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

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

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

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

можно считать при этом, что степень $u(x)$ меньше $n$:

$$u(x) = s_0 + s_1 x + \ldots + s_{n-1} x^{n-1}.$$

Отсюда, ввиду равенства $f(\alpha) = 0$, следует:

$$\varphi(\alpha)\, u(\alpha) = 1$$

и поэтому, ввиду равенства $\varphi(\alpha) = \beta$, мы получаем:

$$\beta^{-1} = u(\alpha) = s_0 + s_1 \alpha + \ldots + s_{n-1} \alpha^{n-1}.$$

Таким образом, совокупность элементов поля $\overline{P}$, имеющих вид (2), составляет подполе поля $\overline{P}$; это и будет искомое поле $P(\alpha)$. Так как мы видели, далее, что при разыскании суммы и произведения элементов $\beta$ и $\gamma$ вида (2) нужно знать лишь коэффициенты выражений этих элементов через степени $\alpha$, то можно утверждать справедливость следующего результата: если существует, помимо $\overline{P}$, другое расширение $\overline{P'}$ поля $P$, также содержащее некоторый корень $\alpha'$ многочлена $f(x)$, и если $P(\alpha')$ есть минимальное подполе поля $\overline{P'}$, содержащее $P$ и $\alpha'$, то *поля $P(\alpha)$ и $P(\alpha')$ будут изоморфными*, причем для получения изоморфного соответствия между ними нужно элементу $\beta$ вида (2) из $P(\alpha)$ сопоставить элемент

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

из $P(\alpha')$, имеющий те же коэффициенты. Этим доказана вторая половина теоремы.

Переходим к доказательству основной первой половины этой теоремы, причем изложенное выше подскажет нам пути для этого. Нам дан многочлен $f(x)$ степени $n \geqslant 2$, неприводимый над полем $P$, и нужно построить расширение поля $P$, содержащее корень для $f(x)$. Для этого возьмем все кольцо многочленов $P[x]$ и разобьем его на непересекающиеся классы, отнеся в один класс многочлены, дающие при делении на заданный нам многочлен $f(x)$ одинаковые остатки. Иными словами, многочлены $\varphi(x)$ и $\psi(x)$ относятся к одному классу, если их разность нацело делится на $f(x)$.

Условимся обозначать полученные классы буквами $A$, $B$, $C$ и т. д. и следующим вполне естественным способом определим сумму и произведение классов. Возьмем любые два класса $A$ и $B$, выберем в классе $A$ некоторый многочлен $\varphi_1(x)$, в классе $B$ — некоторый многочлен $\psi_1(x)$ и обозначим через $\chi_1(x)$ сумму этих многочленов,

$$\chi_1(x) = \varphi_1(x) + \psi_1(x),$$

а через $\theta_1(x)$ — их произведение,

$$\theta_1(x) = \varphi_1(x) \cdot \psi_1(x).$$

Выберем теперь в классе $A$ любой другой многочлен $\varphi_2(x)$, в классе $B$ — любой многочлен $\psi_2(x)$ и обозначим через $\chi_2(x)$ и $\theta_2(x)$ соответственно их сумму и произведение:

$$\chi_2(x) = \varphi_2(x) + \psi_2(x),$$
$$\theta_2(x) = \varphi_2(x) \cdot \psi_2(x).$$

По условию многочлены $\varphi_1(x)$ и $\varphi_2(x)$ лежат в одном классе $A$, а поэтому их разность $\varphi_1(x) - \varphi_2(x)$ нацело делится на $f(x)$; этим же свойством обладает и разность $\psi_1(x) - \psi_2(x)$. Отсюда следует, что разность

$$\begin{aligned}\chi_1(x) - \chi_2(x) &= [\varphi_1(x) + \psi_1(x)] - [\varphi_2(x) + \psi_2(x)] = \\ &= [\varphi_1(x) - \varphi_2(x)] + [\psi_1(x) - \psi_2(x)]\end{aligned} \tag{4}$$

также нацело делится на многочлен $f(x)$. Это же верно и для разности $\theta_1(x) - \theta_2(x)$, так как

$$\begin{aligned}\theta_1(x) - \theta_2(x) &= \varphi_1(x)\,\psi_1(x) - \varphi_2(x)\,\psi_2(x) = \\ &= \varphi_1(x)\,\psi_1(x) - \varphi_1(x)\,\psi_2(x) + \varphi_1(x)\,\psi_2(x) - \varphi_2(x)\,\psi_2(x) = \\ &= \varphi_1(x)\,[\psi_1(x) - \psi_2(x)] + [\varphi_1(x) - \varphi_2(x)]\,\psi_2(x).\end{aligned} \tag{5}$$

Равенство (4) показывает, что многочлены $\chi_1(x)$ и $\chi_2(x)$ лежат в одном классе. Иными словами, сумма любого многочлена из класса $A$ с любым многочленом из класса $B$ принадлежит ко вполне определенному классу $C$, который не зависит от того, какие именно многочлены выбраны в качестве «представителей» в классах $A$ и $B$; назовем этот класс $C$ *суммой* классов $A$ и $B$:

$$C = A + B.$$

Аналогично, ввиду (5), не зависит от выбора представителей в классах $A$ и $B$ и тот класс $D$, в котором лежит произведение любого многочлена из $A$ на любой многочлен из $B$; этот класс назовем *произведением* классов $A$ и $B$:

$$D = AB.$$

Покажем, что совокупность классов, на которые разбито нами кольцо многочленов $P[x]$, после указанного введения операций сложения и умножения превращается в поле. В самом деле, справедливость законов ассоциативности и коммутативности для обеих операций и закона дистрибутивности вытекает из справедливости этих законов в кольце $P[x]$, так как операции над классами сводятся на операции над многочленами, лежащими в этих классах. Роль нуля играет, очевидно, класс, составленный из многочленов, нацело делящихся на многочлен $f(x)$. Этот класс назовем *нулевым* и будем обозначать символом 0. Противоположным для класса $A$, составленного из многочленов, дающих

при делении на $f(x)$ остаток $\varphi(x)$, будет служить класс, составленный из многочленов, дающих при делении на $f(x)$ остаток $-\varphi(x)$. Отсюда вытекает, что в множестве классов выполнимо однозначное вычитание.

Для доказательства того, что в множестве классов выполнимо деление, нужно показать, что существует класс, играющий роль единицы, и что для всякого класса, отличного от нулевого, существует обратный класс. Единицей будет, очевидно, класс многочленов, дающих при делении на $f(x)$ остаток 1; этот класс назовем *единичным* и будем обозначать символом $E$.

Пусть теперь дан класс $A$, отличный от нулевого. Многочлен $\varphi(x)$, выбранный в классе $A$ в качестве представителя, не будет, следовательно, нацело делиться на $f(x)$, и поэтому, ввиду неприводимости многочлена $f(x)$, эти два многочлена взаимно просты. В кольце $P[x]$ существуют, таким образом, многочлены $u(x)$ и $v(x)$, удовлетворяющие равенству

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

откуда

$$\varphi(x)\,u(x)=1-f(x)\,v(x). \tag{6}$$

Правая часть равенства (6) при делении на $f(x)$ дает в остатке 1, т. е. принадлежит к единичному классу $E$. Если класс, к которому принадлежит многочлен $u(x)$, мы обозначим через $B$, то равенство (6) показывает, что

$$AB=E,$$

откуда $B=A^{-1}$. Этим доказано существование обратного класса для всякого ненулевого класса, т. е. закончено доказательство того, что классы составляют поле.

Обозначим это поле через $\overline{P}$ и покажем, что *оно является расширением поля* $P$. Всякому элементу $a$ поля $P$ соответствует класс, составленный из многочленов, дающих при делении на $f(x)$ остаток $a$; сам элемент $a$, рассматриваемый как многочлен нулевой степени, принадлежит к этому классу. Все классы этого специального вида составляют в поле $\overline{P}$ подполе, изоморфное полю $P$. Действительно, взаимная однозначность соответствия очевидна; с другой стороны, в этих классах можно выбрать в качестве представителей элементы поля $P$, а поэтому сумме (произведению) элементов из $P$ будет соответствовать сумма (произведение) соответствующих классов. В дальнейшем мы имеем право, следовательно, не различать элементы поля $P$ и соответствующие им классы.

Обозначим, наконец, через $X$ класс, составленный из многочленов, дающих при делении на $f(x)$ остаток $x$. Этот класс является вполне определенным элементом поля $\overline{P}$, и мы хотим показать, что *он служит корнем для многочлена* $f(x)$. Пусть

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

Обозначим через $A_i$ класс, соответствующий в указанном выше смысле элементу $a_i$ поля $P$, $i=0, 1, \ldots, n$, и найдем, чему равен элемент

$$A_0X^n+A_1X^{n-1}+\ldots+A_{n-1}X+A_n \tag{7}$$

поля $\overline{P}$. Считая представителями классов $A_i$ элементы $a_i, i=0,1,\ldots,n$, а представителем класса $X$ — многочлен $x$ и используя определение сложения и умножения классов, мы получаем, что в классе (7) содержится сам многочлен $f(x)$. Однако $f(x)$ нацело делится на самого себя, и поэтому класс (7) оказывается нулевым. Таким образом, заменяя в (7) классы $A_i$ соответствующими им элементами $a_i$ поля $P$, мы получаем, что в поле $\overline{P}$ имеет место равенство

$$a_0X^n+a_1X^{n-1}+\ldots+a_{n-1}X+a_n=0,$$

т. е. класс $X$ действительно является корнем многочлена $f(x)$.

Этим заканчивается доказательство теоремы о существовании корня. Заметим, что, взяв за $P$ поле действительных чисел и положив $f(x)=x^2+1$, мы получим еще один способ построения поля комплексных чисел.

Из теоремы о существовании корня могут быть выведены следствия, аналогичные тем, которые выводились в § 24 из основной теоремы алгебры комплексных чисел. Сначала сделаем одно замечание. Так как всякий линейный множитель $x-c$ многочлена $f(x)$ неприводим, то он должен входить в то единственное разложение на неприводимые множители, которым обладает $f(x)$.

Число линейных множителей в разложении $f(x)$ на неприводимые множители не может превосходить, однако, степени этого многочлена. Мы приходим к следующему результату:

*Многочлен $f(x)$ степени $n$ может иметь в поле $P$ не более $n$ корней, если даже каждый из корней считать столько раз, какова его кратность.*

Назовем *полем разложения* для многочлена $f(x)$ степени $n$ над полем $P$ такое расширение $Q$ поля $P$, в котором для $f(x)$ содержится $n$ корней (считая кратные корни столько раз, какова их кратность). Над полем $Q$ многочлен $f(x)$ будет раскладываться, следовательно, на линейные множители, причем никакое дальнейшее расширение поля $Q$ уже не может привести к появлению новых корней для $f(x)$.

*Для всякого многочлена $f(x)$ из кольца $P[x]$ существует над полем $P$ поле разложения.*

В самом деле, если многочлен $f(x)$ степени $n$, $n\geqslant 1$, имеет $n$ корней в самом поле $P$, то $P$ будет искомым полем разложения. Если же $f(x)$ не разлагается над $P$ на линейные множители, то берем один из его нелинейных неприводимых множителей $\varphi(x)$ и, на основании теоремы о существовании корня, расширяем $P$ до поля $P'$, содержащего корень для $\varphi(x)$. Если над $P'$ многочлен $f(x)$

все еще не разлагается на линейные множители, то снова расширяем поле, создавая корень еще для одного из оставшихся нелинейных неприводимых множителей. После конечного числа шагов мы придем, очевидно, к полю разложения для $f(x)$.

Понятно, что $f(x)$ может обладать многими различными полями разложения. Можно было бы доказать, что все минимальные поля, содержащие поле $P$ и $n$ корней многочлена $f(x)$ (где $n$ — степень этого многочлена), изоморфны между собой. Мы не будем, однако, использовать этого утверждения и поэтому не приводим его доказательства.

**Кратные корни.** В предшествующем параграфе было доказано, что многочлен $f(x)$ над полем $P$ характеристики 0 тогда и только тогда не имеет кратных множителей, если он взаимно прост со своей производной, а также было отмечено, что отсутствие у $f(x)$ кратных множителей над $P$ влечет за собой отсутствие таких множителей над любым расширением $\overline{P}$ поля $P$. Применяя это к случаю когда $\overline{P}$ есть некоторое поле разложения для $f(x)$, и вспоминая определение кратного корня, мы приходим к следующему результату:

*Если многочлен $f(x)$ над полем $P$ характеристики 0 не имеет кратных корней в данном поле разложения, то он взаимно прост со своей производной $f'(x)$. Обратно, если $f(x)$ взаимно прост со своей производной, то он не имеет кратных корней ни в каком из своих полей разложения.*

Отсюда, в частности, вытекает, что *многочлен $f(x)$, неприводимый над полем $P$ характеристики 0, не может иметь кратных корней ни в каком расширении этого поля.* Для полей конечной характеристики это утверждение перестает быть справедливым — обстоятельство, играющее заметную роль в общей теории полей.

В заключение заметим, что *для случая произвольного поля сохраняются и формулы Вьета* (см. § 24); при этом корни многочлена берутся в некотором поле разложения этого многочлена.

## § 50*. Поле рациональных дробей

*Теория рациональных дробей, изложенная* в § 25, *полностью сохраняется и в случае произвольного основного поля.* Однако при переходе от поля действительных чисел к произвольному полю $P$ взгляд на выражения $\frac{f(x)}{g(x)}$ как на функции переменного $x$ должен быть отброшен, так как он, как мы знаем, неприменим уже к многочленам. Перед нами стоит задача определить, какой смысл нужно придать этим выражениям в том случае, когда коэффициенты принадлежат к произвольному полю $P$. Точнее, мы хотим построить поле, в котором содержалось бы кольцо многочленов $P[x]$, причем так, чтобы операции сложения и умножения, определенные в этом новом поле, в применении к многочленам совпадали бы