условия 3) вытекает непосредственно из равенства (7): если $f_k(\alpha)=0$, то $f_{k-1}(\alpha)=-f_{k+1}(\alpha)$.

Применим метод Штурма к рассматривавшемуся в предыдущем параграфе многочлену

$$h(x)=x^5+2x^4-5x^3+8x^2-7x-3.$$

Мы не будем при этом предварительно проверять, что $h(x)$ не имеет кратных корней, так как метод построения системы Штурма, изложенный выше, одновременно служит для проверки взаимной простоты многочлена и его производной.

Найдем систему Штурма для $h(x)$, применяя указанный метод. При этом в процессе деления мы будем, в отличие от алгоритма Евклида, умножать и сокращать лишь на произвольные положительные числа, так как знаки остатков играют в методе Штурма основную роль. Мы получим такую систему:

$$\begin{aligned}
h(x)&=x^5+2x^4-5x^3+8x^2-7x-3,\\
h_1(x)&=5x^4+8x^3-15x^2+16x-7,\\
h_2(x)&=66x^3-150x^2+172x+61,\\
h_3(x)&=-464x^2+1135x+723,\\
h_4(x)&=-32\,599\,457x-8\,486\,093,\\
h_5(x)&=-1.
\end{aligned}$$

Определим знаки многочленов этой системы при $x=-\infty$ и $x=\infty$, для чего, как было указано, следует смотреть лишь на знаки старших коэффициентов и на степени этих многочленов. Мы получим такую таблицу:

| | $h(x)$ | $h_1(x)$ | $h_2(x)$ | $h_3(x)$ | $h_4(x)$ | $h_5(x)$ | Число перемен знаков |
|---|---|---|---|---|---|---|---|
| $-\infty$ | $-$ | $+$ | $-$ | $-$ | $+$ | $-$ | 4 |
| $\infty$ | $+$ | $+$ | $+$ | $-$ | $-$ | $-$ | 1 |

Таким образом, при переходе $x$ от $-\infty$ к $\infty$ система Штурма теряет три перемены знаков, а поэтому многочлен $h(x)$ имеет ровно три действительных корня. Отсюда видно, что при построении в предыдущем параграфе графика этого многочлена мы не упустили ни одного из корней.

Применим метод Штурма к другому многочлену, более простому. Пусть дан многочлен

$$f(x)=x^3+3x^2-1.$$

Найдем число его действительных корней, а также целые границы, между которыми каждый из этих корней расположен, причем не будем строить заранее графика этого многочлена.

Система Штурма для многочлена $f(x)$ будет

$$\begin{aligned}
f(x)&=x^3+3x^2-1\\
f_1(x)&=3x^2+6x,\\
f_2(x)&=2x+1,\\
f_3(x)&=1.
\end{aligned}$$

Найдем число перемен знаков в этой системе при $x=-\infty$ и $x=\infty$

| | $f(x)$ | $f_1(x)$ | $f_2(x)$ | $f_3(x)$ | Число перемен знаков |
|---|---|---|---|---|---|
| $-\infty$ | $-$ | $+$ | $-$ | $+$ | 3 |
| $\infty$ | $+$ | $+$ | $+$ | $+$ | 0 |

Многочлен $f(x)$ обладает, следовательно, тремя действительными корнями. Для более точного определения положения этих корней продолжим предыдущую таблицу:

| | $f(x)$ | $f_1(x)$ | $f_2(x)$ | $f_3(x)$ | Число перемен знаков |
|---|---|---|---|---|---|
| $x=-3$ | $-$ | $+$ | $-$ | $+$ | 3 |
| $x=-2$ | $+$ | 0 | $-$ | $+$ | 2 |
| $x=-1$ | $+$ | $-$ | $-$ | $+$ | 2 |
| $x=0$ | $-$ | 0 | $+$ | $+$ | 1 |
| $x=1$ | $+$ | $+$ | $+$ | $+$ | 0 |

Таким образом, система Штурма многочлена $f(x)$ теряет по одной перемене знаков при переходе $x$ от $-3$ к $-2$, от $-1$ к 0 и от 0 к 1. Корни $\alpha_1$, $\alpha_2$ и $\alpha_3$ этого многочлена удовлетворяют, следовательно, неравенствам:

$$-3<\alpha_1<-2,\quad -1<\alpha_2<0,\quad 0<\alpha_3<1.$$

## § 41. Другие теоремы о числе действительных корней

Теорема Штурма полностью решает вопрос о числе действительных корней многочлена. Ее существенным недостатком является, однако, громоздкость вычислений, выполняемых при построении системы Штурма, как читатель мог убедиться, проделав все вычисления, относящиеся к первому из рассмотренных выше примеров. Ввиду этого сейчас будут доказаны две теоремы, не дающие точного числа действительных корней, а лишь ограничивающие это число сверху. Эти теоремы, применяемые после того, как при помощи графика число действительных корней уже ограничено

снизу, позволяют иногда найти точное число действительных корней, не прибегая к методу Штурма.

Пусть дан многочлен $f(x)$ $n$-й степени с действительными коэффициентами, причем допускаем, что он может обладать кратными корнями. Рассмотрим систему его последовательных производных

$$f(x)=f^{(0)}(x),\ f'(x),\ f''(x),\ \ldots,\ f^{(n-1)}(x),\ f^{(n)}(x), \tag{1}$$

из которых последняя равна старшему коэффициенту $a_0$ многочлена $f(x)$, умноженному на $n!$, и поэтому все время сохраняет постоянный знак. Если действительное число $c$ не служит корнем ни одного из многочленов системы (1), то обозначим через $S(c)$ число перемен знаков в упорядоченной системе чисел

$$f(c),\ f'(c),\ f''(c),\ \ldots,\ f^{(n-1)}(c),\ f^{(n)}(c).$$

Таким образом можно рассматривать целочисленную функцию $S(x)$, определенную для тех значений $x$, которые не обращают в нуль ни одного из многочленов системы (1).

Посмотрим, как меняется число $S(x)$ при возрастании $x$. Пока $x$ не пройдет через корень ни одного из многочленов (1), число $S(x)$ не может измениться. Ввиду этого мы должны рассмотреть два случая: переход $x$ через корень многочлена $f(x)$ и переход $x$ через корень одной из производных $f^{(k)}(x)$, $1\leqslant k\leqslant n-1$.

Пусть $\alpha$ будет $l$-кратный корень многочлена $f(x)$, $l\geqslant 1$, т. е.

$$f(\alpha)=f'(\alpha)=\ldots=f^{(l-1)}(\alpha)=0,\ f^{(l)}(\alpha)\neq 0.$$

Пусть положительное число $\varepsilon$ столь мало, что отрезок $(\alpha-\varepsilon,\ \alpha+\varepsilon)$ не содержит корней многочленов $f(x)$, $f'(x)$, $\ldots$, $f^{(l-1)}(x)$, отличных от $\alpha$, а также не содержит ни одного корня многочлена $f^{(l)}(x)$. Докажем, что в системе чисел

$$f(\alpha-\varepsilon),\ f'(\alpha-\varepsilon),\ \ldots,\ f^{(l-1)}(\alpha-\varepsilon),\ f^{(l)}(\alpha-\varepsilon)$$

всякие два соседних числа имеют противоположные знаки, тогда как все числа

$$f(\alpha+\varepsilon),\ f'(\alpha+\varepsilon),\ \ldots,\ f^{(l-1)}(\alpha+\varepsilon),\ f^{(l)}(\alpha+\varepsilon)$$

имеют один и тот же знак. Так как каждый из многочленов системы (1) является производной от предыдущего многочлена, то нам нужно лишь доказать, что если $x$ проходит через корень $\alpha$ многочлена $f(x)$, то, независимо от кратности этого корня, до перехода $f(x)$ и $f'(x)$ имели разные знаки, а после перехода их знаки совпадают. Если $f(\alpha-\varepsilon)>0$, то $f(x)$ убывает на отрезке $(\alpha-\varepsilon,\ \alpha)$, а потому $f'(\alpha-\varepsilon)<0$; если же $f(\alpha-\varepsilon)<0$, то $f(x)$ возрастает, и потому $f'(\alpha-\varepsilon)>0$. В обоих случаях, следовательно, знаки различны. С другой стороны, если $f(\alpha+\varepsilon)>0$, то $f(x)$ возрастает на отрезке $(\alpha,\ \alpha+\varepsilon)$, а потому $f'(\alpha+\varepsilon)>0$; аналогично из $f(\alpha+\varepsilon)<0$

следует $f'(\alpha+\varepsilon)<0$. Таким образом, после перехода через корень $\alpha$ знаки $f(x)$ и $f'(x)$ должны совпадать.

Из доказанного следует, что при переходе $x$ через $l$-кратный корень многочлена $f(x)$ система

$$f(x),\ f'(x),\ \ldots,\ f^{(l-1)}(x),\ f^{(l)}(x)$$

теряет $l$ перемен знаков.

Пусть $\alpha$ будет теперь корнем производных

$$f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ 1\leqslant k\leqslant n-1,\ l\geqslant 1,$$

но не служит корнем ни для $f^{(k-1)}(x)$, ни для $f^{(k+l)}(x)$. По доказанному выше, переход $x$ через $\alpha$ влечет за собой потерю в системе

$$f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ f^{(k+l)}(x)$$

$l$ перемен знаков. Правда, этот переход создает, возможно, новую перемену знаков между $f^{(k-1)}(x)$ и $f^{(k)}(x)$, однако, ввиду $l\geqslant 1$, при переходе $x$ через $\alpha$ число перемен знаков в системе

$$f^{(k-1)}(x),\ f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ f^{(k+l)}(x)$$

или не меняется, или же уменьшается. Оно может уменьшиться при этом лишь на четное число, так как многочлены $f^{(k-1)}(x)$ и $f^{(k+l)}(x)$ не меняют своих знаков при переходе $x$ через значение $\alpha$.

Из полученных результатов вытекает, что *если числа $a$ и $b$, $a<b$, не являются корнями ни для одного из многочленов системы* (1), *то число действительных корней многочлена $f(x)$, заключенных между $a$ и $b$ и подсчитываемых каждый столько раз, какова его кратность, равно разности $S(a)-S(b)$ или меньше этой разности на четное число.*

Для того чтобы ослабить ограничения, наложенные на числа $a$ и $b$, введем следующие обозначения. Пусть действительное число $c$ не является корнем многочлена $f(x)$, хотя, быть может, служит корнем для некоторых других многочленов системы (1). Обозначим через $S_+(c)$ число перемен знаков в системе чисел

$$f(c),\ f'(c),\ f''(c),\ \ldots,\ f^{(n-1)}(c),\ f^{(n)}(c), \tag{2}$$

подсчитываемое следующим образом: если

$$f^{(k)}(c)=f^{(k+1)}(c)=\ldots=f^{(k+l-1)}(c)=0, \tag{3}$$

но

$$f^{(k-1)}(c)\neq 0,\ f^{(k+l)}(c)\neq 0, \tag{4}$$

то считаем $f^{(k)}(c)$, $f^{(k+1)}(c)$, $\ldots$, $f^{(k+l-1)}(c)$ имеющими такой же знак, как у $f^{(k+l)}(c)$; это равносильно, очевидно, тому, что при подсчете числа перемен знаков в системе (2) нули предполагаются вычеркнутыми. С другой стороны, через $S_-(c)$ обозначим число перемен знаков в системе (2), подсчитываемое следующим образом: если имеют место условия (3) и (4), то считаем, что $f^{(k+i)}(c)$,

$0 \leqslant i \leqslant l-1$, имеет такой же знак, как и $f^{(k+l)}(c)$, если разность $l-i$ четная, и противоположный знак, если эта разность нечетная.

Если мы хотим теперь определить число действительных корней многочлена $f(x)$, заключенных между $a$ и $b$, $a<b$, причем $a$ и $b$ не являются корнями $f(x)$, но служат, быть может, корнями для других многочленов системы (1), то поступаем следующим образом. Пусть $\varepsilon$ столь мало, что отрезок $(a, a+2\varepsilon)$ не содержит корней многочлена $f(x)$, а также отличных от $a$ корней всех остальных многочленов системы (1); с другой стороны, пусть $\eta$ столь мало, что отрезок $(b-2\eta, b)$ также не содержит корней $f(x)$ и отличных от $b$ корней остальных многочленов системы (1). Тогда интересующее нас число действительных корней многочлена $f(x)$ будет равно числу действительных корней этого многочлена, заключенных между $a+\varepsilon$ и $b-\eta$, т. е., по доказанному выше, равно разности $S(a+\varepsilon)-$ $-S(b-\eta)$ или меньше этой разности на четное число. Легко видеть, однако, что

$$S(a+\varepsilon)=S_+(a), \quad S(b-\eta)=S_-(b).$$

Этим доказана следующая

Теорема Бюдана—Фурье. *Если действительные числа $a$ и $b$, $a<b$, не являются корнями многочлена $f(x)$ с действительными коэффициентами, то число действительных корней этого многочлена, заключенных между $a$ и $b$ и подсчитываемых каждый столько раз, какова его кратность, равно разности $S_+(a)-S_-(b)$ или меньше этой разности на четное число.*

Обозначим символом $\infty$ столь большое положительное значение неизвестного $x$, что знаки соответствующих ему значений всех многочленов системы (1) совпадают со знаками их старших коэффициентов. Так как этими коэффициентами будут последовательно числа $a_0$, $na_0$, $n(n-1)a_0$, ..., $n!a_0$, знаки которых совпадают, то $S(\infty)=S_-(\infty)=0$. С другой стороны, так как

$$f(0)=a_n, \; f'(0)=a_{n-1}, \; f''(0)=a_{n-2}2!,$$
$$f'''(0)=a_{n-3}3!, \; \ldots, \; f^{(n)}(0)=a_0\cdot n!,$$

где $a_0$, $a_1$, ..., $a_n$ — коэффициенты многочлена $f(x)$, то $S_+(0)$ совпадает с числом перемен знаков в системе коэффициентов многочлена $f(x)$, причем коэффициенты, равные нулю, не учитываются. Таким образом, применяя теорему Бюдана—Фурье к отрезку $(0, \infty)$, мы приходим к следующей теореме:

Теорема Декарта. *Число положительных корней многочлена $f(x)$, засчитываемых каждый столько раз, какова его кратность, равно числу перемен знаков в системе коэффициентов этого многочлена (причем равные нулю коэффициенты не учитываются) или меньше этого числа на четное число.*

Для определения числа отрицательных корней многочлена $f(x)$ достаточно, очевидно, применить теорему Декарта к многочлену

$f(-x)$. При этом, если ни один из коэффициентов многочлена $f(x)$ не равен нулю, то, очевидно, переменам знаков в системе коэффициентов многочлена $f(-x)$ соответствуют сохранения знаков в системе коэффициентов многочлена $f(x)$ и обратно. Таким образом, *если многочлен $f(x)$ не имеет равных нулю коэффициентов, то число его отрицательных корней (считаемых с их кратностями) равно числу сохранений знаков в системе коэффициентов или меньше его на четное число.*

Укажем еще одно доказательство теоремы Декарта, не опирающееся на теорему Бюдана — Фурье. Докажем сначала следующую лемму:

*Если $c>0$, то число перемен знаков в системе коэффициентов многочлена $f(x)$ меньше числа перемен знаков в системе коэффициентов произведения $(x-c)f(x)$ на нечетное число.*

Действительно, собирая в скобки стоящие рядом члены одного знака, запишем следующим образом многочлен $f(x)$, старший коэффициент $a_0$ которого считаем положительным:

$$f(x)=(a_0x^n+\ldots+b_1x^{k_1+1})-(a_1x^{k_1}+\ldots+b_2x^{k_2+1})+\ldots$$
$$\ldots+(-1)^s(a_sx^{k_s}+\ldots+b_{s+1}x^t). \quad (5)$$

Здесь $a_0>0$, $a_1>0$, ..., $a_s>0$, в то время как $b_1, b_2, \ldots, b_s$ положительны или равны нулю; однако $b_{s+1}$ считаем строго положительным, т. е. $x^t$, где $t\geqslant 0$, является наименьшей степенью неизвестного $x$, входящей в многочлен $f(x)$ с отличным от нуля коэффициентом. Скобка

$$(a_0x^n+\ldots+b_1x^{k_1+1})$$

случайно может состоять при этом лишь из одного слагаемого, а именно тогда, когда $k_1+1=n$. Аналогичное замечание применимо и к другим скобкам формулы (5).

Запишем теперь многочлен, равный произведению $(x-c)f(x)$, причем будем выделять лишь члены, содержащие $x$ в степенях $n+1$, $k_1+1$, ..., $k_s+1$ и $t$. Мы получим:

$$(x-c)f(x)=(a_0x^{n+1}+\ldots)-(a_1'x^{k_1+1}+\ldots)+\ldots$$
$$\ldots+(-1)^s(a_s'x^{k_s+1}+\ldots-cb_{s+1}x^t), \quad (6)$$

где $a_i'=a_i+cb_i$, $i=1, 2, \ldots, s$, и поэтому, так как $c>0$, все $a_i'$ строго положительны. Таким образом, в системе коэффициентов многочлена $f(x)$ между членами $a_0x^n$ и $-a_1x^{k_1}$ (а также между членами $-a_1x^{k_1}$ и $a_2x^{k_2}$ и т. д.) была одна перемена знаков, а у многочлена $(x-c)f(x)$ между соответствующими членами $a_0x^{n+1}$ и $-a_1'x^{k_1+1}$ (соответственно между членами $-a_1'x^{k_1+1}$ и $a_2'x^{k_2+1}$ и т. д.) будет или одна перемена знаков, или больше, но тогда непременно на четное число. Точные места этих перемен знаков нас не будут

при этом интересовать; может случиться, например, что коэффициент при $x^{k_1+2}$ в (6) отрицателен, как и коэффициент $-a_1'$, а поэтому между этими двумя соседними коэффициентами нет перемены знаков, т. е. в первой скобке перемены знаков расположены где-то раньше. Заметим теперь, что последняя скобка в (5) не содержала никаких перемен знаков, в то время как последняя скобка в (6) их содержит, притом нечетное число: достаточно учесть, что последние отличные от нуля коэффициенты многочленов $f(x)$ и $(x-c)f(x)$, т. е. $(-1)^s b_{s+1}$ и $(-1)^{s+1} b_{s+1} c$, имеют разные знаки. Таким образом, при переходе от $f(x)$ к $(x-c)f(x)$ общее число перемен знаков в системе коэффициентов непременно увеличивается, притом на нечетное число (сумма нескольких слагаемых, одно из которых нечетно, а остальные четны, будет, понятно, нечетной!). Лемма доказана.

Для доказательства теоремы Декарта обозначим через $\alpha_1, \alpha_2, \ldots, \alpha_k$ все положительные корни многочлена $f(x)$. Таким образом,

$$f(x) = (x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_k)\varphi(x),$$

где $\varphi(x)$ — многочлен с действительными коэффициентами, уже не имеющий положительных действительных корней. Отсюда следует, что первый и последний отличный от нуля коэффициенты многочлена $\varphi(x)$ одного знака, т. е. система коэффициентов этого многочлена содержит четное число перемен знаков. Применяя теперь доказанную выше лемму последовательно к многочленам

$$\varphi(x),\ (x-\alpha_1)\varphi(x),\ (x-\alpha_1)(x-\alpha_2)\varphi(x),\ \ldots,\ f(x),$$

мы получим, что число перемен знаков в системе коэффициентов каждый раз увеличивается на нечетное число, т. е. на единицу плюс четное число, а поэтому число перемен знаков в системе коэффициентов многочлена $f(x)$ больше числа $k$ на четное число.

Применим теоремы Декарта и Бюдана — Фурье к рассматривавшемуся выше многочлену

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3.$$

Число перемен знаков в системе коэффициентов равно трем, и поэтому, по теореме Декарта, $h(x)$ может иметь три или один положительный корень. С другой стороны, $h(x)$ не имеет равных нулю коэффициентов, а так как в системе коэффициентов два сохранения знаков, то $h(x)$ либо имеет два отрицательных корня, либо не имеет ни одного. Сравнивая с результатами, полученными ранее при помощи графика, мы получаем, что два есть точное число отрицательных корней нашего многочлена.

Для точного определения числа положительных корней воспользуемся теоремой Бюдана — Фурье, причем применим ее к отрезку $(1, \infty)$, так как в § 39 уже было показано, что 1 служит нижней границей положительных

корней многочлена $h(x)$. Последовательные производные $h(x)$ также уже были выписаны в § 39. Найдем их знаки при $x=1$ и $x=\infty$:

| | $h(x)$ | $h'(x)$ | $h''(x)$ | $h'''(x)$ | $h^{IV}(x)$ | $h^{V}(x)$ | Число перемен знаков |
|---|---|---|---|---|---|---|---|
| $x=1$ | $-$ | $+$ | $+$ | $+$ | $+$ | $+$ | 1 |
| $x=\infty$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | 0 |

Отсюда следует, что система производных теряет при переходе $x$ от 1 до $\infty$ одну перемену знаков, а поэтому $h(x)$ имеет ровно один положительный корень.

В связи с этим примером заметим, что вообще при разыскании числа действительных корней многочлена следует начинать с построения графика и применения теорем Декарта и Бюдана—Фурье, лишь в крайних случаях переходя к построению системы Штурма.

Теорема Декарта допускает некоторое уточнение в том частном случае, когда заранее известно, что все корни многочлена действительные, как это имеет место, например, для характеристического многочлена симметрической матрицы. Именно:

*Если все корни многочлена $f(x)$ действительные, а свободный член отличен от нуля, то число $k_1$ положительных корней этого многочлена равно числу $s_1$ перемен знаков в системе его коэффициентов, а число $k_2$ отрицательных корней равно числу $s_2$ перемен знаков в системе коэффициентов многочлена $f(-x)$.*

Действительно, при наших предположениях

$$k_1+k_2=n, \tag{7}$$

где $n$ — степень многочлена $f(x)$, и, по теореме Декарта,

$$k_1 \leqslant s_1, \quad k_2 \leqslant s_2. \tag{8}$$

Докажем, что

$$s_1+s_2 \leqslant n. \tag{9}$$

Доказательство будем вести индукцией по $n$, так как при $n=1$ ввиду $a_0 \neq 0$, $a_1 \neq 0$ перемена знаков имеется лишь у одного из многочленов

$$f(x)=a_0x+a_1, \quad f(-x)=-a_0x+a_1,$$

т. е. для этого случая $s_1+s_2=1$. Пусть формула (9) уже доказана для многочленов, степень которых меньше $n$. Если

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

где $l \leqslant n-1$, $a_{n-l} \neq 0$, то положим

$$g(x) = a_{n-l}x^l + \ldots + a_n.$$

Тогда

$$f(x) = a_0x^n + g(x), \qquad f(-x) = (-1)^n a_0 x^n + g(-x).$$

Если $s_1'$ и $s_2'$ будут соответственно числа перемен знаков в системах коэффициентов многочленов $g(x)$ и $g(-x)$, то, по индуктивному предположению (ясно, что $l \geqslant 1$),

$$s_1' + s_2' \leqslant l.$$

Если $l = n-1$, то перемена знаков на первом месте, т. е., для $f(x)$, между $a_0$ и $a_1 = a_{n-l}$ будет лишь у одного из многочленов $f(x)$, $f(-x)$, а поэтому

$$s_1 + s_2 = s_1' + s_2' + 1 \leqslant l + 1 = n.$$

Если же $l \leqslant n-2$, то возможны перемены знаков на первых местах у каждого из многочленов $f(x)$, $f(-x)$, однако и в этом случае

$$s_1 + s_2 \leqslant s_1' + s_2' + 2 \leqslant l + 2 \leqslant (n-2) + 2 = n.$$

Сопоставляя (7), (8) и (9), получаем, что

$$k_1 = s_1, \quad k_2 = s_2,$$

что и требовалось доказать.

## § 42. Приближенное вычисление корней

Изложенные в предшествующих параграфах методы позволяют произвести *отделение* действительных корней многочлена $f(x)$ с действительными коэффициентами, т. е. для каждого из корней указать границы, между которыми находится только один этот корень. Если эти границы достаточно узки, то любое число, заключенное между ними, можно считать приближенным значением искомого корня. Таким образом, после того как методом Штурма (или каким-либо другим, более экономным способом) будет установлено, что между рациональными числами $a$ и $b$ содержится лишь один корень многочлена $f(x)$, остается задача настолько сузить эти границы, чтобы новые границы $a'$ и $b'$ обладали наперед заданным числом совпадающих первых десятичных знаков; этим искомый корень будет вычислен с заданной точностью.

Существует много методов, позволяющих достаточно быстро находить приближенное значение корня с требуемой точностью. Мы укажем два из них, теоретически более простые и общие и при совместном употреблении достаточно быстро приводящие к цели. Следует заметить, что методы, которые будут сейчас изложены, применимы не только к многочленам, но и к более широким классам непрерывных функций.

Будем считать дальше, что $\alpha$ есть простой корень многочлена $f(x)$, так как от кратных корней мы всегда можем освободиться,

и что корень $\alpha$ уже отделен границами $a$ и $b$, $a<\alpha<b$; отсюда следует, в частности, что $f(a)$ и $f(b)$ имеют разные знаки.

**Метод линейной интерполяции** (называемый также методом ложного положения). В качестве приближенного значения корня $\alpha$ можно было бы принять, например, полусумму границ $a$ и $b$, $\frac{a+b}{2}$, т. е. середину отрезка, имеющего концами $a$ и $b$. Более естественно, однако, предположить, что корень лежит ближе к той из границ $a$, $b$, которой соответствует меньшее по абсолютной величине значение многочлена. Метод линейной интерполяции состоит в том, что в качестве приближенного значения корня $\alpha$ берется число $c$, делящее отрезок $(a, b)$ на части, пропорциональные абсолютным величинам чисел $f(a)$ и $f(b)$, т. е.

$$\frac{c-a}{b-c}=-\frac{f(a)}{f(b)};$$

знак минус в правой части поставлен ввиду того, что $f(a)$ и $f(b)$ имеют разные знаки. Отсюда

$$c=\frac{bf(a)-af(b)}{f(a)-f(b)}. \tag{1}$$

Геометрически, как показывает рис. 10, метод линейной интерполяции заключается в том, что на отрезке $(a, b)$ кривая $y=f(x)$ заменяется ее хордой, соединяющей точки $A(a, f(a))$ и $B(b, f(b))$, и в качестве приближенного значения корня $\alpha$ принимается абсцисса точки пересечения этой хорды с осью $x$.

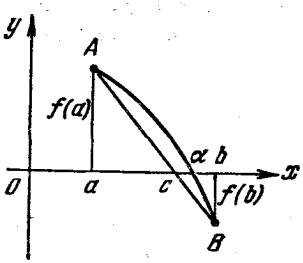

Рис. 10.

**Метод Ньютона.** Так как $\alpha$ — простой корень многочлена $f(x)$, то $f'(\alpha)\neq 0$. Примем, что также и $f''(\alpha)\neq 0$, так как иначе вопрос сводится к вычислению корня многочлена $f''(x)$, имеющего меньшую степень, чем $f(x)$. Примем, далее, что отрезок $(a, b)$ не только не содержит корней $f(x)$, отличных от $\alpha$, но и не содержит ни одного корня многочлена $f'(x)$, а также и многочлена $f''(x)$ [1]. Таким образом, как следует из курса математического анализа, кривая $y=f(x)$ на отрезке $(a, b)$ либо монотонно возрастает, либо монотонно убывает, а также либо во всех точках этого отрезка обращена выпуклостью вверх, либо во всех точках обращена выпуклостью вниз. В расположении кривой на отрезке $(a, b)$

[1] Сужение границ, приводящее к тому, что это условие будет удовлетворяться, достигается обычно без всяких затруднений, так как методы, изложенные ранее, позволяют установить число корней многочленов $f'(x)$ и $f''(x)$ в любом отрезке.

могут встретиться, следовательно, четыре случая, представленных на черт. 11—14.

Обозначим через $a_0$ тот из пределов $a$ и $b$, в котором знак $f(x)$ совпадает со знаком $f''(x)$. Так как $f(a)$ и $f(b)$ имеют разные знаки, а $f''(x)$ сохраняет знак на всем отрезке $(a, b)$, то такое $a_0$ может быть указано. В случаях, представленных на рис. 11 и 14,

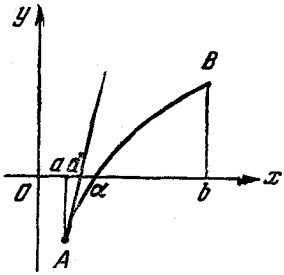


Рис. 11.

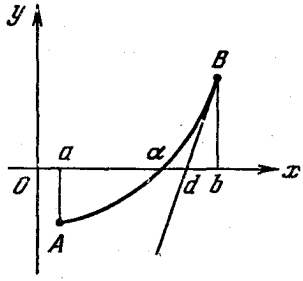


Рис. 12.

будет $a_0 = a$, в двух других случаях $a_0 = b$. В точке кривой $y = f(x)$ с абсциссой $a_0$, т. е. в точке с координатами $(a_0, f(a_0))$, проведем касательную к этой кривой и обозначим через $d$ абсциссу точки пересечения этой касательной с осью $x$. Рис. 11—14 показывают,

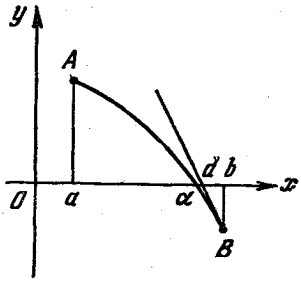


Рис. 13.

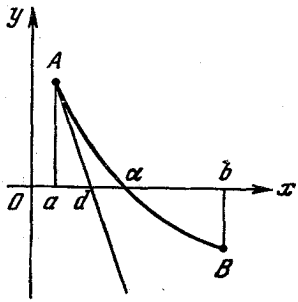


Рис. 14.

что число $d$ можно считать приближенным значением корня $\alpha$. Метод Ньютона состоит, следовательно, в замене кривой $y = f(x)$ на отрезке $(a, b)$ ее касательной в одной из границ этого отрезка. Условие, наложенное на выбор точки $a_0$, очень существенно: рис. 15 показывает, что без соблюдения этого условия точка пересечения касательной с осью $x$ может вовсе не давать приближения к искомому корню.

Выведем формулу, по которой разыскивается число $d$. Как известно, уравнение касательной к кривой $y=f(x)$ в точке $(a_0, f(a_0))$ может быть записано в виде

$$y-f(a_0)=f'(a_0)(x-a_0).$$

Подставляя сюда координаты $(d, 0)$ точки пересечения касательной с осью $x$, получим:

$$-f(a_0)=f'(a_0)(d-a_0),$$

откуда

$$d=a_0-\frac{f(a_0)}{f'(a_0)}. \qquad (2)$$

Если читатель соединит на рис. 11—14 точки $A$ и $B$ хордами, то обнаружит, что *методы линейной интерполяции и Ньютона*

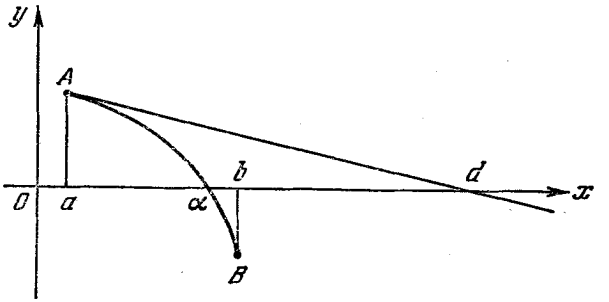


Рис. 15.

*во всех случаях дают приближение к истинному значению корня $\alpha$ с разных сторон.* Целесообразно поэтому, если отрезок $(a, b)$ уже таков, как это требуется в методе Ньютона, комбинировать эти два метода. Мы получим этим путем много более тесные границы $c$ и $d$ для корня $\alpha$. Если они еще не дают требуемой точности приближения, то к этим пределам следует еще раз применить указанные оба метода (см. рис. 16) и т. д., причем можно доказать, что этот процесс действительно позволяет вычислить корень $\alpha$ с любой точностью.

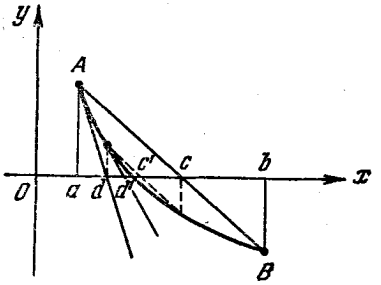


Рис. 16.

Применим эти методы к рассматривавшемуся в предшествующих параграфах многочлену

$$h(x)=x^5+2x^4-5x^3+8x^2-7x-3.$$

Мы знаем, что этот многочлен обладает простым корнем $\alpha_1$, заключенным в границах $1 < \alpha_1 < 2$. Можно сказать заранее, что эти границы слишком широки для того, чтобы методы линейной интерполяции и Ньютона, примененные лишь по одному разу, могли дать хороший результат. Применим их, однако, чтобы иметь один пример, не требующий сложных вычислений.

Как мы видели в предшествующем параграфе, при $x=1$ производные $h'(x)$, $h''(x), \ldots, h^{V}(x)$ получают положительные значения. Отсюда следует, на основании результатов § 39, что значение $x=1$ служит для $h'(x)$, а также и для $h''(x)$ верхней границей положительных корней. Отрезок (1, 2) не содержит, следовательно, корней этих производных, а поэтому к нему можно применить метод Ньютона. Кроме того, $h''(x)$ всюду в этом отрезке положительна, а так как

$$h(1) = -4, \quad h(2) = 39,$$

то нужно принять $a_0 = 2$. Учитывая, что $h'(2) = 109$, мы по формуле (2) получаем:

$$d = 2 - \frac{39}{109} = \frac{179}{109} = 1{,}64\ldots$$

С другой стороны, формула (1) дает:

$$c = \frac{2\cdot(-4) - 1\cdot 39}{-4-39} = \frac{47}{43} = 1{,}09\ldots$$

и, следовательно, корень $\alpha_1$ заключен в границах

$$1{,}09 < \alpha_1 < 1{,}65.$$

Мы получили слишком незначительное сужение границ для того, чтобы признать этот результат удовлетворительным. Конечно, к вновь полученным границам можно было бы еще раз применить наши методы. Целесообразно, однако, с самого начала найти для $\alpha_1$ достаточно тесные границы, например с точностью до 0,1 или даже 0,01, и лишь затем применять эти методы. Это сразу сделает, понятно, все вычисления весьма громоздкими, но при решении конкретных задач, требующих достаточно точного знания корней многочлена, на это приходится идти.

Вернемся к нашему многочлену $h(x)$ и его корню $\alpha_1$, причем заметим, что все значения многочленов, приводимые ниже, вычисляются методом Горнера. Так как

$$h(1{,}3) = -0{,}13987, \quad h(1{,}31) = 0{,}0662923851,$$

то

$$1{,}3 < \alpha_1 < 1{,}31,$$

т. е. мы нашли значение корня $\alpha_1$ с точностью до 0,01. Применим теперь к этим новым границам метод линейной интерполяции:

$$c = \frac{1{,}31\cdot(-0{,}13987) - 1{,}3\cdot 0{,}0662923851}{-0{,}13987 - 0{,}0662923851} = \frac{0{,}26940980063}{0{,}2061623851} = 1{,}30678\ldots$$

Применим к этим же границам метод Ньютона, причем следует положить $a_0 = 1{,}31$. Так как

$$h'(1{,}31) = 20{,}92822405,$$

то

$$d = 1{,}31 - \frac{0{,}0662923851}{20{,}92822405} = \frac{27{,}3496811204}{20{,}92822405} = 1{,}30683\ldots$$

Таким образом,

$$1{,}30678 < \alpha_1 < 1{,}30684,$$

и поэтому, полагая $\alpha_1 = 1{,}30681$, мы сделаем ошибку, меньшую чем 0,00003.

Мы не показали до сих пор, что изложенные выше методы на самом деле позволяют вычислить корень с любой точностью, т. е. не доказали сходимости этих методов. Докажем это хотя бы для метода Ньютона.

Пусть, как и выше, простой корень $\alpha$ многочлена $f(x)$ содержится в отрезке $(a, b)$, выбранном так, как это необходимо для применения метода Ньютона. Отсюда следует, в частности, существование таких положительных чисел $A$ и $B$, что всюду на отрезке $(a, b)$

$$|f'(x)| > A, \quad |f''(x)| < B. \tag{3}$$

Введем обозначение

$$C = \frac{B}{2A}$$

и положим, что

$$C(b-a) < 1. \tag{4}$$

Для выполнения этого неравенства придется, возможно, заменить границы $(a, b)$ корня $\alpha$ более узкими границами; это не отразится, однако, на справедливости неравенств (3). Пусть $a_0$ будет та из границ $a$, $b$, в которой следует применять метод Ньютона. На основании формулы (2) мы последовательно получим в качестве приближенных значений корня $\alpha$ числа $a_1, a_2, \ldots, a_k, \ldots$, лежащие в отрезке $(a, b)$ и связанные между собой равенствами

$$a_k = a_{k-1} - \frac{f(a_{k-1})}{f'(a_{k-1})}, \quad k = 1, 2, \ldots \tag{5}$$

Пусть

$$\alpha = a_k + h_k, \quad k = 0, 1, 2, \ldots \tag{6}$$

Тогда

$$0 = f(\alpha) = f(a_k) + h_k f'(a_k) + \frac{h_k^2}{2} f''(a_k + \theta h_k),$$

где $0 < \theta < 1$. Так как $f'(a_k) \neq 0$ ввиду условия, наложенного на отрезок $(a, b)$, то, учитывая (5) и (6), получим:

$$-\frac{h_k^2}{2}\frac{f''(a_k+\theta h_k)}{f'(a_k)} = h_k + \frac{f(a_k)}{f'(a_k)} = \alpha - \left(a_k - \frac{f(a_k)}{f'(a_k)}\right) = \alpha - a_{k+1} = h_{k+1}.$$

Отсюда

$$|h_{k+1}| = h_k^2 \left|\frac{f''(a_k+\theta h_k)}{2f'(a_k)}\right| < h_k^2 \frac{B}{2A} = Ch_k^2, \quad k = 0, 1, 2, \ldots$$

Таким образом,

$$|h_{k+1}| < Ch_k^2 < C^3 h_{k-1}^4 < C^7 h_{k-2}^8 < \ldots < C^{2^{k+1}-1} h_0^{2^{k+1}}$$

или, так как $|h_0| = |\alpha - a_0| < b - a$,

$$|h_{k+1}| < C^{-1}[C(b-a)]^{2^{k+1}}, \quad k = 0, 1, 2, \ldots \tag{7}$$

Отсюда, ввиду условия (4), следует, что *разность* $h_k$ *между корнем* $\alpha$ *и его приближенным значением* $a_k$, *полученным последовательным применением метода Ньютона, стремится к нулю при возрастании* $k$, что и требовалось доказать.

Отметим, что формула (7) дает *оценку погрешности* для $(k+1)$-го шага, что существенно, если метод Ньютона применяется один, а не в комбинации с методом линейной интерполяции.

В курсах теории приближенных вычислений читатель может познакомиться со способами более рационального расположения вычислений в изложенных выше методах, облегчающими их применение. В этих же курсах можно найти изложение многих других методов приближенного вычисления корней. Среди них наиболее совершенным является *метод Лобачевского* (иногда ошибочно называемый методом Греффе). Этот метод позволяет находить приближенные значения всех корней сразу, в том числе и комплексных, причем не требует предварительного отделения корней; он связан, однако, с весьма громоздкими вычислениями. В основе этого метода лежит излагаемая ниже, в гл. 11, теория симметрических многочленов.

## ГЛАВА ДЕСЯТАЯ

# ПОЛЯ И МНОГОЧЛЕНЫ

### § 43. Числовые кольца и поля

В очень многих предшествующих разделах курса мы оказывались в следующем положении: излагая материал, мы допускали к рассмотрению или любые комплексные числа, или же только действительные числа, но затем должны были делать замечание, что полученные результаты остаются справедливыми, если ограничиться лишь действительными числами (или, соответственно, что они дословно переносятся на случай любых комплексных чисел). Как правило, во всех этих случаях можно было заметить, что изложенная теория полностью сохранилась бы и в том случае, если бы мы допустили к рассмотрению лишь рациональные числа. Настало время показать читателю истинные причины этого параллелизма с тем, чтобы излагать дальнейший материал в естественной для него общности, т. е. на общепринятом алгебраическом языке. С этой целью мы введем понятие поля, а также более широкое, но в нашем курсе играющее лишь служебную роль, понятие кольца.

Очевидно, что системы всех комплексных, всех действительных и всех рациональных чисел, равно как и система всех целых чисел, *обладают тем общим свойством, что в каждой из них не только сложение и умножение, но и вычитание можно выполнять, оставаясь в пределах самой этой системы.* Это свойство указанных числовых систем отличает их, например, от системы положительных целых или положительных действительных чисел.

Всякая система чисел, комплексных или, в частности, действительных, содержащая сумму, разность и произведение любых двух своих чисел, называется *числовым кольцом.* Таким образом, системы всех целых, рациональных, действительных и комплексных чисел являются числовыми кольцами. С другой стороны, никакая система положительных чисел не будет кольцом, так как если $a$ и $b$ — два различных положительных числа, то либо $a-b$, либо $b-a$ отрицательно. Не будет кольцом и никакая система отрицательных чисел хотя бы потому, что произведение двух отрицательных чисел положительно.

Числовые кольца далеко не исчерпываются рассмотренными выше четырьмя примерами. Сейчас будут указаны некоторые другие при-

меры, причем проверка утверждения, что рассматриваемая система чисел действительно является кольцом, каждый раз предоставляется читателю.

Четные числа составляют кольцо; вообще при любом натуральном $n$ совокупность целых чисел, нацело делящихся на $n$, будет кольцом. Нечетные числа кольца не составляют, так как сумма двух нечетных чисел четна.

Кольцом будет совокупность рациональных чисел, знаменатели записей которых в виде несократимой дроби являются какими-либо степенями числа 2; к этой совокупности принадлежат, в частности, все целые числа, так как их несократимые записи имеют знаменателем число 1, т. е. два в нулевой степени. В этом примере вместо числа 2 можно взять, конечно, любое простое число $p$. Вообще, беря любое множество простых чисел, конечное или даже бесконечное, и рассматривая систему рациональных чисел, знаменатели несократимых записей которых могут делиться лишь на простые числа, принадлежащие к взятому множеству, мы также получим кольцо. С другой стороны, совокупность рациональных чисел, знаменатели несократимых записей которых не делятся на квадрат никакого простого числа, не будет кольцом, так как указанное свойство чисел не сохраняется при их умножении.

Переходим к примерам числовых колец, не лежащих целиком в кольце рациональных чисел. Совокупность чисел вида

$$a+b\sqrt{2}, \tag{1}$$

где $a$ и $b$ — любые рациональные числа, будет кольцом; к этому кольцу принадлежат, в частности, все рациональные числа (при $b=0$), а также само число $\sqrt{2}$ (при $a=0$, $b=1$). Мы получили бы также кольцо, если бы ограничились лишь числами вида (1) с целыми коэффициентами $a$, $b$. В этих примерах можно, конечно, вместо числа $\sqrt{2}$ взять $\sqrt{3}$ или $\sqrt{5}$ и т. д.

Система чисел вида

$$a+b\sqrt[3]{2} \tag{2}$$

с любыми рациональными (или лишь с любыми целыми) коэффициентами $a$, $b$ не будет кольцом, так как произведение числа $\sqrt[3]{2}$ на самого себя нельзя, как легко проверить, записать в виде (2) [1]. Однако система чисел вида

$$a+b\sqrt[3]{2}+c\sqrt[3]{4} \tag{3}$$

с любыми рациональными коэффициентами $a$, $b$, $c$ уже будет кольцом, и это же имеет место, если ограничиться случаем целых коэффициентов.

---

[1]) Действительно, пусть

$$\sqrt[3]{4}=a+b\sqrt[3]{2}, \tag{2'}$$

где числа $a$ и $b$ рациональны. Умножая обе части этого равенства на $\sqrt[3]{2}$,

Рассмотрим теперь все действительные числа, которые можно получить, применяя несколько раз операции сложения, умножения и вычитания к хорошо известному читателю числу $\pi$ и каким-либо рациональным числам. Это будут числа, которые могут быть записаны в виде

$$a_0 + a_1\pi + a_2\pi^2 + \ldots + a_n\pi^n, \tag{4}$$

где $a_0, a_1, a_2, \ldots, a_n$ — рациональные числа, $n \geqslant 0$. Заметим, что никакое число не может обладать двумя различными записями вида (4) — в противном случае, беря разность двух таких записей, мы получили бы, что число $\pi$ удовлетворяет некоторому уравнению с рациональными коэффициентами; методами математического анализа доказывается, однако, что $\pi$ не может удовлетворять на самом деле никакому уравнению с рациональными коэффициентами, т. е. является числом трансцендентным. Не используя, впрочем, этого результата, т. е. не предполагая, что запись числа в виде (4) однозначна, можно все же показать, что числа вида (4) составляют кольцо.

Кольцом будет также совокупность чисел, получающихся из числа $\pi$ и рациональных чисел при помощи операций сложения, умножения, вычитания и деления, примененных несколько раз. Для доказательства нет необходимости искать для рассматриваемых чисел какую-либо специальную хорошую запись (хотя она и может быть найдена): если числа $\alpha$ и $\beta$ получены из числа $\pi$ и некоторых рациональных чисел указанными операциями, то это же верно, понятно, и для чисел $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, а также (при $\beta \neq 0$) для числа $\frac{\alpha}{\beta}$.

Наконец, взяв совокупность комплексных чисел $a+bi$ с любыми рациональными $a$, $b$, мы получим кольцо; это же будет иметь место, если мы ограничимся целыми коэффициентами $a$, $b$.

Рассмотренные примеры не могут дать полного представления о том, сколь разнообразными бывают числовые кольца. Мы не будем пока, однако, продолжать наш список примеров и перейдем к рассмотрению одного специального и очень важного типа числовых

---

получим:

$$2 = a\sqrt[3]{2} + b\sqrt[3]{4}.$$

Подставляя сюда выражение (2′) для $\sqrt[3]{4}$, мы после очевидных преобразований придем к равенству

$$(a+b^2)\sqrt[3]{2} = 2 - ab. \tag{2''}$$

Если $a+b^2 \neq 0$, то

$$\sqrt[3]{2} = \frac{2-ab}{a+b^2},$$

что невозможно, так как справа стоит рациональное число. Если же $a+b^2=0$, то, ввиду (2″), и $2-ab=0$. Из этих двух равенств вытекает $b^3=-2$, что снова невозможно ввиду рациональности числа $b$.

колец. Мы знаем, конечно, что в системах всех рациональных, всех действительных и всех комплексных чисел можно неограниченно выполнять деление (кроме деления на нуль), в то время как деление целых чисел выводит за пределы системы этих чисел. До сих пор мы не обращали серьезного внимания на это различие, в действительности же оно очень существенно и приводит к следующему определению.

Числовое кольцо называется *числовым полем*, если оно содержит частное любых двух своих чисел (делитель предполагается, конечно, отличным от нуля). Можно говорить, следовательно, о поле рациональных чисел, поле действительных чисел, полекомплексных чисел, в то время как кольцо целых чисел полем не является.

Некоторые из рассмотренных выше примеров числовых колец в действительности являются полями. Сначала заметим, что не существует числовых полей, отличных от поля рациональных чисел и целиком в нем содержащихся (систему, состоящую из одного нуля, мы не будем считать полем). Справедливо даже следующее более общее утверждение:

*Поле рациональных чисел содержится целиком во всяком числовом поле.*

Пусть, в самом деле, дано некоторое числовое поле, которое мы обозначим буквой $P$. Если $a$ — любое число поля $P$, отличное от нуля, то $P$ содержит и частное от деления числа $a$ на самого себя, т. е. число единицу. Складывая единицу с самой собою несколько раз, мы получим, что все натуральные числа содержатся в поле $P$. С другой стороны, в поле $P$ должна содержаться разность $a-a$, т. е. число нуль, а поэтому к $P$ принадлежит и результат вычитания любого натурального числа из нуля, т. е. любое целое отрицательное число. Наконец, в поле $P$ лежат и частные целых чисел, т. е. вообще все рациональные числа.

В поле комплексных чисел содержится много различных полей, и поле рациональных чисел будет лишь наименьшим среди них. Так, рассмотренное выше кольцо чисел вида

$$a+b\sqrt{2} \tag{5}$$

с любыми рациональными (а не только лишь с целыми) коэффициентами $a$, $b$ будет полем. В самом деле рассмотрим частное двух чисел вида (5), $a+b\sqrt{2}$ и $c+d\sqrt{2}$, причем второе число считаем отличным от нуля; отлично от нуля, следовательно, и число $c-d\sqrt{2}$, и потому

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2}.$$

Мы получили снова число вида (5), причем коэффициенты остаются рациональными. В этом примере число $\sqrt{2}$ можно заменить,

понятно, квадратным корнем из любого рационального числа, из которого в самом поле рациональных чисел не извлекается квадратный корень. Так, поле составляют числа вида $a+bi$ с рациональными $a$, $b$.

## § 44. Кольцо

В различных отделах математики, а также в применениях математики к технике и естествознанию приходится весьма часто встречаться с положением, когда алгебраические операции производятся не над числами, а над объектами совсем иной природы. Большое число таких примеров можно найти в предшествующих главах книги — напомним умножение и сложение матриц, сложение векторов, операции над многочленами, операции над линейными преобразованиями. Общее определение *алгебраической операции*, которому удовлетворяют операции сложения и умножения в числовых кольцах, а также операции в указанных примерах, состоит в следующем.

Пусть дано некоторое множество $M$, состоящее или из чисел, или из объектов геометрической природы, вообще из некоторых вещей, которые мы будем называть *элементами* этого множества. Говорят, что *в множестве $M$ определена алгебраическая операция*, если указан закон, по которому любой паре элементов $a$, $b$ из этого множества однозначным образом ставится в соответствие некоторый третий элемент $c$, также принадлежащий к $M$. Эта операция может быть названа *сложением*, и тогда $c$ будет называться *суммой* элементов $a$ и $b$ и обозначаться символом $c=a+b$; эта операция может быть названа *умножением*, т. е. $c$ будет *произведением* элементов $a$ и $b$, $c=ab$; возможно, наконец, что для операции, определенной в множестве $M$, будет введена новая терминология и символика.

В каждом из числовых колец определены две независимые операции — сложение и умножение. Что же касается вычитания и деления, то их нельзя считать новыми операциями, так как они являются обратными соответственно для сложения и для умножения, если мы примем следующее общее определение *обратной операции*.

Пусть в множестве $M$ определена алгебраическая операция, например сложение. Говорят, что *для этой операции существует обратная операция* — вычитание, если для любой пары элементов $a$, $b$ из $M$ существует в $M$ такой элемент $d$, притом лишь единственный, который удовлетворяет равенству $b+d=a$. Элемент $d$ называется тогда *разностью* элементов $a$ и $b$ и обозначается символом $d=a-b$.

В числовых полях обратной операцией обладает, очевидно, как сложение, так и умножение (последнее, правда, ограниченно: делитель должен быть отличным от нуля). В числовых же кольцах, не являющихся полями (как, например, в кольце целых чисел), обратной операцией обладает лишь сложение.

С другой стороны, в системе всех многочленов от неизвестного $x$, коэффициенты которых принадлежат к фиксированному числовому полю $P$, также определены две операции — сложение и умножение, причем сложение обладает обратной операцией — вычитанием.

И в числовых кольцах, и в системе многочленов операции сложения и умножения обладают, как известно, следующими свойствами ($a$, $b$, $c$ — произвольные числа из рассматриваемого числового кольца или произвольные многочлены из рассматриваемой системы):

I. Сложение коммутативно: $a+b=b+a$.

II. Сложение ассоциативно: $a+(b+c)=(a+b)+c$.

III. Умножение коммутативно: $ab=ba$.

IV. Умножение ассоциативно: $a(bc)=(ab)c$.

V. Сложение и умножение связаны законом дистрибутивности:

$$(a+b)c=ac+bc.$$

Мы уже подготовлены теперь к общему определению понятия кольца, одного из важнейших понятий алгебры.

Множество $R$ называется *кольцом*, если в нем определены две операции — сложение и умножение, обе коммутативные и ассоциативные, а также связанные законом дистрибутивности, причем сложение обладает обратной операцией — вычитанием.

Таким образом, примерами колец являются числовые кольца и кольца многочленов от неизвестного $x$ с коэффициентами из данного числового поля или даже из данного числового кольца. Укажем еще один пример, хорошо выясняющий широту понятия кольца.

Курс математического анализа начинается с определения функции действительного переменного $x$. Рассмотрим совокупность функций, определенных для всех действительных значений $x$ и принимающих действительные значения, и следующим образом определим в этой совокупности алгебраические операции: *суммой* двух функций $f(x)$ и $g(x)$ будет функция, значение которой при любом $x=x_0$ равно сумме значений заданных функций, т. е. равно $f(x_0)+g(x_0)$, *произведением* этих функций — функция, значение которой при всяком $x=x_0$ равно произведению $f(x_0)\cdot g(x_0)$. Сумма и произведение существуют, очевидно, для любых двух функций из рассматриваемой совокупности. Справедливость свойств I — V проверяется без всяких затруднений — сложение и умножение функций сводятся к сложению и умножению их значений при всяком $x$, т. е. к операциям над действительными числами, для которых свойства I — V имеют место. Наконец, считая *разностью* функций $f(x)$ и $g(x)$ функцию, значение которой при любом $x=x_0$ равно разности $f(x_0)-g(x_0)$, мы придем к операции вычитания, обратной сложению. Этим доказано, что *совокупность функций, определенных для всех действительных $x$, после введения в нее описанным выше способом операций сложения и умножения превращается в кольцо.*

Другие примеры колец функций можно получить, сохраняя данные выше определения операций над функциями, но рассматривая функции, определенные, например, лишь для положительных значений переменного $x$, или функции, определенные для значений $x$ из отрезка $[0, 1]$. Вообще кольцом будет система всех функций, имеющих некоторую данную область определения. Можно было бы получить также примеры колец, рассматривая не все функции, определенные в данной области, а лишь изучаемые в курсе математического анализа непрерывные функции. Можно было бы, с другой стороны, рассматривать комплексные функции комплексного переменного. Вообще, различных колец функций, как и различных числовых колец, чрезвычайно много.

Переходим к установлению некоторых простейших свойств колец, непосредственно вытекающих из определения кольца. Эти свойства для случая чисел вполне привычны, однако читателю, быть может, покажется иногда неожиданным, что они являются следствиями лишь условий I—V и существования однозначного вычитания.

Сначала несколько замечаний о значении условий I—V. Роль *законов коммутативности* не требует пояснений. Значение *законов ассоциативности* состоит в следующем: в определении алгебраической операции говорится о сумме или произведении лишь двух элементов. Если же мы попытаемся определить, например, произведение трех элементов $a$, $b$, $c$, то встретимся с таким затруднением: произведения $au$ и $vc$, где $bc=u$, $ab=v$, могут, вообще говоря, не совпадать, т. е. $a(bc)\neq(ab)c$. Закон ассоциативности требует, чтобы эти произведения были равны одному и тому же элементу кольца: этот элемент естественно принять в качестве произведения $abc$, записываемого уже без всяких скобок. Больше того, *закон ассоциативности позволяет однозначным образом определить произведение (соответственно, сумму) для любого конечного числа элементов кольца*, т. е. позволяет доказать независимость произведения любых $n$ элементов от первоначального распределения скобок.

Докажем это утверждение индукцией по числу $n$. Для $n=3$ оно уже доказано, поэтому полагаем $n>3$, причем считаем, что для всех чисел, меньших $n$, наше утверждение уже доказано. Пусть даны элементы $a_1, a_2, \ldots, a_n$ и пусть в этой системе некоторым образом распределены скобки, указывающие на порядок, в каком должно выполняться умножение. Последним шагом будет умножение произведения первых $k$ элементов $a_1a_2\ldots a_k$ (где $1\leqslant k\leqslant n-1$) на произведение $a_{k+1}a_{k+2}\ldots a_n$. Так как эти произведения состоят из меньшего, чем $n$, числа множителей и поэтому, по предположению, однозначно определены, то нам остается доказать для любых $k$ и $l$ равенство

$$(a_1a_2\ldots a_k)(a_{k+1}a_{k+2}\ldots a_n)=(a_1a_2\ldots a_l)(a_{l+1}a_{l+2}\ldots a_n).$$

Для этого достаточно рассмотреть случай $l=k+1$. В этом случае, однако, полагая

$$a_1a_2\ldots a_k=b,\quad a_{k+2}a_{k+3}\ldots a_n=c,$$

мы получаем на основании закона ассоциативности

$$b(a_{k+1}c)=(ba_{k+1})c.$$

Этим наше утверждение доказано.

Можно говорить, в частности, о произведении $n$ равных между собою элементов, т. е. ввести понятие о *степени* $a^n$ элемента $a$ с целым положительным показателем $n$. Легко проверить, что все обычные правила оперирования с показателями остаются справедливыми в любом кольце. Закон ассоциативности сложения приводит аналогичным образом к понятию о *кратном* $na$ элемента $a$ с целым положительным коэффициентом $n$.

*Закон дистрибутивности*, т. е. обычное правило раскрытия скобок, является единственным требованием в определении кольца, связывающим сложение и умножение; лишь благодаря этому закону совместное изучение двух указанных операций дает больше, чем можно было бы получить при их раздельном изучении. В формулировке закона дистрибутивности участвует сумма лишь двух слагаемых. Без всякого труда доказывается, однако, справедливость равенства

$$(a_1+a_2+\ldots+a_k)\,b=a_1b+a_2b+\ldots+a_kb$$

при любом $k$, а затем и общего правила умножения суммы на сумму.

*Во всяком кольце выполняется закон дистрибутивности и для разности.* Действительно, по определению разности элемент $a-b$ удовлетворяет равенству

$$b+(a-b)=a.$$

Умножая обе части этого равенства на $c$ и применяя к левой части равенства закон дистрибутивности, мы получаем:

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

Элемент $(a-b)\,c$ является, следовательно, разностью элементов $ac$ и $bc$:

$$(a-b)\,c=ac-bc.$$

Весьма важные свойства колец вытекают из существования вычитания. Если $a$ есть произвольный элемент кольца $R$, то разность $a-a$ будет некоторым вполне определенным элементом кольца. Его роль аналогична роли нуля в числовых кольцах, однако по определению он может зависеть от выбора элемента $a$, и поэтому мы обозначим его пока через $0_a$.

Докажем, что на самом деле элементы $0_a$ для всех $a$ равны между собой. Действительно, если $b$ есть произвольный другой элемент кольца $R$, то, прибавляя к обеим частям равенства

$$a+(b-a)=b$$

элемент $0_a$ и используя равенство $0_a+a=a$, мы получаем:

$$0_a+b=0_a+a+(b-a)=a+(b-a)=b.$$

Таким образом, $0_a=b-b=0_b$.

Мы доказали, *что всякое кольцо $R$ обладает однозначно определенным элементом, сумма которого с любым элементом $a$ этого кольца равна $a$*. Будем называть этот элемент *нулем* кольца $R$ и обозначать символом 0, не считая серьезной опасность смешать его с числом нуль. Таким образом,

$$a+0=a \text{ для всех } a \text{ из } R.$$

Далее, *во всяком кольце для любого элемента $a$ существует однозначно определенный противоположный элемент $-a$, удовлетворяющий равенству*

$$a+(-a)=0,$$

а именно, этим элементом будет разность $0-a$; однозначность вытекает из однозначности вычитания. Очевидно, что $-(-a)=a$. Разность $b-a$ двух любых элементов кольца можно записать теперь в виде

$$b-a=b+(-a).$$

Действительно,

$$[b+(-a)]+a=b+[(-a)+a]=b+0=b.$$

*Для любого элемента $a$ кольца и любого целого положительного числа $n$ имеет место равенство*

$$n(-a)=-(na).$$

Действительно, группировкой слагаемых получаем:

$$na+n(-a)=n[a+(-a)]=n\cdot 0=0.$$

Мы получили теперь возможность определить *отрицательные кратные* элемента кольца: если $n>0$ то равные между собой элементы $n(-a)$ и $-(na)$ будут обозначаться через $(-n)a$. Условимся, наконец, *нулевым кратным* $0\cdot a$ любого элемента $a$ считать нуль рассматриваемого кольца.

Определение нуля дано нами лишь при помощи операции сложения и ей обратной, т. е. без использования умножения. В случае чисел, однако, число нуль и по отношению к умножению обладает одним характерным и притом очень важным свойством. Оказывается, что этим свойством обладает нуль любого кольца: *во всяком кольце произведение любого элемента на нуль равно нулю*. Доказательство непосредственно опирается на закон дистрибутивности: если $a$ есть произвольный элемент кольца $R$, то, каков бы ни был вспомогательный элемент $x$ этого кольца, мы получим:

$$a\cdot 0=a(x-x)=ax-ax=0.$$

Пользуясь этим свойством нуля, можно доказать, что *во всяком кольце для любых элементов $a$, $b$ справедливо равенство*

$$(-a)b=-ab.$$

Действительно,

$$ab+(-a)b=[a+(-a)]b=0\cdot b=0.$$

Отсюда следует, что хорошо известное и все же несколько таинственное правило умножения отрицательных чисел — «минус на минус дает плюс» — также вытекает из определения кольца, т. е. *в любом кольце имеет место равенство*

$$(-a)(-b)=ab.$$

В самом деле,

$$(-a)(-b)=-[a(-b)]=-(-ab)=ab.$$

Читатель без труда докажет теперь, что во всяком кольце для кратных (в том числе и отрицательных) любого элемента остаются справедливыми все правила оперирования с кратными некоторого числа.

Таким образом, алгебраические операции в произвольном кольце обладают многими привычными нам свойствами операций над числами. Не следует думать, однако, что любое свойство сложения и умножения чисел сохраняется во всяком кольце. Так, умножение чисел обладает свойством, обратным рассмотренному выше: если произведение двух чисел равно нулю, то хотя бы один из множителей равен нулю. Это свойство уже не может быть распространено на любые кольца — в некоторых кольцах можно указать такие пары отличных от нуля элементов, произведение которых равно нулю, т. е. $a\neq 0$, $b\neq 0$, но $ab=0$; элементы $a$, $b$ с этим свойством называются *делителями нуля*.

Примеров колец с делителями нуля нельзя найти, понятно, среди числовых колец. Не содержат делителей нуля и кольца многочленов с числовыми коэффициентами. Многие кольца функций обладают, однако, делителями нуля. Заметим, прежде всего, что нулем во всяком кольце функций будет функция, равная нулю при всех значениях переменного $x$. Построим теперь следующие функции $f(x)$ и $g(x)$, определенные для всех действительных значений $x$:

$$f(x)=0 \quad \text{при} \quad x\leqslant 0, \quad f(x)=x \quad \text{при} \quad x>0;$$
$$g(x)=x \quad \text{при} \quad x\leqslant 0, \quad g(x)=0 \quad \text{при} \quad x>0.$$

Обе эти функции отличны от нуля, так как не при всех значениях $x$ равны нулю их значения; произведение же этих функций равно нулю.

Не все требования I — V, входящие в определение кольца, являются в одинаковой мере необходимыми. Развитие науки показывает, что в то время как свойства еложения I и II и закон дистрибутивности V имеют место во всех приложениях, включение в определение кольца свойств умножения III и IV часто оказывается излишне стеснительным, суживая возможную область применимости этого понятия. Так, множество квадратных матриц порядка $n$ с действительными элементами, рассматриваемое с операциями сложения и умножения матриц, удовлетворяет всем требованиям, входящим в определение кольца, за исключением закона коммутативности умножения.

С некоммутативными умножениями приходится встречаться так часто и в таких важных случаях, что в настоящее время под термином «кольцо» понимают обычно *некоммутативное кольцо* (точнее, не обязательно коммутативное кольцо, в смысле возможной некоммутативности умножения), называя тот частный тип колец, в которых требование III выполняется, *коммутативными кольцами*.

В последнее время повышается интерес и к кольцам с неассоциативным умножением и общая теория колец уже строится сейчас как теория неассоциативных (т. е. не обязательно ассоциативных) колец. Простейшим примером таких колец является множество векторов трехмерного евклидова пространства относительно операций сложения и (известного из курса аналитической геометрии) векторного умножения векторов.

## § 45. Поле

Подобно тому как среди числовых колец были выделены и названы числовыми полями те кольца, в которых можно выполнять деление (кроме деления на нуль), естественно сделать это и в общем случае. Заметим сначала, что *ни в каком кольце невозможно деление на нуль* ввиду доказанного выше свойства нуля по отношению к умножению: разделить элемент $a$ на нуль означает найти в кольце такой элемент $x$, что $0 \cdot x = a$, что при $a \neq 0$ невозможно, так как левая часть равна нулю.

Введем следующее определение:

Кольцо $P$ называется *полем*, если оно состоит не только из одного нуля и если в нем деление выполнимо, притом однозначным образом, во всех случаях, кроме случая деления на нуль, т. е. если для любых элементов $a$ и $b$ из $P$, из которых $b$ отлично от нуля, существует в $P$ такой элемент $q$, притом лишь единственный, который удовлетворяет равенству $bq = a$. Элемент $q$ называется *частным* элементов $a$ и $b$ и обозначается символом $q = \frac{a}{b}$ [1]).

Примерами полей служат, понятно, все числовые поля. Кольцо многочленов от неизвестного $x$ с действительными коэффициентами или вообще с коэффициентами из некоторого числового поля не является полем — существующее для многочленов деление с остатком отличается, конечно, от деления «нацело», предполагающегося в определении поля. С другой стороны, легко видеть, что *совокупность всех дробно-рациональных функций с действительными коэффициентами* (см. § 25) *будет полем*, содержащим кольцо многочленов, подобно тому как поле рациональных чисел содержит кольцо целых чисел.

Среди колец функций можно указать некоторые другие примеры полей; мы не будем, однако, на них останавливаться и перейдем к примерам совсем иного рода.

---

[1]) Единственность деления в поле, как и предполагавшаяся в определении кольца единственность вычитания, в действительности без труда могут быть доказаны при помощи других требований, входящих в определение поля или, соответственно, кольца.

Все числовые кольца и вообще кольца, которые мы до сих пор рассматривали, содержат бесконечно много элементов. Существуют, однако, кольца и даже поля, состоящие лишь из конечного числа элементов. Простейшие примеры *конечных колец* и *конечных полей*, существенно используемые в особой ветви математики — теории чисел, строятся следующим образом.

Берем любое натуральное число $n$, отличное от 1. Целые числа $a$ и $b$ называются *сравнимыми по модулю* $n$,

$$a \equiv b \pmod{n},$$

если эти числа дают при делении на $n$ один и тот же остаток, т. е. если их разность нацело делится на $n$. Все кольцо целых чисел распадается на $n$ непересекающихся классов,

$$C_0,\ C_1,\ \ldots,\ C_{n-1}, \tag{1}$$

сравнимых между собой по модулю $n$ чисел, причем класс $C_k$, $k=0, 1, \ldots, n-1$, состоит из чисел, дающих при делении на $n$ в остатке $k$. Оказывается, что можно вполне естественным способом определить сложение и умножение этих классов.

Возьмем с этой целью любые (притом не обязательно различные) классы $C_k$ и $C_l$ из системы (1). Складывая любое число из класса $C_k$ с любым числом из класса $C_l$, мы будем получать числа, лежащие в одном вполне определенном классе, а именно в классе $C_{k+l}$, если $k+l<n$, или в классе $C_{k+l-n}$, если $k+l \geqslant n$. Это приводит к такому определению *сложения классов*:

$$\begin{aligned} C_k + C_l &= C_{k+l} \quad \text{при} \quad k+l<n, \\ C_k + C_l &= C_{k+l-n} \quad \text{при} \quad k+l \geqslant n. \end{aligned} \tag{2}$$

С другой стороны, умножая любое число класса $C_k$ на любое число класса $C_l$, мы будем получать числа, снова лежащие во вполне определенном классе, а именно в классе $C_r$, где $r$ — остаток при делении произведения $kl$ на $n$. Мы принимаем поэтому такое определение *умножения классов*:

$$C_k \cdot C_l = C_r, \text{ где } kl = nq + r,\ 0 \leqslant r < n. \tag{3}$$

*Система* (1) *классов целых чисел, сравнимых между собой по модулю* $n$, *будет кольцом по отношению к операциям, определенным условиями* (2) *и* (3). В самом деле, справедливость требований I—V из определения кольца без труда устанавливается непосредственной проверкой, но вытекает также из справедливости этих требований в кольце целых чисел и той связи между операциями над целыми числами и операциями над классами, которая указана выше. Роль нуля играет, очевидно, класс $C_0$, состоящий из чисел, нацело делящихся на $n$. Противоположным для класса $C_k$, $k=1, 2, \ldots, n-1$, будет класс $C_{n-k}$. В системе классов (1) можно

определить, следовательно, вычитание, т. е. эта система удовлетворяет всем требованиям, входящим в определение кольца. Условимся обозначать полученное кольцо через $Z_n$.

*Если число $n$ составное, то кольцо $Z_n$ обладает делителями нуля* и поэтому, как будет показано ниже, не может быть полем. В самом деле, если $n=kl$, где $1<k<n$, $1<l<n$, то классы $C_k$ и $C_l$ отличны от нулевого класса $C_0$, но на основании определения умножения классов (см. (3)) $C_k \cdot C_l = C_0$.

*Если же число $n$ простое, то кольцо $Z_n$ будет полем.*

В самом деле, пусть даны классы $C_k$ и $C_m$, причем $C_k \neq C_0$, т. е. $1 \leqslant k \leqslant n-1$. Нужно показать, что можно разделить $C_m$ на $C_k$, т. е. найти такой класс $C_l$, что $C_k \cdot C_l = C_m$. Если $C_m = C_0$, то и $C_l = C_0$. Если же $C_m \neq C_0$, то рассмотрим систему чисел

$$k,\ 2k,\ 3k,\ \ldots,\ (n-1)\,k. \tag{4}$$

Все эти числа лежат вне нулевого класса $C_0$, так как произведение двух натуральных чисел, меньших простого числа $n$, не может на $n$ делиться. Далее, никакие два числа $sk$ и $tk$ из системы (4), $s<t$, не могут лежать в одном классе, так как тогда их разность

$$tk - sk = (t-s)\,k$$

делилась бы на $n$, что снова противоречит простоте числа $n$. Таким образом, в каждом ненулевом классе лежит ровно одно число из системы (4). В частности, в классе $C_m$ лежит число $lk$, где $1 \leqslant l \leqslant n-1$, т. е. $C_l \cdot C_k = C_m$, а тогда класс $C_l$ и будет искомым частным от деления $C_m$ на $C_k$.

Мы получили, таким образом, бесконечно много различных конечных полей: поле $Z_2$, состоящее всего из двух элементов, а также поля $Z_3$, $Z_5$, $Z_7$, $Z_{11}$ и т. д.

Переходим к рассмотрению некоторых свойств полей, вытекающих из существования деления. Эти свойства аналогичны свойствам колец, основанным на существовании вычитания, и доказываются такими же рассуждениями, поэтому проведение доказательств предоставляется читателю.

*Всякое поле $P$ обладает однозначно определенным элементом, произведение которого на любой элемент $a$ этого поля равно $a$.* Этот элемент, совпадающий с равными между собою частными $\frac{a}{a}$ для всех $a$, отличных от нуля, называется *единицей* поля $P$ и обозначается символом 1. Таким образом,

$$a \cdot 1 = a \quad \text{для всех } a \text{ из } P.$$

*Во всяком поле для любого элемента $a$, отличного от нуля, существует однозначно определенный обратный элемент $a^{-1}$, удовлетворяющий равенству*

$$a \cdot a^{-1} = 1,$$

а именно, $a^{-1}=\frac{1}{a}$. Очевидно, что $(a^{-1})^{-1}=a$. Частное $\frac{b}{a}$ можно записать теперь в виде

$$\frac{b}{a}=b\cdot a^{-1}.$$

Для любого элемента $a$, отличного от нуля, и любого целого положительного числа $n$ имеет место равенство

$$(a^{-1})^n=(a^n)^{-1}.$$

Обозначая эти равные между собою элементы через $a^{-n}$, мы приходим к *отрицательным степеням* элемента поля, для которых сохраняются обычные правила оперирования. Положим, наконец, $a^0=1$ для всех $a$.

Существование единицы не является характерным свойством полей: единицей обладает, например, кольцо целых чисел. Вместе с тем, пример кольца четных чисел показывает, что не все кольца обладают единицей. С другой стороны, *всякое кольцо, обладающее единицей и содержащее обратный элемент для любого элемента, отличного от нуля, будет полем.* Действительно, в этом случае частным $\frac{b}{a}$, $a\neq 0$, будет служить произведение $ba^{-1}$. Единственность этого частного доказывается без затруднений.

Заметим, что *никакое поле не содержит делителей нуля.* Действительно, пусть $ab=0$, но $a\neq 0$. Умножая обе части равенства на элемент $a^{-1}$, мы получим слева $(a^{-1}a)b=1\cdot b=b$, а справа $a^{-1}\cdot 0=0$, т. е. $b=0$. Отсюда следует, что *во всяком поле любое равенство можно сократить на общий множитель, отличный от нуля.* В самом деле, если $ac=bc$ и $c\neq 0$, то $(a-b)c=0$, откуда $a-b=0$, т. е. $a=b$.

Из определения частного $\frac{a}{b}$ (где $b\neq 0$) и доказанной выше возможности записывать его в виде произведения $ab^{-1}$ без труда может быть выведено, что *во всяком поле сохраняются все обычные правила обращения с дробями,* а именно:

$$\frac{a}{b}=\frac{c}{d} \text{ тогда и только тогда, если } ad=bc;$$

$$\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd};$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd};$$

$$\frac{-a}{b}=-\frac{a}{b}.$$

**Характеристика поля.** Не все свойства числовых полей сохраняются в случае произвольного поля. Так, складывая число 1 само с собою несколько раз, т. е. беря любое целое положительное

кратное единицы, мы никогда не получим нуля, и вообще все эти кратные, т. е. все натуральные числа, отличны друг от друга. Если же мы будем брать целые кратные единицы в каком-либо конечном поле, то среди них непременно будут равные, так как это поле обладает лишь конечным числом различных элементов. Если все целые кратные единицы поля $P$ являются различными элементами поля $P$, т. е. $k\cdot 1 \neq l\cdot 1$ при $k \neq l$, то говорят, что поле $P$ имеет *характеристику нуль*; таковы, например, все числовые поля. Если же существуют такие целые числа $k$ и $l$, что $k > l$, но в $P$ имеет место равенство $k\cdot 1 = l\cdot 1$, то $(k-l)\cdot 1 = 0$, т. е. в $P$ существует такое положительное кратное единицы, которое оказывается равным нулю. В этом случае $P$ называется полем *конечной характеристики*, а именно *характеристики* $p$, если $p$ есть тот первый положительный коэффициент, с которым единица поля $P$ обращается в нуль. Примерами полей конечной характеристики служат все конечные поля; существуют, впрочем, и бесконечные поля, имеющие конечную характеристику.

*Если поле $P$ имеет характеристику $p$, то число $p$ будет простым.*

Действительно, из равенства $p = st$, где $s < p$, $t < p$, вытекало бы равенство $(s\cdot 1)(t\cdot 1) = p\cdot 1 = 0$, т. е., так как в поле не может быть делителей нуля, или $s\cdot 1 = 0$, или $t\cdot 1 = 0$, что, однако, противоречит определению характеристики как наименьшего положительного коэффициента, обращающего единицу поля в нуль.

*Если характеристика поля $P$ равна $p$, то для любого элемента $a$ из этого поля имеет место равенство $pa = 0$. Если же характеристика поля $P$ равна 0 и $a$ — элемент этого поля, $n$ — целое число, то из $a \neq 0$ и $n \neq 0$ следует $na \neq 0$.*

Действительно, в первом случае элемент $pa$, т. е. сумму $p$ слагаемых, равных $a$, можно, вынося $a$ за скобки, представить в виде

$$pa = a(p\cdot 1) = a\cdot 0 = 0.$$

Во втором случае из равенства $na = 0$, т. е. $a(n\cdot 1) = 0$, следовало бы при $a \neq 0$ равенство $n\cdot 1 = 0$, т. е., так как характеристика поля равна нулю, $n = 0$.

**Подполя, расширения.** Пусть в поле $P$ некоторая часть его элементов, составляющая множество $P'$, сама оказывается полем по отношению к тем операциям, которые определены в поле $P$, т. е. для любых двух элементов $a$, $b$ из $P'$ содержащиеся в поле $P$ элементы $a+b$, $ab$, $a-b$ и, при $b \neq 0$, $\frac{a}{b}$ принадлежат к $P'$ (законы I—V, выполняясь в $P$, будут, конечно, выполняться и в $P'$). Тогда $P'$ называется *подполем* поля $P$, а $P$ — *расширением* поля $P'$. Понятно, что нуль и единица поля $P$ будут содержаться также в $P'$ и служить для $P'$ нулем и единицей. Так, поле рациональных чисел

является подполем поля действительных чисел; все числовые поля будут подполями поля комплексных чисел.

Пусть в поле $P$ даны подполе $P'$ и элемент $c$, лежащий вне $P'$, и пусть мы нашли минимальное подполе $P''$ поля $P$, содержащее и $P'$, и $c$. Такое минимальное подполе может быть только одно, так как если бы $P'''$ было еще одно подполе с этими свойствами, то пересечение подполей $P''$ и $P'''$ (т. е. совокупность элементов, общих обоим подполям) содержало бы $P'$ и элемент $c$ и вместе с любыми двумя своими элементами содержало бы их сумму (эта сумма должна содержаться и в $P''$, и в $P'''$, а потому и в их пересечении), а также их произведение, разность и частное; иными словами, это пересечение само было бы подполем, в противоречие с минимальностью подполя $P''$. Мы будем говорить, что поле $P''$ *получено присоединением к полю $P'$ элемента $c$*, и употреблять запись $P''=P'(c)$.

Понятно, что поле $P'(c)$ содержит, помимо элемента $c$ и всех элементов поля $P'$, также все элементы, которые получаются из них при помощи сложения, умножения, вычитания и деления. В качестве примера укажем на рассматривавшееся в § 43 расширение поля рациональных чисел, состоящее из чисел вида $a+b\sqrt{2}$ с рациональными $a$, $b$: это расширение получается присоединением к полю рациональных чисел числа $\sqrt{2}$.

## § 46*. Изоморфизм колец (полей). Единственность поля комплексных чисел

В теории колец большую роль играет понятие изоморфизма. Именно, кольца $L$ и $L'$ называются *изоморфными*, если между ними можно установить такое взаимно однозначное соответствие, при котором для любых элементов $a$, $b$ из $L$ и соответствующих им элементов $a'$, $b'$ из $L'$ сумме $a+b$ соответствует сумма $a'+b'$, а произведению $ab$ соответствует произведение $a'b'$.

Пусть между кольцами $L$ и $L'$ установлено изоморфное соответствие. *При этом соответствии нулю* 0 *кольца $L$ соответствует нуль* $0'$ *кольца $L'$*. Действительно, пусть элементу 0 соответствует элемент $c'$ из $L'$. Берем произвольный элемент $a$ из $L$ и соответствующий ему элемент $a'$ из $L'$. Тогда элементу $a+0$ должен соответствовать элемент $a'+c'$; но $a+0=a$, поэтому $a'+c'=a'$, откуда $c'=0'$. Далее, *элементу $-a$ соответствует элемент $-a'$*. Действительно, пусть элементу $-a$ соответствует элемент $d'$. Тогда элементу $a+(-a)=0$ должен соответствовать элемент $a'+d'$, т. е. $a'+d'=0'$, откуда $d'=-a'$. Отсюда следует, что *разности элементов из $L$ соответствует разность соответствующих элементов в $L'$*. Аналогичными рассуждениями можно показать, что если кольцо $L$ обладает единицей, то образ этого элемента (т. е. элемент, соответствующий ему в $L'$ при рассматриваемом изоморфизме) будет единицей кольца $L'$, и если элемент $a$ из $L$

обладает обратным элементом $a^{-1}$, то образом элемента $a^{-1}$ в $L'$ будет элемент, обратный к $a'$.

Отсюда следует, что *кольцо, изоморфное полю, само будет полем.* Легко видеть также, что свойство кольца не иметь делителей нуля также сохраняется при изоморфном соответствии. Вообще, изоморфные кольца могут отличаться друг от друга природой своих элементов, но они тождественны по своим алгебраическим свойствам; всякая теорема, доказанная относительно некоторого кольца, будет справедливой для всех колец, с ним изоморфных, если только в доказательстве теоремы использовались лишь свойства операций, а не индивидуальные свойства элементов этого кольца. По этой причине *мы не будем считать изоморфные кольца или поля различными*; они будут для нас лишь разными экземплярами одного и того же кольца или поля.

Применим это понятие к вопросу о построении поля комплексных чисел. Изложенная в § 17 конструкция поля комплексных чисел, основанная на использовании точек плоскости, не является единственно возможной. Вместо точек можно было бы взять отрезки (векторы) на плоскости, выходящие из начала координат, и, задавая эти векторы их компонентами $a$, $b$ на осях координат, определить сложение и умножение векторов при помощи тех же самых формул (2) и (3) из § 17, как и в случае точек плоскости. Можно было бы, далее, вообще отказаться от привлечения геометрического материала; замечая, что и точки плоскости, и векторы на плоскости задаются упорядоченными парами действительных чисел $(a, b)$, можно просто взять совокупность всех таких пар и в ней ввести сложение и умножение по формулам (2) и (3) из указанного параграфа.

На самом деле все эти поля оказались бы по своим алгебраическим свойствам неразличимыми, как показывает следующая теорема:

*Все расширения поля действительных чисел $D$, полученные присоединением к полю $D$ корня уравнения*

$$x^2+1=0, \tag{1}$$

*изоморфны между собой.*

Пусть, в самом деле, дано какое-либо поле $P$, являющееся расширением поля $D$ и содержащее элемент, удовлетворяющий уравнению (1). Выбор обозначения для этого элемента находится в нашем распоряжении, и мы употребим для этой цели букву $i$. Таким образом, имеет место равенство $i^2+1=0$ (откуда $i^2=-1$), где возведение в степень и сложение нужно понимать в смысле операций, определенных в поле $P$. Мы хотим найти сейчас поле $D(i)$, получающееся присоединением к полю $D$ элемента $i$, т. е. найти минимальное подполе поля $P$, содержащее и поле $D$, и элемент $i$.

Рассмотрим для этой цели все те элементы $\alpha$ поля $P$, которые можно записать в виде

$$\alpha=a+bi, \tag{2}$$

где $a$ и $b$ — произвольные действительные числа, а произведение числа $b$ на элемент $i$ и сумму числа $a$ с этим произведением следует понимать в смысле операций, определенных в поле $P$. Никакой элемент $\alpha$ поля $P$ не может обладать двумя различными записями такого вида: из

$$\alpha = a + bi = \bar{a} + \bar{b}i$$

и $b \neq \bar{b}$ следовало бы

$$i = \frac{\bar{a} - a}{b - \bar{b}},$$

т. е. $i$ оказалось бы действительным числом; если же $b = \bar{b}$, то и $a = \bar{a}$. К числу элементов поля $P$, записываемых в виде (2), принадлежат, в частности, все действительные числа (случай $b = 0$), а также сам элемент $i$ (случай $a = 0$, $b = 1$).

Покажем, что ***совокупность всех элементов вида*** (2) ***составляет подполе поля*** $P$; это и будет тогда искомым полем $D(i)$. Пусть нам даны элементы $\alpha = a + bi$ и $\beta = c + di$. Тогда, используя коммутативность и ассоциативность сложения и закон дистрибутивности, имеющие место в поле $P$, получаем:

$$\alpha + \beta = (a + bi) + (c + di) = (a + c) + (bi + di),$$

откуда

$$\alpha + \beta = (a + c) + (b + d)\, i, \tag{3}$$

т. е. эта сумма снова принадлежит к рассматриваемому множеству элементов. Далее,

$$-\beta = (-c) + (-d)\, i,$$

так как, ввиду (3), тогда будет справедливо равенство $\beta + (-\beta) = 0 + 0i = 0$; поэтому

$$\alpha - \beta = \alpha + (-\beta) = (a - c) + (b - d)\, i, \tag{3'}$$

т. е. и вычитание не выводит нас за пределы рассматриваемого множества. Снова используя свойства I—V, имеющие место для операций в поле $P$ (см. § 44), и опираясь на равенство $i^2 = -1$, мы получаем:

$$\alpha\beta = (a + bi)(c + di) = ac + adi + bci + bdi^2,$$

т. е.

$$\alpha\beta = (ac - bd) + (ad + bc)\, i; \tag{4}$$

таким образом, произведение двух любых элементов вида (2) снова будет элементом этого же вида. Предположим, наконец, что $\beta \neq 0$, т. е. хотя бы одно из чисел $c$, $d$ отлично от нуля. Тогда будет также $c - di \neq 0$ и

$$(c + di)(c - di) = c^2 - (di)^2 = c^2 - d^2 i^2 = c^2 + d^2,$$

причем $c^2+d^2 \neq 0$. Поэтому, используя отмечавшееся в предшествующем параграфе утверждение, что во всяком поле сохраняются все обычные правила обращения с дробями, а поэтому, в частности, дробь не меняется от умножения ее числителя и знаменателя на один и тот же отличный от нуля элемент, получаем:

$$\frac{\alpha}{\beta}=\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)i}{c^2+d^2},$$

т. е. элемент

$$\frac{\alpha}{\beta}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i \tag{4'}$$

снова имеет вид (2).

Покажем теперь, что *полученное нами подполе $D(i)$ поля $P$ изоморфно тому полю из точек плоскости, которое было построено в* § 17. Сопоставляя элементу $a+bi$ поля $D(i)$ точку $(a, b)$, мы получим ввиду доказанной единственности записи вида (2) для элементов поля $D(i)$ взаимно однозначное соответствие между элементами этого поля и всеми точками плоскости. При этом соответствии действительному числу $a$ соответствует точка $(a, 0)$ ввиду равенства $a=a+0i$, а элементу $i=0+1\cdot i$ сопоставляется точка $(0, 1)$. С другой стороны, сравнивая формулы (3) и (4) настоящего параграфа с формулами (2) и (3) из § 17, мы получаем, что сумме и произведению элементов $\alpha$ и $\beta$ поля $D(i)$ сопоставляются точки, являющиеся суммой и соответственно произведением точек, сопоставленных элементам $\alpha$ и $\beta$.

Этим, так как все поля, изоморфные некоторому данному полю, изоморфны между собой, заканчивается доказательство теоремы. Мы видим, в частности, что выбор в § 17 формул (2) и (3) для определения операций над точками не был случайным и не может быть изменен.

Помимо способов построения поля комплексных чисел, рассматривавшихся выше, существуют и многие другие. Укажем один из них, использующий сложение и умножение матриц.

Рассмотрим некоммутативное кольцо матриц второго порядка над полем действительных чисел. Очевидно, что скалярные матрицы

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

составляют в этом кольце подполе, изоморфное полю действительных чисел. Оказывается, однако, что *в кольце матриц второго порядка над полем действительных чисел можно найти также подполе, изоморфное полю комплексных чисел.* В самом деле, поставим в соответствие всякому комплексному числу $a+bi$ *матрицу*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

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 $\varphi$, 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 $\alpha$ кольца $L$ называется *алгебраическим над полем $P$*, если существует такое уравнение $n$-й степени, $n \geqslant 1$, с коэффициентами из поля $P$, которому элемент $\alpha$ удовлетворяет; если же такого уравнения не существует, то элемент $\alpha$ называется *трансцендентным над полем $P$*. Понятно, что элемент $x$ кольца $P[x]$ трансцендентен над полем $P$.

Справедлива следующая теорема:

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

В самом деле, всякий элемент $\beta$ 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 $\beta$ 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 $\alpha$, в противоречие с трансцендентностью этого элемента. Складывая элементы вида (4) по правилам сложения в кольце $L$, можно, понятно, складывать коэффициенты при одинаковых степенях $\alpha$; 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 $\alpha$, 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.

## § 48. Разложение многочленов на неприводимые множители

На основании теоремы о существовании корня в § 24 для полей комплексных и действительных чисел были доказаны существование и единственность разложения многочлена на неприводимые множители. Эти результаты являются частными случаями общих теорем, относящихся к многочленам над произвольным полем $P$. Настоящий параграф посвящается изложению этой общей теории, параллельной теории разложения целых чисел на простые множители.

Определим сначала те многочлены, которые играют в кольце многочленов такую же роль, какую в кольце целых чисел играют простые числа. Заранее подчеркнем, что в этом определении будет идти речь лишь о многочленах, степень которых больше или равна единице; это вполне соответствует тому, что при определении простых чисел и изучении разложений целых чисел на простые множители числа 1 и $-1$ исключаются из рассмотрения.

Пусть дан многочлен $f(x)$ степени $n$, $n \geqslant 1$, с коэффициентами из поля $P$. Ввиду свойства V из § 21 все многочлены нулевой степени будут служить делителями для $f(x)$. С другой стороны, по VII, делителями для $f(x)$ будут и все многочлены $cf(x)$, где $c$ — отличный от нуля элемент из $P$, причем ими исчерпываются все делители многочлена $f(x)$, имеющие степень $n$. Что же касается делителей для $f(x)$, степень которых больше 0, но меньше $n$, то они могут в кольце $P[x]$ существовать, а могут и отсутствовать. В первом случае многочлен $f(x)$ называется *приводимым* в поле $P$ (или над полем $P$), во втором случае — *неприводимым* в этом поле.

Вспоминая определение делителя, можно сказать, что *многочлен $f(x)$ степени $n$ приводим в поле $P$, если он может быть разложен над этим полем (т. е. в кольце $P[x]$) в произведение двух множителей, степени которых меньше $n$*:

$$f(x) = \varphi(x)\psi(x), \tag{1}$$

*и $f(x)$ неприводим в поле $P$, если в любом его разложении вида* (1) *один из множителей имеет степень* 0, *другой — степень $n$.*

Следует обратить особое внимание на то обстоятельство, что о приводимости или неприводимости многочлена можно говорить лишь по отношению к данному полю $P$, так как многочлен, неприводимый в этом поле, может оказаться приводимым в некотором его расширении $\overline{P}$. Так, многочлен $x^2-2$ с целыми коэффициентами неприводим в поле рациональных чисел — он не может быть разложен в произведение двух множителей первой степени с рациональными коэффициентами. Однако в поле действительных чисел этот многочлен оказывается приводимым, как показывает равенство

$$x^2-2=(x-\sqrt{2})(x+\sqrt{2}).$$

Многочлен $x^2+1$ неприводим не только в поле рациональных чисел, но и в поле действительных чисел; он делается приводимым, однако, в поле комплексных чисел, так как

$$x^2+1=(x-i)(x+i).$$

Укажем некоторые основные свойства неприводимых многочленов, причем будем помнить, что речь идет о многочленах, неприводимых в поле $P$.

α) *Всякий многочлен первой степени неприводим.*

В самом деле, если бы этот многочлен был разложим в произведение множителей меньшей степени, то эти множители должны были бы иметь степень 0. Однако произведение любых многочленов нулевой степени снова будет многочленом нулевой степени, а не первой.

β) *Если многочлен $p(x)$ неприводим, то неприводимым будет и всякий многочлен $cp(x)$, где $c$ — отличный от нуля элемент из $P$.*

Это свойство следует из свойств I и VII § 21. Оно позволит нам там, где это будет нужно, ограничиваться рассмотрением неприводимых многочленов, старшие коэффициенты которых равны единице.

γ) *Если $f(x)$ — произвольный, а $p(x)$ — неприводимый многочлен, то либо $f(x)$ делится на $p(x)$, либо же эти многочлены взаимно просты.*

Если $(f(x), p(x))=d(x)$, то $d(x)$, будучи делителем неприводимого многочлена $p(x)$, либо имеет степень 0, либо же есть многочлен вида $cp(x)$, $c\neq 0$. В первом случае $f(x)$ и $p(x)$ взаимно просты, во втором $f(x)$ делится на $p(x)$.

δ) *Если произведение многочленов $f(x)$ и $g(x)$ делится на неприводимый многочлен $p(x)$, то хотя бы один из этих множителей делится на $p(x)$.*

Действительно, если $f(x)$ не делится на $p(x)$, то, по γ), $f(x)$ и $p(x)$ взаимно просты, а тогда, по свойству б) из § 21, многочлен $g(x)$ должен делиться на $p(x)$.

Свойство δ) без труда распространяется на случай произведения любого конечного числа множителей.

Следующие две теоремы являются главной целью всего настоящего параграфа.

*Всякий многочлен $f(x)$ из кольца $P[x]$, имеющий степень $n$, $n\geqslant 1$, разлагается в произведение неприводимых множителей.*

Действительно, если многочлен $f(x)$ сам неприводим, то указанное произведение состоит всего из одного множителя. Если же он приводим, то может быть разложен в произведение множителей меньшей степени. Если среди этих множителей снова имеются приводимые, то производим их дальнейшее разложение на множители, и т. д. Этот процесс должен остановиться после конечного числа шагов, так как при любом разложении $f(x)$ на множители сумма

степеней этих множителей должна равняться $n$ и поэтому число множителей, зависящих от $x$, не может превосходить $n$.

Разложение целых чисел на простые множители однозначно, если ограничиваться рассмотрением целых положительных чисел. Однако в кольце всех целых чисел однозначность имеет место лишь с точностью до знаков: так, $-6=2\cdot(-3)=(-2)\cdot 3$, $10=2\cdot 5=(-2)\cdot(-5)$ и т. д. Аналогичное положение имеет место и в кольце многочленов. Если

$$f(x)=p_1(x)\,p_2(x)\ \ldots\ p_s(x)$$

есть разложение многочлена $f(x)$ в произведение неприводимых множителей и если элементы $c_1, c_2, \ldots, c_s$ из поля $P$ таковы, что их произведение равно 1, то

$$f(x)=[c_1p_1(x)]\cdot[c_2p_2(x)]\ldots[c_sp_s(x)]$$

также будет, ввиду β), разложением $f(x)$ в произведение неприводимых множителей. Оказывается, что этим исчерпываются все разложения $f(x)$:

*Если многочлен $f(x)$ из кольца $P[x]$ двумя способами разложен в произведение неприводимых множителей:*

$$f(x)=p_1(x)\,p_2(x)\ \ldots\ p_s(x)=q_1(x)\,q_2(x)\ \ldots\ q_t(x), \tag{2}$$

*то $s=t$ и, при соответствующей нумерации, имеют место равенства*

$$q_i(x)=c_ip_i(x),\quad i=1,\ 2,\ \ldots,\ s, \tag{3}$$

*где $c_i$ — отличные от нуля элементы из поля $P$.*

Эта теорема верна для многочленов первой степени, так как они неприводимы. Мы будем поэтому вести доказательство индукцией по степени многочлена, т. е. будем доказывать теорему для $f(x)$, предполагая, что для многочленов меньшей степени она уже доказана.

Так как $q_1(x)$ является делителем для $f(x)$, то, ввиду свойства δ) и равенства (2), $q_1(x)$ будет делителем хотя бы для одного из многочленов $p_i(x)$, например для $p_1(x)$. Так как, однако, многочлен $p_1(x)$ неприводим, а степень $q_1(x)$ больше нуля, то существует такой элемент $c_1$, что

$$q_1(x)=c_1p_1(x). \tag{4}$$

Подставляя это выражение $q_1(x)$ в (2) и сокращая на $p_1(x)$ (что законно, так как в кольце $P[x]$ нет делителей нуля), мы получим равенство

$$p_2(x)\,p_3(x)\ \ldots\ p_s(x)=[c_1q_2(x)]\,q_3(x)\ \ldots\ q_t(x).$$

Так как степень многочлена, равного этим произведениям, меньше степени $f(x)$, то уже доказано, что $s-1=t-1$, откуда $s=t$, и что существуют такие элементы $c_2', c_3, \ldots, c_s$, что $c_2'p_2(x)=c_1q_2(x)$,

откуда $q_2(x) = (c_1^{-1} c_2') p_2(x)$, и $c_i p_i(x) = q_i(x)$, $i = 3, \ldots, s$. Полагая $c_1^{-1} c_2' = c_2$ и учитывая (4), мы полностью получим равенства (3).

Доказанной сейчас теореме можно дать такую более короткую формулировку: *всякий многочлен разлагается на неприводимые множители однозначно с точностью до множителей нулевой степени.*

Всегда можно рассматривать, впрочем, разложение следующего специального вида, *которое будет для каждого многочлена уже вполне однозначным*: берем любое разложение многочлена $f(x)$ на неприводимые множители и из каждого из этих множителей выносим за скобки старший коэффициент. Мы получим разложение

$$f(x) = a_0 p_1(x) p_2(x) \ldots p_s(x), \tag{5}$$

где все $p_i(x)$, $i = 1, 2, \ldots, s$, являются неприводимыми многочленами со старшими коэффициентами, равными единице. Множитель $a_0$ будет равен старшему коэффициенту многочлена $f(x)$, как легко доказать, выполнив перемножение в правой части равенства (5).

Неприводимые множители, входящие в разложение (5), не обязаны быть все различными. Если неприводимый многочлен $p(x)$ встречается в разложении (5) несколько раз, то он называется *кратным множителем* для $f(x)$, а именно *k-кратным* (в частности двукратным, трехкратным и т. д.), если в разложении (5) содержится ровно $k$ множителей, равных $p(x)$. Если же множитель $p(x)$ входит в (5) лишь один раз, то он называется *простым* (или *однократным*) *множителем* для $f(x)$.

Если в разложении (5) множители $p_1(x), p_2(x), \ldots, p_l(x)$ отличны друг от друга, а всякий другой множитель равен одному из них, и если $p_i(x)$, $i = 1, 2, \ldots, l$, является $k_i$-кратным множителем многочлена $f(x)$, то разложение (5) можно переписать в следующем виде:

$$f(x) = a_0 p_1^{k_1}(x) p_2^{k_2}(x) \ldots p_l^{k_l}(x). \tag{6}$$

Именно этой записью мы будем дальше обычно пользоваться, не оговаривая особо, что показатели равны кратностям соответствующих множителей, т. е. что $p_i(x) \neq p_j(x)$ при $i \neq j$.

*Если даны разложения многочленов $f(x)$ и $g(x)$ на неприводимые множители, то наибольший общий делитель $d(x)$ этих многочленов равен произведению множителей, входящих одновременно в оба разложения, причем каждый множитель берется в степени, равной меньшей из его кратностей в обоих данных многочленах.*

Действительно, указанное произведение будет делителем для каждого из многочленов $f(x)$, $g(x)$, а поэтому и для $d(x)$. Если бы это произведение было отличным от $d(x)$, то в разложении $d(x)$ на неприводимые множители либо содержался бы множитель, который не входит в разложение хотя бы одного из многочленов $f(x)$ и $g(x)$,

что невозможно, либо же один из множителей имел бы бо́льшую степень, чем он имеет в разложении одного из многочленов $f(x)$ и $g(x)$, что снова невозможно.

Эта теорема аналогична тому правилу, по которому разыскивается обычно наибольший общий делитель целых чисел. Она не может заменить, однако, в случае многочленов алгоритм Евклида. Действительно, так как простых чисел, меньших данного целого положительного числа, лишь конечное число, то разложение целого числа на простые множители достигается конечным числом проб. Это уже не имеет места в кольце многочленов над бесконечным основным полем, и в общем случае нельзя дать способа для практического разложения многочленов на неприводимые множители. Больше того, даже решение вопроса, является ли многочлен $f(x)$ неприводимым в данном поле $P$, оказывается в общем случае весьма трудным. Так, описание всех неприводимых многочленов для случая полей комплексных и действительных чисел было получено в § 24 в качестве следствия из очень глубокой теоремы о существовании корня. Что же касается поля рациональных чисел, то о многочленах, неприводимых над этим полем, в § 56 будут сделаны лишь некоторые высказывания частного характера.

Мы показали, что в кольце многочленов, как и в кольце целых чисел, имеет место разложение на «простые» (неприводимые) множители и что это разложение в некотором смысле однозначно. Возникает вопрос, можно ли перенести эти результаты на более широкие классы колец. Мы ограничимся при этом случаем таких коммутативных колец, которые обладают единицей и не содержат делителей нуля.

Назовем *делителем единицы* такой элемент $a$ кольца, для которого в этом кольце существует обратный элемент $a^{-1}$,

$$aa^{-1}=1.$$

В кольце целых чисел это будут числа 1 и $-1$, в кольце многочленов $P[x]$ — все многочлены нулевой степени, т. е. отличные от нуля числа из поля $P$. Элемент $c$, отличный от нуля и не являющийся делителем единицы, назовем *простым* элементом кольца, если во всяком его разложении в произведение двух множителей, $c=ab$, один из этих множителей непременно является делителем единицы. В кольце целых чисел простыми элементами будут простые числа, в кольце многочленов — неприводимые многочлены.

Будет ли всякий элемент рассматриваемого кольца, отличный от нуля и не являющийся делителем единицы, разлагаться в произведение простых множителей? Если да, то будет ли такое разложение однозначным? Последнее нужно понимать в таком смысле: если

$$a=p_1p_2\ldots p_k=q_1q_2\ldots q_l$$

— два разложения элемента $a$ на простые множители, то $k=l$ и (возможно, после изменения нумерации)

$$q_i=p_ic_i,\quad i=1,\ 2,\ \ldots,\ k,$$

где $c_i$ — делитель единицы.

Оказывается, что в общем случае на оба вопроса должен быть дан отрицательный ответ. Мы ограничимся одним примером, а именно, укажем кольцо, в котором разложение на простые множители хотя и возможно, но не является однозначным.

Рассмотрим комплексные числа вида

$$\alpha = a + b\sqrt{-3}, \tag{7}$$

где $a$ и $b$ — целые числа. Все такие числа составляют кольцо без делителей нуля, содержащее единицу; действительно,

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (bc + ad)\sqrt{-3}. \tag{8}$$

Назовем *нормой* числа $\alpha = a + b\sqrt{-3}$ целое положительное число

$$N(\alpha) = a^2 + 3b^2.$$

Ввиду (8) *норма произведения равна произведению норм,*

$$N(\alpha\beta) = N(\alpha)\,N(\beta). \tag{9}$$

Действительно,

$$(ac - 3bd)^2 + 3(bc + ad)^2 = a^2c^2 + 9b^2d^2 + 3b^2c^2 + 3a^2d^2 = (a^2 + 3b^2)(c^2 + 3d^2).$$

Если число $\alpha$ является в нашем кольце делителем единицы, т. е. число $\alpha^{-1}$ также имеет вид (7), то, по (9),

$$N(\alpha)\cdot N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1,$$

а поэтому $N(\alpha) = 1$, так как числа $N(\alpha)$ и $N(\alpha^{-1})$ — целые и положительные. Если $\alpha = a + b\sqrt{-3}$, то из $N(\alpha) = 1$ следует

$$N(\alpha) = a^2 + 3b^2 = 1;$$

это возможно, однако, лишь при $b = 0$, $a = \pm 1$. Таким образом, *в нашем кольце, как и в кольце целых чисел, делителями единицы будут лишь числа* 1 *и* $-1$ *и лишь эти числа имеют норму, равную единице.*

Равенство (9) для нормы произведения переносится, понятно, на случай любого конечного числа множителей. Отсюда легко вывести, что *всякое число* $\alpha$ *из нашего кольца может быть разложено в произведение конечного числа простых множителей;* проведение доказательства мы предоставим читателю.

*Однозначность разложения на простые множители уже нельзя, однако, утверждать.* Справедливы, например, равенства

$$4 = 2\cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

В нашем кольце нет других делителей единицы, кроме чисел 1 и $-1$, а поэтому число $1 + \sqrt{-3}$ (как и число $1 - \sqrt{-3}$) не может отличаться от числа 2 лишь на множитель, являющийся делителем единицы. Нам остается показать, что *каждое из чисел* 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ *будет в рассматриваемом кольце простым.* Действительно, норма каждого из этих трех чисел равна числу 4. Пусть $\alpha$ — любое из этих чисел и пусть

$$\alpha = \beta\gamma.$$

Тогда, по (9), возможен один из трех случаев:

1) $N(\beta) = 4$, $N(\gamma) = 1$; 2) $N(\beta) = 1$, $N(\gamma) = 4$; 3) $N(\beta) = N(\gamma) = 2$.

В первом случае число $\gamma$ будет, как мы знаем, делителем единицы, во втором случае делителем единицы будет $\beta$. Что же касается третьего случая, то он вообще невозможен ввиду невозможности равенства

$$a^2 + 3b^2 = 2$$

при целых $a$ и $b$.

**Кратные множители.** Хотя, как уже указано выше, мы не умеем разлагать многочлены на неприводимые множители, тем не менее существуют методы, позволяющие узнать, обладает ли данный многочлен кратными множителями, и в случае положительного ответа

дающие возможность свести изучение этого многочлена к изучению многочленов, уже не содержащих кратных множителей. Эти методы требуют, однако, наложения некоторых ограничений на основное поле. Именно, все дальнейшее содержание настоящего параграфа будет излагаться в предположении, что поле $P$ имеет характеристику 0. Без этого ограничения теоремы о кратных множителях, которые будут доказаны ниже, уже теряют силу; вместе с тем, с точки зрения приложений, случай полей характеристики нуль является наиболее важным, так как сюда относятся, в частности, все числовые поля.

Заметим сначала, что на рассматриваемый случай переносятся и понятие производной многочлена, введенное в § 22 для многочленов с комплексными коэффициентами, и основные свойства этого понятия [1]). Докажем теперь следующую теорему:

*Если $p(x)$ является $k$-кратным неприводимым множителем многочлена $f(x)$, $k \geqslant 1$, то он будет $(k-1)$-кратным множителем производной этого многочлена. В частности, простой множитель многочлена не входит в разложение производной.*

В самом деле, пусть

$$f(x) = p^k(x)\, g(x), \tag{10}$$

причем $g(x)$ уже не делится на $p(x)$. Дифференцируя равенство (10), получаем:

$$\begin{aligned} f'(x) &= p^k(x)\, g'(x) + kp^{k-1}(x)\, p'(x)\, g(x) = \\ &= p^{k-1}(x)\,[p(x)\, g'(x) + kp'(x)\, g(x)]. \end{aligned}$$

Второе из слагаемых, стоящих в скобках, не делится на $p(x)$; действительно, $g(x)$ не делится на $p(x)$ по условию, $p'(x)$ имеет меньшую степень, т. е. также не делится на $p(x)$, а отсюда, ввиду неприводимости многочлена $p(x)$ и свойств δ) из настоящего параграфа и IX из § 21, следует наше утверждение. С другой стороны, первое слагаемое суммы, стоящей в квадратных скобках, делится на $p(x)$, а поэтому вся эта сумма не может делиться на $p(x)$, т. е. множитель $p(x)$ на самом деле входит в $f'(x)$ с кратностью $k-1$.

Из нашей теоремы и из указанного выше способа разыскания наибольшего общего делителя двух многочленов следует, что если дано разложение многочлена $f(x)$ на неприводимые множители:

$$f(x) = a_0 p_1^{k_1}(x)\, p_2^{k_2}(x) \ \ldots \ p_l^{k_l}(x), \tag{11}$$

то *наибольший общий делитель многочлена $f(x)$ и его производной обладает следующим разложением на неприводимые множители:*

$$(f(x),\ f'(x)) = p_1^{k_1-1}(x)\, p_2^{k_2-1}(x) \ \ldots \ p_l^{k_l-1}(x), \tag{12}$$

---

[1]) Для полей конечной характеристики теряет силу утверждение, что производная многочлена степени $n$ имеет степень $n-1$.

где, понятно, множитель $p_i^{k_i-1}(x)$ следует при $k_i=1$ заменять единицей. В частности, *многочлен $f(x)$ тогда и только тогда не содержит кратных множителей, если он взаимно прост со своей производной.*

Мы научились, следовательно, отвечать на вопрос о существовании кратных множителей у данного многочлена. Больше того, так как ни производная многочлена, ни наибольший общий делитель двух многочленов не зависят от того, рассматриваем ли мы поле $P$ или его любое расширение $\overline{P}$, то в качестве следствия из доказанного сейчас результата мы получаем:

*Если многочлен $f(x)$ с коэффициентами из поля $P$ характеристики нуль не имеет над этим полем кратных множителей, то у него не будет кратных множителей ни над каким расширением $\overline{P}$ поля $P$.*

В частности, если $f(x)$ неприводим над $P$, а $\overline{P}$ — некоторое расширение поля $P$, то, хотя $f(x)$ уже может быть над $\overline{P}$ приводимым, однако заведомо не будет делиться на квадрат неприводимого (над $\overline{P}$) многочлена.

**Выделение кратных множителей.** Если дан многочлен $f(x)$ с разложением (11) и если через $d_1(x)$ мы обозначим наибольший общий делитель $f(x)$ и его производной $f'(x)$, то (12) будет разложением для $d_1(x)$. Деля (11) на (12), мы получим:

$$v_1(x)=\frac{f(x)}{d_1(x)}=a_0p_1(x)p_2(x)\ \ldots\ p_l(x),$$

т. е. получим многочлен, не содержащий кратных множителей, причем всякий неприводимый множитель для $v_1(x)$ будет множителем и для $f(x)$. Этим разыскание неприводимых множителей для $f(x)$ сводится к разысканию их для многочлена $v_1(x)$, имеющего, вообще говоря, меньшую степень и, во всяком случае, содержащего лишь простые множители. Если эта задача для $v_1(x)$ будет решена, то останется определить лишь кратность найденных неприводимых множителей в $f(x)$, что достигается применением алгоритма деления.

Усложняя изложенный сейчас метод, можно сразу перейти к рассмотрению нескольких многочленов без кратных множителей, причем, найдя неприводимые множители этих многочленов, мы не только найдем все неприводимые множители для $f(x)$, но и будем знать их кратности.

Пусть (11) будет разложением $f(x)$ на неприводимые множители, причем наивысшая кратность множителей есть $s$, $s\geqslant 1$. Обозначим через $F_1(x)$ произведение всех однократных множителей многочлена $f(x)$, через $F_2(x)$ — произведение всех двукратных множителей, но взятых лишь по одному разу, и т. д., наконец, через $F_s(x)$ — произведение всех $s$-кратных множителей, также взятых лишь по одному разу; если при этом для некоторого $j$ в $f(x)$ отсутствуют $j$-кратные множители, то полагаем $F_j(x)=1$. Тогда $f(x)$ будет делиться на $k$-ю степень многочлена $F_k(x)$, $k=1, 2, \ldots, s$, и разложение (11) примет вид

$$f(x)=a_0F_1(x)F_2^2(x)F_3^3(x)\ \ldots\ F_s^s(x),$$

а разложение (12) для $d_1(x) = (f(x), f'(x))$ перепишется в виде

$$d_1(x) = F_2(x) F_3^2(x) \ldots F_s^{s-1}(x).$$

Обозначая через $d_2(x)$ наибольший общий делитель многочлена $d_1(x)$ и его производной и вообще через $d_k(x)$ наибольший общий делитель многочленов $d_{k-1}(x)$ и $d'_{k-1}(x)$, мы таким же путем получим:

$$d_2(x) = F_3(x) F_4^2(x) \ldots F_s^{s-2}(x),$$
$$d_3(x) = F_4(x) F_5^2(x) \ldots F_s^{s-3}(x),$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$d_{s-1}(x) = F_s(x),$$
$$d_s(x) = 1.$$

Отсюда

$$v_1(x) = \frac{f(x)}{d_1(x)} = a_0 F_1(x) F_2(x) F_3(x) \ldots F_s(x),$$
$$v_2(x) = \frac{d_1(x)}{d_2(x)} = F_2(x) F_3(x) \ldots F_s(x),$$
$$v_3(x) = \frac{d_2(x)}{d_3(x)} = F_3(x) \ldots F_s(x),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$v_s(x) = \frac{d_{s-1}(x)}{d_s(x)} = F_s(x),$$

и поэтому, наконец,

$$F_1(x) = \frac{v_1(x)}{a_0 v_2(x)}, \quad F_2(x) = \frac{v_2(x)}{v_3(x)}, \quad \ldots, \quad F_s(x) = v_s(x).$$

Таким образом, пользуясь лишь приемами, не требующими знания неприводимых множителей многочлена $f(x)$, а именно взятием производной, алгоритмом Евклида и алгоритмом деления, мы можем найти многочлены $F_1(x)$, $F_2(x)$, ..., $F_s(x)$ без кратных множителей, причем всякий неприводимый множитель многочлена $F_k(x)$, $k = 1, 2, \ldots, s$, будет $k$-кратным для $f(x)$.

Изложенный здесь метод нельзя, понятно, считать методом для разложения многочлена на неприводимые множители, так как для случая $s = 1$, т. е. для многочлена без кратных множителей, мы получим лишь $f(x) = F_1(x)$.

## § 49*. Теорема существования корня

Само собою разумеется, что доказанная в § 23 основная теорема о существовании для всякого числового многочлена корня в поле комплексных чисел не может быть перенесена на случай произвольного поля. В настоящем параграфе будет доказана теорема, в некоторой мере заменяющая в общей теории полей указанную основную теорему алгебры комплексных чисел.

Пусть дан многочлен $f(x)$ над полем $P$. Естественно возникает следующий вопрос: если многочлен $f(x)$ вообще не имеет корней в поле $P$, то существует ли такое расширение $\overline{P}$ поля $P$, в котором

для $f(x)$ уже найдется хотя бы один корень? При этом можно считать, что степень многочлена $f(x)$ больше единицы: для многочленов нулевой степени вопрос не имеет смысла, а всякий многочлен первой степени $ax+b$ обладает корнем $-\frac{b}{a}$ в самом поле $P$. С другой стороны, можно ограничиться, очевидно, случаем когда многочлен $f(x)$ неприводим: если он приводим над $P$, то корень любого из его неприводимых множителей будет служить корнем и для него самого.

Ответ на интересующий нас вопрос дает следующая теорема существования корня:

*Для всякого многочлена $f(x)$, неприводимого над полем $P$, существует такое расширение этого поля, в котором содержится корень для $f(x)$. Все минимальные поля, содержащие поле $P$ и какой-либо корень этого многочлена, изоморфны между собой.*

Докажем сначала вторую половину этой теоремы.

Пусть дан неприводимый над $P$ многочлен

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

причем $n\geqslant 2$, т. е. $f(x)$ не имеет корней в самом поле $P$. Предположим, что существует расширение $\overline{P}$ поля $P$, содержащее корень $\alpha$ для $f(x)$, и докажем следующую лемму, необходимую для дальнейшего, но представляющую и самостоятельный интерес:

*Если лежащий в $\overline{P}$ корень $\alpha$ многочлена $f(x)$, неприводимого над $P$, служит корнем также для некоторого многочлена $g(x)$ из кольца $P[x]$, то $f(x)$ будет делителем для $g(x)$.*

В самом деле, над полем $\overline{P}$ многочлены $f(x)$ и $g(x)$ обладают общим делителем $x-\alpha$ и поэтому не являются взаимно простыми. Свойство многочленов не быть взаимно простыми не зависит, однако, от выбора поля, поэтому можно перейти к полю $P$ и применить свойство $\gamma$) из предшествующего параграфа.

Найдем теперь минимальное подполе $P(\alpha)$ поля $\overline{P}$, содержащее поле $P$ и элемент $\alpha$. К нему заведомо принадлежат все элементы вида

$$\beta=b_0+b_1\alpha+b_2\alpha^2+\ldots+b_{n-1}\alpha^{n-1}, \tag{2}$$

где $b_0, b_1, b_2, \ldots, b_{n-1}$ — элементы поля $P$. Никакой элемент поля $\overline{P}$ не может обладать двумя различными записями вида (2): если имеет место также равенство

$$\beta=c_0+c_1\alpha+c_2\alpha^2+\ldots+c_{n-1}\alpha^{n-1},$$

причем хотя бы при одном $k$ $c_k\neq b_k$, то $\alpha$ будет корнем многочлена

$$g(x)=(b_0-c_0)+(b_1-c_1)x+(b_2-c_2)x^2+\ldots+(b_{n-1}-c_{n-1})x^{n-1},$$

что противоречит доказанной выше лемме, так как степень $g(x)$ меньше степени $f(x)$.

К числу элементов поля $\overline{P}$, имеющих вид (2), принадлежат все элементы поля $P$ (при $b_1 = b_2 = \ldots = b_{n-1} = 0$), а также сам элемент $\alpha$ (при $b_1 = 1$, $b_0 = b_2 = \ldots = b_{n-1} = 0$). Докажем, что *элементы вида* (2) *составляют все искомое подполе* $P(\alpha)$. В самом деле, если даны элементы $\beta$ (с записью (2)) и

$$\gamma = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1},$$

то, на основании свойств операций в поле $\overline{P}$,

$$\beta \pm \gamma = (b_0 \pm c_0) + (b_1 \pm c_1)\alpha + (b_2 \pm c_2)\alpha^2 + \ldots + (b_{n-1} \pm c_{n-1})\alpha^{n-1},$$

т. е. сумма и разность двух любых элементов вида (2) снова будут элементами такого же вида.

Если мы перемножим $\beta$ и $\gamma$, то получим выражение, содержащее $\alpha^n$ и более высокие степени $\alpha$. Однако из (1) и равенства $f(\alpha) = 0$ вытекает, что $\alpha^n$, а поэтому и $\alpha^{n+1}$, $\alpha^{n+2}$ и т. д., можно выразить через меньшие степени элемента $\alpha$. Наиболее простой способ разыскания выражения для $\beta\gamma$ состоит в следующем: пусть

$$\varphi(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}, \quad \psi(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1},$$

откуда $\varphi(\alpha) = \beta$, $\psi(\alpha) = \gamma$. Перемножим многочлены $\varphi(x)$ и $\psi(x)$ и разделим это произведение на $f(x)$; мы получим

$$\varphi(x)\,\psi(x) = f(x)\,q(x) + r(x), \tag{3}$$

где

$$r(x) = d_0 + d_1x + \ldots + d_{n-1}x^{n-1}.$$

Беря значения обеих частей равенства (3) при $x = \alpha$, мы получим:

$$\varphi(\alpha)\,\psi(\alpha) = f(\alpha)\,q(\alpha) + r(\alpha),$$

т. е., ввиду $f(\alpha) = 0$,

$$\beta\gamma = d_0 + d_1\alpha + \ldots + d_{n-1}\alpha^{n-1}.$$

Таким образом, произведение двух элементов вида (2) снова будет элементом такого же вида.

Покажем, наконец, что если элемент $\beta$ имеет вид (2), причем $\beta \neq 0$, то элемент $\beta^{-1}$, существующий в поле $\overline{P}$, также может быть записан в виде (2). Для этого возьмем многочлен

$$\varphi(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$$

из кольца $P[x]$. Так как степень $\varphi(x)$ ниже степени $f(x)$, а многочлен $f(x)$ неприводим над $P$, то $\varphi(x)$ и $f(x)$ взаимно просты и поэтому, по §§ 21 и 47, в кольце $P[x]$ существуют такие многочлены $u(x)$ и $v(x)$, что

$$\varphi(x)\,u(x) + f(x)\,v(x) = 1;$$