Этим путем все поле комплексных чисел отображается, притом взаимно однозначно, на часть кольца матриц второго порядка, причем из равенств

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

вытекает, что это отображение изоморфное, так как матрицы, стоящие в правых частях равенств, соответствуют комплексным числам $(a+c)+(b+d)\,i=(a+bi)+(c+di)$ и $(ac-bd)+(ad+bc)\,i=(a+bi)\,(c+di)$. В частности, роль мнимой единицы i играет матрица

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Полученный нами результат указывает на еще один возможный способ построения поля комплексных чисел, столь же удовлетворительный, как и те, которые рассматривались выше.

§ 47. Линейная алгебра и алгебра многочленов над произвольным полем

В тех из предшествующих глав книги, которые посвящены линейной алгебре, роль основного поля играло обычно поле действительных чисел. Без труда проверяется, однако, что очень многое из этих глав дословно переносится на случай произвольного основного поля.

Так, *для произвольного основного поля P остаются справедливыми изложенные в гл. 1 метод Гаусса для решения систем линейных уравнений, теория определителей и правило Крамера.* Лишь замечание о кососимметрических определителях, приведенное в конце § 4, требует предположения, что характеристика поля P отлична от двух. Впрочем, доказательство свойства 4 из этого же параграфа также теряет силу, если характеристика поля P равна двум, хотя само это свойство остается справедливым.

Полезно отметить также, что неоднократно высказывавшееся в гл. 1 утверждение о существовании у неопределенной системы линейных уравнений бесконечного множества различных решений сохраняет силу в случае любого бесконечного основного поля P, но перестает быть справедливым, если поле P конечно.

Далее, *полностью переносятся на случай произвольного основного поля изложенные в гл. 2 теория линейной зависимости векторов, теория ранга матрицы и общая теория систем линейных уравнений, а также алгебра матриц из гл. 3.*

Общая теория квадратичных форм, построенная в § 26, *переносится на случай любого основного поля P, характеристика которого отлична от двух.* Без этого ограничения, как легко показать, основная теорема этого параграфа уже перестает быть справедливой.

Пусть, например, $P=Z_2$, т. е. является полем, состоящим из двух элементов 0 и 1, причем $1+1=0$, откуда $-1=1$, и пусть над этим полем дана квадратичная форма $f=x_1x_2$. Если существует линейное преобразование

$$x_1=b_{11}y_1+b_{12}y_2,$$
$$x_2=b_{21}y_1+b_{22}y_2,$$

приводящее f к каноническому виду, то в равенстве

$$f=(b_{11}y_1+b_{12}y_2)(b_{21}y_1+b_{22}y_2)=b_{11}b_{21}y_1^2+(b_{11}b_{22}+b_{12}b_{21})\,y_1y_2+b_{12}b_{22}y_2^2$$

коэффициент $b_{11}b_{22}+b_{12}b_{21}$ при произведении y_1y_2 должен быть равен нулю. Этот коэффициент равен, однако, определителю взятого нами линейного преобразования, так как будет ли $b_{12}b_{21}=1$ или же $b_{12}b_{21}=0$, — в обоих случаях $b_{12}b_{21}=-b_{12}b_{21}$. Наше линейное преобразование оказалось вырожденным.

Дальнейшее содержание гл. 6 существенно относится к квадратичным формам с комплексными или действительными коэффициентами.

Наконец, *для случая произвольного основного поля P сохраняется вся построенная в гл. 7 теория линейных пространств и их линейных преобразований.* Впрочем, понятие характеристического корня связано с теорией многочленов над произвольным полем, о которой речь будет идти ниже. Заметим, что теорема из § 33 о связи между характеристическими корнями и собственными значениями примет теперь следующую формулировку: характеристические корни линейного преобразования φ, лежащие в основном поле P, и только они, служат собственными значениями этого преобразования.

Что же касается теории евклидовых пространств (гл. 8), то она существенно связана с полем действительных чисел.

На случай произвольного основного поля P могут быть перенесены и некоторые из изложенных выше разделов алгебры многочленов. Предварительно необходимо, однако, придать точный смысл понятию многочлена над произвольным полем.

Дело в том, что в § 20 указывались две точки зрения на понятие многочлена — формально-алгебраическая и теоретико-функциональная. Они обе могут быть перенесены на случай произвольного основного поля. Будучи, однако, равносильными для случая числовых полей (см. § 24) и, как легко проверить, для бесконечных полей вообще, *для конечных полей они уже перестают быть равносильными.*

Рассмотрим, например, введенное в § 45 поле Z_2, состоящее из двух элементов 0 и 1, причем $1+1=0$. Многочлены $x+1$ и x^2+1 с коэффициентами из этого поля являются различными, т. е. не удовлетворяют алгебраическому определению равенства многочленов. Вместе с тем, оба эти многочлена при $x=0$ получают значение 1, а при $x=1$ — значение 0, т. е. как «функции» от «переменного» x, принимающего значения в поле Z_2, они должны считаться равными. В поле Z_3, состоящем из трех элементов: 0, 1, 2, причем

$1+2=0$, в таком же положении находятся многочлены x^3+x+1 и $2x+1$. Такие примеры можно указать вообще для всех конечных полей.

Таким образом, в теории, относящейся к случаю произвольного поля P, невозможно принять теоретико-функциональную точку зрения на многочлены. Необходимо, следовательно, придать полную ясность формально-алгебраическому определению многочлена. С этой целью мы проведем такое построение кольца многочленов над произвольным полем P, которое не использует с самого начала обычной записи многочленов через «неизвестное» x.

Рассмотрим всевозможные упорядоченные конечные системы элементов поля P, имеющие вид

$$(a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n), \tag{1}$$

причем n произвольно, $n \geqslant 0$, но при $n>0$ должно быть $a_n \neq 0$. Определяя для систем вида (1) сложение и умножение в соответствии с формулами (3) и (4) § 20, мы превратим совокупность этих систем в коммутативное кольцо; доказательства необходимых для этого свойств дословно повторяют то, что делалось в § 20 для числовых многочленов.

В построенном нами кольце системы вида (a) (случай $n=0$) составляют подполе, изоморфное полю P. Это позволяет отождествить такие системы с соответствующими элементами a поля P, т. е. положить

$$(a)=a \text{ для всех } a \text{ из } P. \tag{2}$$

С другой стороны, обозначим систему (0, 1) буквой x,

$$x=(0,\ 1).$$

Тогда, применяя указанное выше определение умножения, мы получим, что $x^2=(0,\ 0,\ 1)$ и вообще

$$x^k=(\underbrace{0,\ 0,\ \ldots,\ 0}_{k \text{ раз}},\ 1). \tag{3}$$

Используя теперь определения сложения и умножения упорядоченных систем, а также равенства (2) и (3), мы получим:

$$\begin{aligned}
&(a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n)=\\
&\quad=(a_0)+(0,\ a_1)+(0,\ 0,\ a_2)+\ldots\\
&\qquad\ldots+(\underbrace{0,\ 0,\ \ldots,\ 0}_{n-1 \text{ раз}},\ a_{n-1})+(\underbrace{0,\ 0,\ \ldots,\ 0}_{n \text{ раз}},\ a_n)=\\
&\quad=(a_0)+(a_1)(0,\ 1)+(a_2)(0,\ 0,\ 1)+\ldots\\
&\qquad\ldots+(a_{n-1})(\underbrace{0,\ 0,\ \ldots,\ 0}_{n-1 \text{ раз}},\ 1)+(a_n)(\underbrace{0,\ 0,\ \ldots,\ 0}_{n \text{ раз}},\ 1)=\\
&\qquad\qquad=a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1}+a_nx^n.
\end{aligned}$$

Таким образом, всякая упорядоченная система вида (1) может быть записана в виде многочлена относительно x с коэффициентами из поля P, причем эта запись будет, очевидно, однозначной. Опираясь, наконец, на уже доказанную коммутативность сложения, можно перейти к записи по убывающим степеням x.

Мы построим, следовательно, коммутативное кольцо, которое естественно назвать *кольцом многочленов от неизвестного x над полем P*. Это кольцо обозначается символом $P[x]$.

В кольце $P[x]$ содержится само поле P, как уже было показано выше. Далее, как и в случае колец многочленов над числовыми полями (см. § 20), *кольцо $P[x]$ обладает единицей, не содержит делителей нуля и не является полем.*

Если поле P содержится в большем поле $\overline{P}$, то кольцо $P[x]$ будет подкольцом кольца $\overline{P}[x]$: всякий многочлен с коэффициентами из P можно считать, понятно, многочленом и над полем $\overline{P}$, а сумма и произведение многочленов зависят только от их коэффициентов и поэтому не меняются при переходе к большему полю.

Для того чтобы лучше представить себе истинный объем понятия «кольцо многочленов над полем P», посмотрим на него еще с одной стороны.

Пусть поле P содержится в качестве подкольца в некотором коммутативном кольце L. Элемент α кольца L называется *алгебраическим над полем P*, если существует такое уравнение n-й степени, $n \geqslant 1$, с коэффициентами из поля P, которому элемент α удовлетворяет; если же такого уравнения не существует, то элемент α называется *трансцендентным над полем P*. Понятно, что элемент x кольца $P[x]$ трансцендентен над полем P.

Справедлива следующая теорема:

Если элемент α кольца L трансцендентен над полем P, то подкольцо L', полученное присоединением элемента α к полю P (т. е. минимальное подкольцо кольца L, содержащее поле P и элемент α), *изоморфно кольцу многочленов $P[x]$*.

В самом деле, всякий элемент β кольца L, который может быть записан в виде

$$\beta = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n, \qquad n \geqslant 0, \tag{4}$$

с коэффициентами $a_0, a_1, \ldots, a_{n-1}, a_n$ из поля P, будет содержаться в подкольце L'. Элемент β не может обладать двумя различными записями вида (4), так как, вычитая из одной записи другую, мы получили бы, что существует уравнение над полем P, удовлетворяемое элементом α, в противоречие с трансцендентностью этого элемента. Складывая элементы вида (4) по правилам сложения в кольце L, можно, понятно, складывать коэффициенты при одинаковых степенях α; это совпадает, однако, с правилом сложения многочленов. С другой стороны, перемножая элементы вида (4) по правилам

умножения в кольце L, мы можем, пользуясь законом дистрибутивности, совершить почленное перемножение, а затем собрать подобные члены; это приводит, очевидно, к известному нам правилу умножения многочленов. Этим доказано, что элементы вида (4) составляют в кольце L подкольцо, содержащее поле P и элемент α, т. е. совпадающее с L', и что это подкольцо изоморфно кольцу многочленов $P[x]$.

Мы видим, что сделанный выше выбор определений для операций над многочленами не был случайным: он вполне определяется тем, что элемент x кольца $P[x]$ должен быть трансцендентным над полем P.

Заметим, что при построении кольца многочленов $P[x]$ мы нигде не использовали деления элементов поля P и лишь один раз, а именно, при доказательстве утверждения о степени произведения многочленов, должны были бы сослаться на отсутствие в поле P делителей нуля. Можно, следовательно, взять произвольное коммутативное кольцо L и, повторяя проведенное выше построение, получить *кольцо многочленов $L[x]$ над кольцом L*; если при этом кольцо L не содержит делителей нуля, то степень произведения многочленов будет равна сумме степеней сомножителей и поэтому кольцо многочленов $L[x]$ также не будет содержать делителей нуля.

Возвращаясь к многочленам с коэффициентами из произвольного поля P, заметим, что на этот случай переносится по существу вся теория делимости многочленов, изложенная в §§ 20—22 нашей книги. Именно, *в кольце $P[x]$ имеет место алгоритм деления с остатком*, причем и частное, и остаток сами будут принадлежать к кольцу $P[x]$. Далее, *в кольце $P[x]$ имеет смысл понятие делителя и сохраняются все его основные свойства.* При этом то обстоятельство, что алгоритм деления не выводит за пределы основного поля P, позволяет утверждать, что *свойство многочлена $\varphi(x)$ быть делителем для $f(x)$ не зависит от того, рассматриваем ли мы поле P или же его любое расширение.*

В кольце $P[x]$ сохраняются также определение и все свойства наибольшего общего делителя, в том числе сохраняются алгоритм Евклида и теорема, доказанная в § 21 *при помощи этого алгоритма.* Заметим, что так как алгоритм деления с остатком не зависит, как мы знаем, от того, какое поле выбрано в качестве основного, то можно утверждать, что *наибольший общий делитель двух данных многочленов также не зависит от того, рассматриваем ли мы поле P или же его произвольное расширение $\overline{P}$.*

Наконец, *для многочленов над полем P сохраняет смысл понятие корня и остаются справедливыми основные свойства корней.* Сохраняется и теория кратных корней; впрочем, к этому вопросу мы вернемся еще раз в конце следующего параграфа.

Эти замечания позволят нам в дальнейшем при изучении многочленов над любым полем P ссылаться на § 20—22.