§ 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 α является в нашем кольце делителем единицы, т. е. число α^{-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* α *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 α — 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 γ будет, как мы знаем, делителем единицы, во втором случае делителем единицы будет β. 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

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

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