\mathfrak{b}$ *взаимно просты, то* $\mathfrak{a}$ *взаимно просто с* $\mathfrak{b}$, *а* $\mathfrak{b}$ *взаимно просто с* $\mathfrak{a}$ (см. § 81).

Доказательство. Пусть $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$; таким образом $a + b = 1$. Достаточно доказать, что $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{a}$. Если x принадлежит $\mathfrak{a} : \mathfrak{b}$, то $x\mathfrak{b} \subseteq \mathfrak{a}$; поэтому $xb \equiv 0\ (\mathfrak{a})$, откуда также

$$x(a + b) \equiv 0\ (\mathfrak{a}),$$
$$x \cdot 1 \equiv 0\ (\mathfrak{a}),$$

т. е. x принадлежит $\mathfrak{a}$, что и требовалось доказать.

---

1) Отсюда следует $\mathfrak{o}^2 = (1)\cdot(1) = (1) = \mathfrak{o}$, т. е. $\mathfrak{o}^2 = \mathfrak{o}$, что в кольце без единицы не имеет места.

Обратное неверно; например, в кольце полиномов $K[x, y]$ идеалы (x), (y) взаимно простые друг с другом, но тем не менее, они не взаимно просты:

$$(x, y) \neq \mathfrak{o},$$
$$\left.\begin{aligned}(x):(y) &= (x),\\ (y):(x) &= (y).\end{aligned}\right\}$$

Если $\mathfrak{a}$ и $\mathfrak{b}$ взаимно простые, то общее решение сравнений находится совершенно так же, как это делается в теории чисел. Пусть даны два сравнения:

$$\left.\begin{aligned}f(\xi) &\equiv 0\,(\mathfrak{a})\\ g(\xi) &\equiv 0\,(\mathfrak{b})\end{aligned}\right\} \qquad \big(f(x),\ g(x) \in \mathfrak{o}[x]\big).$$

Пусть известно решение для каждого сравнения в отдельности. Если, например, $\xi \equiv \alpha$ — решение первого, $\xi \equiv \beta$ — решение второго сравнения, то элемент ξ, удовлетворяющий двум сравнениям, найдется следующим образом:

$$\xi = b\alpha + a\beta,$$

где a и b — элементы, удовлетворяющие (1) и (2). Легко видеть, что $\xi \equiv \alpha\,(\mathfrak{a})$ и $\xi \equiv \beta\,(\mathfrak{b})$, т. е. ξ действительно удовлетворяет данным сравнениям.

Общее наименьшее кратное двух взаимно простых идеалов равно их произведению.

Доказательство. В § 81 было доказано, что

$$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b},$$
$$[\mathfrak{a} \cap \mathfrak{b}]\cdot(\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{ab}.$$

Если теперь $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ и в $\mathfrak{o}$ существует единица, то второе соотношение приводится к

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab};$$

таким образом

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

Для обобщения этой теоремы на случай большего числа идеалов необходимо остановиться на следующей лемме:

Если $\mathfrak{a}$ *взаимно просто с* $\mathfrak{b}$ *и* $\mathfrak{c}$, *то* $\mathfrak{a}$ *также взаимно просто с произведением* $\mathfrak{bc}$ *и с пересечением* $\mathfrak{b} \cap \mathfrak{c}$.

Доказательство. Из

$$a + b = 1,$$
$$a' + c = 1$$

следует:

$$(a + b)(a' + c) = 1,$$
$$aa' + ac + a'b + bc = 1,$$
$$a'' + bc = 1,$$

где $a'' = aa' + ac + a'b$ — опять элемент из $\mathfrak{a}$. Отсюда следует, что

$$(\mathfrak{a}, \mathfrak{bc}) = \mathfrak{o},$$

а потому и подавно

$$(\mathfrak{a}, \mathfrak{b} \cap \mathfrak{c}) = \mathfrak{o}.$$

Если в $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ любые два идеала взаимно просты, и

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}] = \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1},$$

то

$$\begin{aligned}[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] &= [\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}] \cap \mathfrak{a}_n = \\ &= (\mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = \\ &= \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}\mathfrak{a}_n,\end{aligned}$$

откуда по индукции получаем теорему:

Общее наименьшее кратное конечного множества попарно взаимно простых идеалов равно их произведению.

Прежнее замечание о решении сравнения по взаимно простым идеалам справедливо также и для случая многих идеалов:

Если $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_r$ — *идеалы и любые два из этих идеалов взаимно просты, то сравнения*

$$\xi \equiv \alpha_i \ (\mathfrak{a}_i) \qquad (i = 1, 2, \ldots, r)$$

всегда разрешимы относительно ξ.

Доказательство. Пусть найдено

$$\eta \equiv \alpha_i \ (\mathfrak{a}_i) \qquad (i = 1, 2, \ldots, r-1).$$

Тогда определяем ξ следующим образом:

$$\left.\begin{aligned}\xi &\equiv \eta \ ([\mathfrak{a}_1, \ldots, \mathfrak{a}_{r-1}]), \\ \xi &\equiv \alpha_r \ (\mathfrak{a}_r),\end{aligned}\right\}$$

что всегда возможно, так как $\mathfrak{a}_r$ и $[\mathfrak{a}_1, \ldots, \mathfrak{a}_{r-1}]$ взаимно просты.

Если в $\mathfrak{o}$ *справедлив постулат о цепях делителей, то всякий идеал можно представить в виде пересечения идеалов такого рода, что любые два идеала взаимно просты и ни один идеал уже не является пересечением собственных делителей, попарно взаимно простых.*

Для доказательства возьмем несократимое представление

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

данного идеала $\mathfrak{a}$ через примарные идеалы и найдем последовательность примарных идеалов, не взаимно простых с $\mathfrak{q}_1$ и между собою. Обозначим их пересечение через $\mathfrak{a}_1$. Подобным же образом из оставшихся идеалов получаем последовательно идеалы $\mathfrak{a}_2, \ldots, \mathfrak{a}_s$. Представление

$$\mathfrak{a} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_s] \tag{3}$$

обладает искомыми свойствами. В самом деле, во-первых, $\mathfrak{a}_i$ и $\mathfrak{a}_k$ при $i \neq k$ взаимно просты, так как компоненты $\mathfrak{a}_i$ взаимно просты с компонентами $\mathfrak{a}_k$. Во-вторых, невозможно, чтобы, например, $\mathfrak{a}_1$ было пересечением двух его взаимно простых собственных делителей. А именно, если бы имело место

$$\begin{aligned}\mathfrak{a}_1 &= \mathfrak{b} \cap \mathfrak{c} = \mathfrak{bc}, \\ (\mathfrak{b}, \mathfrak{c}) &= \mathfrak{o},\end{aligned}$$

то всякий простой идеал, принадлежащий $\mathfrak{a}_1$, делил бы $\mathfrak{bc}$ и потому был бы делителем $\mathfrak{b}$ или $\mathfrak{c}$. Но все эти простые идеалы между собой не

взаимно просты; поэтому, если один из простых идеалов делит, например, $\mathfrak{b}$, то все эти простые идеалы должны делить $\mathfrak{b}$, но не $\mathfrak{c}$. Соответствующие примарные компоненты делят $\mathfrak{bc}$, откуда следует, что они делят $\mathfrak{b}$ (так как их простые идеалы не делят $\mathfrak{c}$). Поэтому $\mathfrak{a}_1$ делит также $\mathfrak{b}$:

$$\mathfrak{b} \subseteq \mathfrak{a}_1,$$

что невозможно, так как $\mathfrak{b}$ есть собственный делитель идеала $\mathfrak{a}_1$.

Вместо представления (3) согласно нашей теореме можно записать $\mathfrak{a}$ в виде произведения:

$$\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2 \dots \mathfrak{a}_s.$$

Задача 1. Доказать *„третью теорему единственности“*, которая говорит об единственном определении идеалов $\mathfrak{a}_1, \dots, \mathfrak{a}_s$, входящих в (3). (Для доказательства придется вернуться ко второй теореме единственности.)

С мультипликативным разложением идеала $\mathfrak{a}$ связано аддитивное разложение кольца $\mathfrak{o}$ и кольца вычетов $\frac{\mathfrak{o}}{\mathfrak{a}}$. Докажем прежде всего следующее:

Если $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ *— попарно взаимно простые идеалы и*

$$\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_r = [\mathfrak{a}_1, \dots, \mathfrak{a}_r],$$

$$\mathfrak{b}_\nu = \mathfrak{a}_1 \dots \mathfrak{a}_{\nu-1}\, \mathfrak{a}_{\nu+1} \dots \mathfrak{a}_r = [\mathfrak{a}_1, \dots, \mathfrak{a}_{\nu-1}, \mathfrak{a}_{\nu+1}, \dots, \mathfrak{a}_r],$$

то

$$\mathfrak{o} = (\mathfrak{b}_1, \dots, \mathfrak{b}_r),$$

и притом аддитивное представление любого элемента $\mathfrak{o}$ *в виде суммы элементов* $\mathfrak{b}_1, \dots, \mathfrak{b}_r$ *есть единственное по модулю* $\mathfrak{a}$.

Доказательство. Из определения $\mathfrak{a}$ и $\mathfrak{b}_\nu$ следует, что

$$\mathfrak{a} = \mathfrak{a}_\nu \cap \mathfrak{b}_\nu = \mathfrak{a}_\nu \cdot \mathfrak{b}_\nu .$$

Пусть b — произвольный элемент $\mathfrak{o}$. Находим $b_1, \dots, b_{r-1}$ из сравнений

$$b \equiv b\,(\mathfrak{a}_\nu); \quad b_\nu \equiv 0\,(\mathfrak{b}_\nu).$$

Тогда для $\nu = 1, 2, \dots, r-1$:

$$b \equiv \sum_1^{r-1} b_\lambda\,(\mathfrak{a}_\nu).$$

Если положим

$$b - \sum_1^{r-1} b_\lambda = b_r,$$

то

$$b_r \equiv 0\,(\mathfrak{a}_\nu)$$

для

$$\nu = 1, 2, \dots, r-1,$$

откуда

$$b_r \equiv 0\,(\mathfrak{b}_r).$$

Тем самым искомое представление

$$b = \sum_1^r b_\nu$$

получено. Теперь, если существуют два таких представления

$$b = \sum_1^r b_\nu = \sum_1^r b'_\nu,$$

то, так как по модулю $\mathfrak{a}_\mu$ все $\mathfrak{b}_\nu$ при $\nu \neq \mu$ сравнимы с нулем, имеем:

$$b_\mu \equiv b'_\mu \ (\mathfrak{a}_\mu).$$

Таким образом разность $b_\mu - b'_\mu$ принадлежит $\mathfrak{a}_\mu$ и $\mathfrak{b}_\mu$ и тем самым принадлежит $\mathfrak{a} = \mathfrak{a}_\mu \cap \mathfrak{b}_\mu$. Следовательно, $\mathfrak{b}_\mu \equiv \mathfrak{b}'_\mu \ (\mathfrak{a})$, что и требовалось доказать.

Если теперь перейдем к кольцу вычетов $\overline{\mathfrak{o}} = \frac{\mathfrak{o}}{\mathfrak{a}}$, заменяя все элементы b соответствующими классами вычетов $\overline{b}$ и полагая $\overline{\mathfrak{b}}_\nu = \frac{\mathfrak{b}_\nu}{\mathfrak{a}}$, $\overline{\mathfrak{a}}_\nu = \frac{\mathfrak{a}_\nu}{\mathfrak{a}}$, то получим единственное представление всех элементов $\overline{b}$ из $\overline{\mathfrak{o}}$ в виде:

$$\overline{b} = \overline{b}_1 + \overline{b}_2 + \ldots + \overline{b}_r; \quad \overline{b}_\nu \in \overline{\mathfrak{b}}_\nu. \tag{4}$$

Так как представление единственное, то сумма $\overline{\mathfrak{o}} = (\overline{\mathfrak{b}}_1, \ldots, \overline{\mathfrak{b}}_r)$ *прямая* в смысле § 42. Далее имеем $\overline{\mathfrak{a}}_\nu \cdot \overline{\mathfrak{b}}_\nu = (0)$, откуда, в силу того, что $\overline{\mathfrak{b}}_\mu$ $(\mu \neq \nu)$ есть подмножество идеала $\overline{\mathfrak{a}}_\nu$, следует:

$$\overline{\mathfrak{b}}_\mu \cdot \overline{\mathfrak{b}}_\nu = 0.$$

Итак: *кольцо* $\overline{\mathfrak{o}} = \frac{\mathfrak{o}}{\mathfrak{a}}$ *представляет собой прямую сумму колец* $\overline{\mathfrak{b}}_1, \ldots, \overline{\mathfrak{b}}_r$, *причем* $\overline{\mathfrak{b}}_\mu \cdot \overline{\mathfrak{b}}_\nu = 0$ *для всяких* $\mu \neq \nu$.

Любому b из $\mathfrak{o}$ соответствует $\overline{b}$, а $\overline{b}$ соответствует $\overline{b}_1$. Оба соответствия представляют собой гомоморфизмы колец; таким образом соответствие $b \to \overline{b}_1$ является также гомоморфизмом колец. Если $\overline{b}_1 = 0$, то $\overline{b} \in \overline{\mathfrak{a}}_1$, и потому $b \in \mathfrak{a}_1$, и обратно. Отсюда в силу теоремы о гомоморфизме следует:

$$\overline{\mathfrak{b}}_1 \cong \frac{\mathfrak{o}}{\mathfrak{a}_1}.$$

Очевидно, что также и для всякого ν

$$\overline{\mathfrak{b}}_\nu \cong \frac{\mathfrak{o}}{\mathfrak{a}_\nu}.$$

2. Применяя разложение (4) к единице 1 кольца $\overline{\mathfrak{o}}$, получим:

$$1 = \overline{e}_1 + \overline{e}_2 + \ldots + \overline{e}_r; \quad \overline{e}_\nu^2 = \overline{e}_\nu; \quad \overline{e}_\mu \overline{e}_\nu = 0 \text{ для } \mu \neq \nu,$$

где $\overline{e}_\nu$ суть единицы колец $\overline{\mathfrak{b}}_\nu$.

§ 86. ЕДИНООБРАЗНЫЕ ИДЕАЛЫ

Пусть $\mathfrak{o}$ — снова кольцо с единицей.

Единичный идеал $\mathfrak{o}$ всегда является простым. Какие же примарные идеалы могут принадлежать $\mathfrak{o}$? Оказывается, что только $\mathfrak{o}$. Действительно, если $\mathfrak{q}$ — примарный идеал, принадлежащий $\mathfrak{o}$, то $1 \in \mathfrak{o}$, откуда $1^p \in \mathfrak{q}$ и $\mathfrak{q} = \mathfrak{o}$.

Пусть единичный идеал $\mathfrak{o}$ входит в число простых идеалов $\mathfrak{p}_i$, принадлежащих пересечению $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] \neq \mathfrak{o}$. Тогда примарные идеалы $\mathfrak{q}_i$, принадлежащие $\mathfrak{o}$, равны $\mathfrak{o}$ и потому будут лишними. Следовательно: *если представление* $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ *несократимо и* $\mathfrak{a} \neq \mathfrak{o}$, *то единичный идеал не может входить в число соответствующих простых идеалов.*

Отсюда сразу вытекает, как только в $\mathfrak{o}$ оказывается справедливым постулат о цепи делителей, что *всякий идеал* $\mathfrak{a} \neq \mathfrak{o}$ *делится по крайней мере на одно простое* $\mathfrak{p} \neq \mathfrak{o}$. *Если идеал* $\mathfrak{a}$ *не примарен, то он делится даже по меньшей мере на два простых делителя не равных* $\mathfrak{o}$.

Идеал, который имеет лишь один простой делитель помимо $\mathfrak{o}$, называется по Дедекинду *единообразным*. По предыдущей теореме единообразный идеал $\mathfrak{q}$ примарен. Кроме того, соответствующий простой идеал $\mathfrak{p}$ должен быть свободен от делителей, ибо если бы $\mathfrak{a}' \neq \mathfrak{o}$ было собственным делителем идеала $\mathfrak{p}$, то $\mathfrak{a}'$ делилось бы на простое $\mathfrak{p}' \neq \mathfrak{o}$, являющееся собственным делителем идеала $\mathfrak{p}$; таким образом $\mathfrak{q}$ допускало бы два различных и не равных $\mathfrak{o}$ простых делителя $\mathfrak{p}$ и $\mathfrak{p}'$, что противоречит единообразности $\mathfrak{q}$. Справедливо сравнение

$$\mathfrak{p}^{\rho} \equiv 0 \,(\mathfrak{q}). \tag{1}$$

Из соотношения (1) следует, если $\mathfrak{p}$ свободно от делителей, также единообразность $\mathfrak{q}$. Если $\mathfrak{p}'$ — произвольный простой делитель $\mathfrak{q}$, то из (1) следует:

$$\mathfrak{p}^{\rho} \equiv 0 \,(\mathfrak{p}'),$$

откуда

$$\mathfrak{p} \equiv 0 \,(\mathfrak{p}');$$

таким образом либо $\mathfrak{p}' = \mathfrak{p}$, либо $\mathfrak{p}' = \mathfrak{o}$, т. е. $\mathfrak{q}$ имеет делителями только $\mathfrak{p}$ и $\mathfrak{o}$.

Итак, понятия:

1) единообразный идеал,

2) примарный идеал, принадлежащий простому идеалу $\mathfrak{p}$, свободному от делителей,

3) делитель степени $\mathfrak{p}^{\rho}$ простого идеала $\mathfrak{p}$, свободного от делителей, — равнозначны. Далее оказывается справедливым такое предложение:

Если идеал $\mathfrak{m}$ *обладает изолированным единообразным примарным компонентом* $\mathfrak{q}$, *имеющим показателем* ρ *и принадлежащим простому идеалу* $\mathfrak{p}$, *то для всякого целого числа* $\sigma \geqslant \rho$:

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^{\sigma}). \tag{2}$$

Доказательство. Из

$$\mathfrak{m} \equiv 0 \,(\mathfrak{q})$$

и

$$\mathfrak{p}^{\sigma} \equiv 0 \,(\mathfrak{q})$$

следует:

$$(\mathfrak{m}, \mathfrak{p}^{\sigma}) \equiv 0 \,(\mathfrak{q}). \tag{3}$$

С другой стороны, пусть

$$\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_2, \ldots, \mathfrak{q}_s]$$

есть представление $\mathfrak{m}$ через примарные компоненты. Идеал $(\mathfrak{m}, \mathfrak{p}^{\sigma})$ единообразен, а потому примарен; соответствующий простой идеал равен $\mathfrak{p}$. Произведение $\mathfrak{q}\mathfrak{q}_2 \ldots \mathfrak{q}_s$ делится на $(\mathfrak{m}, \mathfrak{p}^{\sigma})$; но $\mathfrak{q}_2 \ldots \mathfrak{q}_s$, так как $\mathfrak{q}$ по предположению *изолировано*, не делится на $\mathfrak{p}$; таким образом $\mathfrak{q}$ должно делиться на $(\mathfrak{m}, \mathfrak{p}^{\sigma})$:

$$\mathfrak{q} \equiv 0 \,(\mathfrak{m}, \mathfrak{p}^{\sigma}). \tag{4}$$

Из (3) и (4) следует (2).

Следствие. При $\sigma \geqslant \rho$

$$\mathfrak{p}^\sigma \equiv 0\,(\mathfrak{q}) \equiv 0\,(\mathfrak{m},\ \mathfrak{p}^{\sigma+1}),$$

откуда

$$\mathfrak{p}^\sigma \equiv 0\,(\mathfrak{m},\ \mathfrak{p}^{\sigma+1}). \tag{5}$$

При $\sigma < \rho$ условие (5) уже не выполняется. В самом деле, если бы имело место

$$\mathfrak{p}^\sigma \equiv 0\,(\mathfrak{m},\ \mathfrak{p}^{\sigma+1})$$

для некоторого $\sigma < \rho$, то при умножении на $\mathfrak{p}^{\rho-\sigma-1}$ получилось бы:

$$\mathfrak{p}^{\rho-1} \equiv 0\,(\mathfrak{m}\mathfrak{p}^{\rho-\sigma-1},\ \mathfrak{p}^\rho) \equiv 0\,(\mathfrak{m},\ \mathfrak{q}) \equiv 0\,(\mathfrak{q}),$$

что противоречит определению показателя ρ.

Итак, *показатель ρ идеала $\mathfrak{q}$ есть наименьшее число, для которого выполняется* (5).

Существуют области целостности $\mathfrak{o}$ с единицей, в которых имеет место постулат о цепях делителей, и всякий простой идеал, отличный от нулевого, свободен от делителей. Например, сюда относится кольцо главных идеалов (см. § 17), точно так же несколько позднее будут даны типичные примеры для числового и функционального поля и для кольца $C[\sqrt{-3}]$. В этих кольцах все *примарные идеалы, кроме нулевого, очевидно, единообразны.* Затем здесь всякие отличные друг от друга и от нуля простые идеалы взаимно просты. Отсюда следует, что два примарных идеала, принадлежащие различным и не равным нулю простым идеалам, также взаимно просты. Наконец, все примарные компоненты идеала изолированы и потому определяются единственным образом. Итак, *идеал, отличный от нулевого, допускает единственное представление в виде пересечения взаимно простых единообразных примарных идеалов.* Согласно § 85 это представление равно произведению:

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_r.$$

Согласно теоремам конца § 95 кольцо вычетов $\frac{\mathfrak{o}}{\mathfrak{a}}$ есть прямая сумма колец $\frac{\mathfrak{o}}{\mathfrak{q}_\nu}$, для которых $\frac{\mathfrak{o}}{\mathfrak{q}_\nu} \cdot \frac{\mathfrak{o}}{\mathfrak{q}_\mu} = 0$ $(\nu \neq \mu)$. Эти кольца примарны, т. е. в них всякий делитель нуля нильпотентен.

В кольце главных идеалов примарные идеалы $\mathfrak{q}_i$ одновременно равны степени простых идеалов. От тех или иных ограничений зависит, будет ли это иметь место для более общих колец; мы позднее увидим, что таким условием является „целозамкнутость“ (§ 98).

Теория идеалов областей целостности, в которых любой простой идеал, кроме нуля, свободен от делителей, развита Крулем значительно проще, чем общая теория идеалов § 82—84. А именно, из постулата о цепях делителей легко следует, что для всякого идеала $\mathfrak{a}$ существует произведение степеней простых идеалов, делителей $\mathfrak{a}$, которое в свою очередь делится на $\mathfrak{a}$ (см. § 100, лемма 1):

$$\mathfrak{p}_1^{\rho_1} \cdot \mathfrak{p}_2^{\rho_2} \ldots \mathfrak{p}_r^{\rho_r} \equiv 0\,(\mathfrak{a}),$$

$$\mathfrak{a} \equiv 0\,(\mathfrak{p}_i) \qquad (i = 1, \ldots, r).$$

Если $\mathfrak{a} = \mathfrak{q}$ единообразно, то, кроме 0, существует по крайней мере одно $\mathfrak{p}_i = \mathfrak{p}$ и $\mathfrak{p}^{\rho_i} \equiv 0\,(\mathfrak{q})$, причем заново выведено свойство единообразного идеала делить

степени простого идеала. Если $\mathfrak{a} \neq (0)$ не единообразно, то простые идеалы $\mathfrak{p}_i$ и тем самым также степени $\mathfrak{p}_i^{\rho_i}$ между собою взаимно просты, откуда взаимно просты и идеалы $\mathfrak{q}_i = \left(\mathfrak{a}, \mathfrak{p}_i^{\rho_i}\right)$, и их пересечение равно их произведению:

$$[\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_r.$$

$\mathfrak{a}$ делится на все $\mathfrak{q}_i$ и потому также делится на их произведение. С другой стороны, произведение

$$\mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_r = \left(\mathfrak{a}, \mathfrak{p}_1^{\rho_1}\right) \cdot \left(\mathfrak{a}, \mathfrak{p}_2^{\rho_2}\right) \ldots \left(\mathfrak{a}, \mathfrak{p}_r^{\rho_r}\right)$$

согласно закону дистрибутивности (§ 81) приводится к сумме идеалов, делящихся на $\mathfrak{a}$. Следовательно,

$$\mathfrak{a} \equiv 0 \,(\mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_r) \equiv 0 \,(\mathfrak{a}),$$

откуда

$$\mathfrak{a} \equiv [\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_r.$$

$\mathfrak{q}_i$ как делители $\mathfrak{p}_i^{\rho_i}$, очевидно, делятся только на простые идеалы $\mathfrak{p}_i$ и $\mathfrak{o}$; других простых делителей быть не может. Поэтому $\mathfrak{q}_i$ единообразны. Единственность $\mathfrak{q}_i$ следует из того, что согласно вышеизложенному для всякого разложения $\mathfrak{a} = [\mathfrak{q}_1', \ldots, \mathfrak{q}_r']$ необходимо должно быть $\mathfrak{q}_i' = \left(\mathfrak{a}, \mathfrak{p}_i^{\sigma}\right)$.

ГЛАВА ТРИНАДЦАТАЯ

ТЕОРИЯ ПОЛИНОМИАЛЬНЫХ ИДЕАЛОВ

В этой главе общая теория идеалов будет применена к (коммутативной) области полиномов. Кроме общей теории, будет предполагаться известной только теория полей (глава пятая).

§ 87. АЛГЕБРАИЧЕСКОЕ МНОГООБРАЗИЕ

Пусть K — коммутативное поле. Последовательность n элементов $\{\xi_1, \ldots, \xi_n\}$ произвольного алгебраического поля расширения K называется *точкой* n-мерного пространства R_n. Точка $\{\xi_1, \ldots, \xi_n\}$ будет коротко обозначаться через ξ; ξ_i называются *координатами* ξ.

Пусть $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$ — область полиномов n переменных $x_1, \ldots, x_n$. Ее элементы, полиномы, будут обозначаться символами $f = f(x) = f(x_1, \ldots, x_n)$, g, h, ... Точка ξ называется *корнем* полинома $f(x)$, если $f(\xi) = f(\xi_1, \ldots, \xi_n) = 0$. Общие корни полиномов $f_1, \ldots, f_r$, т. е. решения системы уравнений

$$f_1(\xi) = 0, \ldots, f_r(\xi) = 0, \tag{1}$$

если только множество решений не пустое, образуют так называемое *алгебраическое многообразие* $\mathfrak{M}$. Известны, например, „алгебраические кривые" на плоскости и „алгебраические поверхности" в пространстве, изображающиеся соответственно уравнениями $f(\xi_1, \xi_2) = 0$ и $f(\xi_1, \xi_2, \xi_3) = 0$, а также „кривые в пространстве", определяющиеся двумя уравнениями, и т. д. Точка ξ с координатами из K также образует алгебраическое многообразие — все пространство R_n.

Как фактически определяются решения (1), было выяснено в одиннадцатой главе. Здесь нас интересует другой вопрос: какие общие теоремы можно высказать относительно алгебраических многообразий и, в частности, как они классифицируются по „измерениям“ на кривые, поверхности и т. д.

Если из „образующих полиномов“ $f_1, \ldots, f_r$ алгебраического многообразия $\mathfrak{M}$ образовать идеал $\mathfrak{a} = (f_1, \ldots, f_r)$, то можно усмотреть, что все точки многообразия (корни $f_1, \ldots, f_r$) являются также корнями полиномов $f = g_1 f_1 + \ldots + g_r f_r$ идеала; поэтому $\mathfrak{M}$ можно также охарактеризовать как совокупность всех общих корней полиномов идеала $\mathfrak{a}$ или, короче выражаясь, *всех корней идеала* $\mathfrak{a}$. То, что $\mathfrak{a}$ обладает конечным базисом, отнюдь не является ограничением, налагаемым на $\mathfrak{a}$, ибо всякий идеал $\mathfrak{o}$ обладает конечным базисом (см. § 80). Итак, *алгебраическое многообразие* $\mathfrak{M}$ *состоит из точек* ξ, *которые являются корнями идеала* $\mathfrak{a}$ *в* $\mathsf{K}[x_1, \ldots, x_n]$. $\mathfrak{M}$ называют *многообразием корней* $\mathfrak{a}$ или, короче, *многообразием* $\mathfrak{a}$.

Идеал, содержащий $\mathfrak{a}$ (делитель $\mathfrak{a}$), определяет часть многообразия $\mathfrak{M}$. Но может случиться, что различные идеалы будут определять одно и то же алгебраическое многообразие $\mathfrak{M}$; например, вместе с $\mathfrak{a}$ также и $\mathfrak{a}^2$ обладает многообразием $\mathfrak{M}$. Но среди всех этих идеалов выделяется один: совокупность *всех* полиномов f, принимающих во всех точках многообразия $\mathfrak{M}$ значение нуль. Эта совокупность содержит все идеалы, которые определяют многообразие $\mathfrak{M}$, и она образует идеал, так как, если f и g исчезают для всех точек $\mathfrak{M}$, то исчезают также кратное f и $f - g$. Многообразие этого идеала есть $\mathfrak{M}$. Такой идеал называется идеалом, *принадлежащим* многообразию.

Если полином f во всех точках многообразия равен нулю, то говорят, что полином f *содержит* многообразие $\mathfrak{M}$ (потому что многообразие $f = 0$ в этом случае содержит многообразие $\mathfrak{M}$). Таким образом идеал, принадлежащий многообразию $\mathfrak{M}$, состоит из всех полиномов, содержащих $\mathfrak{M}$.

Пересечение $\mathfrak{M} \cap \mathfrak{N}$ двух алгебраических многообразий $\mathfrak{M}$ и $\mathfrak{N}$ является, если оно не пустое, также алгебраическим многообразием. А именно, если $\mathfrak{M}$ определяется идеалом $\mathfrak{a} = (f_1, \ldots, f_r)$ и $\mathfrak{N}$ идеалом $\mathfrak{b} = (g_1, \ldots, g_s)$, то пересечение $\mathfrak{M} \cap \mathfrak{N}$, очевидно, есть многообразие, которое определяется идеалом $(\mathfrak{a}, \mathfrak{b}) = (f_1, \ldots, f_r, g_1, \ldots, g_s)$.

Но и *объединение* двух алгебраических многообразий $\mathfrak{M}$, $\mathfrak{N}$ оказывается также алгебраическим многообразием; оно определяется идеалом пересечения (общим наименьшим кратным) $\mathfrak{a} \cap \mathfrak{b}$ (или произведением $\mathfrak{a} \cdot \mathfrak{b}$). Прежде всего ясно, что любая точка объединения является либо корнем всех полиномов из $\mathfrak{a}$, либо корнем всех полиномов из $\mathfrak{b}$; таким образом в каждом случае она будет корнем всех полиномов $\mathfrak{a} \cap \mathfrak{b}$ и, в частности, полиномов $\mathfrak{a} \cdot \mathfrak{b}$. Но если точка ξ не принадлежит объединению $\{\mathfrak{M}, \mathfrak{N}\}$, то существуют в $\mathfrak{a}$ полином f и в $\mathfrak{b}$ полином g, которые в точке ξ не исчезают; но тогда произведение fg, принадлежащее $\mathfrak{a} \cap \mathfrak{b}$ (и $\mathfrak{a} \cdot \mathfrak{b}$), также не исчезает в точке ξ и потому ξ не может быть корнем $\mathfrak{a} \cap \mathfrak{b}$ (или $\mathfrak{a} \cdot \mathfrak{b}$). Итак, корнями $\mathfrak{a} \cap \mathfrak{b}$ (а также $\mathfrak{a} \cdot \mathfrak{b}$) могут быть точки $\{\mathfrak{M}, \mathfrak{N}\}$ и только эти точки.

Отсюда следует, что объединение конечного множества алгебраических многообразий (например, конечного числа точек, кривых и т. д.) также есть алгебраическое многообразие.

Многообразие, которое можно представить в виде объединения двух собственных частей многообразия, называется *сложным* или *приводимым*. Несложное многообразие называется *неразложимым* или *неприводимым*.

Суждение о приводимости многообразия зависит еще от основного поля K. Например, пара точек $\xi_1 = 0$, $\xi_2 = \pm\sqrt{2}$ в рациональном числовом поле образует неприводимое многообразие — многообразие корней идеала $(x_1, x_2^2 - 2)$, которое, однако, после присоединения $\sqrt{2}$ распадается на две составные части (точки).

Известен следующий критерий неприводимости: *многообразие* $\mathfrak{M}$ *тогда и только тогда неприводимо, если принадлежащий идеал является простым, т. е. если из „fg содержит* $\mathfrak{M}$*“ следует: „f или g содержит* $\mathfrak{M}$*“.*

Доказательство. Пусть прежде всего $\mathfrak{M}$ приводимо: $\mathfrak{M} = \mathfrak{M}_1 \vee \mathfrak{M}_2$, где $\mathfrak{M}_1$ и $\mathfrak{M}_2$ — собственные части многообразия $\mathfrak{M}$. В идеале, принадлежащем $\mathfrak{M}_1$, существует полином f, который не содержит $\mathfrak{M}$, так как в противном случае было бы $\mathfrak{M}_1 \supseteq \mathfrak{M}$. Точно так же в идеале, принадлежащем $\mathfrak{M}_2$, имеется полином g, не содержащий $\mathfrak{M}$. Произведение fg содержит $\mathfrak{M}_1$ и $\mathfrak{M}_2$ и потому содержит $\mathfrak{M}$. Таким образом идеал, принадлежащий $\mathfrak{M}$, не может быть простым.

Во-вторых, пусть $\mathfrak{M}$ неприводимо. Если бы произведение fg содержало $\mathfrak{M}$, но f и g не содержали бы $\mathfrak{M}$, то $\mathfrak{M}$ можно было бы представить в виде объединения двух собственных частичных многообразий $\mathfrak{M}_1$ и $\mathfrak{M}_2$, которые определяются следующим образом: $\mathfrak{M}_1$ состоит из точек $\mathfrak{M}$, удовлетворяющих уравнению $f = 0$, а $\mathfrak{M}_2$ — из точек $\mathfrak{M}$, удовлетворяющих уравнению $g = 0$. В таком случае любая точка ξ $\mathfrak{M}$ будет принадлежать $\mathfrak{M}_1$ или $\mathfrak{M}_2$, так как из $f(\xi)\,g(\xi) = 0$ следует, что $f(\xi) = 0$ или $g(\xi) = 0$. Но это противоречит неприводимости $\mathfrak{M}$.

Благодаря связи между простыми идеалами и неприводимыми многообразиями, к которым они принадлежат, получается наглядное представление о многообразии простых идеалов, а отсюда видно, каким образом простой идеал может делиться на другой идеал. Например, на плоскости имеем, исходя из нулевого идеала, принадлежащего многообразию точек всей плоскости, что его делителями являются простые идеалы (f), принадлежащие к неразложимой кривой $f = 0$; затем его делителями будут простые идеалы, принадлежащие точкам (или системам сопряженных точек, если поле K не алгебраически замкнуто), наконец, делителем всех простых идеалов будет единичный идеал, совершенно не имеющий корней.

Что фактически не существует других простых идеалов, кроме идеалов, принадлежащих неприводимым многообразиям, и единичного идеала $\mathfrak{o}$, видно легко из теоремы Гильберта о корнях (§ 75). А именно, на основании этой теоремы имеем: пусть $\mathfrak{p}$ — простой идеал, отличный от единичного, $\mathfrak{M}$ — его многообразие корней. Если полином f всюду исчезает на $\mathfrak{M}$, то из теоремы Гильберта следует $f^\rho \equiv 0\ (\mathfrak{p})$, но отсюда, так как $\mathfrak{p}$ простое, вытекает $f \equiv 0\ (\mathfrak{p})$. Таким образом $\mathfrak{p}$ есть идеал, принадлежащий многообразию, а $\mathfrak{M}$ должно быть неприводимым, так как иначе $\mathfrak{p}$ не было бы простым.

Но мы в ближайших параграфах дадим иное доказательство теоремы о том, что всякий простой идеал, отличный от единичного, принадлежит своему многообразию, а отсюда заново выведем теорему Гильберта о корнях.

Задача 1. Разложить многообразие идеала $(x_1^2 + x_2^2 - 1, x_1^2 - x_3^3 - 1)$ на неприводимые части относительно:

a) рационального числового поля Γ;

b) гауссовского числового поля $\Gamma(i)$;

c) поля всех алгебраических чисел.

В геометрии очень часто переходят от обычного „аффинного" n-мерного пространства R_n к проективному P_n, точки которого определяются $n+1$ однородными координатами $\xi_0, \xi_1, \ldots, \xi_n$, не равными нулю все одновременно. Эти координаты можно умножать на отличный от нуля множитель (см. сноску [2] на стр. 17). Всякой точке $\{\xi_1, \ldots, \xi_n\}$ пространства R_n соответствует точка $\{1, \xi_1, \ldots, \xi_n\}$ проективного пространства P_n; таким образом R_n можно рассматривать как часть P_n, которая дополняется до P_n „несобственной сверхплоскостью" $\xi_0 = 0$.

Любому идеалу $\mathfrak{a}$ из $\mathsf{K}[x_1, \ldots, x_n]$ соответствует идеал $\mathfrak{a}^*$ из $\mathsf{K}[x_0, \ldots, x_n]$, образованный из форм (однородных полиномов) $f(x_0, \ldots, x_n)$, которые при $x_0 = 1$ переходят в полиномы $\mathfrak{a}$. Такой идеал, образованный из однородных полиномов, называется *однородным идеалом* или H-идеалом. В частности $\mathfrak{a}^*$ можно назвать H-идеалом, принадлежащим $\mathfrak{a}$. H-идеалы обладают тем свойством, что если $\{\xi_0, \ldots, \xi_n\}$ — корень, то и $\{\lambda\xi_0, \ldots, \lambda\xi_n\}$ $(\lambda \neq 0)$ — также корень; мы скажем в этом случае, что точка ξ P_n есть корень H-идеала. Эти корни H-идеала в проективном пространстве образуют *многообразие H-идеала в проективном пространстве*.

Для данного многообразия $\mathfrak{M}$ из R_n можно найти в P_n алгебраическое (наименьшее) многообразие $\mathfrak{M}^*$, содержащее $\mathfrak{M}$; для этого достаточно взять идеал $\mathfrak{a}$, принадлежащий $\mathfrak{M}$, и H-идеал $\mathfrak{a}^*$, принадлежащий $\mathfrak{a}$. $\mathfrak{M}^*$ как раз и будет многообразием $\mathfrak{a}^*$ в P_n. Читателю представляется доказать, что $\mathfrak{M}^*$ действительно содержит $\mathfrak{M}$ и является наименьшим многообразием такого рода в P_n, а также доказать, что $\mathfrak{M}$ состоит из таких точек $\mathfrak{M}^*$, которые не лежат на несобственной сверхплоскости.

Если $\mathfrak{M}$ неприводимо, то, очевидно, также неприводимо $\mathfrak{M}^*$.

Задачи. 2. Привести доказательство последнего утверждения.

3. Если полином f принадлежит H-идеалу, то однородные составные части различной степени, на которые аддитивно разлагается f, также принадлежат H-идеалу.

4. Любой H-идеал обладает конечным базисом, состоящим из конечного числа форм.

§ 88. АЛГЕБРАИЧЕСКИЕ ФУНКЦИИ

Рассмотрим, каким образом точки алгебраического многообразия могут быть представлены в виде алгебраических функций от параметров. Для этого необходимо рассмотреть некоторые общие свойства алгебраических функций.

Под *рациональным полем функций* мы подразумеваем поле $\mathsf{K}(t_1, \ldots, t_r)$ рациональных функций от переменных $t_1, \ldots, t_r$. Под *алгебраическим полем функций* мы всегда будем подразумевать алгебраическое расширение рационального поля функций $\mathsf{K}(t_1, \ldots, t_r)$. Элементы такого поля называются *алгебраическими функциями* $t_1, \ldots, t_r$.

Совершенно ясно, что подразумевать под значением рациональной функции $\varphi = \dfrac{f(t_1, \ldots, t_r)}{g(t_1, \ldots, t_r)}$ (f и g — полиномы) для частных значений неизвестных $\tau_1, \ldots, \tau_r$ из поля K: надо для этого в выражении φ заменить t через τ, и, если только $g(\tau_1, \ldots, \tau_r)$ не исчезает, получаем:

$$\varphi(\tau_1, \ldots, \tau_r) = \frac{f(\tau_1, \ldots, \tau_r)}{g(\tau_1, \ldots, \tau_r)}.$$

Значения $\tau_1, \ldots, \tau_r$ могут также принадлежать алгебраическому полю Ω

расширения K; тогда значение φ также будет принадлежать этому полю расширения. Так как Ω обладает бесконечным числом элементов, то в нашем распоряжении имеется для каждого τ_ν бесконечное множество значений; поэтому всегда существуют такие $\tau_1, \ldots, \tau_r$, для которых $g(\tau_1, \ldots, \tau_r) \neq 0$.

Для алгебраических функций понятие значения уже не столь непосредственно очевидно, так как алгебраические функции как элементы поля связаны с неизвестными $t_1, \ldots, t_r$ уравнениями, а не выражаются непосредственно через $t_1, \ldots, t_r$. Если f — функция поля, то f удовлетворяет неприводимому уравнению:

$$a_0(t)f^h + a_1(t)f^{h-1} + \ldots + a_h(t) = 0, \qquad (1)$$

где $a_0, \ldots, a_h$ — рациональные функции $t_1, \ldots, t_r$ (с коэфициентами из K), которые можно, очевидно, считать целыми рациональными и взаимно простыми. Если придадим $t_1, \ldots, t_r$ какие-нибудь значения $\tau_1, \ldots, \tau_r$ из K или из $\Omega \supseteq \mathsf{K}$, то значениями функции будут все корни уравнения (1) в алгебраическом поле расширения при $t = \tau$. Если $a_0(\tau) \neq 0$ или $a_\nu(\tau)$ при $\nu < h$ отлично от нуля, то такие значения всегда существуют. Функция f, вообще говоря, *многозначна*: значению аргумента соответствует несколько значений функции.

Пусть дано несколько функций $f_1, \ldots, f_s$ из какого-нибудь поля функций. Мы будем рассматривать только такие системы значений $\varphi_1, \ldots, \varphi_s$ функций (при $t_1 = \tau_1, \ldots, t_r = \tau_r$ в некотором поле Ω), которые удовлетворяют алгебраическим уравнениям $F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0$ (с коэфициентами из K), имеющим место в поле функций; таким образом для этих значений из $F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0$ следует

$$F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0\ ^1).$$

Отсюда получается, что нельзя комбинировать любые значения многозначной функции f_1 с произвольными значениями $f_2, \ldots, f_s$, так как от этого могут нарушиться соотношения между f. Например, если $f_1 = \sqrt{t}$ и $f_2 = -f_1$, т. е. $f_1^2 = t$, $f_2^2 = t$, то при $\tau = 1$ в нашем распоряжении имеются значения $\varphi_1 = \pm 1$ и $\varphi_2 = \pm 1$, но $\varphi_1 = +1$ нельзя комбинировать с $\varphi_2 = +1$, так как это противоречит условию $f_1 + f_2 = 0$.

Покажем теперь, что в поле Ω всегда существуют (притом бесконечное множество) системы значений $\tau_1, \ldots, \tau_r$ и соответствующие значения $\varphi_1, \ldots, \varphi_s$ функций, которые удовлетворяют упомянутым выше требованиям. Для этой цели напишем неприводимое уравнение относительно f_1 в поле $\mathsf{K}(t_1, \ldots, t_r)$, неприводимое уравнение относительно f_2 в поле $\mathsf{K}(f_1, t_1, \ldots, t_r)$ и т. д. и разделим все уравнения на начальные коэфициенты:

$$\left.\begin{aligned} &f_1^h + a_1(t)\, f_1^{h-1} + \ldots + a_h(t) = 0, \\ &f_2^k + b_1(f_1, t)\, f_2^{k-1} + \ldots + b_k(f_1, t) = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} \qquad (2)$$

---

[1]) Для одной функции f это само собой выполняется, если только значения функции определены на основании (1), так как уравнение $F(f, t_1, \ldots, t_r) = 0$ есть следствие неприводимого уравнения (1).

Коэфициенты второго уравнения суть рациональные функции от f_1 и, так как f_1 — алгебраическая функция, то их можно считать целыми рациональными относительно f_1. Точно так же можно считать коэфициенты третьего уравнения целыми рациональными относительно f_2 и f_1 и т. д. В конце концов во все уравнения знаменателями войдут исключительно полиномы от $t_1, \ldots, t_r$. Пусть $V(t_1, \ldots, t_r)$ — общее кратное всех этих знаменателей, отличное от нуля. Выберем $\tau_1, \ldots, \tau_r$ так, чтобы имело место $V(\tau_1, \ldots, \tau_r) \neq 0$, и определим затем последовательно $\varphi_1, \ldots, \varphi_s$ из уравнений (2) при этих значениях τ:

$$\varphi_1^h + a_1(\tau)\,\varphi_1^{h-1} + \ldots + a_h(\tau) = 0,$$
$$\varphi_2^k + b_1(\varphi_1, \tau)\,\varphi_2^{k-1} + \ldots + b_k(\varphi_1, \tau) = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Мы утверждаем, что найденные $\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_s$ действительно удовлетворяют поставленным требованиям, т. е. что из

$$F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0,$$

где F — полином от $r+s$ неизвестных $u_1, \ldots, u_s, t_1, \ldots, t_r$ с коэфициентами из K следует:

$$F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0.$$

Для полинома F, содержащего только $t_1, \ldots, t_r$, утверждение очевидно. Воспользуемся методом индукции по номеру q входящей в F последней функции f_q. Пусть предложение уже доказано для полинома $F(u_1, \ldots, u_{q-1}, t_1, \ldots, t_r)$.

q-е уравнение из (2) имеет вид:

$$G(f_1, \ldots, f_q, t_1, \ldots, t_r) = f_q^m + d_1(f, t)\,t_q^{m-1} + \ldots + d_m(f, t) = 0$$

где $G(f_1, \ldots, f_{q-1}, u_q, t_1, \ldots, t_r) = G(u_q)$ — неприводимый в $\mathsf{K}(f_1, \ldots, f_{q-1}, t_1, \ldots, t_r)$ полином от переменной u_q. Из $F(f_1, \ldots, f_q, t_1, \ldots, t_r) = 0$ следует, что $F(f_1, \ldots, f_{q-1}, u_q, t_1, \ldots, t_r) = F(u_q)$ делится на $G(u_q)$. При этом можно так распорядиться, чтобы после деления в знаменатели вошли множителями только такие полиномы $t_1, \ldots, t_r$, которые входят и в G. Все эти множители войдут также в $V(t_1, \ldots, t_r)$. Итак, имеем:

$$F(u_q) = G(u_q)\,H(u_q). \tag{3}$$

Сравнивая слева и справа коэфициенты при степенях u_q и умножая на соответствующую степень $V(t_1, \ldots, t_r)$, получим ряд целых рациональных уравнений относительно $f_1, \ldots, f_{q-1}, t_1, \ldots, t_r$. Согласно индуктивному предположению эти уравнения останутся в силе и после замены t через τ и f через φ. Разделив затем снова на соответствующую степень $V(\tau_1, \ldots, \tau_r)$, получим, что уравнение (3) сохранится в силе и после замены t через τ и f через φ. Если еще заменим u_q через φ_q, то первый множитель правой части станет равным нулю, и

$$F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0,$$

что и требовалось доказать.

Мы здесь не будем разбирать различных методов определения $\varphi_1, \ldots, \varphi_s$ для таких $\tau_1, \ldots, \tau_r$, которые не удовлетворяют условию $V(\tau_1, \ldots, \tau_r) \neq 0$.

Эти значения можно получить предельным переходом, а также разложением в ряд в окрестности особых точек и т. д. Мы оставим в стороне также введение символа ∞, которое полезно для тех случаев, когда не существует конечных значений $\varphi_1, \ldots, \varphi_s$. Читателя, интересующегося подробностями, мы отсылаем к литературе по теории алгебраических функций [1]). Ниже окажется полезной следующая теорема, которая является в известном смысле обращением вышеизложенного:

Если соотношение $F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0$ *удовлетворяется для всех допустимых значений аргументов* τ *и соответствующих им значений функций, то в поле функций также удовлетворяется уравнение* $F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0$.

Доказательство. Если бы имело место $F(f_1, \ldots, f_s, t_1, \ldots, t_r) \neq 0$, то можно было бы составить функцию

$$f_{s+1} = \frac{1}{F(f_1, \ldots, f_s, t_1, \ldots, t_r)}$$

и установить для $f_1, \ldots, f_s, f_{s+1}$ допустимую систему значений $\varphi_1, \ldots, \varphi_s, \varphi_{s+1}, \tau_1, \ldots, \tau_r$. Соотношение

$$1 = f_{s+1} \cdot F(f_1, \ldots, f_s, t_1, \ldots, t_r)$$

должно оставаться в силе и при $f_\nu \to \varphi_\nu$, $t_\lambda \to \tau_\lambda$. Но по предположению $F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0$, откуда

$$1 = 0,$$

что нелепо.

§ 89. ПАРАМЕТРИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ АЛГЕБРАИЧЕСКИХ МНОГООБРАЗИЙ

Если $\xi_1, \ldots, \xi_n$ — алгебраические функции $t_1, \ldots, t_r$, то для частных допустимых значений $\tau_1, \ldots, \tau_r$ аргументов соответствующие значения $\xi_1', \ldots, \xi_n'$ всякий раз определяют точку ξ' в R_n, причем эти точки могут заполнить все многообразие или часть многообразия. Мы будем тогда говорить о *параметрическом представлении* многообразия алгебраическими функциями $\xi_1, \ldots, \xi_n$ параметров $t_1, \ldots, t_r$.

Например, точки плоскости R_2

$$\xi_1 = \frac{1 - t^2}{1 + t^2}, \quad \xi_2 = \frac{2t}{1 + t^2} \tag{1}$$

удовлетворяют уравнению

$$\xi_1^2 + \xi_2^2 = 1. \tag{2}$$

Но не все точки окружности (2) могут быть представлены уравнениями (1), так как, например, точка $(-1, 0)$ удовлетворяет уравнению (2), а выражение $\frac{1 - t^2}{1 + t^2}$ никак не может быть сделано равным -1.

---

[1]) См., например, Jordan, Cours d'analyse, изд. 3, т. 2, стр. 622—693, 1913 Hurwitz-Courant, Funktionentheorie, изд. 3, стр. 480—527, 1929; случай многих переменных см. B. L. v. d. Waerden, Zur Produktzerlegung der Ideale in ganz abgeschlossenen Ringen, „Math. Ann.", т. 101, стр. 293—308, § 8, 1929.

Таким образом может оказаться, что не все точки многообразия определяются параметрическим представлением. Но мы можем всегда взять наименьшее многообразие, содержащее точки ξ' параметрического представления.

Алгебраическое многообразие, содержащее точки ξ', определяется уравнениями $f=0$, которым удовлетворяют все точки ξ'. Чтобы получить наименьшее среди таких алгебраических многообразий, надо взять *все* уравнения $f=0$, удовлетворяющиеся точками ξ'.

Полиномы $f(x_1, \ldots, x_n)$, которые во всех точках ξ' обращаются в нуль, можно согласно § 88 охарактеризовать также тем, что для них имеет место в поле функций $\mathsf{K}(\xi_1, \ldots, \xi_n)$ уравнение $f(\xi)=0$. Эти полиномы образуют идеал в области полиномов $\mathfrak{o}=\mathsf{K}[x_1, \ldots, x_n]$. Идеал будет даже простым, так как из $f(\xi)\cdot g(\xi)=0$ следует в поле функций, что $f(\xi)=0$ или $g(\xi)=0$. Корни этого простого идеала $\mathfrak{p}$ образуют, как мы уже видели выше, наименьшее алгебраическое многообразие, содержащее все точки параметрического представления. Назовем такое многообразие $\mathfrak{M}$ *алгебраическим многообразием параметрических функций* $\xi_1, \ldots, \xi_n$.

Соответствие

$$f(x) \to f(\xi)$$

или

$$\sum \alpha_\lambda x_1^{\lambda_1} \ldots x_n^{\lambda} \to \sum \alpha_\lambda \xi_1^{\lambda_1} \ldots \xi_n^{\lambda_n}$$

определяет гомоморфное отображение $\mathfrak{o}=\mathsf{K}[x]$ на кольцо $\mathsf{K}[\xi]$. Полином f, переходящий в нуль, порождает идеал $\mathfrak{p}$. Согласно теореме о гомоморфизмах

$$\mathsf{K}[\xi] \cong \frac{\mathfrak{o}}{\mathfrak{p}}. \tag{3}$$

Отсюда снова усматриваем, что $\mathfrak{p}$ должно быть простым идеалом.

Определение идеала $\mathfrak{p}$, а тем самым также многообразия $\mathfrak{M}$, зависит не от выбора независимых переменных $t_1, \ldots, t_r$, функциями которых являются $\xi_1, \ldots, \xi_n$, а исключительно от алгебраических свойств элементов ξ поля. Обратно, согласно (3) алгебраические свойства ξ вполне определяются идеалом $\mathfrak{p}$. Поле, к которому принадлежат ξ, есть поле отношений кольца $\mathsf{K}[\xi]$ и потому изоморфно полю отношений $\frac{\mathfrak{o}}{\mathfrak{p}}$.

Простой идеал $\mathfrak{p}$ *принадлежит многообразию* $\mathfrak{M}$. В самом деле, если полином f исчезает всюду на $\mathfrak{M}$, то, в частности, $f(\xi')=0$ для всех точек ξ' параметрического представления, а отсюда следует, что $f \equiv 0 (\mathfrak{p})$. Так как $\mathfrak{p}$ простое, то согласно § 87 $\mathfrak{M}$ неприводимо в поле K. Итак, n алгебраических функций $\xi_1, \ldots, \xi_n$ определяют собой неприводимое алгебраическое многообразие в параметрическом представлении.

Функции $\frac{f(\xi_1, \ldots, \xi_n)}{g(\xi_1, \ldots, \xi_n)}$ поля $\mathsf{K}(\xi)$ во всех точках ξ' многообразия $\mathfrak{M}$, в которых знаменатель $g(\xi')$ не обращается в нуль, принимают определенные значения $\frac{f(\xi')}{g(\xi')}$. Две функции $\frac{f(\xi)}{g(\xi)}$ и $\frac{f_1(\xi)}{g_1(\xi)}$ тогда и только тогда

равны в поле $K(\xi)$, если их значения $\frac{f(\xi')}{g(\xi')}$ и $\frac{f_1(\xi')}{g_1(\xi')}$ равны во всех точках ξ', для которых $g(\xi')$ и $g_1(\xi')$ не равны нулю, так как из

$$f(\xi)g_1(\xi) = f_1(\xi)g(\xi)$$

следует:

$$f(\xi')g_1(\xi') = f_1(\xi')g(\xi')$$

для всех ξ', и обратно. Поэтому можно функции поля $K(\xi)$ рассматривать как *функции многообразия* $\mathfrak{M}$.

Величины $\xi_1, \ldots, \xi_n$ можно также рассматривать как координаты „точки" ξ, а именно такой точки, координаты которой уже не постоянные, взятые из алгебраического расширения поля K, а функции из трансцендентного расширения. Точка ξ называется *общей точкой* многообразия $\mathfrak{M}$, потому что из нее получается при частных значениях параметров обычная точка $\xi' \mathfrak{M}$ (причем все уравнения $f(\xi) = 0$ остаются в силе). ξ называется также *общим корнем* $\mathfrak{p}$ на основании следующего определения: ξ *называется общим корнем* $\mathfrak{p}$, *если из* $f(\xi) = 0$ *следует* $f \equiv 0\,(\mathfrak{p})$, *и обратно, для любого* f *из* $K[x]$.

Мы видели, что ко всякой системе функций $\xi_1, \ldots, \xi_n$ принадлежит простой идеал с общим корнем ξ. Посмотрим, будет ли для любого простого идеала $\mathfrak{p}$ существовать общий корень. При этом, очевидно, следует исключить случай $\mathfrak{p} = \mathfrak{o}$, так как единичный идеал $\mathfrak{o}$ вообще не имеет корней. Мы утверждаем, что *любой простой идеал* $\mathfrak{p} \neq \mathfrak{o}$ *имеет общий корень.*

Для доказательства возьмем прежде всего кольцо $\bar{\mathfrak{o}} = \frac{\mathfrak{o}}{\mathfrak{p}}$ вычетов по $\mathfrak{p}$. В силу гомоморфизма $\mathfrak{o} \sim \bar{\mathfrak{o}}$ полиному f соответствует класс вычетов $\bar{f}$; в частности, постоянной α соответствует класс вычетов $\bar{\alpha}$. Разным постоянным соответствуют разные классы, так как если $\bar{\alpha} = \bar{\beta}$ и $\alpha \neq \beta$, то $\alpha \equiv \beta\,(\mathfrak{p})$, откуда $\alpha - \beta = \gamma$ и $\gamma\gamma^{-1} = 1$ содержатся в $\mathfrak{p}$, т. е. $\mathfrak{p}$ — единичный идеал, что противоречит предположению. Итак, поле K постоянных α изоморфно отображается на поле $\bar{K}$, состоящее из образов $\bar{\alpha}$ этих постоянных. Согласно § 11 (см. конец) можно построить кольцо $\mathfrak{o}^*$, изоморфное $\bar{\mathfrak{o}}$ и содержащее K; для этого следует заменить элементы из $\bar{K}$ соответствующими элементами из K. $\mathfrak{o}^*$ опять-таки гомоморфный образ $\mathfrak{o}$, и при гомоморфном отображении $\mathfrak{o} \to \mathfrak{o}^*$ постоянные будут соответствовать самим себе. Переменным $x_1, \ldots, x_n$ соответствуют некоторые величины из $\mathfrak{o}^*$, которые мы обозначим через $\xi_1, \ldots, \xi_n$. Полиному $f(x) = \sum \alpha_\lambda x_1^{\lambda_1} \ldots x_n^{\lambda_n}$ соответствует выражение $f(\xi) = \sum \alpha_\lambda \xi_1^{\lambda_1} \ldots \xi_n^{\lambda_n}$. Таким образом $\mathfrak{o}^* = K[\xi_1, \ldots, \xi_n]$, и мы нашли изоморфизм (3).

Кольцо $K[\xi]$ можно заключить в поле отношений $K(\xi_1, \ldots, \xi_n)$. Таким образом ξ суть элементы поля функций. Из $f^* = f(\xi) = 0$ всегда следует $f = f(x) \equiv 0\,(\mathfrak{p})$, и обратно, в силу чего ξ есть общий корень идеала $\mathfrak{p}$, что и требовалось доказать.

Все доказанное можно объединить в следующую схему:

общий корень ξ

$\downarrow\uparrow$

простой идеал $\mathfrak{p} \neq \mathfrak{o}$

$\downarrow\uparrow$

неприводимое многообразие $\mathfrak{M}$.

В начале этого параграфа мы исходили из произвольного общего корня ξ (системы n алгебраических функций) и для него строили простой идеал $\mathfrak{p}$ и многообразие $\mathfrak{M}$. Но $\mathfrak{p}$ также было идеалом, принадлежащим $\mathfrak{M}$, и $\mathfrak{p}$ определяло общий корень ξ однозначно с точностью до изоморфизма; таким образом цепь выводов можно обратить. В заключение мы доказали, что всякое $\mathfrak{p} \neq \mathfrak{o}$ имеет общий корень ξ. Так как для всякого произвольного алгебраического многообразия существует простой идеал $\mathfrak{p}$, принадлежащий многообразию, то все соотношения, отмеченные в схеме стрелками, *взаимно однозначны*. В частности, отсюда вытекает, что *всякое неприводимое многообразие допускает параметрическое представление через алгебраические функции* $\xi_1, \ldots, \xi_n$ (а именно, можно всегда рассматривать некоторые ξ как алгебраические функции остальных ξ) и, наконец, что *любой простой идеал* $\mathfrak{p} \neq \mathfrak{o}$ *принадлежит многообразию своих корней*. Единственным идеалом без корней является $\mathfrak{o}$. Поэтому этот идеал также вполне определяется своими корнями.

Задачи. 1. Идеал

$$(x_1x_3 - x_2^2,\ x_2x_3 - x_1^3,\ x_3^2 - x_1^2x_2)$$

в $K[x_1, x_2, x_3]$ является простым, так как он имеет общий корень

$$\{t^3,\ t^4,\ t^5\}.$$

2. Идеал

$$(x_1^2 + x_2^2 - x_3^2,\ x_1^2 - x_2^2 + 1)$$

в $K[x_1, x_2, x_3]$ является простым и имеет общий корень

$$\left\{\frac{1-t^2}{2t},\ \frac{1+t^2}{2t},\ \frac{\sqrt{2(1+t^2)}}{2t}\right\}.$$

3. Идеал

$$(x_1x_4 - x_2x_3,\ x_2^3 - x_1^2x_3,\ x_3^3 - x_2x_4^2,\ x_2^2x_4 - x_1x_3^2)$$

в $K[x_1, x_2, x_3, x_4]$ является простым и имеет общий корень

$$\{t_1^4,\ t_1^3t_2,\ t_1t_2^3,\ t_2^4\}.$$

4. Если $\mathfrak{p}$ — простой идеал в $K[x_1, \ldots, x_n]$ и имеет общий корень $\{\xi_1, \ldots, \xi_n\}$, то соответствующий в $K[x_0, \ldots, x_n]$ H-идеал $\mathfrak{p}^*$ (см. конец § 87) является простым и обладает общим корнем $\{\lambda, \lambda\xi_1, \ldots, \lambda\xi_n\}$, где λ — переменная величина.

§ 90. ЧИСЛО ИЗМЕРЕНИЙ

Пусть $\xi_1, \ldots, \xi_n$ — алгебраические функции от $t_1, \ldots, t_r$. Тогда степень трансцендентности s системы $\{\xi_1, \ldots, \xi_n\}$ (см. § 62) меньше или равна r. Она равна r в том случае, когда, обратно, $t_1, \ldots, t_r$ также

алгебраически зависят от ξ; в частности, $s=r$, когда t принадлежит полю $\mathsf{K}(\xi_1, \ldots, \xi_n)$. Еще более частный случай тот, когда для $t_1, \ldots, t_r$ среди ξ существует $r=s$ алгебраически независимых функций. Если число r параметров больше степени трансцендентности s, то будем иметь *„лишние параметры"*. Наименьшее число параметров, с которыми можно обойтись, равно s. Это число называется числом *измерений многообразия* $\mathfrak{M}$ или *числом измерений простого идеала* $\mathfrak{p}$, принадлежащего $\mathfrak{M}$. Таким образом число измерений простого идеала, отличного от единичного, совпадает со степенью трансцендентности его общего корня ξ.

Очевидно, что число измерений простого идеала $\mathfrak{p} \neq \mathfrak{o}$ может принимать значения от 0 до n. Единичному идеалу, не имеющему корней, мы припишем число измерений, равное -1.

Если ξ — общий корень простого идеала $\mathfrak{p}$, ξ' — произвольный корень того же идеала, то можно каждому полиному $f(\xi)$ из $\mathsf{K}[\xi]$ сопоставить полином $f(\xi')$ из $\mathsf{K}[\xi']$. Так как из $f(\xi)=g(\xi)$ следует $f(x) \equiv g(x)\,(\mathfrak{p})$, и отсюда $f(\xi')=g(\xi')$, то соответствие $f(\xi) \to f(\xi')$ однозначно. Так как при этом соответствии, очевидно, сумма переходит в сумму, а произведение — в произведение, то получаем гомоморфизм

$$\mathsf{K}[\xi] \sim \mathsf{K}[\xi']. \tag{1}$$

Если соответствие есть изоморфизм, то ξ' — также общий корень $\mathfrak{p}$, и обратно.

В случае идеала $\mathfrak{p}$ нулевого измерения все величины ξ должны быть алгебраическими относительно K; следовательно, все рациональные функции ξ необходимо должны быть целыми рациональными: $\mathsf{K}(\xi)=\mathsf{K}[\xi]$. Таким образом $\mathsf{K}[\xi]$ есть *поле*. Если затем ξ — опять произвольный корень, то гомоморфизм (1) необходимо должен быть изоморфизмом, так как для поля существует только взаимно однозначный гомоморфизм и отображение на нулевое кольцо. В итоге получается следующая теорема:

В случае простого идеала нулевого измерения все корни являются общими и друг с другом эквивалентны [1]).

Координаты $\xi_1, \ldots, \xi_n$ или $\xi'_1, \ldots, \xi'_n$ в этом случае являются алгебраическими величинами (так как степень трансцендентности равна нулю). Если считать, что все корни лежат в одном и том же (например алгебраически замкнутом) поле Ω, то в силу (1) они будут алгебраически сопряженными. Число этих сопряженных точек в подходящем поле Ω меньше или равно [и, если $\mathsf{K}(\xi)$ первого рода, в точности равно] степени поля $\mathsf{K}(\xi)$ относительно K. Итак:

Неприводимое алгебраическое многообразие нулевого измерения состоит из конечного числа алгебраически сопряженных точек.

В частности, если само K алгебраически замкнуто, то существует только один корень ξ из самого поля K, и принадлежащим ему идеалом является

$$\mathfrak{p}=(x_1-\xi_1, \ldots, x_n-\xi_n).$$

---

[1]) Т. е. при изоморфизме они переходят друг в друга, причем основное поле K остается неподвижным.

Теорема. *Степень трансцендентности корня r-мерного простого идеала меньше или равна r; если же степень трансцендентности корня равна r, то корень является общим.*

Доказательство. Если ξ' — корень, у которого степень трансцендентности равна s, то имеет место гомоморфизм (1). Если $\xi'_1, \ldots, \xi'_s$ алгебраически независимы, то $\xi_1, \ldots, \xi_s$ также алгебраически независимы, так как из всякого алгебраического соотношения между ξ необходимо следует такое же соотношение между ξ'. Отсюда следует, что $r \geqslant s$. Если $r = s$, то все ξ алгебраически зависят от $\xi_1, \ldots, \xi_s$. Если при гомоморфизме (1) полином $f(\xi)$, отличный от нуля, переходит в нуль, то в поле $\mathsf{K}(\xi)$ элемент $\frac{1}{f}$ может быть записан следующим образом:

$$\frac{1}{f(\xi_1, \ldots, \xi_n)} = \frac{g(\xi_1, \ldots, \xi_n)}{h(\xi_1, \ldots, \xi_s)}.$$

Но отсюда следует, что

$$h(\xi_1, \ldots, \xi_s) = g(\xi_1, \ldots, \xi_n) f(\xi_1, \ldots, \xi_n).$$

При гомоморфизме (1) f переходит в 0; следовательно, и $h(\xi_1, \ldots, \xi_s)$ также должно переходить в 0, т. е.

$$h(\xi'_1, \ldots, \xi'_s) = 0,$$

что противоречит алгебраической независимости $\xi'_1, \ldots, \xi'_s$. Таким образом при гомоморфизме (1) отличный от нуля полином не может перейти в нуль; итак, (1) в случае $r = s$ является изоморфизмом. Отсюда сразу вытекает, что ξ' — общий корень.

Любой корень ξ' идеала $\mathfrak{p}$ можно рассматривать как общий корень некоторого идеала $\mathfrak{p}'$. Но тогда из $f \equiv 0 (\mathfrak{p})$ следует $f(\xi') = 0$ или $f \equiv 0 (\mathfrak{p}')$; отсюда видно, что $\mathfrak{p}'$ есть делитель $\mathfrak{p}$. Обратно, таким образом может быть получен любой простой делитель $\mathfrak{p}'$ идеала $\mathfrak{p}$, отличный от $\mathfrak{o}$, так как всякий идеал $\mathfrak{p}' \neq \mathfrak{o}$ обладает общим корнем ξ'. Из вышеприведенной теоремы непосредственно вытекает такое предложение:

Всякий делитель $\mathfrak{p}'$ идеала $\mathfrak{p}$ имеет измерение $r' \leqslant r$; если $r' = r$, то $\mathfrak{p}' = \mathfrak{p}$.

Под измерением произвольного алгебраического многообразия мы подразумеваем максимальное число среди измерений его составных неприводимых частей. Одномерные алгебраические многообразия называются *кривыми*, двумерные — *поверхностями*, а многообразия $n-1$ измерения — *сверхповерхностями*. Единственным n-мерным многообразием в R_n является все пространство R_n; этому многообразию принадлежит нулевой идеал [так как, если $\xi_1, \ldots, \xi_n$ алгебраически независимы, то из $f(\xi) = 0$ следует, что $f = 0$].

Задачи. 1. Главный идеал (p), где p — неразложимый полином, отличный от постоянной, является $(n-1)$-мерным простым идеалом.

2. Обратно, всякий $(n-1)$-мерный простой идеал есть главный идеал.

3. Всякий d-мерный простой идеал $\mathfrak{p}$ ($d > 0$) допускает по крайней мере один $(d-1)$-мерный простой делитель. (Если $\xi_{d+1}, \ldots, \xi_n$ — алгебраические функции $\xi_1, \ldots, \xi_d$, то берем согласно § 88 частный корень $\mathfrak{p}$, придавая ξ_d частное значение и оставляя $\xi_1, \ldots, \xi_{d-1}$ неопределенными).

Если перейти от открытого пространства R_n к проективному пространству P_n, то согласно § 87 неприводимому многообразию $\mathfrak{M}$ из R_n (с принадлежащим простым идеалом $\mathfrak{p}$) будет отвечать такое же многообразие $\mathfrak{M}^*$ в P_n (с принадлежащим ему простым идеалом $\mathfrak{p}^*$). Если d — измерение $\mathfrak{p}$, то измерение $\mathfrak{p}^*$ равно $d+1$, так как неопределенный множитель пропорциональности λ увеличивает на единицу степень трансцендентности общего корня (см. § 89, задача 4). Однако $\mathfrak{M}^*$ принимается d-мерным [а не $(d+1)$-мерным] на том геометрическом основании, что $\mathfrak{M}^*$ совпадает с $\mathfrak{M}$, если исключить несобственные точки. Например, если $\mathfrak{M}$ — кривая, то образ $\mathfrak{M}^*$, получающийся из $\mathfrak{M}$ присоединением конечного числа точек, также называется кривой. Таким образом под измерением многообразия в проективном пространстве всегда подразумевается измерение принадлежащего ему простого идеала, уменьшенное на единицу.

§ 91. ПРИМАРНЫЙ ИДЕАЛ

Основная задача теории полиномиальных идеалов состоит в том, *чтобы обнаружить, когда полином f принадлежит данному идеалу*

$$\mathfrak{m} = (f_1, \ldots, f_r).$$

При этом под решением задачи здесь подразумевается не численное решение, состоящее из конечного числа операций [1]), а способ, который исключительно базируется на структуре идеала и на геометрических соотношениях между корнями идеала и его элементами f. Такой способ впервые был предложен Э. Ласкером [2]); он связан с разложением идеала на примарные компоненты.

В основном ласкеровский метод состоит в следующем: согласно теореме разложения § 83 идеал $\mathfrak{m}$ можно представить как пересечение примарных идеалов:

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s].$$

Отсюда, чтобы полином f принадлежал идеалу $\mathfrak{m}$, необходимо и достаточно, чтобы f принадлежал всем примарным идеалам $\mathfrak{q}_\nu$. Таким образом надо установить условия, которым должен удовлетворять полином, чтобы принадлежать примарному идеалу.

Согласно § 82 примарному идеалу $\mathfrak{q}$ соответствует простой идеал $\mathfrak{p}$ и „показатель“ ρ, обладающие следующими свойствами:

1. $\mathfrak{p}^\rho \equiv 0\,(\mathfrak{q}) \equiv 0\,(\mathfrak{p})$.

2. Из $fg \equiv 0\,(\mathfrak{q})$ и $f \not\equiv 0\,(\mathfrak{p})$ следует $g \equiv 0\,(\mathfrak{q})$. В случае $\mathfrak{q} \neq \mathfrak{o}$ простой идеал $\mathfrak{p}$ принадлежит неприводимому многообразию $\mathfrak{M}$. В силу 1 все корни $\mathfrak{q}$ являются также корнями $\mathfrak{p}$, и обратно. Таким образом *многообразие примарного идеала $\mathfrak{q} \neq \mathfrak{o}$ неприводимо и совпадает с многообразием соответствующего простого идеала.*

Отсюда в силу теоремы о разложении вытекает, что многообразие идеала $\mathfrak{m}$ есть объединение неприводимых многообразий, а именно многообразий его примарных компонентов. Следовательно:

Всякое алгебраическое многообразие может быть представлено в виде объединения конечного числа неприводимых многообразий.

---

[1]) См. J. König, Einleitung in die allgemeine Theorie der algebraischen Grössen (B. G. Teubner, Leipzig 1903), а также G. Hermann, Die Frage der endlichvielen Schritte in der Theorie der Polynomideale, Math. Ann.“, т. 95, стр. 736–788.

[2]) E. Lasker, Zur Theorie der Moduln und Ideale, „Math. Ann.“, т. 60, стр. 20—116, 1905.

Неприводимые многообразия примарных компонентов $\mathfrak{m}$ вполне определяются принадлежащими им простыми идеалами.

При этом „окутанные" простые идеалы (§ 84) могут быть откинуты, так как соответствующие им многообразия содержатся в многообразиях неокутанных („изолированных") простых идеалов. Так как простые идеалы в их совокупности определяются однозначно, то имеем, что *разложение алгебраического многообразия на неприводимые также определяется однозначно.*

Пусть $\mathfrak{q}$ — примарный идеал для простого идеала $\mathfrak{p}$ с показателем ρ, а $\mathfrak{M}$ — пусть его многообразие. Если f есть полином, содержащий $\mathfrak{M}$, то $f \equiv 0\,(\mathfrak{p})$, откуда $f^{\rho} \equiv 0\,(\mathfrak{q})$. Но если f не содержит $\mathfrak{M}$, то в силу приведенного выше свойства 2 во всяком сравнении по модулю $\mathfrak{q}$ можно опустить множитель f. С помощью этих двух критериев часто удается обнаружить справедливость сравнения $f^{\rho} \equiv 0\,(\mathfrak{q})$ или $g \equiv 0\,(\mathfrak{q})$. Первое сравнение на основании теоремы о разложении сразу может быть распространено на любой идеал $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$. А именно, если f — полином, содержащий многообразие $\mathfrak{M}$ идеала $\mathfrak{m}$, а ρ — наибольший из показателей примарных идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, то

$$f^{\rho} \equiv 0\,(\mathfrak{q}_i) \qquad (\text{для } i = 1, \ldots, s),$$

откуда

$$f^{\rho} \equiv 0\,(\mathfrak{m}).$$

Тем самым снова доказана *теорема Гильберта о корнях* (§ 75), и притом с тем уточнением, что показатель ρ зависит только от идеала $\mathfrak{m}$.

С другой стороны, если f — полином, который не содержит ни одного из многообразий примарных идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, то всякое сравнение вида

$$fg \equiv 0\,(\mathfrak{m})$$

можно сократить на f, откуда

$$g \equiv 0\,(\mathfrak{m}).$$

Иными словами,

$$\mathfrak{m} : (f) = \mathfrak{m}.$$

Это равенство (§ 84) возможно только тогда, когда f не делится на простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, принадлежащие $\mathfrak{m}$ (т. е. не содержит их неприводимых многообразий). Вообще равенство

$$\mathfrak{m} : \mathfrak{a} = \mathfrak{m} \tag{1}$$

для произвольного идеала $\mathfrak{a}$ справедливо только тогда (см. § 84), *когда* $\mathfrak{a}$ *не делится на* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ или, что одно и то же, *если многообразие* $\mathfrak{a}$ *не содержит ни одного из многообразий простых идеалов* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Эта теорема часто оказывается полезной при нахождении простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, принадлежащих заданному идеалу $\mathfrak{m}$. А именно, пусть требуется установить, является ли простой идеал $\mathfrak{p}$ равным одному из $\mathfrak{p}_\nu$; для этого берут идеал $\mathfrak{a}$, делящийся на $\mathfrak{p}$, например $\mathfrak{a} = \mathfrak{p}$, и смотрят, имеет ли место (1) или его отрицание, т. е. смотрят, будет ли из $g\mathfrak{a} \equiv 0\,(\mathfrak{m})$ следовать $g \equiv 0\,(\mathfrak{m})$ или $g \not\equiv 0\,(\mathfrak{m})$. Если оказывается справедливым (1), то $\mathfrak{p}$ не может быть равным $\mathfrak{p}_\nu$. Этим мето-

дом мы, например, в § 95 докажем, что простые идеалы, принадлежащие идеалу с базисом из r элементов, имеют все измерение $n-r$, если измерения последних не превосходят числа $n-r$.

Под *числом измерений* (или просто измерением) примарного идеала подразумевается измерение соответствующего простого идеала (или измерение многообразия корней). Под измерением или *наивысшим измерением* идеала $\mathfrak{a} \neq \mathfrak{o}$ подразумевается наибольшее из измерений примарных компонентов (или соответствующих простых идеалов). Это число представляет также измерение многообразия $\mathfrak{a}$.

Если измерения всех примарных идеалов, принадлежащих $\mathfrak{a}$, равны, например равны d, то идеал $\mathfrak{a}$ называется *не смешанным идеалом измерения* d.

Задачи. 1. Идеал $(x_1^2,\ x_2x_3+1)$ примарен и имеет показатель 2, и принадлежащий ему простой идеал равен $(x_1,\ x_2x_3+1)$.

2. Степень p^ρ неразложимого полинома p, отличного от постоянной, порождает $(n-1)$-мерный примарный идеал.

Полином f, отличный от постоянной, порождает не смешанный $(n-1)$-мерный идеал.

3. Если $\mathfrak{p}$ — простой идеал задачи 1, § 89, то $\mathfrak{p}^2$ не примарно. [Полином $(x_2x_3-x_1^3)^2-(x_2^2-x_1x_3)(x_3^2-x_1^2x_2)$ делится на x_1, а другой делитель не принадлежит к $\mathfrak{p}^2$.]

§ 92. ТЕОРЕМА НЁТЕРА

В предыдущем параграфе рассматривалась следующая задача:

Каким условиям должен удовлетворять полином f, чтобы он мог принадлежать идеалу $\mathfrak{m}$?

Здесь мы с помощью разложения на примарные идеалы решим эту задачу полностью для случая идеала нулевого измерения. Прежде всего приведем такую лемму:

Если Σ — *поле расширения* K *и* $f, f_1, \ldots, f_r$ — *полиномы из* $\mathsf{K}[x] = \mathsf{K}[x_1, \ldots, x_n]$, *то из*

$$f \equiv 0\,(f_1, \ldots, f_r) \text{ в } \sum[x]$$

следует:

$$f \equiv 0\,(f_1, \ldots, f_r) \text{ в } \mathsf{K}[x].$$

Доказательство. Пусть

$$f = \sum g_i f_i, \tag{1}$$

где g_i — полиномы с коэфициентами из Σ. Эти коэфициенты выразим линейно через конечное число линейно независимых элементов $1, \omega_1, \omega_2, \ldots$ поля Σ. Тогда каждый член g_if_i суммы (1) примет вид:

$$(g_{i0}+g_{i1}\omega_1+g_{i2}\omega_2+\ldots)f_i,$$

где g_{ik} — полином с коэфициентами из K. Таким образом из (1) получается:

$$f = \sum g_{i0}f_i + \omega_1 \sum g_{i1}f_i + \omega_2 \sum g_{i2}f_i + \ldots;$$

но так как элементы поля $1, \omega_1, \omega_2, \ldots$ линейно независимы, то члены справа и слева совпадают, откуда

$$f = \sum g_{i0} f_i,$$

что и требовалось доказать.

Теперь, чтобы ответить на вопрос — когда $f \equiv 0\,(f_1, \ldots, f_r)$, расширим произвольно поле K, например присоединим корни идеала $(f_1, \ldots, f_r)$. Если рассматриваемое сравнение справедливо в расширенной области $\Sigma\,[x]$, то оно должно быть также справедливым до расширения.

При соответствующем расширении основного поля алгебраическое многообразие нулевого измерения распадается исключительно на отдельные точки; таким образом в случае надобности мы всегда можем предположить, что каждый из рассматриваемых простых идеалов нулевого измерения имеет корнем только одну из точек (а не систему сопряженных точек).

Простой идеал $\mathfrak{p}$ нулевого измерения свободен от делителей, так как кольцо вычетов $\frac{\mathfrak{o}}{\mathfrak{p}}$ согласно § 90 образует поле. Отсюда следует, что примарный идеал нулевого измерения единообразен, так как примарный идеал согласно § 86 всегда единообразен, если его простой идеал свободен от делителей. Далее, из теорем § 86 следует, что всякий изолированный примарный компонент $\mathfrak{q}$ нулевого измерения идеала $\mathfrak{m}$ представляется в виде

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^{\rho}). \tag{2}$$

При этом показатель ρ есть наименьшее число σ, для которого

$$\mathfrak{p}^{\sigma} \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\sigma+1}). \tag{3}$$

Смысл равенства (2) станет еще более ясным, если основное поле предварительно расширить так, чтобы рассматриваемый однородный идеал $\mathfrak{q}$ имел только один корень $a = \{a_1, \ldots, a_n\}$. Равенство (2) показывает, что для $f \equiv 0\,(\mathfrak{q})$ необходимо и достаточно, чтобы

$$f \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\rho}). \tag{4}$$

Если $\mathfrak{m} = (f_1, \ldots, f_r)$ и $y_\nu = x_\nu - a_\nu$, то $\mathfrak{p} = (y_1, \ldots, y_n)$. Располагая все полиномы по восходящим степеням y_ν, получим, что $\mathfrak{p}^{\rho}$ состоит из полиномов, содержащих только произведения y_ν со степенью большей или равной ρ. Таким образом сравнение (4) говорит о том, что f совпадает с линейной комбинацией $\sum g_\nu f_\nu$ с точностью до членов степени ρ и выше. Умножим $f_1, \ldots, f_r$ на 1 и на все произведения y_ν степени меньшей ρ и в полученных полиномах откинем все члены со степенью большей или равной ρ. Обозначим полученные таким образом полиномы через $h_1, \ldots, h_k$. Тогда сравнение (4) означает, что f равно линейной комбинации от $h_1, \ldots, h_k$ с постоянными коэфициентами с точностью до членов степени большей или равной ρ. В частности, (4) наверное удовлетворяется, если

$$f = P_1 f_1 + \ldots + P_r f_r, \tag{5}$$

где $P_1(y), \ldots, P_r(y)$ — формальные степенные ряды [1]). В самом деле,

[1]) Относительно сходимости этих рядов мы, конечно, ничего не предполагаем.

тогда можно для каждого значения σ эти степенные ряды оборвать на членах степени σ и констатировать совпадение обеих частей по модулю $\mathfrak{p}^\sigma$. Собственно говоря, в критерии (5) требуется несколько более, чем надо: достаточно было потребовать, чтобы обе части (5) совпадали с точностью до членов степеней больших или равных ρ.

Подобным же образом устанавливается справедливость или несправедливость сравнения (3) для каждого σ: (3) показывает, что с помощью полиномов $\sum g_\nu f_\nu$ можно представить все произведения степени σ, если опустить члены со степенью большей σ. Для каждого корня a полиномов $f_1, \ldots, f_r$ испытываются значения $\sigma = 1, 2, \ldots$, пока не найдется σ, для которого имеет место (3): это σ и будет тогда показателем $\mathfrak{q}$.

В случае идеала $\mathfrak{m}$ нулевого измерения все примарные компоненты также нулевого измерения и изолированные; к ним можно применить указанный выше критерий $f \equiv 0\,(\mathfrak{q})$. Если критерий выполняется для всех корней, то $f \equiv 0\,(\mathfrak{m})$. Отсюда получается следующая теорема:

Если показатель $\mathfrak{p}$ идеала $\mathfrak{m}$ нулевого измерения определяется как наименьшее натуральное число σ, для которого удовлетворяется (3) *при* $\mathfrak{p} = (x_1 - a_1, \ldots, x_n - a_n)$, *где* $a = \{a_1, \ldots, a_n\}$ — *произвольный корень* $\mathfrak{m}$, *и полином f удовлетворяет сравнению* (4) *для всех таких* $\mathfrak{p}$, *то имеет место* $f \equiv 0\,(\mathfrak{m})$.

Эта теорема впервые была высказана М. Нётером для случая $\mathfrak{m} = (f_1, f_2)$, где f_1 и f_2 — полиномы двух переменных [1]): это знаменитая *„теорема Нётера“*, которая послужила основой „геометрического направления“ в теории алгебраических функций. Нётер вместо более слабого условия (4) пользовался условием (5) в предположении, что оно удовлетворяется для всех корней. Бертини [2]) принадлежит требование совпадения членов со степенью, не превосходящей $\rho - 1$ (относительно $y_1, \ldots, y_n$); он же указал предел для показателей ρ [3]). Ласкер и Маколей обобщили эти результаты на случай n измерений. Условие $f \equiv 0\ (\mathfrak{m}, \mathfrak{p}^\sigma)$, достаточное для $f \equiv 0\,(\mathfrak{q})$, мы назовем по Маколею *условием Нётера в точке a*.

§ 93. ЧАСТНЫЕ СЛУЧАИ И ПРИЛОЖЕНИЯ ТЕОРЕМЫ НЁТЕРА

Каждый из полиномов $f_1, \ldots, f_r$, образующих базис идеала $(f_1, \ldots, f_r)$, определяет некоторое алгебраическое многообразие (сверхповерхность) $f_\nu = 0$ в n-мерном пространстве. Точно так же полином f определяет сверхповерхность $f = 0$. Если f разлагается на неприводимые множители: $f = p_1^{\rho_1} p_2^{\rho_2} \ldots$, то многообразие $f = 0$ также распадается на неприводимые части $p_1 = 0, p_2 = 0, \ldots$, причем $p_1 = 0$ мы будем считать ρ_1 раз, $p_2 = 0$ будем считать ρ_2 раз и т. д.

---

[1]) Noether, M. Über einen Satz aus der Theorie der algebraischen Funktionen „Math. Ann.“, т. 6, стр. 351—359, 1873.

[2]) Bertini E., Zum Fundamentalsatz aus der Theorie der algebraischen Funktionen, „Math. Ann.“, т. 34, стр. 447—449, 1889.

[3]) Более точные границы даны P. Dubreil, Thèse de Doctorat, Paris 1930. См. также у H. Kapferer, Notwendig- und hinreichende Multiplizitätsbedingungen zum Noetherschen Fundamentalsatz, Sitzungsber. der Heidelberger Akademie 1927, 8. Abhandlung.

Если разложение f в ряд по степеням $y_\nu = x_\nu - a_\nu$ начинается с членов s-й степени ($s \geqslant 0$):

$$f = c_0 y_1^s + c_1 y_1^{s-1} y_2 + \ldots + c_\omega y_n^s + \ldots,$$

то говорят, что сверхповерхность $f = 0$ *имеет в* $a = \{a_1, \ldots, a_n\}$ *s-кратную точку*. Член s-го порядка $c_0 y_1^s + \ldots + c_\omega y_n^s$, будучи приравнен нулю, дает сверхповерхность, состоящую исключительно из „прямых линий", проходящих через a (*касательный конус* к сверхповерхности $f = 0$ с вершиной в точке a).

Простейшим случаем теоремы Нётера является тот, когда среди сверхповерхностей $f_1 = 0, \ldots, f_r = 0$, определяющих идеал $\mathfrak{m}$ нулевого измерения, сверхповерхности $f_1 = 0, \ldots, f_n = 0$ имеют в a простую точку, причем эта точка лежит на касательных сверхповерхностях:

$$\begin{aligned} f_1 &= c_{11} y_1 + \ldots + c_{1n} y_n + \ldots, \\ f_2 &= c_{21} y_1 + \ldots + c_{2n} y_n + \ldots, \\ &\ldots\ldots\ldots\ldots\ldots \\ f_n &= c_{n1} y_1 + \ldots + c_{nn} y_n + \ldots \end{aligned}$$

Линейные формы $\sum_{\mu=1}^{n} c_{\lambda\mu} y_\mu$ линейно независимы.

В этом случае среди линейных комбинаций от функций $f_1, \ldots, f_n$ по модулю $\mathfrak{p}^2$, где $\mathfrak{p}$ — простой идеал $(x_1 - a_1, \ldots, x_n - a_n)$, встречаются также и $y_1, \ldots, y_n$, т. е.

$$(y_1, \ldots, y_n) \equiv 0 \left((f_1, \ldots, f_n), \mathfrak{p}^2\right),$$

а потому

$$\mathfrak{p} \equiv 0 (\mathfrak{m}, \mathfrak{p}^2).$$

Отсюда следует, что идеал $\mathfrak{m}$ в точке a имеет изолированный примарный компонент $\mathfrak{q}$ с показателем 1, т. е. $\mathfrak{q} = \mathfrak{p}$. Таким образом полином, имеющий корень a, должен делиться на $\mathfrak{q}$. Если все корни a идеала $\mathfrak{m}$ являются такими „простыми точками пересечения", то для $f \equiv 0 (\mathfrak{m})$ достаточно, чтобы f содержало все эти корни.

При рассмотрении более сложных случаев мы ограничимся двумя переменными x_1, x_2 и идеалом $\mathfrak{m}$, порожденным двумя взаимно простыми полиномами f_1, f_2. Так как f_1 и f_2 взаимно просты относительно x_2, то

$$1 = g_1 f_1 + g_2 f_2,$$

где g_1 и g_2 рациональны относительно x_1 и целые рациональные функции относительно x_2. Умножив обе части равенства на отличный от нуля полином $h(x_1)$, приведем равенство к целому рациональному виду относительно x_1. Отсюда получим:

$$h(x_1) \equiv 0 (f_1, f_2).$$

Существует только конечное число значений координат x_1 и x_2 корней (f_1, f_2): имеется только конечное число корней a [1]). Если присоединить

[1]) Согласно § 79 число корней не должно превосходить произведения степеней f_1 и f_2.

их координаты к основному полю, то для каждого корня a изолированный примарный компонент $\mathfrak{q}$ идеала $\mathfrak{m}=(f_1, f_2)$ будет принадлежать простому идеалу $\mathfrak{p}=(y_1, y_2)=(x_1-a_1, x_2-a_2)$.

Простейший случай, когда общая точка a кривых $f_1=0$ и $f_2=0$ простая и касательные не совпадают, мы уже исследовали: получилось, что $\rho=1$ и $\mathfrak{q}=\mathfrak{p}$. Следующим по очереди простым случаем является тот, когда точка a имеет кратность r для $f_1=0$ и кратность s для $f_2=0$, но касательные $f_2=0$ не сливаются с касательными $f_1=0$. Если положим

$$f_1=c_0y_1^r+c_1\,y_1^{r-1}y_2+\ldots+c_ry_2^r+\ldots,$$
$$f_2=d_0y_1^s+d_1y_1^{s-1}y_2+\ldots+d_sy_2^s+\ldots,$$

то касательные f_1, f_2 найдутся, если определим корни форм $c_0y_1^r+\ldots+c_ry_2^r$ и $d_0y_1^s+\ldots+d_sy_2^s$. Таким образом если касательные f_1 отличны от касательных f_2, то в силу § 71 результант

$$R=\begin{vmatrix} c_0 & c_1 & \ldots & c_r & & \\ & c_0 & c_1 & \ldots & c_r & \\ & & \ldots & \ldots & \ldots & \\ d_0 & d_1 & \ldots & d_s & & \\ & d_0 & d_1 & \ldots & d_s & \\ & & \ldots & \ldots & \ldots & \end{vmatrix}$$

этих двух форм не должен равняться нулю.

Попытаемся теперь найти такое σ, для которого

$$\mathfrak{p}^\sigma\equiv 0\left((f_1, f_2), \mathfrak{p}^{\sigma+1}\right).$$

Чтобы из f_1, f_2 и $\mathfrak{p}^{\sigma+1}$ получить произведения y_ν степени σ, умножим f_1 на всевозможные произведения степени $\sigma-r$ и f_2 на всевозможные произведения степени $\sigma-s$ и затем опустим все члены со степенью, большей σ. Это даст нам самое большее

$$(\sigma-r+1)+(\sigma-s+1)=2\sigma-r-s+2$$

линейно независимых выражений. Если желательно отсюда получить линейными комбинациями все $\sigma+1$ произведений степени σ, то должно иметь место:

$$2\sigma-r-s+2\geqslant\sigma+1,$$
$$\sigma\geqslant r+s-1.$$

Положим $\sigma=r+s-1$ и выпишем полученные выражения:

$$\begin{aligned} &c_0y_1^\sigma+c_1y_1^{\sigma-1}y_2+\ldots+c_ry_1^{\sigma-r}y_2^r,\\ &c_0y_1^{\sigma-1}y_2+c_1y_1^{\sigma-2}y_2^2+\ldots,\\ &\qquad\ldots\ldots;\\ &d_0y_1^\sigma+d_1y_1^{\sigma-1}y_2+\ldots+d_sy_1^{\sigma-s}y_2^s,\\ &d_0y_1^{\sigma-1}y_2+d_1y_1^{\sigma-2}y_2^2+\ldots,\\ &\qquad\ldots\ldots \end{aligned}$$

Тогда в силу $R \not\equiv 0$ мы будем иметь $\sigma + 1$ линейно независимых форм, от которых линейно зависят все произведения степени σ. Таким образом

$$\mathfrak{p}^\sigma \equiv 0\left((f_1, f_2), \mathfrak{p}^{\sigma+1}\right) \quad \text{при} \quad \sigma = r + s - 1.$$

Следовательно, *показатель примарного идеала* $\mathfrak{q}$ *в случае различных касательных равен* $r + s - 1$. Полином, обращающийся в нуль порядка $r + s - 1$ в точке a, тем самым принадлежит идеалу $\mathfrak{q}$. Этот результат был известен еще М. Нётеру.

Далее рассмотрим тот случай, когда кривая $f_1 = 0$ имеет в a простую точку, а $f_2 = 0$ совершенно произвольно. Таким образом пусть

$$f_1 = a_1 y_1 + a_2 y_2 + \ldots$$

и $a_1 \not\equiv 0$. Откинем все произведения, степени которых больше или равны $\sigma + 1$. Ясно, что полином f можно совершенно освободить от y_1, если из него вычесть некоторое кратное полинома f_1. Поступим проще всего так: прежде всего, вычитая кратное f_1, удалим члены с первой степенью y_1, затем, вычитая кратное полинома $y_1 f_1$, удалим члены с y_1^2, и т. д. до членов с y_1^σ. Применяя эти преобразования также к полиному f_2, получим:

$$f - g f_1 \equiv c_0 + c_1 y_2 + c_2 y_2^2 + \ldots + c_\sigma y_2^\sigma (\mathfrak{p}^{\sigma+1}), \tag{1}$$

$$f_2 - h f_1 \equiv d_0 + d_1 y_2 + d_2 y_2^2 + \ldots + d_\sigma y_2^\sigma (\mathfrak{p}^{\sigma+1}). \tag{2}$$

Коэфициенты c_ν и d_ν, очевидно, определяются единственным образом. Если увеличивать показатель σ, то каждый из степенных рядов допускает дальнейшее продолжение; увеличивая σ неограниченно, получим так называемые бесконечные ряды Пюизе [1]).

Подобным же образом для произведений y степени σ, порождающих идеал $\mathfrak{p}^\sigma$, имеем:

$$y_1^\nu y_2^{\sigma-\nu} \equiv b_\nu y_2^\sigma \left((f_1), \mathfrak{p}^{\sigma+1}\right).$$

Таким образом в кольце вычетов по модулю $\left((f_1), \mathfrak{p}^{\sigma+1}\right)$ вычисления проводятся совершенно так же, как и для степенных рядов от y_2, заканчивающихся на члене y_2^σ. Легко видеть, что сравнение

$$\mathfrak{p}^\sigma \equiv 0\left((f_1, f_2), \mathfrak{p}^{\sigma+1}\right) \tag{3}$$

только тогда удовлетворяется, когда некоторое $d_k \not\equiv 0 \,(k \leqslant \sigma)$; следовательно, наименьшее σ, для которого удовлетворяется (3), равно наименьшему k, для которого $d_k \not\equiv 0$. *Итак, показатель* ρ *идеала* $\mathfrak{q}$ *равен индексу первого отличного от нуля члена ряда* (2).

Точно так же легко найти, что сравнение

$$f \equiv 0\left((f_1, f_2), \mathfrak{p}^{\sigma+1}\right) \quad [\sigma + 1 = \rho] \tag{4}$$

справедливо только тогда, если $c_0 = c_1 = \ldots = c_\sigma = 0$. Иными словами: *если* $f \equiv 0\,(\mathfrak{q})$, *то в разложении* (1) *должны быть только члены, содержащие* y_2^σ, *и более высокие степени* y_2.

[1]) См. Puiseux, Mémoire sur la théorie des fonctions algébriques, Journal de Liouville, т. 1, стр. 15, 1854; Jordan C., Cours d'analyse I (3-е издание), стр. 346–357, 1909; K. Hensel und G. Landsberg, Theorie der algebraischen Funktionen einer Veränderlichen, Leipzig 1902.

Можно показать, что найденный выше показатель ρ вместе с тем определяет кратность точки a пересечения кривых $f_1 = 0$ и $f_2 = 0$ (см. § 79).

В геометрических приложениях теоремы Нётера часто встречается случай, когда полиномы f, f_1, f_2 получаются из однородных полиномов F, F_1, F_2 с помощью подстановки $x_0 = 1$. Возникает в связи с этим такой вопрос. При каких условиях из

$$f = g_1 f_1 + g_2 f_2 \tag{5}$$

вытекает

$$F = G_1 F_1 + G_2 F_2, \tag{6}$$

где G_1 и G_2 — также формы?

Предположим, что при $x_0 = 0$ формы F_1 и F_2 не имеют общего делителя, отличного от постоянной (т. е. не имеют общих корней, кроме тривиальных $x_1 = 0$ и $x_2 = 0$). Очевидно, что линейным преобразованием трех переменных x_0, x_1, x_2, расширяя в случае надобности поле коэфициентов K, всегда можно обеспечить справедливость этого предположения.

Производя подстановку $x_1 \to \frac{x_1}{x_0}$, $x_2 \to \frac{x_2}{x_0}$ и умножив на соответствующую степень x_0, получим из (5) уравнение вида:

$$x_0^h \cdot F = H_1 F_1 + H_2 F_2, \tag{7}$$

где H_1 и H_2 — формы.

Преобразуем это уравнение так, чтобы оно сократилось на множитель x_0. Если подставим в левую и правую части $x_0 = 0$, то получим:

$$0 = H_{10} F_{10} + H_{20} F_{20}.$$

Так как по предположению F_{10} и F_{20} взаимно просты, то H_{10} должно делиться на F_{20}, а H_{20} — на F_{10}:

$$H_{10} = G_0 F_{20},$$

$$H_{20} = -G_0 F_{10}.$$

Но H_1 совпадает с H_{10} до членов с x_0; точно так же совпадают H_2 с H_{20}, F_1 с F_{10} и F_2 с F_{20}, откуда следует:

$$H_1 = G_0 F_2 + x_0 K_1,$$

$$H_2 = -G_0 F_1 + x_0 K_2,$$

где K_1 и K_2 — формы. Подставляя в (7), получим:

$$x_0^h F = x_0 K_1 F_1 + x_0 K_2 F_2.$$

Это равенство можно сократить на x_0. Повторяя h раз эти преобразования, получим уравнение вида (6). Итак:

Для уравнения (5) *необходимо и достаточно, чтобы для всех общих корней форм F_1 и F_2 полиномы F, F_1, F_2, которые сделаны неоднородными, удовлетворяли условиям Нётера.*

Если рассматривать величины x_0, x_1, x_2 как однородные координаты точки проективной плоскости, то $F = 0$ будет кривой, содержащей все точки пересечения кривых $F_1 = 0$ и $F_2 = 0$ и, кроме того, во всех этих точках должны выполняться известные условия Нётера, чтобы имело место уравнение (5). Это уравнение прежде всего важно в силу следующей теоремы:

Если кривая $F_2 = 0$ степени m пересекается с кривой $F = 0$ степени $n + p$ в $m(n + p)$ точках, причем каждая точка считается с соответствующей кратностью (§ 79), *и если из этих $m(n + p)$ точек $m \cdot n$ точек лежат на кривой $F_1 = 0$ степени n, то остальные $m \cdot p$ точки лежат на кривой $G_1 = 0$ степени p, в предположении, что кривая $F = 0$ во всех $m \cdot n$ точках удовлетворяет условиям Нётера* [*с идеалом* (F_1, F_2)].

Действительно, из формулы (6), очевидно, следует, что $F=0$ и $F_2=0$ пересекаются в тех же точках, что и $F_1G_1=0$ с $F_2=0$.

Относительно других геометрических выводов, вытекающих из этой теоремы, см. в учебнике F. Severi, Vorlesungen über algebraische Geometrie (немецкий перевод E. Löffler), 1921, а также краткую заметку автора в „Math. Ann.", т. 104, стр. 472, 1931.

Задачи. 1. Если коническое сечение пересекается с кривой третьего порядка, в шести различных точках и эти точки сгруппированы по 3 парам, причем точки каждой пары соединены прямой, а эти прямые также пересекаются с кривой, то получаемые три точки лежат на одной прямой.

2. Теорема Паскаля является частным случаем задачи 1 (здесь кривая третьего порядка распадается на три прямые).

3. Касательные к трем точкам кривой третьего порядка, лежащим на одной прямой, пересекают эту кривую еще в трех точках, лежащих на прямой.

4. В частности, из задачи 3 следует, что прямая, соединяющая две точки перегиба, пересекает кривую третьего порядка в точке перегиба.

5. Если две окружности пересекают другие две окружности в восьми точках, кроме изотропных точек проективной плоскости, и четыре из этих восьми точек лежат на одной из окружностей, то остальные четыре точки также лежат на окружности.

6. Если возьмем на каждой стороне треугольника $A_1A_2A_3$ по точке, отличной от вершин углов, а именно B_1 на стороне A_2A_3, причем B_1 отлично от A_2 и A_3 и т. д., то окружности $A_1B_2B_3$, $A_2B_3B_1$, $A_3B_1B_2$ проходят через одну точку.

§ 94. ПЕРЕХОД ОТ МНОГОМЕРНОГО ИДЕАЛА К ИДЕАЛУ НУЛЕВОГО ИЗМЕРЕНИЯ

В этом параграфе мы попытаемся распространить на многомерные идеалы теоремы, доказанные в § 92 для идеалов нулевого измерения.

При этом воспользуемся следующим методом: если $\mathfrak{q}$ есть примарный идеал в $\mathsf{K}[x]$ измерения d, $\mathfrak{p}$ — соответствующий простой идеал, $\{\xi_1, \ldots, \xi_n\}$ — его общий корень и $\xi_1, \ldots, \xi_d$ алгебраически независимы [1]), то идеалы $\mathfrak{q}$ и $\mathfrak{p}$ подстановкой $x_1=\xi_1, \ldots, x_d=\xi_d$ мы приведем к идеалам нулевого измерения. Произведем эту подстановку для всех полиномов q идеала $\mathfrak{q}$; тогда полиномы q перейдут в полиномы q' из $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$, порождающие идеал $\mathfrak{q}'$. Очевидно, достаточно применить подстановку $x_1=\xi_1, \ldots, x_d=\xi_d$ к полиномам $q_1, \ldots, q_r$ базиса; тогда получатся полиномы $q_1', \ldots, q_r'$, порождающие идеал $\mathfrak{q}'$:

$$\mathfrak{q}'=(q_1', \ldots, q_r').$$

Идеал $\mathfrak{q}'$, очевидно, состоит из полиномов q', разделенных на полином φ от $\xi_1, \ldots, \xi_d$, отличный от нуля, так как полиномы q' образуют идеал в $\mathsf{K}[\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n]$; чтобы получить отсюда идеал в $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$, надо еще разделить их на φ.

Подобным же образом из $\mathfrak{p}$ получается идеал $\mathfrak{p}'$ и вообще из $\mathfrak{m}=(f_1, \ldots, f_r)$ — идеал $\mathfrak{m}'=(f_1', \ldots, f_r')$.

Геометрически подстановка $x_1=\xi_1, \ldots, x_d=\xi_d$, означает, что все рассматриваемые многообразия пересекаются линейным пространством $x_1=\xi_1, \ldots, x_d=\xi_d$, которое определяется общей точкой многообразия $\mathfrak{q}$.

---

[1]) Таким образом $\xi_1, \ldots, \xi_d$ можно будет рассматривать как независимые переменные (мы их могли бы обозначить через $t_1, \ldots, t_d$), а прочие ξ считать алгебраическими функциями от этих переменных.

Если $f(x_1, \ldots, x_n)$ — полином и $f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$ принадлежит $\mathfrak{q}'$, то по предыдущему

$$f(\xi, x) = \frac{q'}{\varphi(\xi_1, \ldots, \xi_d)} = \frac{q(\xi, x)}{\varphi(\xi)}, \quad q(x) \equiv 0 \,(\mathfrak{q}),$$

откуда

$$q(\xi, x) = \varphi(\xi) f(\xi, x).$$

Отсюда вытекает в силу алгебраической независимости $\xi_1, \ldots, \xi_d$:

$$q(x) = \varphi(x) f(x) \equiv 0 \,(\mathfrak{q}).$$

Но из $\varphi(\xi) \neq 0$ следует $\varphi(x) \not\equiv 0 \,(\mathfrak{p})$, а потому

$$f(x) \equiv 0 \,(\mathfrak{q}).$$

Чтобы выяснить, когда полином $f(x)$ принадлежит $\mathfrak{q}$, достаточно проверить, принадлежит ли соответствующее $f' = f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$ идеалу $\mathfrak{q}'$. Таким образом $\mathfrak{q}'$ определяет $\mathfrak{q}$ однозначно [1]).

Теперь мы утверждаем, *что идеал* $\mathfrak{q}'$ *в* $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ *примарен и обладает простым идеалом* $\mathfrak{p}'$; *показатель* $\mathfrak{q}'$ *равен показателю* $\mathfrak{q}$; $\{\xi_{d+1}, \ldots, \xi_n\}$ *есть общий корень идеала* $\mathfrak{p}'$, *измерение которого равно нулю.*

Доказательство. Для того чтобы показать, что $\mathfrak{q}'$ примарно и $\mathfrak{p}'$ — соответствующий простой идеал, достаточно вывести такие свойства:

1. Из $f(\xi, x) g(\xi, x) \equiv 0 \,(\mathfrak{q}')$ и $f(\xi, x) \not\equiv 0 \,(\mathfrak{p}')$ следует $g(\xi, x) \equiv 0 \,(\mathfrak{q}')$.
2. Из $f(\xi, x) \equiv 0 \,(\mathfrak{q}')$ следует $f(\xi, x) \equiv 0 \,(\mathfrak{p}')$.
3. Из $f(\xi, x) \equiv 0 \,(\mathfrak{p}')$ следует $f(\xi, x)^\rho \equiv 0 \,(\mathfrak{q}')$.

Здесь f и g предполагаются целыми рациональными относительно $\xi_1, \ldots, \xi_d$, так как в противном случае мы бы их умножили на соответствующее $\varphi(\xi)$. Тогда в силу высказанного выше замечания можно везде ξ заменить через x, $\mathfrak{q}'$ — через $\mathfrak{q}$, $\mathfrak{p}'$ — через $\mathfrak{p}$, так как, например, $f(\xi, x) \equiv 0 \,(\mathfrak{q}')$ эквивалентно $f(x) \equiv 0 \,(\mathfrak{q})$ и т. д. Но после такой замены 1, 2, 3 будут выражать не что иное, как то, что $\mathfrak{q}$ примарно и $\mathfrak{p}$ — соответствующий простой идеал. Вместе с тем мы показали, что показатели $\mathfrak{q}'$ и $\mathfrak{q}$ совпадают.

Покажем теперь, что $\{\xi_{d+1}, \ldots, \xi_n\}$ есть общий корень идеала $\mathfrak{p}'$. Для этого докажем, что из

$$f(\xi_1, \ldots, \xi_d, \xi_{d+1}, \ldots, \xi_n) = 0,$$

где f рационально относительно $\xi_1, \ldots, \xi_d$ и целый рациональный полином относительно $\xi_{d+1}, \ldots, \xi_n$, следует:

$$f(\xi, x) \equiv 0 \;\; (\mathfrak{p}'),$$

и обратно. Снова можно предположить, что f является целой рациональной функцией относительно $\xi_1, \ldots, \xi_d$. Но тогда $f(\xi, x) \equiv 0 \,(\mathfrak{p}')$ будет эквивалентно $f(x) \equiv 0 \,(\mathfrak{p})$; таким образом доказана и эта часть

---

[1]) Это справедливо, как это видно из доказательства, для всякого примарного идеала $\mathfrak{r}$, об адающего тем свойством, что $x_1, \ldots, x_d$ независимы по модулю соответствующего простого идеала $\mathfrak{s}$, т. е. что из $\varphi(x_1, \ldots, x_d) \neq 0$ следует $\varphi \not\equiv 0 \,(\mathfrak{s})$. Если, напротив, существует в $\mathfrak{s}$ $\varphi(x_1, \ldots, x_d) \neq 0$, то $\varphi(x)^\rho \equiv 0 \,(\mathfrak{r})$, откуда $1 = \varphi(\xi)^{-\rho} \varphi(\xi)^\rho \equiv 0 \,(\mathfrak{r}')$, и $\mathfrak{r}'$ является единичным идеалом.

теоремы, если только воспользоваться замечанием, что $\{\xi_1, \ldots, \xi_n\}$ есть общий корень идеала $\mathfrak{p}$.

Наконец $\xi_{d+1}, \ldots, \xi_n$ являются алгебраическими относительно $K(\xi_1, \ldots, \xi_d)$, откуда следует, что $\mathfrak{p}'$ нулевого измерения. Тем самым теорема доказана полностью.

Точно так же можно показать, что *если* $\mathfrak{q}$ *— примарный компонент идеала* $\mathfrak{m} = (f_1, \ldots, f_r)$, *то* $\mathfrak{q}'$ *будет также примарным компонентом соответствующего идеала* $\mathfrak{m}' = (f_1', \ldots, f_r')$.

Действительно, если $\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_2, \ldots, \mathfrak{q}_s]$ — несократимое представление идеала $\mathfrak{m}$ через максимальные примарные компоненты, то $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}_2', \ldots, \mathfrak{q}_s']$, так как полиномы $f(\xi, x)$ идеала $\mathfrak{m}'$ и полиномы из $[\mathfrak{q}', \mathfrak{q}_2', \ldots]$ при умножении на некоторые многочлены $\varphi(\xi_1, \ldots, \xi_d) \not\equiv 0$ можно преобразовать в такие выражения $g(\xi, x)$, что $g(x_1, \ldots, x_d, x_{d+1}, \ldots, x_n)$ будут принадлежать $\mathfrak{m}$, $\mathfrak{q}$ и $\mathfrak{q}_2, \ldots, \mathfrak{q}_s$. Если бы в представлении $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}_2', \ldots, \mathfrak{q}_s']$ $\mathfrak{q}'$ было лишним, то мы бы имели $[\mathfrak{q}_2', \ldots, \mathfrak{q}_s'] \equiv 0\,(\mathfrak{q}')$. Если положить $\mathfrak{m}_1 = [\mathfrak{q}_2, \ldots, \mathfrak{q}_s]$, то отсюда вытекало бы $\mathfrak{m}_1' = [\mathfrak{q}_2', \ldots, \mathfrak{q}_s'] \equiv 0\,(\mathfrak{q}')$. Если f — произвольный элемент $\mathfrak{m}_1$, то $f' \equiv 0\ (\mathfrak{m}_1') \equiv 0\,(\mathfrak{q}')$, откуда $f \equiv 0\ (\mathfrak{q})$. Отсюда следовало бы, что $\mathfrak{m}_1 \equiv 0\ (\mathfrak{q})$, т. е. что в представлении $\mathfrak{m}$ идеал $\mathfrak{q}$ был бы лишним, что противоречит несократимости представления идеала $\mathfrak{m}$. Следовательно, в $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}_2', \ldots, \mathfrak{q}_s']$ $\mathfrak{q}'$ не может быть лишним. Если устранить лишние $\mathfrak{q}_\nu'$, то получится несократимое представление, содержащее $\mathfrak{q}'$. Если $\mathfrak{p}_\nu$ и $\mathfrak{p}_\nu'$ — простые идеалы, принадлежащие соответственно $\mathfrak{q}_\nu$ и $\mathfrak{q}_\nu'$, то $\mathfrak{p} \neq \mathfrak{p}_\nu$, а потому в силу замеченной выше однозначности (см. сноску на стр. 76) $\mathfrak{p}' \neq \mathfrak{p}_\nu'$. В случае $\mathfrak{p}_\nu' = \mathfrak{o}$, когда уже не имеет места однозначность, точно так же $\mathfrak{p}' \neq \mathfrak{p}_\nu'$. Итак, в представлении $\mathfrak{m}'$ $\mathfrak{q}'$ есть единственный принадлежащий к $\mathfrak{p}'$ идеал. Но это значит, что $\mathfrak{q}'$ есть примарный компонент идеала $\mathfrak{m}'$.

Если $\mathfrak{q}$ есть *изолированный компонент* $\mathfrak{m}$, то $\mathfrak{q}'$ *является также изолированным компонентом* $\mathfrak{m}'$. Доказательство совершенно аналогично приведенному выше.

Изложенный метод приведения всех примарных идеалов к идеалу нулевого измерения дает возможность узнать, принадлежит ли данный полином f данному идеалу $\mathfrak{m} = (f_1, \ldots, f_r)$ при условии, что известно заранее разложение $\mathfrak{m}$ на примарные компоненты

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s].$$

В самом деле, для каждого примарного компонента $\mathfrak{q}$ находим соответствующее $\mathfrak{q}'$ нулевого измерения, затем расширяем поле $K(\xi_1, \ldots, \xi_d)$ так, чтобы $\mathfrak{q}'$ распалось на дальнейшие примарные идеалы, имеющие каждый по корню $a^{(\nu)}$, и с помощью „нётеровских условий“

$$f' \equiv 0\,(\mathfrak{q}', \mathfrak{p}_\nu'^{\rho}),\ \mathfrak{p}_\nu' = (x_{d+1} - a_{d+1}^{(\nu)}, \ldots, x_n - a_n^{(\nu)}) \qquad (1)$$

исследуем согласно § 92, принадлежит ли полином f' идеалам $\mathfrak{q}_\nu' = (\mathfrak{q}', \mathfrak{p}_\nu'^{\rho})$ и тем самым $\mathfrak{q}'$. Так как корни $\mathfrak{p}_\nu'$ сопряжены относительно $K(\xi_1, \ldots, \xi_d)$, то $\mathfrak{p}_\nu'$, а потому и $\mathfrak{q}_\nu'$ сопряжены относительно $K(\xi_1, \ldots, \xi_d)$; таким образом достаточно исследовать для каждого $\mathfrak{q}'$ одно $\mathfrak{q}_\nu'$. Сле-

довательно, нужно присоединить только один корень каждого $\mathfrak{q}'$, Пуеть таким корнем является $\{\xi_{d+1}, \ldots, \xi_n\}$. Отсюда вместо $\mathfrak{p}'$ будем иметь простой идеал

$$\mathfrak{p}_\xi = (x_{d+1} - \xi_{d+1}, \ldots, x_n - \xi_n);$$

вместо сравнения (1) мы можем взять более удобное сравнение

$$f' \equiv 0 \ (\mathfrak{m}', \mathfrak{p}_\xi^\rho), \tag{2}$$

так как (2) также необходимо для $f \equiv 0$ $(\mathfrak{m})$, и из (2) сразу следует (1). Условие (2), выполняющееся для всякого примарного компонента $\mathfrak{q}$ идеала $\mathfrak{m}$, известно под названием *критерия Генцельта* или *теоремы Генцельта о корнях*.

В частности, если $\mathfrak{q}$ есть изолированный компонент идеала $\mathfrak{m}$ (откуда $\mathfrak{q}'$ есть изолированный компонент идеала $\mathfrak{m}'$), то можно так же, как в § 86, определить из

$$\mathfrak{p}_\xi^\rho \equiv 0 \ (\mathfrak{m}', \mathfrak{p}_\xi^{\rho+1})$$

показатель ρ.

Из условий (1) для $f \equiv 0$ $(\mathfrak{q})$ явствует с полной очевидностью геометрическое значение примарных идеалов: принадлежность к примарному идеалу обусловливает известные требования на начальные члены разложения полинома f по степеням $x_1 - \xi_1, \ldots, x_n - \xi_n$ для общей точки ξ неприводимого многообразия, например, требование, чтобы f обращалось в нуль в этой общей точке, или чтобы сверхповерхность $f = 0$ в этой общей точке касалась другой сверхповерхности, и т. д.

Задачи. 1. Пользуясь методом приведения к идеалу нулевого измерения, показать, что $(n-1)$-мерный примарный идеал в $\mathsf{K}[x_1, \ldots, x_n]$ является главным идеалом.

2. Несмешанный $(n-1)$-мерный идеал в $\mathsf{K}[x_1, \ldots, x_n]$ есть главный идеал, и обратно.

§ 95. НЕСМЕШАННЫЕ ИДЕАЛЫ

Для несмешанных идеалов, у которых все примарные компоненты имеют одно и то же измерение d, все эти примарные компоненты изолированные; их многообразия и общие точки сразу получаются с помощью теории исключения (§ 74), а критерии для $f \equiv 0$ $(\mathfrak{m})$ из предыдущего параграфа принимают более простой вид. Весьма существенно поэтому иметь возможность заранее установить несмешанность некоторых идеалов. Прежде всего установим некоторые критерии, с помощью которых можно узнать, обладает ли рассматриваемый идеал компонентами нулевого измерения.

Если $\mathfrak{m} = (f_1, \ldots, f_r)$ есть идеал в $\mathfrak{o} = \mathsf{K}[x]$, а $\mathfrak{M}$ — идеал в $\mathfrak{O} = \Omega[x]$ (с тем же базисом), порожденный идеалом $\mathfrak{m}$, причем Ω — алгебраическое (самое удобное — взять его алгебраически замкнутым) поле расширения K, то согласно лемме § 92 пересечение $\mathfrak{M} \cap \mathfrak{o}$ равно $\mathfrak{m}$. Если $\mathfrak{M}$ разлагается на примарные компоненты

$$\mathfrak{M} = [\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_s], \tag{1}$$

то

$$\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o} = [\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_s, \mathfrak{o}] = [\mathfrak{Q}_1 \cap \mathfrak{o}, \mathfrak{Q}_2 \cap \mathfrak{o}, \ldots, \mathfrak{Q}_s \cap \mathfrak{o}]^{1}) \tag{2}$$

Далее имеет место следующее предложение:

---

[1]) Среди идеалов $\mathfrak{Q}_\nu \cap \mathfrak{o}$ некоторые вообще могут быть друг с другом тождественны. А именно, два сопряженных (относительно K) $\mathfrak{Q}_\nu$ имеют одно и то же пересечение с $\mathfrak{o}$.

Если $\mathfrak{O}$ примарно относительно простого идеала $\mathfrak{P}$, то $\mathfrak{O} \cap \mathfrak{o}$ примарно в кольце $\mathfrak{o}$ относительно простого идеала $\mathfrak{P} \cap \mathfrak{o}$ [1]).

Доказательство получается без труда с помощью известных трех критериев:

1. Из $fg \equiv 0$ $(\mathfrak{O} \cap \mathfrak{o})$, $f \not\equiv 0$ $(\mathfrak{P} \cap \mathfrak{o})$ следует $g \equiv 0$ $(\mathfrak{O} \cap \mathfrak{o})$.
2. Из $f \equiv 0$ $(\mathfrak{O} \cap \mathfrak{o})$ следует $f \equiv 0$ $(\mathfrak{P} \cap \mathfrak{o})$.
3. Из $f \equiv 0$ $(\mathfrak{P} \cap \mathfrak{o})$ следует $f^{\rho} \equiv 0$ $(\mathfrak{O} \cap \mathfrak{o})$ для f и g из $\mathfrak{o}$.

Далее: *если ξ есть общий корень идеала $\mathfrak{P}$ (в поле расширения поля Ω), то ξ есть также общий корень идеала $\mathfrak{P} \cap \mathfrak{o}$.* В самом деле, если $\mathfrak{P}$ состоит из всех полиномов кольца $\mathfrak{O}$, имеющих корнем ξ, то $\mathfrak{P} \cap \mathfrak{o}$ будет состоять из всех полиномов кольца $\mathfrak{o}$ с корнем ξ.

Следствие. Измерение идеала $\mathfrak{P}$ равно измерению идеала $\mathfrak{P} \cap \mathfrak{o}$.

Таким образом, если $\mathfrak{M}$ в силу (1) есть пересечение примарных идеалов определенных измерений, то $\mathfrak{m}$ согласно (2) является пересечением примарных идеалов, имеющих те же измерения. В частности, если $\mathfrak{M}$ не имеет компонентов нулевого измерения, то $\mathfrak{m}$ также не имеет компонентов подобного рода, а если $\mathfrak{M}$ несмешанный идеал, то и $\mathfrak{m}$ не смешано. (Обратное также справедливо, но доказывается несколько труднее и для нас не представляет интереса.)

Методами § 94 задача о k-мерных компонентах идеала $\mathfrak{M}$ может быть сведена к случаю компонентов нулевого измерения. При соответствующем выборе поля Ω каждый из компонентов идеала $\mathfrak{M}$ нулевого измерения будет иметь только по одному корню a; простой идеал, принадлежащий этому компоненту, имеет вид $\mathfrak{p} = (x_1 - a_1, \ldots, x_n - a_n)$. При этом решение вопроса о том, будет ли существовать примарный компонент, принадлежащий $\mathfrak{p}$, зависит от равенства:

$$\mathfrak{M} : \mathfrak{p} = \mathfrak{M},$$

т. е. зависит от того, следует ли из

$$f\mathfrak{p} \equiv 0 \ (\mathfrak{M})$$

сравнение

$$f \equiv 0 \ (\mathfrak{M})$$

или нет.

Если l — какая-то линейная комбинация от $x_1 - a_1, \ldots, x_n - a_n$, то из $f\mathfrak{p} \subseteq \mathfrak{M}$ следует, что $fl \equiv 0$ $(\mathfrak{M})$; если можно обнаружить, что (для подходяще выбранного l) из $fl \equiv 0$ $(\mathfrak{M})$ вытекает $f \equiv 0$ $(\mathfrak{M})$, то идеал $\mathfrak{M}$, и тем самым также $\mathfrak{m}$, наверное, не обладает примарным компонентом нулевого измерения с корнем a. При этом метод доказательства часто проводится так же, как в § 93 (мелкий шрифт), когда из $x_0^h F = H_1 F_1 + H_2 F_2$ было выведено $F = G_1 F_1 + G_2 F_2$. Общая теорема, которая получается с помощью этого метода доказательства, гласит:

Если идеал $(f_1, \ldots, f_r)$, отличный от $\mathfrak{o}$, с r элементами базиса, имеет измерение $d \leqslant n - r$, то он является несмешанным $(n-r)$-мерным идеалом.

Эта теорема уже встречалась для $r = 1$ в § 91 (задача 2); таким образом можно применить метод полной индукции по r и предположить, что для случая $r - 1$ полиномов базиса теорема для всякого числа n переменных справедлива.

Покажем, что идеал $(f_1, \ldots, f_r)$ при $k < n - r$ не обладает k-мерными примарными компонентами. Предположим противное, и пусть $\mathfrak{q}$ будет такой компонент. Тогда с помощью приема § 94 можно понизить измерение $\mathfrak{q}$ до нуля; от этого число n переменных и наивысшее измерение d идеала $(f_1, \ldots, f_r)$ понизятся на k; при этом, конечно, неравенство $d \leqslant n - r$ останется в силе. Таким образом остается только показать, что такой идеал $(f_1, \ldots, f_r)$ в случае $n - r > 0$ не имеет совсем примарных компонентов нулевого измерения, причем в силу сделанного выше замечания можно предположить, что примарный компонент нулевого измерения в основном (а может быть и в расширенном) поле допускает только один корень a.

Прежде всего покажем, что при $d \leqslant n - r$ полиномы $f_1, \ldots, f_r$ базиса можно выбрать так, чтобы каждый из идеалов $(f_1, \ldots, f_i)$ был не более чем $(n - i)$-го измерения. Для $i = 1$ и $f_1 \not\equiv 0$ это требование само собой выполняется. Предпо-

[1]) Во избежание ложных истолкований замечу, что обратное неверно: если $\mathfrak{O} \cap \mathfrak{o}$ примарно, то $\mathfrak{O}$ может и не быть примарным. Существуют (см. § 87) примеры простых идеалов $\mathfrak{m}$ в $\mathfrak{o}$, которые при расширении основного поля K до Ω распадаются на различные примарные компоненты.

ложим, что нам удалось получить идеал $(f_1, \ldots, f_{i-1})$, имеющий измерение, меньшее или равное $n-i+1$. В каждом из неприводимых $(n-i+1)$-мерных многообразий идеала $(f_1, \ldots, f_{i-1})$ (если только такие многообразия существуют) возьмем по точке, не принадлежащей многообразию $(f_1, \ldots, f_r)$. В каждой такой точке по крайней мере один из полиномов $f_i, f_{i+1}, \ldots, f_r$ не обращается в нуль; следовательно, некоторая линейная комбинация $f_i^* = f_i + \mu_{i+1} f_{i+1} + \ldots + \mu_r f_r$ в каждой из этих точек будет отлична от нуля. Эту линейную комбинацию мы возьмем в качестве i-го элемента базиса вместо f_i; тогда измерение идеала $(f_1, \ldots, f_{i-1}, f_i^*)$ не превзойдет $n-i$, в то время как идеал $(f_1, \ldots, f_r)$ при замене f_i через f_i^* останется неизменным.

Чтобы доказать, что $(f_1, \ldots, f_r)$ не обладает в a компонентами нулевого измерения, возьмем линейный полином

$$l = (x_1 - a_1) + c_2(x_2 - a_2) + \ldots + c_n(x_n - a_n),$$

где c определены так, что l отлично от нуля для всякого общего корня $(n-r)$-мерного простого идеала, принадлежащего $(f_1, \ldots, f_r)$, и $(n-r+1)$-мерного простого идеала, принадлежащего $(f_1, \ldots, f_{r-1})$. Если мы покажем, что из

$$lf \equiv 0\ (f_1, \ldots, f_r)$$

следует

$$f \equiv 0\ (f_1, \ldots, f_r),$$

то все будет готово.

При подстановке

$$x_1 = a_1 - \sum_{\nu=2}^{n} c_\nu (x_\nu - a_\nu)$$

l обратится в 0, а полином f перейдет в полином $f_0 \equiv f \pmod{l}$. Равенство

$$lf = g_1 f_1 + \ldots + g_r f_r \tag{3}$$

после этой подстановки перейдет в

$$0 = g_{10} f_{10} + \ldots + g_{r0} f_{r0}. \tag{4}$$

Измерение идеала $(f_{10}, \ldots, f_{r-1,0})$ в $K[x_2, \ldots, x_n]$ в силу выбора l не превосходит $n-r$, откуда в силу индуктивного предположения этот идеал несмешанный и $(n-r)$-мерный, а f_{r0} не содержит $(n-r)$-мерных многообразий нашего идеала; следовательно, из (4) получается:

$$g_{r0} \equiv 0\ (f_{10}, \ldots, f_{r-1,0}),$$

а отсюда

$$g_r \equiv h_r l\ (f_1, \ldots, f_{r-1}).$$

Подставив в (3), получим:

$$lf \equiv h_r l f_r\ (f_1, \ldots, f_{r-1}),$$

$$l(f - h_r f_r) \equiv 0\ (f_1, \ldots, f_{r-1}).$$

Так как идеал $(f_1, \ldots, f_{r-1})$ несмешанный и l в общих корнях примарных идеалов отлично от нуля, то

$$f - h_r f_r \equiv 0\ (f_1, \ldots, f_{r-1}),$$

$$f \equiv 0\ (f_1, \ldots, f_r).$$

Тем самым доказательство закончено.

Задачи. 1. Если f_1 и f_2 не имеют общего делителя, отличного от постоянной, и $(f_1, f_2) \neq 0$, то идеал (f_1, f_2) несмешанный и $(n-2)$-го измерения.

2 Пусть имеют место предположения задачи 1. Если в общих точках неприводимых составных частей многообразия идеала (f_1, f_2) „тангенциальные пространства" сверхповерхностей $f_1 = 0$ и $f_2 = 0$ различны (их определение см. в § 93), то для выполнения сравнения $f \equiv 0\ (f_1, f_2)$ необходимо и достаточно, чтобы f содержало это многообразие.

3. Каким требованиям должен удовлетворять полином f, чтобы он мог принадлежать идеалу

$$\left(x_1^2+x_2^2-x_3^2,\ x_1+x_4,\ x_2+x_4\right)?$$

Дальнейшие теоремы о несмешанных идеалах можно найти в книжке F. S. Macaulay, Algebraic Theory of Modular Systems, Cambridge Tracts in Mathematics 19, Cambridge 1916.

§ 96. СТЕПЕНЬ МНОГООБРАЗИЯ И ЕГО ТОЧКИ ПЕРЕСЕЧЕНИЯ С ЛИНЕЙНЫМИ ПРОСТРАНСТВАМИ

Мы будем здесь искать точки пересечения неприводимого алгебраического многообразия $\mathfrak{M}$ с линейным многообразием L_{n-r}, состоящим из корней r линейных полиномов

$$\left.\begin{aligned} l_1 &= l'_1 - t_1 = \sum_{k=1}^{n} s_{1k}x_k - t_1,\\ &\cdots\cdots\cdots\cdots\cdots\\ l_r &= l'_r - t_r = \sum_{k=1}^{n} s_{rk}x_k - t_r. \end{aligned}\right\} \qquad (1)$$

Прежде всего рассмотрим случай, когда все s_{ik} и t_i переменные. Тогда пространство L_{n-r} называется *общим линейным подпространством* измерения $n-r$.

Присоединим сперва величины s_{ik} к K и вместе с $l'_1, \ldots, l'_r$ возьмем еще новые линейные комбинации $l'_{r+1}, \ldots, l'_n$, так что в общем получится n линейно независимых форм, которые можно принять за новые переменные вместо $x_1, \ldots, x_n$. Пусть эти новые переменные $l'_1, \ldots, l'_n$ для корня ξ из $\mathfrak{M}$ принимают значения $\lambda_1, \ldots, \lambda_n$, и пусть

$$\lambda_i = \sum_{k=1}^{n} s_{ik}\xi_k \qquad (i=1, \ldots, r). \quad (2)$$

Среди этих λ_i существует, если d — измерение $\mathfrak{M}$, максимум d алгебраически независимых величин. Отсюда следует, что среди них самое большее d величин могут быть приняты равными новым переменным t_i; *поэтому если существуют точки пересечения $\mathfrak{M}$ с L_{n-r}, то можно считать* $r \leqslant d$. В случае $r=d$ каждая точка пересечения должна иметь степень трансцендентности, равную d, тем самым эта точка будет общей точкой $\mathfrak{M}$.

Теперь покажем, что в случае $r=d$ действительно существуют точки пересечения и притом в конечном числе. Тогда для $r<d$, как это легко видеть, будет бесконечное число точек пересечения.

Заметим сперва, что $r=d$ величин (2) алгебраически независимы, если в качестве ξ взять общий корень. В самом деле, если бы они были зависимы, то в силу леммы § 77 они были бы зависимыми и при частных значениях s_{ik}; но можно частные значения s_{ik} выбрать так, чтобы λ_i стали равными $\xi_1, \ldots, \xi_d$ или какой-нибудь группе d элементов из $\xi_1, \ldots, \xi_n$, а группа этих элементов алгебраически независима. Тем самым линейно независимые $\lambda_1, \ldots, \lambda_d$ можно отождествить в силу

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_d) \cong \mathsf{K}(s_{ik}, t_1, \ldots, t_r)$$

с неизвестными $t_1, \ldots, t_d$. Прочие λ, а потому также и ξ, будут алгебраическими функциями этих неизвестных, т. е. поле

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_n) = \mathsf{K}(s_{ik}, \xi_1, \ldots, \xi_n)$$

является алгебраическим относительно $\mathsf{K}(s_{ik}, t_j)$ [1]). Но уравнения (2) означают, что точка ξ принадлежит пространству L_{n-r}; таким образом существование точки пересечения доказано. Так как поля

$$\mathsf{K}(s_{ik}, \xi_1, \ldots, \xi_n) = \mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_n),$$

порожденные корнями, эквивалентны, то во всяком соответствующем поле расширения $\mathsf{K}(s, t)$ будет существовать только конечное число сопряженных систем значений для $\lambda_1, \ldots, \lambda_n$ или $\xi_1, \ldots, \xi_n$. *Таким образом* $\mathfrak{M}$ *и* L_{n-d} *имеют конечное число точек пересечения, и эти точки друг с другом сопряжены относительно* $\mathsf{K}(s, t)$. Число точек пересечения называется *степенью* многообразия $\mathfrak{M}$.

Посмотрим теперь, что произойдет с точками пересечения, если неизвестные s, t заменить величинами из K. Возьмем вместо пространства R_n проективное пространство P_n и вместо многообразия $\mathfrak{M}$ — соответствующее многообразие $\mathfrak{M}^*$ в P_n; это делается для того, чтобы наши выводы обладали общностью. Тогда к старым переменным прибавится еще одна переменная x_0 и l_ν станут однородными. Полагая $t_1 = -s_{10}$, $t_2 = -s_{20}$ и т. д., получим вместо (1) формы:

$$l_1^* = \sum_{k=0}^{n} s_{1k}x_k,$$

$$\ldots\ldots\ldots\ldots$$

$$l_d^* = \sum_{k=0}^{n} s_{dk}x_k.$$

Так как пересечение $\mathfrak{M}^*$ с „несобственной плоскостью“ $\xi_0 = 0$ имеет измерение меньшее, чем $\mathfrak{M}^*$, то оно не имеет общих точек с $(n-d)$-мерным пространством L_{n-d}. Таким образом точками пересечения могут быть только точки, принадлежащие $\mathfrak{M}$, т. е. конечное число сопряженных точек.

Если $(f_1^*, \ldots, f_s^*)$ — идеал, принадлежащий $\mathfrak{M}^*$, причем f_ν^* согласно § 87 (задача 4) могут быть взяты однородными, то точки пересечения $\mathfrak{M}^*$ с L_{n-d}^* являются общими корнями форм

$$f_1^*, \ldots, f_s^*, l_1^*, \ldots, l_d^*. \tag{3}$$

Эти формы, будучи приравнены нулю, составят систему однородных уравнений, к которой можно применить теорию главы 11 (§ 76 и 79).

Следующие выводы, которые выяснят нам, что произойдет с решениями $\xi^{(\nu)}$ $(\nu = 1, \ldots, g)$ этой системы уравнений после замены параметров s_{ik} другими величинами σ_{ik} (из K или из поля расширения над K), базируются исключительно на общих свойствах системы однородных уравнений; поэтому эти выводы справедливы не только для системы (3), но также и для всякой системы форм, в которые кроме „неизвестных“ x или ξ входят еще неопределенные параметры s_{ik}.

Найдем для каждого частного значения $s_{ik} \to \sigma_{ik}$ такие точки $\eta^{(1)}, \ldots, \eta^{(g)}$, что *все алгебраические соотношения между величинами* s_{ik} и $\xi_i^{(\nu)}$, *однородные относительно ряда величин* $\left\{\xi_0^{(\nu)}, \ldots, \xi_n^{(\nu)}\right\}$, *переносятся также на величины* σ_{ik} и $\eta_l^{(\nu)}$. Иными словами: если для полинома $F(s_{ik}, x_i^{(\nu)})$, однородного относительно ряда $\left\{x_0^{(\nu)}, \ldots, x_n^{(\nu)}\right\}$ переменных, имеет место равенство

$$F\left(s_{ik}, \xi_i^{(\nu)}\right) = 0, \tag{4}$$

---

[1]) Точнее: изоморфизм

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_d) \simeq \mathsf{K}(s_{ik}, t_1, \ldots, t_r)$$

может быть расширен до изоморфизма

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_d, \xi_1, \ldots, \xi_n) \simeq \mathsf{K}(s_{ik}, t_1, \ldots, t_r, \xi_1^*, \ldots, \xi_n^*),$$

а ξ^* можно снова обозначить через ξ.

то мы хотим, чтобы также имело место

$$F\left(\sigma_{ik},\ \eta_i^{(\nu)}\right) = 0. \tag{5}$$

В частности, если бы это было справедливым для форм (3), то все $\eta^{(\nu)}$ были бы корнями форм (3) при частных значениях параметров.

Можно убедиться, что всегда существуют η, удовлетворяющие этому требованию. А именно среди форм F, обладающих свойством (4), мы можем в силу § 80 выбрать конечное число таких форм, от которых все остальные будут линейно зависеть (коэфициентами линейной зависимости будут формы). Следовательно, систему уравнений (4) можно заменить конечной системой. Исключая затем из этой системы уравнений последовательно величины $\xi^{(g)},\ \xi^{(g-1)},\ \ldots,\ \xi^{(1)}$ методом системы результантов (§ 76) (причем всякий раз будем иметь однородные уравнения), получим, наконец, уравнения, содержащие только s_{ik}. Эти уравнения должны удовлетворяться тождественно для s_{ik}. Отсюда следует, что уравнения удовлетворяются также при частных значениях $s_{ik} \to \sigma_{ik}$, а это значит, что система (5) решается относительно η.

Сделаем еще одно замечание: если исключены из (4) не все ξ, а только $\xi^{(g)},\ \xi^{(g-1)},\ \ldots,\ \xi^{(2)}$, то останутся s_{ik} и $\xi^{(1)}$. Теперь, если даны такие величины $\eta_i^{(1)}$, относительно которых известно, что все алгебраические соотношения, имеющие место между s_{ik} и $\xi_i^{(1)}$ и однородные относительно $\xi_i^{(1)}$, справедливы также для σ_{ik} и $\eta_i^{(1)}$, то можно определить так же, как и выше, такие $\eta^{(2)},\ \ldots,\ \eta^{(g)}$, чтобы снова удовлетворялись все уравнения (5) и вместе с тем выполнялось указанное выше требование. Это замечание мы используем несколько позже.

Приведенный выше метод устанавливает только существование величин η, но не определяет этих величин однозначно. Чтобы их найти, составим u-результант R_u (см. § 79) систем форм (3), т. е. общий наибольший делитель системы результантов форм (3) и общей линейной формы $u_x = u_0 x_0 + \ldots + u_n x_n$. Так как формы (3) имеют только конечное число общих корней, то в силу § 79 их u-результант R_u распадается на линейные множители, соответствующие этим корням $\xi^{(\nu)}$:

$$R_u\left(s_{ik},\ u_k\right) = c \prod_{\nu=1}^{g} \left(u_0 \xi_0^{(\nu)} + \ldots + u_n \xi_n^{(\nu)}\right)^{\rho_\nu} \quad (c \text{ — постоянная}). \tag{6}$$

Чтобы вывести из (6) соответствующее соотношение для η, мы должны прежде всего исключить постоянную c и сделать уравнение однородным. Это достигается следующим образом: пусть $a_1(s),\ \ldots,\ a_h(s)$ — коэфициенты произведения степеней u_k в левой части (6) и $cb_1(\xi),\ \ldots,\ cb_h(\xi)$ — соответствующие коэфициенты справа. Тогда при $i = 1, 2, \ldots, h$ должно быть $a_i(s) = cb_i(\xi)$, а это приводит к

$$a_i(s) b_k(\xi) - a_k(s)\ b_i(\xi) = 0 \quad (i,\ k = 1,\ \ldots,\ h).$$

Эти однородные уравнения сохраняются и при частных значениях

$$s_{ik} \to \sigma_{ik},\ \xi_i^{(\nu)} \to \eta_i^{(\nu)}.$$

Отсюда

$$a_i(\sigma)\, b_k(\eta) - a_k(\sigma)\ b_i(\eta) = 0;$$

следовательно, так как не все $b_i(\eta)$ равны нулю, то

$$a_i(\sigma) = \gamma b_i(\eta),$$

$$R_u\left(\sigma_{ik},\ u_k\right) = \gamma \prod_{\nu=1}^{g} \left(u_0 \eta_0^{(\nu)} + \ldots + u_n \eta_n^{(\nu)}\right)^{\rho_\nu}. \tag{7}$$

Если $R_u(\sigma, u)$ не обращается тождественно в нуль, то должно иметь место $\gamma \neq 0$. Тогда равенство (7) дает способ вычисления η: величины η найдутся при разложении на множители полинома $R_u(\sigma_{ik}, u_k)$. Вместе с тем отсюда следует, что η определяются однозначно до порядка следования; все это в предположении, что

R_u не исчезает тождественно. Последнее всегда имеет место, если полиномы (3) при частных значениях параметров имеют в P_n только конечное число общих корней. А именно, так как $R_u(s_{ik}, u_k)$ есть общий делитель системы результантов форм (3) и u_x, то $R_u(\sigma_{ik}, u_k)$ есть общий делитель системы результантов форм (3) и u_x при частных значениях параметров, а эта система результантов не обращается в нуль в случае конечного числа общих корней форм (3).

Таким образом мы должны исключить случай, когда частное линейное пространство L^*_{n-r} имеет бесконечное число точек, общих с $\mathfrak{M}^*$. Если существует только конечное число таких общих точек, то мы можем указанным методом *определить однозначно с точностью до порядка следования g точек пересечения $\eta^{(1)}, \ldots, \eta^{(g)}$, в которые*, как мы будем говорить, ξ *переходят при частных s_{ik}.*

Одна и та же точка пересечения η может несколько раз встречаться среди $\eta^{(\nu)}$. Число, указывающее, сколько раз встречается η среди $\eta^{(1)}, \ldots, \eta^{(g)}$, называется *кратностью* точки η как точки пересечения $\mathfrak{M}^*$ с L^*_{n-r}. *Сумма кратностей всех точек пересечения равна степени g*, как это сразу видно.

Возникает теперь следующий вопрос: существует ли точка пересечения кратности нуль, т. е. такая точка, которая не встречается среди $\eta^{(1)}, \ldots, \eta^{(g)}$? Для совершенно произвольной системы уравнений при соответствующем подборе частных значений параметров такие решения кратности нуль могут при случае встретиться [1]). Но мы покажем, что для нашей задачи (пересечение L^*_{n-r} и $\mathfrak{M}^*$) такие решения не могут иметь места, так что всякая наперед заданная точка пересечения η может быть принята за $\eta^{(1)}$.

Согласно сделанному выше (стр. 83) замечанию достаточно показать, что алгебраические соотношения $F\left(s_{ik}, \xi_i^{(1)}\right) = 0$, однородные относительно $\xi_i^{(1)}$, при частных значениях $s_{ik} \to \sigma_{ik}$, $\xi^{(1)} \to \eta$ остаются в силе. Пусть $\eta_0 \neq 0$, что всегда можно достигнуть соответствующей нумерацией координат; тогда можно положить $\xi_0^{(1)} = \eta_0 = 1$. Затем можно s_{i0} исключить из $F\left(s_{ik}, \xi_i^{(1)}\right)$ на основании соотношения

$$s_{i0} + \sum_{k=1}^{n} s_{ik}\xi_k^{(1)} = 0,$$

которое сохраняется и при частных значениях входящих в него величин; для этого достаточно s_{i0} заменить через $-\sum_{k=1}^{n} s_{ik}\xi_k^{(1)}$. Если считать s_{ik} $(k \neq 0)$ присоединенными к основному полю K, то $\xi^{(1)}$ будет общей точкой $\mathfrak{M}$ (см. начало этого параграфа), и всякое соотношение $F\left(\xi_i^{(1)}\right) = 0$, справедливое для общей точки $\xi^{(1)}$, справедливо также для любой частной точки η из $\mathfrak{M}$. Таким образом $F\left(s_{ik}, \eta_i\right) = 0$, а отсюда $F\left(\sigma_{ik}, \eta_i\right) = 0$, что и требовалось доказать. Итак, всякая точка пересечения $\mathfrak{M}^*$ и L^*_{n-d} обладает кратностью, отличной от нуля, и сумма этих кратностей, как мы уже заметили, равна степени $\mathfrak{M}^*$.

Эту же задачу можно решить совершенно иначе, а именно с помощью гильбертовских „характеристических функций". Об этом см., например, у B. L. v. d. Waerden, On Hilbert's function, Proc. Kon. Ak. Amsterdam, т. 31, стр. 749, 1928.

Задачи. 1. Пересечение d-мерного многообразия $\mathfrak{M}$ с общим L_{n-r} является в случае $r < d$ $(d-r)$-мерным многообразием той же степени, что и $\mathfrak{M}$.

2. Если пересечение d-мерного многообразия $\mathfrak{M}^*$ проективного пространства P_n с частным L_{n-r} $(r < d)$ имеет измерение, не превосходящее $d-r$, то неприводимым составным частям, на которые распадается это пересечение, можно приписать такие кратности, что сумма произведений кратностей на степени равна степени $\mathfrak{M}^*$ [надо пересечь всеобщим линейным пространством L_{n-d+r}].

---

[1]) См. B. L. v. d. Waerden, Der Multiplizitätsbegriff der algebraischen Geometrie, „Math. Ann.", т. 97, стр. 756—774, § 5.

ГЛАВА ЧЕТЫРНАДЦАТАЯ

ЦЕЛЫЕ АЛГЕБРАИЧЕСКИЕ ВЕЛИЧИНЫ

Исторически теория идеалов развилась из теории целых алгебраических чисел и теории полиномиальных идеалов. Эти две теории преследуют совершенно различные цели. В то время как центральной задачей полиномиальных идеалов является нахождение их корней и установление необходимых и достаточных условий принадлежности полинома идеалу, задачей теории целых алгебраических чисел является вопрос о разложении элемента на множители.

Например, в кольце величин $a+b\sqrt{-5}$, где a и b — целые рациональные числа, теорема об единственности разложения элемента на множители не выполняется. Так, число 9 допускает два существенно различных разложения:

$$9=3\cdot 3=(2+\sqrt{-5})\,(2-\sqrt{-5})$$

на неразложимые множители [1]). Это обстоятельство побудило Дедекинда расширить область элементов. Он первый ввел для этого понятие идеала. Дедекинду удалось затем показать, что в некоторой расширенной области элементов всякий идеал разлагается единственным образом на произведение простых идеалов [2]). (Куммер до Дедекинда добился однозначности разложения на множители в поле деления окружности, но для этого он ввел так называемые „идеальные числа".) В самом деле, обращаясь к приведенному выше примеру, имеем:

$$(3)=\mathfrak{p}_1\mathfrak{p}_2,$$

где

$$\mathfrak{p}_1=(3,\ 2+\sqrt{-5}),\ \mathfrak{p}_2=(3,\ 2-\sqrt{-5}),\ (2+\sqrt{-5})=\mathfrak{p}_1^2;$$

$$(2-\sqrt{-5})=\mathfrak{p}_2^2,$$

откуда получается для главного идеала (9) (единственное) разложение

$$9=\mathfrak{p}_1^2\,\mathfrak{p}_2^2.$$

---

[1]) Неразложимость чисел 3 и $2\pm\sqrt{-5}$ следует легко из того, что их норма (§ 35) равна 9. Если бы они были разложимы, то либо оба сомножителя имели бы норму, равную ± 3, либо один сомножитель имел бы норму, равную ± 1. Но число $a+b\sqrt{-5}$ не может иметь нормой ± 3, так как иначе имело бы место

$$a^2+5b^2=\pm 3,$$

что для целых значений a, b невозможно. Число, обладающее нормой ± 1, необходимо должно быть равно ± 1, так как

$$a^2+5b^2=\pm 1$$

удовлетворяется только при $a=\pm 1$, $b=0$.

[2]) Любопытно отметить, что в кольце чисел $a+b\sqrt{-3}$ (§ 17, задача 5) число 4 допускает два различных разложения; но здесь единственность разложения достигается присоединением

$$\rho=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$$

(см. § 16, задача 5). Однако для кольца $C[\sqrt{-5}]$, как мы увидим, подобное конечное расширение невозможно.

В этой главе будет изложена „классическая (дедекиндовская) теория идеалов целых величин поля с современной точки зрения, принадлежащей Э. Нётер [1]). При этом знание общей теории идеалов двенадцатой главы необязательно.

§ 97. КОНЕЧНЫЕ $\mathfrak{R}$-МОДУЛИ

Мы будем рассматривать модули относительно (необязательно коммутативного) кольца $\mathfrak{R}$, т. е. модули, для которых $\mathfrak{R}$ образует (левую) область операторов. При этом рассматриваемые модули мы будем предполагать содержащимися либо в самом $\mathfrak{R}$ (левые идеалы $\mathfrak{R}$), либо в кольце $\mathfrak{S}$ расширения.

Под *конечным* $\mathfrak{R}$-модулем подразумевается модуль $\mathfrak{M}$, порожденный конечным базисом $(a_1, \ldots, a_h)$; иными словами, элементы $\mathfrak{M}$ выражаются линейно через $a_1, \ldots, a_h$:

$$m = r_1 a_1 + \ldots + r_h a_h + n_1 a_1 + \ldots + n_h a_h \qquad (1)$$

$$(r_\nu \in \mathfrak{R},\ n_\nu \text{ — целые числа}).$$

(Если $\mathfrak{R}$ имеет единицу, то члены $n_1 a_1, \ldots, n_h a_h$ оказываются лишними.) В этом случае пишут: $\mathfrak{M} = (a_1, \ldots, a_h)$.

Говорят, что для модуля $\mathfrak{M}$ выполняется *постулат о цепях делителей*, если всякая последовательность подмодулей $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$, где $\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset, \ldots$, состоит из конечного числа различных членов.

Теорема. *Если для $\mathfrak{M}$ справедлив постулат о цепях делителей, то всякий подмодуль $\mathfrak{M}$ обладает конечным базисом, и обратно.*

Эта теорема представляет обобщение теоремы § 80 о базисе идеала и постулата о цепях делителей § 80 и доказывается точно так же. Однако, чтобы быть независимым от главы 12, приведем все же ее доказательство.

Чтобы найти базис подмодуля $\mathfrak{N}$, возьмем прежде всего элемент a_1 из $\mathfrak{N}$. Если $(a_1) = \mathfrak{N}$, то теорема доказана; если же $(a_1) \neq \mathfrak{N}$, то берем из $\mathfrak{N}$ элемент a_2, не содержащийся в (a_1). Если $(a_1, a_2) = \mathfrak{N}$, то все доказано; в противном случае берем a_3 и т. д. Так как последовательность модулей

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots$$

не бесконечна, то $\mathfrak{N}$ имеет конечный базис.

Обратно, если всякий подмодуль $\mathfrak{M}$ обладает конечным базисом и

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \ldots$$

последовательность подмодулей $\mathfrak{M}$, то объединение $\mathfrak{B}$ всех $\mathfrak{M}_\nu$ является также подмодулем, обладающим конечным базисом:

$$\mathfrak{B} = (a_1, \ldots, a_r).$$

Но все a_ν содержатся в одном из $\mathfrak{M}_\nu$ последовательности, например в $\mathfrak{M}_\omega$; поэтому $\mathfrak{B} \subseteq \mathfrak{M}_\omega$, откуда $\mathfrak{B} = \mathfrak{M}_\omega$. Таким образом последовательность заканчивается на $\mathfrak{M}_\omega$.

---

[1]) E. Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, Math. Ann., т. 96, стр. 26—61, 1926.

Нижеследующая теорема показывает, при каких условиях для $\mathfrak{M}$ имеет место постулат о цепях делителей:

Если в $\mathfrak{R}$ постулат о цепях делителей выполняется для левых идеалов и $\mathfrak{M}$ — конечный $\mathfrak{R}$-модуль, то в $\mathfrak{M}$ выполняется постулат о цепях делителей для $\mathfrak{R}$-модулей. Этому равносильно такое предложение (на основании предыдущей теоремы):

Если в $\mathfrak{R}$ любой левый идеал обладает конечным базисом и $\mathfrak{M}$ имеет конечный $\mathfrak{R}$-базис, то всякий подмодуль $\mathfrak{M}$ будет также иметь конечный $\mathfrak{R}$-базис.

Доказательство совершенно аналогично доказательству гильбертовской теоремы о базисе (§ 80). Пусть $\mathfrak{M}=(a_1, \ldots, a_h)$ и $\mathfrak{N}$ — подмодуль $\mathfrak{M}$. Элементы $\mathfrak{N}$ можно записать в виде (1). Если в выражении (1) среди $2h$ коэфициентов $r_1, \ldots, n_h$ последние $2h-l$ равны нулю, то мы будем говорить *о выражении с длиной* меньшей или равной l. Рассмотрим теперь все встречающиеся в $\mathfrak{N}$ выражения с длиной меньшей или равной l. Их l-е коэфициенты (r_l или n_{l-h}) образуют, как это легко видеть, левый идеал в $\mathfrak{R}$ или в кольце C целых чисел. Этот идеал обладает конечным базисом

$$(b_{l1}, \ldots, b_{ls_l}).$$

Каждое из $b_{l\nu}$ является последним (l-м) коэфициентом (r_l или n_{l-h}) некоторого определенного выражения (1), которое мы обозначим через $B_{l\nu}$:

$$B_{l\nu}=r_1a_1+\ldots.+b_{l\nu}a_l$$

или

$$=r_1a_1+\ldots+b_{l\nu}a_{l-h}.$$

Мы утверждаем, что все эти $B_{l\nu}$ ($l=1, \ldots, 2h, \nu=1, \ldots, s_l$) образуют базис $\mathfrak{N}$. В самом деле, если вычесть из элемента (1) длины l некоторую линейную комбинацию $B_{l1}, \ldots, B_{ls_l}$, то можно будет освободиться от его последнего (l-го) коэфициента, т. е. получим выражение меньшей длины; длину этого выражения можно снова уменьшить указанным способом, пока, наконец, не придем к нулю. Таким образом выходит, что всякий элемент $\mathfrak{N}$ записывается в виде линейной комбинации $B_{l\nu}$, что и требовалось доказать. Если один из идеалов $(b_{l1}, \ldots, b_{ls_l})=(0)$, то соответствующие $B_{l\nu}$ оказываются для базиса даже бесполезными.

Замечания. Если $\mathfrak{R}$ имеет единицу, которую можно рассматривать как единичный оператор, то в (1) можно снова опустить все члены $n_1a_1, \ldots, n_ha_h$; доказательство в соответствии с этим упрощается.

В частности, если $\mathfrak{R}$ — кольцо главных идеалов, то всякий идеал $\mathfrak{N}$ имеет базис, состоящий только из одного элемента; таким образом для каждого l будем иметь только одно b_l и B_l. В этом случае поэтому оказывается, что базис $(B_1, \ldots, B_h)$ содержит столько элементов, сколько их имеется в первоначальном базисе $\mathfrak{M}$. Если базис $(a_1, \ldots, a_h)$ модуля $\mathfrak{M}$ линейно независим, то очень легко показать, что базис $(B_1, \ldots, B_h)$ после устранения B_l, соответствующих $b_l=0$, также будет линейно независимым (см. § 106).

§ 98. ЦЕЛЫЕ ВЕЛИЧИНЫ ОТНОСИТЕЛЬНО КОЛЬЦА

Пусть $\mathfrak{R}$ есть подкольцо кольца $\mathfrak{T}$.

Элемент t кольца $\mathfrak{T}$ называется *целым относительно* $\mathfrak{R}$, если все степени [1]) t принадлежат конечному $\mathfrak{R}$-модулю $(a_1, \ldots, a_m)$. Иными словами, все степени t линейно выражаются через конечное число величин $a_1, \ldots, a_m$ из $\mathfrak{T}$:

$$t^\varrho = r_1 a_1 + \ldots + r_m a_m + n_1 a_1 + \ldots + n_m a_m \qquad (1)$$

$(r_\nu \in \mathfrak{R}$, n_ν — целые числа).

В частности, элемент r из $\mathfrak{R}$ является целым относительно $\mathfrak{R}$, так как $r, r^2, r^3, \ldots$ принадлежат $\mathfrak{R}$-модулю (r). Единица кольца $\mathfrak{T}$, если только она существует, есть всегда целая величина относительно $\mathfrak{R}$.

Если $\mathfrak{T}$ — поле, содержащее поле отношений $\mathbf{P}$ кольца $\mathfrak{R}$, то все степени целой величины t зависят линейно от конечного числа элементов $a_1, \ldots, a_m$ с коэфициентами из $\mathbf{P}$, так как $\mathbf{P}$ содержит не только кольцо $\mathfrak{R}$, но и единицу. Поэтому среди степеней t имеется только конечное число степеней, линейно независимых относительно $\mathbf{P}$; таким образом t есть алгебраический элемент относительно $\mathbf{P}$. Поэтому вместо „целые величины“ говорят также *„целые алгебраические величины“*. Однако не всякая алгебраическая величина является целой алгебраической; например, $\frac{1}{2}$ или $\sqrt{\frac{1}{2}}$ есть алгебраическое число относительно поля рациональных чисел, но не целое число относительно кольца целых чисел.

Если $\mathfrak{R}$ — кольцо, в котором удовлетворяется постулат о делителях для левых идеалов, то в силу § 97 постулат о цепи делителей будет справедлив также для подмодулей конечного $\mathfrak{R}$-модуля $(a_1, \ldots, a_m)$. В частности, последовательность модулей

$$(t) \subseteq (t, t^2) \subseteq \ldots$$

состоит из конечного числа различных членов; отсюда следует, что степень t линейно выражается через низшие степени:

$$t^h = r_1 t + \ldots + r_{h-1} t^{h-1} + n_1 t + \ldots + n_{h-1} t^{h-1}. \qquad (2)$$

Если, обратно, t есть элемент кольца $\mathfrak{T}$, для которого при соответствующих h имеет место представление вида (2), то можно все высшие степени величины t последовательно выразить линейно через конечное число степеней $t, t^2, \ldots, t^{h-1}$, откуда согласно нашему определению получается, что t есть целая величина. Итак, мы доказали следующую теорему:

Если в кольце $\mathfrak{R}$ *имеет место для левых идеалов постулат о цепях делителей, то наличие уравнения* (2) *является необходимым и достаточным, чтобы* t *было целым относительно* $\mathfrak{R}$.

---

[1]) В этом параграфе имеются в виду только степени с положительными показателями.

Если $\mathfrak{R}$ имеет единицу, то к степени t можно еще присоединить $t^0 = 1$, а в уравнении (2) отбросить $n_1 t + \ldots + n_{h-1} t^{h-1}$; таким образом вместо (2) получится более простое уравнение:

$$t^h - r_{h-1} t^{h-1} - \ldots - r_0 = 0,$$

характерная особенность которого состоит в том, что коэфициент при старшей степени t равен единице.

Примеры. *Целыми алгебраическими числами* называются такие алгебраические числа, которые являются целыми относительно кольца C обыкновенных целых чисел. Таким образом эти числа можно определить как корни уравнения с целыми коэфициентами и со старшим коэфициентом, равным единице. *Целые алгебраические функции* $x_1, \ldots, x_n$ это такие функции из алгебраического поля расширения $\mathsf{K}(x_1, \ldots, x_n)$, которые являются целыми относительно области $\mathsf{K}[x_1, \ldots, x_n]$ полиномов. *Абсолютно целыми алгебраическими функциями* $x_1, \ldots, x_n$ называются функции, целые относительно целочисленной области $C[x_1, \ldots, x_n]$ полиномов.

В коммутативном кольце $\mathfrak{T}$ *сумма, разность и произведение двух целых относительно* $\mathfrak{R}$ *величин — также целые величины.* Иными словами: *величины* $\mathfrak{T}$, *целые относительно* $\mathfrak{R}$, *образуют кольцо* $\mathfrak{S}$.

Доказательство. Если степени s, t линейно выражаются соответственно через $a_1, \ldots, a_m$ и $b_1, \ldots, b_n$, то степени $s+t$, $s-t$ или $s \cdot t$ будут линейно выражаться через $a_1, \ldots, a_m, b_1, \ldots, b_n, a_1 b_1, a_1 b_2, \ldots, a_m b_n$.

Если теперь ввести постулат о цепях делителей для идеалов кольца $\mathfrak{S}$, то можно будет высказать такую теорему:

Если $\mathfrak{S}$ *— кольцо целых (относительно подкольца* $\mathfrak{R}$*) величин, содержащихся в коммутативном кольце* $\mathfrak{T}$ *и элемент* t *из* $\mathfrak{T}$ *является целым относительно* $\mathfrak{S}$, *то* t*—также целое относительно* $\mathfrak{R}$ *(т. е. содержится в* $\mathfrak{S}$*). Или, выражаясь иначе: если* t *удовлетворяет уравнению вида (2), коэфициенты которого* r_ν*—целые относительно* $\mathfrak{R}$, *то само* t*—целое относительно* $\mathfrak{R}$.

Доказательство. Применяя несколько раз уравнение (2), мы выразим линейно все степени $t^{h+\lambda}$ через $t, t^2, \ldots, t^{h-1}$, причем коэфициенты линейной зависимости будут либо целыми числами, либо целыми рациональными функциями от произведений степеней r_ν. Для каждого r_ν существует конечное число величин из $\mathfrak{T}$, через которые линейно выражаются степени r_ν с коэфициентами из $\mathfrak{R}$ и с целочисленными коэфициентами; таким образом все произведения степеней r_ν выражаются линейно через конечное число произведений этих величин. Если умножим эти последние произведения на $t, t^2, \ldots, t^{h-1}$ и присоединим еще $t, t^2, \ldots, t^{h-1}$, то получим снова конечное число величин, через которые линейно выражаются все степени t с целыми коэфициентами и с коэфициентами из $\mathfrak{R}$.

Кольцо $\mathfrak{S}$ называется *целозамкнутым в надкольце* $\mathfrak{T}$, если всякая величина $\mathfrak{T}$, целая относительно $\mathfrak{S}$, принадлежит $\mathfrak{S}$. В частности, область целостности $\mathfrak{S}$ называется *всюду целозамкнутой*, если она целозамкнута в своем поле отношений Σ. Легко видеть, что в этом случае элемент t поля Σ, все степени t^ρ которого выражаются дробью

с одним и тем же знаменателем из $\mathfrak{S}$, принадлежит $\mathfrak{S}$. Величины, от которых зависят все степени целого t, всегда можно привести к общему знаменателю, так как этих величин конечное число. Если, обратно, все степени t представляются дробями с знаменателем s, то все они выражаются линейно через s^{-1}.

Теперь из предыдущей теоремы вытекает, что в случае коммутативности $\mathfrak{T}$ кольцо $\mathfrak{S}$ величин из $\mathfrak{T}$, *целых относительно* $\mathfrak{R}$, *целозамкнуто в* $\mathfrak{T}$ [1]), *если только имеет место постулат о цепях делителей для идеалов* $\mathfrak{S}$.

Нижеследующая теорема приводит к достаточному, но не необходимому критерию целозамкнутости области целостности:

Область целостности с единицей, в которой выполняется теорема об однозначном разложении на простые множители, целозамкнута в своем поле отношений.

Доказательство. Элемент поля отношений можно представить в виде дроби $\frac{a}{b}$, где a и b не имеют общего простого множителя. Если все степени дроби $\frac{a}{b}$ можно освободить от знаменателей, умножив на некоторую величину c, то ca^n, а потому и c должны делиться на b^n для всякого n, что возможно только в том случае, когда b есть делитель единицы; поэтому $\frac{a}{b} = ab^{-1}$ принадлежит области целостности.

Из теоремы следует, что кольцо главных идеалов (в частности кольцо C целых чисел), а также целочисленная область полиномов и любая область полиномов относительно коммутативного поля целозамкнуты.

Задачи. 1. Корни из единицы поля всегда целые относительно любого подкольца.

2. Какие числа гауссовского числового поля $\Gamma(i)$ являются целыми относительно C? Какие числа поля $\Gamma(\rho)$ кубичных корней из единицы $\left(\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right)$ являются целыми?

3. Если область целостности $\mathfrak{R}$ целозамкнута, то область полиномов $\mathfrak{R}[x]$ также целозамкнута.

§ 99. ЦЕЛЫЕ ВЕЛИЧИНЫ ПОЛЯ

Пусть $\mathfrak{R}$ — область целостности, P — ее поле отношений, Σ — коммутативное конечное поле расширения P и $\mathfrak{S}$ — кольцо целых относительно $\mathfrak{R}$ величин Σ. Очевидно, что $\mathfrak{S}$ есть кольцо расширения об-

---

[1]) Эту теорему можно доказать и в том случае, если вместо постулата о цепи делителей предположить, что $\mathfrak{R}$ целозакнуто в своем поле отношений P и $\mathfrak{T}$ — конечное поле расширения P. Для доказательства следует $\mathfrak{T}$ расширить до поля Галуа $\mathfrak{T}'$ относительно P, а $\mathfrak{S}$ — до кольца $\mathfrak{S}'$ целых величин $\mathfrak{T}'$. Если элемент t является целым относительно $\mathfrak{S}$, то он будет целым относительно $\mathfrak{S}'$, и величины, сопряженные t (относительно P), а потому также элементарные симметрические функции этих сопряженных величин будут целыми относительно $\mathfrak{S}'$, т. е. коэфициенты уравнения, определяющего t, суть целые величины. Но тогда в силу целозамкнутости $\mathfrak{R}$ эти коэфициенты должны принадлежать $\mathfrak{R}$, откуда t является целым относительно $\mathfrak{R}$ и $t \in \mathfrak{S}$.

ласти $\mathfrak{R}$. Схематически связь между кольцами $\mathfrak{R}$, $\mathfrak{S}$ и полями P, Σ можно записать так:

$$\begin{array}{ccc} \mathfrak{R} & \subset & \mathfrak{S} \\ \cap & & \cap \\ \mathsf{P} & \subset & \Sigma. \end{array}$$

На протяжении настоящего параграфа все эти соотношения будут сохраняться. Вместо термина „целый относительно $\mathfrak{R}$“ будет употребляться просто термин „целый“.

Примеры. Если $\mathfrak{R}$ есть кольцо обыкновенных целых чисел, то P — поле рациональных чисел, Σ — числовое поле (конечное относительно P) и $\mathfrak{S}$ — кольцо целых алгебраических чисел поля Σ.

Если $\mathfrak{R}$ есть область полиномов: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, то P есть поле рациональных функций, Σ получается присоединением конечного числа алгебраических функций, а $\mathfrak{S}$ состоит из целых алгебраических функций поля Σ и т. д.

Основной целью является изучение теории идеалов в $\mathfrak{S}$. Возникает вопрос, будет ли постулат о цепях делителей распространяться на $\mathfrak{S}$, если он справедлив для $\mathfrak{R}$. Согласно теоремам § 97 на этот вопрос можно ответить утвердительно в том случае, если удастся найти для $\mathfrak{S}$ $\mathfrak{R}$-базис. Таким образом эта задача будет нашей ближайшей целью.

Выскажем прежде всего такую вспомогательную теорему:

Если σ есть *элемент* из Σ, *то* $\sigma = \frac{s}{r}$, *где* $s \in \mathfrak{S}$, $r \in \mathfrak{R}$.

Доказательство. Элемент σ удовлетворяет уравнению с коэфициентами из P. Эти коэфициенты дробны относительно $\mathfrak{R}$. Умножив их на произведение знаменателей, получим величины из $\mathfrak{R}$:

$$r_0\sigma^m + r_1\sigma^{m-1} + \ldots + r_m = 0.$$

Если положить $r_0 = r$ и умножить на r^{m-1}, то получится:

$$(r\sigma)^m + r_1(r\sigma)^{m-1} + r_2 r(r\sigma)^{m-2} + \ldots + r_m r^{m-1} = 0.$$

Таким образом мы видим, что $r\sigma$ — целое относительно $\mathfrak{R}$. Если положим $r\sigma = s$, то теорема будет доказана.

Из этой теоремы вытекает, что Σ есть поле отношений кольца $\mathfrak{S}$.

Если элемент ξ *является целым, то все элементы, сопряженные* ξ (*в поле* Ω *расширения* Σ, *причем* Ω *есть поле Галуа относительно* P), *будут целыми.*

Доказательство. Конечное множество величин Σ, через которые по предположению линейно выражаются степени ξ, переходит при некотором изоморфизме Σ в другое конечное множество величин, от которых линейно зависят степени элемента, сопряженного ξ.

Так как сумма и произведение целых величин также целые, то элементарные симметрические функции ξ и его сопряженных суть целые. От-

сюда следует, что *если целая величина* ξ *удовлетворяет уравнению, неприводимому в* P *и со старшим коэфициентом, равным единице, то все остальные коэфициенты должны быть целыми относительно* $\mathfrak{R}$. *В частности, если* $\mathfrak{R}$ *целозамкнуто в* P, *то все эти коэфициенты лежат в* $\mathfrak{R}$.

Таким образом, когда $\mathfrak{R}$ целозамкнуто, с помощью этой теоремы легко установить, является ли данная величина ξ целой: для этого нет надобности рассматривать все уравнения, которым удовлетворяет ξ, и искать среди них уравнение с целыми коэфициентами; достаточно взять неприводимое уравнение со старшим коэфициентом, равным единице. Если его коэфициенты целые, то ξ также целое; в противном случае ξ не будет целым.

Теперь введем следующие ограничения:

I. $\mathfrak{R}$ *целозамкнуто в своем поле отношений* P.

II. *В* $\mathfrak{R}$ *выполняется постулат о цепях делителей для идеалов.*

III. Σ *есть расширение первого рода поля* P.

В силу § 34 из III вытекает, что Σ порождается „примитивным элементом" σ, а именно $\Sigma = \mathsf{P}(\sigma)$.

Согласно высказанной выше теореме $\sigma = \frac{s}{r}$ $(s \in \mathfrak{S},\ r \in \mathfrak{R})$; таким образом целая величина s порождает также поле. s удовлетворяет уравнению n-й степени, где n — степень $\left(\frac{\Sigma}{\mathsf{P}}\right)$ поля. Всякий элемент ξ поля Σ можно представить в виде суммы:

$$\xi = \sum_{0}^{n-1} \rho_k s^k \quad (\rho_k \in \mathsf{P}). \tag{1}$$

Заменяя в (1) s его сопряженными s_ν (s_ν лежат в некотором поле, которое содержит Σ и является полем Галуа относительно P), получим уравнения:

$$\xi_\nu = \sum_{0}^{n-1} \rho_k s_\nu^k \qquad (\nu = 1,\ 2,\ \ldots,\ n). \tag{2}$$

Согласно § 34 должно быть всего n сопряженных. Определитель этой системы уравнений равен:

$$D = |s_\nu^k| = \prod_{\lambda<\mu} (s_\lambda - s_\mu),$$

так как D — определитель Вандермонда. Его квадрат есть симметрическая функция от s_ν и потому содержится в P. Так как сопряженные s_ν все различны, то $D \neq 0$. Отсюда следует, что система уравнений (2) разрешима:

$$\rho_k = \frac{\sum S_{k\nu}\, \xi_\nu}{D},$$

где $S_{k\nu}$ и D — полиномы от s_ν; поэтому $S_{k\nu}$ и D целы относительно $\mathfrak{R}$

Умножив это уравнение на D^2, получим:

$$D^2\rho_k = \sum_{\nu} DS_{k\nu}\xi_\nu . \tag{3}$$

Теперь пусть ξ — элемент $\mathfrak{S}$, т. е. ξ является целым. Тогда ξ_ν и тем самым правая часть (3) будут также целыми Но левая часть есть элемент P. Таким образом, согласно целозамкнутости $\mathfrak{R}$ в P, $D^2\rho_k$ должно лежать в $\mathfrak{R}$. Если положить $D^2\rho_k = r_k$, то будем иметь $\rho_k = r_k D^{-2}$, а потому из (1) вытекает, что

$$\xi = \sum_{0}^{n-1} r_k D^{-2} s^k.$$

Любой элемент ξ кольца $\mathfrak{S}$ линейно выражается через $D^{-2}s^0$, $D^{-2}s^1$, ..., $D^{-2}s^{n-1}$ с коэфициентами из $\mathfrak{R}$.

Иными словами: $\mathfrak{S}$ содержится в конечном $\mathfrak{R}$-модуле

$$\mathfrak{M} = (D^{-2}s^0,\ D^{-2}s^1, \ldots, D^{-2}s^{n-1}).$$

Отсюда в силу теорем § 97 следует, *что* $\mathfrak{S}$, *а также всякий подмодуль кольца* $\mathfrak{S}$ *и в частности всякий идеал кольца* $\mathfrak{S}$ *обладают конечным базисом относительно* $\mathfrak{R}$ *или, что одно и то же, что для* $\mathfrak{R}$*-модулей и в частности для идеалов кольца* $\mathfrak{S}$ *выполняется постулат о цепях делителей.* Если $\mathfrak{R}$—кольцо главных идеалов, то $\mathfrak{S}$ и любой подмодуль $\mathfrak{S}$ обладают даже линейно независимым $\mathfrak{R}$-базисом.

К тому же результату мы придем даже и тогда, если III не будет иметь места, а именно если Σ есть расширение второго рода (с характеристикой p), причем предполагается, что кольцо корней $\mathfrak{R}^{\frac{1}{p^1}}$), содержащее корни p-й степени из элементов $\mathfrak{R}$, конечно относительно $\mathfrak{R}$. Это ограничение встречается во всех практически интересных случаях. Например, если $\mathfrak{R}$ — область полиномов: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, а K получено из простого поля Π присоединением конечного числа алгебраических или трансцендентных величин $\vartheta_1, \ldots, \vartheta_r$:

$$\mathsf{K} = \Pi(\vartheta_1, \ldots, \vartheta_r),$$

то

$$\mathfrak{R}^{\frac{1}{p}} = \mathsf{K}^{\frac{1}{p}}\left[x_1^{\frac{1}{p}}, \ldots, x_n^{\frac{1}{p}}\right] =$$

$$= \Pi\left(\vartheta_1^{\frac{1}{p}}, \ldots, \vartheta_r^{\frac{1}{p}}\right)\left[x_1^{\frac{1}{p}}, \ldots, x_n^{\frac{1}{p}}\right].$$

Таким образом $\mathfrak{R}^{\frac{1}{p}}$ имеет конечный $\mathfrak{R}$-базис, состоящий из элементов

$$\vartheta_1^{\alpha_1 : p}, \ldots, \vartheta_r^{\alpha_r : p},\ x_1^{\beta_1 : p}, \ldots, x_n^{\beta_n : p}\ \begin{pmatrix} 0 \leqslant \alpha_i < p, \\ 0 \leqslant \beta_k < p \end{pmatrix}.$$

Если вместо III ввести это условие конечности, то конечность $\mathfrak{S}$ докажется следующим образом.

[1]) Это кольцо определяется совершенно так же, как поле корней в § 33.

Прежде всего из конечности $\mathfrak{R}^{1:p}$ относительно $\mathfrak{R}$ следует в силу изоморфизма $\mathfrak{R} \simeq \mathfrak{R}^{1:p}$ (см. § 33), что $\mathfrak{R}^{1:p^2}$ тоже конечно относительно $\mathfrak{R}^{1:p}$ и т. д. Продолжая подобным образом, мы, наконец, получим, что $\mathfrak{R}^{1:p^e}$ конечно относительно $\mathfrak{R}$.

Теперь пусть Δ — наибольшее расширение поля P первого рода, которое содержится в Σ. Пусть e — показатель Σ. Тогда Σ лежит между Δ и $\Delta^{1:p^e}$.

Если $\mathfrak{D}$ — кольцо целых величин Δ, то $\mathfrak{D}^{1:p^e}$ будет кольцом целых величин $\Delta^{1:p^e}$, так как элемент $\Delta^{1:p^e}$ тогда и только тогда является целым, если его p^e-я степень целая. Поэтому кольцо $\mathfrak{S}$ лежит между $\mathfrak{D}$ и $\mathfrak{D}^{1:p^e}$. $\mathfrak{D}$ конечно относительно $\mathfrak{R}$, как расширение первого рода. В силу изоморфизма

$$\mathfrak{D} \simeq \mathfrak{D}^{1:p^e}.$$

$\mathfrak{D}^{1:p^e}$ конечно относительно $\mathfrak{R}^{1:p^e}$. Но $\mathfrak{R}^{1:p^e}$ по предположению конечно относительно $\mathfrak{R}$; поэтому $\mathfrak{D}^{1:p^e}$ конечно относительно $\mathfrak{R}$. Таким образом, как и прежде, $\mathfrak{S}$ заключается в конечном $\mathfrak{R}$-модуле, а потому становятся справедливыми все наши прежние выводы.

Под *$\mathfrak{R}$-порядком* в Σ подразумевается подкольцо от Σ, которое содержит $\mathfrak{R}$ и образует конечный $\mathfrak{R}$-модуль. По вышеизложенному $\mathfrak{S}$ и всякое кольцо между $\mathfrak{S}$ и $\mathfrak{R}$ образуют $\mathfrak{R}$-порядок. Обратно, из определения целого элемента сразу следует, что всякий $\mathfrak{R}$-порядок кольца Σ в Σ содержит только целые величины, т. е. содержится в $\mathfrak{S}$. Поэтому $\mathfrak{S}$ можно охарактеризовать как максимальный $\mathfrak{R}$-порядок в Σ. $\mathfrak{S}$ называется также *главным порядком* поля Σ. Если речь идет об „идеалах поля", „делителей единиц поля" и т. д., то под этим разумеются идеалы $\mathfrak{S}$, делители единицы $\mathfrak{S}$ и т. д. Согласно § 98 $\mathfrak{S}$ целозамкнуто в Σ.

Большинство результатов настоящего параграфа остается в силе и в том случае, когда Σ не поле, а коммутативная гиперкомплексная система относительно P. Эту систему можно представить в виде суммы полей, которые при умножении взаимно уничтожаются. Но наши результаты уже неприменимы к некоммутативной гиперкомплексной системе относительно P, а именно все зло в том, что сумма двух целых величин здесь уже не всегда является целой. Поэтому совокупность целых величин не образует порядка; хотя всякий порядок состоит из целых величин, но главного порядка, содержащего все порядки, не существует. При некоторых ограничениях, налагаемых на Σ, получаются различные максимальные $\mathfrak{R}$-порядки такого рода, что любой целый элемент содержится по крайней мере в одном из максимальных $\mathfrak{R}$-порядков. (См. об этом у L. E. Dickson, Algebras and their Arithmetics, Chicago 1923; E. Artin, Zur Arithmetik der hyperkomplexen Systeme, Abh. Math. Sem. Hamburg, т. 5, стр. 261—289, 1927; H. Brandt, Zur Idealtheorie Dedekindscher Algebren, Commentarii Mathematici Helvetici, т. 2, стр. 13—17, 1930.)

Согласно вышедоказанному во всех $\mathfrak{R}$-порядках Σ выполняется постулат о цепях делителей. Поэтому для этих порядков имеют место также теоремы разложения и единственности разложения § 83 и 84 (представление идеалов в виде пересечения примарных идеалов).

Эта теория идеалов значительно упрощается в том случае, когда всякий простой идеал, отличный от нуля, порядка $\mathfrak{o}$ свободен от делителей (см. § 86, конец). Следующая теорема показывает, когда это имеет место:

Если в $\mathfrak{R}$ всякий простой идеал, не равный нулю, свободен от делителей, то в любом $\mathfrak{R}$-порядке $\mathfrak{o}$ простой идеал, отличный от нуля, также свободен от делителей.

Доказательство. Пусть $\mathfrak{p}$ — простой идеал в $\mathfrak{o}$, содержащий элемент t, отличный от нуля. t удовлетворяет уравнению с коэфициентами из $\mathfrak{R}$ и со старшим коэфициентом, равным единице. Возьмем такое уравнение наинизшей степени:

$$t^h + a_1 t^{h-1} + \ldots + a_h = 0,$$

в котором $a_h \not\equiv 0$, так как в противном случае все уравнение можно было бы сократить на t. Отсюда имеем, что $a_h \equiv 0\,(t) \equiv 0\,(\mathfrak{p})$; таким образом a_h принадлежит пересечению $\mathfrak{p} \cap \mathfrak{R}$. Это пересечение образует простой идеал в $\mathfrak{R}$, так как если произведение двух элементов $\mathfrak{R}$ принадлежит $\mathfrak{R} \cap \mathfrak{p}$, т. е. $\mathfrak{p}$, то один из сомножителей должен принадлежать $\mathfrak{p}$; но тогда этот сомножитель принадлежит $\mathfrak{R} \cap \mathfrak{p}$. Так как a_h принадлежит простому идеалу $\mathfrak{R} \cap \mathfrak{p}$, то этот простой идеал отличен от нуля и потому свободен от делителей.

Если теперь $\mathfrak{a}$ — собственный делитель $\mathfrak{p}$, u — элемент $\mathfrak{a}$, не принадлежащий $\mathfrak{p}$, то u также удовлетворяет уравнению

$$u^l + b_1 u^{l-1} + \ldots + b_l = 0,$$

откуда должно удовлетворяться сравнение

$$u^k + c_1 u^{k-1} + \ldots + c_k \equiv 0\,(\mathfrak{p})$$

наинизшей степени. В этом сравнении опять должно быть $c_k \not\equiv 0\,(\mathfrak{p})$, так как в противном случае сравнение можно было сократить на u. Теперь получается, что $c_k \equiv 0\,(u) \equiv 0\,(\mathfrak{a})$, т. е. c_k принадлежит пересечению $\mathfrak{a} \cap \mathfrak{R}$, но не пересечению $\mathfrak{p} \cap \mathfrak{R}$. Следовательно, это пересечение $\mathfrak{a} \cap \mathfrak{R}$ есть собственный делитель $\mathfrak{p} \cap \mathfrak{R}$ и потому равно единичному идеалу $\mathfrak{R}$. Отсюда $\mathfrak{a}$ содержит единицу, а потому $\mathfrak{a} = \mathfrak{o}$, что и требовалось доказать.

В частности условия этой теоремы выполняются тогда, если $\mathfrak{R}$ есть кольцо главных идеалов (кольцо целых чисел, область полиномов одного переменного). В этом случае для $\mathfrak{o}$ имеет место теорема о том, что всякий идеал, отличный от нулевого и единичного идеалов, разлагается однозначно на произведение взаимно простых примарных идеалов, не равных $\mathfrak{o}$.

Но для главного порядка $\mathfrak{S}$, как мы увидим ниже, справедливо не только это. Оказывается, что в $\mathfrak{S}$ примарные идеалы равны степени простых идеалов; таким образом выходит, что *всякий идеал есть произведение степеней простых идеалов*. Ниже мы приводим непосредственное доказательство этого основного результата „классической" дедекиндовской теории идеала, свободное от понятия примарного идеала. Это будет сделано в следующем параграфе методом, предложенным В. Круллем [1]).

Задачи. 1. Если $\mathfrak{R}$ — кольцо главных идеалов, $(\omega_1, \ldots, \omega_n)$ — линейно независимый базис порядка $\mathfrak{o}$, который в этом случае всегда существует,

---

[1]) W. Krull, Zur Theorie der allgemeinen Zahlringe, Math. Ann., т 99 стр. 51—70, 1928.

и $(\omega_1^{(i)}, \ldots, \omega_n^{(i)})$ — сопряженный базис в поле Галуа расширения P, то дискриминант поля

$$D = \begin{vmatrix} \omega_1^{(1)} & \ldots & \omega_n^{(1)} \\ \cdot & \cdot & \cdot \\ \omega_1^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}^2$$

является целым, рациональным и отличным от нуля.

2. Пусть $\Sigma = \mathsf{P}(\sqrt{d})$ и $\mathfrak{R}$ целозамкнуто в P. Доказать, что целыми относительно $\mathfrak{R}$ могут быть только такие числа $\xi = a + b\sqrt{d}$, норма и след которых:

$$S(\xi) = \xi + \xi' = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a,$$
$$N(\xi) = \xi \cdot \xi' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

принадлежат $\mathfrak{R}$.

3. Если в задаче 2 $\mathfrak{R}$ есть область $\mathsf{K}[x]$ полиномов одного неизвестного и d — полином, не содержащий кратных множителей, то $\xi = a + b\sqrt{d}$ только тогда целое, если a и b принадлежат $\mathfrak{R}$.

4. Если в задаче 2 $\mathfrak{R}$ есть кольцо C целых чисел и d — целое число, свободное от квадратов, то базис главного порядка в случае $d \not\equiv 1\ (4)$ состоит из чисел $1, \sqrt{d}$; в случае же $d \equiv 1\ (4)$ базис состоит из чисел $1, \frac{1+\sqrt{d}}{2}$.

§ 100. АКСИОМАТИЧЕСКОЕ ОБОСНОВАНИЕ КЛАССИЧЕСКОЙ ТЕОРИИ ИДЕАЛОВ

Пусть $\mathfrak{o}$ — область целостности (коммутативное кольцо без делителей нуля), в которой выполняются следующие три аксиомы:

I. Постулат о цепи делителей для идеалов.

II. Все простые идеалы, отличные от нулевого идеала (0), свободны от делителей.

III. $\mathfrak{o}$ целозамкнуто в поле отношений Σ.

В качестве примеров колец подобного рода можно привести: 1) кольцо главных идеалов; 2) главный порядок, который получается при конечном расширении поля отношений кольца главных идеалов по схеме § 99 (в частности, так получаются главные порядки в числовом поле и в поле функций одного переменного).

Элементы Σ, целые относительно $\mathfrak{o}$, которые лежат согласно III в $\mathfrak{o}$, будут называться просто *целыми*. В частности, единица Σ всегда целая; поэтому $\mathfrak{o}$ — область целостности с единицей.

Рассмотрим теперь вместе с идеалами $\mathfrak{o}$ (или $\mathfrak{o}$-модулями в $\mathfrak{o}$) еще $\mathfrak{o}$-*модули* в Σ, т. е. такие подмножества от Σ, которые вместе с a и b содержат также $a - b$ и ra (где r — целое). Если такой $\mathfrak{o}$-модуль имеет конечный базис, то его называют также *дробным идеалом*. Если $\mathfrak{o}$-модуль $\mathfrak{a}$ состоит только из целых величин ($\mathfrak{a} \subseteq \mathfrak{o}$), то он является идеалом в обычном смысле или, как мы теперь будем говорить, *целым идеалом*.

Под *суммой* или общим наибольшим делителем $(\mathfrak{a}, \mathfrak{b})$ двух $\mathfrak{o}$-модулей $\mathfrak{a}$ и $\mathfrak{b}$ мы подразумеваем (как и для идеалов) модуль, состоящий из

всех сумм $a+b$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Точно так же под произведением $\mathfrak{ab}$ подразумевается модуль, порожденный всеми произведениями ab, или совокупность всех сумм $\Sigma a_\nu b_\nu$.

Суммы и произведения $\mathfrak{o}$-модулей с конечным базисом также имеют конечный базис.

В нижеследующих теоремах готическими буквами мы будем обозначать исключительно *целые идеалы в* $\mathfrak{o}$, *отличные от нулевого идеала* (0), а буквой $\mathfrak{p}$ — всегда *простой идеал*, не равный нулю.

Лемма 1. *Для всякого идеала* $\mathfrak{a}$ *существует такое произведение простых идеалов* $\mathfrak{p}_i$, *делителей* $\mathfrak{a}$, *которое делится на* $\mathfrak{a}$:

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0 \ (\mathfrak{a})\ ^{1}).$$

Первое доказательство. Если считать известной теорему о разложении (§ 83), то

$$\mathfrak{a} = [\mathfrak{q}_1, \dots, \mathfrak{q}_s],$$

$$\mathfrak{p}_i^{\varrho_i} \equiv 0 \ (\mathfrak{q}_i),$$

$$\prod_1^s \mathfrak{p}_i^{\varrho_i} \equiv 0 \ ([\mathfrak{q}_1, \dots, \mathfrak{q}_s]) \equiv 0 \ (\mathfrak{a}).$$

Второе доказательство. Можно, не обращаясь к примарным идеалам, доказать лемму следующим образом.

Если $\mathfrak{a}$ — простой идеал, то лемма очевидна. Если $\mathfrak{a}$ — не простой идеал, то существует такое произведение $\mathfrak{bc}$ двух главных идеалов, что

$$\mathfrak{bc} \equiv 0 \ (\mathfrak{a}), \ \mathfrak{b} \not\equiv 0 \ (\mathfrak{a}), \ \mathfrak{c} \not\equiv 0 \ (\mathfrak{a}).$$

Идеалы $\mathfrak{b}' = (\mathfrak{b}, \mathfrak{a})$, $\mathfrak{c}' = (\mathfrak{c}, \mathfrak{a})$ являются собственными делителями $\mathfrak{a}$ и

$$\mathfrak{b}'\mathfrak{c}' = (\mathfrak{b}, \mathfrak{a}) \cdot (\mathfrak{c}, \mathfrak{a}) = (\mathfrak{bc}, \mathfrak{ba}, \mathfrak{ac}, \mathfrak{a}^2) \equiv 0 \ (\mathfrak{a}, \mathfrak{a}, \mathfrak{a}, \mathfrak{a}) \equiv 0 \ (\mathfrak{a}).$$

Если считать теорему справедливой для идеалов $\mathfrak{b}'$ и $\mathfrak{c}'$, то существует произведение $\mathfrak{p}_1 \dots \mathfrak{p}_s \equiv 0 \ (\mathfrak{b}')$ и другое произведение $\mathfrak{p}_{s+1} \dots \mathfrak{p}_r \equiv 0 \ (\mathfrak{c}')$. Тогда произведение $\mathfrak{p}_1 \dots \mathfrak{p}_s \mathfrak{p}_{s+1} \dots \mathfrak{p}_r \equiv 0 \ (\mathfrak{b}' \cdot \mathfrak{c}') \equiv 0 \ \mathfrak{a})$, а потому теорема верна для $\mathfrak{a}$. Если бы теорема не была верна для $\mathfrak{a}$, то она также не имела бы места для собственных делителей $\mathfrak{b}'$ и $\mathfrak{c}'$; для $\mathfrak{b}'$ и $\mathfrak{c}'$ подобным же образом получили бы собственный делитель, для которого теорема несправедлива, и т. д.; таким образом мы бы имели бесконечную последовательность собственных делителей, что противоречит аксиоме 1. Отсюда следует справедливость теоремы для любого идеала $\mathfrak{a}$.

Лемма 2. *Если* $\mathfrak{p}$ — *простое, то из* $\mathfrak{ab} \equiv 0 \ (\mathfrak{p})$ *следует, что* $\mathfrak{a} \equiv 0 \ (\mathfrak{p})$ *или* $\mathfrak{b} \equiv 0 \ (\mathfrak{p})$ [2]).

Доказательство. Если бы $\mathfrak{a} \not\equiv 0 \ (\mathfrak{p})$ и $\mathfrak{b} \not\equiv 0 \ (\mathfrak{p})$, то существовали бы элементы a из $\mathfrak{a}$ и b из $\mathfrak{b}$, не содержащиеся в $\mathfrak{p}$. Тогда произведение ab лежало бы в $\mathfrak{ab}$, т. е. в $\mathfrak{p}$, что противоречит свойствам простого идеала $\mathfrak{p}$.

Обозначим через $\mathfrak{p}^{-1}$ совокупность (целых или дробных) величин a, для которых $a\mathfrak{p}$ является целым [3]). Очевидно, что $\mathfrak{p}^{-1}$ есть $\mathfrak{o}$-модуль.

---

[1]) Лемма основана исключительно на постулате о цепях делителей.

[2]) См. § 82.

[3]) $a\mathfrak{p}$ — это совокупность всех произведений ac, где $c \in \mathfrak{p}$.

Лемма 3. *Если* $\mathfrak{p} \neq \mathfrak{o}$, *то* $\mathfrak{p}^{-1}$ *содержит не целый элемент.*

Доказательство. Пусть c — произвольный элемент $\mathfrak{p}$, отличный от нуля. Согласно лемме 1 существует произведение простых идеалов

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0\,(c).$$

Можно предположить, что это произведение несократимо, т. е. что никакая часть произведения, как, например, $\mathfrak{p}_2 \dots \mathfrak{p}_r$, не сравнима с нулем по модулю c. Так как $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$ делится на $\mathfrak{p}$, то на $\mathfrak{p}$ должен делиться один из сомножителей, например $\mathfrak{p}_1$, и потому $\mathfrak{p}_1$ должно быть равно $\mathfrak{p}$.

Следовательно,

$$\mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0\,(c),$$
$$\mathfrak{p}_2 \dots \mathfrak{p}_r \not\equiv 0\,(c).$$

Таким образом в $\mathfrak{p}_2 \dots \mathfrak{p}_r$ существует элемент b, не принадлежащий (c). Для этого элемента

$$\mathfrak{p}b \equiv 0\,(\mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r) \equiv 0\,(c)\ ^{1}).$$

Отсюда вытекает, что $\mathfrak{p}\,\frac{b}{c}$ является целым; поэтому $\frac{b}{c}$ лежит в $\mathfrak{p}^{-1}$. Но в силу $b \not\equiv 0\,(c)$ $\frac{b}{c}$ не может быть целым, что и требовалось доказать.

Теорема 1. *Если* $\mathfrak{p} \neq \mathfrak{o}$, *то*

$$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}.$$

Доказательство. По определению $\mathfrak{p}^{-1}$, $\mathfrak{o} \subseteq \mathfrak{p}^{-1}$, откуда $\mathfrak{p} = \mathfrak{o}\,\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. Таким образом целый идеал $\mathfrak{p}\mathfrak{p}^{-1}$ делит $\mathfrak{p}$, откуда $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ или $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$. Допустим, что

$$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}.$$

Тогда мы бы имели, что $\mathfrak{p}\,(\mathfrak{p}^{-1})^2 = (\mathfrak{p}\mathfrak{p}^{-1})\,\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, точно так же $\mathfrak{p}\,(\mathfrak{p}^{-1})^3 = \mathfrak{p}$ и т. д. Если $a \neq 0$ — произвольный элемент $\mathfrak{p}$ и b — один из элементов $\mathfrak{p}^{-1}$, то $ab^e \in \mathfrak{p}\,(\mathfrak{p}^{-1})^e$ должно быть целым, и таким образом степени b выражаются дробями с одним и тем же знаменателем a. Отсюда получается, что b целое. Это справедливо для всякого b из $\mathfrak{p}^{-1}$, что противоречит лемме 3.

Теперь мы в состоянии доказать основную теорему о разложении на множители:

Теорема 2. *Всякий идеал* $\mathfrak{a}$ *есть произведение простых идеалов.*

Доказательство. Можно предположить, что $\mathfrak{a} \neq \mathfrak{o}$. Пусть согласно лемме 1

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0\,(\mathfrak{a}) \equiv 0\,(\mathfrak{p}_1) \tag{1}$$

и число r выбрано настолько малым, что произведение с меньшим числом сомножителей уже не может быть сравнимо с нулем по $\mathfrak{a}$. Если умножить (1) на $\mathfrak{p}_1^{-1}$, то получится

$$\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0\,(\mathfrak{p}_1^{-1}\mathfrak{a}) \equiv 0\,(\mathfrak{o});$$

---

1) Эти выводы могут быть упрощены, если считать известной общую теорию идеалов. А именно если $c \equiv 0\,(\mathfrak{p})$, то $\mathfrak{p}$ встречается среди простых идеалов, принадлежащих (c). Таким образом согласно § 84 (c): $\mathfrak{p} \neq (c)$, т. е. существует такой элемент b, не принадлежащий (c), что $\mathfrak{p}b \equiv 0\,(c)$.

таким образом $\mathfrak{p}_1^{-1}\mathfrak{a}$ есть целый идеал, который входит в произведение простых идеалов, причем число сомножителей меньше r. Теперь, применяя метод индукции по r, предположим, что теорема верна для идеалов, которые делят произведение k ($k < r$) простых идеалов, отличных от нулевого идеала (для идеала, делящего *только один* простой идеал, не равный нулевому, теорема очевидна). Тогда теорема будет справедлива в частности для $\mathfrak{p}_1^{-1}\mathfrak{a}$, т. е.

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2' \dots \mathfrak{p}_s'.$$

Умножив обе части на $\mathfrak{p}_1$, получим искомое разложение идеала $\mathfrak{a}$. Единственность этого разложения вытекает из следующей теоремы:

Теорема 3. *Если* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$ и $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$, $\mathfrak{b} = \mathfrak{p}_1' \dots \mathfrak{p}_s'$, *то простой идеал, отличный от* $\mathfrak{o}$ *и входящий в разложение* $\mathfrak{b}$, *входит также в разложение* $\mathfrak{a}$ *и притом входит туда по меньшей мере столько раз, сколько раз он встречается в* $\mathfrak{b}$.

Доказательство. Пусть $\mathfrak{p}_1' \neq \mathfrak{o}$. Так как $\mathfrak{p}_1'$ — делитель $\mathfrak{a}$, то $\mathfrak{p}_1'$ должен встречаться среди $\mathfrak{p}_i$ (лемма 2). Пусть, например, $\mathfrak{p}_1 = \mathfrak{p}_1'$. Имеем:

$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv 0\,(\mathfrak{p}_1^{-1}\mathfrak{b}),$$

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2 \dots \mathfrak{p}_r,$$

$$\mathfrak{p}_1^{-1}\mathfrak{b} = \mathfrak{p}_2' \dots \mathfrak{p}_s'.$$

Предположим, что наше утверждение доказано для меньших значений s (для $s = 0$, $\mathfrak{b} = \mathfrak{o}$ и теорема тривиальна). Тогда каждый из идеалов $\mathfrak{p}_2', \dots, \mathfrak{p}_s'$, отличный от нуля, будет встречаться по меньшей мере столько же раз и среди $\mathfrak{p}_2, \dots, \mathfrak{p}_r$. Таким образом теорема доказана.

Следствия. 1. *Разложение идеала на произведение простых идеалов единственно с точностью до порядка следования множителей и до множителей* $\mathfrak{o}$.

2. *Из делимости следует разложение на множители*: *именно если* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$, *то* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, *где* $\mathfrak{c}$ — *целый идеал.*

В самом деле, возьмем разложение $\mathfrak{a}$ на простые множители и устраним те множители, которые входят в $\mathfrak{b}$ (при этом принимается в расчет кратность, с которой они входят в $\mathfrak{b}$); в результате получится $\mathfrak{c}$.

Если $\mathfrak{o}$ — коммутативное кольцо с делителями нуля, то результаты этого параграфа остаются в силе, если только ограничиться идеалами, которые не состоят исключительно из делителей нуля. Аксиомы I и II предполагаются верными для идеалов, не являющихся делителями нуля, а в аксиоме III следует заменить поле отношений кольцом отношений, т. е. кольцом всех дробей $\frac{a}{b}$, где b — не делитель нуля. В результате будем иметь теоремы 1, 2, 3 для идеалов рассматриваемого рода.

§ 101. ЕДИНСТВЕННОСТЬ РАЗЛОЖЕНИЯ И АКСИОМЫ I—III

Мы видели, что из аксиом I—III (§ 100) получились как следствия теоремы 2 и 3, приводящие к единственному разложению идеала на простые множители. Оказывается, что, обратно, из единственности разложения вытекают аксиомы I—III, а именно:

Пусть $\mathfrak{o}$ *— область целостности с единицей. Пусть в* $\mathfrak{o}$ *всякий идеал* $\mathfrak{a}$ [1]) *разлагается на произведение простых идеалов:* $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$, *причем, если* $\mathfrak{a}$ *делится на* $\mathfrak{b}$, *то сомножители разложения* $\mathfrak{b}$, *отличные от* $\mathfrak{o}$ *входят в* $\mathfrak{a}$ *по меньшей мере столько раз, сколько раз они встречаются в* $\mathfrak{b}$. *Тогда выполняются аксиомы* I—III.

Доказательство. Постулат о цепях делителей (аксиома I) следует непосредственно из того, что всякий идеал $\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \dots \mathfrak{p}_r^{\rho_r}$ имеет только конечное число делителей $\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \dots \mathfrak{p}_r^{\sigma_r}$ $(\sigma_i \leqslant \rho_i)$. В частности, простой идеал $\mathfrak{p}$ имеет делителями только $\mathfrak{p}$ и $\mathfrak{o}$; таким образом аксиома II также выполняется.

Чтобы доказать аксиому III (целозамкнутость $\mathfrak{o}$ в поле отношений Σ), возьмем элемент λ из Σ, целый относительно $\mathfrak{o}$; тогда λ^m будет линейно выражаться через $\lambda^0, \dots, \lambda^{m-1}$ или, что одно и то же, лежать в $\mathfrak{o}$-модуле $\mathfrak{l} = (\lambda^0, \lambda^1, \dots, \lambda^{m-1})$. Если $\lambda = \frac{a}{b}$, то $\mathfrak{l}$ при умножении на $\mathfrak{b} = (b^{m-1})$ становится целым идеалом. Кроме того, $\mathfrak{l}$ удовлетворяет, очевидно, уравнению $\mathfrak{l}^2 = \mathfrak{l}$. Умножив на $\mathfrak{b}^2$, получим:

$$(\mathfrak{l}\mathfrak{b})^2 = (\mathfrak{l}\mathfrak{b})\,\mathfrak{b}.$$

Отсюда следует в силу единственности:

$$\mathfrak{l}\mathfrak{b} = \mathfrak{b},$$

откуда после умножения обеих частей на $b^{-(m-1)}$ будем иметь:

$$\mathfrak{l} = \mathfrak{o}.$$

Таким образом λ есть элемент кольца $\mathfrak{o}$, что и требовалось доказать.

Разберем теперь некоторые дополнения к теоремам 2 и 3.

Из следствия II § 100 получается, что метод определения общего наибольшего делителя и наименьшего кратного идеалов такой же, как и для целых чисел с помощью разложения на простые множители.

Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — два каких-нибудь идеала:

$$\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \dots \mathfrak{p}_r^{\rho_r},$$
$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \dots \mathfrak{p}_r^{\sigma_r}$$

(среди ρ_i и σ_i могут быть нули). Всякий их общий делитель может содержать только простые множители $\mathfrak{p}_i$ и притом с показателями меньшими или равными τ_i, где τ_i — наименьшее из чисел ρ_i, σ_i. Общий наибольший делитель $(\mathfrak{a}, \mathfrak{b})$ должен делиться на любой общий делитель и в частности на $\mathfrak{p}_i^{\tau_i}$. Поэтому он может быть равен только

$$\mathfrak{p}_1^{\tau_1} \dots \mathfrak{p}_r^{\tau_r}.$$

Точно так же общее наименьшее кратное $\mathfrak{a} \cap \mathfrak{b}$ (пересечение) идеалов $\mathfrak{a}$ и $\mathfrak{b}$ равно идеалу

$$\mathfrak{p}_1^{\mu_1} \dots \mathfrak{p}_r^{\mu_r},$$

где μ_i — наибольшее из чисел ρ_i, σ_i.

---

1) Здесь тоже целые идеалы, отличные от нулевого, будут обозначаться готическими буквами.

Теорема 4. *Если* $\mathfrak{a} \equiv 0\ (\mathfrak{b})$, *то в* $\mathfrak{b}$ *существует такой элемент* b, *что* $(\mathfrak{a}, b) = \mathfrak{b}$.

Доказательство. Пусть

$$\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \dots \mathfrak{p}_r^{\rho_r}$$
$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \dots \mathfrak{p}_r^{\sigma_r} \qquad (0 \leqslant \sigma_i \leqslant \rho_i).$$

Требуется найти такое b, которое кроме делителя $\mathfrak{b}$ других общих множителей с $\mathfrak{a}$ не имеет. Положим

$$\mathfrak{c} = \mathfrak{p}_1^{\sigma_1+1} \dots \mathfrak{p}_r^{\sigma_r+1},$$
$$\mathfrak{c}_i = \mathfrak{c} : \mathfrak{p}_i = \mathfrak{p}_1^{\sigma_1+1} \dots \mathfrak{p}^{\sigma_i} \dots \mathfrak{p}_r^{\sigma_r+1}.$$

Тогда $\mathfrak{c}_i \not\equiv 0\ (\mathfrak{c})$. Таким образом существует элемент b_i, лежащий в $\mathfrak{c}_i$, но не в $\mathfrak{c}$. Отсюда имеем:

$$b_i \equiv 0\left(\mathfrak{p}_j^{\sigma_j+1}\right) \qquad \text{для } j \neq i,$$
$$b_i \not\equiv 0\left(\mathfrak{p}_i^{\sigma_i+1}\right).$$

Сумма

$$b = b_1 + \dots + b_r$$

делится на $\mathfrak{b}$ (так как $\mathfrak{b}$ делит все b_i). Но

$$b \equiv b_i \not\equiv 0\left(\mathfrak{p}_i^{\sigma_i+1}\right);$$

таким образом b, кроме множителей $\mathfrak{b}$, других общих множителей с $\mathfrak{a}$ не имеет.

Следствия. 1. *В кольце вычетов* $\frac{o}{\mathfrak{a}}$ *всякий идеал* $\frac{\mathfrak{b}}{\mathfrak{a}}$ *является главным.* А именно, $\frac{\mathfrak{b}}{\mathfrak{a}}$ порождается классом вычетов $\mathfrak{a} + b$.

2. *Всякий идеал* $\mathfrak{b}$ *обладает двучленным базисом* (a, b), *где* $a \neq 0$ — *произвольно взятый из* $\mathfrak{b}$ *элемент.*

В самом деле, пусть a — какой-нибудь элемент идеала $\mathfrak{b}$, отличный от нуля, и $\mathfrak{a} = (a)$. Тогда из теоремы 4 получается, что $(a, b) = \mathfrak{b}$.

3. *Любой идеал* $\mathfrak{b}$ *можно умножить на такой идеал* $\mathfrak{m}$, *взаимно простой с данным идеалом* $\mathfrak{c}$, *что в произведении получится главный идеал.*

Доказательство. Положим $\mathfrak{a} = \mathfrak{c}\mathfrak{b}$. Из теоремы 4 получается, что

$$(\mathfrak{a}, b) = \mathfrak{b}. \tag{1}$$

Но так как b делится на $\mathfrak{b}$, то мы можем положить

$$(b) = \mathfrak{m}\mathfrak{b},$$

откуда из (1) имеем:

$$(\mathfrak{c}\mathfrak{b}, \mathfrak{m}\mathfrak{b}) = \mathfrak{b}.$$

Таким образом $\mathfrak{c}$ и $\mathfrak{m}$ должны быть взаимно простыми.

Задача. Пусть Ω — кольцо всех отношений $\frac{a}{b}$, где a и b целые величины, а b не делится на данные простые идеалы $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. Тогда

всякому идеалу $\mathfrak{a}$ из $\mathfrak{o}$ соответствует идеал $\mathfrak{A}$ кольца Ω, состоящий из дробей $\frac{a}{b}$, где $a \in \mathfrak{a}$. Простым идеалам $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ соответствуют простые идеалы $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, а всем остальным простым идеалам соответствует единичный идеал Ω. Любой идеал Ω разлагается единственным образом на произведение степеней $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$. Кроме того, в Ω все идеалы главные.

§ 102. ДРОБНЫЕ ИДЕАЛЫ

Мы в § 100 условились называть $\mathfrak{o}$-модуль в поле отношений Σ *дробным идеалом*, если он имеет конечный базис. Таким образом идеалы в $\mathfrak{o}$ или „целые идеалы" можно рассматривать как частный случай дробных идеалов.

Если $(\sigma_1, \ldots, \sigma_r)$ — базис дробного идеала, то, умножив элементы базиса на общий знаменатель, получим целый идеал.

Если, обратно, $\mathfrak{o}$-модуль $\mathfrak{a}$ при умножении на целую величину $b \neq 0$ становится целым, то $b\mathfrak{a}$ как целый идеал имеет конечный базис

$$b\mathfrak{a} = (a_1, \ldots, a_r),$$

откуда

$$\mathfrak{a} = \left(\frac{a_1}{b}, \ldots, \frac{a_r}{b}\right).$$

Тем самым доказано следующее предложение:

$\mathfrak{o}$-модуль в Σ тогда и только тогда является конечным, если он при умножении на целую величину $b \neq 0$ превращается в целый идеал.

Мы уже видели, что вместе с $\mathfrak{a}$ и $\mathfrak{b}$ также $\mathfrak{a} \cdot \mathfrak{b}$ и $(\mathfrak{a}, \mathfrak{b})$ имеют конечный базис; отсюда следует, что $\mathfrak{a} \cdot \mathfrak{b}$, $(\mathfrak{a}, \mathfrak{b})$ — дробные идеалы. Но это же заключение справедливо и для *модуля отношения* $\mathfrak{a} : \mathfrak{b}$, где $\mathfrak{a}$, $\mathfrak{b}$ — целые идеалы и $\mathfrak{b} \neq (0)$ [1]). В самом деле, если $b \neq 0$ — какой-нибудь элемент $\mathfrak{b}$, то

$$b \cdot (\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{b} \cdot (\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a} \subseteq \mathfrak{o};$$

поэтому $\mathfrak{a} : \mathfrak{b}$ при умножении на b превратится в целый идеал.

В частности, $\mathfrak{o} : \mathfrak{p} = \mathfrak{p}^{-1}$ есть всегда дробный идеал.

Целый или дробный идеал, не равный нулю, обладает обратным идеалом.

Доказательство. Пусть $\mathfrak{c} \neq (0)$ — дробный или целый идеал, а $b \neq 0$ выбрано так, что $b\mathfrak{c}$ является целым:

$$b\mathfrak{c} = \mathfrak{a}. \tag{1}$$

Если $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$, то, умножая (1) на $\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \ldots \mathfrak{p}_r^{-1}$, получаем, согласно теореме 1 (§ 100):

$$(\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \ldots \mathfrak{p}_r^{-1} b)\, \mathfrak{c} = \mathfrak{o},$$

а это доказывает существование обратного идеала

$$\mathfrak{c}^{-1} = \mathfrak{p}_1^{-1} \ldots \mathfrak{p}_r^{-1} b.$$

---

[1]) Под модулем отношения $\mathfrak{a} : \mathfrak{b}$ (в Σ) мы подразумеваем совокупность элементов λ из Σ, для которых $\lambda\mathfrak{b} \subseteq \mathfrak{a}$.

Из этой теоремы следует, что *целые и дробные идеалы, отличные от нуля, образуют абелеву группу.*

Итак, уравнение $\mathfrak{ac} = \mathfrak{b}$ однозначно разрешается относительно $\mathfrak{c}$. Его решение мы будем обозначать через $\mathfrak{a}^{-1}\mathfrak{b}$ или $\frac{\mathfrak{b}}{\mathfrak{a}}$.

Из прежних теорем вытекает еще такое предложение:

Дробный идеал равен отношению двух целых идеалов; таким образом его можно представить в виде:

$$\frac{\mathfrak{p}_1' \dots \mathfrak{p}_s'}{\mathfrak{p}_1'' \dots \mathfrak{p}_t''}.$$

При этом можно сократить идеалы, встречающиеся одновременно в числителе и в знаменателе.

Дробный главный идеал (λ) *равен такому отношению двух целых главных идеалов, что ни один из* r *данных простых идеалов не входит одновременно в числитель и знаменатель.*

Доказательство. Пусть мы произвели сокращение в дроби

$$(\lambda) = \frac{\mathfrak{p}_1' \dots \mathfrak{p}_s'}{\mathfrak{p}_1'' \dots \mathfrak{p}_t''}$$

и пусть дано r простых идеалов $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. Если знаменатель превратить в главный идеал (d), умножив на идеал $\mathfrak{b}$, взаимно простой с произведением $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, то получится:

$$(\lambda) = \frac{\mathfrak{b}\mathfrak{p}_1' \dots \mathfrak{p}_s'}{\mathfrak{b}\mathfrak{p}_1'' \dots \mathfrak{p}_t''} = \frac{\mathfrak{b}\mathfrak{p}_1' \dots \mathfrak{p}_s'}{(d)},$$

откуда

$$\mathfrak{b}\mathfrak{p}_1' \dots \mathfrak{p}_s' = (\lambda d).$$

Таким образом числитель также стал главным идеалом. Ни один из идеалов $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ не входит одновременно в числитель и знаменатель.

Задача. Отношение идеалов $\mathfrak{a}^{-1}\mathfrak{b} = \frac{\mathfrak{b}}{\mathfrak{a}}$ равно модулю отношений $\mathfrak{b} : \mathfrak{a}$.

Читателя, желающего более глубоко познакомиться с теорией идеалов в числовых полях, мы отсылаем к книге E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923. Что касается теории идеалов в поле функций и ее приложений, то мы отсылаем читателя к основной работе Дедекинда и Вебера: Crelles Journal, т. 92, стр. 181—190, 1882, а также ко второму тому учебника Вебера по алгебре. См. также Schmidt F. K., Analytische Zahlentheorie in Körpern der Charakteristik p. Math. Zeitschr., т. 33, стр. 1—32, 1931.

§ 103. ТЕОРИЯ ИДЕАЛОВ ПРОИЗВОЛЬНОЙ ЦЕЛОЗАМКНУТОЙ ОБЛАСТИ ЦЕЛОСТНОСТИ

Существует много важных областей целостности, которые удовлетворяют аксиомам I и III § 100, но не аксиоме II. В качестве примера можно привести кольцо полиномов $K[x_1, \dots, x_n]$ нескольких переменных, кольцо целочисленных полиномов $C[x_1, \dots, x_n]$ и их конечные целозамкнутые расширения (главные порядки). Во всех таких кольцах простой идеал, отличный от нуля и единичного идеала, имеет собственным делителем простой идеал подобного же рода. Таким

образом в этих кольцах теория идеалов § 100 не имеет места. Но мы покажем, что если равенство идеалов заменить „квази-равенством", то теория § 100 в основном останется в силе.

Итак, пусть $\mathfrak{o}$ — область целостности, целозамкнутая в своем поле отношений Σ. Будем обозначать готическими буквами дробные идеалы, отличные от нулевого идеала, т. е. $\mathfrak{o}$ — модули в Σ, которые при умножении на не исчезающую величину из $\mathfrak{o}$ становятся целыми идеалами. Под обратным идеалом $\mathfrak{a}^{-1}$ подразумевается такая совокупность элементов r из Σ, для которых $r\mathfrak{a}$ — целое.

Определение. $\mathfrak{a}$ *квази-равно* $\mathfrak{b}$, если $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$. В обозначении: $\mathfrak{a} \sim \mathfrak{b}$. Соотношение $\sim$, очевидно, обладает свойствами возвратности, симметрии и транзитивности.

Точно так же $\mathfrak{a}$ называется *квази-делителем* $\mathfrak{b}$, $\mathfrak{b}$ *квази-кратным* $\mathfrak{a}$, если $\mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$ или, что одно и то же, если $\mathfrak{a}^{-1}\mathfrak{b}$ — целый идеал. В этом случае мы будем писать: $\mathfrak{a} \leqslant \mathfrak{b}$ или $\mathfrak{b} \geqslant \mathfrak{a}$.

Символы $\leqslant$ и $\sim$ обладают следующими простейшими свойствами:

1. Из $\mathfrak{a} \supseteq \mathfrak{b}$ следует $\mathfrak{a} \leqslant \mathfrak{b}$ (доказательство очевидно).

2. Если $\mathfrak{a}$ — главный идеал: $\mathfrak{a} = (a)$, то, обратно, из $\mathfrak{a} \leqslant \mathfrak{b}$ следует $\mathfrak{a} \supseteq \mathfrak{b}$. В самом деле, тогда $\mathfrak{a}^{-1} = (a^{-1})$; так как $\mathfrak{a}^{-1}\mathfrak{b}$ — целый идеал, то $a^{-1}\mathfrak{b}$ также целый идеал, т. е. все элементы $\mathfrak{b}$ делятся на a.

3. Если одновременно $\mathfrak{a} \leqslant \mathfrak{b}$ и $\mathfrak{a} \geqslant \mathfrak{b}$, то $\mathfrak{a} \sim \mathfrak{b}$.

4. Для всех квази-кратных $\mathfrak{b}$ идеала $\mathfrak{a}$, в частности для всех $\mathfrak{b}$, квази-равных $\mathfrak{a}$, имеет место соотношение $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$. (Получается, как непосредственное следствие того, что $\mathfrak{b}\mathfrak{a}^{-1}$ — целое.)

В частности, $\mathfrak{a} \subseteq (\mathfrak{a}^{-1})^{-1}$. Отсюда согласно 1 имеем, что $\mathfrak{a} \geqslant (\mathfrak{a}^{-1})^{-1}$. С другой стороны, $\mathfrak{a}^{-1}(\mathfrak{a}^{-1})^{-1}$ является целым, откуда $\mathfrak{a} \leqslant (\mathfrak{a}^{-1})^{-1}$. Поэтому

5. $$\mathfrak{a} \sim (\mathfrak{a}^{-1})^{-1}.$$

В силу 4 и 5 $(\mathfrak{a}^{-1})^{-1}$ является идеалом, квази-равным $\mathfrak{a}$ и содержащим $\mathfrak{a}$. Мы его обозначим через $\mathfrak{a}^*$.

6. Если $\mathfrak{a} \leqslant \mathfrak{b}$, то $\mathfrak{a}\mathfrak{c} \leqslant \mathfrak{b}\mathfrak{c}$. В самом деле, $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{a}$ — целое, а потому $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c} \subseteq \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$, откуда $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{b}$ является целым, или $\mathfrak{c}\mathfrak{a} \leqslant \mathfrak{c}\mathfrak{b}$.

7. Если $\mathfrak{a} \sim \mathfrak{b}$, то $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c}$ (следствие 6).

8. Если $\mathfrak{a} \sim \mathfrak{b}$ и $\mathfrak{c} \sim \mathfrak{d}$, то $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$ (ибо согласно 7 $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$).

Если объединить в один класс все идеалы, квази-равные некоторому идеалу, то в силу 8 класс произведения $\mathfrak{a}\mathfrak{c}$ зависит только от класса $\mathfrak{a}$ и класса $\mathfrak{c}$. Таким образом *произведение* двух последних классов мы можем определить как класс произведения $\mathfrak{a}\mathfrak{c}$.

9. При перемножении классов единицей будет класс идеалов, квази-равных единичному идеалу $\mathfrak{o}$, так как для всякого $\mathfrak{a}$ имеет место $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$.

10. Все квази-кратные $\mathfrak{o}$, в частности все идеалы единичного класса, являются целыми. (Частный случай 2: стоит только положить $\mathfrak{a} = 1$.) Отсюда как следствие получается, что все идеалы, квази-равные целому идеалу, тоже целые.

Теперь мы докажем важнейшее свойство обратных идеалов:

11. $$\mathfrak{a}\mathfrak{a}^{-1} \sim \mathfrak{o}.$$

Очевидно, что $\mathfrak{a}\mathfrak{a}^{-1} \geqslant \mathfrak{o}$, так как $\mathfrak{a}\mathfrak{a}^{-1}$ — целое. Остается доказать, что $\mathfrak{a}\mathfrak{a}^{-1} \leqslant \mathfrak{o}$ или $(\mathfrak{a}\mathfrak{a}^{-1})^{-1} \subseteq \mathfrak{o}$. Если λ принадлежит $(\mathfrak{a}\mathfrak{a}^{-1})^{-1}$, то $\lambda\mathfrak{a}\mathfrak{a}^{-1}$ является целым, откуда $\lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, $\lambda^2\mathfrak{a}^{-1} \subseteq \lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$ и т. д., вообще $\lambda^n\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$. Таким образом $\lambda^n\mathfrak{a}^{-1}\mathfrak{a}$ — целое. Если μ есть произвольный элемент идеала $\mathfrak{a}^{-1}\mathfrak{a}$, то все степени λ при умножении на μ станут целыми. Из целозамкнутости $\mathfrak{o}$ отсюда следует (совершенно так же, как в соответствующем месте § 100), что само λ — целое.

Из 11 следует, что класс $\mathfrak{a}^{-1}$ представляется классом, обратным классу $\mathfrak{a}$: произведение классов $\mathfrak{a}$ и $\mathfrak{a}^{-1}$ равно единичному классу. Отсюда имеем:

Теорема 1. *Классы квази-равных идеалов образуют группу.*

12. Из $\mathfrak{a} \geqslant \mathfrak{b}$ следует $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}$, где $\mathfrak{c}$ — целый идеал, причем $\mathfrak{c}$ можно выбрать так, что $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$. А именно, если положить $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{c}$, то $\mathfrak{c}$ будет целым, а отсюда умножая равенство на $\mathfrak{b}$, получим $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}$, а также $\mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{b}^{-1}\mathfrak{a} \subseteq \mathfrak{o}\mathfrak{a} = \mathfrak{a}$.

Теперь будем обозначать готическими буквами только *целые* идеалы, отличные от нуля. Такой идеал $\mathfrak{p}$ мы назовем *неразложимым*, если он не квази-равен $\mathfrak{o}$, и произведение $\mathfrak{ab} \sim \mathfrak{p}$ необходимо содержит множитель единичного класса или, что в силу 12 одно и то же, если $\mathfrak{p}$ не квази-равно $\mathfrak{o}$ и имеет квази-делителями либо идеалы, квази-равные $\mathfrak{p}$ либо идеалы, квази-равные $\mathfrak{o}$.

Если неразложимый идеал $\mathfrak{p}$ заменить квази-равным идеалом $\mathfrak{p}^*$, содержащим $\mathfrak{p}$, то всякий целый собственный делитель $\mathfrak{p}^*$ не будет квази-равен $\mathfrak{p}$. Таким образом этот делитель должен быть квази-равен $\mathfrak{o}$. Идеал, который квази-делится на $\mathfrak{p}$ или $\mathfrak{p}^*$, должен согласно 4 делиться на $\mathfrak{p}^*$. Отсюда следует:

13. $\mathfrak{p}^*$ есть простой идеал. Именно, если произведение $\mathfrak{bc}$ двух главных идеалов $\mathfrak{b}$ и $\mathfrak{c}$ делится на $\mathfrak{p}^*$, но $\mathfrak{b}$ не делится на $\mathfrak{p}^*$, то $(\mathfrak{b}, \mathfrak{p}^*)$ есть собственный делитель идеала $\mathfrak{p}^*$; таким образом $(\mathfrak{b}, \mathfrak{p}^*) \sim \mathfrak{o}$. Отсюда

$$\mathfrak{c} = \mathfrak{oc} \sim (\mathfrak{b}, \mathfrak{p}^*)\,\mathfrak{c} = (\mathfrak{bc}, \mathfrak{p}^*\mathfrak{c}) \geqslant (\mathfrak{p}^*, \mathfrak{p}^*) = \mathfrak{p}^*,$$

т. е. $\mathfrak{c}$ квази-делится на $\mathfrak{p}^*$, а потому делится на $\mathfrak{p}^*$.

Подобным же образом имеем:

14. Если произведение $\mathfrak{bc}$ квази-делится на неразложимый идеал $\mathfrak{p}$, то один из множителей ($\mathfrak{b}$ или $\mathfrak{c}$) квази-делится на $\mathfrak{p}$. В самом деле, из квази-делимости на $\mathfrak{p}$ следует делимость на $\mathfrak{p}^*$, а затем доказательство проводится, как и в 13.

Если мы еще введем для $\mathfrak{o}$ постулат о цепях делителей, то получим:

15. Всякая последовательность целых идеалов $\mathfrak{a}_1 > \mathfrak{a}_2 > \ldots$, где каждый следующий идеал является собственным квази-делителем предыдущего, состоит из конечного числа членов. Действительно, если мы заменим идеалы $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$, квази-равными им идеалами $\mathfrak{a}_1^*, \mathfrak{a}_2^*, \ldots$, содержащими соответственно $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$, то мы получим последовательность целых идеалов $\mathfrak{a}_1^* \subset \mathfrak{a}_2^* \subset \ldots$, которая согласно постулату о цепях делителей не бесконечна.

Из 14 и 15 следуют единственность и возможность разложения всех целых идеалов на неразложимые идеалы так же, как в § 17. Таким образом имеет место следующая теорема.

Теорема 2. *Всякий целый идеал, отличный от нулевого идеала, квази-равен произведению неразложимых идеалов* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ (в качестве их могут быть взяты также простые идеалы $\mathfrak{p}_1^*, \mathfrak{p}_2^*, \ldots, \mathfrak{p}_r^*$), *причем это произведение определяется однозначно с точностью до порядка следования и квази-равенства.*

Согласно 2 два главных идеала только тогда квази-делят друг друга (квази-равны), если между ними имеет место делимость (равенство). Присоединяя к главным идеалам классы неглавных идеалов, получим новую область, в которой согласно теореме 2 выполняется однозначное разложение на простые множители, чем и достигается цель „классической теории идеалов“ [1].

Но чтобы установить связь полученной теории с общей теорией идеалов и частной теорией идеалов § 100, мы должны выяснить, какие простые идеалы неразложимы и какие идеалы квази-равны $\mathfrak{o}$.

---

[1]) Если в $\mathfrak{o}$ не выполняется постулат о цепях делителей, то теорема 2 может оказаться неверной. Вместо нее Е. Артин высказал такое предложение: если даны два разложения идеала на множители:

$$\mathfrak{a} \sim \mathfrak{b}_1\mathfrak{b}_2 \ldots \mathfrak{b}_m \sim \mathfrak{c}_1\mathfrak{c}_2 \ldots \mathfrak{c}_n,$$

то можно разложить оба произведения еще так, чтобы они совпали с точностью до порядка следования множителей и до квази-равенства:

$$\mathfrak{b}_\lambda \sim \prod_\mu \mathfrak{b}_{\lambda\mu}, \quad \mathfrak{c}_\nu \sim \prod_\omega \mathfrak{c}_{\nu\omega},$$

где $\mathfrak{b}_{\lambda\mu} \sim \mathfrak{c}_{\nu\omega}$ в каком-то порядке.

Доказательство основано на следующем обобщении леммы § 85: из $(\mathfrak{a}, \mathfrak{b}) \sim \mathfrak{o}$ и $(\mathfrak{a}, \mathfrak{c}) \sim \mathfrak{o}$ следует $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}) \sim \mathfrak{o}$. Лемма доказывается легко, и с ее помощью без труда получается доказательство теоремы Е. Артина, стоит только положить $(\mathfrak{b}_1, \mathfrak{c}_1) = \mathfrak{b}_{11}$; $\mathfrak{b}_1 \sim \mathfrak{b}_{11}\mathfrak{b}_1'$; $(\mathfrak{b}_1', \mathfrak{c}_2) = \mathfrak{b}_{12}$; $\mathfrak{b}_1' \sim \mathfrak{b}_{12}\mathfrak{b}_1''$; $(\mathfrak{b}_1'', \mathfrak{c}_3) = \mathfrak{b}_{13}$ и т. д.

Мы видели, что при неразложимом $\mathfrak{p}$ идеал $\mathfrak{p}^*$ простой. Докажем теперь такое предложение:

16. Собственное кратное идеала $\mathfrak{p}^*$, отличное от нуля, не может быть простым. Именно, если $\mathfrak{a}$ есть такое кратное, то $\mathfrak{a} \geqslant \mathfrak{p}^*$; отсюда согласно 12 $\mathfrak{a} \sim \mathfrak{p}^*\mathfrak{q}$, причем $\mathfrak{p}^*\mathfrak{q} \equiv 0\ (\mathfrak{a})$. Так как в разложении $\mathfrak{q}$ простых множителей меньше, чем в $\mathfrak{a}$, то $\mathfrak{q} \not\equiv 0\ (\mathfrak{a})$; точно так же $\mathfrak{p}^* \not\equiv 0\ (\mathfrak{a})$. Итак, $\mathfrak{a}$ не простой идеал.

Теперь рассмотрим разложение произвольного простого идеала $\mathfrak{p}$. Либо $\mathfrak{p} \sim \mathfrak{o}$, либо в разложение $\mathfrak{p} \sim \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$ входит неразложимый множитель $\mathfrak{p}_1$. Тогда $\mathfrak{p} \geqslant \mathfrak{p}_1$, откуда $\mathfrak{p} \subseteq \mathfrak{p}_1^*$; но так как собственное кратное $\mathfrak{p}_1^*$ не может быть простым, то $\mathfrak{p} = \mathfrak{p}_1^*$. Следовательно, $\mathfrak{p}^* = \left(\mathfrak{p}_1^*\right)^* = \mathfrak{p}_1^* = \mathfrak{p}$.

Итак:

17. Простой идеал $\mathfrak{p}$ либо квази-равен $\mathfrak{o}$, либо неразложим и равен соответствующему $\mathfrak{p}^*$.

Во втором случае $\mathfrak{p}$ не имеет собственного простого кратного, отличного от нулевого идеала. В первом же случае, как мы покажем, такое кратное существует.

18. Если $\mathfrak{p} \sim \mathfrak{o}$, то существует неразложимый простой идеал $\mathfrak{p}_\nu^*$, который является собственным кратным идеала $\mathfrak{p}$. В самом деле, если $p \neq 0$ — элемент идеала $\mathfrak{p}$ и $(p) \sim \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r \sim \mathfrak{p}_1^*\mathfrak{p}_2^* \dots \mathfrak{p}_r^*$, то из 2 следует, что $\mathfrak{p}_1^*\mathfrak{p}_2^* \dots \mathfrak{p}_r^* \equiv 0\ (p) \equiv 0\ (\mathfrak{p})$, откуда $\mathfrak{p}_\nu^* \equiv 0\ (\mathfrak{p})$, причем $\mathfrak{p}_\nu^* \neq \mathfrak{p}$, так как иначе было бы $\mathfrak{p}_\nu^* \sim \mathfrak{o}$.

Назовем простой идеал *высшим*, если он не обладает собственным простым кратным, отличным от нуля; напротив, если такое кратное существует, то мы назовем идеал *низшим*. 16, 17 и 18 тогда объединяются в следующую теорему.

Теорема 3. *Любой высший простой идеал $\mathfrak{p}$ неразложим и равен своему $\mathfrak{p}^*$; любой низший простой идеал квази-равен $\mathfrak{o}$.*

Идеал, не принадлежащий единичному классу, в силу теоремы 2 о разложении делится по крайней мере на один высший простой идеал $\mathfrak{p} = \mathfrak{p}^*$. Идеал же единичного класса не делится на высший простой идеал.

19. Если $\mathfrak{a} \geqslant \mathfrak{b}$, то существует такой идеал $\mathfrak{c}$ единичного класса, что $\mathfrak{ac} \equiv 0\ (\mathfrak{b})$. А именно, полагая $\mathfrak{c} \equiv \mathfrak{b}^{-1}\mathfrak{b}$, получим $\mathfrak{ac} = \left(\mathfrak{ab}^{-1}\right)\mathfrak{b} \subseteq \mathfrak{b}$, так как $\mathfrak{ab}^{-1}$ — целый идеал.

Если каждый из двух идеалов квази-делится на другой, то они квази-равны. Но квази-равенство можно охарактеризовать еще иначе.

20. Если $\mathfrak{a} \sim \mathfrak{b}$, то существуют такие $\mathfrak{c} \sim \mathfrak{o}$ и $\mathfrak{d} \sim \mathfrak{o}$, что $\mathfrak{ac} = \mathfrak{bd}$. Действительно, из $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$ следует $\mathfrak{a}\left(\mathfrak{b}^{-1}\mathfrak{b}\right) = \left(\mathfrak{aa}^{-1}\right)\mathfrak{b}$.

В кольцах, рассмотренных в § 100, отличный от нуля простой идеал делится в силу аксиомы II только на самого себя и $\mathfrak{o}$; таким образом в этих кольцах только $\mathfrak{o}$ будет низшим простым идеалом. Так как всякий идеал $\mathfrak{a} \neq \mathfrak{o}$ делится на некоторый простой идеал, отличный от $\mathfrak{o}$ [1]), то $\mathfrak{a}$ не квази-равно $\mathfrak{o}$. Поэтому единичный класс состоит только из единичного идеала $\mathfrak{o}$. Кроме того, из 19 следует, что квази-делимость и делимость равносильны, а отсюда или из 20 получается, что квази-равенство и равенство также равносильны. Следовательно, теория идеалов § 100 является частным случаем нашей теории.

Также легко установить связь с общей теорией идеалов двенадцатой главы. Прежде всего легко видеть, что всякий примарный идеал, соответствующий простой идеал которого является низшим, должен быть квази-равен $\mathfrak{o}$. Назовем такой примарный идеал *низшим*, а другие примарные идеалы *высшими*. Идеал $\mathfrak{a}$ тогда и только тогда квази-равен $\mathfrak{o}$, если все его примарные компоненты низшие. Если два идеала $\mathfrak{a}$ и $\mathfrak{b}$ имеют одни и те же высшие (но не обязательно низшие) примарные компоненты, то $\mathfrak{a} \sim \mathfrak{b}$. Среди идеалов, квази-равных $\mathfrak{a}$, находится идеал $\mathfrak{a}^*$, содержащий $\mathfrak{a}$; он получится, если в разложении $\mathfrak{a} = [\mathfrak{q}_1, \dots, \mathfrak{q}_r]$ опустить все низшие примарные компоненты. Теоремы разложения и единственности получатся, если пренебречь низшими примарными компонентами и обратить внимание только на высшие компоненты. Высшие примарные идеалы делятся только на высшие простые идеалы; отсюда получается (с помощью теоремы 2), что *высший примарный идеал квази-равен степени простого идеала.*

---

[1]) Для доказательства ищут среди различных делителей $\mathfrak{a}$, отличных от $\mathfrak{o}$, наибольший; он будет свободен от делителей, а потому прост.

Пример. Кольцо $C[x, \sqrt{2x}]$ вполне замкнуто в поле отношений $\Gamma(\sqrt{2x})$ и удовлетворяет всем предположениям этого параграфа. В области главных идеалов главный идеал $(2x)$ допускает следующие два существенно различные разложения:

$$(2x) = (2)\cdot(x) = (\sqrt{2x})^2.$$

Таким образом в области главных идеалов не выполняется единственность разложения. Простые идеалы

$$\mathfrak{p}_1 = (x, \sqrt{2x}) \text{ и } \mathfrak{p}_2 = (2, \sqrt{2x})$$

не квази-равны $\mathfrak{o}$, так как $\mathfrak{p}_1^{-1}$ и $\mathfrak{p}_2^{-1}$ содержат соответственно не целые элементы $\frac{\sqrt{2x}}{x}$ и $\frac{\sqrt{2x}}{2}$. Простой идеал

$$\mathfrak{p}_3 = (2, x, \sqrt{2x})$$

является собственным делителем $\mathfrak{p}_1$ и $\mathfrak{p}_2$ и потому квази-равен $\mathfrak{o}$. Имеем:

$$\mathfrak{p}_1^2 = (x^2, x\sqrt{2x}, 2x) = (x)\cdot(x, \sqrt{2x}, 2) = (x)\cdot\mathfrak{p}_3 \sim (x),$$

$$\mathfrak{p}_2^2 = (2^2, 2\sqrt{2x}, 2x) = (2)\cdot(2, \sqrt{2x}, x) = (2)\cdot\mathfrak{p}_3 \sim (2),$$

$$\mathfrak{p}_1\mathfrak{p}_2 = (2x, 2\sqrt{2x}, x\sqrt{2x}) = (\sqrt{2x})\cdot(\sqrt{2x}, 2, x) = (\sqrt{2x})\cdot\mathfrak{p}_3 \sim (\sqrt{2x}).$$

Главные идеалы (x) и (2) примарны, но не равны, а только квази-равны степеням простых идеалов. Главный идеал $(\sqrt{2x})$ является общим наименьшим кратным $\mathfrak{p}_1$ и $\mathfrak{p}_2$, но не равен, а только квази-равен их произведению. Пример этот показывает, как необходимо введение квази-равенства вместо равенства для того, чтобы получить разложение на простые множители главных идеалов.

Задачи. 1. Все результаты этого параграфа справедливы также для колец с делителями нуля, если только поле отношений заменить кольцом отношений и ограничиться идеалами, не состоящими исключительно из делителей нуля (см. конец § 100).

2. Обратно, из теоремы 1 следует целозамкнутость кольца $\mathfrak{o}$. Точно так же целозамкнутость следует из теоремы 2 и первой половины 12 (см. § 101).

3. Доказать целозамкнутость кольца вычетов

$$\mathfrak{o} = K\frac{[x, y, z]}{(xy - z^2)}$$

и разложить главные идеалы (x), (y), (z) в $\mathfrak{o}$ на простые множители.

4. Распространить теорему 4 § 101 и ее следствия на самое общее целозамкнутое кольцо.

5. Доказать, что $\mathfrak{a} : \mathfrak{b} \sim \mathfrak{a}\mathfrak{b}^{-1}$.

Краткое резюме

Следующее сопоставление показывает, какое значение имеют аксиомы I (постулат о цепях делителей), II (всякий простой идеал свободен от делителей), III (целозамкнутость) для теории идеалов области целостности.

Из I следует, что всякий идеал есть общее наименьшее кратное примарных идеалов; соответствующие простые идеалы определяются однозначно.

Из I и II следует, что всякий идеал есть произведение единообразных примарных идеалов, причем имеет место единственность произведения.

Из I и III следует, что всякий идеал квази-равен произведению степеней простых идеалов; при этом произведение единственно с точностью до квази-равенства.

Из I, II, III следует, что всякий идеал равен произведению степеней простых идеалов; при этом разложение единственно.

ГЛАВА ПЯТНАДЦАТАЯ

ЛИНЕЙНАЯ АЛГЕБРА

Предметом линейной алгебры являются *линейные формы* (с коэфициентами из кольца $\mathfrak{K}$), *модули* из линейных форм и гомоморфизмы таких модулей или *линейные преобразования*. Теория распадается на различные отделы в соответствии с различными предположениями, которые можно делать относительно основного кольца или поля $\mathfrak{K}$. Вводный параграф справедлив для произвольного (также и не коммутативного) кольца $\mathfrak{K}$.

Настоящее изложение линейной алгебры основано исключительно на теории групп с операторами (глава 6); при этом будут использованы только основы этой теории.

§ 104. МОДУЛИ, ЛИНЕЙНЫЕ ФОРМЫ, ВЕКТОРЫ, МАТРИЦЫ

Пусть $\mathfrak{K}$ — кольцо с единицей ε; его элементы мы в этом параграфе будем обозначать греческими буквами и иногда называть *скалярами*.

Пусть $\mathfrak{M}$ (правый) $\mathfrak{K}$-модуль, т. е. аддитивная абелева группа, для которой $\mathfrak{K}$ является правой мультипликаторной областью, и пусть помимо групповых аксиом имеют место следующие правила оперирования:

$$(a+b)\lambda = a\lambda + b\lambda,$$
$$a(\lambda+\mu) = a\lambda + a\mu,$$
$$a(\lambda\mu) = (a\lambda)\mu\ ^{1}).$$

Латинскими буквами обозначены элементы $\mathfrak{M}$. Из дистрибутивного закона следует, как и обычно, тот же закон для вычитания, мультипликативные свойства знака минус и то обстоятельство, что произведение равно нулю, когда один из сомножителей равен нулю (нуль из $\mathfrak{K}$ или из $\mathfrak{M}$).

Единица кольца $\mathfrak{K}$ может и не быть единичным оператором: $a\varepsilon$ может оказаться для некоторых a отличным от a (например все правила оперирования удовлетворяются, если положить $a\lambda = 0$ для любого a и λ). Но в этом случае всегда можно положить

$$a = (a - a\varepsilon) + a\varepsilon. \tag{1}$$

Первый член $a - a\varepsilon$ будет уничтожаться правым множителем ε, а второй при умножении на ε не меняется. Первый член образует подмодуль $\mathfrak{M}_0$ модуля $\mathfrak{M}$, уничтожающийся элементом ε; поэтому $\mathfrak{M}_0$ будет уничтожаться любым элементом $\varepsilon\lambda$ из $\mathfrak{K}$; второй член $a\varepsilon$ образует подмодуль $\mathfrak{M}_1$, для которого ε — единичный оператор. Подмодули $\mathfrak{M}_0$ и $\mathfrak{M}_1$ могут иметь общим элементом только нуль, так как, если бы $m \neq 0$ было их общим элементом, то, с одной стороны, мы бы имели $m\varepsilon = 0$, а с другой, $m\varepsilon = m$, что невозможно. Таким образом из (1) следует,

---

[1]) Все теоремы, которые будут доказаны ниже, остаются в силе и тогда, если $\mathfrak{K}$ — левая мультипликаторная область. Если $\mathfrak{K}$ — левая мультипликаторная область, то последнее правило оперирования принимает следующий вид:

$$(\lambda\mu)a = \lambda(\mu a),$$

т. е. операция умножения на $\lambda\mu$ идет здесь в обратном порядке (сперва a умножается на μ и затем на λ).

что $\mathfrak{M}$ равно прямой сумме $\mathfrak{M}_0 + \mathfrak{M}_1$. Итак, если откинуть в $\mathfrak{M}$ неинтересную часть $\mathfrak{M}_0$, то останется модуль, для которого ε будет единичным оператором. *Поэтому в дальнейшем мы будем предполагать, что единица ε вместе с тем является единичным оператором* $\mathfrak{M}$: $a\varepsilon = a$ для всякого a. Отныне мы будем обозначать эту единицу через 1.

Модуль $\mathfrak{M}$ называется *конечным* (относительно K), если его элементы линейно выражаются через конечное множество элементов $u_1, \ldots, u_n$:

$$u = u_1\lambda_1 + \ldots + u_n\lambda_n.$$

В этом случае мы будем писать:

$$\mathfrak{M} = (u_1\mathsf{K}, \ldots, u_n\mathsf{K}) \text{ или } \mathfrak{M} = (u_1, \ldots, u_n).$$

Предположим еще, что u_i *линейно независимы*, т. е. что из $\sum u_i\alpha_i = 0$ следует $\alpha_i = 0$. При этом предположении $\mathfrak{M}$ называется (*n-членным*) *модулем линейных форм.* K называется *областью коэфициентов*; u_j образуют систему *элементов базиса.* В силу линейной независимости u_j всякий элемент из $\mathfrak{M}$ записывается в виде линейной формы $\sum u_j\lambda_j$ *однозначно*, так как из

$$\sum u_j\lambda_j = \sum u_j\mu_j$$

следует:

$$\sum u_j(\lambda_j - \mu_j) = 0,$$

откуда

$$\lambda_j - \mu_j = 0, \text{ или } \lambda_j = \mu_j.$$

Два модуля линейных форм, обладающие одной и той же областью коэфициентов K *и одним и тем же числом элементов базиса, операторно-изоморфны.* Именно, каждому элементу u_j базиса модуля можно привести в соответствие элемент v_j базиса другого модуля и линейную форму $\sum u_j\lambda_j$ сопоставить линейной форме $\sum v_j\lambda_j$.

Из этого изоморфизма следует, если только выполняются все наши предположения, что для теории модулей совершенно безразлично, будут ли u_j неопределенными переменными или чем-нибудь другим. Очень часто бывает, что u_j принадлежит кольцу, содержащему K (например в теории алгебраических числовых модулей). Может также оказаться, что $\mathfrak{M}$ образует модуль *векторов.* При этом под *вектором* подразумевается последовательность $\{\lambda_1, \ldots, \lambda_n\}$ элементов из K. Векторы складываются, если складываются их компоненты; векторы можно умножать на скаляры α из K, для чего надо умножить все компоненты на α. Если ввести следующие линейно независимые векторы:

$$e_1 = (1, 0, \ldots, 0),$$
$$e_2 = (0, 1, \ldots, 0).$$
$$\ldots\ldots\ldots$$
$$e_n = (0, 0, \ldots, 1),$$

то любой вектор $(\lambda_1, \ldots, \lambda_n)$ будет равен линейной форме

$$e_1\lambda_1 + \ldots + e_n\lambda_n;$$

тем самым векторы также приводятся к линейным формам. Все, имеющее отношение к модулям линейных форм, справедливо поэтому также для „векторного пространства“, и обратно.

Операторный гомоморфизм, отображающий модуль $\mathfrak{M} = (u_1, \ldots, u_m)$ линейных форм на модуль $\mathfrak{N} = (v_1, \ldots, v_n)$ линейных форм, называется *линейным отображением* или *линейным преобразованием*. Такое преобразование вполне определяется заданием отображения

$$u_j' = \sum_1^n v_i\alpha_{ij} \qquad (j = 1, \ldots, m) \quad (2)$$

каждого элемента u_j базиса. Иными словами, линейное преобразование вполне определяется *матрицей*

$$A = (\alpha_{ij}) = \begin{pmatrix} \alpha_{11} & \alpha_{12} \ldots \alpha_{1m} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \alpha_{n1} & \alpha_{n2} \ldots \alpha_{nm} \end{pmatrix}^{1)}.$$

Именно, тогда $a = \sum u_j\lambda_j$ будет отображаться на $a' = \sum u_j'\lambda_j$. В случае изменения базиса $(u_1, \ldots, u_m)$ или $(v_1, \ldots, v_n)$ одно и то же линейное преобразование может всякий раз представиться другой матрицей (см. задачу 6). Несмотря на это, линейное преобразование обозначается тем же символом A, что и соответствующая матрица.

Если элемент a отображается при помощи матрицы A на a', то мы будем писать $a' = Aa$; таким образом в случае (2) имеем:

$$Au_j = \sum v_i\alpha_{ij}.$$

Вообще матрица A будет прямоугольной; квадратной она может быть только в случае $m = n$. Например, она будет квадратной при линейном отображении $\mathfrak{M}$ на самого себя.

Пусть с помощью матрицы A $\mathfrak{M} = (u_1, \ldots, u_m)$ отображается на $\mathfrak{N} = (v_1, \ldots, v_n)$, а $\mathfrak{N}$ с помощью матрицы B отображается на $\mathfrak{P} = (w_1, \ldots, w_p)$. Тогда

$$B(Au_j) = B\left(\sum_i v_i\alpha_{ij}\right) = \sum_i (Bv_i)\,\alpha_{ij} = \sum_h \sum_i w_h\beta_{hi}\alpha_{ij};$$

таким образом отображение $\mathfrak{M}$ на $\mathfrak{P}$ определяется *произведением матриц* $C = BA$, причем элементы γ_{hj} матрицы C равны

$$\gamma_{hj} = \sum_i \beta_{hi}\alpha_{ij}.$$

---

[1]) При наших обозначениях j-му уравнению (2) соответствует j-й столбец матрицы A.

Итак, для $u \in \mathfrak{M}$

$$(BA)\,u = B\,(Au).$$

Произведение AB только тогда имеет смысл, когда число столбцов A равно числу строк B. Только тогда произведение AB будет определять отображение.

Сумма двух линейных отображений $\mathfrak{M}$ на $\mathfrak{N}$ определяется равенством:

$$(A+B)\,u = Au + Bu;$$

соответствующая матрица состоит из элементов $\alpha_{ik} + \beta_{ik}$ и носит *название суммы матриц* A и B; она имеет смысл, если A и B имеют одинаковое число строк и столбцов.

Из определения суммы и произведения вытекают такие правила оперирования (справедливые только тогда, когда рассматриваемые произведения имеют смысл):

$$A\,(BC) = (AB)\,C,$$
$$A + (B + C) = (A + B) + C,$$
$$A(B + C) = AB + AC,$$
$$(B + C)\,A = BA + CA.$$

С помощью матриц $(u_1, \ldots, u_m)$, $(v_1, \ldots, v_n)$ и т. д., состоящих из одной строки, можно формулу (2) записать в матричной форме:

$$(u_1', \ldots, u_m') = (v_1, \ldots, v_n)\cdot A.$$

Линейную форму $\sum u_i\lambda_i$ целесообразно записывать в виде произведения *строки* $(u_1, \ldots, u_m)$ на *столбец* $\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_m\end{pmatrix}$, который можно отождествить с *вектором* $(\lambda_1, \ldots, \lambda_m)$. Линейная форма $\sum u_j\lambda_j$ преобразуется при помощи линейного отображения A в

$$\sum Au_j\lambda_j = \sum\sum v_i\alpha_{ij}\lambda_j;$$

правой линейной форме опять соответствует вектор, а именно:

$$\begin{pmatrix}\lambda_1'\\ \vdots\\ \lambda_n'\end{pmatrix} = A\cdot\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_m\end{pmatrix}.$$

Каждое λ_i' получается из некоторой *строки* матрицы A умножением на $\lambda_1, \ldots, \lambda_m$ и суммированием.

Отображение $\mathfrak{M} = (u_1, \ldots, u_n)$ на самого себя определяется квадратной матрицей:

$$u_j' = \sum u_i\alpha_{ij}. \qquad (3)$$

Эти квадратные матрицы образуют кольцо, которое можно рассматривать как область (левых) операторов векторного пространства.

Чтобы u_j' формулы (3) составляли также базис $\mathfrak{M}$, необходимо, *во-первых*, чтобы они были линейно независимы, т. е. чтобы из

$$\sum u_j' \mu_j = 0,$$

или

$$\sum_i \sum_j u_i \alpha_{ij} \mu_j = 0,$$

или, наконец, $\sum \alpha_{ij}\mu_j = 0$ всегда следовало $\mu_j = 0$; иными словами, между столбцами

$$\begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{n1} \end{pmatrix}, \quad \begin{pmatrix} \alpha_{12} \\ \vdots \\ \alpha_{n2} \end{pmatrix}, \ldots$$

не должно быть линейной зависимости. Отсюда следует, что матрица A не должна обращаться в нуль при умножении справа на столбец $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$, отличный от нуля. Но тогда для всякой матрицы $B \neq 0$ $AB \neq 0$, и мы можем сказать, что A *не является левым делителем нуля*. *Во-вторых*, надо, чтобы, обратно, все u_i выражались через u_i':

$$u_k = \sum u_j' \beta_{jk}. \tag{4}$$

Для этого должно выполняться тождество:

$$u_k = \sum u_i \alpha_{ij} \beta_{jk},$$

которое получается при подстановке (3) в (4). Иными словами, должна существовать такая матрица B, что $A \cdot B$ равно *единичной матрице*

$$E = \begin{pmatrix} \varepsilon & & 0 \\ & \varepsilon & \\ & & \ddots \\ 0 & & \varepsilon \end{pmatrix}.$$

Таким образом:

Преобразование (3) *дает новый базис тогда и только тогда, если матрица A не является левым делителем нуля и обладает правой обратной матрицей B.*

Если эти требования выполняются, то, и, обратно, u_i образуют базис, если u_i' элементы базиса, т. е. также имеет место

$$BA = E.$$

Затем еще следует, что A не может быть правым делителем нуля, так как если бы для строки $S \neq 0$ произведение SA было равно нулю, то отсюда следовало бы, что

$$0 = SAB = SE = S \neq 0.$$

Наконец, A может обладать только *единственной* правой обратной матрицей, так как A не является левым делителем нуля.

Поэтому единственную правую (и левую) обратную матрицу B мы можем обозначить через A^{-1}. Матрицу A, удовлетворяющую указанным требованиям, мы будем называть *обратимой* в $\mathfrak{K}$. Итак:

Переход к новому базису осуществляется с помощью обратимой матрицы.

Если величины $u_1', \ldots, u_n$ рассматривать как неизвестные в области полиномов $\mathfrak{K}[u_1, \ldots, u_n]$, то получим другое истолкование линейных преобразований. В этом случае формулы (3), (4) будут определять *линейную подстановку*, переводящую старые неизвестные в новые u'. Подстановкой (4) форма $f(u_1, \ldots, u_n)$ переводится в форму $f'(u_1', \ldots, u_n')$; в частности линейная форма $\sum u_k\lambda_k$ переходит в линейную форму

$$\sum u_k\lambda_k = \sum\sum u_j'\beta_{jk}\lambda_k = \sum u_j'\lambda_j',$$

причем новые коэфициенты будут равны:

$$\lambda_j' = \sum_k \beta_{jk}\lambda_k. \tag{5}$$

Формула (5) представляет линейное преобразование вектора $(\lambda_1, \ldots, \lambda_n)$ с матрицей B.

Если, с другой стороны, переменным u_i дать частные значения μ_i из поля $\mathfrak{K}$ и составить согласно с (3)

$$\mu_k' = \sum \mu_j\alpha_{jk}, \tag{6}$$

то получится также линейное преобразование (с транспонированной матрицей $\widetilde{A}$ [1])) в векторном пространстве или в модуле линейных форм; на этот раз область операторов будет *левой*, так как коэфициенты преобразования стоят *справа* от векторных компонентов.

Преобразования (5), (6) связаны друг с другом требованием инвариантности суммы $\sum \mu_k\lambda_k$:

$$\sum \mu_k\lambda_k = \sum \mu_k'\lambda_k'$$

и называются *контрагредиентными друг с другом.* При этом между матрицами $\widetilde{A}$ и $\widetilde{B}$ имеет место следующее соотношение:

$$\widetilde{A} = \widetilde{B}^{-1}.$$

Задачи. 1. Если квадратная матрица обладает правой и левой обратной матрицей, то она обратима (т. е. обе обратные матрицы равны и единственные).

2. Если A — левый делитель нуля и обладает правой обратной матрицей, то A обладает бесчисленным множеством правых обратных матриц (автору неизвестно, могут ли вообще требования задачи выполняться для конечной квадратной матрицы; но высказанная теорема справедлива также для бесконечных матриц, и в этом случае легко найти пример, отвечающий требованиям задачи. Для конечных матриц в поле или в области целостности требования наверняка не удовлетворяются; см. § 105.

3. Обратимые матрицы кольца $\mathfrak{K}$ с единицей, состоящие из n рядов, образуют группу: *линейную однородную группу в* $\mathfrak{K}$ или группу автоморфизмов n-членного модуля линейных форм.

---

[1]) Замена строк столбцами и обратно называется транспонированием.

4. Все квадратные матрицы n-го порядка образуют кольцо, *полное кольцо матриц* K или кольцо автоморфизмов n-членного модуля линейных форм. Это кольцо обладает базисом, линейно независимым относительно K; элементами базиса являются матрицы C_{ij}, у которых на пересечении i-й строки и j-го столбца стоит единица, а остальные элементы равны нулю.

5. Гомоморфизмы модулей линейных форм с бесконечным числом переменных (причем рассматриваются всякий раз линейные формы с конечным числом переменных) представляются только такими бесконечными матрицами, у которых в каждом столбце содержится конечное число элементов, отличных от нуля. Распространить теорию обратимых матриц на этот случай.

6. Если линейное отображение $\mathfrak{M} = (u_1, \ldots, u_n)$ на $\mathfrak{N} = (v_1, \ldots, v_n)$ представляется матрицей A и новые базисы $u_1', \ldots, u_n', v_1', \ldots, v_n'$ получаются с помощью преобразований:

$$(u_1', \ldots, u_n') = (u_1, \ldots, u_n)\, P,$$
$$(v_1', \ldots, v_n') = (v_1, \ldots, v_n)\, Q,$$

то относительно новых базисов отображение будет определяться матрицей

$$A' = Q^{-1} A P.$$

7. Если матрицу A, состоящую из n строк и m столбцов, каким-нибудь образом разбить на прямоугольные клеточки, например:

$$A = \left(\begin{array}{c|c|c} \alpha_{11} \cdots & \alpha_{1i} \cdots & \alpha_{1j} \cdots \alpha_{1m} \\ \vdots & & \vdots \\ \hline & & \\ \alpha_{k1} & & \\ \vdots & & \\ \alpha_{n1} \cdots & \cdots\cdots & \cdots\cdots \alpha_{nm} \end{array}\right) = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix},$$

а матрицу B, состоящую из m строк и q столбцов, также разбить на клеточки, но так, чтобы при соответствующем наложении горизонтальные сечения B совпадали с вертикальными сечениями $(1, i, j)$ матрицы A:

$$B = \left(\begin{array}{c|c|c} \beta_{11} \cdots & \beta_{1h} \cdots & \cdots \beta_{1q} \\ \vdots & & \vdots \\ \hline \beta_{i1} & & \\ \vdots & & \\ \hline \beta_{j1} & & \\ \vdots & & \\ \beta_{m1} \cdots & \cdots\cdots & \cdots \beta_{mq} \end{array}\right) = \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{pmatrix},$$

то можно A умножить на B так, как если бы клеточки A_{ij}, B_{ik} были элементами

$$AB = \begin{pmatrix} \sum A_{1j}B_{j1} & \sum A_{1j}B_{j2} & \sum A_{1j}B_{j3} \\ \sum A_{2j}B_{i1} & \sum A_{2j}B_{i2} & \sum A_{2j}B_{i3} \end{pmatrix}.$$

§ 105. МОДУЛИ ОТНОСИТЕЛЬНО ПОЛЯ. ЛИНЕЙНЫЕ УРАВНЕНИЯ

Допустим теперь, что K — поле (не обязательно коммутативное), модуль $\mathfrak{M}$ конечен и единица является единичным оператором. Если между элементами базиса $u_1, \ldots, u_n$ существует линейная зависимость $\sum u_i\lambda_i = 0$, причем, например, $\lambda_n \neq 0$, то можно равенство умножить на λ_n^{-1} и u_n выразить линейно через остальные элементы базиса. Таким образом $u_1, \ldots, u_{n-1}$ образуют также базис. Продолжая подобным образом наши рассуждения, мы придем, наконец, к линейно независимому базису. Тем самым всякий конечный модуль рассматриваемого рода есть модуль линейных форм.

Модуль, отличный от нулевого модуля (0), называется (как и обыкновенная абелева группа) *простым*, если он не обладает, кроме нулевого модуля, собственным подмодулем. Оказывается справедливой следующая теорема: *простой K-модуль может быть только одночленным, а одночленный K-модуль — простым.*

Доказательство. 1. Пусть $\mathfrak{M}$ — простой. Тогда любой элемент $u \neq 0$ должен порождать весь модуль; таким образом $\mathfrak{M}$ есть одночленный модуль.

2. Пусть $\mathfrak{M}$ есть одночленный модуль: $\mathfrak{M} = (u)$. Если $\mathfrak{N} \neq (0)$ подмодуль и $u\lambda$ — элемент из $\mathfrak{N}$, отличный от нуля, то $\mathfrak{N}$ содержит также $u\lambda\lambda^{-1} = u$, откуда $\mathfrak{M} = \mathfrak{N}$. Таким образом $\mathfrak{M}$ — простой модуль.

n-членный модуль есть прямая сумма простых модулей $(u_1) = u_1\mathsf{K}\ldots$, $(u_n) = u_n\mathsf{K}$. Подмодули $(u_1, \ldots, u_n)$, $(u_1, \ldots, u_{n-1}), \ldots (u_1)$, (0) образуют *композиционный ряд*, так как $(u_1, \ldots, u_i)/(u_1, \ldots, u_{i-1})$ суть одночленные простые фактор-модули. *Итак, число членов n-модуля равно длине композиционного ряда и потому не зависит от выбора базиса.*

Число членов K-модуля называется также (*линейным*) *рангом модуля относительно* K.

Единственность линейного ранга нами была обнаружена еще в § 28 несколько иным путем. Базис подмодуля может быть дополнен до базиса всего модуля; но это не что иное, как теоретикогрупповая теорема о том, что через любой подмодуль можно провести композиционный ряд. Дополнение базиса подмодуля до базиса $\mathfrak{M}$ происходит таким образом, что недостающие элементы базиса выбираются из u_j (т. е. из данного базиса $\mathfrak{M}$); согласно § 42 это объясняется тем обстоятельством, что модуль $\mathfrak{M}$ есть прямая сумма простых одночленных модулей. Но все это есть не что иное, как теорема Штейница (§ 28).

Собственный подмодуль $\mathfrak{M}$ имеет композиционный ряд меньшей длины, чем $\mathfrak{M}$; таким образом число членов подмодуля должно быть меньше числа членов $\mathfrak{M}$. Отсюда следует, *что n линейно независимых элементов $v_k = \sum u_i\alpha_{ik}$ модуля $\mathfrak{M}$ порождают $\mathfrak{M}$*, так как они не могут порождать собственный подмодуль. Условие линейной независимости означает, что матрица A не является левым делителем нуля; но если v

образуют новый базис $\mathfrak{M}$, то матрица обратима. Таким образом мы видим, что *если квадратная матрица поля* K *не является левым делителем нуля, то она обратима.* В этом случае матрица называется *правильной*; но если она есть левый делитель нуля (т. е. не обратима и потому есть также правый делитель нуля), то она называется *особенной.* Все эти определения распространяются и на матрицы области целостности $\mathfrak{R}$, так как $\mathfrak{R}$ всегда можно заключить в поле. В области целостности $\mathfrak{R}$ правильная матрица может оказаться необратимой, но в поле отношений K она должна быть обратимой. Что касается особенных матриц, то они не только в поле, но и в кольце будут делителями нуля, так как столбец, уничтожающий матрицу, после умножения на общий знаменатель становится целым

Теория линейных уравнений основана на теореме Штейница (§ 28). Систему таких уравнений можно записать в виде:

$$l_i(\xi) = \beta_i \qquad (i = 1, \ldots, m), \tag{1}$$

причем l_i суть линейные формы от n элементов ξ_k:

$$l_i(\xi) = \sum \alpha_{ik}\xi_k.$$

Если заменим ξ_k неизвестными x_k, то l_i будут линейными формами этих неизвестных:

$$l_i = \sum \alpha_{ik}x_k. \tag{2}$$

Число r линейно независимых форм l_i называется *рангом* системы уравнений. Очевидно, что для разрешимости системы уравнений необходимо, чтобы линейные соотношения $\sum u_i l_i \equiv 0$ (относительно x) распространялись на правые части β_i. Если это выполняется и l_i зависят, например, от $l_1, \ldots, l_r$, то все уравнения (1) являются следствиями первых r уравнений. $r \leqslant n$, так как может существовать самое большее n линейно независимых форм переменных $x_1, \ldots, x_n$. Согласно теореме Штейница можно дополнить $l_1, \ldots, l_r$ $n - r$ неизвестными x_i (а именно $x_{r+1}, \ldots, x_n$) до базиса всех линейных форм x. Это значит, что

$$x_i = \sum_{r+1}^{n} \gamma_{ij}x_j + \sum_{1}^{r} \delta_{ik}l_k \quad (i = 1, \ldots, r). \tag{3}$$

Теорема. *Чтобы получить все решения уравнения* (1), *надо в* (3) *заменить* l_i *через* β_i, *а* $x_{r+1}, \ldots, x_n$ *заменить совершенно произвольными величинами* $\xi_{r+1}, \ldots, \xi_n$ *из* K; *тогда значения* $\xi_1, \ldots, \xi_r$ *неизвестных* $x_1, \ldots, x_r$ *найдутся из* (3).

Для доказательства отметим, что $l_1, \ldots, l_r, x_{r+1}, \ldots, x_n$ образуют линейно независимый базис модуля $(x_1, \ldots, x_n)$. Таким образом если подставить (3) в (2), то получатся тождества относительно

$$l_1, \ldots, l_r, x_{r+1}, \ldots, x_n,$$

которые сохранятся и после замены l_i через β_i и x_j через произвольные ξ_j. Следовательно, эти ξ являются решениями (1). Если же подставить (2) в (3), то получится тождество относительно x, которое останется в силе и после замены x величинами ξ, удовлетворяющими (1). Таким образом мы имеем все решения (1).

Все это показывает, что приведенный выше критерий разрешимости также и достаточен и что ранг системы уравнений равен числу неизвестных, подлежащих определению; значения остальных неизвестных совершенно произвольны.

Пользуясь методом *последовательных исключений*, можно установить, какие именно l_i линейно независимы, и вывести формулы (3). Для этого решается сперва одно из уравнений

$$l_i = \sum a_{ik} x_k$$

относительно некоторого x_j, и затем x_j подставляется в остальные уравнения; в результате элемент базиса x_j заменится l_i. Продолжаем этот процесс замены элементов базиса. В итоге либо в новый базис войдут все l, либо некоторые l_k не войдут в базис. В последнем случае для l_k получатся выражения, не содержащие x, и l_k будут линейно зависеть от l_i. Тогда эти линейные соотношения окажутся справедливыми и для β_i; точнее выражаясь, l_i можно заменить известными β_i. Пусть для определенности $(l_1, \ldots, l_r, x_{r+1}, \ldots, x_n)$ — новый базис, который получился при последовательном исключении. Тогда всякое $x_i\,(i = 1, \ldots, r)$ будет линейно выражаться через элементы рассматриваемого базиса, т. е. получим формулы (3).

Отсюда следует, что *если коэфициенты системы уравнений принадлежат некоторому подполю, то в этом же подполе лежат коэфициенты формул* (3), *а также коэфициенты линейной зависимости между левыми частями уравнений. Ограничиваясь указанным подполем, можно высказать вполне определенное суждение о разрешимости или несовместности системы.*

В частности для коммутативного K с помощью *теории определителей* получаются более точные формулы решения и алгебраические критерии разрешимости и линейной зависимости. Но особенно важен следующий критерий правильности матрицы; *квадратная матрица A в коммутативном поле или области целостности правильна, если ее определитель $|A|$ отличен от нуля.* Если сверх того определитель равен делителю единицы области целостности, то матрица в этой области обратима, так как в формулах решения определитель войдет только в знаменатель.

Применяя правило умножения определителей

$$|AB| = |A| \cdot |B|$$

к случаю $AB = E$, $|E| = 1$, получим обратную теорему. Итак, *в области целостности обратимы только такие матрицы, у которых определитель равен делителю единицы* (*унимодулярные матрицы*).

Задачи 1. Система однородных уравнений $\sum \alpha_{ik} \xi_k = 0$ в поле всегда разрешима и все решения $\{\xi_1, \ldots, \xi_n\}$, рассматриваемые как векторы, получаются из $n - r$ частных, линейно независимых решений. При $r = n$ существует только нулевое решение.

2. Пусть n — число членов некоторого K-модуля, m — число членов подмодуля и f — число членов фактор-модуля (модуля вычетов). Тогда $f = n - m$.

3. Между числом членов n, m двух подмодулей некоторого K-модуля, числом членов s их суммы и числом членов d их пересечения имеет место следующая зависимость:

$$s + d = n + m.$$

Проективное пространство. Одночленные подмодули n-членного модуля линейных форм или векторов можно отождествить с *лучами* векторного пространства $R_n(\mathsf{K})$ или с *точками* проективного $(n-1)$-мерного пространства $P_{n-1}(\mathsf{K})$. Компоненты вектора (они определяются с точностью до пропорционального множителя) называются однородными *координатами точки*. Лучи подмодуля образуют *линейное подпространство* проективного пространства. Из задачи 1 следует, что r линейно независимых уравнений координат определяют подпространство $(n-r-1)$-го измерения. Так как пересечение подмодулей есть также подмодуль, то отсюда следует, что пересечение линейных пространств в свою очередь является линейным (или пустым) пространством. Наконец, из задачи 3 следует, что между измерениями l, m двух линейных подпространств, измерением d их пересечения и измерением s наименьшего пространства, содержащего данные пространства, имеет место соотношение:

$$d + s = l + m,$$

причем $d = -1$, когда пересечение пустое.

§ 106. МОДУЛИ В КОЛЬЦЕ ГЛАВНЫХ ИДЕАЛОВ. ЭЛЕМЕНТАРНЫЕ ДЕЛИТЕЛИ

Допустим теперь, что кольцо K не содержит делителей нуля и что либо (*первый случай*) для всякого элемента a из K определена целая неотрицательная абсолютная величина $|a|$ и возможно левое и правое деление (см. § 13)

$$a = bq + r, \quad |r| < |b|, \quad a = q'b + r', \quad |r'| < |b|;$$

либо (*второй случай*) K коммутативно и в K всякий идеал является главным. (В этом случае согласно § 16 K называется кольцом главных идеалов.)

Кольцо C целых чисел подходит под оба эти случая. Область полиномов $\mathsf{P}[x]$, где P — поле, отвечает первому случаю, если только мы будем подразумевать под абсолютной величиной степень полинома, увеличенную на единицу, а нулю припишем абсолютную величину, равную нулю.

В обоих случаях в K всякий левый или правый идеал будет главным, и для любых элементов a и b существует общий наибольший правый делитель $d = (a,b)$ со свойством

$$a = \alpha d; \quad b = \beta d; \quad d = \lambda a + \mu b = \lambda\alpha d + \mu\beta d, \quad 1 = \lambda\alpha + \mu\beta. \qquad (1)$$

Точно так же существует левый делитель d', обладающий теми же свойствами. Во втором (коммутативном) случае согласно § 17 в K выполняется единственность разложения на множители. В этом случае из (1) следует обратимость матрицы

$$\begin{pmatrix} \alpha & -\mu \\ \beta & \lambda \end{pmatrix},$$

преобразующей вектор $\begin{pmatrix} d \\ 0 \end{pmatrix}$ в $\begin{pmatrix} a \\ b \end{pmatrix}$. Очевидно, что обратная матрица

$$\begin{pmatrix} \lambda & \mu \\ -\beta & \alpha \end{pmatrix}$$

переводит $\begin{pmatrix} a \\ b \end{pmatrix}$ в $\begin{pmatrix} d \\ 0 \end{pmatrix}$.

Теорема. *Пусть* $\mathfrak{M}$ *будет модуль линейных форм относительно* K *с линейно независимым базисом* $(u_1, \ldots, u_n)$. *Тогда любой его подмодуль* $\mathfrak{N}$ *будет также модулем линейных форм; при этом число элементов базиса* $\mathfrak{N}$ *не превосходит* n.

Доказательство. Для нулевого модуля $\mathfrak{M} = (0)$ теорема тривиальна. Допустим, что она доказана для $(n-1)$-членного модуля $\mathfrak{M}$.

Если $\mathfrak{N}$ состоит только из линейных форм переменных $u_1, \ldots, u_{n-1}$, то в силу индуктивного предположения все доказано. Но если $\mathfrak{N}$ содержит линейные формы $u_1\lambda_1 + \ldots + u_n\lambda_n$, $\lambda_n \neq 0$, то λ_n в K образует правый идеал; таким образом это будет главный идеал (μ_n), $\mu_n \neq 0$. Отсюда следует, что $\mathfrak{N}$ содержит также форму $l = u_1\mu_1 + \ldots + u_n\mu_n$. Последний коэфициент λ_n формы $u_1\lambda_1 + \ldots + u_n\lambda_n$ можно сделать равным нулю, если вычесть из $u_1\lambda_1 + \ldots + u_n\lambda_n$ форму l, умноженную на соответствующее α. В результате получим линейные формы от переменных $u_1, \ldots, u_{n-1}$, принадлежащие $\mathfrak{N}$. Они образуют подмодуль, который согласно индуктивному предположению обладает линейно независимым базисом $(l_1, \ldots, l_{m-1})$, где $m - 1 \leqslant n - 1$. Но тогда $l_1, \ldots, l_{m-1}, l$ порождают $\mathfrak{N}$. $l_1, \ldots, l_{m-1}, l$ независимы, так как если бы имело место

$$l_1\beta_1 + \ldots + l_{m-1}\beta_{m-1} + l\beta = 0, \quad \beta \neq 0,$$

то после сравнения коэфициентов при u_n получилось бы $\mu_n\beta = 0$, что невозможно.

Замечание. Линейная независимость $l_1, \ldots, l_m$ $(l_m = l)$ объясняется, очевидно, тем, что каждое l_i по построению содержит такое u_j, которое не входит в $l_1, \ldots, l_{i-1}$.

Задачи. 1. Если $\mathfrak{M}$ есть модуль целочисленных линейных форм и дано, что подмодуль $\mathfrak{N}$ порожден конечным множеством линейных форм

$$v_k = \sum u_i\alpha_{ik},$$

то линейно независимый базис $(l_1, \ldots, l_m)$ можно построить с помощью конечного числа операций.

2. Пользуясь базисом $(l_1, \ldots, l_m)$ задачи 1, указать критерий, с помощью которого можно узнать, принадлежит ли данная линейная форма $\beta_1u_1 + \ldots + \beta_nu_n$ модулю $\mathfrak{N}$ (т. е., иными словами, будет ли система линейных дифантовых уравнений

$$\sum \alpha_{ik}\xi_k = \beta_i$$

разрешима в целых числах ξ_k).

Теорема об элементарных делителях. *Если* $\mathfrak{N}$ *— подмодуль модуля* $\mathfrak{M}$ *линейных форм, то существует такой базис* $(u_1, \ldots, u_n)$ *и базис* $(v_1, \ldots, v_m)$ *модуля* $\mathfrak{N}$, *что*

$$\left.\begin{array}{l} v_i = u_i\varepsilon_i \\ \varepsilon_{i+1} \equiv 0 \ (\varepsilon_i) \end{array}\right\} \ (i = 1, \ldots, m).$$

(В некоммутативном случае последнее условие делимости выполняется слева и справа.)

Доказательство. Возьмем сперва какой-нибудь базис $(u_1, \ldots, u_n)$ модуля $\mathfrak{M}$ и какой-нибудь базис $(v_1, \ldots, v_m)$ подмодуля $\mathfrak{N}$; пусть

$$v_k = \sum u_i\alpha_{ik}$$

или

$$(v_1, \ldots, v_m) = (u_1, \ldots, u_n) \cdot A.$$

Пользуясь некоторыми преобразованиями, можно матрицу A привести к диагональной форме:

$$\begin{pmatrix} \varepsilon_1 & & & 0 \\ & \varepsilon_2 & & \\ & & \ddots & \\ 0 & & & \varepsilon_m \end{pmatrix}. \tag{2}$$

Это следующие операции:

1. Перестановка двух u или v, равносильная перестановке двух строк или столбцов A.

2. Замена u_i через $u_i + u_j\lambda\,(j \neq i)$, что равносильно вычитанию из j-й строки i-й строки A, умноженной слева на λ:

$$v_k = \sum u_i\alpha_{ik} = \ldots + (u_i + u_j\lambda)\,\alpha_{ik} + \ldots + u_j(\alpha_{jk} - \lambda\alpha_{ik}) + \ldots$$

3. Замена v_k через $v_k - v_j\lambda\,(j \neq k)$, что равносильно вычитанию из k-го столбца j-го столбца, умноженного справа на λ:

$$v_k - v_j\lambda = \sum u_i(\alpha_{ik} - \alpha_{ij}\lambda).$$

Если в K возможно деление, то этими операциями все исчерпывается. В противном случае надо еще добавить преобразования вида:

4.

$$(u_i, u_j) = (u_i', u_j')\begin{pmatrix} \lambda & \mu \\ -\beta & \alpha \end{pmatrix}.$$

5.

$$(v_i', v_j') = (v_i, v_j)\begin{pmatrix} \lambda & -\beta \\ \mu & \alpha \end{pmatrix}.$$

Прежде всего рассмотрим *первый* (простейший) *случай*.

Станем преобразовывать матрицу A с помощью операций 1, 2, 3 так, *чтобы наименьший по абсолютной величине элемент A, отличный от нуля, принял возможно меньшее не равное нулю абсолютное значение*. С помощью операций 1 этот наименьший элемент можно передвинуть на место α_{11}. Если затем все остальные элементы первого столбца сделать по возможности наименьшими, вычитая соответствующие кратные первой строки, то их абсолютная величина будет меньше $|\alpha_{11}|$, т. е. станет равной нулю. Точно так же с помощью операции 3 можно обратить в нули элементы первой строки, причем от этого первый столбец не изменится. После таких операций элементы матрицы будут делиться на α_{11} (и притом слева и справа). В самом деле, если бы, например, α_{ik} не делилось слева на α_{11}, то при помощи алгоритма деления мы бы получили:

$$\alpha_{ik} = \alpha_{11}q + r,\ r \neq 0,\ |r| < |\alpha_{11}|.$$

Складывая первую строку с i-й и вычитая затем первый столбец, умноженный на q, из k-го, получим вместо α_{ik} элемент r, причем $|r| < |\alpha_{11}|$, что противоречит минимальности α_{11}.

(Если α_{ik} не делится справа на α_{11}, то операции 2, 3 применяются в обратном порядке.)

После всех этих операций наша матрица примет следующий вид:

$$\begin{pmatrix} \alpha_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix},$$

где элементы A' являются кратными (левыми и правыми) α_{11}. Дальнейшие преобразования матрицы A уже не меняют первую строку и столбец; изменяться будет только A'. Если после какой-нибудь из этих операций оказалось бы, что не все элементы делятся (справа и слева) на α_{11}, то мы получили бы по вышедоказанному элемент $r \neq 0$, абсолютная величина которого была бы меньше $|\alpha_{11}|$, что невозможно. Таким образом все время будет сохраняться делимость на α_{11}. В результате A' примет вид:

$$\begin{pmatrix} \alpha_{22} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{pmatrix},$$

где все элементы A'' делятся с двух сторон на α_{22}. Продолжая подобные преобразования, мы получим, наконец, искомую нормальную форму (2). Случай, когда часть матриц $A, A', A'', \ldots$ состоит только из нулей, исключается, так как это означало бы, что некоторые v_k равны нулю, что невозможно, так как на каждом этапе преобразования v_k образуют линейно независимый базис $\mathfrak{N}$. Таким образом первый случай теоремы доказан.

Во втором случае ход доказательства совершенно такой же, только — так как здесь абсолютная величина $|\alpha|$ не имеет смысла — надо выставить другое требование минимальности, а именно, *надо взять элемент, разлагающийся на наименьшее число простых множителей.* Вместо деления здесь будут применяться операции 4, 5; благодаря этому два элемента a, b одной и той же строки или столбца заменятся величинами d,0, где d — общий наибольший делитель a,b. Если $a = \alpha_{11}$ и b не делятся на α_{11}, то d будет иметь меньше простых множителей, чем α_{11}, и требование минимальности нарушается. Таким образом все элементы первой строки и столбца должны делиться на α_{11}; поэтому они с помощью операций 2 и 3 могут быть приведены к нулю, и т. д. [1]).

Замечания 1. Операции 1—5 равносильны умножению матрицы A слева и справа на матрицу, обратимую в $\mathfrak{K}$. В самом деле, если $(u_1', \ldots, u_n') = (u_1, \ldots, u_n)B$ и $(v_1', \ldots, v_m') = (v_1, \ldots, v_m)C$ суть новые базисы, то $(v_1', \ldots, v_m') = (v_1, \ldots, v_m)C = (u_1, \ldots, u_n)AC = (u_1', \ldots, u_n')B^{-1}AC$. Таким образом теорема об элементарных делителях равносильна существованию двух таких обратимых матриц B, C, что $B^{-1}AC$ есть матрица вида (2).

[1]) Доказательство настоящей теоремы для некоммутативного кольца $\mathfrak{K}$ с алгоритмом деления (например для области полиномов $P[x]$, где P — некоммутативное поле), кажется, в литературе еще не встречалось. Автору пока не удалось найти условий, объединяющих два упомянутых выше случая.

2. Тот же метод приведения матрицы A оказывается пригодным и тогда, если v линейно зависимы; тогда часть матриц $A, A', A'', \ldots$ может оказаться нулевой, и мы вместо нормальной формы получим более общего вида матрицу:

$$B^{-1}AC = \begin{pmatrix} \varepsilon_1 & & & 0 \\ & \ddots & & \\ & & \varepsilon_r & \\ 0 & & & 0 \end{pmatrix}, \tag{3}$$

где r — ранг A. Условие делимости величин ε_i остается то же.

3. В коммутативном случае субдетерминанты k-го порядка матрицы $D = B^{-1}AC$ линейно зависят от подобных же субдетерминантов A; точно так же определители k-го порядка $A = BDC^{-1}$ линейно зависят от определителей k-го порядка D. Таким образом определители k-го порядка матрицы A имеют с точностью до делителей единицы такой же общий наибольший делитель δ_k, что и соответствующие определители D. Но для D мы получаем:

$$\delta_k = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_k \qquad (k \leqslant r),$$

откуда

$$\delta_k = \delta_{k-1}\, \varepsilon_k \qquad (1 < k \leqslant r). \tag{4}$$

δ_k называются *делителями детерминантов* матрицы A, ε_k — *элементарными делителями* матрицы A. Из (4) следует, что *элементарные делители* ε_k *равны отношению* $\frac{\delta_k}{\delta_{k-1}}$ *делителей детерминантов*.

4. В следующем параграфе будет еще раз показано, что в коммутативном случае элементарные делители ε_k определяются матрицей A однозначно с точностью до делителей единицы. Именно будет показано, что элементарные делители (поскольку они не являются делителями единицы) зависят только от фактор-модуля $\frac{\mathfrak{M}}{\mathfrak{N}}$, который в свою очередь определяется матрицей A.

Целый ряд изящных теорем о целочисленных модулях можно найти у A. Châtelet, Leçons sur la théorie des Nombres, Paris 1913.

Задачи. 3. Привести матрицу

$$A = \begin{pmatrix} 4 & 3 & 6 & 2 \\ 2 & 3 & 6 & 4 \\ 6 & 6 & 13 & 5 \end{pmatrix}$$

к диагональному виду (3).

4. Всякая линейная диофантова система уравнений

$$\sum_1^n \alpha_{ik}\xi_k = \beta_i \qquad (i = 1, \ldots, m) \tag{5}$$

(α_{ik} и β_i — целые числа) может быть приведена с помощью унимодулярных преобразований над ξ_k и уравнениями к виду:

$$\varepsilon_i \eta_i = \gamma_i \qquad (i = 1, \ldots, r;\ \varepsilon_i \neq 0),$$
$$0 = \delta_j \qquad (j = r+1, \ldots, m).$$

При этом условием разрешимости системы в целых числах является

$$\gamma_i \equiv 0\,(\varepsilon_i);\ \delta_j = 0.$$

Числа $\eta_i\ (i \leqslant r)$ определяются из уравнений, а остальные η_j произвольны. ξ_k — линейные целочисленные функции произвольных η_j.

5. Линейная система уравнений (5) тогда и только тогда разрешима в целых числах, если из

$$\sum_1^m \lambda_i \alpha_{ik} \equiv 0\,(d) \qquad (k = 1, \ldots, n)$$

для произвольных целых чисел λ_i и d всегда следует, что

$$\sum_1^m \lambda_i \beta_i \equiv 0\,(d).$$

§ 107. ОСНОВНАЯ ТЕОРЕМА АБЕЛЕВЫХ ГРУПП

Пусть $\mathfrak{G}$ будет аддитивная абелева группа с конечным числом образующих, т. е. модуль. Относительно мультипликаторной области K группы $\mathfrak{G}$ (если таковая задана) мы предположим, что K есть кольцо без делителей нуля с алгоритмом деления или кольцо главных идеалов. Если же мультипликаторная область не дана, то за мультипликаторную область мы примем кольцо целых чисел. Здесь мы будем операторы писать слева от элементов модуля.

Пусть сперва $\mathfrak{G}$ — циклическая группа: $\mathfrak{G} = (g)$. Совокупность элементов μ из K, уничтожающих g, образует левый идеал $\mathfrak{a}$ кольца K: из $\mu_1 g = 0$ и $\mu_2 g = 0$ следует, что $(\mu_1 - \mu_2) g = 0$, а из $\mu g = 0$ следует, что $\varkappa \mu g = 0$ для всякого $\varkappa$ из K. Всякому λ из K приводится в соответствие λg, в силу

$$(\lambda + \mu) g = \lambda g + \mu g,$$
$$(\lambda \mu) g = \lambda (\mu g)$$

это соответствие является операторным гомоморфизмом относительно K. Отсюда согласно теореме изоморфизма

$$\mathfrak{G} \cong \frac{\mathsf{K}}{\mathfrak{a}},$$

т. е. *циклический K-модуль $\mathfrak{G}$ изоморфен модулю вычетов K по левому идеалу, уничтожающему элементы $\mathfrak{G}$.*

Отсюда в случае обыкновенной циклической группы $\mathfrak{G}$ мы снова приходим к выводу, что $\mathfrak{G}$ изоморфно аддитивной группе целых чисел или группе классов вычетов по целому числу. Если целое число $n > 0$ есть элемент базиса идеала $\mathfrak{a}$, то n равно порядку циклической группы (g) или порядку элемента g (см. § 7).

Доказанная выше теорема справедлива независимо от частных предположений относительно K. Но если K коммутативно, свободно от делителей нуля и всякий идеал K является главным, в частности если

$\mathfrak{a} = (\alpha)$, $\alpha \neq 0$, то мы можем высказать нечто большее. Разложим, если это возможно, α на два взаимно простых сомножителя:

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

$$1 = \lambda\rho + \mu\sigma,$$

и возьмем циклические группы $\mathfrak{G}_1 = (\rho g)$, $\mathfrak{G}_2 = (\sigma g)$. Тогда $\mathfrak{G}_1$ будет уничтожаться элементом σ, $\mathfrak{G}_2$ — элементом ρ. Так как

$$g = \lambda\rho g + \mu\sigma g,$$

то $\mathfrak{G}$ равно сумме $\mathfrak{G}_1$ и $\mathfrak{G}_2$. Пересечение $\mathfrak{G}_1 \cap \mathfrak{G}_2$ уничтожается элементами ρ и σ, а поэтому $\mathfrak{G}_1 \cap \mathfrak{G}_2$ уничтожается элементом $1 = \lambda\rho + \mu\sigma$; следовательно, $\mathfrak{G}_1 \cap \mathfrak{G}_2 = (0)$ и сумма прямая:

$$\mathfrak{G} = \mathfrak{G}_1 + \mathfrak{G}_2.$$

Если затем разложить σ или ρ на взаимно простые множители, то $\mathfrak{G}_1$ или $\mathfrak{G}_2$ распадутся на сумму. *Итак, циклическая группа $\mathfrak{G}$ равна прямой сумме циклических групп, которые уничтожаются соответствующими степенями простых элементов* [1]). *Произведение этих степеней простых элементов равно α.* Для групп подобного рода мы будем употреблять термин „*группы простых степеней*“.

Теперь возьмем общий случай, когда $\mathfrak{G}$ есть $\mathfrak{K}$-модуль с конечным числом образующих $g_1, \ldots, g_n$, т. е. элементы $\mathfrak{G}$ имеют вид:

$$\lambda_1 g_1 + \ldots + \lambda_n g_n.$$

С помощью переменных $u_1, \ldots, u_n$ составим модуль

$$\mathfrak{M} = (u_1, \ldots, u_n)$$

линейных форм; тогда всякой линейной форме $\sum \lambda_i u_i$ из $\mathfrak{M}$ будет соответствовать элемент $\sum \lambda_i g_i$ из $\mathfrak{G}$. Соответствие снова будет гомоморфизмом модулей, откуда

$$\mathfrak{G} \cong \frac{\mathfrak{M}}{\mathfrak{N}},$$

где $\mathfrak{N}$ — подмодуль линейных форм $\sum \lambda_i u_i$, для которых $\sum \lambda_i g_i = 0$. В силу § 106 мы можем ввести новые базисы $(v_1, \ldots, v_m)$ и $(u_1', \ldots, u_n')$ $(m \leqslant n)$ для $\mathfrak{N}$ и $\mathfrak{M}$, причем

$$v_i = \varepsilon_i u_i', \qquad \text{для } i = 1, \ldots, m.$$

$$\varepsilon_{i+1} \equiv 0 \,(\varepsilon_i)$$

В силу гомоморфизма элементам u' соответствуют элементы $h_1, \ldots, h_n$ группы $\mathfrak{G}$. Все элементы $\mathfrak{G}$ имеют вид $\mu_1 h_1 + \ldots + \mu_n h_n$, а такие элементы равны нулю тогда и только тогда, если

$$\mu_1 u_1' + \ldots + \mu_n u_n' \equiv 0 \,(v_1, \ldots, v_m),$$

т. е. если

$$\left.\begin{array}{l} \mu_1 \equiv 0 \,(\varepsilon_1) \\ \ldots\ldots \\ \mu_m \equiv 0 \,(\varepsilon_m) \end{array}\right\} \quad \begin{array}{l} \mu_{m+1} = 0, \\ \ldots\ldots \\ \mu_n = 0. \end{array}$$

[1]) Т. е. простых элементов кольца $\mathfrak{K}$. В случае обыкновенных абелевых групп речь идет об обыкновенных простых числах.

Это означает, что сумма $\mu_1 h_1 + \ldots + \mu_n h_n$ тогда и только тогда равна нулю, когда коэфициенты μ_i делятся на ε_i при $i = 1, \ldots, m$, а все остальные коэфициенты равны нулю.

Эту теорему можно сформулировать еще так:

Группа $\mathfrak{G}$ *равна прямой сумме* $(h_1) + \ldots + (h_n)$ *циклических групп, и идеалом, уничтожающим* (h_i), *является*:

$$(\varepsilon_i) \text{ при } i = 1, \ldots, m,$$

$$(0) \text{ при } i = m+1, \ldots, n.$$

Это — *основная теорема абелевых групп с конечным числом образующих.*

В случае обыкновенных абелевых групп ε_i равны порядкам циклических групп $(h_1), \ldots, (h_m)$, в то время как остальные $(h_{m+1}), \ldots, (h_n)$, бесконечного порядка.

Небесполезны следующие три дополнения к основной теореме;

a) Можно исключить ε_i, которые являются делителями единицы.

b) Циклические группы допускают дальнейшее разложение на группы простых степеней.

c) Единственность.

Для „b" и „c" $\mathfrak{K}$ предполагается *коммутативным.*

a) Пусть, например, ε_1 — делитель единицы, т. е. (ε_1) — единичный идеал $\mathfrak{K}$; тогда $\mathfrak{K}h_1 = (0)$, и циклическую группу $\mathfrak{K}h_1$ можно устранить из разложения $\mathfrak{K}h_1 + \ldots + \mathfrak{K}h_n$.

Идеалы (ε_i), (0), оставшиеся после исключения делителей единицы, можно теперь обозначить в *обратном порядке* через $\mathfrak{a}_1, \ldots, \mathfrak{a}_q$; тогда получим, что

$$\mathfrak{a}_i \equiv 0 \, (\mathfrak{a}_{i+1}).$$

b) Группа (h_i), уничтожающаяся идеалом (0), изоморфна $\mathfrak{K}$. Но группы, уничтожающиеся идеалами $(\varepsilon_i) \neq (0)$, согласно доказанному ранее, распадутся на группы простых степеней. Сами уничтожающие простые степени найдутся при разложении ε_i на множители. Сумма всех групп, встречающихся в разложении $\mathfrak{G}$ и принадлежащих простому числу p, равна $\mathfrak{B}_p$ и состоит из элементов $\mathfrak{G}$, которые уничтожаются достаточно большой степенью p^ρ. Итак, *группа* $\mathfrak{B}_p$ *определяется однозначно.* Если $\mathfrak{U}$ — сумма групп, для которых $\mathfrak{a} = (0)$, то

$$\mathfrak{G} = \sum_p \mathfrak{B}_p + \mathfrak{U}.$$

Обратно, при дальнейшем разложении $\mathfrak{B}_p$ мы получим группы простых степеней, которые определяются не абсолютно-однозначно, но, как мы увидим, все же однозначно с точностью до изоморфизма. Для всякого $\mathfrak{B}_p$ существует последовательность подгрупп $\mathfrak{B}_{p,\rho}$; $\mathfrak{B}_{p,\rho-1}$; $\ldots$; $\mathfrak{B}_{p,0}$, которая определяется однозначно. $\mathfrak{B}_{p,\nu}$ состоит из элементов $\mathfrak{B}_p$, которые уничтожаются числом p^ν. Первая группа этого ряда равна $\mathfrak{B}_p$; последняя группа состоит только из нуля.

В силу изоморфизма

$$\mathfrak{U} \cong \frac{\mathfrak{G}}{\sum_p \mathfrak{B}_p}$$

группа $\mathfrak{U}$ с точностью до изоморфизма определяется однозначно.

c) Теорема единственности. *Идеалы* $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_q$, $\mathfrak{a}_i \equiv 0\,(\mathfrak{a}_{i+1})$, *уничтожающие компоненты прямой суммы* $\mathfrak{G} = \mathfrak{H}_1 + \ldots + \mathfrak{H}_q$, *определяются по модулю* $\mathfrak{G}$ *однозначно* (или, что одно и то же, группы $\mathfrak{H}_i$ определяются однозначно с точностью до изоморфизма).

Доказательство. Единственность будет показана, если удастся установить независимо от разложения $\mathfrak{G}$ на прямую сумму число идеалов $\mathfrak{a}_i$, содержащих заданную степень p^σ (p — простой элемент $\mathfrak{K}$). Именно, если p^σ входит в k из таких идеалов, то p^σ в силу свойства делимости идеалов $\mathfrak{a}_i$ должно содержаться в $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$; тем самым станет известно, в какие $\mathfrak{a}_i$ входит p^σ. Те $\mathfrak{a}_i$, которые содержат неограниченно большие степени p, равны нулю, а остальные однозначно определяются разложением на простые множители.

Если p^σ входит в идеал, уничтожающий циклическую группу $\mathfrak{H}_i$, то

$$\frac{p^{\sigma-1}\mathfrak{H}_i}{p^\sigma \mathfrak{H}_i}$$

есть циклическая группа, которая уничтожается идеалом (p), т. е. простая группа. Если, напротив, p^σ не входит в рассматриваемый идеал, то $p^\sigma \mathfrak{H}_i = p^{\sigma-1}\mathfrak{H}_i$, откуда $\frac{p^{\sigma-1}\mathfrak{H}_i}{p^\sigma \mathfrak{H}_i} = (0)$. Поэтому $\frac{p^{\sigma-1}\mathfrak{G}}{p^\sigma \mathfrak{G}}$ равно прямой сумме простых групп, причем число этих групп равно числу идеалов $\mathfrak{a}_i$, делящихся на p^σ. Таким образом k равно длине композиционного ряда для $\frac{p^{\sigma-1}\mathfrak{G}}{p^\sigma \mathfrak{G}}$ и тем самым определяется однозначно.

Задачи. 1. Привести полностью последнюю, намеченную в конце часть доказательства.

2. Среди групп $\mathfrak{U}$, построенных в „b“, имеется модуль линейных форм относительно кольца C целых чисел, и число его циклических слагаемых равно рангу $\mathfrak{G}$ (ранг равен максимальному числу линейно независимых элементов относительно $\mathfrak{K}$).

3. Привести второе доказательство единственности с помощью длины композиционных рядов групп, построенных в „b“ и их фактор-групп. Отсюда также можно вывести ранг модуля $\mathfrak{U}$ (задача 2).

Для частного случая конечных абелевых групп (областью операторов здесь будет кольцо целых чисел) можно указать следующее прямое доказательство основной теоремы, основанное на полной индукции по порядку группы.

Возьмем элемент z_0 наивысшего порядка, порождающий циклическую группу $\mathfrak{Z}_0$. Согласно индуктивному предположению фактор-группа $\frac{\mathfrak{G}}{\mathfrak{Z}_0}$ равна прямой сумме циклических групп:

$$\frac{\mathfrak{G}}{\mathfrak{Z}_0} = \mathfrak{Z}_1 + \ldots + \mathfrak{Z}_r.$$

$\mathfrak{Z}_1$ порождается классом вычетов z_1, из которого мы возьмем представитель z_1. Пусть a_1 — число (порядок), уничтожающее z_1; таким образом $a_1 z_1 = 0$, $a_1 z_1 \in \mathfrak{Z}_0$, например $a_1 z_1 = b z_0$. Если z_1 заменим через $z_1 - q z_0$ ($z_1 - q z_0$ содержатся в том же классе вычетов z_1), то $a_1 (z_1 - q z_0) = b z_0 - q a_1 z_0 = (b - q a_1) z_0$; мы всегда

можем b заменить его наименьшим вычетом по a_1, откуда можно предположить, что $b < |a_1|$. Если n — порядок z_0, то порядок z_1 равен $\frac{a_1 n}{(b, n)}$, причем

$$\left|\frac{a_1 n}{(b, n)}\right| \leqslant n ,$$

$$a_1 \leqslant (b, n) \leqslant b \qquad (\text{если } b \neq 0).$$

Но неравенство $a_1 \leqslant b$ противоречит $b < a_1$. Таким образом должно быть $b = 0$. Отсюда следует, что $a_1 z_1 = 0$, и порядок z_1 равен порядку z_1. То же самое справедливо для классов вычетов, которые определяются элементами $z_2, \ldots, z_r$. Благодаря (1) всякий элемент $\mathfrak{G}$ сравним с линейной комбинацией $z_1, \ldots, z_r$ по модулю $\mathfrak{Z}_0$:

$$g \equiv c_1 z_1 + \ldots + c_r z_r (\mathfrak{Z}_0), \tag{2}$$

и коэфициенты c_i определяются однозначно по модулям $a_1, \ldots, a_r$, где a_i порядок класса $\overline{z_i}$ или элемента z_i. Из (2) следует, что

$$g - (c_1 z_1 + \ldots + c_r z_r) = c_0 z_0,$$

причем $c_0 z_0$ определяется однозначно. Таким образом $\mathfrak{G}$ есть прямая сумма циклических групп $\mathfrak{Z}_0, \ldots, \mathfrak{Z}_r$, порожденных $z_0, \ldots, z_r$.

Эти группы можно затем разложить, как выше, еще на группы простых степеней.

Легко видеть, что те же рассуждения справедливы и тогда, когда мультипликаторной областью является кольцо полиномов $\mathsf{P}[u]$. В этом случае вместо абсолютных величин $|a|$ следует рассматривать степени полиномов. Кроме того, предполагается, что группа $\mathfrak{G}$ обладает конечным рангом относительно поля P; по этому рангу проводится полная индукция. Из конечности ранга $\mathfrak{G}$ следует, что для всякого элемента z группы среди величин $z, uz, u^2 z, \ldots$ существует только конечное число линейно независимых; иными словами, всякое z уничтожается полиномом $f(u) \neq 0$, благодаря чему вступает в силу вышеприведенное доказательство.

Можно подобным же образом доказать непосредственно и общий случай основной теоремы, т. е. привести доказательство, не опирающееся на теорию элементарных делителей, и вывести отсюда обратно теорему об элементарных делителях § 106[1]).

Небесполезно заметить, что все доказанное в этом параграфе можно сразу распространить на мультипликативные абелевы группы, если вместо суммы писать произведение.

Для конечных абелевых групп употребительно следующее обозначение: например, символом $\mathfrak{A}_{2,\,2,\,4,\,3}$ обозначается прямая сумма (прямое произведение) циклических групп порядков 2, 2, 4, 3 [таким образом уничтожающими идеалами будут (2), (2), (4), (3)]. Целесообразно обозначение распространить также на циклические слагаемые бесконечного порядка [т. е. такие, которые уничтожаются идеалом (0)]; например, прямую сумму двух циклических групп с уничтожающими идеалами (4), (0) можно обозначить через $\mathfrak{A}_{4,\,0}$.

Задачи. 4. Если абелева группа порядка n — циклическая, то n — наименьшее число, которое уничтожает все элементы группы; если, напротив, группа не циклическая, то существует собственный делитель n, который уничтожает элементы группы.

---

[1]) См. H. Prüfer, Theorie der Abelschen Gruppen, „Math. Zeitschr". т. 20 стр. 165—187, а также K. Shoda, Proc. Imp. Acad. Tokio, т. 6, стр. 217—219 1930.

5. С помощью 4 доказать, что мультипликативная группа классов вычетов по модулю p^k, числа которых не делятся на p, является циклической, за исключением $p=2$ и $k\geqslant 3$, когда она типа $\mathfrak{A}_{2,\,2^{k-2}}$. (Вычислить порядки элементов $1+p$ и g, где g — первообразный корень модуля p.)

6. Мультипликативная группа классов вычетов n, числа которых взаимно простые с n, изоморфна прямому произведению групп вычетов по модулям наивысших простых степеней, входящих в n.

§ 108. ПРЕДСТАВЛЕНИЯ И МОДУЛИ ПРЕДСТАВЛЕНИЙ

Под *представлением кольца* $\mathfrak{o}$ *с помощью линейных преобразований или матриц* K подразумевается гомоморфизм

$$\mathfrak{o} \backsim \mathfrak{D},$$

где $\mathfrak{D}$ — кольцо квадратных матриц r-го порядка с элементами из K. Если гомоморфизм является изоморфизмом, то представление будет *точным*. Если $\mathfrak{o}$ и K гиперкомплексны относительно поля P, то по большей части кроме кольцевого гомоморфизма требуется также операторный гомоморфизм относительно P: если $a \to A$, то должно быть $a\rho \to A\rho$ для $\rho \in \mathsf{P}$.

В приложениях K большей частью является полем. В случае гиперкомплексных чисел P содержится в центре K.

Под *модулем представления* $\mathfrak{o}$ относительно K подразумевается „*двойной модуль*“ $\mathfrak{M}$, для которого $\mathfrak{o}$ образует левую, а K правую мультипликаторную область, причем

1. $\mathfrak{M}$ можно рассматривать как модуль линейных форм относительно K:

$$\mathfrak{M} = u_1\mathsf{K} + \ldots + u_n\mathsf{K}.$$

2. Для $a \in \mathfrak{o}$, $u \in \mathfrak{M}$, $\lambda \in \mathsf{K}$,

$$a(u\lambda) = (au)\lambda. \tag{1}$$

Последнее требование означает, что умножение на a есть операторный гомоморфизм K модуля $\mathfrak{M}$, т. е. представляет линейное преобразование. Линейное преобразование будет определяться квадратной матрицей $A = (\alpha_{ik})$:

$$\left.\begin{aligned} a \cdot u_k &= \sum u_j \alpha_{jk}, \\ a \cdot \sum u_k \lambda_k &= \sum\sum u_j \alpha_{jk} \lambda_k. \end{aligned}\right\} \tag{2}$$

Итак, каждому a из $\mathfrak{o}$ соответствует матрица A в K. Вследствие свойств модуля произведению и сумме двух элементов a, b кольца $\mathfrak{o}$ соответствует также произведение и сумма линейных преобразований или матриц. *Таким образом соответствие* $a \to A$ *есть представление кольца* $\mathfrak{o}$.

Если, обратно, представление кольца $\mathfrak{o}$ задано линейным преобразованием модуля линейных форм $\mathfrak{M}$ относительно K, то можно сделать из $\mathfrak{M}$ двойной модуль, определив произведения $a \cdot u$ ($a \in \mathfrak{o}$, $u \in \mathfrak{M}$) с помощью (2). Тогда обратно будут выполняться все свойства двойного модуля и правило (1), т. е. $\mathfrak{M}$ будет *модулем представления*.

Итак, всякому модулю представления соответствует представление $\mathfrak{o}$ *с помощью линейных преобразований или, после выбора* K*-базиса* $(u_1, \ldots, u_n)$*, с помощью матриц* K*; обратно, всякому представлению соответствует модуль представления.* Если в силу

$$(u'_1, \ldots, u'_n) = (u_1, \ldots, u_n) P$$

базис $(u_1, \ldots, u_n)$ переходит в другой базис $(u'_1, \ldots, u'_n)$, то линейное преобразование будет определяться матрицей:

$$A' = P^{-1} A P.$$

Таким образом элементам a кольца будут соответствовать новые матрицы A'; в этом случае говорят об *эквивалентном представлении.* Так как переход к эквивалентному представлению есть не что иное, как переход к другому базису одного и того же (или операторно изоморфного) модуля представления, то *изоморфным модулям представлений соответствуют эквивалентные представления, и обратно.*

Если $\mathfrak{o}$ и K гиперкомплексны относительно коммутативного поля P, входящего в центр K, и из $a \to A$ следует $a\rho \to A\rho$, то для модуля представления имеем:

$$(a\rho)\, u (= (\rho a)\, u) = (au)\rho.$$

Таким образом скаляры ρ из K можно писать в любом месте произведения: скаляры перестановочны со всеми рассматриваемыми величинами.

Система линейных преобразований модуля $\mathfrak{M}$ линейных форм, в частности представление кольца, называется *приводимой*, если все преобразования системы преобразуют данное линейное подпространство $\mathfrak{N}$ ($\mathfrak{N} \neq (0)$ и $\neq \mathfrak{M}$) в самого себя. В этом случае $\mathfrak{N}$ называется *инвариантным подпространством.* Если рассматривать $\mathfrak{M}$ как двойной модуль относительно $\mathfrak{o}$ и K, причем речь идет о представлении кольца $\mathfrak{o}$, то инвариантное подпространство $\mathfrak{N}$ будет допускать все элементы $\mathfrak{o}$ в качестве левых операторов. Отсюда следует, что *представление кольца тогда и только тогда приводимо, если соответствующий модуль представления обладает (двойным) подмодулем* $\mathfrak{N}$.

Пусть теперь K будет поле. Чтобы установить, как выглядят матрицы приводимого представления, будем исходить из K-базиса $\mathfrak{N}$ и дополним его до K-базиса $\mathfrak{M}$ (см. § 105). Пусть

$$\mathfrak{N} = v_1 \mathsf{K} + \ldots + v_r \mathsf{K},$$

$$\mathfrak{M} = v_1 \mathsf{K} + \ldots + v_r \mathsf{K} + w_1 \mathsf{K} + \ldots + w_t \mathsf{K}.$$

Линейное преобразование модуля $\mathfrak{N}$ в самого себя означает, что

$$\left.\begin{aligned} v'_j &= \sum v_i \rho_{ij}, \\ w'_j &= \sum v_i \sigma_{ij} + \sum w_i \tau_{ij}. \end{aligned}\right\} \qquad (3)$$

Если положить $R=(\rho_{ij})$, $S=(\sigma_{ij})$, $T=(\tau_{ij})$, то преобразование будет представляться матрицей

$$A=\begin{pmatrix} R & S \\ 0 & T \end{pmatrix}. \tag{4}$$

Следовательно, *система матриц тогда и только тогда приводима, если все матрицы системы с помощью преобразования* $A'=P^{-1}AP$ *(переход к новому базису) могут быть представлены в виде* (4).

Из (3) следует

$$\left.\begin{aligned} (v_1', \ldots, v_r') &= (v_1, \ldots, v_r)\cdot R, \\ (w_1', \ldots, w_t') &\equiv (w_1, \ldots, w_t)\cdot T \ (\mathrm{mod.}\ \mathfrak{N}). \end{aligned}\right\} \tag{5}$$

Отсюда имеем:

Если для приводимого представления кольца $\mathfrak{o}$ *инвариантный подмодуль* $\mathfrak{N}$ *и фактор-модуль* $\frac{\mathfrak{M}}{\mathfrak{N}}$ *рассматривать как модули представления, то соответствующие представления будут определяться составными частями* R *и* T *матрицы* (4).

Если взять в качестве $\mathfrak{N}$ максимальный инвариантный подмодуль $\mathfrak{M}_{l-1}$, внутри $\mathfrak{M}_{l-1}$ — его максимальный инвариантный подмодуль $\mathfrak{M}_{l-2}$ и т. д., исчерпывая таким образом композиционный ряд

$$\mathfrak{M}=\mathfrak{M}_l,\ \mathfrak{M}_{l-1},\ \ldots,\ \mathfrak{M}_0=(0),$$

то при подходящем выборе базиса матрицы представления будут выглядеть следующим образом:

$$\begin{pmatrix} R_{11} & \cdots & \cdots & R_{1l} \\ 0 & R_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & R_{ll} \end{pmatrix}. \tag{6}$$

Диагональные клеточки R_{ii} определяют представления, принадлежащие композиционным факторам $\frac{\mathfrak{M}_i}{\mathfrak{M}_{i-1}}$; так как эти композиционные факторы суть простые двойные модули (т. е. не имеют инвариантных подмодулей), то соответствующие представления *неприводимы*. Процесс, приводящий к (6), называется *приведением* представления. Согласно теореме Жордана и Гёльдера (§ 41) композиционные факторы определяются однозначно с точностью до порядка следования и до операторного изоморфизма; отсюда получается, что *неприводимые составные части* R_{ii} *представления* (6) *определяются однозначно с точностью до порядка следования и до эквивалентных представлений.*

Если в (3) отсутствуют σ_{ij}, то это значит, что не только $(v_1, \ldots, v_r)$, но также и $(w_1, \ldots, w_t)$ является инвариантным подмодулем, т. е. $\mathfrak{M}$ есть *прямая сумма двух инвариантных подмодулей* $\mathfrak{N}$, $\mathfrak{Q}$. Тогда матрица (4) принимает такой вид:

$$A=\begin{pmatrix} R & 0 \\ 0 & T \end{pmatrix},$$

где представление R увязано с $\mathfrak{N}$, а T — с $\mathfrak{Q}$. В этом случае говорят, что представление $a\to A$ *распадается* на представления $a\to R$ и $a\to T$.

Если двойной модуль $\mathfrak{M}$ вполне приводим в смысле § 42, т. е. равен прямой сумме простых двойных модулей, то представление, связанное с $\mathfrak{M}$, определяется матрицей

$$\begin{pmatrix} R_{11} & & & 0 \\ & R_{22} & & \\ & & \ddots & \\ 0 & & & R_{uu} \end{pmatrix}, \tag{7}$$

где отдельные клеточки отвечают неприводимым представлениям; очевидно, что среди них могут встречаться также и одинаковые представления. Такое представление называется *вполне приводимым.*

Задачи. 1. Представление (гомоморфное) конечной или бесконечной группы может быть дополнено с помощью линейных подстановок до представления „группового кольца" (§ 10, задача 13); стоит только сопоставить элементу группы g_i матрицу G_i, а линейной комбинации $\sum g_i\lambda_i$ матрицу $\sum G_i\lambda_i$.

2. Если $\mathfrak{o}$ — кольцо с единицей, и в представлении кольца $\mathfrak{o}$ единице соответствует единичная матрица, то для модуля представления это означает, что единица является единичным оператором. Показать с помощью одной теоремы § 104, что любое представление $\mathfrak{o}$ распадается на такое представление, для которого единице соответствует единичная матрица, и на такое, для которого всякому элементу $\mathfrak{o}$ соответствует нулевая матрица:

$$A = \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix}.$$

3. Представление тогда и только тогда вполне приводимо, если для любого инвариантного подпространства $\mathfrak{N}$ можно найти такое другое инвариантное подпространство $\mathfrak{Q}$, что

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{Q}.$$

4. Если $(u_1', \ldots, u_n') = (u_1, \ldots, u_n)P$ — гомоморфное отображение модуля представления на самого себя, то матрица P перестановочна со всеми матрицами представления:

$$AP = PA,$$

и обратно.

§ 109. НОРМАЛЬНЫЙ ВИД МАТРИЦЫ КОММУТАТИВНОГО ПОЛЯ

Пусть $\mathfrak{M} = (u_1, \ldots, u_n)$ будет модуль линейных форм относительно коммутативного поля K и

$$u_k \to v_k = \sum u_i\alpha_{ik}\ ^{1})$$

будет линейное преобразование $\mathfrak{M}$ на самого себя. Приведем матрицу $A = (\alpha_{ik})$ к возможно простому нормальному виду

$$A' = P^{-1}AP,$$

[1]) Так как K коммутативно, то совершенно безразлично, будем ли мы иметь коэфициенты справа или слева.

заменяя старый базис новым базисом

$$(u'_1, \ldots, u'_n) = (u_1, \ldots, u_n) P$$

(где P — обратимая матрица K). Отметим отличие от постановки вопроса в § 106, где шла речь о двух новых базисах (v') и (u') и было положено $A' = B^{-1} AC$. Теперь, стало быть, возможности преобразования ограничиваются; в связи с этим мы налагаем на K больше требований: мы предполагаем, что K есть поле.

Будем рассматривать степени матрицы A как мероморфное представление степеней переменной x и расширим это представление до представления области $\mathsf{K}[x]$ полиномов, приводя в соответствие полиному

$$f(x) = \sum \alpha_\nu x^\nu$$

матрицу

$$f(A) = \sum \alpha_\nu A^\nu.$$

Представление гомоморфно, так как степени A перестановочны друг с другом и с коэфициентами α_ν.

Этому представлению принадлежит модуль представления $\mathfrak{M}$, если только определить произведение полинома из $\mathsf{K}[x]$ на $u \in \mathfrak{M}$ с помощью равенства

$$\left(\sum \alpha_\nu x^\nu\right) u = \sum \alpha_\nu A^\nu u.$$

Модуль представления $\mathfrak{M}$ является двойным модулем относительно $\mathsf{K}[\lambda]$ и K; но так как величины K престановочны друг с другом и со всеми другими величинами, то мы можем их записать также слева от элементов $\mathfrak{M}$:

$$u\lambda = \lambda u,$$

таким образом $\mathfrak{M}$ можно рассматривать просто как $\mathsf{K}[x]$-модуль.

Так как кольцо полиномов $\mathsf{K}[\lambda]$ удовлетворяет всем условиям § 106 (область целостности с делением, или в $\mathsf{K}[\lambda]$ всякий идеал является главным), то можно применить теорему § 107 [1]): модуль $\mathfrak{M}$ равен прямой сумме циклических $\mathsf{K}[x]$-модулей $(w_1), \ldots, (w_r)$, причем (w_i) уничтожается либо идеалом (0), либо идеалом $\mathfrak{a}$, порожденным некоторым полиномом из $\mathsf{K}[x]$. Но случай нулевого идеала (0) следует исключить, так как для всякого $w = w_\nu$ среди величин $w, xw, x^2w, \ldots$ может оказаться самое большее n линейно независимых; таким образом существует полином $\sum \alpha_\nu x^\nu \neq 0$, для которого

$$\sum \alpha_\nu x^\nu w = 0.$$

Поэтому всякое $w = w_\nu$ имеет „уничтожающим полиномом" наинизшей степени

$$f_\nu(x) = f(x) = x^k + \alpha_{k-1} x^{k-1} + \ldots + \alpha_0,$$

---

[1]) Это вытекает также из краткого прямого доказательства, приведенного в конце § 107.

и мы имеем:

$$f_{\nu+1} \equiv 0\,(f_\nu).$$

Величины w, $xw, \ldots,$ $x^{k-1}w$ линейно независимы относительно K и потому могут быть приняты за K-базис циклического $\mathsf{K}\,[x]$-модуля $(w) = (w,\ xw,\ x^2w,\ \ldots)$. Имеем:

$$\begin{aligned} Aw &= xw, \\ Axw &= x^2w, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ Ax^{k-1}w &= x^kw = -\alpha_0 w - \alpha_1 \cdot xw - \ldots - \alpha_{k-1} \cdot x^{k-1}w. \end{aligned}$$

Следовательно, преобразование A модуля $(w,\ xw,\ \ldots)$ в самого себя представляется матрицей

$$A_\nu = \begin{pmatrix} 0 \ldots & 0 & -\alpha_0 \\ 1 & 0 \ldots 0 & -\alpha_1 \\ 0 & 1 & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ 0 \ldots & 1 & -\alpha_{k-1} \end{pmatrix}. \qquad (1)$$

Эта матрица называется *сопутствующей матрицей*; каждому w_ν отвечает сопутствующая матрица такого типа. Так как $\mathfrak{M}$ есть прямая сумма (w_ν), то для матрицы A получается *первый нормальный тип*:

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}, \qquad (2)$$

где A_ν — *сопутствующие матрицы типа* (1).

Из теоремы единственности § 107 следует, что полиномы $f_\nu(x)$, а потому также сопутствующие матрицы A_ν, *определяются модулем* $\mathfrak{M}$ *однозначно.*

После этого можно разложить A_ν, представив циклические модули (w_ν) в виде прямых сумм циклических подмодулей, которые уничтожаются степенями неприводимых полиномов. Равенство (2) сохранится; только сопутствующие матрицы (1) будут теперь принадлежать степеням $(p(x))^\rho$ неприводимых полиномов (*второй нормальный тип*). И здесь также сопутствующие матрицы определяются однозначно до порядка их следования в (2). Полиномы $(p(x))^\rho$ называются иногда *элементарными делителями* матрицы A. Слово „элементарный делитель" здесь имеет, конечно, другое значение, чем в § 106. В § 110 будет установлена связь между этими понятиями.

С помощью композиционных рядов циклических модулей (w_ν) можно произвести еще дальнейшее уточнение понятия „нормальный тип". Мы ограничимся только случаем, когда встречающиеся неприводимые поли

номы $p(x)$ *линейны*, что в частности всегда имеет место для алгебраически замкнутого поля K. Таким образом пусть будет

$$p = x - \lambda,$$
$$f(x) = (x-\lambda)^{\rho}.$$

В качестве элементов базиса возьмем

$$\begin{aligned} v_1 &= (x-\lambda)^{\rho-1} w, \\ v_2 &= (x-\lambda)^{\rho-2} w, \\ &\cdots\cdots\cdots \\ v_\rho &= w; \end{aligned}$$

тогда

$$(x-\lambda) v_1 = 0,$$
$$(x-\lambda) v_\mu = v_{\mu-1} \quad (1 < \mu \leqslant \rho)$$

или

$$\left.\begin{aligned} Av_1 &= xv_1 = \lambda v_1, \\ Av_\mu &= xv_\mu = \lambda v_\mu + v_{\mu-1}. \end{aligned}\right\} \tag{3}$$

Тогда A_1 приведется к

$$A_1 = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix},$$

и точно так же получим:

$$A_\nu = \begin{pmatrix} \lambda_\nu & 1 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ & & \ddots & 1 \\ 0 & & & \lambda_\nu \end{pmatrix},$$

так как w_ν соответствует λ_ν. Эти A_ν подставим в (2), чтобы получить *третий нормальный вид. Характеристические корни*[1]) λ_ν и порядок ρ_ν матриц A_ν снова *определяются однозначно.*

Все векторы v_μ, принадлежащие одному и тому же корню λ, порождают модуль $\mathfrak{V}_\lambda$, который уничтожается некоторой степенью полинома $x - \lambda$ (§ 107); этот модуль называется *частью пространства, принадлежащей корню* λ. Весь модуль $\mathfrak{M}$ равен прямой сумме таких частичных пространств. Среди них существует упомянутая в § 107 последовательность подпространств, уничтожающихся полиномами $(x-\lambda)^{\rho}$, $(x-\lambda)^{\rho-1}$, ..., 1. Векторы w, уничтожающиеся полиномом $(x-\lambda)$, называются *собственными векторами* матрицы A, принадлежащими *собственному значению* λ. Для них, очевидно, имеет место:

$$Aw = \lambda w.$$

[1]) Этот термин будет разъяснен в следующем параграфе.

Матрица A иногда записывается в виде *схемы* следующего рода: если характеристический корень, например λ_1, входит в клеточки порядков $\rho, \sigma, \ldots, \tau$, то $\rho, \sigma, \ldots, \tau$ заключают в круглые скобки и затем объединяют в прямоугольные скобки все круглые скобки, соответствующие разным λ_ν. Так, схема $[(21)1]$ означает, что мы имеем дело с матрицей типа

$$\begin{pmatrix} \begin{vmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{vmatrix} & & \\ & \begin{vmatrix} \lambda_1 \end{vmatrix} & \\ & & \begin{vmatrix} \lambda_2 \end{vmatrix} \end{pmatrix}.$$

Если все ρ равны единице, т. е. если полиномы $f_\nu(x)$, из которых получаются $(p(x))^\rho$ при разложении на простые множители, не содержат кратных множителей, то мы имеем случай *полной приводимости* (см. § 108), когда нормальная форма (2) имеет вид:

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & & \ddots \\ 0 & & \lambda_n \end{pmatrix}. \tag{4}$$

В силу

$$f_{\nu+1} \equiv 0 \,(f_\nu)$$

для этого достаточно, чтобы наивысший элементарный делитель $f_r(x)$ не имел кратных множителей.

В следующем параграфе будут приведены методы определения характеристических корней и нормальных форм.

Задачи. 1. Наивысший элементарный делитель может быть охарактеризован как полином $f(x)$ наинизшей степени, для которого имеет место

$$f(x)\,\mathfrak{M} = 0 \quad \text{или} \quad f(A) = 0.$$

2. Определить для произвольной матрицы A, заданной во второй или третьей нормальной форме, совокупность матриц, перестановочных с A (см. § 108, задача 4).

§ 110. ЭЛЕМЕНТАРНЫЙ ДЕЛИТЕЛЬ И ХАРАКТЕРИСТИЧЕСКАЯ ФУНКЦИЯ

При преобразовании

$$A' = P^{-1}AP$$

матрица $xE - A$ переходит в

$$P^{-1}(xE - A)P = xP^{-1}EP - P^{-1}AP = xE - A'.$$

Определим элементарные делители матрицы $xE - A$ в $\mathfrak{K}[x]$ в смысле § 106. Так как они инвариантны относительно одновременного правого и левого умножения на произвольную обратимую матрицу, то мы можем определить эти элементарные делители также для $xE - A'$, где A' —

первая нормальная форма § 109. Согласно (1), (2) § 109 $xE - A'$ состоит из клеток вида

$$xE_1 - A_1 = \begin{pmatrix} x & 0 & \cdots & 0 & \beta_0 \\ -1 & x & & & \cdot \\ 0 & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & x & \beta_{h-2} \\ \cdot & & \cdot & \cdot & \\ 0 & \cdots & 0 & -1 & x+\beta_{h-1} \end{pmatrix}.$$

Для определения элементарных делителей приведем эту матрицу к диагональному виду. Если прибавить к первой строке вторую, третью и т. д., h-ю строки, умноженные соответственно на x, x^2, ..., x^{h-1}, то получится:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & f(x) \\ -1 & x & & & \beta_1 \\ 0 & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & x & \beta_{h-2} \\ \cdot & & \cdot & \cdot & \\ 0 & \cdots & 0 & -1 & x+\beta_{h-1} \end{pmatrix}.$$

Переставляя строки так, чтобы первая строка очутилась внизу, получим под главной диагональю нули. Легко видеть, что прибавляя кратные предыдущих столбцов к последующим, можно все элементы, стоящие над главной диагональю, обратить в нули. Таким образом в итоге матрица примет вид:

$$\begin{pmatrix} -1 & & & 0 \\ & -1 & & \\ & & \ddots & \\ & & & -1 \\ 0 & & & f(x) \end{pmatrix}.$$

Расположив теперь все эти клетки друг за другом и переставив строки и столбцы так, чтобы на главной диагонали впереди шли -1, придем к искомой диагональной форме:

$$\begin{pmatrix} -1 & & & & 0 \\ & -1 & & & \\ & & \ddots & & \\ & & & -1 & \\ & & & & f_1(x) \\ & & & & & \ddots \\ 0 & & & & & & f_r(x) \end{pmatrix}.$$

Итак, полиномы $f_\nu(x)$ (вместе с некоторыми единицами) являются элементарными делителями матрицы $xE - A$. Степени неприводимых полиномов, на которые они распадаются, являются элементарными делителями матрицы A в смысле § 109.

Характеристический полином (*характеристическая функция*)

$$\chi(x) = \prod_1^r f_\nu(x)$$

матрицы A уничтожает модуль $\mathfrak{M}$, так как модуль $\mathfrak{M}$ уничтожается множителем $f_r(x)$; поэтому

$$\chi(A) = 0. \tag{1}$$

Характеристический полином равен делителю наивысшей степени детерминанта $|xE - A|$. Отсюда следует, что он с точностью до постоянной равен детерминанту $|xE - A|$. Сразу видно, что постоянная равна единице, откуда

$$\chi(x) = |xE - A|. \tag{2}$$

Характеристическое уравнение (1) для матрицы A получается также непосредственно из (2). Именно,

$$xu_k = \sum u_i \alpha_{ik},$$

и после исключения всех u из этой системы уравнений будем иметь (так как x и его степени перестановочны с α_{ik}):

$$\begin{vmatrix} x - \alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ \vdots & & & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & x - \alpha_{nn} \end{vmatrix} \cdot u_j = 0,$$

или

$$|xE - A|\, u_j = 0;$$

т. е. $\chi(x) = |xE - A|$ уничтожает все u_j, а потому уничтожает весь модуль $\mathfrak{M}$, что и требовалось доказать.

Коэфициенты характеристической функции $\chi(x)$ матрицы A согласно предыдущему инвариантны относительно преобразования $A \to P^{-1}AP$. Наиболее существенны первый и последний коэфициенты, а именно *след* A — коэфициент при $-x^{n-1}$:

$$Sp(A) = \sum \alpha_{ii}$$

и *норма* A, т. е. коэфициент при $(-1)^n x^0$:

$$N(A) = |A|.$$

Корнями характеристической функции будут *характеристические корни* λ_ν, которые были введены еще в предыдущем параграфе [там они были корнями $f_\nu(x)$]. Отсюда получается практически удобный способ определения этих λ и нормальных форм предыдущего параграфа: прежде всего определяют λ_ν, решая уравнение

$$\chi(x) = |xE - A| = 0,$$

затем находят v_1 из линейного уравнения

$$Av_1 = \lambda_\nu v_1$$

[см. (3), § 109]. В случае кратных корней ($\rho > 1$) остальные $v_2, \ldots, v_\rho$ легче всего найти из (3) § 109; при этом v_1, принадлежащие одинаковым λ_ν, можно заменить соответствующей линейной комбинацией.

Уравнение $\chi(\lambda) = 0$, корни которого равны λ_ν, имеет многочисленные приложения в теории вековых возмущений. Именно по этой причине $\chi(\lambda) = 0$ называется также *вековым уравнением*.

Задачи. 1. Определить нормальные формы матриц

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

2. Провести классификацию проективных отображений проективной плоскости на самое себя:

$$\begin{pmatrix} \xi_1' \\ \xi_2' \\ \xi_3' \end{pmatrix} = A \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix}$$

и определить положение инвариантных точек и прямых этого отображения.

§ 111. КВАДРАТИЧНЫЕ И ЭРМИТОВСКИЕ ФОРМЫ

Пусть K — коммутативное поле с характеристикой, отличной от 2. Чтобы исследовать значения, которые принимает квадратичная форма

$$f(x_1, \ldots, x_n) = \sum_i \sum_k \beta_{ik} x_i x_k \quad (\beta_{ik} = \beta_{ki})$$

при частных значениях $x_i = c_i$ из K, условимся считать $c_1, \ldots, c_n$ компонентами вектора u и положим, что

$$f(u, u) = f(c_1, \ldots, c_n) = \sum\sum \beta_{ik} c_i c_k.$$

Пусть $v = (d_1, \ldots, d_n)$ есть второй вектор; рассмотрим следующее выражение:

$$f(u + \lambda v, u + \lambda v) = \sum\sum \beta_{ik} c_i c_k + 2\lambda \sum\sum \beta_{ik} c_i d_k + \lambda^2 \sum\sum \beta_{ik} d_i d_k =$$

$$= f(u, u) + 2\lambda f(u, v) + \lambda^2 f(v, v),$$

где

$$f(u, v) = \sum\sum \beta_{ik} c_i d_k.$$

Очевидно, что билинейная форма $f(u, v)$ связана инвариантно (т. е. независимо от выбора базиса векторов) с формой $f(u, u)$; $f(u, v)$ называется *полярной формой* относительно $f(u, u)$.

Если базис $(u_1, \ldots, u_n)$ векторов u пространства R_n заменить новым базисом $(u_1', \ldots, u_n')$, где u_i' связано со старыми векторами $u_1, \ldots, u_n$ линейным преобразованием P:

$$u_j' = \sum u_i \pi_{ij},$$

то, как мы знаем, компоненты c_i вектора преобразуются следующим образом:

$$c_i = \sum \pi_{ij} c_j',$$

а квадратичная форма f перейдет в

$$f = \sum\sum \beta_{ik} c_i c_k = \sum\sum\sum\sum \beta_{ik}\pi_{ij}\pi_{kl} c_j' c_l'$$

с коэфициентами

$$\beta_{jl}' = \sum\sum \beta_{ik}\pi_{ij}\pi_{kl}.$$

Это равенство можно записать в матричном виде, если только ввести матрицы $A = (\beta_{ik})$, $A' = (\beta_{ik}')$ и транспонированную матрицу $\widetilde{P}$. Тогда окажется, что

$$A' = \widetilde{P}AP. \tag{1}$$

Как видим, матрица из коэфициентов квадратичной формы преобразуется совершенно иначе, чем матрица линейного преобразования, которая при новом базисе равна $A' = P^{-1}AP$.

Чтобы привести данную квадратичную форму f с помощью преобразования к простейшему виду, возьмем такой вектор v_1, чтобы $f(v_1, v_1) \neq 0$, что всегда возможно, если f не равно тождественно нулю. Тогда уравнение $f(v_1, u) = 0$ определит подпространство R_{n-1} векторного пространства R_n, причем R_{n-1} не содержит v_1. Если в этом подпространстве можно выбрать такой вектор v_2, что $f(v_2, v_2) \neq 0$, то уравнение $f(v_2, u) = 0$ вместе с предыдущим будет определять подпространство R_{n-2}, причем R_{n-2} не содержит v_2. В конце концов мы придем к подпространству R_{n-r}, и $f(u, u)$ будет равно нулю для всех u из R_{n-r}; отсюда [1]) также $f(u, v) = 0$ для u и v из R_{n-r}. Может случиться, что $r = n$; тогда R_{n-r} будет нулевым пространством. В противном случае мы берем в R_{n-r} произвольно векторный базис $v_{r+1}, \ldots, v_n$, откуда

$$\begin{aligned} &f(v_i, v_k) = 0 && (i \neq k), \\ &f(v_i, v_i) = \gamma_i \neq 0 && (i = 1, \ldots, r), \\ &f(v_i, v_i) = 0 && (i = r+1, \ldots, n). \end{aligned}$$

Если

$$v = \sum d_i v_i,$$

то

$$f(v, v) = \sum\sum d_i d_k f(v_i, v_k) = \sum_1^r d_i^2 \gamma_i. \tag{2}$$

Таким образом форма f, как говорят, *привелась к сумме квадратов*. Для векторов w пространства R_{n-r} имеет место

$$f(w, u) = 0$$

[1]) Здесь вступает в силу предположение о том, что характеристика не равна 2.

для всякого u; этим уравнением w вполне определяются. Итак, пространство R_{n-r} и его измерение $n-r$ инвариантно связаны с формой f. Поэтому число квадратов r в форме (2) также инвариантно: оно называется *рангом* формы f.

Пусть теперь K — расположенное поле[1]) (§ 63). Число отрицательных γ_i в (2) можно назвать *индексом инерции* f. Мы покажем, что этот индекс инерции также является инвариантным (*закон инерции Сильвестра*).

Пусть эта же форма f относительно другого базиса v_i' имеет вид:

$$f=\sum_1^r d_i'^2\gamma_i';$$

пусть, например, $\gamma_1, \ldots, \gamma_h$ — положительные, $\gamma_{h+1}, \ldots, \gamma_r$ — отрицательные величины; точно так же $\gamma_1', \ldots, \gamma_k'$ положительны, а $\gamma_{k+1}', \ldots, \gamma_r'$ отрицательны. Если бы, например, имело место $k>h$, то линейные уравнения

$$d_1=0, \ldots, d_h=0, \quad d_{k+1}'=0, \ldots, d_r'=0$$

определяли бы пространство, у которого число измерений было бы больше $n-r$. Для вектора u этого пространства мы бы имели, с одной стороны, что $f(u, u)=\sum_{h+1}^r d_i^2\gamma_i\leqslant 0$, а, с другой стороны, $f(u, u)=$ $=\sum_1^k d_i'^2\gamma_i'\geqslant 0$, откуда $f(u, u)=0$ и все d_i и d_i' равны нулю. Поэтому u лежало бы в R_{n-r}. Но тогда пространство, имеющее больше, чем $n-r$ измерений, содержалось бы в $(n-r)$-мерном пространстве, что невозможно.

Если в (2) все γ_i положительны, то в случае $r=n$ форма называется *определенной формой*, а в общем случае *полуопределенной*. Определенные формы характеризуются тем, что они для всякого вектора $u\neq 0$ имеют положительное значение; что касается полуопределенных форм, то они всегда больше или равны нулю.

Из (2) непосредственно следует, что определенная форма после присоединения к полю K величины $\sqrt{\gamma_i}$ преобразуется в *„единичную форму“*

$$E(u, u)=\sum d_i^2.$$

Эрмитовские формы во многом схожи с квадратичными. Присоединим к расположенному полю K квадратный корень Θ из отрицательной величины α, например $\Theta=\sqrt{-1}$. В отличие от элементов $\mathsf{K}(\Theta)$, мы будем величины K называть „действительными“, так как в приложениях K большей частью является полем действительных чисел и $\Theta=\sqrt{-1}$.

---

[1]) В русской терминологии более принят термин „упорядоченное поле“ (вообще „упорядоченное множество“). *(Прим. ред.).*

Каждой величине $c = a + b\Theta$ сопряжено $\bar{c} = a - b\Theta$. Произведение $c\bar{c} = a^2 - b^2\Theta^2$ всегда действительно и больше или равно нулю, причем равенство может быть только для $c = 0$.

Под *эрмитовской формой* мы подразумеваем выражение

$$H(u, u) = \sum\sum h_{ik}\bar{c}_i c_k \qquad (h_{ik} = \bar{h}_{ki}).$$

Для любого вектора u значение формы H действительно.

Если, как и в начале этого параграфа, возьмем

$$H(u + \lambda v, \quad u + \lambda v) = \sum\sum h_{ik}\bar{c}_i c_k + \lambda \sum\sum h_{ik}\bar{c}_i d_k +$$

$$+ \bar{\lambda}\sum\sum h_{ik}\bar{d}_i c_k + \lambda\bar{\lambda}\sum\sum h_{ik}\bar{d}_i d_k,$$

то коэфициентом при λ будет *полярная форма*

$$H(u, v) = \sum\sum h_{ik}\bar{c}_i d_k.$$

Кроме того, имеет место

$$H(v, u) = \overline{H(u, v)}.$$

Формула преобразования (1) справедлива также для эрмитовских форм; надо только под $\widetilde{P}$ подразумевать транспонированную сопряженную матрицу $(\widetilde{\pi}_{ij} = \bar{\pi}_{ji})$. Полученные выше результаты относительно представления квадратичных форм в виде суммы квадратов сохраняются также и для эрмитовских форм. Эрмитовская форма приводится к нормальному виду:

$$H(u, u) = \sum_1^r \bar{c}_i c_i \gamma_i \quad (\gamma_i \text{ действительны}). \qquad (3)$$

Форма H называется снова *определенной*, если $H(u, u)$ всегда положительно, кроме $u = 0$, или если $r = n$ и все $\gamma_1, \ldots, \gamma_n$ положительны. После присоединения квадратных корней из этих γ_i всякая определенная форма преобразуется в *единичную форму*:

$$E(u, u) = \sum \bar{c}_i c_i.$$

Теперь речь будет итти исключительно об эрмитовских формах. Чтобы все нижеизложенное имело место также и для квадратичных форм, надо рассматриваемые величины выбрать из $\mathfrak{K}$ и опустить все верхние черточки.

Возьмем в качестве *основной формы* определенную форму $G(u, u)$ ранга n и обозначим матрицу ее коэфициентов (g_{ik}) через G. Если в частности $G(u, u)$ — единичная форма, то G равно единичной матрице E. Два вектора u, v называются *перпендикулярными*, если $G(u, v) = 0$. Но тогда $G(v, u)$ также равно нулю. Векторы v, перпендикулярные к вектору $u \neq 0$, образуют линейное подпространство: *пространство, перпендикулярное* u. Если G — определенная форма, то $G(u, u) \neq 0$, откуда следует, что само u не принадлежит перпендикулярному

пространству R_{n-1}. Система n перпендикулярных друг к другу векторов $v_1, \ldots, v_n$ базиса называется *полной ортогональной системой векторов*. Ортогональная система называется *нормированной*, если $G(v_j, v_j) = 1$.

Линейные преобразования A, для которых

$$G(Au, v) = G(u, Av) \qquad \text{(для всех } u \text{ и } v\text{)},$$

называются *эрмитовскими симметричными* или просто *симметричными преобразованиями*. Для симметричности преобразований необходимо, чтобы имело место

$$\sum\sum\sum g_{il}\bar{a}_{ij}\bar{c}_j c_l = \sum\sum\sum g_{jk}\bar{c}_j a_{kl} c_l,$$

или

$$\sum_i g_{il}\bar{a}_{ij} = \sum_k g_{jk} a_{kl},$$

или

$$\tilde{A}G = GA.$$

Если в частности G есть единичная форма, то условие симметрии примет следующий простой вид:

$$\tilde{A} = A \quad \text{или} \quad \bar{a}_{lk} = a_{ki},$$

откуда ясно происхождение термина „симметричный".

Линейные преобразования U, оставляющие инвариантной основную форму $G(u, u)$:

$$G(Au, Au) = G(u, u) \quad \text{или} \quad \tilde{A}GA = G,$$

называются *унитарными* или в случае действительных чисел *ортогональными*. Очевидно, что тогда имеет место также $G(Au, Av) = G(u, v)$. Если в частности $G = E$, что всегда можно предположить в случае определенной формы, то

$$\tilde{A}A = E, \quad \text{или} \quad \tilde{A} = A^{-1}, \quad \text{или} \quad A\tilde{A} = E.$$

Отсюда получаются условия ортогональности:

$$\sum \bar{a}_{lk} a_{il} = \delta_{kl} = \begin{cases} 0 & \text{для } k \neq l, \\ 1 & \text{для } k = l, \end{cases}$$

или равносильные им условия

$$\sum a_{ik}\bar{a}_{jk} = \delta_{ij}.$$

Действительное ортогональное преобразование называется *поворотом*.

Если симметричное или унитарное преобразование A преобразует вектор u, отличный от нуля, в λu:

$$Au = \lambda u, \tag{4}$$

т. е. если A оставляет инвариантным луч, образованный вектором u, то A также оставляет инвариантным R_{n-1}, перпендикулярное к u.

Доказательство. Если v принадлежит R_{n-1}, т. е. $G(u, v) = 0$, то для симметричного A имеет место

$$G(u, Av) = G(Au, v) = G(\lambda u, v) = \lambda G(u, v) = 0,$$

а для унитарного A:

$$G(u, Av) = G(AA^{-1}u, Av) = G(A^{-1}u, v) = G(\lambda^{-1}u, v) = \\ = \lambda^{-1}G(u, v) = 0.$$

Вектор $u \neq 0$, удовлетворяющий равенству (4), называется *собственным вектором* преобразования A, λ называется *собственным значением*.

Мы уже в § 110 видели, что собственные значения находятся из „*векового уравнения*“

$$\chi(\lambda) = \begin{vmatrix} \lambda - \alpha_{11} & -\alpha_{12} \dots \\ -\alpha_{21} & \lambda - \alpha_{22} \dots \\ \dots & \dots \end{vmatrix} = 0, \tag{5}$$

а соответствующие собственные векторы определяются из уравнений

$$\sum \alpha_{ik} c_k = \lambda c_i, \tag{6}$$

равносильных (4).

Если мы теперь предположим, что поле K действительно замкнуто (например K — поле действительных чисел), в силу чего $\mathsf{K}(\Theta)$ алгебраически замкнуто (см. § 67), то вековое уравнение (5) обязательно будет иметь в $\mathsf{K}(\Theta)$ корень λ_1, которому будет соответствовать собственный вектор e_1. Пространство R_{n-1}, перпендикулярное к e_1, преобразуется с помощью A в самого себя, и если A в R_n симметрично или унитарно, то A симметрично или унитарно в R_{n-1}. Отсюда снова выводим, что в R_{n-1} существует собственный вектор e_2, причем внутри R_{n-1} имеется пространство R_{n-2}, перпендикулярное к R_{n-1} и инвариантное относительно A, и т. д.

Таким образом в конечном счете получим полную систему n линейно независимых собственных векторов $e_1, \dots, e_n$, *перпендикулярных между собою*:

$$Ae_\nu = \lambda_\nu e_\nu .$$

Матрица A относительно нового базиса $(e_1, \dots, e_n)$ принимает диагональный вид:

$$A_1 = P^{-1}AP = \begin{pmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & & \ddots \\ 0 & & \lambda_n \end{pmatrix}. \tag{7}$$

Если нормировать e_ν так, чтобы имело место $G(e_\nu, e_\nu) = 1$ [1]), то G в случае базиса $(e_1, \dots, e_n)$ будет равна единичной форме E. Если

[1]) Такое нормирование для действительно замкнутого K всегда возможно, так как корень квадратный из положительной величины $G(e_\nu, e_\nu)$ существует и содержится в K.

матрица A симметрична, то A_1 должна быть также симметричной и потому должна совпадать с $\widetilde{A}_1$, а отсюда следует, что

$$\lambda_\nu = \overline{\lambda}_\nu \quad \text{или} \quad \lambda_\nu \in \mathsf{K}.$$

Характеристический полином матрицы A или A_1 равен

$$\chi(x) = \prod_1^n (x - \lambda_n),$$

в силу чего *вековое уравнение* $\chi(\lambda) = 0$ *симметрической матрицы* A *имеет только действительные корни.*

Если, сверх того, матрицы A и G действительны, то e_ν как решения действительных уравнений (6) действительны. *Отсюда следует, что действительная симметричная матрица* A *приводится действительными преобразованиями к диагональному виду* (7).

При доказательстве этой теоремы мы исходили из существования корней λ_ν в $\mathsf{K}(\Theta)$, а затем показали, что λ_ν должны быть действительными. Можно доказать эту теорему применительно к случаю поля действительных чисел; об этом см. у R. Courant und D. Hilbert, Methoden der mathematischen Physik, т. I, § 3, 1924 (имеется русский перевод).

С симметрическим преобразованием A инвариантно связана эрмитовская форма:

$$H(u, u) = G(u, Au) = G(Au, u),$$

матрица которой, очевидно, равна

$$H = GA,$$

откуда может быть определена также матрица A:

$$A = G^{-1}H.$$

Если A и G приведены к диагональному виду, то $H = GA$ также принимает диагональную форму, причем преобразованная форма будет выглядеть так:

$$H(u, u) = \sum \bar{c}_\nu c_\nu \lambda_\nu.$$

Отсюда получается следующее предложение:

Всякая пара эрмитовских форм G, H, *среди которых одна, например* G, *определенная, приводится одним и тем же преобразованием к виду*

$$G(u, u) = \sum \bar{c}_\nu c_\nu,$$

$$H(u, u) = \sum \bar{c}_\nu c_\nu \lambda_\nu,$$

λ_i являются характеристическими корнями матрицы $A = G^{-1}H$ или, что одно и то же, корнями векового уравнения

$$|\lambda g_{ik} - h_{jk}| = 0.$$

В частности *любая пара действительных квадратичных форм, из которых одна определенная, приводится одновременно действительным преобразованием к сумме квадратов*:

$$G(u, u) = \sum c_\nu^2,$$

$$H(u, u) = \sum c_\nu^2 \lambda_\nu .$$

Полное изложение, посвященное классификации пары квадратичных форм, см. у L. E. Dickson, Modern algebraic Theories, Chicago 1926 (см. также немецкий перевод E. Bodewig, Leipzig 1929).

Задачи. 1. Если r векторов $v_1, \ldots, v_r$ порождают R_r, то векторы, перпендикулярные к v_i, образуют R_{n-r}, а все пространство R_n равно прямой сумме $R_r + R_{n-r}$.

2. Если симметрическое или унитарное преобразование A оставляет инвариантным пространство R_r, то перпендикулярное к нему R_{n-r} также инвариантно относительно A.

3. Всякая система симметрических или унитарных преобразований вполне приводима.

4. Определитель D унитарного преобразования по модулю равен единице, т. е. $D\bar{D} = 1$. Определитель действительного ортогонального преобразования равен ± 1.

5. Унитарные, а также действительные ортогональные преобразования векторного пространства на самого себя образуют группу.

ГЛАВА ШЕСТНАДЦАТАЯ

ТЕОРИЯ ГИПЕРКОМПЛЕКСНЫХ ВЕЛИЧИН

§ 112. СИСТЕМА ГИПЕРКОМПЛЕКСНЫХ ВЕЛИЧИН

Под *гиперкомплексной системой* (или *алгеброй*) относительно коммутативного поля P мы разумеем согласно § 10 кольцо, которое образует конечный модуль линейных форм относительно P:

$$\mathfrak{o} = b_1\mathsf{P} + \ldots + b_n\mathsf{P},$$

причем элементы P перестановочны с элементами $\mathfrak{o}$. Таким образом элементы $\mathfrak{o}$ имеют вид:

$$a = b_1\lambda_1 + \ldots + b_n\lambda_n = \lambda_1 b_1 + \ldots + \lambda_n b_n \quad (\lambda_i \in \mathsf{P}).$$

Если b_i линейно независимы относительно P, то число n будет *рангом* системы. Гиперкомплексная система $\mathfrak{o}$ вполне определяется элементами базиса, их таблицей умножения и полем P. Если P не вызывает сомнения, то пишут тогда просто $\mathfrak{o} = (b_1, \ldots, b_n)$. На таблицу умножения должно быть наложено единственное условие, состоящее в том, чтобы элементы базиса удовлетворяли ассоциативному закону:

$$b_\lambda (b_\mu b_\nu) = (b_\lambda b_\mu) b_\nu .$$

Примеры гиперкомплексных систем:

a) *Полное кольцо квадратных матриц* n-го порядка относительно P. Элементы базиса c_{ik} удовлетворяют равенствам:

$$c_{ij}c_{jl} = c_{il}, \quad c_{ij}c_{kl} = 0 \qquad (j \neq k)$$

(см. § 104, задача 4).

b) *Групповое кольцо* конечной группы $\mathfrak{G}$. Элементы базиса этого кольца вместе с тем являются элементами $\mathfrak{G}$ (см. § 10, задача 13). Здесь ранг равен порядку группы.

c) Все конечные поля расширения P, содержащие P в центре. Ранг здесь равен степени поля. Примером может служить конечное коммутативное поле расширения, которое было рассмотрено в главе 5.

d) Кольцо кватернионов $\mathfrak{v} = (1, j, k, l)$ ранга 4, которое определяется следующей таблицей умножения:

$$j^2 = k^2 = l^2 = -1,$$
$$jk = -kj = l,$$
$$kl = -lk = j,$$
$$lj = -jl = k$$

(см. § 10, задача 12).

e) Кольцо вычетов по идеалу $\mathfrak{a}$ нулевого измерения области полиномов $\mathsf{P}[x_1, \ldots, x_n]$ образует (коммутативную) гиперкомплексную систему относительно P. Ранг здесь будет называться *степенью* идеала $\mathfrak{a}$.

f) Кольцо вычетов по рациональному простому числу p, взятому из порядка числового поля, образует коммутативную гиперкомплексную систему относительно $\mathsf{P} = \frac{C}{(p)}$, где C — кольцо целых рациональных чисел. Ранг здесь равен степени числового поля.

Задачи. 1. Гиперкомплексная система без делителей нуля образует поле [1]) (сравнить ранги систем $a\mathfrak{v}$ и $\mathfrak{v}$ при $a \neq 0$).

2. Если в гиперкомплексной системе $\mathfrak{v}$ существует не делитель нуля a, то уравнения $xa = b$ и $ax = b$ разрешимы; тогда существует единица, и всякий не делитель нуля обладает в $\mathfrak{v}$ обратным элементом.

3. Кольцо кватернионов тогда и только тогда свободно от делителей нуля (т. е. образует поле [1]) если в основном поле P сумма четырех квадратов равна нулю только в том случае, когда равны нулю все четыре члена (использовать тождество, которое было приведено в задаче 12 § 10).

4. Алгебраически замкнутое поле не может быть расширено до гиперкомплексной системы, свободной от делителей нуля.

5. Если P — (коммутативное) поле, характеристика которого отлична от 2, то существует только следующие три типа гиперкомплексных систем ранга 2 и с единицей (все они коммутативны; почему?):

a) $(1, c)$, где c^2 лежит в P и не является там квадратом. Система образует коммутативное поле относительно P.

b) $(1, c)$, где c^2 — квадрат элемента $\gamma \neq 0$ поля P. Система равна

[1]) Здесь терминология автора расходится с общепринятой, согласно которой „полем" называется исключительно коммутативная система величин без делителей нуля. *(Прим. ред.)*

прямой сумме двух полей $(c-\gamma)\mathsf{P}=\mathsf{P}_1$ и $(c+\gamma)\mathsf{P}=\mathsf{P}_2$; P_1 и P_2 изоморфны P и взаимно уничтожаются: $\mathsf{P}_1\mathsf{P}_2=(0)$.

c) $(1, c)$, где $c^2=0$ (*система двоичных чисел*).

6. Кольцо вычетов гиперкомплексной системы с единицей по двустороннему идеалу также образует гиперкомплексную систему относительно того же основного поля („разностная алгебра").

§ 113. ГИПЕРКОМПЛЕКСНАЯ СИСТЕМА КАК ГРУППА С ОПЕРАТОРАМИ. ОБОБЩЕНИЯ

Гиперкомплексная система $\mathfrak{o}$, рассматриваемая как абелева группа относительно сложения, допускает две области операторов.

Во-первых, это будет поле P. Допустимыми подгруппами относительно этой области операторов являются все *линейные системы*, т. е. подмножества системы $\mathfrak{o}$, которые вместе с a, b содержат также λa (для всякого λ из P) и $a-b$. Линейные системы имеют ранг, не превосходящий n, где n — ранг $\mathfrak{o}$ (§ 28).

Во-вторых, областью операторов будет сама система $\mathfrak{o}$, так как элементы $\mathfrak{o}$ можно по произволу считать левыми или правыми операторами. Здесь допустимыми подгруппами будут *левые*, *правые* и *двусторонние идеалы*.

Мы будем рассматривать только такие (левые, правые или двусторонние) идеалы системы $\mathfrak{o}$, для которых поле P также образует область операторов. Это значит, что мы будем считать допустимыми левыми идеалами только такие подгруппы, которые вместе с a содержат не только $ra\,(r\in\mathfrak{o})$, но также и любое $\lambda a\,(\lambda\in\mathsf{P})$ и то же самое для правых идеалов. Таким образом допустимые идеалы образуют линейные системы. Подобным же образом два левых идеала считаются *операторно-изоморфными*, если существует изоморфизм, переводящий всякое ra в $\overline{ra}$ и λa в $\lambda\overline{a}$, когда a переходит в $\overline{a}$ [1]). Левый идеал называется *простым* или *минимальным*, если он не содержит допустимых идеалов, кроме самого себя и идеала (0).

При этих ограничениях, налагаемых на понятие идеала, для гиперкомплексной системы будут иметь место так называемые *условия максимальности и минимальности*, заключающиеся в следующем:

Всякое не пустое множество (правых, левых и двусторонних) идеалов содержит (по меньшей мере) один максимальный идеал, т. е. такой идеал, который не содержится ни в одном из остальных идеалов множества; это же множество содержит минимальный идеал, не содержащий другие идеалы множества.

В самом деле, согласно нашему условию любой идеал образует вместе с тем линейную систему, и в каждом не пустом множестве линейных систем ранга меньшего или равного n существует система наибольшего и наименьшего ранга.

Чтобы представить в самом общем виде основные теоремы гиперкомплексной алгебры, мы на протяжении этой главы будем говорить

[1]) Нельзя смешивать этот изоморфизм с кольцевым изоморфизмом, так как при кольцевом изоморфизме ra переходит в $\overline{r}\,\overline{a}$, а не в $\overline{ra}$, где r и a принадлежат рассматриваемому подкольцу.

не только о гиперкомплексных системах, но иметь вообще в виду кольцо $\mathfrak{o}$, для которого выполняются только что сформулированные условия максимальности и минимальности, хотя бы для левых идеалов. Более того, мы будем иногда предполагать, что имеет место либо только условие максимальности, либо только условие минимальности [1]). Для кольца $\mathfrak{o}$ может существовать (но не обязательно) область операторов Ω (которая играет роль прежнего $\mathbf{P}$); операторы $\lambda, \mu, \ldots$ этой области должны обладать свойствами:

$$\lambda(a+b) = \lambda a + \lambda b,$$
$$\lambda(ab) = (\lambda a)\, b = a\,(\lambda b).$$

Если такая область операторов существует, то понятие идеала мы, как и выше, ограничиваем требованием, чтобы идеал вместе с a содержал также λa ($\lambda \in \Omega$). В тех случаях, когда желательно отметить идеалы подобного рода, мы будем говорить о *допустимых* правых и левых идеалах. И здесь также постулируется условие максимальности или минимальности.

Очевидно, что кольцо, удовлетворяющее только условиям максимальности и минимальности, сильно расширяет область приложения нашей теории, так как существует чрезвычайно большое число колец, которые удовлетворяют этим условиям, но тем не менее не образуют гиперкомплексной системы. Например, условиям максимальности и минимальности удовлетворяют все конечные кольца (в частности кольца вычетов по идеалу $\mathfrak{a} \neq (0)$ из порядка числового поля). Еще более частным примером является кольцо вычетов по целому числу кольца C. В ближайших задачах 3, 4 и 5 указано, какие коммутативные кольца должны удовлетворять этим условиям. Но нашей основной целью все же остается исследование гиперкомплексной системы.

Полезно еще заметить, что условие минимальности является гораздо более ограничительным, чем условие максимальности. В самом деле, уже в § 80 мы видели, что существует широкий класс колец с делителями и без делителей нуля, удовлетворяющих условию максимальности, в то время как условие минимальности удовлетворяется, например, для кольца без делителей нуля только тогда, когда кольцо есть поле (об этом будет подробнее ниже).

Необходимо выяснить, какие из понятий теории идеалов (сумма, произведение и т. д.) сохраняют значение для некоммутативного кольца с областью операторов или без области операторов. Прежде всего ясно, что (как и вообще для группы с операторами) *пересечение* $\mathfrak{a} \cap \mathfrak{b}$ и *сумма* $(\mathfrak{a}, \mathfrak{b})$ двух допустимых правых (левых) идеалов $\mathfrak{a}$ и $\mathfrak{b}$ всегда образуют также допустимые правые (левые) идеалы. *Произведение* $\mathfrak{a} \cdot \mathfrak{b}$ (множество всех сумм вида $\sum ab$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$), как это видно непосредственно, является допустимым правым идеалом, если второй сомножитель есть допустимый правый идеал, и $\mathfrak{ab}$ есть допустимый левый идеал, когда первый сомножитель есть допустимый левый идеал. Другой сомножитель может оказаться совершенно произвольным множеством

[1]) Согласно § 80 условие максимальности равносильно постулату о цепях делителей.

или также быть элементом $\mathfrak{o}$; например, $\mathfrak{r}$—совокупность всех произведений вида $ra\,(a \in \mathfrak{r})$, есть правый идеал, если $\mathfrak{r}$ — правый идеал.

Как и обычно, для модулей и в частности для идеалов кольца $\mathfrak{o}$ имеют место законы ассоциативности и дистрибутивности:

$$\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\,\mathfrak{c},$$
$$\mathfrak{a}(\mathfrak{b},\ \mathfrak{c}) = (\mathfrak{a}\mathfrak{b},\ \mathfrak{a}\mathfrak{c}),$$
$$(\mathfrak{b},\ \mathfrak{c})\,\mathfrak{a} = (\mathfrak{b}\mathfrak{a},\ \mathfrak{c}\mathfrak{a}).$$

Здесь $\mathfrak{a}$ может быть даже произвольным множеством, а также отдельным элементом.

Если в кольце выполняется условие минимальности, например, для левых идеалов и $\mathfrak{o}$ не нулевое кольцо, то множество *всех* левых идеалов, отличных от нуля, должно содержать минимальный идеал; мы его назовем просто *минимальным левым идеалом*. Этот идеал характеризуется тем, что он не обладает собственным подидеалом, отличным от нуля, и потому может быть назван также *простым левым идеалом*.

Если (односторонний или двусторонний) идеал $\mathfrak{a}$ кольца $\mathfrak{o}$ равен прямой сумме односторонних или двусторонних идеалов:

$$\mathfrak{a} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n,$$

$n > 1$, и каждое $\mathfrak{a}_\nu \neq 0$, то идеал $\mathfrak{a}$ (односторонний или двусторонний) называется *разложимым в прямую сумму*. Если же такое разложение невозможно, то говорят, что идеал $\mathfrak{a}$ *неразложим в прямую сумму*.

Чтобы показать, насколько решающее значение имеет условие минимальности, докажем следующие теоремы:

Если $\mathfrak{o}$ есть кольцо с условием минимальности для левых идеалов, a — элемент кольца $\mathfrak{o}$, причем a не является правым делителем нуля в $\mathfrak{o}$, то уравнение $xa = b$ разрешимо для всякого b.

Доказательство. Среди множества идеалов $\mathfrak{o}a^\mu$ $(\mu = 1, 2, \ldots)$ должен существовать минимальный идеал, например $\mathfrak{o}a^m$. Так как $\mathfrak{o}a^{m+1} \subseteq \mathfrak{o}a^m$, а случай $\mathfrak{o}a^{m+1} \subset \mathfrak{o}a^m$ исключается, то должно иметь место $\mathfrak{o}a^{m+1} = \mathfrak{o}a^m$; следовательно, произведение ba^m может также быть записано в виде ca^{m+1}:

$$ba^m = ca^{m+1}.$$

Но так как равенство можно сократить на a^m, то отсюда следует:

$$b = ca;$$

таким образом уравнение $xa = b$ разрешимо.

Точно так же, *если $\mathfrak{o}$ — кольцо с условием минимальности для правых идеалов и a не является левым делителем нуля, то $ax = b$ разрешимо.*

Из этих теорем вытекает:

Если $\mathfrak{o}$ есть кольцо без делителей нуля с условием минимальности для правых и левых идеалов, то $\mathfrak{o}$ есть поле.

Задачи. 1. Для кольца с единицей упомянутое выше ограничение понятия идеала, которое налагается в случае операторной области P или Ω, оказывается несущественным: всякий идеал допускает умножение на P или Ω.

2. Для выполнения условий максимальности и минимальности для левых идеалов области $\mathfrak{o}$ необходимо и достаточно существование композиционного ряда для этих левых идеалов.

3. В коммутативном кольце с условием минимальности кольцо вычетов по простому идеалу всегда является полем и потому всякий его простой идеал свободен от делителей.

4. Неразложимое на прямую сумму коммутативное кольцо с условием минимальности примарно [т. е. идеал (0) примарен]; примарное коммутативное кольцо неразложимо на прямую сумму.

5. Пусть $\mathfrak{a}$ — идеал коммутативного кольца $\mathfrak{o}$, в котором выполняется условие максимальности (теорема о делителях). Для того чтобы в кольце вычетов $\frac{\mathfrak{o}}{\mathfrak{a}}$ удовлетворялось условие минимальности, необходимо и достаточно, чтобы всякий простой делитель $\mathfrak{p}$ идеала $\mathfrak{a}$ был идеалом кольца $\mathfrak{o}$, свободным от делителей. [Для „необходимости" надо использовать задачу 3; для „достаточности" надо представить на основании § 85 и 86 кольцо $\frac{\mathfrak{o}}{\mathfrak{a}}$ в виде прямой суммы примарных колец.]

§ 114. НИЛЬПОТЕНТНЫЕ ИДЕАЛЫ

Элемент a кольца $\mathfrak{o}$ называется *нильпотентным*, если для некоторого ρ имеет место $a^\rho = 0$. Идеал (левый или правый) $\mathfrak{a}$ называется *нильпотентным*, если некоторая его степень $\mathfrak{a}^\rho$ равна идеалу (0). Оказываются справедливыми следующие теоремы:

1. *Сумма* $(\mathfrak{l}_1, \mathfrak{l}_2)$ *двух нильпотентных левых идеалов образует нильпотентный левый идеал.*

Доказательство. Пусть $\mathfrak{l}_1^n = \mathfrak{l}_2^m = (0)$. Рассмотрим идеал $(\mathfrak{l}_1, \mathfrak{l}_2)^{n+m-1}$. Этот левый идеал равен сумме, отдельные слагаемые которой равны произведению $n+m-1$ сомножителей $\mathfrak{l}_1$ или $\mathfrak{l}_2$. В таком произведении $\mathfrak{l}_1$ должен встречаться по меньшей мере n раз или $\mathfrak{l}_2$ — по меньшей мере m раз. Пусть, например, $\mathfrak{l}_1$ встречается n раз. Тогда слагаемое имеет вид:

$$\ldots \mathfrak{l}_1 \ldots \mathfrak{l}_1 \ldots \mathfrak{l}_1 \ldots,$$

где точками обозначены возможные множители $\mathfrak{l}_2$. Так как $\mathfrak{o}\mathfrak{l}_1 \subset \mathfrak{l}_1$, то $\ldots \mathfrak{l}_1 \ldots \mathfrak{l}_1 \ldots \mathfrak{l}_1 \ldots \subset \mathfrak{l}_1^n = (0)$, откуда:

$$(\mathfrak{l}_1, \mathfrak{l}_2)^{n+m-1} = (0).$$

2. *Нильпотентный левый идеал* (*или правый идеал*) *содержится в нильпотентном двустороннем идеале.*

Доказательство. Пусть $\mathfrak{l}$ — нильпотентный левый идеал: $\mathfrak{l}^\rho = (0)$. Тогда идеал $\mathfrak{l}\mathfrak{o}$ также будет нильпотентным:

$$(\mathfrak{l}\mathfrak{o})^\rho = \mathfrak{l}(\mathfrak{o}\mathfrak{l})^{\rho-1}\mathfrak{o} \subset \mathfrak{l}^{\rho-1}\mathfrak{o} = \mathfrak{l}^\rho\mathfrak{o} = (0).$$

Поэтому правый идеал $(\mathfrak{l}, \mathfrak{l}\mathfrak{o})$ равен сумме двух нильпотентных левых идеалов, в силу чего он сам является нильпотентным левым идеалом, а это значит, что $(\mathfrak{l}, \mathfrak{l}\mathfrak{o})$ есть двусторонний нильпотентный идеал.

Если под собственно нильпотентной величиной w мы будем подразумевать элемент $\mathfrak{o}$, порождающий нильпотентный двусторонний идеал, то можно высказать такую теорему:

3. *Все элементы нильпотентного левого или правого идеала суть собственно нильпотентные элементы.*

Доказательство. Если w содержится в нильпотентном левом идеале, то в силу 2 w содержится также в нильпотентном двустороннем идеале, откуда и получается, что двусторонний идеал, порожденный w, должен быть также нильпотентным.

Согласно 3 собственно нильпотентные элементы можно определить как элементы, порождающие нильпотентный левый или правый идеал.

4. *Совокупность всех собственно нильпотентных элементов есть двусторонний идеал, который содержит все нильпотентные правые и левые идеалы.*

Доказательство. Если w_1 и w_2 — собственно нильпотентные элементы и $\mathfrak{w}_1$, $\mathfrak{w}_2$ — порождаемые ими двусторонние идеалы, то $w_1 - w_2$ содержится в идеале $(\mathfrak{w}_1, \mathfrak{w}_2)$, который в силу 1 является нильпотентным. Точно так же cw_1 и $w_1 c$ суть собственно нильпотентные элементы, так как они принадлежат $\mathfrak{w}_1$. Следовательно, совокупность собственно нильпотентных элементов образует двусторонний идеал. Остальная часть теоремы следует из 3.

Совокупность всех собственно нильпотентных элементов кольца $\mathfrak{o}$ называется его радикалом.

Определение. *Кольцо без радикала* — это кольцо, радикал которого равен (0), или также кольцо, в котором идеал (0) является единственным нильпотентным идеалом.

Таким образом в „кольце с радикалом" должен существовать нильпотентный левый или правый идеал и потому согласно 2 существует также нильпотентный двусторонний идеал $\mathfrak{a} \neq (0)$. Легко видеть, что тогда существует такой двусторонний идеал $\mathfrak{c} \neq (0)$, что $\mathfrak{c}^2 = (0)$. Именно, если ρ есть наименьшее число, для которого имеет место $\mathfrak{a}^\rho = (0)$, то достаточно положить $\mathfrak{c} = \mathfrak{a}^{\rho-1}$.

Если в $\mathfrak{o}$ выполняется условие максимальности для левых идеалов, то существует максимальный нильпотентный левый идеал $\mathfrak{l}$. Он должен содержать все собственно нильпотентные элементы w, так как в противном случае идеал $(w, \mathfrak{l})$ содержал бы $\mathfrak{l}$. Следовательно, $\mathfrak{l}$ равно радикалу, а отсюда вытекает, что сам радикал есть нильпотентный идеал.

Отсюда далее следует такое предложение:

Кольцо вычетов $\frac{\mathfrak{o}}{\mathfrak{w}}$ кольца, удовлетворяющего условию максимальности, по радикалу $\mathfrak{w}$ есть кольцо без радикала.

Доказательство. В $\frac{\mathfrak{o}}{\mathfrak{w}}$ левый идеал можно всегда принять за группу классов вычетов $\frac{\mathfrak{l}}{\mathfrak{w}}$, где $\mathfrak{l}$ — левый идеал кольца $\mathfrak{o}$. Если

$$\left(\frac{\mathfrak{l}}{\mathfrak{w}}\right)^\rho = (0),$$

то любое произведение ρ классов вычетов из $\mathfrak{l}$ (по модулю $\mathfrak{w}$) равно

нулю, в силу чего любое произведение ρ элементов из $\mathfrak{l}$ содержится в $\mathfrak{w}$:

$$\mathfrak{l}^{\rho} \subseteq \mathfrak{w}, \quad \mathfrak{w}^{\tau} = (0), \quad \mathfrak{l}^{\rho\tau} = (\mathfrak{l}^{\rho})^{\tau} \subseteq \mathfrak{w}^{\tau} = (0);$$

следовательно, $\mathfrak{l}$ есть нильпотентный идеал, а потому

$$\mathfrak{l} \subseteq \mathfrak{w}, \quad \mathfrak{l}_{\mathfrak{w}} = (0).$$

Кольцо без радикала, удовлетворяющее условию минимальности для левых идеалов, называется *полупростым*. Этот термин может быть объяснен так: полупростота накладывает, если, кроме условия минимальности, предположить еще существование единичного элемента, несколько меньшие условия, чем простота, т. е. отсутствие в $\mathfrak{o}$ двусторонних идеалов, кроме (0) и самого $\mathfrak{o}$. В самом деле, предположив в $\mathfrak{o}$ существование единичного элемента, мы убедимся, что само $\mathfrak{o}$ не может быть нильпотентным идеалом; таким образом радикалом простой системы с единичным элементом может быть только (0).

Задачи. 1. Среди гиперкомплексных систем задачи 5 § 112 первые две системы полупростые; напротив, в последней системе линейная система (c) образует радикал.

2. Гиперкомплексная система ранга 3 с таблицей умножения

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

обладает радикалом. Найти этот радикал. Кольцо вычетов по радикалу равно прямой сумме двух полей.

3. Система всех матриц n-го порядка поля K является простой.

4. В случае коммутативного кольца собственно нильпотентные элементы совпадают с нильпотентными элементами. Вывести отсюда следующее предложение: кольцо вычетов $\frac{c}{(m)}$ по целому рациональному числу m тогда и только тогда не имеет радикала, если m не содержит квадрата.

5. То же самое показать для кольца вычетов по идеалу главного порядка числового поля.

6. Радикал коммутативного примарного кольца является простым идеалом, принадлежащим нулевому идеалу.

7. Если $(0) = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ есть разложение идеала (0) коммутативного кольца $\mathfrak{o}$ на примарные компоненты и $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ суть соответствующие простые идеалы, то $[\mathfrak{p}_1, \ldots, \mathfrak{p}_r]$ есть радикал.

§ 115. ПОЛНАЯ ПРИВОДИМОСТЬ КОЛЬЦА БЕЗ РАДИКАЛА

Все групповые термины (прямая сумма, операторный изоморфизм и т. д.), встречающиеся в этом параграфе, относятся к кольцу $\mathfrak{o}$ и его левым идеалам, которые рассматриваются как абелевы группы с (левой) операторной областью $\mathfrak{o}$ (возможно еще существование P или Ω; см. § 113).

Целью настоящего параграфа является доказательство следующей *основной теоремы о полупростом кольце*:

Кольцо $\mathfrak{o}$ *без радикала с условием минимальности для левых идеалов обладает единицей и равно прямой сумме простых левых идеалов. Обратно: кольцо с единицей, равное прямой сумме простых левых идеалов, есть кольцо без радикала с условием минимальности для левых идеалов.*

Для доказательства полезны следующие леммы, которые также сами по себе представляют интерес.

Лемма 1. *Если* $\mathfrak{l}$ *— левый идеал,* a *— элемент кольца* $\mathfrak{o}$, *то* $\mathfrak{l}$ *отображается операторно-гомоморфно на* $\mathfrak{l}a$ *с помощью соответствия*

$$x \to xa.$$

Доказательство.

$$(x+y)\,a = xa + ya,$$
$$(rx)\cdot a = r\cdot(xa),$$
$$(\lambda x)\cdot a = \lambda\cdot(xa)\ ^{1}).$$

Лемма 2. *Минимальный (он же простой) левый идеал* $\mathfrak{l}$ *либо операторно-гомоморфно отображается на идеал* (0), *либо гомоморфизм есть изоморфизм.*

Доказательство. Совокупность элементов a идеала $\mathfrak{l}$, соответствующих нулю, образует левый идеал $\mathfrak{a} \subseteq \mathfrak{l}$; таким образом либо $\mathfrak{a} = (0)$, либо $\mathfrak{a} = \mathfrak{l}$. В первом случае соответствие будет изоморфным.

Определение. Элемент e кольца $\mathfrak{o}$ называется идемпотентным, если $e^2 = e$ (отсюда $e^3 = e$ и т. д.).

Отсюда следует, что нулевой элемент и единица (если только она существует) всегда идемпотентны.

Лемма 3. *Минимальный левый идеал* $\mathfrak{l}$ *либо нильпотентен и притом* $\mathfrak{l}^2 = (0)$, *либо содержит идемпотентный элемент* e, *каковой является порождающим для* $\mathfrak{l}$:

$$e^2 = e \in \mathfrak{l}, \quad \mathfrak{l} = \mathfrak{o}e.$$

Доказательство. Пусть $\mathfrak{l}^2 \neq (0)$. Тогда в $\mathfrak{l}$ существует некоторое a, для которого $\mathfrak{l}a \neq (0)$. Согласно лемме 1 соответствие $x \to xa$ является гомоморфизмом, а согласно лемме 2 мы имеем даже изоморфизм; этот изоморфизм переводит $\mathfrak{l}$ в $\mathfrak{l}a$, и притом

$$\mathfrak{l}a \neq (0), \quad \mathfrak{l}a \subseteq \mathfrak{l},$$

откуда

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

Следовательно, любой элемент $\mathfrak{l}$ можно представить в виде xa ($x \in \mathfrak{l}$), в частности для самого a имеет место:

$$a = ea.$$

Отсюда, во-первых, вытекает, что $e \neq 0$; во-вторых, $ea = e^2a$; таким

[1]) Доказательство справедливо и тогда, когда a взято из $\mathfrak{o}$-модуля, а не только из $\mathfrak{o}$.

образом e и e^2 при изоморфизме $x \to xa$ определяют один и тот же элемент ea, откуда

$$e^2 = e.$$

Идеал $\mathfrak{o}e$ не равен нулю (так как $\mathfrak{o}e$ содержит элемент $e^2 = e$) и содержится в $\mathfrak{l}$. Поэтому $\mathfrak{l} = \mathfrak{o}e$, и все доказано.

Лемма 4. *Если e — идемпотентный элемент и $\mathfrak{l} = \mathfrak{o}e$, то $\mathfrak{o}$ есть прямая сумма идеала $\mathfrak{l}$ и другого левого идеала $\mathfrak{l}'$:*

$$\mathfrak{o} = \mathfrak{l} + \mathfrak{l}'.$$

Далее, для всех x из $\mathfrak{l}$ имеет место

$$xe = x,$$

а для всех x' из $\mathfrak{l}'$:

$$x'e = 0.$$

Доказательство. Для a из $\mathfrak{o}$ положим $a = ae + (a - ae)$ (левое разложение Peirce'a). Элементы ae образуют левый идеал $\mathfrak{o}e = \mathfrak{l}$. Элементы $a - ae$ образуют также левый идеал $\mathfrak{l}'$, так как

$$(a - ae) - (b - be) = (a - b) - (a - b)e,$$
$$r(a - ae) = ra - (ra)e,$$
$$\lambda(a - ae) = \lambda a - (\lambda a)e.$$

$a - ae$ уничтожается элементом e:

$$(a - ae)e = ae - ae^2 = 0,$$

а ae при умножении на e остается без изменения:

$$(ae)e = ae^2 = ae.$$

Нуль — единственный элемент, который при умножении на e уничтожается и в то же время не меняется. Следовательно, $\mathfrak{l}$ и $\mathfrak{l}'$ могут иметь общим элементом только нуль, т. е. сумма $\mathfrak{o} = \mathfrak{l} + \mathfrak{l}'$ прямая.

Теперь мы в состоянии доказать первую часть основной теоремы.

Теорема 1. *Кольцо без радикала с условием минимальности для левых идеалов равно прямой сумме простых левых идеалов.*

Доказательство. Для нулевого кольца теорема очевидна. Поэтому пусть $\mathfrak{o}$ отлично от нулевого кольца, а $\mathfrak{l}_1$ — минимальный левый идеал, отличный от нуля. Согласно леммам 3 и 4

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}'.$$

Если $\mathfrak{l}'$ не нуль, то в $\mathfrak{l}'$ находим минимальный левый идеал $\mathfrak{l}_2$, отличный от нуля; тогда согласно леммам 3 и 4

$$\mathfrak{o} = \mathfrak{l}_2 + \mathfrak{l}^*,$$

а если ограничиться в этой сумме элементами $\mathfrak{l}'$, то получится:

$$\mathfrak{l}' = \mathfrak{l}_2 + \mathfrak{l}'',$$

откуда

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}''.$$

В случае $\mathfrak{l}'' \neq (0)$ снова находим в $\mathfrak{l}''$ минимальный левый идеал $\mathfrak{l}_3 \neq (0)$, откуда с помощью тех же соображений получим:

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}_3 + \mathfrak{l}'''$$

и т. д. Последовательность $\mathfrak{o} \supset \mathfrak{l}' \supset \mathfrak{l}'' \supset \mathfrak{l}''' \supset \ldots$ согласно условию минимальности должна содержать минимальный идеал. Обозначим его через $\mathfrak{l}_n$ и продолжим разложение до $\mathfrak{l}_n$. Тогда

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \ldots + \mathfrak{l}_n,$$

и таким образом теорема 1 *доказана*.

Каждый идеал $\mathfrak{l}_i$ порождается идемпотентным элементом

$$\mathfrak{l}_i = \mathfrak{o}e_i, \quad e_i^2 = e_i \in \mathfrak{l}_i.$$

Затем, так как $\mathfrak{l}'$ уничтожается элементом e_1, имеем:

$$e_2e_1 = 0, \; e_3e_1 = 0, \; \ldots, \; e_ne_1 = 0;$$

точно так же, так как $\mathfrak{l}''$ уничтожается e_2:

$$e_3e_2 = 0, \; \ldots, \; e_ne_2 = 0$$

и т. д.; вообще

$$e_ke_i = 0 \text{ для } k > i.$$

Чтобы доказать существование единицы, поступим следующим образом. Возьмем

$$e_{12} = e_1 + e_2 - e_1e_2.$$

Тогда

$$e_1e_{12} = e_1^2 + e_1e_2 - e_1^2e_2 = e_1,$$
$$e_2e_{12} = e_2e_1 + e_2^2 - e_2e_1e_2 = e_2,$$
$$(e_1e_2)\,e_{12} = e_1\,(e_2e_{12}) = e_1e_2.$$

Следовательно,

$$(e_1 + e_2 - e_1e_2)\,e_{12} = e_1 + e_2 - e_1e_2,$$
$$e_{12}^2 = e_{12}.$$

Таким образом e_{12} идемпотентно и содержится в $\mathfrak{l}_1 + \mathfrak{l}_2$. Но согласно приведенным выше расчетам среди xe_{12} встречаются как e_1, так и e_2; отсюда вытекает, что $\mathfrak{o}e_{12}$ содержит $\mathfrak{l}_1 + \mathfrak{l}_2$. Поэтому

$$\mathfrak{l}_1 + \mathfrak{l}_2 = \mathfrak{o}e_{12}.$$

Далее,

$$e_ke_{12} = 0 \quad \text{для} \quad k > 2.$$

Можно положить

$$e_{123} = e_{12} + e_3 - e_{12}e_3;$$

тогда подобным же образом окажется, что

$$e_{123}^2 = e_{123},$$
$$\mathfrak{o}e_{123} = \mathfrak{o}e_{12} + \mathfrak{l}_3 = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}_3.$$

Продолжая подобным образом, получим, наконец, равностепенный элемент $e = e_{12\ldots n}$ со свойством

$$\mathfrak{o}e = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n = \mathfrak{o}.$$

Согласно лемме 4 e есть правая единица для $\mathfrak{o} = \mathfrak{o}e$. Чтобы показать, что e есть также левая единица, воспользуемся правым разложением кольца $\mathfrak{o}$ (см. лемму 4). Тогда

$$\mathfrak{o} = e\mathfrak{o} + \mathfrak{r},$$
$$e\mathfrak{r} = (0),$$
$$\mathfrak{r} = \mathfrak{r}e \text{ (так как } e \text{ — правая единица),}$$

откуда

$$\mathfrak{r}^2 = \mathfrak{r}e\mathfrak{r} = (0);$$

следовательно, из того, что $\mathfrak{o}$ есть кольцо без радикала, следует:

$$\mathfrak{r} = (0),$$
$$\mathfrak{o} = e\mathfrak{o}.$$

Таким образом e — левая единица.

Тем самым первая часть основной теоремы *доказана*.

Для доказательства ее второй части используем следующую **лемму:**

Лемма 5. *Если кольцо $\mathfrak{o}$ с единицей равно прямой сумме n левых идеалов:*

$$\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n$$

и для единицы в частности имеем разложение

$$1 = e_1 + \ldots + e_n \quad (e_i \in \mathfrak{l}_i),$$

то

$$\mathfrak{l}_i = \mathfrak{o}e_i, \; e_i^2 = e_i, \; e_ie_k = 0 \text{ для } i \neq k.$$

Доказательство. Для всякого a из $\mathfrak{l}_1$ имеем:

$$a = a \cdot 1 = ae_1 + ae_2 + \ldots + ae_n.$$

С другой стороны,

$$a = a + 0 + \ldots + 0;$$

отсюда на основании свойства прямой суммы

$$ae_1 = a, \; ae_2 = 0, \; \ldots, \; ae_n = 0.$$

Если в частности положить $a = e_1$, то получится:

$$e_1^2 = e_1, \; e_1e_2 = 0, \; \ldots, \; e_1e_n = 0.$$

Точно так же имеем:

$$e_i^2 = e_i, \; e_ie_k = 0 \text{ для } i \neq k.$$

Далее уравнение $ae_1 = a$ показывает, что всякое a из $\mathfrak{l}_1$ можно записать в виде ae_1; отсюда следует, что

$$\mathfrak{l}_1 = \mathfrak{o}e_1,$$

и вообще

$$\mathfrak{l}_i = \mathfrak{o}e_i.$$

Заметим еще следующее. Если кольцо $\mathfrak{o}$ есть прямая сумма n *простых левых идеалов* или, как говорят, вполне *приводимо слева*, то прежде всего следует существование композиционного ряда (из левых идеалов) длины n (§ 42). Таким образом любой левый идеал обладает композиционным рядом, длина которого не превосходит n. Отсюда вытекает, что в любом непустом множестве левых идеалов существует идеал наименьшей длины, т. е. минимальный идеал. *Таким образом условие минимальности есть следствие полной приводимости* (точно также можно было доказать соблюдение условия максимальности). Далее получается, что всякий левый идеал является слагаемым прямой суммы (§ 42).

Если дополнительно допустить существование единицы, то весьма легко показать, что рассматриваемое кольцо $\mathfrak{o}$ есть кольцо без радикала. А именно если $\mathfrak{l}$ есть нильпотентный идеал, например $\mathfrak{l}^\rho = (0)$, то

$$\mathfrak{o} = \mathfrak{l} + \mathfrak{l}';$$

согласно лемме 5 в $\mathfrak{l}$ существует образующий элемент e_1, для которого имеет место $e_1^2 = e_1$. Тогда будем иметь также $e_1^\rho = e_1$. С другой стороны, из того, что e_1 — нильпотентно, следует $e_1^\rho = 0$; отсюда следует, что $e_1 = 0$ и $\mathfrak{l} = (0)$. Поэтому нильпотентным идеалом может быть только (0).

Итак, вторая часть основной теоремы также доказана.

Задачи. 1. Кольцо без делителей нуля с условием минимальности для левых идеалов образует поле.

2. Разложить кольцо с радикалом задачи 2 § 114 на неразложимые (относительно прямой суммы) левые (правые) идеалы и показать, что эти идеалы непростые.

3. Система всех квадратных матриц n-го порядка поля K вполне приводима (слева и справа).

4. Доказать следующее обращение леммы 5:

Если в кольце $\mathfrak{o}$ с единицей

$$1 = e_1 + \ldots + e_n,$$

$$e_i^2 = e_i, \quad e_i e_k = 0 \quad \text{для } i \neq k,$$

то

$$\mathfrak{o} = \mathfrak{o}e_1 + \ldots + \mathfrak{o}e_n$$

есть разложение кольца $\mathfrak{o}$ на левые идеалы и

$$\mathfrak{o} = e_1\mathfrak{o} + \ldots + e_n\mathfrak{o}$$

есть его разложение на правые идеалы.

§ 116. ДВУСТОРОННЕЕ РАЗЛОЖЕНИЕ И РАЗЛОЖЕНИЕ ЦЕНТРА

В § 115 мы говорили о разложении кольца $\mathfrak{o}$ в прямую сумму левых идеалов. Здесь мы увидим, что можно сказать о разложении

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n \tag{1}$$

на *двусторонние* идеалы.

Прежде всего непосредственно видно, что в разложении (1) слагаемые $\mathfrak{a}_i$ взаимно уничтожаются:

$$\mathfrak{a}_i\mathfrak{a}_k = (0) \quad \text{для } i \neq k,$$

так как $\mathfrak{a}_i\mathfrak{a}_k$ содержится как в $\mathfrak{a}_i$, так и в $\mathfrak{a}_k$.

Идеал $\mathfrak{a}_i$ можно также рассматривать как кольцо. Поэтому разложение (1) можно рассматривать как представление $\mathfrak{o}$ в виде суммы колец, которые взаимно уничтожаются.

Если, обратно, дано такое разложение $\mathfrak{o}$ в сумму взаимно уничтожающихся колец $\mathfrak{a}_i$, то эти кольца необходимо должны быть двусторонними идеалами кольца $\mathfrak{o}$, так как

$$\mathfrak{o}\mathfrak{a}_i = (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)\cdot\mathfrak{a}_i = (\mathfrak{a}_1\mathfrak{a}_i, \ldots, \mathfrak{a}_n\mathfrak{a}_i) = \mathfrak{a}_i^2 \subseteq \mathfrak{a}_i$$

и точно так же

$$\mathfrak{a}_i\mathfrak{o} \subseteq \mathfrak{a}_i.$$

Далее оказывается, что *любой (односторонний или двусторонний) идеал кольца $\mathfrak{a}_i$ является таким же идеалом в $\mathfrak{o}$*. В самом деле, если, например, $\mathfrak{l}$ есть левый идеал кольца $\mathfrak{a}_1$, то

$$\mathfrak{o}\mathfrak{l} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)\,\mathfrak{l} = (\mathfrak{a}_1\mathfrak{l}, \mathfrak{a}_2\mathfrak{l}, \ldots, \mathfrak{a}_n\mathfrak{l}) = \mathfrak{a}_1\mathfrak{l} \subseteq \mathfrak{l}.$$

Если в частности идеалы $\mathfrak{a}_i$ двусторонне простые, то они согласно этой теореме как кольца также двусторонне простые. Часто вместо „двусторонне простые кольца“ говорят коротко: *простые кольца*. Итак, простыми кольцами называются кольца, которые не содержат двусторонних идеалов, кроме самих себя и единичного идеала.

Если кольцо $\mathfrak{o}$ с единицей разлагается в прямую сумму неразложимых двусторонних идеалов, отличных от (0):

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n,$$

то идеалы $\mathfrak{a}_i$ определяются однозначно.

Доказательство. Если

$$\mathfrak{o} = \mathfrak{c}_1 + \ldots + \mathfrak{c}_m,$$

то

$$\mathfrak{c}_1 = \mathfrak{o}\mathfrak{c}_1 = (\mathfrak{a}_1\mathfrak{c}_1, \mathfrak{a}_2\mathfrak{c}_1, \ldots, \mathfrak{a}_n\mathfrak{c}_1).$$

Сумма справа прямая, так как

$$\mathfrak{a}_1\mathfrak{c}_1 \subseteq \mathfrak{a}_1, \ldots, \mathfrak{a}_n\mathfrak{c}_1 \subset \mathfrak{a}_n.$$

Но так как $\mathfrak{c}_1$ неразложимо, то все произведения справа должны быть равны (0), за исключением лишь одного, например $\mathfrak{a}_1\mathfrak{c}_1$. Тогда

$$\mathfrak{c}_1 = \mathfrak{a}_1\mathfrak{c}_1 \subset \mathfrak{a}_1.$$

Обратно, точно так же оказывается, что $\mathfrak{a}_1$ должно содержаться в $\mathfrak{c}_i$:

$$\mathfrak{c}_1 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{c}_i;$$

отсюда следует, что $i = 1$ и $\mathfrak{c}_1 = \mathfrak{a}_1$. Итак, любое $\mathfrak{c}_i$ равно некоторому $\mathfrak{a}_i$.

Мы увидим, что в случае одностороннего разложения эта однозначность не сохраняется.

Для *коммутативного* кольца всякий идеал является двусторонним. Отсюда из основной теоремы § 115 в связи с леммой 5 следует, что полупростое коммутативное кольцо $\mathfrak{o}$ равно сумме простых колец с единицей эти простые кольца взаимно уничтожаются. Но простое коммутативное кольцо с единицей образует поле, так как кратности ax элемента $a \neq 0$ образуют идеал, отличный от (0), т. е. все кольцо. Итак (теорема Дедекинда): *Коммутативное кольцо без радикала с условием минимальности равно прямой сумме коммутативных полей, которые взаимно уничтожаются.*

Сходное разложение получается для коммутативного кольца с радикалом и единицей. Оказывается, что такое кольцо равно прямой сумме примарных колец. Доказательство проводится следующим образом: постулируя условия максимальности и минимальности, разлагаем нулевой идеал согласно § 86 на единообразные примарные идеалы (см. § 113, задача 3) и отсюда согласно § 85 (см. конец) выводим разложение $\mathfrak{o}$ на сумму слагаемых.

Под *центром* кольца $\mathfrak{o}$ мы разумеем совокупность элементов a кольца $\mathfrak{o}$, которые перестановочны со всеми элементами $\mathfrak{o}$:

$$ax = xa \quad \text{для всех } x.$$

Центр образует подкольцо, так как из $ax = xa$ и $bx = xb$ следует:

$$(a - b)x = ax - bx = xa - xb = x(a - b)$$

и

$$(ab)x = axb = x(ab).$$

Если $\mathfrak{o}$ обладает еще оперативной областью в смысле § 113, то центр $\mathfrak{Z}$ является допустимым подкольцом, так как если a — какой-нибудь элемент центра, то для всех операторов λ и всех x имеет место

$$(\lambda a)x = \lambda(ax) = \lambda(xa) = x(\lambda a),$$

в силу чего λa также принадлежит центру.

Очевидно, что центр есть коммутативное подкольцо. Возможная единица кольца всегда принадлежит центру.

Если $\mathfrak{o}$ есть кольцо без радикала, то $\mathfrak{Z}$ есть тоже кольцо без радикала.

Доказательство. Пусть радикал кольца $\mathfrak{Z}$ отличен от (0); тогда в кольце $\mathfrak{Z}$ существует такой идеал $\mathfrak{c} \neq (0)$, что $\mathfrak{c}^2 = (0)$. Идеал $\mathfrak{c}$ порождает в $\mathfrak{o}$ левый идеал $\mathfrak{b} = (\mathfrak{c}, \mathfrak{o}\mathfrak{c})$, а так как $\mathfrak{c}$ перестановочно с $\mathfrak{o}$, то

$$\mathfrak{b}^2 = (\mathfrak{c}, \mathfrak{o}\mathfrak{c})^2 = (\mathfrak{c}^2, \mathfrak{c}\mathfrak{o}\mathfrak{c}, \mathfrak{o}\mathfrak{c}^2, \mathfrak{o}\mathfrak{c}\mathfrak{o}\mathfrak{c}) = (\mathfrak{c}^2, \mathfrak{o}\mathfrak{c}^2, \mathfrak{o}^2\mathfrak{c}^2) = (0);$$

следовательно, в $\mathfrak{o}$ существует нильпотентный идеал $\mathfrak{b} \neq (0)$, что противоречит предположению.

Если $\mathfrak{o}$ есть прямая сумма двусторонних идеалов:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n, \tag{1}$$

то центр $\mathfrak{Z}$ кольца $\mathfrak{o}$ равен прямой сумме центров $\mathfrak{Z}_i$ колец $\mathfrak{a}_i$:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \ldots + \mathfrak{Z}_n.$$

Доказательство. Прежде всего центры $\mathfrak{Z}_i$ колец $\mathfrak{a}_i$ содержатся в $\mathfrak{Z}$. В самом деле, если $\mathfrak{a}_i$ принадлежит $\mathfrak{Z}_i$, то для произвольного

$$x = x_1 + \ldots + x_n \qquad (x_j \in \mathfrak{a}_j)$$

из $\mathfrak{o}$ имеем:

$$a_i x = a_i x_i = x_i a_i = x a_i;$$

все произведения $a_i x_k$ и $x_k a_i$ при $i \neq k$ равны нулю.

Затем любой элемент a из $\mathfrak{Z}$ согласно (1) допускает разложение

$$a = a_1 + \ldots + a_n \qquad (a \in \mathfrak{a}_j),$$

и для произвольного x_i из $\mathfrak{a}_i$ имеет место

$$a_i x_i = a x_i = x_i a = x_i a_i;$$

в силу этого a_i содержится в $\mathfrak{Z}_i$. Таким образом $\mathfrak{Z}$ равно сумме колец $\mathfrak{Z}_i$, причем $\mathfrak{Z}_i$ взаимно уничтожаются. Из $0 = a_1 + \ldots + a_n$ $(a_i \in \mathfrak{Z}_i)$ следует, что $a_i = 0$, так как сумма (1) прямая; следовательно, и сумма $\mathfrak{Z}_i$ тоже прямая.

Задачи. 1. Если $\mathfrak{Z} = \mathfrak{Z}_1 + \ldots + \mathfrak{Z}_n$ — разложение центра $\mathfrak{Z}$ кольца $\mathfrak{o}$ с единицей, и

$$\mathfrak{a}_i = \mathfrak{o}\mathfrak{Z}_i,$$

то $\mathfrak{a}_i$ — двусторонние идеалы $\mathfrak{o}$ и

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n,$$

причём $\mathfrak{Z}_i = \mathfrak{a}_i \cap \mathfrak{Z}$ есть центр кольца $\mathfrak{a}_i$.

2. Если в (1) идеалы $\mathfrak{a}_\nu$ неразложимы в прямые суммы, то $\mathfrak{Z}_\nu$ также неразложимы в прямые суммы.

3. Центр $\mathfrak{Z}$ гиперкомплексной системы $\mathfrak{o}$ образует снова гиперкомплексную систему; если $\mathfrak{o}$ — система без радикала, то $\mathfrak{Z}$ — прямая сумма полей.

4. Если $\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n$ — двустороннее разложение кольца с единицей, то всякий минимальный левый идеал $\mathfrak{o}$ содержится в одном из $\mathfrak{a}_\nu$.

5. Центр группового кольца группы $\mathfrak{G}$ состоит из сумм

$$\sum \lambda_\nu a_\nu,$$

причем элементы a_ν из одного класса сопряженных элементов $\mathfrak{G}$ имеют одни и те же коэфициенты λ_ν. В $\mathfrak{o}$ существует столько линейно независимых центральных элементов, сколько существует классов в $\mathfrak{G}$.

§ 117. КОЛЬЦО АВТОМОРФИЗМОВ ВПОЛНЕ ПРИВОДИМОГО МОДУЛЯ

В § 115 мы видели, что полупростое кольцо, рассматриваемое как левый $\mathfrak{o}$-модуль, вполне приводимо. Здесь мы займемся определением кольца автоморфизмов этого вполне приводимого модуля.

Итак, пусть $\mathfrak{M}$ будет вполне приводимый модуль с некоторой мультипликаторной областью. Под „автоморфизмами“ $\mathfrak{M}$ в этом параграфе мы разумеем все операторные гомоморфизмы модуля $\mathfrak{M}$ на самого себя, а не только 1-изоморфизмы $\mathfrak{M}$ на самого себя. В силу § 38 такие автоморфизмы образуют кольцо; надо исследовать структуру этого кольца автоморфизмов.

Пусть в частности рассматриваемый модуль $\mathfrak{M}$ есть модуль линейных форм относительно поля K (элементы K будут записываться в виде правых операторов), и пусть $\mathfrak{M}$ сверх того обладает левыми операторами $A, B, \ldots$, удовлетворяющими условию $(Am)\varkappa = A(m\varkappa)$. Очевидно, что левые операторы порождают линейные преобразования модуля линейных форм (см. § 104). Автоморфизмы этого двойного модуля будут опять-таки линейными преобразованиями Θ, перестановочными с $A, B, \ldots$:

$$\Theta(Am) = A(\Theta m)$$

(более общий случай подобного рода см. в задаче 1).

Рассмотрим сперва гомоморфные отображения простого модуля $\mathfrak{M}_1$. Подмодуль элементов, отображающихся на нуль, либо равен всему $\mathfrak{M}_1$, либо состоит только из нуля. В последнем случае отображение будет 1-изоморфизмом. Итак, *при всяком гомоморфизме простой модуль* $\mathfrak{M}_1$ *отображается либо на нуль, либо отображение представляет* 1-*изоморфизм.*

Если $\mathfrak{M}_1$ отображается на себя и отображение не является нулевым оператором (отображающим $\mathfrak{M}_1$ на нуль), то отображение 1-изоморфно и переводит $\mathfrak{M}_1$ в подмодуль, отличный от нуля, т. е. в $\mathfrak{M}_1$. Для такого 1-автоморфизма всегда существует обратный автоморфизм, т. е. *кольцо автоморфизмов простого модуля образует поле.*

Подобным же образом получается, что *если* $\mathfrak{M}_1$ *гомоморфно отображается на другой простой модуль* $\mathfrak{M}_2$ *и отображение не является нулевым оператором, то отображение должно быть* 1-*изоморфизмом, т. е.* $\mathfrak{M}_1 \backsimeq \mathfrak{M}_2$.

Теперь мы в состоянии определить автоморфизмы модуля

$$\mathfrak{M} = \mathfrak{M}_1 + \ldots + \mathfrak{M}_r,$$

где $\mathfrak{M}_i$ — простые модули. Прежде всего заметим, что если элемент m разложен на свои компоненты:

$$m = m_1 + \ldots + m_r, \tag{1}$$

то любое из соответствий $m \to m_\nu$ представляет гомоморфизм. Обозначим эти соответствия через H_ν. Вместо (1) можно теперь написать:

$$m = \sum_\nu H_\nu m. \tag{2}$$

Чтобы судить о произвольном автоморфизме Θ, достаточно судить о его влиянии на компоненты $m_\nu = H_\nu m$, так как

$$\Theta m = \sum_\nu \Theta m_\nu. \tag{3}$$

Разложим элементы Θm_ν на компоненты:

$$\Theta m_\nu = \sum_\mu H_\mu \Theta m_\nu. \tag{4}$$

Оператор $H_\mu \Theta$, примененный к элементу m_ν модуля $\mathfrak{M}_\nu$, определяет гомоморфизм, отображающий $\mathfrak{M}_\nu$ на $\mathfrak{M}_\mu$. Обозначим этот гомоморфизм

через $\Theta_{\mu\nu}$. r^2 гомоморфизмов $\Theta_{\mu\nu}$ можно расположить в виде квадратной матрицы. Если $\mathfrak{M}_\nu$ не изоморфно $\mathfrak{M}_\mu$, от $\Theta_{\mu\nu}$ необходимо должно быть нулевым оператором. Вместо (4) теперь мы пишем:

$$\Theta m_\nu = \sum_\mu \Theta_{\mu\nu} m_\nu. \tag{5}$$

Если подставить (5) в (3), то получится:

$$\Theta m = \sum_\mu \sum_\nu \Theta_{\mu\nu} m_\nu = \sum_\mu \sum_\nu \Theta_{\mu\nu} H_\nu m, \tag{6}$$

или

$$\Theta = \sum_\mu \sum_\nu \Theta_{\mu\nu} H_\nu. \tag{7}$$

Так как, обратно, из (6) или (7) можно вывести (5), положив $m = m_\nu$, и так как (5) однозначно определяет гомоморфизм $\Theta_{\mu\nu}$, то отсюда следует, что всякий гомоморфизм представляется однозначно в виде (7).

Если η — второй гомоморфизм:

$$\eta = \sum_\mu \sum_\nu \eta_{\mu\nu} H_\nu,$$

то сумма и произведение η и Θ вычисляются следующим образом:

$$\eta + \Theta = \sum_\mu \sum_\nu (\eta_{\mu\nu} + \Theta_{\mu\nu}) H_\nu,$$

$$\eta\Theta = \sum_\lambda \sum_\mu \eta_{\lambda\mu} H_\mu \sum_{\mu'} \sum_\nu \Theta_{\mu'\nu} H_\nu =$$

$$= \sum_\lambda \sum_\mu \eta_{\lambda\mu} \sum_\nu \Theta_{\mu\nu} H_\nu \text{ [1]} =$$

$$= \sum_\lambda \sum_\nu \left(\sum_\mu \eta_{\lambda\mu} \Theta_{\mu\nu} \right) H_\nu.$$

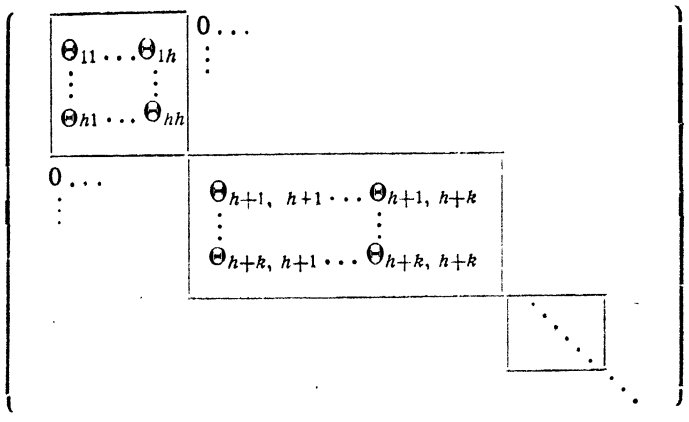
Итак, всякому Θ *соответствует матрица* $(\Theta_{\mu\nu})$, *а сумме и произведению соответствует сумма и произведение матриц. Элементы* $\Theta_{\mu\nu}$ *матрицы равны нулю, если индексы* μ *и* ν *принадлежат не изоморфным модулям* $\mathfrak{M}_\mu$ *и* $\mathfrak{M}_\nu$; $\Theta_{\mu\nu}$ *представляет гомоморфизм между* $\mathfrak{M}_\nu$ *и* $\mathfrak{M}_\mu$, *если* $\mathfrak{M}_\mu$ *и* $\mathfrak{M}_\nu$ *изоморфны.*

Объединим теперь модули $\mathfrak{M}_\lambda$ в классы изоморфных модулей и занумеруем их так, чтобы, например, $\mathfrak{M}_1, \ldots, \mathfrak{M}_h$, затем $\mathfrak{M}_{h+1}, \ldots, \mathfrak{M}_{h+k}$ и т. д. были между собой изоморфны; тогда матрицы $(\Theta_{\mu\nu})$ распадутся

---

[1]) Для $\mu \neq \mu'$ имеет место $H_\mu \Theta_{\mu'\nu} = 0$, так как любой элемент $\mathfrak{M}_{\mu'}$ уничтожается гомоморфизмом H_μ. Напротив, для $\mu = \mu'$ имеет место $H_\mu \Theta_{\mu'\nu} = \Theta_{\mu\nu}$, так как элементы $\mathfrak{M}_\mu$ инвариантны относительно H_μ.

на квадратные „клеточки", состоящие из h, k, ... строк и столбцов, так, что вне „клеточек" будут стоять только нули:



Если вписать в первую клеточку произвольные элементы, а в остальные — нули, то получится кольцо матриц $\mathfrak{A}_1$, которое образует подкольцо первоначального кольца матриц $\mathfrak{A}$; точно так же, если вписывать всюду, кроме второй клеточки, нули, то получится кольцо $\mathfrak{A}_2 \subseteq \mathfrak{A}$ и т. д. Ясно, что любой элемент $\mathfrak{A}$ равен сумме элементов из $\mathfrak{A}_1$, $\mathfrak{A}_2$, ..., и что элементы $\mathfrak{A}_1$, $\mathfrak{A}_2$, ... друг друга уничтожают. Но это означает, что *кольцо $\mathfrak{A}$ есть прямая сумма взаимно уничтожающих колец* $\mathfrak{A}_1$, $\mathfrak{A}_2$, ...

Чтобы выявить структуру кольца $\mathfrak{A}$, достаточно рассмотреть отдельные $\mathfrak{A}_\lambda$, например $\mathfrak{A}_1$. Элементам $\mathfrak{A}_1$ соответствуют квадратные матрицы h-го порядка

$$\begin{pmatrix} \Theta_{11} \dots \Theta_{1h} \\ \vdots \\ \Theta_{h1} \dots \Theta_{hh} \end{pmatrix},$$

находящиеся в первой „клеточке".

Θ_{11} есть элемент поля автоморфизмов $\mathfrak{K}_1$ модуля $\mathfrak{M}_1$. Остальные элементы $\Theta_{\mu\nu}$ не принадлежат этому полю, а представляют гомоморфизмы между $\mathfrak{M}_\nu$ и $\mathfrak{M}_\mu$. Однако мы их можем однозначно отобразить на элементы $\mathfrak{K}_1$, взяв 1-изоморфизмы Γ_1, ..., Γ_h, отображающие $\mathfrak{M}_1$, ..., $\mathfrak{M}_h$ на $\mathfrak{M}_1$. В качестве Γ_1 мы примем тождественный автоморфизм. Если теперь мы любому $\Theta_{\mu\nu}$ сопоставим соответствующий элемент

$$\Theta'_{\mu\nu} = \Gamma_\mu \Theta_{\mu\nu} \Gamma_\nu^{-1}, \tag{8}$$

принадлежащий $\mathfrak{K}_1$ (ибо Γ_ν^{-1} отображает $\mathfrak{M}_1$ на $\mathfrak{M}_\nu$, $\Theta_{\mu\nu}$ отображает $\mathfrak{M}_\nu$ на $\mathfrak{M}_\mu$ и Γ_μ отображает $\mathfrak{M}_\mu$ снова на $\mathfrak{M}_1$), то, очевидно, сумме $\eta_{\mu\nu} + \Theta_{\mu\nu}$ соответствует сумма $\eta'_{\mu\nu} + \Theta'_{\mu\nu}$, а произведению $\eta_{\lambda\mu}\Theta_{\mu\nu}$, поскольку оно имеет смысл [1]), соответствует также произведение

$$\eta'_{\lambda\mu}\Theta'_{\mu\nu} = \Gamma_\lambda \eta_{\lambda\mu} \Gamma_\mu^{-1} \Gamma_\mu \Theta_{\mu\nu} \Gamma_\nu^{-1} = \Gamma_\lambda (\eta_{\lambda\mu}\Theta_{\mu\nu}) \Gamma_\nu^{-1}.$$

[1]) Произведение $\eta_{\lambda\mu}\Theta_{\mu'\nu}$ только тогда имеет смысл, когда $\mu = \mu'$, так как $\Theta_{\mu'\nu}$ отображает $\mathfrak{M}_\nu$ на $\mathfrak{M}_{\mu'}$ и если произведение имеет смысл, то $\eta_{\lambda\mu}$ должно отображать $\mathfrak{M}_{\mu'}$ на какой-то модуль.

Таким образом всякой матрице $(\Theta_{\mu\nu})$ будет соответствовать взаимно однозначно матрица $(\Theta'_{\mu\nu})$ с элементами из K_1 и сумме и произведению матриц

$$\left.\begin{aligned}\sigma_{\mu\nu} &= \eta_{\mu\nu} + \Theta_{\mu\nu},\\ \pi_{\lambda\nu} &= \sum \eta_{\lambda\mu}\Theta_{\mu\nu}\end{aligned}\right\}$$

будут соответствовать также сумма и произведение матриц. Очевидно, что *любой* элемент K_1 при заданных μ, ν и Γ_μ, Γ_ν может быть записан в виде $\Theta'_{\mu\nu}$ в смысле (8). Отсюда следует, что $\mathfrak{A}_1$ *изоморфно кольцу всех квадратных матриц h-го порядка с элементами из поля* K_1, *поля автоморфизмов простого модуля* $\mathfrak{M}_1$.

Задачи. 1. Если дана вполне приводимая система матриц

$$A = \begin{pmatrix} \boxed{\begin{matrix} A_1 & & \\ & A_1 & \\ & & \ddots \\ & & & A_1 \end{matrix}} & & \\ & \boxed{\begin{matrix} A_2 & & \\ & A_2 & \\ & & \ddots \\ & & & A_2 \end{matrix}} & \\ & & \ddots \end{pmatrix},$$

где матрица A_1 первой клеточки пробегает h эквивалентных друг другу неприводимых систем; точно так же A_2 во второй клеточке пробегает k эквивалентных систем, которые, однако, не эквивалентны системе A_1, и т. д., то мы имеем систему перестановочных матриц вида:

$$T = \begin{pmatrix} \boxed{\begin{matrix} T_{11} \dots T_{1h} \\ \vdots \quad \vdots \\ T_{h1} \dots T_{hh} \end{matrix}} & & \\ & \boxed{\begin{matrix} T_{h+1,\,h+1} \dots T_{h+1,\,h+k} \\ \vdots \quad \vdots \\ T_{h+k,\,h+1} \dots T_{h+k,\,h+k} \end{matrix}} & \\ & & \ddots \end{pmatrix},$$

где матрицы T_{ik} первой клеточки перестановочны с системой A_1, T_{ik} второй клеточки перестановочны с системой A_2 и т. д. Матрицы T_{11}, перестановочные с неприводимой системой A_1, образуют поле конечной степени относительно основного поля K.

2. Если основное поле K алгебраически замкнуто, то матрицы T_{11} задачи 1, перестановочные с неприводимой системой матриц, могут быть равны только кратным λE единичной матрицы E.

§ 118. СТРУКТУРА ВПОЛНЕ ПРИВОДИМОГО КОЛЬЦА С ЕДИНИЦЕЙ

Пусть $\mathfrak{o}$ — полупростое кольцо или, что в силу § 115 одно и то же, вполне приводимое слева кольцо с единицей. Как модуль (причем само $\mathfrak{o}$ можно рассматривать как левую мультипликаторную область) $\mathfrak{o}$ равно прямой сумме простых модулей (левых идеалов):

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \ldots + \mathfrak{l}_r.$$

Построим теперь кольцо автоморфизмов этого модуля. Если Γ есть операторный автоморфизм, переводящий единицу в элемент c:

$$\Gamma 1 = c,$$

то Γ переводит произвольный элемент a в

$$\Gamma a = \Gamma(a \cdot 1) = a \cdot \Gamma 1 = ac.$$

С другой стороны, если c есть произвольный элемент и всякое a кольца $\mathfrak{o}$ переводится в ac, то соответствие будет операторным гомоморфизмом в силу

$$(a+b)c = ac + bc,$$
$$(ab)c = a(bc).$$

Таким образом каждому элементу c взаимно однозначно соответствует автоморфизм Γ. Сумме $c+d$ соответствует сумма $\Gamma + \Delta$; но произведение cd соответствует обратное произведение $\Delta\Gamma$, так как

$$a(cd) = (ac)d = \Delta(ac) = \Delta\Gamma a.$$

Два кольца $\mathfrak{o}$ и $\mathfrak{o}'$, которые отображаются взаимно однозначно друг на друга так, что сумме $a+b$ соответствует сумма $a'+b'$, произведению $a \cdot b$ — обратное произведение $b' \cdot a'$, мы назовем *обратно-изоморфными*. Таким образом мы видим, что кольцо $\mathfrak{o}$ обратно-изоморфно своему кольцу автоморфизмов.

С другой стороны, согласно § 117 кольцо автоморфизмов вполне приводимого модуля изоморфно прямой сумме взаимно уничтожающихся колец матриц, причем элементы матриц всякий раз берутся из некоторого поля (поля автоморфизмов простого модуля).

Таким образом кольцо $\mathfrak{o}$ обратно-изоморфно прямой сумме колец матриц, которые взаимно уничтожаются.

Для всякого кольца можно построить однозначно с точностью до изоморфизма колец обратное кольцо, приводя в соответствие элементу кольца a новый символ a' и определив сумму и произведение с помощью равенств $a'+b' = (a+b)'$, $a'b' = (b \cdot a)'$. Кольцо, обратное полю, очевидно, также является полем. Построим для кольца матриц поля K обратное кольцо; для этого надо построить поле K', обратное K, и матрицу $(a'_{\lambda\mu})$ перевести в транспонированную матрицу $(a'_{\mu\lambda})$. Наконец, кольцо, обратное прямой сумме колец, также равно прямой сумме колец, которые обратно-изоморфны слагаемым. Из всего этого получается следующая теорема:

Кольцо $\mathfrak{o}$ *равно прямой сумме колец* $\mathfrak{a}_\nu$, *каждое из которых изоморфно полному кольцу матриц относительно поля* $\mathsf{K}^{(\nu)}$, *причем эти* $\mathfrak{a}_\nu$ *друг друга уничтожают. Существует столько* $\mathfrak{a}_\nu$, *сколько имеется не изоморфных левых идеалов* $\mathfrak{l}_\nu$ *в прямой сумме.*

Тем самым структура полупростого кольца полностью выяснена.

Если $\mathfrak{a}_\nu$ взаимно уничтожаются, то $\mathfrak{a}_\nu$ суть идеалы из $\mathfrak{o}$. Если кольцо $\mathfrak{o}$ двусторонне простое, то существует только одно $\mathfrak{a}_\nu$, равное $\mathfrak{a}_1$. Итак:

Вполне приводимое слева двусторонне простое кольцо с единицей изоморфно полному кольцу матриц относительно некоторого поля. Все минимальные левые идеалы операторно-изоморфны.

Обратное также справедливо. А именно:

Кольцо $\mathfrak{o}$ *матриц* n*-го порядка относительно поля* K *является (двусторонне) простым и вполне приводимым слева, а кольцо автоморфизмов минимальных левых идеалов кольца* $\mathfrak{o}$ *обратно-изоморфно* K.

Доказательство. Пусть $c_{11}, \ldots, c_{1n}, \ldots, c_{n1}, \ldots, c_{nn}$ — элементы базиса кольца матриц (§ 112, а). Пусть затем $\mathfrak{a} \neq (0)$ — двусторонний идеал и

$$a = \sum \gamma_{ik} c_{ik}$$

элемент идеала $\mathfrak{a}$, отличный от нуля. Один из коэфициентов γ_{ik} должен быть отличен от нуля; пусть, например, $\gamma_{23} \neq 0$. Тогда к $\mathfrak{a}$ принадлежит также (для всех λ и μ) элемент

$$\gamma_{23}^{-1} c_{\lambda 2}\, a c_{3\mu} = \gamma_{23}^{-1} \sum_{i,k} \gamma_{ik} c_{\lambda 2} c_{ik} c_{3\mu} =$$
$$= \gamma_{23}^{-1} \gamma_{23} c_{\lambda 2} c_{23} c_{3\mu} = c_{\lambda\mu},$$

т. е. $\mathfrak{a}$ содержит все элементы базиса $\mathfrak{o}$. Следовательно, $\mathfrak{a} = \mathfrak{o}$. Таким образом $\mathfrak{o}$ есть простое кольцо с единицей.

K-модуль $\mathfrak{l} = (c_{11}, c_{21}, \ldots, c_{n1})$, как легко видеть, образует минимальный левый идеал $\mathfrak{o}$. В самом деле, прежде всего произведение $c_{ik} c_{l1}$ любого элемента базиса c_{ik} кольца $\mathfrak{o}$ на любой элемент базиса c_{l1} модуля $\mathfrak{l}$ либо равно нулю, либо равно c_{i1}, т. е. является также элементом модуля $\mathfrak{l}$. Минимальность $\mathfrak{l}$ следует из того, что произвольный элемент $\alpha \neq 0$ идеала $\mathfrak{l}$ всегда порождает весь идеал $\mathfrak{l}$. Именно, если

$$a = \sum \alpha_k c_{k1}$$

и, например, $\alpha_2 \neq 0$, то

$$\alpha_2^{-1} c_{j2} a = \alpha_2^{-1} \alpha_2 c_{j2} c_{21} = c_{j1} \qquad (j = 1, \ldots, n)$$

также принадлежит левым кратным a.

Точно так же можно убедиться, что вообще $\mathfrak{l}_\nu = (c_{1\nu}, c_{2\nu}, \ldots, c_{n\nu})$ образует простой левый идеал кольца $\mathfrak{o}$. Так как $\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \ldots + \mathfrak{l}_n$, то $\mathfrak{o}$ слева вполне приводимо.

Наконец, найдем поле автоморфизмов $\mathfrak{l}$. Операторный автоморфизм, переводящий, например, c_{11} в

$$a = \sum \alpha_k c_{k1}, \qquad (1)$$

должен переводить любое $x \cdot c_{11}$ в $x \cdot a$; в частности c_{11}^2 ($c_{11}^2 = c_{11}$) переводится в

$$c_{11} a = \sum \alpha_k c_{11} c_{k1} = \alpha_1 c_{11},$$

причем должен получиться снова элемент a. Таким образом в (1) отпадают все члены, кроме $\alpha_1 c_{11}$, и автоморфизм переводит $x \cdot c_{11}$ в $x \cdot (\alpha_1 c_{11}) = (x c_{11}) \cdot \alpha_1$. Итак, автоморфизм состоит в том, что элементы $\mathfrak{l}$ (все они имеют вид $x c_{11}$) умножаются просто справа на α_1. Элементы поля α_1 связаны обратно-изоморфно с соответствующими автоморфизмами; таким образом поле автоморфизмов минимального левого идеала обратно-изоморфно K.

Подобным же образом можно показать, что полное кольцо матриц относительно поля K также вполне приводимо справа. Поле автоморфизмов минимального правого идеала будет прямо-изоморфно K. Далее в соединении с теоремами § 116 следует, что прямая сумма взаимно уничтожающихся колец матриц также вполне приводима (слева и справа). Таким образом совершенно равносильны следующие понятия:

a) кольцо без радикала с условием минимальности для левых (или правых) идеалов;

b) вполне приводимое слева или справа кольцо с единицей;

c) прямая сумма двусторонне простых идеалов, каждый из которых изоморфен (как кольцо) с полным кольцом матриц.

Отныне мы будем обозначать кольцо матриц n-го порядка поля K через K_n, единичную матрицу через E. Мы утверждаем, что *если* Z — *центр поля* K, *то* $Z \cdot E$ *есть центр кольца* K_n.

Доказательство. Если матрица

$$a = (\alpha_{ik}) = \sum \alpha_{ik} c_{ik}$$

принадлежит центру кольца K_n, то она должна быть перестановочна с $c_{1\mu}$; отсюда

$$c_{1\mu} \sum_{i,k} \alpha_{ik} c_{ik} = \left(\sum_{i,k} \alpha_{ik} c_{ik} \right) \cdot c_{1\mu},$$

$$\sum_k \alpha_{\mu k} c_{1k} = \sum_i \alpha_{i1} c_{i\mu}.$$

Сравнивая коэфициенты слева и справа, получим:

$$\alpha_{\mu k} = 0 \quad \text{для } \mu \neq k,$$

$$\alpha_{\mu\mu} = \alpha_{11},$$

откуда

$$a = \begin{pmatrix} \alpha_{11} & & 0 \\ & \alpha_{11} & \\ & & \ddots \\ 0 & & \alpha_{11} \end{pmatrix} = \alpha_{11} \cdot E = \alpha \cdot E,$$

Чтобы $a = \alpha \cdot E$ было перестановочно со всяким $\beta \cdot E$, необходимо, чтобы α принадлежало центру поля K, что и требовалось показать.

Увязывая этот результат с результатами § 116 и замечая, что центры двух обратно-изоморфных колец, очевидно, изоморфны в обычном смысле, получим:

Центр полупростого кольца $\mathfrak{o}$ *равен прямой сумме полей, которые содержатся в каждом из двусторонних компонентов; эти поля представляются в виде* $Z \cdot E$, *где* Z — *центр поля автоморфизмов.*

Задачи. 1. Полупростая гиперкомплексная система $\mathfrak{o}$ относительно алгебраически замкнутого поля Ω равна прямой сумме колец матриц Ω.

2. Кольцо кватернионов $(1, j, k, l)$ относительно поля P с характеристикой, отличной от 2, является двусторонне простым и потому либо образует поле, либо изоморфно кольцу всех матриц второго порядка поля P.

§ 119. ПРОИЗВЕДЕНИЕ ГИПЕРКОМПЛЕКСНЫХ СИСТЕМ. РАСШИРЕНИЕ ОСНОВНОГО ПОЛЯ

Пусть $\mathfrak{o}_1 = (b_1, \ldots, b_n)$ и $\mathfrak{o}_2 = (c_1, \ldots, c_m)$ — две гиперкомплексные системы относительно основного поля P. Под *произведением* $\mathfrak{o}_1 \times \mathfrak{o}_2$ подразумевается система:

$$\mathfrak{o}_1 \times \mathfrak{o}_2 = (b_1 c_1, \ldots, b_\nu c_\mu, \ldots, b_n c_m),$$

где b_ν перестановочны с c_μ, т. е. умножение определяется равенством:

$$(b_\lambda c_\mu)(b_\rho c_\sigma) = (b_\lambda b_\rho)(c_\mu c_\sigma).$$

Таким образом элементы системы произведения представляются в виде сумм

$$\sum\sum \alpha_{\lambda\mu} b_\lambda c_\mu.$$

Эти суммы можно также записать либо в виде

$$\sum b'_\mu c_\mu,$$

где b'_μ — элементы кольца $\mathfrak{o}_1$, либо в виде

$$\sum b_\lambda c'_\lambda,$$

где c'_λ — элементы кольца $\mathfrak{o}_2$. Первая из приведенных записей показывает, что произведение систем не зависит от выбора базиса кольца $\mathfrak{o}_1$; вторая запись показывает независимость произведения от базиса кольца $\mathfrak{o}_2$.

Легко видеть, что

$$\mathfrak{o}_1 \times \mathfrak{o}_2 = \mathfrak{o}_2 \times \mathfrak{o}_1,$$

$$\mathfrak{o}_1 \times (\mathfrak{o}_2 \times \mathfrak{o}_3) = (\mathfrak{o}_1 \times \mathfrak{o}_2) \times \mathfrak{o}_3.$$

Достойно внимания произведение системы $\mathfrak{o}$ на коммутативное поле Λ конечной степени относительно P; элементы этого произведения записываются в виде:

$$\lambda_1 b_1 + \ldots + \lambda_n b_n = b_1 \lambda_1 + \ldots + b_n \lambda_n \quad (\lambda_i \in \Lambda),$$

если $\mathfrak{o} = (b_1, \ldots, b_n)$, т. е. произведение $\Lambda \times \mathfrak{o}$ образует гиперкомплексную систему с теми же элементами базиса, что и $\mathfrak{o}$, но основным полем

будет уже не P, а Δ. Обозначим такую систему $\Delta \times \mathfrak{o}$ через $\mathfrak{o}_\Delta$. Тот же самый символ $\mathfrak{o}_\Delta$ можно распространить и на случай бесконечного поля Δ расширения над P. Наконец, мы будем пользоваться вместо $\Delta \times \mathfrak{o}$ в случае надобности символом $\mathfrak{o}_\Delta$ и тогда, когда Δ — гиперкомплексная система относительно P.

При таком расширении основного поля могут утратиться существенные свойства системы $\mathfrak{o}$; например, поле кватернионов $(1, j, k, l)$ при расширении рационального числового поля Γ до $\Gamma(i)$ не только перестает быть полем, но и приобретает делителей нуля:

$$j^2 + 1 = j^2 - i^2 = (j - i)(j + i) = 0,$$

причем система кватернионов относительно $\Gamma(i)$ будет изоморфна системе матриц с элементами базиса

$$c_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad c_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad c_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad c_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

причем изоморфизм осуществляется при помощи следующего соответствия:

$$1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = c_{11} + c_{22},$$

$$j \to \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i(c_{11} - c_{22}),$$

$$k \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = c_{12} - c_{21},$$

$$l \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = i(c_{12} + c_{21}).$$

Пусть $\mathfrak{S}$ — простая гиперкомплексная система. Что можно сказать относительно структуры $\mathfrak{S}_\Sigma$?

Мы начнем со случая, когда $\mathfrak{S}$ и Σ — *коммутативные поля.*

Если $\mathfrak{S}$ — конечное коммутативное поле расширения P первого рода, то $\mathfrak{S}_\Sigma$ не имеет радикала, каково бы ни было (коммутативное) поле Σ расширения P; если же $\mathfrak{S}$ второго рода, то $\mathfrak{S}_\Sigma$ при соответствующем Σ обладает радикалом.

Доказательство. Если $\mathfrak{S}$ — поле первого рода, Θ — примитивный элемент $\mathfrak{S}$ (§ 34), $\varphi(z)$ — неприводимый полином с корнем Θ и n — степень полинома $\varphi(z)$, то

$$\mathfrak{S} = \mathsf{P}(\Theta) = \mathsf{P} + \mathsf{P}\Theta + \ldots + \mathsf{P}\Theta^{n-1} \cong \frac{\mathsf{P}[z]}{(\varphi(z))},$$

а потому после расширения основного поля

$$\mathfrak{S}_\Sigma = \Sigma + \Sigma\Theta + \ldots + \Sigma\Theta^{n-1} \cong \frac{\Sigma[z]}{(\varphi(z))}.$$

Так как $\varphi(z)$ в $\Sigma[z]$ также не имеет кратных множителей, то степень полинома $f(z)$, $f(z) \not\equiv 0 (\varphi(z))$ не может быть сравнима с нулем по $\varphi(z)$, т. е. в $\frac{\Sigma[z]}{(\varphi(z))}$,

кроме нуля, не существует нильпотентных элементов. Следовательно, $\mathfrak{S}_\Sigma$ есть кольцо без радикала [1]).

Если же $\mathfrak{S}$ — поле второго рода и Θ элемент $\mathfrak{S}$ второго рода, то $\mathfrak{S}$ содержит подполе $P(\Theta)$, а $\mathfrak{S}_\Sigma$ — подкольцо $\Sigma(\Theta) \cong \frac{\Sigma[z]}{(\varphi(z))}$. При соответствующем выборе поля Σ полином $\varphi(z)$ будет иметь кратные корни в Σ, и потому в $\Sigma[z]$ будет существовать полином $f(z) \not\equiv 0\ (\varphi(z))$, степень которого сравнима с нулем по $\varphi(z)$. Следовательно, в $\frac{\Sigma[z]}{(\varphi(z))}$ существует нильпотентный элемент, отличный от нуля; в силу этого и в $\Sigma(\Theta)$ существует элемент подобного рода, который порождает нильпотентный идеал в $\mathfrak{S}_\Sigma$ (в самом деле, в коммутативном кольце $\mathfrak{o}$ всякий нильпотентный элемент r порождает нильпотентный идеал $r\mathfrak{o}$). Теорема доказана полностью.

Теперь переходим к случаю, когда $\mathfrak{S}$ — не коммутативное поле. В этом случае справедлива следующая лемма:

Если $\mathfrak{S}$ — поле конечного ранга относительно P с центром $Z \supseteq P$, и Σ — гиперкомплексная система с единицей относительно P (в частности и конечное поле расширения P) и $\mathfrak{o} = \mathfrak{S}_\Sigma$, $\mathfrak{Z} = Z_\Sigma$, то всякий двусторонний идеал $\mathfrak{a}$ кольца $\mathfrak{o}$ порождается двусторонним идеалом в $\mathfrak{Z}$.

Доказательство. Пусть

$$\Sigma = z_1 P + \ldots + z_q P,$$

откуда

$$\mathfrak{o} = \mathfrak{S}_\Sigma = z_1 \mathfrak{S} + \ldots + z_q \mathfrak{S}.$$

Построим теперь с помощью $z_1, \ldots, z_q$ для произвольного $\mathfrak{S}$-модуля $\mathfrak{a}$ в $\mathfrak{o}$ $\mathfrak{S}$-базис $(l_1, \ldots, l_r)$, нормированный особым образом.

Если $\mathfrak{a} = a_1\mathfrak{S} + \ldots + a_r\mathfrak{S}$ есть $\mathfrak{S}$-модуль ранга r, то согласно § 28 можно $a_1, \ldots, a_r$ присоединением некоторых z_ν, например $z_{r+1}, \ldots, z_q$, дополнить до $\mathfrak{S}$-базиса кольца $\mathfrak{o}$; тогда всякий элемент $\mathfrak{o}$ будет по модулю $\mathfrak{a}$ сравним с линейной формой $z_{r+1}, \ldots, z_q$ с коэфициентами из $\mathfrak{S}$. В частности для $i = 1, \ldots, r$ имеет место

$$z_i \equiv \sum_{k=r+1}^{q} z_k \gamma_{ik} \pmod{\mathfrak{a}}, \qquad \gamma_{ik} \in \mathfrak{S}.$$

Если положить

$$l_i = z_i - \sum_{k=r+1}^{q} z_k \gamma_{ik},$$

то l_i — линейно независимые элементы $\mathfrak{a}$ и потому образуют $\mathfrak{S}$-базис для $\mathfrak{a}$:

$$\mathfrak{a} = l_1\mathfrak{S} + \ldots + l_r\mathfrak{S},$$

Этот базис обладает тем свойством, что для $d \in \mathfrak{a}$ из $d = \sum_1^r l_i \delta_i$ следует:

$$d = \sum_1^r z_i \delta_i + \sum_{r+1}^{q} z_k \varepsilon_k;$$

---

[1]) Еще точнее можно судить о структуре $\mathfrak{S}_\Sigma$ на основании § 85 (см. конец этого параграфа): $\mathfrak{S}_\Sigma$ равна прямой сумме полей $\mathfrak{S}_1, \ldots, \mathfrak{S}_r$, которые соответствуют неприводимым сомножителям $\varphi_1, \ldots, \varphi_r$ полинома $\varphi(z)$ в $\Sigma[z]$; а именно, $\mathfrak{S}_\nu \cong \frac{\Sigma[z]}{(\varphi_\nu(z))}$. Если в частности Σ алгебраически замкнуто, то число полей $\mathfrak{S}_\nu$, на которые распадается $\mathfrak{S}_\Sigma$, равно степени $\varphi(z)$ или рангу $\mathfrak{S}$, и поля $\mathfrak{S}_\nu$ изоморфны Σ.

в последнем выражении при $z_1, \ldots, z_r$ стоят те же коэфициенты, что и при $l_1, \ldots, l_r$ в первом выражении. Два элемента a, у которых в этом выражении совпадают первые r коэфициентов, равны.

Если в частности a есть двусторонний идеал кольца o, то вместе с l_i также

$$\varkappa l_i = z_i\varkappa - \sum_{k=r+1}^{q} z_k \varkappa \gamma_{ik}$$

и

$$l_i\varkappa = z_i\varkappa - \sum_{k=r+1}^{q} z_k \gamma_{ik}\varkappa$$

принадлежат a. Так как коэфициенты при $z_1, \ldots, z_r$ в этих двух выражениях равны, то элементы $\varkappa l_i$ и $l_i\varkappa$ в силу приведенного выше замечания тоже равны. Если сравнить в обоих выражениях коэфициенты при $z_{r+1}, \ldots, z_q$, то получим:

$$\varkappa\gamma_{ik} = \gamma_{ik}\varkappa.$$

Таким образом все γ_{ik} принадлежат центру Z поля $\mathfrak{S}$; отсюда l_i принадлежат $Z_\Sigma = \mathfrak{Z}$. Следовательно, a будет порождаться $\mathfrak{Z}$-идеалом $(l_1, \ldots, l_r)$.

Дополнение. Теорема справедлива и тогда, когда вместо Σ взято бесконечное алгебраическое поле Ω расширения. Именно, если a — двусторонний идеал в $o = \mathfrak{S}_\Omega$, то a, как и o, имеет конечный ранг относительно Ω, т. е. конечный базис. Элементы базиса, выраженные в виде $\sum \omega_i\sigma_i (\omega_i \in \Omega, \sigma_i \in \mathfrak{S})$, содержат лишь конечное число ω_i, порождающих конечное подполе Σ поля Ω. Таким образом a будет порождаться идеалом $\mathfrak{S}_\Sigma$, и потому можно применить предыдущую теорему.

Если центр Z системы $\mathfrak{S}$ есть поле расширения первого рода относительно P, а Σ, как и выше, — (конечное или бесконечное) *коммутативное алгебраическое поле расширения*, то из этой теоремы прежде всего вытекает, что $\mathfrak{S}_\Sigma$ *есть кольцо без радикала.* В самом деле, радикал $\mathfrak{S}_\Sigma$ должен как двусторонний идеал порождаться нильпотентным идеалом в $\mathfrak{Z}$, а $\mathfrak{Z} = Z_\Sigma$ согласно первой теореме этого параграфа не имеет радикала. Но мы можем еще точнее определить структуру кольца $\mathfrak{S}_\Sigma$. Прежде всего легко видеть, что $\mathfrak{Z} = Z_\Sigma$ есть центр кольца $\mathfrak{S}_\Sigma$. Поэтому двустороннее разложение кольца $\mathfrak{S}_\Sigma$ определяется разложением его центра $\mathfrak{Z}$. Так как Z_Σ разлагается самое большее на n полей, где n — ранг Z относительно P, то получается следующий результат:

Число компонентов кольца $\mathfrak{S}_\Sigma$ *равно числу компонентов центра* Z_Σ, *т. е. не превосходит ранга поля* Z *относительно* P. *Если в частности* Z *совпадает с основным полем* $(Z = \mathsf{P})$, *то* $\mathfrak{S}_\Sigma$ *есть двустороннее простое кольцо и потому изоморфно полному кольцу матриц поля* $\mathsf{K} \supseteq Z$.

Если в частности Σ есть алгебраически замкнутое поле Ω относительно P (§ 60), то $\mathsf{K} = \Omega$, в силу чего $\mathfrak{S}_\Omega$ изоморфно полному кольцу матриц (например матриц m-го порядка) поля Ω (§ 118, задача 1). Ранг кольца $\mathfrak{S}_\Omega$ относительно Ω равен m^2; отсюда ранг поля $\mathfrak{S}$ относительно P $(= Z)$ также равен m^2. Таким образом:

Поле $\mathfrak{S}$ *конечного ранга относительно своего центра* Z *всегда имеет рангом полный квадрат* m^2 *и при расширении поля* Z *до алгебраически замкнутого поля* Ω *переходит в кольцо матриц* m*-го порядка.*

Число m называется *индексом* поля $\mathfrak{S}$.

Теорема о том, что все двусторонние идеалы $\mathfrak{S}_\Sigma$ порождаются идеалами Z_Σ, в силу вышеизложенного справедлива и тогда, если Σ является некоммутативным полем конечного ранга относительно P, причем элементы поля Σ должны быть перестановочны с P. В этом случае мы вместо $\mathfrak{S}_\Sigma$ будем писать $\mathfrak{S} \times \Sigma$ и $Z \times \Sigma$ вместо Z_Σ. Если Z' есть центр поля Σ, то можно применить еще раз теорему о том, что двусторонние идеалы поля $Z \times \Sigma$ порождаются идеалами поля $Z \times Z'$. Как и выше, приходим к выводу, что $\mathfrak{S} \times \Sigma$ (если Z или Z' первого рода) *не имеет радикала и распадается на такое же число двусторонне простых идеалов, что и произведение* $Z \times Z'$ *центров.*

Рассмотрим теперь вместо поля *простую систему* $\mathfrak{S}$ *с единицей*. Такая система $\mathfrak{S}$ изоморфна кольцу всех матриц r-го порядка поля K. Обозначим это кольцо через K_r и докажем, что

$$\mathsf{K}_r \cong \mathsf{K} \times \mathsf{P}_r, \tag{1}$$

$$\mathsf{P}_r \times \mathsf{P}_s \cong \mathsf{P}_{rs}. \tag{2}$$

Формула (1) получится сразу после того, как мы представим все элементы кольца K_r в виде $\sum c_{ij}\varkappa_{ij} = \sum c_{ij}(e\varkappa_{ij})$, $\varkappa_{ij} \in \mathsf{K}$, где c_{ij} перестановочны с $\varkappa_{ij}$ и e есть единичная матрица r-го порядка. Элементы $e\varkappa$ образуют подкольцо $e\mathsf{K} \cong \mathsf{K}$, а c_{ij} порождают подкольцо, изоморфное P_r.

(2) получается так: если P_r порождается r^2 величинами c'_{ik}, а P_s — s^2 величинами c''_{jl}, то $\mathsf{P}_r \times \mathsf{P}_s$ будет порождаться величинами

$$c_{ij,kl} = c'_{ik} \cdot c''_{jl},$$

число которых равно r^2s^2. Кроме того, имеет место

$$c_{ij,kl} \cdot c_{mn,pq} = \begin{cases} 0, \text{ если } k \neq m \text{ или } l \neq n, \\ c_{ij,pq}, \text{ если } k = m,\ l = n. \end{cases}$$

Если rs пар индексов ij заменить индексом α, пробегающим все значения от 1 до rs, а kl заменить индексом β, то получим:

$$c_{\alpha\beta} \cdot c_{\gamma\delta} = \begin{cases} 0 \text{ для } \beta \neq \gamma, \\ c_{\alpha\delta} \text{ для } \beta = \gamma, \end{cases}$$

откуда и вытекает изоморфизм между $\mathsf{P}_r \times \mathsf{P}_s$ и P_{rs}.

Из (1) вытекает, если Σ есть поле конечного ранга относительно P:

$$\mathfrak{S}_\Sigma \cong \Sigma \times \mathsf{K}_r \cong \Sigma \times \mathsf{K} \times \mathsf{P}_r \cong \mathsf{K}_\Sigma \times \mathsf{P}_r. \tag{3}$$

Тем самым вопрос относительно структуры $\mathfrak{S}_\Sigma$ приводится к исследованию структуры кольца K_Σ. Если центр поля Σ есть поле первого рода относительно P (или в частности центр равен P), то, как мы выше видели, K_Σ не имеет радикала и распадается на двусторонне простые кольца, т. е. на кольца матриц порядков r', r'', ...:

$$\mathsf{K}_\Sigma \cong \mathsf{K}'_{r'} + \mathsf{K}''_{r''} + \dots,$$

$$\mathfrak{S}_\Sigma \cong (\mathsf{K}'_{r'} + \mathsf{K}''_{r''} + \dots) \times \mathsf{P}_r \cong \mathsf{K}'_{r'} \times \mathsf{P}_r + \mathsf{K}''_{r''} \times \mathsf{P}_r + \dots \cong$$

$$\cong \mathsf{K}' \times \mathsf{P}_{r'} \times \mathsf{P}_r + \mathsf{K}'' \times \mathsf{P}_{r''} \times \mathsf{P}_r + \dots \cong$$

$$\cong \mathsf{K}' \times \mathsf{P}_{r'r} + \mathsf{K}'' \times \mathsf{P}_{r''r} + \dots \cong \mathsf{K}'_{r'r} + \mathsf{K}''_{r''r} + \dots;$$

стало быть, $\mathfrak{S}_\Sigma$ *есть также кольцо без радикала, которое распадается на такое же число колец матриц, что и* K_Σ, *только порядок матриц умножается на* r.

Наиболее важным случаем является тот случай, когда основное поле P совпадает с центром Z поля K. В этом случае K_Σ будет по предыдущему простым, откуда

$$\mathsf{K}_\Sigma \cong \mathsf{K}'_{r'},$$

а потому

$$\mathfrak{S}_\Sigma \cong \mathsf{K}'_{r'r}.$$

Итак: *простое кольцо* $\mathfrak{S} = \mathsf{K}_r$ *при алгебраическом расширении центра* Z *остается простым. Если поле* K *при расширении переходит в кольцо матриц порядка* r' *поля* K', *то* $\mathfrak{S} = \mathsf{K}_r$ *переходит в кольцо матриц порядка* $r'r$ *того же поля* K'.

Если поле Σ можно еще расширить, например расширить до $T \supset \Sigma$, то K' может снова „распасться", т. е. перейти в кольцо матриц порядка $r'' > 1$. Тогда K_T будет кольцом матриц $r''r'$, а $\mathfrak{S}_T$ — кольцом матриц порядка $r''r'r$. При дальнейшем расширении порядок кольца матриц будет возрастать, пока мы не придем к алгебраически замкнутому полю Ω и не получим кольца матриц поля Ω. Тогда *„разложение"* будет *полным*.

Вообще, чтобы получить полное разложение, можно и не пользоваться алгебраически замкнутым полем Ω; для этого вполне достаточно такое подполе $T \subset \Omega$, для которого K_T (и точно так же $\mathfrak{S}_T$) превращается в кольцо матриц поля T. При дальнейшем расширении порядок матриц уже не будет возрастать. Такое поле T называется, как и Ω, *полем разложения* систем K и $\mathfrak{S}$. Мы позже еще вернемся к полю разложения.

Задачи. 1. Для полного разложения простой системы K, достаточно конечное поле расширения центра.

2. Полупростая гиперкомплексная система относительно совершенного основного поля P при всяком расширении этого основного поля остается полупростой.

ГЛАВА СЕМНАДЦАТАЯ

ТЕОРИЯ ПРЕДСТАВЛЕНИЯ ГРУПП И ГИПЕРКОМПЛЕКСНЫХ СИСТЕМ

§ 120. ПОСТАНОВКА ЗАДАЧИ

Пусть $\mathfrak{G}$ — группа. Под *представлением* $\mathfrak{G}$ *через линейные преобразования поля* K мы разумеем групповой гомоморфизм, посредством которого всякому элементу группы a приводится в соответствие линейное преобразование A с коэфициентами из K. Представление называется *точным* или *неточным* в зависимости от того, будет ли оно изоморфным или неизоморфным.

Точно так же под *представлением кольца* $\mathfrak{o}$ *через линейные преобразования* K мы разумеем кольцевой гомоморфизм $a \to A$ (где не только произведение соответствует произведению, но и сумма — сумме). Наконец, если кольцо $\mathfrak{o}$ есть гиперкомплексная система относительно поля P, то мы потребуем, чтобы основное поле P содержалось в центре поля представления K и чтобы кольцевой гомоморфизм был операторным гомоморфизмом относительно P, т. е. чтобы из $a \to A$ следовало $a\rho \to A\rho$ для всех элементов ρ из P. Для модуля представления $\mathfrak{M}$ должно иметь место

$$(a\rho)\,m = (am)\,\rho \quad \text{при} \quad m \in \mathfrak{M}.$$

В дальнейшем мы главным образом будем говорить о представлении конечных групп $\mathfrak{G} = \{a_1, a_2, \ldots, a_h\}$ и гиперкомплексных систем. Задача состоит в том, чтобы найти все представления (если это возможно) и разложить представления на неприводимые составные части. Мы заметим только, что задача представления *групп* может быть сразу приведена к случаю *гиперкомплексной системы*; для этого надо из группы $\mathfrak{G}$ построить *групповое кольцо*

$$\mathfrak{o} = a_1\mathsf{K} + \ldots + a_h\mathsf{K},$$

элементы базиса которого суть элементы $\mathfrak{G}$. Если $a_i \to A_i$ есть представление группы, то

$$\sum a_i x_l \to \sum A_i x_l$$

есть представление системы $\mathfrak{o}$, если только предположить по крайней мере поле K коммутативным. Очевидно, что сумме будет соответствовать сумма, а произведению

$$\left(\sum a_i x_i\right)\left(\sum a_k \lambda_k\right) = \sum a_i a_k x_i \lambda_k$$

соответствует матрица

$$\sum\sum A_i A_k x_i \lambda_k = \left(\sum A_i x_i\right)\left(\sum A_k \lambda_k\right);$$

кроме того, произведению $\left(\sum a_i x_i\right)\cdot\rho$, очевидно, соответствует

$$\left(\sum A_i x_i\right)\cdot\rho.$$

Обратно, представление группового кольца $\mathfrak{o}$ в поле K приводит в соответствие элементам базиса $a_1, \ldots, a_h$ некоторые линейные преобразования, которые образуют представление группы $\mathfrak{G}$. Итак:

Представление конечной группы $\mathfrak{G}$ в коммутативном поле K связано с представлением группового кольца $\mathfrak{o} = a_1\mathsf{K} + \ldots + a_h\mathsf{K}$.

Среди представлений гиперкомплексной системы имеются такие, для которых поле представления K совпадает с основным полем P. Общий случай можно (по крайней мере для коммутативного K) свести к представлениям подобного рода, расширяя основное поле P до K; тогда гиперкомплексная система $\mathfrak{o}$ расширится до $\mathfrak{o}_k$ (§ 119). Если в обычном представлении элементам базиса $b_1, \ldots, b_n$ системы $\mathfrak{o}$ сопоставить матрицы $B_1, \ldots, B_n$ поля K, то элементу $\sum b_l x_l$ ($x_l \in \mathsf{K}$) из $\mathfrak{o}_k$ будет соответствовать матрица $\sum B_l x_l$ и потому представление $\mathfrak{o}$ расширится до представления $\mathfrak{o}_k$.

Итак, любое представление кольца $\mathfrak{o}$ в коммутативном поле K связано с представлением кольца $\mathfrak{o}_k$.

Если мы допустим, что кольцо $\mathfrak{o}$ обладает единицей, то получится дальнейшее ограничение проблемы. Тогда всегда можно предположить, что эта единица является единичным оператором для модуля представлений, т. е. ей соответствует единичная матрица. В противном случае согласно § 104 модуль представления равен прямой сумме $\mathfrak{M}_0 + \mathfrak{M}_1$, причем $\mathfrak{M}_0$ уничтожается $\mathfrak{o}$, а для $\mathfrak{M}_1$ единица является единичным оператором. Таким образом представление распадается на две составные части, где первая часть состоит только из нулевых матриц и потому нас не интересует, а вторая дает представление, при котором единица будет единичным оператором.

Особенно важным представлением гиперкомплексной системы $\mathfrak{o}$ является так называемое *правильное представление*. Мы его получим, если будем само $\mathfrak{o}$ рассматривать как модуль представления ($\mathfrak{o}$-левый и P-правый модуль). Подмодули образуют левые идеалы, а приведенная форма представления будет связана с композиционным рядом левых

идеалов. Правильное представление вполне приводимо, если само $\mathfrak{o}$ вполне приводимо.

На протяжении всей этой главы нужно иметь в виду зависимость между представлениями и модулем представления, установленную в § 108; только тогда будут понятны все выводы.

§ 121. ПРЕДСТАВЛЕНИЕ ГИПЕРКОМПЛЕКСНОЙ СИСТЕМЫ

Теория представления гиперкомплексной системы базируется на следующих двух теоремах:

Теорема 1. *Пусть* $\mathfrak{o}$ *— вполне приводимое (слева) кольцо с единицей и* $\mathfrak{M}$*-конечный (левый)* $\mathfrak{o}$*-модуль. Подмодуль* $\mathfrak{M}_0$*, уничтожающийся кольцом* $\mathfrak{o}$*, пусть равен нулю или вполне приводим. Тогда* $\mathfrak{M}$ *вполне приводимо и его неприводимые составные части либо уничтожаются* $\mathfrak{o}$*, либо изоморфны минимальным левым идеалам* $\mathfrak{o}$*. Все это остается справедливым и тогда, когда для* $\mathfrak{M}$ *и* $\mathfrak{o}$ *дана правая мультипликаторная область* Ω *с обычными свойствами*:

$$(am)\rho = a(m\rho) = (a\rho)m \quad \text{для } a \in \mathfrak{o},\ m \in \mathfrak{M},\ \rho \in \Omega.$$

Доказательство. Как мы уже видели, достаточно ограничиться случаем, когда единица $\mathfrak{o}$ есть единичный оператор. Если

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \ldots + \mathfrak{l}_r, \tag{1}$$

$$\mathfrak{M} = (m_1, \ldots, m_s) = (\mathfrak{o}m_1, \ldots, \mathfrak{o}m_s), \tag{2}$$

то, подставляя (1) в (2), получим:

$$\mathfrak{M} = (\ldots, \mathfrak{l}_i m_k, \ldots). \tag{3}$$

Модули $\mathfrak{l}_i m_k$, отличные от нуля, изоморфны $\mathfrak{l}_i$ (см. § 115, леммы 1 и 2); следовательно, эти $\mathfrak{l}_i m_k$ являются также минимальными $\mathfrak{o}$-модулями. Каждый из них либо содержится в сумме предшествующих, либо имеет общим элементом с этой суммой только нуль. Если выкинуть из суммы (3) $\mathfrak{l}_i m_k$, содержащиеся в сумме предшествующих $\mathfrak{l}_i m_k$, то сумма станет прямой.

В случае гиперкомплексной системы Ω будет, очевидно, одновременно полем коэфициентов P и полем представления, а $\mathfrak{M}$ — модулем представления. Так как всякий модуль представления конечен относительно P, и тем самым (если $\mathfrak{o}$ обладает единицей e) конечен относительно $e\mathsf{P} \subseteq \mathfrak{o}$ [1]), то получается *полная приводимость всех представлений вполне приводимой гиперкомплексной системы с единицей (или системы без радикала)*.

Левые идеалы $\mathfrak{l}_1, \ldots, \mathfrak{l}_r$ кольца $\mathfrak{o}$ можно получить, разлагая $\mathfrak{o}$ на двусторонние идеалы:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s,$$

а затем разлагая простые кольца $\mathfrak{a}_\nu$ на левые идеалы. Идеалы $\mathfrak{l}_i$, содержащиеся в $\mathfrak{a}_\nu$, уничтожаются идеалами $\mathfrak{a}_\mu$, где $\mu \neq \nu$. Следовательно, в представлении, получающемся с помощью $\mathfrak{l}_i$, все $\mathfrak{a}_\mu$, за исключением одного идеала $\mathfrak{a}_\nu$, изобразятся нулями. Идеал $\mathfrak{a}_\nu$ с точностью до эквивалентности обладает единственным неприводимым представлением, так как

[1]) и так как модуль $\mathfrak{M}_0$, уничтожающийся кольцом $\mathfrak{o}$, автоматически вполне приводим как конечный P-модуль.

все минимальные левые идеалы $\mathfrak{a}_\nu$ операторно изоморфны. Кроме того, представление $\mathfrak{a}_\nu$ является *точным*, так как $\mathfrak{a}_\nu$ есть двусторонний простой идеал. Ниже мы разберем эти представления более подробно.

Теорема, обратная 1, тривиальна. Именно, если любой конечный $\mathfrak{o}$-модуль вполне приводим, то само $\mathfrak{o}$ также вполне приводимо, так как $\mathfrak{o}$ есть конечный модуль с базисом, состоящим из единицы. Таким образом мы получаем теорему:

Если $\mathfrak{o}$ — гиперкомплексная система с единицей, и все представления системы $\mathfrak{o}$ вполне приводимы, то само $\mathfrak{o}$ вполне приводимо.

Теорема 1 дает возможность обозреть все представления системы без радикала, в то время как теорема 2 относится к *неприводимым* представлениям системы с радикалом.

Теорема 2. *Если $\mathfrak{o}$ — кольцо с условиями максимальности и минимальности для левых идеалов и $\mathfrak{c}$ — радикал кольца $\mathfrak{o}$, то всякий неприводимый $\mathfrak{o}$-модуль $\mathfrak{M}$ либо уничтожается кольцом $\mathfrak{o}$, либо изоморфен простому левому идеалу кольца $\frac{\mathfrak{o}}{\mathfrak{c}}$ без радикала. Все это остается справедливым также и при наличии мультипликаторной области Ω.*

Доказательство. Должно быть $\mathfrak{c}\mathfrak{M} = (0)$, так как в противном случае $\mathfrak{c}\mathfrak{M} = \mathfrak{M}$, откуда

$$\mathfrak{M} = \mathfrak{c}\mathfrak{M} = \mathfrak{c}^2\mathfrak{M} = \ldots = (0).$$

Поэтому $\mathfrak{M}$ можно рассматривать как $\frac{\mathfrak{o}}{\mathfrak{c}}$-модуль. В самом деле, все элементы одного и того же класса вычетов по $\mathfrak{c}$ при умножении на элемент $\mathfrak{M}$ дают одно и то же произведение. $\frac{\mathfrak{o}}{\mathfrak{c}}$ как кольцо без радикала обладает единицей и вполне приводимо. Отсюда с помощью теоремы 1 и следует наше утверждение.

В частности из теоремы 2 получается, что простые композиционные факторы $\mathfrak{o}$ встречаются уже в композиционном ряду $\frac{\mathfrak{o}}{\mathfrak{c}}$ (или $\mathfrak{o}$ по $\mathfrak{c}$).

В случае представлений теорема 2 означает, что *все неприводимые представления гиперкомплексной системы $\mathfrak{o}$ содержатся в правильном представлении* (*и даже в правильном представлении* $\frac{\mathfrak{o}}{\mathfrak{c}}$). И здесь все двусторонне простые компоненты $\frac{\mathfrak{o}}{\mathfrak{c}}$ будут представляться нулем, кроме, может быть, одного компонента, который будет представляться точно. Таким образом, *неприводимое* представление совершенно произвольной гиперкомплексной системы есть в сущности представление *простой* системы (если только это представление не нулевое, что в силу неприводимости возможно лишь в случае представлений первой степени).

Неприводимые представления, о которых говорится в теоремах 1 и 2, связаны с простым кольцом посредством левых идеалов. Построим теперь эти неприводимые представления для простой гиперкомплексной системы в явном виде.

В силу § 118 простая гиперкомплексная система $\mathfrak{o}$ с единицей изоморфна полному кольцу матриц в поле Λ, откуда

$$\mathfrak{o} = c_{11}\Lambda + c_{12}\Lambda + \ldots + c_{nn}\Lambda.$$

Минимальный идеал $\mathfrak{l}$ будет определяться равенством:

$$\mathfrak{l} = c_{11}\Lambda + c_{21}\Lambda + \ldots + c_{n1}\Lambda.$$

Основное поле P, в котором также должно иметь место представление, содержится в Λ, а Λ имеет конечную степень относительно P. Очевидно, что ранг кольца $\mathfrak{o}$ равен степени поля Λ, увеличенной в n^2 раз.

Обратимся сперва к случаю $\Lambda = \mathsf{P}$. Это может быть, например, тогда, если P алгебраически замкнуто. Тогда с помощью базиса (c_{11}, c_{21}, ..., c_{n1}) идеала $\mathfrak{l}$ можно явным образом построить матрицу представления. Если $a = \sum_{i,k=1}^{n} c_{ik}\alpha_{ik}$ — элемент кольца $\mathfrak{o}$, то имеет место

$$ac_{k1} = \sum_{i=1}^{n} c_{ik}c_{k1}\alpha_{ik} = \sum_{i=1}^{n} c_{i1}\alpha_{ik};$$

следовательно, представление, связанное с $\mathfrak{l}$, *приводит в соответствие элементу* a *матрицу* (α_{ik}). Изоморфизм кольца $\mathfrak{o}$ с полным кольцом матриц (α_{ik}) как раз и будет тем неприводимым представлением, которое связано с минимальным левым идеалом $\mathfrak{l}$. Это неудивительно, так как мы выше доказали, что с точностью до эквивалентности может существовать только *одно* неприводимое представление.

Достойно внимания, что в рассматриваемом случае $\Lambda = \mathsf{P}$ матрицы представления всегда образуют *полное* кольцо матриц n-го порядка.

Если система $\mathfrak{o}$ полупростая, т. е. равна прямой сумме $\mathfrak{a}_1 + \mathfrak{a}_2 + \ldots + \mathfrak{a}_s$ простых колец, и левый идеал $\mathfrak{l}$ является, например, левым идеалом в $\mathfrak{a}_\nu$, то, чтобы найти представление элемента a, связанное с $\mathfrak{l}$, надо прежде всего записать a в виде суммы $a_1 + a_2 + \ldots + a_s$ и затем член a_ν заменить соответствующей матрицей (α_{ik}), а остальные члены заменить нулевыми матрицами, так как эти члены $a_1, \ldots, a_{\nu-1}, a_{\nu+1}, \ldots, a_s$ уничтожают идеал $\mathfrak{l}$.

Иными словами, надо в кольцо $\mathfrak{a}_\nu$ ввести матричные единицы $c_{ik}^{(\nu)}$ ($i, k = 1, \ldots, n_\nu$) и представить каждый элемент a кольца $\mathfrak{o}$ в виде

$$a = \sum \alpha_{ik}^{(\nu)} c_{ik}^{(\nu)}.$$

Тогда $(\alpha_{ik}^{(\nu)})$ и будет матрицей представления a при ν-м неприводимом представлении (причем представление будет связано с левым идеалом $\mathfrak{a}_\nu$).

Во-вторых, если Λ — собственное надполе P:

$$\Lambda = \lambda_1\mathsf{P} + \ldots + \lambda_r\mathsf{P},$$

то, сопоставляя каждому β из Λ матрицу B системы уравнений

$$\beta\lambda_j = \sum \lambda_i\beta_{ij}, \quad B = (\beta_{ij}),$$

мы получим правильное представление Λ в P. Если $\mathfrak{o}$ простое, то

$$\mathfrak{l} = c_{11}\Lambda + \ldots + c_{n1}\Lambda = (c_{11}\lambda_1\mathsf{P} + \ldots + c_{11}\lambda_r\mathsf{P}) + \ldots + (c_{n1}\lambda_1\mathsf{P} + \ldots + c_{n1}\lambda_r\mathsf{P}).$$

Если мы представим с помощью этого базиса элемент $\beta \cdot c_{ik}$ кольца $\mathfrak{o}$, то будем иметь:

$$\beta c_{ik} \to \begin{pmatrix} 0 \dots 0 \dots 0 \\ \vdots \quad \vdots \quad \vdots \\ 0 \dots B \dots 0 \\ \vdots \quad \vdots \quad \vdots \\ 0 \dots 0 \dots 0 \end{pmatrix},$$

где нули изображают нулевые матрицы r-го порядка, а матрица B занимает k-е место в i-й строке. Отсюда следует, что

$$\sum_{i,k=1}^{n} \alpha_{ik} c_{ik} \to \begin{pmatrix} A_{11} \dots A_{1n} \\ \vdots \quad \vdots \\ A_{n1} \dots A_{nn} \end{pmatrix},$$

где A_{ik} — опять матрицы, которые соответствуют α_{ik} при правильном представлении поля Λ.

Почти непосредственным следствием нашего результата о том, что в случае алгебраически замкнутого поля кольцо матриц представления есть полное кольцо матриц, является *теорема Бёрнсайда* (*Burnside*). Если под *абсолютно неприводимой* [1]) системой матриц подразумевать систему, неприводимую при любом алгебраическом расширении поля K, то теорему Бёрнсайда можно сформулировать следующим образом:

Абсолютно неприводимая система $\mathfrak{S}$ *матриц* n*-го порядка, содержащая вместе с двумя матрицами и их произведение, содержит ровно* n^2 *линейно независимых матриц.*

Доказательство. Если Ω — алгебраически замкнутое алгебраическое поле расширения K, то система $\mathfrak{S}$ в Ω также неприводима. Присоединим к $\mathfrak{S}$ все линейные комбинации $\sum A_i \omega_i$ ($A_i \in \mathfrak{S}$, $\omega_i \in \Omega$); тогда расширенная система $\mathfrak{S}'$ будет кольцом, а Ω — областью операторов. Так как может существовать самое большее n^2 линейно независимых матриц, то расширенная система имеет конечный ранг относительно Ω. Таким образом $\mathfrak{S}'$ есть гиперкомплексная система; она образует представление $A \to A$. Но в силу теоремы 2 неприводимое представление гиперкомплексной системы в основном поле Ω является представлением без радикала, а в силу теоремы 1 оно должно быть представлением простой системы. Но в таком представлении при алгебраически замкнутом основном поле всегда существует n^2 линейно независимых матриц: система $\mathfrak{S}'$ есть полное кольцо матриц.

Задачи. 1. Определить все неприводимые представления гиперкомплексной системы, указанной в задаче 2 § 114.

2. Если неприводимая система $\mathfrak{S}$ матриц A теоремы Бёрнсайда образует кольцо, то это кольцо не имеет радикала (если бы $\mathfrak{S}$ имело радикал, то $\mathfrak{S}'$ также имело бы радикал).

3. Если кольцо $\mathfrak{S}$, рассматриваемое в задаче 2, удовлетворяет условию минимальности для левых идеалов, то $\mathfrak{S}$ — простое кольцо (если бы

[1]) В коммутативном поле K.

$\mathfrak{S}$ не было простым, то имело бы место $\mathfrak{S} = \mathfrak{a}_1 + \mathfrak{a}_2$, $\mathfrak{a}_1\mathfrak{a}_2 = (0)$, и тем самым $\mathfrak{S}'$ разлагалось бы подобным же образом).

4. *Обобщение теоремы Бёрнсайда.* Пусть вполне приводимая система $\mathfrak{S}$ матриц в алгебраически замкнутом поле Ω содержит вместе с двумя матрицами и их произведение. Пусть неприводимые составные части системы имеют порядок, равный соответственно $n_1, n_2, \ldots, n_s$ (при этом эквивалентные составные части считаются одинаковыми). Тогда система $\mathfrak{S}$ содержит

$$n_1^2 + n_2^2 + \ldots + n_s^2$$

линейно независимых матриц.

Если $n_1, \ldots, n_s$ — степени колец $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ матриц, на которые разлагается система $\mathfrak{o}$ без радикала, а $r_1, \ldots, r_s$ — ранги полей автоморфизмов левых идеалов колец $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$, наконец, $\mathfrak{D}_1, \ldots, \mathfrak{D}_s$ — неприводимые представления, связанные с этими левыми идеалами, то

$$h = \sum_{\nu=1}^{s} n_\nu^2 r_\nu$$

равно рангу системы $\mathfrak{o}$ и

$$g_\nu = n_\nu r_\nu$$

есть степень представления $\mathfrak{D}_\nu$. После приведения правильное представление будет содержать $\mathfrak{D}_\nu$ ровно n_ν раз. В случае алгебраически замкнутого основного поля $r_\nu = 1$, откуда

$$h = \sum_{\nu=1}^{s} n_\nu^2, \quad g_\nu = n_\nu .$$

6. Если P алгебраически замкнуто и $\mathfrak{o}$ — система с радикалом, то правильное представление содержит неприводимое представление по меньшей мере d раз, где d — степень неприводимого представления. Ранг системы $\mathfrak{o}$ больше суммы квадратов степеней представлений (эта сумма равна рангу кольца $\frac{\mathfrak{o}}{\mathfrak{c}}$).

7. Абсолютно неприводимое представление кольца остается неприводимым и тогда, если Ω есть трансцендентное расширение основного поля K (следует из теоремы Бёрнсайда).

8. Если элементам базиса $a_1, \ldots, a_n$ гиперкомплексной системы $\mathfrak{o}$ соответствуют матрицы $A_1, \ldots, A_n$ представления, и если с помощью неизвестных $x_1, \ldots, x_n$ (которые присоединяются к основному полю Ω) составить „общий элемент“ $x_1a_1 + \ldots + x_na_n$ и его представление $A_x = x_1A_1 + \ldots + x_nA_n$, то определитель матрицы A_x будет функцией от $x_1, \ldots, x_n$, причем:

a) эта функция неприводима в случае абсолютно неприводимого представления;

b) в случае двух эквивалентных неприводимых представлений определитель имеет одно и то же значение, а в случае неэквивалентных представлений — разные значения;

c) определитель разлагается на неприводимые сомножители, соответствующие неприводимым составным частям представления.

[Надо c_{ik} (может быть вместе с базисом радикала) взять в качестве новых элементов базиса и преобразовать соответствующим образом A_x.]

§ 122. ПРЕДСТАВЛЕНИЕ ЦЕНТРА

Центр гиперкомплексной системы $\mathfrak{o}$ при неприводимом представлении должен отображаться на такие матрицы, которые перестановочны со всеми матрицами представления. Если основное поле алгебраически замкнуто, т. е. кольцо матриц представления есть полное кольцо матриц, то центр этого кольца будет состоять только из кратных λE_n единичной матрицы; таким образом центр системы $\mathfrak{o}$ представляется матрицами вида λE_n. То же самое справедливо вообще для абсолютно неприводимых представлений, так как в этом случае можно перейти к алгебраически замкнутому основному полю без нарушения неприводимости. Итак: *в случае абсолютно неприводимого представления гиперкомплексной системы $\mathfrak{o}$ элементы центра представляются кратными единичной матрицы.*

Если система $\mathfrak{o}$ коммутативна, т. е. центр совпадает с системой $\mathfrak{o}$, то все матрицы абсолютно неприводимого представления будут иметь вид λE_n Тогда из неприводимости следует, что представления должны быть первой степени. Итак, *абсолютно неприводимые представления коммутативной гиперкомплексной системы могут быть только первой степени.*

Представление первой степени системы $\mathfrak{o}$ является гомоморфным отображением $\mathfrak{o}$ в поле представления K. Если K коммутативно, то два эквивалентных представления первой степени вообще равны, так как если A — матрица представления, λ — элемент поля K, то

$$\lambda^{-1} A \lambda = A.$$

Отсюда следует, что *число неэквивалентных представлений первой степени в коммутативном поле K коммутативной гиперкомплексной системы $\mathfrak{o}$ равно числу различных гомоморфизмов, отображающих $\mathfrak{o}$ на K.*

Вернемся к некоммутативной системе и допустим, что рассматриваемая система не имеет радикала. Тогда $\mathfrak{o}$ будет равно прямой сумме простых систем:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s,$$

а центр $\mathfrak{Z}$ системы $\mathfrak{o}$ равен сумме s полей $\mathfrak{Z}_i$:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \ldots + \mathfrak{Z}_s \ (\mathfrak{Z}_\nu \text{ — центр } \mathfrak{a}_\nu).$$

Число неэквивалентных неприводимых представлений $\mathfrak{o}$ и $\mathfrak{Z}$ равно числу s двусторонних компонентов в $\mathfrak{o}$ или в $\mathfrak{Z}$, так как всякое такое представление $\mathfrak{D}_\nu$ системы $\mathfrak{o}$ связано с левым идеалом $\mathfrak{a}_\nu$, а всякое такое представление $\mathfrak{D}'_\nu$ центра $\mathfrak{Z}$ связано с $\mathfrak{Z}_\nu$. *Поэтому число неэквивалентных неприводимых представлений системы $\mathfrak{o}$ равно числу неэквивалентных неприводимых представлений ее центра $\mathfrak{Z}$, и неприводимое представление $\mathfrak{D}$ системы $\mathfrak{o}$, при котором все $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$, за исключением $\mathfrak{a}_\nu$,*

представляются нулями, можно сопоставить представлению $\mathfrak{D}'_\nu$ *центра* $\mathfrak{Z}$, *при котором все* $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$, *за исключением* $\mathfrak{Z}_\nu$, *представляются нулями.*

Если в частности основное поле P алгебраически замкнуто, то поля $\mathfrak{Z}_\nu$ будут ранга 1 и изоморфны с P; поэтому в этом случае *число* s *неприводимых представлений* $\mathfrak{o}$ *равно рангу центра* $\mathfrak{Z}$. Так как $\mathfrak{Z}_\nu$ образуют P-модули ранга 1, то отсюда снова следует, что неприводимые представления $\mathfrak{Z}$ должны быть первой степени.

В этом случае связь между неприводимыми представлениями $\mathfrak{D}_\nu$ системы $\mathfrak{o}$ и неприводимыми представлениями (первой степени) ее центра $\mathfrak{Z}$ оказывается чрезвычайно простой. Именно, в случае представления $\mathfrak{D}_\nu$ любой элемент a центра представляется матрицей вида αE_{n_ν}, где E_{n_ν} — единичная матрица n_ν-го порядка. Таким образом любому a принадлежит (при данном ν) определенное α, и мы можем написать:

$$\alpha = \Theta_\nu(a).$$

Функция Θ_ν определяет гомоморфизм центра, т. е.

$$\Theta_\nu(a+b) = \Theta_\nu(a) + \Theta_\nu(b),$$
$$\Theta_\nu(ab) = \Theta_\nu(a)\,\Theta_\nu(b),$$
$$\Theta_\nu(a\lambda) = \Theta_\nu(a)\,\lambda.$$

При этом гомоморфизме все $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$, за исключением $\mathfrak{Z}_\nu$, будут представляться нулем; таким образом гомоморфизм Θ_ν есть как раз представление $\mathfrak{D}'_\nu$ первой степени центра.

Если известен P-базис для модуля $\mathfrak{Z}_\nu$, то представление Θ_ν становится также известным; в качестве такого базиса можно взять единицу e_ν поля $\mathfrak{Z}_\nu$. Если элемент a центра $\mathfrak{Z}$ записать в виде

$$a = \sum_{\nu=1}^{s} e_\nu \lambda_\nu, \tag{1}$$

то

$$a e_\nu = e_\nu^2 \lambda_\nu = e_\nu \lambda_\nu;$$

следовательно, $\lambda_\nu E_{n_\nu}$ будет матрицей представления

$$\Theta_\nu(a) = \lambda_\nu.$$

Для (1) мы можем теперь также написать:

$$a = \sum_{\nu=1}^{s} e_\nu \Theta_\nu(a). \tag{2}$$

Итак: *коэфициенты* $\Theta_\nu(a)$ *разложения элемента* a *центра по равностепенным элементам* e_ν *центра определяют вместе с тем гомоморфизмы или представления первой степени центра.*

Задачи. 1. Число представлений первой степени коммутативной гиперкомплексной системы $\mathfrak{o}$ в алгебраически замкнутом поле Ω расширения P равно рангу $\frac{\mathfrak{o}_\Omega}{\mathfrak{c}}$, где $\mathfrak{c}$ — радикал $\mathfrak{o}_\Omega$.

2. Если K — коммутативное поле относительно P, то число представлений первой степени K в Ω равно приведенной степени поля K относительно $\mathsf{P}\cdot c=(0)$ тогда и только тогда, если K есть поле первого рода относительно P.

3. Степень неприводимого представления $\mathfrak{D}'_\nu$ центра $\mathfrak{Z}$ равна рангу модуля $\mathfrak{Z}_\nu$ относительно P. В представлении $\mathfrak{D}_\nu$ центра $\mathfrak{Z}$ представление $\mathfrak{D}_\nu$ содержится ровно $n_\nu t_\nu$ раз, причем n_ν и t_ν определяются следующим образом: $\mathfrak{a}_\nu$ есть полное кольцо матриц n_ν-го порядка с элементами из поля K_ν, а t_ν — степень K_ν относительно своего центра $\mathfrak{Z}_\nu$.

§ 123. СЛЕДЫ И ХАРАКТЕРЫ

Под *следом элемента a в представлении $\mathfrak{D}$, в записи* $S_{\mathfrak{D}}(a)$ или, короче, $S(a)$, мы разумеем след $S(A)$ матрицы A, соответствующей элементу a. След $S_{\mathfrak{D}}$, который при данном $\mathfrak{D}$ рассматривается как функция от a, называется также *следом представления* $\mathfrak{D}$.

В силу равенства

$$S(P^{-1}AP)=S(A)$$

эквивалентные представления имеют одни и те же следы.

След есть *линейная функция*, т. е. имеет место

$$S(a+b)=S(a)+S(b),\quad S(a\lambda)=S(a)\lambda.$$

След абсолютно неприводимого представления (или, что одно и то же, след неприводимого представления в алгебраически замкнутом поле Ω) называется *характером*. Характер элемента a при ν-м неприводимом представлении $\mathfrak{D}_\nu$ будет обозначаться символом

$$\chi_\nu(a).$$

В случае одного и того же представления индекс ν будет опускаться.

В абсолютно неприводимом представлении $\mathfrak{D}_\nu$ степени n_ν элемент центра z в силу § 122 представляется диагональной матрицей $E_{n_\nu}\cdot\Theta_\nu(z)$, где Θ_ν — гомоморфное отображение центра на поле Ω. След матрицы $E_{n_\nu}\cdot\Theta_\nu(z)$ равен

$$\chi_\nu(z)=n_\nu\cdot\Theta_\nu(z). \tag{1}$$

В частности единица кольца $\mathfrak{o}$ будет представляться единичной матрицей E_{n_ν}, след которой равен n_ν:

$$\chi_\nu(1)=n_\nu.$$

Предположим в дальнейшем, что степень n_ν абсолютно неприводимого представления не делится на характеристику поля Ω. Тогда можно (1) разделить на n_ν, в результате чего получится:

$$\Theta_\nu(z)=\frac{\chi_\nu(z)}{n_\nu}. \tag{2}$$

Так выражаются гомоморфизмы центра через характеры.

Теорема. *Вполне приводимое представление гиперкомплексной системы $\mathfrak{o}$ в поле Ω с характеристикой 0 однозначно с точностью до эквивалентности определяется следами матриц представления.*

Доказательство. Если $\mathfrak{c}$ есть радикал системы $\mathfrak{o}$, то вполне приводимое представление системы $\mathfrak{o}$ также вполне приводимо для $\frac{\mathfrak{o}}{\mathfrak{c}}$. Предположим, что следы матриц, представляющих элементы $\frac{\mathfrak{o}}{\mathfrak{c}}$, известны. Пусть

$$\frac{\mathfrak{o}}{\mathfrak{c}} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n;$$

пусть $e_1, \ldots, e_n$ — единицы колец $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$. Тогда в случае неприводимого представления $\mathfrak{D}_\nu$ элемент e_ν представится единичной матрицей n_ν-го порядка; отсюда

$$S_\nu(e_\nu) = n_\nu,$$

напротив

$$S_\nu(e_\mu) = 0 \quad \text{для } \mu \neq \nu.$$

Теперь вполне приводимое представление станет известным, коль скоро удастся установить, сколько раз входит $\mathfrak{D}_\nu$ в это представление. Если $\mathfrak{D}_\nu$ входит, например, q_ν раз, то наше представление состоит из q_1 клеточек $\mathfrak{D}_1$, q_2 клеточек $\mathfrak{D}_2$ и т. д. Тогда получим:

$$S(e_\nu) = q_\nu n_\nu. \tag{3}$$

Если все $S(e_\nu)$ известны, то из (3) можно определить q_ν. Этим теорема доказана.

Замечание. Следы всех элементов системы $\mathfrak{o}$ известны, если известны следы элементов базиса системы $\mathfrak{o}$. Таким образом если, например, кольцо $\mathfrak{o}$ образует групповое кольцо конечной группы, достаточно найти следы элементов группы; тем самым представление будет определено. Итак, *вполне приводимое представление конечной группы определяется следами элементов группы с точностью до эквивалентности.*

Если $a_1, \ldots, a_n$ — элементы базиса системы $\mathfrak{o}$ и $\chi_\nu(a_i)$ — их следы, соответствующие неприводимым представлениям, то для произвольного представления имеем:

$$S(a_i) = \sum_{\nu=1}^{s} q_\nu \chi_\nu(a_i). \tag{4}$$

Согласно приведенной выше теореме этими уравнениями числа q_ν определяются однозначно.

Задачи. 1. В случае не вполне приводимого представления не только сами представления, но и диагональные неприводимые матрицы, которые содержатся в этих представлениях (композиционные факторы модуля представления) определяются следами однозначно.

2. Вполне приводимое представление бесконечной группы определяется следами однозначно с точностью до эквивалентности.

(Если даны два каких-нибудь представления конечной степени и с одинаковыми следами, то их можно последовательно расширить до представления, а систему матриц представлений можно расширить до кольца. Это кольцо будет гиперкомплексной системой, и тогда будут существовать два представления гиперкомплексной системы.)

§ 124. ПРЕДСТАВЛЕНИЕ АБЕЛЕВЫХ ГРУПП

Абелевы конечные группы представляют красивый и простейший случай теории представлений.

Пусть группа $\mathfrak{G}$ порядка h равна прямому произведению циклических групп порядка $h_1, \ldots, h_r$; тогда любой элемент a группы $\mathfrak{G}$ выразится однозначно в виде:

$$a = c_1^{\lambda_1} c_2^{\lambda_2} \ldots c_r^{\lambda_r} \quad (0 \leqslant \lambda_1 < h_1,\ 0 \leqslant \lambda_2 < h_2, \ldots,\ 0 \leqslant \lambda_r < h_r).$$

Установим неприводимые представления группы в алгебраически замкнутом поле Ω с характеристикой, равной нулю, или с характеристикой, не делящей $h = h_1 h_2 \ldots h_r$.

Прежде всего легко видеть, что неприводимые представления *линейны* (т. е. первой степени). Все дело состоит в том, чтобы всякому элементу a группы сопоставить такое число $\chi(a)$ из Ω, чтобы выполнялось условие гомоморфизма:

$$\chi(ab) = \chi(a)\chi(b). \tag{1}$$

Такая функция χ называется *характером* группы. (Это определение согласуется с определением, приведенным в § 123, так так след матрицы (χ) равен χ.) Мы с самого начала исключим нулевое представление $\chi(a) = 0$ для всех a. Но тогда должно иметь место $\chi(1) = 1$. Далее имеем:

$$\chi(c_1^{\lambda_1} \ldots c_r^{\lambda_r}) = \chi(c_1)^{\lambda_1} \ldots \chi(c_r)^{\lambda_r},$$

$$\chi(c_\nu)^{h_\nu} = \chi(c_\nu^{h_\nu}) = \chi(1) = 1;$$

следовательно, $\chi(c_\nu)$ равно h_ν-му корню ζ_ν из единицы, и представление имеет вид:

$$\chi(c_1^{\lambda_1} \ldots c_r^{\lambda_r}) = \zeta_1^{\lambda_1} \ldots \zeta_r^{\lambda_r}. \tag{2}$$

Обратно, уравнение (2) при любом выборе корней $\zeta_1, \ldots, \zeta_r$ из единицы всегда представляет гомоморфизм группы $\mathfrak{G}$. Относительно корня из единицы ζ_ν в нашем распоряжении имеется h_ν значений; таким образом *всего существует*

$$h = h_1 h_2 \ldots h_r$$

различных характеров, которым соответствует столько же неэквивалентных представлений первой степени.

Если положить все $\zeta_\nu = 1$, то получится *главный характер* χ_0:

$$\chi_0(a) = 1.$$

Здесь можно чрезвычайно легко представить себе, как получаются все представления с помощью приведения правильного представления (см. § 121). Возьмем сперва циклическую группу $\mathfrak{G}$ с образующим элементом c; пусть $c^h = 1$. Тогда правильное представление будет определяться линейным преобразованием $c \cdot c^\lambda = c^{\lambda+1}$ в векторном пространстве $(1,\ c,\ c^2,\ \ldots,\ c^{h-1})$. Чтобы привести представление, введем новый базис

$$(\zeta,\ c) = 1 + \zeta c + \zeta^2 c^2 + \ldots + \zeta^{h-1} c^{h-1} \tag{3}$$

(см. резольвенту Лагранжа в § 50), где ζ пробегает h h-х корней из

единицы. Что это действительно есть базис, следует из того, что c^λ выражаются через (ζ, c). В самом деле, если умножить (3) на ζ^{-r} и просуммировать по всем ζ, то получится:

$$\sum \zeta^{-r}(\zeta, c) = hc^r. \tag{4}$$

Далее легко видеть, что

$$c\cdot(\zeta, c) = \zeta^{-1}\cdot(\zeta, c). \tag{5}$$

Поэтому каждый элемент (ζ, c) базиса определяет некоторое инвариантное подпространство, *и представление вполне приводимо.* Матрица, представляющая элемент c в каждом подпространстве, имеет вид:

$$(\chi(c)) = (\zeta^{-1}).$$

ζ^{-1}, как и ζ, пробегает все h корней из единицы.

В случае прямого произведения циклических групп вместо произведения $c_1^{\lambda_1}c_2^{\lambda_2}\dots c_r^{\lambda_r}$ введем новые элементы базиса:

$$(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r) = (\zeta_1, c_1)(\zeta_2, c_2)\dots(\zeta_r, c_r).$$

Тогда

$$c_\mu\cdot(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r) = \zeta_\mu^{-1}(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r)$$

будет вполне приведенной формой представления, откуда в качестве неприводимых представлений получатся:

$$\chi(c_\mu) = \zeta_\mu^{-1},$$

$$\chi(c_1^{\lambda_1}c_2^{\lambda_2}\dots c_r^{\lambda_r}) = \zeta_1^{-\lambda_1}\zeta_2^{-\lambda_2}\dots\zeta_r^{-\lambda_r}.$$

Таким образом мы получили следующее предложение:

Групповое кольцо абелевой группы, образованное с помощью алгебраически замкнутого поля, вполне приводимо и равно прямой сумме h полей $\mathfrak{Z}_\nu$, которые порождаются новыми векторами $(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r)$ базиса. Все это верно лишь при условии, что характеристика поля не делит порядка группы h.

$(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r)$ должны быть идемпотентны с точностью до множителя. В самом деле, легко получается, что

$$(\zeta_\nu, c_\nu)^2 = h_\nu(\zeta_\nu, c_\nu),$$

откуда

$$(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r)^2 = h(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r),$$

так что элемент

$$\frac{1}{h}(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r)$$

идемпотентен (единица поля $\mathfrak{Z}_\nu$).

Из вышедоказанного следует согласно теореме 1 § 121, что ***всякое представление группы $\mathfrak{G}$ вполне приводимо.***

Характеры подчиняются целому ряду условий, которые можно найти следующим образом: прежде всего произведение двух характеров также есть характер:

$$\chi(a)\chi'(a) = \chi''(a); \tag{6}$$

точно так же существует характер, обратный данному. Следовательно, *характеры образуют группу* $\mathfrak{H}$.

Если ζ_ν есть примитивный h_ν-й корень из единицы, то характер

$$\chi(c_1^{\lambda_1} \dots c_r^{\lambda_r}) = \zeta_\nu^{\lambda_\nu}$$

порождает циклическую подгруппу $\mathfrak{H}_\nu$ порядка h_ν группы $\mathfrak{H}$. Легко видеть, что вся группа $\mathfrak{H}$ равна прямому произведению циклических групп порядка $h_1, \dots, h_r$; следовательно, *группа* $\mathfrak{H}$ *характеров изоморфна данной группе* $\mathfrak{G}$.

Взаимность между группами $\mathfrak{G}$, $\mathfrak{H}$, выражаемую равенствами (1), (6), можно обратить. А именно, число $\chi(a)$ зависит от характера χ и от элемента группы a; и это число при постоянном a является функцией характера χ; согласно (6) эта функция есть гомоморфизм группы характеров $\mathfrak{H}$. Число таких гомоморфизмов равно h; таким образом все гомоморфизмы группы $\mathfrak{H}$ определяются группой $\mathfrak{G}$.

Из (2) после суммирования по всем $\lambda_1, \dots, \lambda_r$ следует:

$$\sum_a \chi(a) = \left(\sum \zeta_1^{\lambda_1}\right)\left(\sum \zeta_2^{\lambda_2}\right)\dots\left(\sum \zeta_r^{\lambda_r}\right) = \begin{cases} h, & \text{если все } \zeta_\nu = 1, \\ 0, & \text{если не все } \zeta_\nu = 1. \end{cases}$$

Поэтому

$$\sum_a \chi(a) = \begin{cases} h \text{ для } \chi = \chi_0, \\ 0 \text{ для } \chi \neq \chi_0. \end{cases} \tag{7}$$

Точно так же справедливо обратное соотношение:

$$\sum_\chi \chi(a) = \begin{cases} h \text{ для } a = 1, \\ 0 \text{ для } a \neq 1. \end{cases} \tag{8}$$

Если в (8) подставить $a = a'a''$, то получится:

$$\sum_\chi \chi(a')\chi(a'') = \begin{cases} h \text{ для } a' = a''^{-1}, \\ 0 \text{ для } a' \neq a''^{-1}. \end{cases} \tag{9}$$

Точно так же имеем:

$$\sum_a \chi'(a)\chi''(a) = \begin{cases} h \text{ для } \chi' = \chi''^{-1}, \\ 0 \text{ для } \chi' \neq \chi''^{-1}. \end{cases} \tag{10}$$

Характер χ^{-1} называется *сопряженным* с χ и будет обозначаться символом $\bar{\chi}$. (В случае числового поля ζ^{-1} есть комплексное число, сопряженное ζ, откуда χ^{-1} есть комплексное число, сопряженное χ.) Так как, очевидно, $\chi(a^{-1}) = \bar{\chi}(a)$, то вместо (9) и (10) можно написать:

$$\sum_\chi \chi(a')\bar{\chi}(a'') = \begin{cases} h \text{ для } a' = a'', \\ 0 \text{ для } a' \neq a''. \end{cases} \tag{11}$$

$$\sum_a \chi'(a)\bar{\chi}''(a) = \begin{cases} h \text{ для } \chi' = \chi'', \\ 0 \text{ для } \chi' \neq \chi''. \end{cases} \tag{12}$$

Каждое из этих равенств означает, что матрица h^2 чисел $\chi(a)$ (где χ — индекс строки, а a — индекс столбца) является обратной относительно транспонированной матрицы чисел $\frac{1}{h}\overline{\chi}(a)$ ($\overline{\chi}$ — индекс строки, a — индекс столбца). Равенство (11) называется *условием ортогональности характеров.*

Характеры абелевых групп имеют многочисленные приложения в теории чисел. Пусть n — натуральное число. Возьмем в качестве $\mathfrak{G}$ мультипликативную группу классов вычетов по модулю n, которые представляются натуральными числами, взаимно простыми с n и не превосходящими n [следовательно, h будет эйлеровой функцией $\varphi(n)$]. Под *характером* $\chi(m)$ *вычетов числа* m, *взаимно простого с* n, подразумевают характер класса вычетов, представителем которого является число m в группе классов вычетов. Если целое число m не взаимно просто с n, то принято полагать $\chi(m)=0$. В силу этого условия можно распространить сумму в (7) или (10) на полную систему вычетов по модулю n, в то время как (1), (6), (8) и (9) справедливы для всех чисел a, b и a', a''.

Задача. Написать все характеры чисел 1, 2, ..., 11 по модулю 12; написать все характеры этих же чисел по модулю 11.

§ 125. ПРЕДСТАВЛЕНИЕ КОНЕЧНЫХ ГРУПП

Мы свели в § 120 задачу представления конечной группы $\mathfrak{G}$ к той же задаче для группового кольца $\mathfrak{o}=(a_1, \ldots, a_h)$. Согласно теореме 1 § 121 все представления будут найдены, коль скоро мы докажем, что это групповое кольцо вполне приводимо. Для этого достаточно доказать следующую *теорему Машке* (Maschke):

Представление конечной группы $\mathfrak{G}$ *в поле* P, *характеристика которого не делит порядка группы* h, *вполне приводимо.*

Доказательство. Пусть модуль представления $\mathfrak{M}$ вполне приводим и пусть $\mathfrak{N}$ есть минимальный (или неприводимый) подмодуль. Покажем, что $\mathfrak{M}$ равен прямой сумме $\mathfrak{N}+\mathfrak{N}'$, где $\mathfrak{N}'$ есть также модуль представления.

$\mathfrak{M}$ как векторное пространство разлагается на сумму $\mathfrak{N}+\mathfrak{N}'$; при этом $\mathfrak{N}'$ еще не обязательно инвариантно относительно $\mathfrak{o}$, т. е. может и не быть модулем представления. Если y — элемент $\mathfrak{N}'$ и a — элемент $\mathfrak{G}$, то ay представляется однозначно в виде суммы элемента $\mathfrak{N}$ и элемента y' из $\mathfrak{N}'$; в силу этого

$$ay \equiv y' \pmod{\mathfrak{N}}.$$

При заданном a элемент y' однозначно определяется элементом y и зависит линейно от y: из $ay \equiv y'$ и $az \equiv z'$ следует $a(y+z)=y'+z'$ и $ay\lambda \equiv y'\lambda$ для $\lambda \in \mathsf{P}$. Таким образом мы можем написать:

$$y' \equiv A'y;\quad A'y \equiv ay \pmod{\mathfrak{N}},$$

где A' — линейный оператор (т. е. линейное преобразование) в $\mathfrak{N}'$ [1]) и зависит еще от a. А именно, операторы A' образуют представление группы $\mathfrak{G}$, так как из $a \to A'$ и $b \to B'$ следует $ab \to A'B'$.

[1]) Если все линейные операторы представить матрицами, как в § 108, то A' будет как раз матрицей T, стоящей в правом нижнем углу.

Положим теперь

$$\frac{1}{h}\sum_a a^{-1}A'y = Qy = y'';$$

тогда y'' также будет линейно зависеть от y и потому y'' образуют линейное подпространство $\mathfrak{N}'' = Q\mathfrak{N}'$. Далее имеет место следующее сравнение по модулю $\mathfrak{N}$:

$$y'' \equiv \frac{1}{h}\sum_a a^{-1}ay = y.$$

Таким образом любой элемент $\mathfrak{M}$ не только сравним с элементом y из $\mathfrak{N}'$ по модулю $\mathfrak{N}$, но сравним также с элементом y'' из $\mathfrak{N}''$, определяющимся однозначно, т. е. имеет место представление $\mathfrak{M}$ в виде прямой суммы:

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{N}''.$$

Наконец, для всякого элемента b из $\mathfrak{G}$ имеет место:

$$by'' = \frac{1}{h}\sum_a ba^{-1}A'y = \frac{1}{h}\sum_a (ab^{-1})^{-1}(A'B'^{-1})B'y =$$
$$= QB'y \in Q\mathfrak{N}' = \mathfrak{N}'';$$

следовательно, $\mathfrak{N}''$ преобразуется операторами b из $\mathfrak{G}$ в самого себя, т. е. $\mathfrak{N}''$ есть модуль представления.

Если $\mathfrak{N}''$ также приводимо, то можно точно таким же образом поступить с $\mathfrak{N}''$, выделив минимальный подмодуль, и т. д. В результате получим полное разложение модуля $\mathfrak{M}$ и тем самым представления.

Чтобы построить все представления группы, достаточно в силу доказанной только что теоремы найти неприводимые представления; неприводимые представления можно найти с помощью минимальных левых идеалов группового кольца (или, что одно и то же, с помощью приведения правильного представления). В приводимом представлении всякое неприводимое представление может повторяться сколь угодно часто.

Согласно § 122 число абсолютно неприводимых представлений равно рангу центра, а центр группового кольца, как это видно без труда, состоит из всех таких сумм

$$\sum_\lambda a_\lambda \rho_\lambda \quad (a_\lambda \in \mathfrak{G},\ \rho_\lambda \in \mathbf{P}), \tag{1}$$

в которых сопряженные элементы группы имеют одинаковые коэфициенты. Элементы, сопряженные с элементом a, образуют „*класс*". Если k_a есть сумма элементов этого класса, то (1) равна сумме k_a с коэфициентами из $\mathbf{P}$. Следовательно, справедлива такая теорема: *центр группового кольца порождается суммами классов* k_a. Таким образом ранг центра равен числу классов, а отсюда следует, что *число неэквивалентных абсолютно неприводимых представлений группы равно числу классов сопряженных элементов.*

Для степеней $n_1, \ldots, n_s$ неприводимых представлений имеет место равенство:

$$n_1^2 + n_2^2 + \ldots + n_s^2 = h,$$

так как групповое кольцо ранга h равно прямой сумме колец матриц рангов $n_1^2, n_2^2, \ldots, n_s^2$.

Всегда существующее представление первой степени, приводящее в соответствие каждому элементу группы число 1, называется „тождественным представлением".

Если имеются и другие представления первой степени, то должен существовать собственный нормальный делитель с абелевой фактор-группой, так как преобразования представлений первой степени друг с другом перестановочны и образуют абелеву группу, гомоморфную данной группе. Если, обратно, существует собственный нормальный делитель с абелевой фактор-группой, то характеры этой абелевой группы определяют представления первой степени. Все остальные представления имеют более высокую степень.

Примеры. 1. *Симметрическая группа* $\mathfrak{S}_3$. Число ее классов равно 3; таким образом имеется 3 ее представления. Знакопеременная группа порождает два смежных класса $\mathfrak{K}_0$, $\mathfrak{K}_1$: классы четных и нечетных подстановок. Два характера этих двух групп:

$$\chi(\mathfrak{K}_0) = 1, \quad \chi(\mathfrak{K}_1) = \pm 1,$$

определяют представления первой степени. В силу

$$n_1^2 + n_2^2 + n_3^2 = 6$$

третье представление должно иметь вторую степень. Если на плоскости возьмем три вектора e_1, e_2, e_3, сумма которых равна нулю, то перестановки этих трех векторов дают точное представление этой группы перестановок; легко видеть, что это представление неприводимо. Если взять e_1 и e_2 в качестве основных векторов, то представление будет таково:

$$\left.\begin{aligned}(1\ 2)\,e_1 &= e_2,\\ (1\ 2)\,e_2 &= e_1,\end{aligned}\right\} \quad \left.\begin{aligned}(1\ 3)\,e_1 &= -e_1 - e_2,\\ (1\ 3)\,e_2 &= e_2,\end{aligned}\right\} \quad \left.\begin{aligned}(2\ 3)\,e_1 &= e_1,\\ (2\ 3)\,e_2 &= -e_1 - e_2,\end{aligned}\right.$$

$$\left.\begin{aligned}(1\ 2\ 3)\,e_1 &= e_2,\\ (1\ 2\ 3)\,e_2 &= -e_1 - e_2,\end{aligned}\right\} \quad \left.\begin{aligned}(1\ 3\ 2)\,e_1 &= -e_1 - e_2,\\ (1\ 3\ 2)\,e_2 &= e_1.\end{aligned}\right.$$

2. *Группа кватернионов* $\mathfrak{Q}_8$:

$$j^4 = 1, \quad k^2 = j^2, \quad kj = j^3k.$$

Число классов равно пяти; следовательно, должно быть пять представлений. Нормальный делитель $\{1, j^2\}$ имеет фактор-группой клейновскую четверную группу, четыре характера которой определяют четыре представления. В силу равенства

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 8$$

пятое представление должно быть второй степени. Если элементам группы $1, j, j^2, j^3, k, jk, j^2k, j^3k$ сопоставить кватернионы $1, j, -1, -j, k, l, -k, -l$, то получится гомоморфное отображение группового кольца $\mathfrak{o}$ на поле кватернионов; следовательно, поле кватернионов должно встречаться среди двусторонних композиционных факторов $\mathfrak{o}$. Это позволяет

найти разложение кольца $\mathfrak{o}$ в рациональном основном поле Γ; именно, мы имеем:

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4 + \mathfrak{a}_5,$$

где $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$, $\mathfrak{a}_4$ изоморфны Γ, $\mathfrak{a}_5$ — изоморфно полю кватернионов. Если перейти к алгебраически замкнутому основному полю (в этом случае вполне достаточно присоединить $i = \sqrt{-1}$), то поле кватернионов разложится на свои составные части, и мы будем иметь матричное представление

$$j \to \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad k \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad l \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

3. *Со знакопеременной группой* $\mathfrak{A}_4$ можно поступить совершенно так же, как и с симметрической группой $\mathfrak{S}_3$. Мы это предоставляем сделать читателю. В результате получатся четыре представления степени 1, 1, 1, 3.

4. *Симметрическая группа* $\mathfrak{S}_4$. Число классов равно пяти; следовательно, должно быть пять представлений. Клейновская четверная группа $\{1, (12)(34), (13)(24), (14)(23)\}$ имеет фактор-группу, изоморфную $\mathfrak{S}_3$. Мы знаем, что $\mathfrak{S}_3$ допускает три неприводимые представления степени 1, 1, 2; эти представления определяют три представления $\mathfrak{S}_4$, тоже степеней 1, 1, 2. Если эти степени обозначить через n_1, n_2, n_3, то из

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24$$

следует, что

$$n_4^2 + n_5^2 = 18.$$

Но это возможно только при $n_4 = 3$, $n_5 = 3$. Если ввести четыре вектора e_1, e_2, e_3, e_4, сумма которых равна нулю, то перестановки этих четырех векторов дают точное представление третьей степени $\mathfrak{S}_4$. Если взять e_1, e_2, e_3 в качестве основных векторов, то представление будет таково:

$$\begin{cases} (1\ 2)\, e_1 = e_2, \\ (1\ 2)\, e_2 = e_1, \\ (1\ 2)\, e_3 = e_3, \end{cases} \quad \begin{cases} (1\ 3)\, e_1 = e_3, \\ (1\ 3)\, e_2 = e_2, \\ (1\ 3)\, e_3 = e_1, \end{cases} \quad \begin{cases} (1\ 4)\, e_1 = -e_1 - e_2 - e_3, \\ (1\ 4)\, e_2 = e_2, \\ (1\ 4)\, e_3 = e_3, \end{cases}$$

$$\begin{cases} (1\ 2\ 3)\, e_1 = e_2, \\ (1\ 2\ 3)\, e_2 = e_3, \\ (1\ 2\ 3)\, e_3 = e_1, \end{cases} \text{ и т. д.}$$

Так как представление точное, то оно не может привестись к представлениям первой и второй степени; следовательно, оно неприводимо. Если умножить на -1 матрицы представления нечетных подстановок, то получится другое также точное и потому неприводимое представление третьей степени, которое неэквивалентно прежнему представлению, так как следы у них различные. Таким образом мы нашли все представления.

Задачи. 1. Элемент $s = \sum_{a \in \mathfrak{E}} a$ группового кольца $\mathfrak{o}$ удовлетворяет уравнениям:

$$bs = s \text{ для } b \in \mathfrak{B}.$$

Какой левый идеал порождается элементом s? Какое представление соответствует этому идеалу? Какой идемпотентный элемент содержится в этом идеале?

2. Если число h элементов группы делится на характеристику поля, то идеал, указанный в задаче 1, будет нильпотентным. Вывести отсюда, что условие, что h не делится на характеристику, также необходимо для теоремы Машке.

§ 126. ГРУППОВЫЕ ХАРАКТЕРЫ

Кронекеровское преобразование произведений. Пусть даны два линейные преобразования A', A''; одно в векторном пространстве $(u_1, \ldots, u_n)$, а другое в векторном пространстве $(v_1, \ldots, v_m)$, причем u и v будут рассматриваться как переменные. Таким образом пусть будет

$$A'u_k = \sum_i u_i \alpha'_{ik},$$

$$A''v_l = \sum_j v_j \alpha''_{jl}.$$

Если к u и v одновременно применить эти преобразования, то произведение $u_k v_l$ преобразуется следующим образом[1]):

$$Au_k v_l = \sum_i \sum_j u_i v_j \alpha'_{ik} \alpha''_{jl}. \tag{1}$$

Такое преобразование A в векторном пространстве $n \cdot m$ линейно независимых величин $u_k v_l$ называется *кронекеровским произведением преобразований* и будет обозначаться через $A' \times A''$. Согласно (1) элементами матрицы A являются произведения $\alpha'_{ik}\alpha''_{jl}$. След A равен

$$\sum_i \sum_j \alpha'_{ii}\alpha''_{jj} = \sum_i \alpha'_{ii} \cdot \sum \alpha''_{jj} = S(A') \cdot S\ (A'').$$

Итак: *след преобразования $A' \times A''$ равен произведению следов преобразований A' и A''.*

Если выполнить относительно u последовательно два преобразования B', A', а над v — преобразование B'' и затем A'', то произведение $u_k v_l$ тем самым подвергнется сначала преобразованию $B' \times B''$ и затем преобразованию $A' \times A''$, т. е. получим, что

$$(A' \times A'') \cdot (B' \times B'') = A'B' \times A''B''. \tag{2}$$

Если матрицы A', B', ... образуют представление $\mathfrak{D}'$ группы $\mathfrak{G}$, а матрицы A'', B'', ... — другое представление $\mathfrak{D}''$ той же группы, то из (2) следует, что преобразования произведений $A = A' \times A''$, $B = B' \times B''$, ... также образуют представление. Это *произведение представлений* $\mathfrak{D}'$, $\mathfrak{D}''$ будет обозначаться символом $\mathfrak{D}' \times \mathfrak{D}''$.

Если, кроме того, мы будем писать $\mathfrak{D}' + \mathfrak{D}''$ для приводимого представления, вполне распадающегося на $\mathfrak{D}'$ и $\mathfrak{D}''$, и условимся считать

[1]) Переменные предполагаются перестановочными с коэфициентами и друг с другом.

эквивалентные представления одинаковыми, то легко видеть, что для суммы и произведения представлений будут иметь место все обычные законы:

$$\mathfrak{D}' + \mathfrak{D}'' = \mathfrak{D}'' + \mathfrak{D}', \quad \mathfrak{D}' \times \mathfrak{D}'' = \mathfrak{D}'' \times \mathfrak{D}',$$
$$\mathfrak{D}' + (\mathfrak{D}'' + \mathfrak{D}''') = (\mathfrak{D}' + \mathfrak{D}'') + \mathfrak{D}''',$$
$$\mathfrak{D}' \times (\mathfrak{D}'' \times \mathfrak{D}''') = (\mathfrak{D}' \times \mathfrak{D}'') \times \mathfrak{D}''',$$
$$\mathfrak{D}' \times (\mathfrak{D}'' + \mathfrak{D}''') = \mathfrak{D}' \times \mathfrak{D}'' + \mathfrak{D}' \times \mathfrak{D}''',$$
$$(\mathfrak{D}'' + \mathfrak{D}') \times \mathfrak{D}' = \mathfrak{D}'' \times \mathfrak{D}' + \mathfrak{D}''' \times \mathfrak{D}'.$$

Если в частности $\mathfrak{G}$ — конечная группа, так что всякое представление вполне разлагается на неприводимые представления $\mathfrak{D}_\nu$, то

$$\mathfrak{D}_\lambda \times \mathfrak{D}_\mu = \sum_\nu c_{\lambda\mu}^\nu \mathfrak{D}_\nu, \tag{3}$$

где $c_{\lambda\mu}^\nu$ — целое число, большее или равное нулю. Поэтому представления $\mathfrak{D}_\nu$ можно рассматривать как образующие коммутативной гиперкомплексной системы $\mathfrak{H}$.

Из (3) для следов вытекает, что

$$S_\lambda(a) \cdot S_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu S_\nu(a).$$

Если представления абсолютно неприводимы, то следы будут характерами, а потому в этом случае можно написать:

$$\chi_\lambda(a) \cdot \chi_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu \chi_\nu(a) \text{ (}\textit{первое соотношение между характерами}\text{)}. \tag{4}$$

Характеры как функции классов. Если a и a' — сопряженные элементы группы:

$$a' = bab^{-1},$$

то для матриц представления следует:

$$A' = BAB^{-1}.$$

Отсюда A и A' имеют одинаковые следы, т. е.

$$S(bab^{-1}) = S(a);$$

в частности

$$\chi(bab^{-1}) = \chi(a).$$

Если мы все элементы группы, сопряженные a, отнесем к одному *классу* $\mathfrak{K}_a$, то каждый из характеров для всех элементов одного класса будет иметь одно и то же значение.

Если h_a — число элементов класса $\mathfrak{K}_a$ и k_a — сумма элементов этого класса (в групповом кольце $\mathfrak{o}$), то характер k_a равен сумме характеров элементов класса, откуда

$$\chi(k_a) = h_a \cdot \chi(a).$$

Как мы видели в § 125, величины k_a порождают центр $\mathfrak{Z}$ группового кольца $\mathfrak{o}$. Согласно же § 123 гомоморфизмы Θ_ν центра $\mathfrak{Z}$ связаны с характерами χ_ν равенствами [1])

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu},$$

где $n_\nu = \chi_\nu(1)$ — степень абсолютно неприводимого представления $\mathfrak{D}_\nu$; в частности

$$\Theta_\nu(k_a) = \frac{\chi_\nu(k_a)}{n_\nu} = \frac{h_a}{n_\nu}\chi_\nu(a). \tag{5}$$

Произведение $k_a k_b$ равно сумме элементов группы, которая также принадлежит центру $\mathfrak{Z}$, и потому целочисленно выражается через сумму классов k_a:

$$k_a \cdot k_b = \sum_c g_{ab}^c k_c. \tag{6}$$

Отсюда для гомоморфизмов Θ_ν имеем:

$$\Theta_\nu(k_a)\cdot\Theta_\nu(k_b) = \sum_c g_{ab}^c \Theta_\nu(k_c). \tag{7}$$

Это равенство с помощью (5) переписывается следующим образом:

$$h_a h_b \chi_\nu(a)\chi_\nu(b) = n_\nu \sum_c g_{ab}^c h_c \chi_\nu(c) \quad \left\{ \begin{array}{l} (\textit{второе соотношение} \\ \textit{между характерами}). \end{array} \right. \tag{8}$$

В суммах (6), (7) и (8) c пробегает систему вычетов всех классов. Если c станет пробегать все элементы группы, то в правой части (8) множитель h_c надо откинуть. Так как Θ_ν — единственные гомоморфизмы центра $\mathfrak{Z}$, то характеры χ_ν являются единственными решениями уравнения (8).

(7) вместе с (6) выражает, что $\Theta_\nu(k_a)$ при постоянном ν образует гомоморфизм центра $\mathfrak{Z}$. Точно так же (4) в сочетании с (3) означает, что $\chi_\nu(a)$ при постоянном a, рассматриваемая как функция $\mathfrak{D}_\nu$, является гомоморфизмом кольца $\mathfrak{H}$ в поле Ω: произведению двух представлений соответствует произведение характеров, а сумме — сумма. Таким образом два коммутативных кольца $\mathfrak{Z}$, $\mathfrak{H}$ взаимны друг к другу; любой элемент базиса k_a центра $\mathfrak{Z}$ определяет гомоморфизм $\chi_\nu(a)$ кольца $\mathfrak{H}$, а любой элемент базиса $\mathfrak{D}_\nu$ кольца $\mathfrak{H}$ определяет гомоморфизм $\Theta_\nu(k_a)$ центра $\mathfrak{Z}$. При этом Θ_ν и χ_ν связаны простым равенством (5). Число найденных подобным образом гомоморфизмов $\mathfrak{H}$ равно числу классов, т. е. равно рангу группы $\mathfrak{H}$. Отсюда следует, что $\mathfrak{H}$ есть система без радикала, так как если бы $\mathfrak{H}$ имело радикал $\mathfrak{c}$, то число возможных гомоморфизмов или представлений первой степени $\mathfrak{H}$ было бы равно рангу $\mathfrak{H}/\mathfrak{c}$. Отсюда вместе с тем получается, что $\chi_\nu(a)$ *исчерпывают все* гомоморфизмы группы $\mathfrak{H}$ в Ω.

[1]) Здесь мы также предполагаем, что ни порядок группы h, ни степени n_ν представлений не делятся на характеристику поля.

Сопряженные характеры. Для всякого представления $a \to A$ существует *сопряженное* (или *контрагредиентное*) *представление* $a \to A'^{-1}$, где A' — транспонированная матрица A. При таком соответствии

$$ab \to (AB)'^{-1} = (B'A')^{-1} = A'^{-1} B'^{-1}.$$

Кроме того $(A')' = A$. Если представление $a \to A$ приводимо, то сопряженное также приводимо, и обратно. Таким образом сопряженное неприводимого представления также неприводимо.

Если от A перейти к эквивалентному представлению $P^{-1}AP$, то сопряженное представление перейдет в

$$(P^{-1}AP)'^{-1} = P'A'^{-1}P'^{-1},$$

т. е. мы получим также эквивалентное представление.

Если мы обозначим через $\mathfrak{D}_{\nu'}$ неприводимое представление, сопряженное $\mathfrak{D}_\nu$ и $\mathfrak{D}_\nu(a) = A$, то

$$\mathfrak{D}_{\nu'}(a^{-1}) = A',$$

и так как след A' равен следу A, то

$$\chi_{\nu'}(a^{-1}) = \chi_\nu(a).$$

Обозначим характер $\chi_{\nu'}$, *сопряженный* к характеру χ_ν, через $\bar{\chi}_\nu$.

Характер равен сумме корней из единицы. В самом деле, любой элемент a группы $\mathfrak{G}$ порождает циклическую подгруппу $\mathfrak{G}_1$, порядок которой m является делителем числа h, а любое неприводимое представление $\mathfrak{D}_\nu$ группы $\mathfrak{G}$ определяет представление $\mathfrak{G}_1$; это представление в силу § 124 вполне разлагается на представления первой степени; элементы матриц этих представлений равны m-м корням из единицы. След матрицы представления равен сумме диагональных элементов, т. е. сумме m-х корней из единицы:

$$\chi(a) = \zeta^{\nu_1} + \zeta^{\nu_2} + \ldots + \zeta^{\nu_n}, \tag{9}$$

где ζ — примитивный m-й корень из единицы.

Транспонированная матрица A', если записать A в указанной выше диагональной форме, равна A, а A'^{-1} получается при замене ζ через ζ^{-1}.

Таким образом

$$\bar{\chi}_a = \zeta^{-\nu_1} + \zeta^{-\nu_2} + \ldots + \zeta^{-\nu_n}.$$

В случае числового поля $\bar{\chi}$ является сопряженно комплексным с χ.

Замена ζ через ζ^{-1} дает начало автоморфизму поля m-х корней из единицы, который переводит χ в $\bar{\chi}$. Аналогичным образом из характера χ при произвольном автоморфизме поля получается алгебраически сопряженный характер χ^*, которому отвечает также алгебраически сопряженное представление, так как всякий изоморфизм поля характеров может быть продолжен до изоморфизма поля представлений. χ^* сопряжено с χ в алгебраическом смысле.

Дальнейшие соотношения между характерами. Если $S(c)$ есть след элемента группы c в правильном представлении, то

$$S(c)=\sum_{\nu} n_\nu \chi_\nu(c),$$

так как правильное представление содержит неприводимое представление $\mathfrak{D}_\nu$ ровно n_ν раз. Но след $S(c)$ можно вычислить и непосредственно: элементы группы $a_1, \ldots, a_h$ образуют базис векторного пространства о правильного представления, причем имеет место

$$ca_i = a_k.$$

Члены с $i=k$ встречаются только тогда, если c равно единице 1 группы; в этом случае любое i равно соответствующему k. Таким образом

$$S(1)=h; \quad S(c)=0 \quad \text{для } c \neq 1,$$

откуда

$$\sum_{\nu} n_\nu \chi_\nu(c) = \begin{cases} h & \text{для } c=1, \\ 0 & \text{для } c \neq 1. \end{cases} \tag{10}$$

Если просуммировать (8) по всем ν и принять во внимание (10), то получится:

$$h_a h_b \sum_{\nu} \chi_\nu(a)\chi_\nu(b) = g^1_{ab} \cdot h. \tag{11}$$

Число g^1_{ab} выражает, сколько раз произведение $a'b'$ принимает значение 1, где a' принадлежит классу $\mathfrak{K}_a$ и b' классу $\mathfrak{K}_b$. Таким образом это число равно нулю, если $\mathfrak{K}_a$ и $\mathfrak{K}_b$ не содержат элементов, обратных относительно друг друга.

Но если такая пара существует, например если $b=a^{-1}$, то для всякого элемента $a'=cac^{-1}$ класса $\mathfrak{K}_a$ найдется обратный элемент $b'=a'^{-1}=cbc^{-1}$ класса $\mathfrak{K}_b$, откуда

$$g^1_{ab} = h_a = h_b.$$

Отсюда, разделив (11) на h_b, получим:

$$h_a \sum_{\nu} \chi_\nu(a)\chi_\nu(b) = \begin{cases} h & \text{для } \mathfrak{K}_b = \mathfrak{K}_a{}^{-1} \text{ (\textit{третье соотношение}} \\ 0 & \text{для } \mathfrak{K}_b \neq \mathfrak{K}_a{}^{-1} \textit{ между характерами}). \end{cases} \tag{12}$$

Равенство (10) получается как частный случай при $a=1$.

Пусть теперь $a_1, \ldots, a_s$ — система представителей всех классов. Если положить

$$\chi_{\nu\mu} = \chi_\nu(a_\mu),$$

$$\eta_{\mu\nu} = \frac{h_\mu}{h}\overline{\chi}_\nu(a_\mu) = \frac{h_\mu}{h}\chi_\nu(a_\mu^{-1}),$$

то равенство (12) означает, что матрицы $\Xi=(\chi_{\mu\nu})$ и $\Upsilon=(\eta_{\mu\nu})$ обратны друг другу:

$$\Upsilon\Xi = E \text{ или } \Upsilon = \Xi^{-1}. \tag{13}$$

Из (13) следует, что

$$\Xi\Upsilon = E$$

или

$$\frac{1}{h}\sum_{\mathfrak{K}_a} h_a \chi_\nu(a)\bar{\chi}_\mu(a) = \begin{cases} 1 \text{ для } \nu = \mu, \\ 0 \text{ для } \nu \neq \mu. \end{cases} \tag{14}$$

При этом a пробегает систему представителей всех классов.

Если a пробегает все элементы группы, то множители h_a должны исчезнуть. Отсюда вытекает *ортогональность характеров*:

$$\sum_{a\in\mathfrak{G}} \bar{\chi}_\mu(a)\chi_\nu(a) = \begin{cases} h \text{ для } \nu = \mu & (\textit{четвертое соотношение} \\ 0 \text{ для } \nu \neq \mu & \textit{между характерами}). \end{cases} \tag{15}$$

Если в частности $\mu = 0$, т. е. χ_μ равно характеру χ_0 тождественного представления, то из (15) получается:

$$\sum_\nu \chi_\nu(a) = \begin{cases} h \text{ для } \nu = 0, \\ 0 \text{ для } \nu \neq 0. \end{cases} \tag{16}$$

Равенство (15) можно использовать для вычисления коэфициентов $c_{\lambda\mu}^{\nu}$ (4), умножив для этого (4) на $\bar{\chi}_\varkappa(a)$ и просуммировав по всем a. Это дает:

$$\sum_a \bar{\chi}_\varkappa(a)\chi_\lambda(a)\chi_\mu(a) = hc_{\lambda\mu}^{\varkappa}.$$

Если заменим $\varkappa$ через $\varkappa'$, где $\mathfrak{D}_{\varkappa'}$ — представление, сопряженное с $\mathfrak{D}_\varkappa$, то получится:

$$\sum_a \chi_\varkappa(a)\chi_\lambda(a)\chi_\mu(a) = hc_{\lambda\mu}^{\varkappa'}.$$

Отсюда следует, что *коэфициент* $c_{\lambda\mu}^{\varkappa'}$, *показывающий с какой кратностью содержится в произведении* $\mathfrak{D}_\lambda \times \mathfrak{D}_\mu$ *представление, сопряженное* $\mathfrak{D}_\varkappa$, *симметричен относительно индексов* λ, μ, $\varkappa$.

Идемпотентные элементы $e_1, \ldots, e_s$ центра, порождающие двусторонне простые идеалы в $\mathfrak{o}$, можно определить, пользуясь равенствами $\Xi\Upsilon = E$ и $\Upsilon\Xi = E$. А именно, в силу § 122 имеем следующие выражения для элементов k_a базиса центра $\mathfrak{Z}$:

$$k_a = \sum_\nu e_\nu \Theta_\nu(k_a) = \sum_\nu e_\nu \frac{h_a}{n_\nu}\chi_\nu(a). \tag{17}$$

Умножив на $\bar{\chi}_\mu(a)$ и суммируя по всем классам $\mathfrak{K}_a$, получим:

$$\sum_{\mathfrak{K}_a} k_a \bar{\chi}_\mu(a) = e_\mu \cdot \frac{h}{n_\mu},$$

или

$$e_\nu = \sum_{\mathfrak{K}_a} k_a \frac{n_\nu}{h}\chi_\nu(a^{-1}).$$

Теорема. *Степень неприводимого представления конечной группы в поле всех алгебраических чисел является делителем порядка группы.*

Доказательство. Если в (7) элемент b^* пробегает систему представителей всех классов и $\Theta_\nu(k_a)$ в левой части считается известной, то мы будем иметь однородную систему уравнений относительно $\Theta_\nu(k_c)$; исключая эти величины, получим:

$$\left| \delta_b^c \Theta_\nu(k_a) - g_{ab}^c \right| = 0$$

(a — постоянное число, а b и c — индексы соответственно строки и столбца), причем

$$\delta_b^c = \begin{cases} 1 \text{ для } b = c, \\ 0 \text{ для } b \neq c. \end{cases}$$

Следовательно, $\Theta_\nu(k_a)$ как корень уравнения с целыми рациональными коэфициентами и со старшим коэфициентом, равным единице, есть целое алгебраическое число. Точно так же из (4) следует, что характеры $\chi_\nu(a)$ суть целые алгебраические числа; но в этом можно убедиться также из (9). Теперь первая половина (14) записывается следующим образом:

$$\frac{n_\nu}{h} \sum_{\mathfrak{K}_a} \Theta_\nu(k_a) \overline{\chi}_\mu(a) = 1 \qquad \text{при } \mu = \nu,$$

или

$$\sum_{\mathfrak{K}_a} \Theta_\nu(k_a) \chi_\nu(a^{-1}) = \frac{h}{n_\nu}.$$

Слева стоит целое алгебраическое число; следовательно, и $\frac{h}{n_\nu}$ — также целое алгебраическое число, т. е. $\frac{h}{n_\nu}$ — целое рациональное число, что и требовалось показать.

Литература. I. Schur, Neue Begründung der Theorie der Gruppencharaktere, Sitzungsber., Berlin 1905. Здесь можно найти обоснование теории представлений конечных групп, независимое от теории гиперкомплексных чисел. Из многочисленной литературы, посвященной групповым характерам, мы здесь укажем только важную работу G. Frobenius, Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen, Sitzungsber., Berlin 1898. См. затем H. Weyl, Gruppentheorie und Quantenmechanik, 2. Aufl., Leipzig 1931.

Задачи. 1. Составить таблицу характеров симметрических групп трех и четырех элементов и вычислить идемпотентные элементы центра группового кольца.

2. Показать, что равенство (8) может быть также записано следующим образом:

$$h\chi_\nu(a)\chi_\nu(b) = n_\nu \sum_d \chi_\nu(adbd^{-1}).$$

3. Представление $\mathfrak{D}_\lambda \times \mathfrak{D}_\mu$ тогда и только тогда содержит тождественное представление и притом лишь один раз, если представления $\mathfrak{D}_\lambda$ и $\mathfrak{D}_\mu$ сопряжены относительно друг друга.

4. В поле комплексных чисел представление, сопряженно-комплексное с некоторым представлением, эквивалентно с сопряженным.

§ 127. ПРЕДСТАВЛЕНИЕ СИММЕТРИЧЕСКИХ ГРУПП [1])

Рассмотрим группу $\mathfrak{S}_n$ перестановок n цифр 1, 2, ..., n и найдем ее абсолютно неприводимые представления в поле Ω всех алгебраических чисел. Впрочем, окажется, что эти представления рациональны, т. е. лежат в поле Γ рациональных чисел.

Будем исходить из группового кольца $\mathfrak{o} = s_1\Omega + \ldots + s_{n!}\Omega$ и рассмотрим его левые идеалы. Каждый из этих левых идеалов равен прямой сумме минимальных левых идеалов; эти минимальные идеалы и определяют нам непроводимые представления. Так как всякий левый идеал порождается идемпотентным элементом, то мы прежде всего найдем идемпотентные элементы.

Разместим цифры 1, 2, ..., n в каком-нибудь порядке в h строках (h произвольно) так, чтобы в ν-й строке стояло α_ν цифр и чтобы имело место

$$\left.\begin{aligned} &\alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_h, \\ &\sum_{\nu=1}^{h} \alpha_\nu = n. \end{aligned}\right\} \tag{1}$$

Первые элементы h строк расположим один под другим; точно так же расположим вторые элементы и т. д.; например, для $n = 7$ расположим элементы так:

$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \\ \cdot & \cdot & \end{matrix} \qquad (\alpha_1, \alpha_2, \alpha_3) = (3, 2, 2),$$

причем точки представляют цифры.

Такое расположение цифр 1, 2, ..., n мы назовем *схемой* Σ_α. Индекс α относится к последовательности цифр $(\alpha_1, \alpha_2, \ldots, \alpha_h)$. Всевозможные индексы α упорядочим следующим образом: $\alpha > \beta$, если первая неисчезающая разность $\alpha_\nu - \beta_\nu$ положительна. Например, при $n = 5$

$$(5) > (4, 1) > (3, 2) > (3, 1, 1) > (2, 2, 1) > (2, 1, 1, 1) > (1, 1, 1, 1, 1).$$

Если дана схема Σ_α, то через p мы обозначим все перестановки, которые перемещают только цифры строк схемы, в то время как сами эти строки остаются неподвижными; буквами же q мы обозначим перестановки, перемещающие только цифры столбцов схемы. Для всякого заданного q мы под σ_q будем подразумевать число $+1$ или -1 в зависимости от того, будет ли q четной или нечетной перестановкой. Если s — какая-нибудь перестановка, то через $s\Sigma_\alpha$ мы обозначим схему, в которую переходит Σ_α при перестановке s. Легко видеть, что если q не перемещает столбцов схемы Σ_α, то sqs^{-1} не перемещает столбцов схемы $s\Sigma_\alpha$, и обратно. Наконец, для данной схемы Σ_α положим (в групповом кольце $\mathfrak{o}$)

$$S_\alpha = \sum_p p,$$

$$A_\alpha = \sum_q q\sigma_q .$$

---

[1]) Приведенное в этом параграфе более простое обоснование теории Фробениуса (Sitzungsber., Berlin 1903, стр. 328) было мне сообщено Нейманом (J. Neumann).

Легко показать, что

$$pS_\alpha = S\ p = S_\alpha, \tag{2}$$

$$A_\alpha q \sigma_q = q A_\alpha \sigma_q = A_\alpha. \tag{3}$$

Из (2) и (3) легко вытекает, что S_α и A_α идемпотентны с точностью до множителя f. Дальнейшие алгебраические свойства S_α и A_α вытекают из следующей *комбинаторной леммы*:

Пусть Σ_α и Σ_β — две схемы указанного выше рода; пусть $\alpha \geqslant \beta$ Если в Σ_α в одной строке никогда не встречаются две цифры, стоящие в Σ_β в одном столбце, то $\alpha = \beta$, и схема Σ_α с помощью перестановки вида pq переходит в схему Σ_β:

$$pq\,\Sigma_\alpha = \Sigma_\beta$$

(*p оставляет на месте строки, а q — столбцы Σ_α*).

Доказательство. Из $\alpha \geqslant \beta$ следует $\alpha_1 \geqslant \beta_1$. В первой строке Σ_α стоит α_1 цифр. Так как эти цифры находятся все в различных столбцах схемы Σ_β, то Σ_β должно иметь по меньшей мере α_1 столбцов, откуда $\alpha_1 \leqslant \beta_1$, и потому $\alpha_1 = \beta_1$. С помощью перестановки q_1', оставляющей на месте столбцы Σ_β, можно передвинуть эти цифры в первую строчку Σ_β.

Теперь из $\alpha \geqslant \beta$ следует, что $\alpha_2 \geqslant \beta_2$. Во второй строке Σ_α стоит α_2 цифр. Так как эти цифры находятся все в различных столбцах $q_1' \Sigma_\beta$, то $q_1' \Sigma_\beta$, не считая первой строки, должна содержать по меньшей мере α_2 столбцов. Отсюда следует, что $\alpha_2 \leqslant \beta_2$, откуда $\alpha_2 = \beta_2$. С помощью перестановки q_2', оставляющей на месте столбцы $q_1' \Sigma_\beta$, а также первую строку, можно перенести указанные цифры во вторую строку Σ_β.

Продолжая этот процесс, получим, наконец, схему $q'\,\Sigma_\beta = q_h' \ldots q_2' q_1' \Sigma_\beta$, строки которой совпадают со строками Σ_α. Следовательно, Σ_α с помощью перестановки p можно перевести в $q'\,\Sigma_\beta$:

$$q'\,\Sigma_\beta = p\,\Sigma_\alpha.$$

Перестановка $q' = q_h' \ldots q_2' q_1'$ оставляет на месте столбцы Σ_β, а потому также столбцы $q'\,\Sigma_\beta = p\,\Sigma_\alpha$. Таким образом при соответственно выбранном q имеет место

$$q' = pq^{-1} p^{-1},$$

а потому

$$pq^{-1} p^{-1}\,\Sigma_\beta = p\Sigma_\alpha,$$

$$\Sigma_\beta = pq\,\Sigma_\alpha,$$

что и требовалось доказать.

Из комбинаторной леммы прежде всего следует, что

$$A_\beta S_\alpha = 0 \quad \text{для} \quad \alpha > \beta. \tag{4}$$

Действительно в силу леммы в случае $\alpha > \beta$ должна существовать пара цифр, стоящая в одной строке Σ_α и в одном столбце Σ_β. Если t — транспозиция, которая переставляет эту пару цифр, то в силу (2) и (3) имеет место

$$A_\beta S_\alpha = A_\beta\, tt^{-1} S_\alpha = -A_\beta S_\alpha,$$

откуда следует (4).

Точно так же можно доказать, что

$$S_\alpha A_\beta = 0 \quad \text{для} \quad \alpha > \beta.$$

Но все $sA_\beta s^{-1}$ также будут уничтожаться при умножении на S_α:

$$S_\alpha s A_\beta s^{-1} = 0 \quad \text{для} \quad \alpha > \beta,$$

так как $sA_\beta s^{-1}$ есть не что иное, как некоторое A_β, но только соответствующее схеме $s\,\Sigma_\beta$. Отсюда после умножения на $s\Omega$ и суммирования по всем s из $\mathfrak{G}$ получим:

$$S_\alpha (\Sigma\ s\Omega)\, A_\beta = (0),$$

или

$$S_\alpha \mathfrak{o} A_\beta = (0) \qquad (\alpha > \beta). \tag{5}$$

Левый идеал $\mathfrak{o}A_\beta$ при $\beta < \alpha$ будет уничтожаться при умножении на S_α; иными словами, S_α будет изображаться нулем в представлении, соответствующем идеалу $\mathfrak{o}A_\beta$. С другой стороны, $S_\alpha A_\alpha \neq 0$, так как коэфициент при единице в произведении $S_\alpha A_\alpha$ не равен нулю. Таким образом S_α не будет изображаться нулем в представлении, связанном с $\mathfrak{o}A_\alpha$, отсюда следует, что это представление содержит по крайней мере одну неприводимую составную часть, которая наверное не встречается ни в одном из $\mathfrak{o}A_\beta$ ($\beta < \alpha$). Эту неприводимую часть мы и собираемся сейчас определить.

В силу (2) и (3) элемент

$$S_\alpha A_\alpha = \sum_p \sum_q pq\sigma_q$$

удовлетворяет равенству:

$$pS_\alpha A\ q\sigma_q = S_\alpha A_\alpha .$$

Докажем, что $S_\alpha A_\alpha$ с точностью до множителя является единственным элементом, удовлетворяющим этому равенству; иными словами, мы докажем, что *если для элемента a кольца* $\mathfrak{o}$ имеет место

$$paq\sigma_q = a \tag{6}$$

для всех p и q, то a должно иметь вид $(S_\alpha A_\alpha)\cdot\lambda$.

Доказательство. Положим

$$a = \sum_s s\gamma_s \qquad (\gamma_s \in \Omega). \tag{7}$$

Подставляя (7) в (6), получим:

$$\sum_s s\gamma_s = \sum_s psq\sigma_q\gamma_s. \tag{8}$$

В левой части встречается только один член с pq, а именно $pq\gamma_{pq}$, в правой части встречается только один член с pq, а именно член, для которого $s = 1$. Сравнивая коэфициенты, получим:

$$\gamma_{pq} = \sigma_q\gamma_1.$$

Возьмем теперь s, которое не имеет вида pq. Тогда $s\Sigma_\alpha$ будет отлично от всех $pq\,\Sigma_\alpha$, и согласно комбинаторной лемме существуют две цифры j, k,

стоящие в Σ_α в одной строке, а в $s\Sigma_\alpha$ в одном столбце. Если t есть транспозиция этих цифр: $t=(jk)$, то $t'=s^{-1}ts$ перемещает только цифры $s^{-1}j$ и $s^{-1}k$, которые в $s^{-1}s\,\Sigma_\alpha=\Sigma_\alpha$ стоят в одном столбце. Поэтому t есть перестановка типа p, а t' — перестановка типа q, и мы можем положить в (8) $p=t$ и $q=t'$; тогда для наших частных s

$$psq=tss^{-1}ts=s,$$
$$\sigma_q=-1;$$

следовательно, сравнивая в (8) члены, содержащие s, справа и слева, получим:

$$\gamma_s=-\gamma_s,\quad \gamma_s=0.$$

Таким образом в (7) могут входить только члены с $s=pq$, $\gamma_s=\sigma_q\gamma_1$, а потому

$$a=\sum_{p,q} pq\sigma_q\gamma_1=(S_\alpha A_\alpha)\gamma_1,$$

что и требовалось доказать.

Из вышедоказанного сразу следует, что для всякого элемента b из $\mathfrak{o}$ элемент $S_\alpha bA_\alpha$ имеет вид $(S_\alpha A_\alpha)\lambda$, так как для любого p и q имеет место

$$pS_\alpha bA_\alpha q\sigma_q=S_\alpha bA_\alpha.$$

Таким образом

$$S_\alpha\mathfrak{o}A_\alpha\subseteq(S_\alpha A_\alpha)\Omega.$$

Если положить

$$S_\alpha A_\alpha=I_\alpha,$$

то мы получим:

$$I_\alpha\mathfrak{o}I_\alpha\subseteq S_\alpha\mathfrak{o}A_\alpha\subseteq I_\alpha\Omega. \tag{9}$$

Теперь мы утверждаем, что $\mathfrak{o}I_\alpha$ есть минимальный левый идеал. В самом деле, если $\mathfrak{l}$ есть под-идеал идеала $\mathfrak{o}I_\alpha$, то из (9) следует, что

$$I_\alpha\mathfrak{l}\subseteq I_\alpha\Omega,$$

откуда, так как $I_\alpha\Omega$ одночленный и потому минимальный Ω-модуль, либо

$$I_\alpha\mathfrak{l}=I_\alpha\Omega,$$

либо

$$I_\alpha\mathfrak{l}=(0).$$

В первом случае

$$\mathfrak{o}I_\alpha=\mathfrak{o}I_\alpha\Omega\subseteq I_\alpha\mathfrak{l}\subseteq\mathfrak{l},$$

откуда

$$\mathfrak{l}=\mathfrak{o}I_\alpha.$$

Во втором случае

$$\mathfrak{l}^2\subseteq\mathfrak{o}I_\alpha\mathfrak{l}=(0),$$

откуда, так как, кроме (0), не существует нильпотентных идеалов $\mathfrak{l}=(0)$.

При $\alpha>\beta$ минимальные левые идеалы $\mathfrak{o}I_\alpha$ и $\mathfrak{o}I_\beta$ не операторно-изоморфны. Действительно, при $\alpha>\beta$ в силу (5) имеет место

$$S_\alpha\mathfrak{o}I_\beta=S_\alpha\mathfrak{o}S_\beta A_\beta\subseteq S_\alpha\mathfrak{o}A_\beta=(0),$$

откуда для любого a', из $\mathfrak{o}I_\beta$

$$S_\alpha a'=0.$$

Если бы теперь имело место $\mathfrak{o}I_\alpha\cong\mathfrak{o}I_\beta$, то для всякого a из $\mathfrak{o}I_\alpha$ мы бы имели также

$$S_\alpha a=0,$$

но это невозможно для

$$a=I_\alpha=S_\alpha A_\alpha,$$

так как

$$S_\alpha^2 A_\alpha = f_\alpha S_\alpha A_\alpha \neq 0.$$

Всякий левый идеал $\mathfrak{o}I_\alpha$ соответствует неприводимому представлению $\mathfrak{D}_\alpha$, а эти представления согласно только что приведенному замечанию для различных α неэквивалентны.

Число найденных подобным образом представлений $\mathfrak{D}_\alpha$ равно числу решений уравнения (1) [1]). Но это число вместе с тем определяет число классов сопряженных перестановок, так как каждый из таких классов состоит из всех элементов, распадающихся на циклы определенной длины $\alpha_1, \alpha_2, \ldots, \alpha_h$, а эти длины мы можем также упорядочить сообразно условиям (1). Но так как число *всех* неэквивалентных неприводимых представлений равно числу классов сопряженных перестановок, то оказывается, *что представления* $\mathfrak{D}_\alpha$ *с точностью до эквивалентности исчерпывают все неприводимые представления симметрической группы* $\mathfrak{S}_n$.

Минимальные левые идеалы $\mathfrak{o}I_\alpha$ определялись выше рационально. Отсюда и следует рациональность неприводимых представлений (а также характеров).

Читателя, интересующегося точным вычислением характеров и степеней представлений, мы отсылаем к трудам Фробениуса [2]), Вейля [3]) и Шура [4]).

§ 128. ПРИЛОЖЕНИЕ ТЕОРИИ ПРЕДСТАВЛЕНИЯ К ТЕОРИИ НЕКОММУТАТИВНЫХ ПОЛЕЙ [5])

Мы уже заметили в § 120, что всякое представление гиперкомплексной системы $\mathfrak{S}$ в коммутативном поле K, содержащем основное поле P, связано с представлением расширенной системы $\mathfrak{S}_\mathsf{K}$. На языке теории модулей представлений это означает, что любой модуль, для которого $\mathfrak{S}$ образует левую, а K — правую мультипликаторную область, можно рассматривать также как левый $\mathfrak{S}_\mathsf{K}$ — модуль. В самом деле, если положить $\mathfrak{S} = a_1\mathsf{P} + \ldots + a_n\mathsf{P}$ и тем самым $\mathfrak{S}_\mathsf{K} = a_1\mathsf{K} + \ldots + a_n\mathsf{K}$, то для элемента m модуля левое умножение на элемент $\mathfrak{S}_\mathsf{K}$ будет определяться равенством

$$(a_1\varkappa_1 + \ldots + a_n\varkappa_n)\, m = a_1 m\varkappa_1 + \ldots + a_n m\varkappa_n.$$

Без особых трудностей можно проверить для $\mathfrak{S}_\mathsf{K}$-модуля правила оперирования; только при выводе ассоциативного закона

$$(bc)\, m = b\,(cm)$$

придется обратиться к коммутативности. Именно, если $b = a_1\varkappa_1$, $c = a_2\varkappa_2$ (очевидно, достаточно ограничиться этим частным случаем), то из

$$(a_1\varkappa_1 \cdot a_2\varkappa_2)\, m = (a_1 a_2 \varkappa_1\varkappa_2)\, m = (a_1 a_2)\, m\,(\varkappa_1\varkappa_2),$$
$$a_1\varkappa_1\,(a_2\varkappa_2 \cdot m) = a_1\varkappa_1\,(a_2 m\varkappa_2) = a_1\,(a_2 m\varkappa_2)\,\varkappa_1 = (a_1 a_2)\, m\,(\varkappa_2\varkappa_1)$$

следует ассоциативный закон, так как $\varkappa_1\varkappa_2 = \varkappa_2\varkappa_1$.

Однако в случае некоммутативного поля все же можно спасти положение, воспользовавшись понятием *обратного кольца* (*поля*) (см. § 118). Обозначим через $\mathfrak{R}'$ кольцо, обратное $\mathfrak{R}$; заметим, что если $\mathfrak{R}$ образует гиперкомплексную систему относительно коммутативного поля P, то $\mathfrak{R}'$ так же можно рассматривать как гиперкомплексную систему относительно P.

---

[1]) Именно, каждому решению уравнения (1) соответствуют различные схемы, которые различаются только расположением цифр и могут давать различные p_α; достаточно для каждого α выбрать одно p_α.

[2]) Frobenius: „Sitzungsber.“, Berlin 1900, стр. 516.

[3]) Weyl, H: „Math. Zeitschr.“, 23, 1925, стр. 271.

[4]) Schur, I.: „Sitzungsber.“, Berlin 1927, стр. 58.

[5]) Выводы, приведенные в этом параграфе, имеют своим первоисточником лекции Э. Нётер, посвященные некоммутативной алгебре (Гёттинген, лето 1928 г.); см. также „Math. Zeitschr.“, 1929.

Модуль, имеющий $\mathfrak{S}$ *левой и* $\mathfrak{K}$ *правой мультипликаторной областью, где* $\mathfrak{S}$ *и* $\mathfrak{K}$ *— гиперкомплексные системы относительно одного и того же основного поля* $\mathfrak{P}$ [1]*, можно рассматривать как левый* $(\mathfrak{S} \times \mathfrak{K}')$*-модуль* [2] *(или как правый* $(\mathfrak{S}' \times \mathfrak{K})$*-модуль).*

Доказательство такое же, как и выше. Пусть

$$\mathfrak{S} = a_1\mathfrak{P} + \ldots + a_n\mathfrak{P}$$

и тем самым

$$\mathfrak{S} \times \mathfrak{K}' = a_1\mathfrak{K}' + \ldots + a_n\mathfrak{K}'.$$

Тогда мы полагаем

$$(a_1\varkappa_1' + \ldots + a_n\varkappa_n')\, m = a_1 m\varkappa_1 + \ldots + a_n m\varkappa_n. \qquad (1)$$

Легко проверить справедливость всех обычных законов оперирования. Ассоциативный закон $(bc)\, m = b\,(cm)$ следует из

$$(a_1\varkappa_1' \cdot a_2\varkappa_2')\, m = (a_1 a_2 \varkappa_1'\varkappa_2')\, m = (a_1 a_2)\, m\,(\varkappa_2\varkappa_1),$$

$$a_1\varkappa_1'\,(a_2\varkappa_2' \cdot m) = a_1\varkappa_1'\,(a_2 m\varkappa_2) = a_1\,(a_2 m\varkappa_2)\,\varkappa_1 = (a_1 a_2)\, m\,(\varkappa_2\varkappa_1).$$

Подобным же образом можно, обратно, левый $(\mathfrak{S} \times \mathfrak{K}')$-модуль рассматривать как левый $\mathfrak{S}$-модуль и правый $\mathfrak{K}$-модуль; это следует из определения $m\varkappa = \varkappa' m$. В сущности дело идет о том, чтобы изоморфизмы модулей, возникающие при умножении элементов модуля на элементы поля $\mathfrak{K}'$, можно было писать не только слева, но и справа; надо только иметь в виду, что при правом умножении сомножители должны итти в обратном порядке: чтобы умножить m справа на $\varkappa_1\varkappa_2$, надо сперва умножить справа на $\varkappa_1$ и затем на $\varkappa_2$; напротив, чтобы m умножить слева на $\varkappa_1'\varkappa_2'$, необходимо сперва умножить слева на $\varkappa_2'$ и затем на $\varkappa_1'$. Изоморфным $(\mathfrak{S} \times \mathfrak{K}')$-модулям соответствуют также изоморфные $\mathfrak{S}$-левые и $\mathfrak{K}$-правые модули, и обратно.

Это обстоятельство допускает многообразные приложения. Рассмотрим в частности случай, когда $\mathfrak{K}$ и $\mathfrak{S}$ — простые гиперкомплексные системы [3]) или некоторые поля конечного ранга относительно $\mathfrak{P}$. Допустим, например, что $\mathfrak{P}$ есть центр поля $\mathfrak{K}$ (и тем самым также $\mathfrak{K}'$). Тогда согласно доказанному в § 119 произведение $\mathfrak{S} \times \mathfrak{K}'$ будет также простой системой. Отсюда в силу § 118 и 121 следует, что все неприводимые левые $(\mathfrak{S} \times \mathfrak{K}')$-модули изоморфны друг с другом и с минимальными левыми идеалами $\mathfrak{S} \times \mathfrak{K}'$. Точно так же произведение $\mathfrak{S}' \times \mathfrak{K}$ образует простую систему, в силу чего все правые $\mathfrak{S}' \times \mathfrak{K}$-модули изоморфны друг с другом и с минимальными правыми идеалами в $\mathfrak{S}' \times \mathfrak{K}$. Тем самым нами доказано следующее предложение:

Если $\mathfrak{S}$ *и* $\mathfrak{K}$ *— простые гиперкомплексные системы относительно* $\mathfrak{P}$ *и центр системы* $\mathfrak{K}$ *равен* $\mathfrak{P}$*, то любой минимальный* $\mathfrak{S}$*-левый и* $\mathfrak{K}$*-правый модуль* $\mathfrak{M}$ *(в частности если* $\mathfrak{K}$ *— поле, то любой неприводимый модуль представления* $\mathfrak{S}$ *в* $\mathfrak{K}$*) получается согласно указанному выше правилу из минимального левого идеала в* $\mathfrak{S} \times \mathfrak{K}'$ *или минимального правого идеала в* $\mathfrak{S}' \times \mathfrak{K}$*. Все эти минимальные двойные модули изоморфны между собой.*

Рассмотрим сперва простейший случай, когда $\mathfrak{S}$ и $\mathfrak{K}$ образуют поле и речь идет о модуле представления $\mathfrak{M}$ ранга 1 относительно $\mathfrak{K}$. Тогда соответствующее представление первой степени отображает $\mathfrak{S}$ изоморфно на подполе Σ поля $\mathfrak{K}$. Так как изоморфизм одновременно является и операторным изоморфизмом относительно $\mathfrak{P}$, то элементы $\mathfrak{P}$ будут при этом отображаться сами на себя. С этим ограничением любой изоморфизм $\mathfrak{S} \cong \Sigma \subseteq \mathfrak{K}$ будет связан с модулем представления $\mathfrak{M}$ ранга 1. Из указанной выше теоремы прежде всего следует, что все эти представления эквивалентны между собой. Это значит, что если даны два

---

[1]) $\mathfrak{K}$ может быть также произвольным кольцом расширения $\mathfrak{P}$, содержащим $\mathfrak{P}$ в центре.

[2]) Это значит, что операторы из $\mathfrak{S} \times \mathfrak{K}'$ должны записываться слева от элементов модуля.

[3]) Под простой системой мы будем в дальнейшем все время подразумевать простую гиперкомплексную систему с единицей.

таких представления $\mathfrak{S} \cong \Sigma_1$ и $\mathfrak{S} \cong \Sigma_2$, то соответствующие элементы s_1 из Σ_1 и s_2 из Σ_2 переходят друг в друга с помощью преобразования

$$s_1 = \varkappa s_2 \varkappa^{-1}. \tag{2}$$

Если взять $\mathfrak{S} = \Sigma_1$ и $\Sigma_2 \cong \Sigma_1$, то будем иметь:

Любой изоморфизм двух подполей Σ_1, Σ_2 *поля* K, *который оставляет неподвижными элементы центра* P, *воспроизводится преобразованием* (2) *с элементом* $\varkappa$ *из* K.

В частности всякий автоморфизм поля K, *оставляющий неподвижными элементы* P, *будет внутренним.*

Точно так же можно доказать вообще, рассматривая неприводимый модуль представления произвольного ранга, что всякая простая система $\mathfrak{S}$ относительно P допускает одно и с точностью до эквивалентности (т. е. до внутреннего преобразования полного кольца матриц) только одно неприводимое представление через матрицы поля K произвольной степени, при условии, что P есть центр поля K. В частности любой автоморфизм кольца матриц K_r, оставляющий на месте элементы поля P, будет внутренним.

Посмотрим теперь, каким образом представление $\mathfrak{S} \cong \Sigma$ первой степени может быть связано с правым идеалом системы $\mathfrak{S}' \times K$. Так как это представление первой степени, то правый идеал $\mathfrak{r}$ должен быть ранга 1 относительно K; таким образом

$$\mathfrak{r} = r\mathsf{K}.$$

Согласно нашему правилу, идеал $\mathfrak{r}$ будет левым $\mathfrak{S}$-модулем, если произведение элемента $r\varkappa$ идеала $\mathfrak{r}$ на элемент s из $\mathfrak{S}$ определить следующим образом:

$$s(r\varkappa) = (r\varkappa)s'; \text{ в частности } sr = rs'.$$

Если представить элемент rs' снова в виде $r\sigma$ ($\sigma \in K$), где все элементы $\mathfrak{r}$ могут быть записаны однозначно, то

$$sr = rs' = r\sigma, \tag{3}$$

и соответствие $s \to \sigma$ и будет искомым представлением $\mathfrak{S} \cong \Sigma$.

Теперь легко определить структуру системы $\mathfrak{S}' \times K \cdot \mathfrak{S}' \times K$ изоморфно кольцу матриц поля автоморфизмов $\mathfrak{r}$. Автоморфизм φ вполне определяется равенствами:

$$\varphi(r) = r\varkappa_0, \tag{4}$$

$$\varphi(r\varkappa) = r\varkappa_0\varkappa \quad \text{для} \quad \varkappa \in K. \tag{5}$$

Если имеет место операторный изоморфизм относительно $\mathfrak{S}' \times K$, то достаточно его взять только относительно $\mathfrak{S}'$:

$$\varphi(rs') = \varphi(r)s'.$$

Отсюда с помощью (3), (4), (5) получается:

$$r\varkappa_0\sigma = r\varkappa_0 s' = rs'\varkappa_0 = r\sigma\varkappa_0,$$

откуда

$$\varkappa_0\sigma = \sigma\varkappa_0,$$

т. е. элемент $\varkappa_0$, связанный с автоморфизмом, должен быть перестановочен со всеми элементами σ из Σ. Элементы τ, перестановочные со всеми элементами системы Σ, образуют подполе T поля K. Каждому автоморфизму φ соответствует взаимно однозначно элемент $\varkappa_0$ из T; сумме $\varphi_1 + \varphi_2$ и произведению $\varphi_1\varphi_2$ соответствует сумма $\varkappa_1 + \varkappa_2$ и произведение $\varkappa_1\varkappa_2$:

$$(\varphi_1 + \varphi_2)(r) = \varphi_1(r) + \varphi_2(r) = r\varkappa_1 + r\varkappa_2 = r(\varkappa_1 + \varkappa_2),$$

$$\varphi_1\varphi_2(r) = \varphi_1(r\varkappa_2) = r\varkappa_1\varkappa_2.$$

Таким образом поле автоморфизмов изоморфно T, а $\mathfrak{S}' \times K$ изоморфно кольцу матриц поля T. Тем самым доказано следующее предложение:

Если $\mathfrak{S}'$ обратно-изоморфно подполю Σ из K и T есть совокупность элементов из K, перестановочных со всеми элементами из Σ, то $\mathfrak{S}' \times \mathsf{K}$ изоморфно кольцу матриц поля T.

Эту теорему можно доказать еще короче: $\mathfrak{S}' \times \mathsf{K}$ изоморфно кольцу матриц поля автоморфизмов минимального правого идеала $\mathfrak{r}$. Этому правому идеалу согласно вышеизложенному соответствует $\mathfrak{S}$-левый и K-правый модуль $\mathfrak{M}$ (ранга 1 относительно K). Операторным автоморфизмам $\mathfrak{r}$ соответствуют операторные автоморфизмы двойного модуля $\mathfrak{M}$. Если теперь рассматривать $\mathfrak{M}$ только как K-модуль, то $\mathfrak{M}$ будет модулем линейных форм ранга 1, и его автоморфизмы φ будут линейными преобразованиями, соответствующими матрице (τ), [(τ) состоит из одной строки и одного столбца], где $\tau \in \mathsf{K}$. Умножение элемента $\mathfrak{M}$ слева на элемент s из $\mathfrak{S}$ также определит линейное преобразование $\mathfrak{M}$, связанное с матрицей (σ); соответствие $s \to \sigma$ как раз и будет представлением $\mathfrak{S}$ в Σ, связанным с $\mathfrak{M}$. Если линейное преобразование φ образует операторный изоморфизм двойного модуля $\mathfrak{M}$ также относительно умножения на элементы s из $\mathfrak{S}$, то преобразование φ при таком умножении должно быть перестановочным. Но это возможно тогда и только тогда, если матрицы (τ), (σ) перестановочны:

$$\tau\sigma = \sigma\tau.$$

τ, обладающие этим свойством, образуют поле T. Матрицы (τ), а потому также элементы τ, взаимно однозначно и изоморфно соответствуют автоморфизмам φ двойного модуля $\mathfrak{M}$; поэтому (τ) и τ взаимно однозначно и изоморфно соответствуют автоморфизмам $\mathfrak{r}$.

Буквально так же доказывается более общая теорема:

Если $\mathfrak{S}$ — простая гиперкомплексная система относительно P, K — поле конечной степени с центром P и $\mathfrak{S} \to \Sigma$ — изоморфное неприводимое представление $\mathfrak{S}$ r-й степени через матрицы K, то совокупность матриц, перестановочных со всеми элементами Σ, образует поле T, а $\mathfrak{S}' \times \mathsf{K}$ изоморфно кольцу матриц поля T. Если Σ коммутативно, то $\mathsf{T} \supseteq \Sigma$.

Если теперь вернуться к представлениям $\mathfrak{S} \to \Sigma$ первой степени и положить

$$\left(\frac{\Sigma}{\mathsf{P}}\right) = \sigma; \quad \left(\frac{\mathsf{T}}{\mathsf{P}}\right) = \tau; \quad \left(\frac{\mathsf{K}}{\mathsf{P}}\right) = m^2,$$

то идеал $\mathfrak{r}$ будет ранга 1 относительно K, т. е. ранга m^2 относительно P. Ранг всего кольца $\mathfrak{S}' \times \mathsf{K}$ равен σm^2, откуда число идеалов $\mathfrak{r}$, на которые распадается $\mathfrak{S}' \times \mathsf{K}$, равно σ. Поэтому порядок матриц кольца матриц $\mathfrak{S}' \times \mathsf{K}$ также равен σ, и ранг идеала $\mathfrak{r}$ относительно T точно так же равен σ. Отсюда следует, что ранг идеала $\mathfrak{r}$ относительно P равен $\sigma\tau$; следовательно,

$$\sigma\tau = m^2. \tag{6}$$

Если положить в частности $\Sigma = \mathsf{K}$, то будем иметь $\mathsf{T} = \mathsf{P}$, в силу чего $\mathsf{K} \times \mathsf{K}'$ есть *полное кольцо матриц поля* P.

Если принять за Σ максимальное коммутативное подполе K, то $\mathsf{T} = \Sigma$, так как только элементы поля Σ перестановочны с элементами из Σ. В самом деле, если бы существовал элемент θ, перестановочный с Σ и не содержащийся в Σ, то $\Sigma(\theta)$ было бы также коммутативным, что противоречит максимальности Σ. Таким образом $\mathfrak{S}' \times \mathsf{K} = \mathfrak{S} \times \mathsf{K}$ будет кольцом матриц поля Σ или самого поля $\mathfrak{S}$. Следовательно, $\mathfrak{S}$ есть то, что мы в § 119 назвали *полем разложения* поля K. Из (6) следует в силу $\tau = \sigma$:

$$\sigma^2 = m^2,$$
$$\sigma = m.$$

Итак:

Максимальные коммутативные подполя Σ поля K суть поля разложения, и их степень равна „индексу“ m поля K.

Следует еще отметить, что любой элемент $\varkappa$ из K содержится по крайней мере в одном максимальном коммутативном подполе Σ. Действительно, $\mathsf{P}(\varkappa)$ наверное коммутативно и может быть дополнено до максимального коммутативного поля.

Теперь применим эти теоремы к некоторым частным задачам.

1. *Определить все некоммутативные поля конечной степени относительно поля действительных чисел.*

Если P — поле действительных чисел, K — искомое поле расширения индекса m, Z — центр поля K и Σ — максимальное коммутативное подполе, то

$$\mathsf{P} \subseteq Z \subseteq \Sigma \subset \mathsf{K};$$

$$\left(\frac{\Sigma}{Z}\right) = m; \qquad \left(\frac{\mathsf{K}}{Z}\right) = m^2.$$

Так как K некоммутативно, то $m > 1$. Для полей Z и Σ могут представиться только две возможности: P и $\mathsf{P}(i)$, где $\mathsf{P}(i)$ — поле комплексных чисел, так как другого коммутативного конечного расширения P не имеет. В силу $m > 1$ $\Sigma \neq Z$; следовательно,

$$\Sigma = \mathsf{P}(i), \quad Z = \mathsf{P}, \quad m = 2.$$

Итак, искомое поле K может иметь только степень $m^2 = 4$.

Изоморфизм $\mathsf{P}(i)$, переводящий i в $-i$, должен быть связан с элементом k из K посредством некоторого преобразования, т. е. должно существовать такое k, что

$$kik^{-1} = -i. \tag{7}$$

Так как k не содержится в $\Sigma = \mathsf{P}(i)$, то $\Sigma(k) = \mathsf{K}$; отсюда $\mathsf{K} = \mathsf{P}(i, k)$. Из (7) следует:

$$k^2ik^{-2} = i,$$

т. е. k^2 перестановочно с i. Так как k^2 также перестановочно с k, то k^2 лежит в центре:

$$k^2 = a \in \mathsf{P}.$$

Если

$$a \geqslant 0, \text{ то } a = b^2,$$
$$k^2 - b^2 = (k - b)(k + b) = 0,$$
$$k - b = 0 \text{ или } k + b = 0,$$

т. е. $k \in \mathsf{P}$; но это невозможно. Таким образом должно иметь место $a < 0$; $a = -b^2 (b \neq 0)$. Умножив k на действительный множитель b^{-1}, получим $k^2 = -1$, причем все указанные свойства числа k от этого не нарушатся. Итак, для i и k удовлетворяются следующие равенства:

$$ki = -ik,$$
$$i^2 = k^2 = -1.$$

Это определяет поле кватернионов. *Таким образом поле кватернионов есть единственно возможное некоммутативное поле конечной степени относительно поля действительных чисел.*

2. *Определить все конечные поля* (*поля с конечным числом элементов*).

Если K — конечное поле, Z — его центр, m^2 — ранг K относительно Z, то любой элемент поля K содержится в некотором максимальном коммутативном подполе Σ степени m относительно Z. Все коммутативные расширения Σ m-й степени конечного поля Галуа Z из p^n элементов эквивалентны между собой (именно, они получаются после присоединения всех корней уравнения $x^q = x$, $q = p^{nm}$, см. § 31). Таким образом:

$$\Sigma = \varkappa \Sigma_0 \varkappa^{-1},$$

где Σ_0 — любое из рассматриваемых полей расширения, а $\varkappa$ — соответствующий элемент поля K.

Если выбросить из K нуль, то K станет группой $\mathfrak{G}$, а Σ — подгруппой $\mathfrak{H}$. При этом Σ окажется сопряженной подгруппой $\varkappa\mathfrak{H}\varkappa^{-1}$, и такие сопряженные подгруппы заполнят всю группу $\mathfrak{G}$ (так как любой элемент поля K содержится в одном из Σ). Но теперь можно воспользоваться следующей групповой леммой:

Лемма. *Собственная подгруппа $\mathfrak{H}$ конечной группы $\mathfrak{G}$ не может вместе со своими сопряженными $s\mathfrak{H}s^{-1}$ заполнить всей группы $\mathfrak{G}$.*

Доказательство. Пусть n и N — порядки групп $\mathfrak{H}$ и $\mathfrak{G}$, j — индекс $\mathfrak{H}$, так что $N=j\cdot n$. Если s и s' принадлежат одному и тому же смежному классу $s\mathfrak{H}$, например

$$s'=sh\,(h\in\mathfrak{H}),$$

то

$$s'\mathfrak{H}s'^{-1}=sh\mathfrak{H}h^{-1}s^{-1}=s\mathfrak{H}s^{-1}.$$

Таким образом существует самое большее столько различных $s\mathfrak{H}s^{-1}$, сколько имеется смежных классов, т. е. не более чем j. Если эти $s\mathfrak{H}s^{-1}$ (к ним принадлежит и $\mathfrak{H}$) заполняют группу $\mathfrak{G}$, то они не должны иметь общих элементов, так как в противном случае они не исчерпали бы всех $N=jn$ элементов. Но так как любая пара $s\mathfrak{H}s^{-1}$ имеет единицу общей, то $s\mathfrak{H}s^{-1}$ не могут быть взаимно простыми, и мы приходим к противоречию.

В нашем случае из этой леммы следует, что $\mathfrak{H}$ не может быть *собственной* подгруппой группы $\mathfrak{G}$, т. е. должно иметь место $\mathfrak{H}=\mathfrak{G}$, а потому $\mathsf{K}=\Sigma_0$. Следовательно, K коммутативно. Итак:

Всякое поле с конечным числом элементов коммутативно, т. е. образует конечное поле Галуа.

Дальнейшие глубоко идущие приложения теории представления к теории гиперкомплексных величин см. у R. Brauer, Über Systeme hyperkomplexer Zahlen, „Math. Zeitschr.“, Bd. 30, стр. 79—107, 1929.

Задачи. 1. Пусть K — поле конечного ранга относительно коммутативного основного поля P, Σ — промежуточное поле, T — поле элементов, перестановочных с Σ. Тогда полем элементов, перестановочных с T, будет опять-таки Σ.

2. Если центр Σ предыдущей задачи равен P, то $\mathsf{K}=\Sigma\times\mathsf{T}$.

3. Если $\mathfrak{S}$ — коммутативное поле конечного ранга относительно P и $\mathfrak{S}\to\Sigma$ — неприводимое представление r-й степени поля $\mathfrak{S}$ в K, то согласно приведенным выше теоремам $\mathfrak{S}'\times\mathsf{K}$ изоморфно кольцу матриц поля $\mathsf{T}\subset\mathsf{K}_r$, которое содержит Σ и состоит из элементов K_r, перестановочных с элементами из Σ. Доказать, что $\mathsf{T}=\Sigma$ и что $\mathfrak{S}$ есть поле разложения K тогда и только тогда, если Σ — максимальное коммутативное подполе K_r. Таким образом полями разложения K будут поля, для которых неприводимые представления суть коммутативные максимальные подполя поля K_r. Их ранг равен $m\cdot r$, где m — индекс поля K.

4. Определить все поля индекса 2 относительно рационального числового поля Γ, рассматриваемого как центр („поле обобщенных кватернионов“).

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ВЫШЛИ В СВЕТ

ВИНОГРАДОВ И. М.

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Ц. 1 р. 25 к. П. 1 р.

ГЛИВЕНКО В. И.

ИНТЕГРАЛ СТИЛЬТЬЕСА

Ц. 4 р. 50 к.

ГЛАГОЛЕВ Н. А.

НАЧЕРТАТЕЛЬНАЯ ГЕОМЕТРИЯ

Ц. 2 р. П. 50 к.

ГЛАГОЛЕВ Н. А.

ПРОЕКТИВНАЯ ГЕОМЕТРИЯ

Ц. 4 р. П. 50 к.

ДУББЕЛЬ

СПРАВОЧНИК ПО МАТЕМАТИКЕ

Ц. 5 р. 50 к. П. 1 р.

СИКОРСКИЙ Ю. С.

ЭЛЕМЕНТЫ ЭЛЛИПТИЧЕСКИХ ФУНКЦИЙ

Ц. 7 р. П. 1 р. 25 к.

УСПЕХИ МАТЕМАТИЧЕСКИХ НАУК

Вып. I

Ц. 7 р. 25 к.

УСПЕХИ МАТЕМАТИЧЕСКИХ НАУК

Вып. II

Ц. 7 р. 25 к.

ОБЪЕДИНЕННОЕ НАУЧНО-ТЕХНИЧЕСКОЕ ИЗДАТЕЛЬСТВО НКТП СССР

ГОТОВЯТСЯ К ПЕЧАТИ

ВЕНКОВ Б. А.

ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ЧИСЕЛ

ХАУСДОРФ

ТЕОРИЯ МНОЖЕСТВ

СУШКЕВИЧ А. К.

ОСНОВЫ ВЫСШЕЙ АЛГЕБРЫ

Т. I, ч. I и II

СТЕПАНОВ В. В.

ДИФЕРЕНЦИАЛЬНЫЕ УРАВНЕНИЯ

УСПЕХИ МАТЕМАТИЧЕСКИХ НАУК

Вып. II

ЗАМЕЧЕННЫЕ ОПЕЧАТКИ

Стр.	*Строка*	*Напечатано*	*Должно быть*	*По чьей вине*
26	11 сверху	$\equiv \underset{\alpha}{O}(\pi l_\alpha)$	$\equiv O\left(\underset{\alpha}{\pi l_\alpha}\right)$	Типогр.
39	11 „	подкольцо q	подкольцо $\mathfrak{d}$	Ред.
50	26 „	$b \equiv b$	$b_\nu \equiv b$	Типогр.
53	16 снизу	§ 95	§ 85	Ред.
82	27 сверху	$\overset{*}{1}$	f_1^*	Типогр.

На последней полосе объявлений, в первой строке снизу следует читать: Вып. III

Зак. 1657, Ван-Дер-Варден