

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

$$u(x) = s_0 + s_1x + \dots + s_{n-1}x^{n-1}.$$

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

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

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

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

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

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

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 $n \geq 2$, 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:

$$\begin{aligned}\chi_2(x) &= \varphi_2(x) + \psi_2(x), \\ \theta_2(x) &= \varphi_2(x) \cdot \psi_2(x).\end{aligned}$$

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

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

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

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

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 *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 и уля 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

$$\varphi(x) u(x) = 1 - f(x) v(x). \quad (6)$$

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 \bar{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 \bar{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 \bar{P} , и мы хотим показать, что он служит корнем для многочлена $f(x)$. Пусть

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n.$$

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

$$A_0X^n + A_1X^{n-1} + \dots + A_{n-1}X + A_n \quad (7)$$

поля \bar{P} . Считая представителями классов A_i элементы $a_i, i=0, 1, \dots, n$, 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 \bar{P} имеет место равенство

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

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 — с 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, сколько 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, сколько 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 , $n \geq 1$, 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 \bar{P} поля P . Применяя это к случаю когда \bar{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

с операциями в кольце $P[x]$; короче, кольцо $P[x]$ должно быть подкольцом этого нового поля. С другой стороны, всякий элемент этого нового поля должен представляться (в смысле деления, определенного в этом поле) в виде частного двух многочленов. Такое поле для всякого P может быть построено, как будет сейчас показано; его обозначают $P(x)$ (неизвестное заключено в круглые скобки!) и называют *полем рациональных дробей* над полем P .

Предположим сначала, что кольцо $P[x]$ уже является подкольцом некоторого поля Q . Если $f(x)$ и $g(x)$ — произвольные многочлены из $P[x]$; причем $g(x) \neq 0$, то в поле Q существует однозначно определенный элемент, равный частному от деления $f(x)$ на $g(x)$. Обозначая этот элемент, как обычно в случае поля, через $\frac{f(x)}{g(x)}$, мы на основании определения частного можем написать равенство

$$f(x) = g(x) \cdot \frac{f(x)}{g(x)}, \quad (1)$$

где произведение нужно понимать в смысле умножения в поле Q . Может случиться, что некоторые частные $\frac{f(x)}{g(x)}$ и $\frac{\psi(x)}{\psi(x)}$ являются одним и тем же элементом поля Q ; условием для этого является обычное условие равенства дробей:

Тогда и только тогда $\frac{f(x)}{g(x)} = \frac{\psi(x)}{\psi(x)}$, если $f(x)\psi(x) = \psi(x)g(x)$.

Действительно, если $\frac{f(x)}{g(x)} = \frac{\psi(x)}{\psi(x)} = \alpha$, то, по (1),

$$f(x) = g(x)\alpha, \quad \psi(x) = \psi(x)\alpha,$$

откуда

$$f(x)\psi(x) = g(x)\psi(x)\alpha = g(x)\phi(x).$$

Обратно, если $f(x)\psi(x) = g(x)\phi(x) = u(x)$ в смысле умножения в кольце $P[x]$, то, переходя к полю Q , мы получаем равенства

$$\frac{f(x)}{g(x)} = \frac{u(x)}{g(x)\psi(x)} = \frac{\phi(x)}{\psi(x)}.$$

Легко видеть, далее, что сумма и произведение любых элементов из Q , являющихся частными многочленов из $P[x]$, снова могут быть представлены в виде таких частных, причем справедливы обычные правила сложения и умножения дробей:

$$\frac{f(x)}{g(x)} + \frac{\psi(x)}{\psi(x)} = \frac{f(x)\psi(x) + g(x)\phi(x)}{g(x)\psi(x)}, \quad (2)$$

$$\frac{f(x)}{g(x)} \cdot \frac{\psi(x)}{\psi(x)} = \frac{f(x)\cdot\phi(x)}{g(x)\cdot\psi(x)}. \quad (3)$$

Действительно, умножая обе части каждого из этих равенств на произведение $g(x)\psi(x)$ и применяя (1), мы получим равенства, справедливые в кольце $P[x]$. Справедливость равенств (2) и (3)

следует теперь из того, что, благодаря отсутствию делителей нуля в поле Q , обе части каждого из полученных равенств можно сократить на отличный от нуля элемент $g(x)\psi(x)$, не нарушая равенств.

Эти предварительные замечания подсказывают нам тот путь, по которому мы должны пойти при построении поля $P(x)$. Пусть даны произвольное поле P и над ним кольцо многочленов $P[x]$. Всякой упорядоченной паре многочленов $f(x), g(x)$, где $g(x) \neq 0$, мы ставим в соответствие символ $\frac{f(x)}{g(x)}$, называемый *рациональной дробью* с числителем $f(x)$ и знаменателем $g(x)$. Подчеркиваем, что это просто символ, соответствующий данной паре многочленов, так как деление многочленов в самом кольце $P[x]$, вообще говоря, невыполнимо, а ни в каком поле кольца $P[x]$ пока еще не содержится; если даже $g(x)$ является делителем для $f(x)$, новый символ $\frac{f(x)}{g(x)}$ следует пока отличать от многочлена, получающегося в качестве частного при делении $f(x)$ на $g(x)$.

Назовем теперь рациональные дроби $\frac{f(x)}{g(x)}$ и $\frac{\varphi(x)}{\psi(x)}$ равными:

$$\frac{f(x)}{g(x)} = \frac{\varphi(x)}{\psi(x)}, \quad (4)$$

если в кольце $P[x]$ имеет место равенство $f(x)\psi(x) = g(x)\varphi(x)$. Очевидно, что всякая дробь равна самой себе, а также, что если одна дробь равна другой, то и вторая равна первой. Докажем транзитивность этого понятия равенства. Пусть даны равенства (4) и

$$\frac{\varphi(x)}{\psi(x)} = \frac{u(x)}{v(x)}. \quad (5)$$

Из равносильных им равенств в кольце $P[x]$

$$f(x)\psi(x) = g(x)\varphi(x), \quad \varphi(x)v(x) = \psi(x)u(x)$$

вытекает

$$f(x)v(x)\psi(x) = g(x)\varphi(x)v(x) = g(x)u(x)\psi(x)$$

и поэтому, после сокращения на не равный нулю (как знаменатель одной из дробей) многочлен $\psi(x)$, получаем:

$$f(x)v(x) = g(x)u(x),$$

откуда, по определению равенства дробей,

$$\frac{f(x)}{g(x)} = \frac{u(x)}{v(x)},$$

что и требовалось доказать.

Объединим теперь в один класс все дроби, равные некоторой данной, и поэтому, в силу транзитивности равенства, равные между собой. Если в одном классе имеется хотя бы одна дробь, не

содержащаяся в другом классе, то, как следует из транзитивности равенства, эти два класса не имеют ни одного общего элемента.

Таким образом, совокупность всех рациональных дробей, написанных при помощи многочленов из кольца $P[x]$, распадается на непересекающиеся классы равных между собой дробей. Мы хотим теперь так определить алгебраические операции в этом множестве классов равных дробей, чтобы оно оказалось полем. Для этого мы будем определять операции над рациональными дробями и каждый раз проверять, что замена слагаемых (или множителей) равными им дробями заменяет сумму (или произведение) также равной дробью. Это позволит говорить о сумме и произведении классов равных дробей.

Предварительно сделаем следующее замечание, которое дальше будет неоднократно применяться: *рациональная дробь превращается в равную дробь, если ее числитель и знаменатель умножаются на один и тот же многочлен, отличный от нуля, или же сокращаются на любой общий множитель*. Действительно,

$$\frac{f(x)}{g(x)} = \frac{f(x)h(x)}{g(x)h(x)},$$

так как в кольце $P[x]$

$$f(x)[g(x)h(x)] = g(x)[f(x)h(x)].$$

Сложение рациональных дробей мы определяем по формуле (2); так как из $g(x) \neq 0$ и $\psi(x) \neq 0$ следует $g(x)\psi(x) \neq 0$, то правая часть этой формулы действительно будет рациональной дробью. Если дано, далее, что

$$\frac{f(x)}{g(x)} = \frac{f_0(x)}{g_0(x)}, \quad \frac{\varphi(x)}{\psi(x)} = \frac{\varphi_0(x)}{\psi_0(x)},$$

т. е.

$$f(x)g_0(x) = g(x)f_0(x), \quad \varphi(x)\psi_0(x) = \psi(x)\varphi_0(x), \quad (6)$$

то, умножая обе части первого из равенств (6) на $\psi(x)\psi_0(x)$, обе части второго равенства — на $g(x)g_0(x)$, а затем складывая эти равенства почленно, мы получим:

$$\begin{aligned} [f(x)\psi(x) + g(x)\varphi(x)]g_0(x)\psi_0(x) &= \\ &= [f_0(x)\psi_0(x) + g_0(x)\varphi_0(x)]g(x)\psi(x), \end{aligned}$$

что равносильно равенству

$$\frac{f(x)\psi(x) + g(x)\varphi(x)}{g(x)\psi(x)} = \frac{f_0(x)\psi_0(x) + g_0(x)\varphi_0(x)}{g_0(x)\psi_0(x)}.$$

Таким образом, если даны два класса равных между собой дробей, то суммы любой дроби из одного класса с любой дробью из другого класса все между собой равны, т. е. лежат в некотором вполне определенном третьем классе. Этот класс называется *суммой* заданных двух классов.

Коммутативность этого сложения непосредственно вытекает из (2), а ассоциативность доказывается следующим образом:

$$\begin{aligned} \left[\frac{f(x)}{g(x)} + \frac{\varphi(x)}{\psi(x)} \right] + \frac{u(x)}{v(x)} &= \frac{f(x)\psi(x) + g(x)\varphi(x)}{g(x)\psi(x)} + \frac{u(x)}{v(x)} = \\ &= \frac{f(x)\psi(x)v(x) + g(x)\varphi(x)v(x) + g(x)\psi(x)u(x)}{g(x)\psi(x)v(x)} = \\ &= \frac{f(x)}{g(x)} + \frac{\varphi(x)v(x) + \psi(x)u(x)}{\psi(x)v(x)} = \frac{f(x)}{g(x)} + \left[\frac{\varphi(x)}{\psi(x)} + \frac{u(x)}{v(x)} \right]. \end{aligned}$$

Из определения равенства дробей без труда следует, что все дроби вида $\frac{0}{g(x)}$, т. е. дроби с равным нулю числителем, равны между собой и что они составляют полный класс равных дробей. Этот класс мы назовем *нулевым* и докажем, что он играет в нашем сложении роль нуля. Действительно, если дана произвольная дробь $\frac{\varphi(x)}{\psi(x)}$, то

$$\frac{0}{g(x)} + \frac{\varphi(x)}{\psi(x)} = \frac{0 \cdot \psi(x) + g(x)\varphi(x)}{g(x)\psi(x)} = \frac{g(x)\varphi(x)}{g(x)\psi(x)} = \frac{\varphi(x)}{\psi(x)}.$$

Из равенства

$$\frac{f(x)}{g(x)} + \frac{-f(x)}{g(x)} = \frac{0}{g^2(x)},$$

правая часть которого принадлежит к нулевому классу, следует теперь, что класс дробей, равных дроби $\frac{-f(x)}{g(x)}$, будет *противоположным* для класса дробей, равных дроби $\frac{f(x)}{g(x)}$. Отсюда, как мы знаем, следует выполнимость однозначного *вычитания*.

Умножение рациональных дробей мы определим по формуле (3), причем, ввиду $g(x)\psi(x) \neq 0$, правая часть этой формулы действительно будет рациональной дробью. Если, далее,

$$\frac{f(x)}{g(x)} = \frac{f_0(x)}{g_0(x)}, \quad \frac{\varphi(x)}{\psi(x)} = \frac{\varphi_0(x)}{\psi_0(x)},$$

т. е.

$$f(x)g_0(x) = g(x)f_0(x), \quad \varphi(x)\psi_0(x) = \psi(x)\varphi_0(x),$$

то, перемножая эти последние равенства почленно, мы получим:

$$f(x)g_0(x)\varphi(x)\psi_0(x) = g(x)f_0(x)\psi(x)\varphi_0(x),$$

что равносильно равенству

$$\frac{f(x)\varphi(x)}{g(x)\psi(x)} = \frac{f_0(x)\varphi_0(x)}{g_0(x)\psi_0(x)}.$$

Таким образом, по аналогии с данным выше определением суммы классов, можно говорить о *произведении* классов равных между собой дробей.

Коммутативность и ассоциативность этого умножения непосредственно следуют из (3), а справедливость закона дистрибутивности доказывается следующим образом:

$$\begin{aligned} \left[\frac{f(x)}{g(x)} + \frac{\varphi(x)}{\psi(x)} \right] \frac{u(x)}{v(x)} &= \frac{f(x)\psi(x) + g(x)\varphi(x)}{g(x)\psi(x)} \cdot \frac{u(x)}{v(x)} = \\ &= \frac{[f(x)\psi(x) + g(x)\varphi(x)]u(x)}{g(x)\psi(x)v(x)} = \frac{f(x)\psi(x)u(x) + g(x)\varphi(x)u(x)}{g(x)\psi(x)v(x)} = \\ &= \frac{f(x)\psi(x)u(x)v(x) + g(x)\varphi(x)u(x)v(x)}{g(x)\psi(x)v^2(x)} = \frac{f(x)u(x)}{g(x)v(x)} + \frac{\varphi(x)u(x)}{\psi(x)v(x)} = \\ &= \frac{f(x)}{g(x)} \cdot \frac{u(x)}{v(x)} + \frac{\varphi(x)}{\psi(x)} \cdot \frac{u(x)}{v(x)}. \end{aligned}$$

Легко видеть, что дроби вида $\frac{f(x)}{f(x)}$, т. е. дроби, числитель которых равен знаменателю, все равны между собой и составляют отдельный класс. Этот класс называется *единичным* и играет в нашем умножении роль единицы:

$$\frac{f(x)}{f(x)} \cdot \frac{\varphi(x)}{\psi(x)} = \frac{f(x)\varphi(x)}{f(x)\psi(x)} = \frac{\varphi(x)}{\psi(x)}.$$

Если, наконец, дробь $\frac{f(x)}{g(x)}$ не принадлежит к нулевому классу, т. е. $f(x) \neq 0$, то существует дробь $\frac{g(x)}{f(x)}$. Так как

$$\frac{f(x)}{g(x)} \cdot \frac{g(x)}{f(x)} = \frac{f(x)g(x)}{g(x)f(x)},$$

а правая часть этого равенства принадлежит к единичному классу, то класс дробей, равных дроби $\frac{g(x)}{f(x)}$, будет *обратным* для класса дробей, равных дроби $\frac{f(x)}{g(x)}$. Отсюда следует выполнимость однозначного деления.

Таким образом, классы равных между собой рациональных дробей с коэффициентами из поля P составляют при нашем определении операций коммутативное поле. Это поле и будет искомым полем $P(x)$. Мы должны еще, впрочем, доказать, что в построенном нами поле содержится подкольцо, изоморфное кольцу $P[x]$, и что всякий элемент поля представим в виде частного двух элементов из этого подкольца.

Если мы произвольному многочлену $f(x)$ из кольца $P[x]$ поставим в соответствие класс рациональных дробей, равных дроби $\frac{f(x)}{1}$ (среди всех дробей содержатся, понятно, и дроби, знаменатель которых равен единице), то получим взаимно однозначное отображение

кольца $P[x]$ внутрь построенного нами поля. Действительно, из равенства

$$\frac{f(x)}{1} = \frac{\varphi(x)}{1}$$

следовало бы $f(x) \cdot 1 = 1 \cdot \varphi(x)$, т. е. $f(x) = \varphi(x)$. Это отображение будет даже изоморфным, как показывают равенства

$$\frac{f(x)}{1} + \frac{g(x)}{1} = \frac{f(x) \cdot 1 + g(x) \cdot 1}{1^2} = \frac{f(x) + g(x)}{1},$$

$$\frac{f(x)}{1} \cdot \frac{g(x)}{1} = \frac{f(x) \cdot g(x)}{1}.$$

Таким образом, *классы дробей, равных дробям вида $\frac{f(x)}{1}$, составляют в нашем поле подкольцо, изоморфное кольцу $P[x]$.* Дробь $\frac{f(x)}{1}$ можно поэтому обозначить просто $f(x)$. Так как, наконец, при $g(x) \neq 0$ класс дробей, равных дроби $\frac{1}{g(x)}$, является обратным для класса дробей, равных дроби $\frac{g(x)}{1}$, то из равенства

$$\frac{f(x)}{1} \cdot \frac{1}{g(x)} = \frac{f(x)}{g(x)}$$

следует, что *все элементы нашего поля можно считать (в смысле операций, определенных в этом поле) частными многочленов из кольца $P[x]$.*

Мы построили над произвольным полем P поле рациональных дробей $P(x)$. Этим же методом, беря вместо кольца многочленов кольцо целых чисел, можно построить поле рациональных чисел. Объединяя эти два случая и используя такой же метод, можно было бы доказать теорему, что вообще всякое коммутативное кольцо без делителей нуля является подкольцом некоторого поля.

ГЛАВА ОДИННАДЦАТАЯ

МНОГОЧЛЕНЫ ОТ НЕСКОЛЬКИХ НЕИЗВЕСТНЫХ

§ 51. Кольцо многочленов от нескольких неизвестных

Нередко приходится рассматривать многочлены, зависящие не от одного, а от двух, трех, вообще от нескольких неизвестных. Так, в первых главах книги нами уже изучались линейные и квадратичные формы, представляющие собой примеры таких многочленов. Вообще *многочленом* $f(x_1, x_2, \dots, x_n)$ от n неизвестных x_1, x_2, \dots, x_n над некоторым полем P называется сумма конечного числа членов вида $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$, где все $k_i \geq 0$, с коэффициентами из поля P ; при этом предполагается, понятно, что многочлен $f(x_1, x_2, \dots, x_n)$ не содержит подобных членов и что рассматриваются лишь члены с отличными от нуля коэффициентами. Два многочлена от n неизвестных, $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$, считаются *равными* (или *тождественно равными*), если равны их коэффициенты при одинаковых членах.

Если дан многочлен $f(x_1, x_2, \dots, x_n)$ над полем P , то его *степенью по отношению к неизвестному* x_i , $i = 1, 2, \dots, n$, называется наивысший показатель, с каким входит x_i в члены этого многочлена. Случайно эта степень может быть равной 0, что означает, что хотя f считается многочленом от n неизвестных $x_1, x_2, \dots, x_i, \dots, x_n$, но неизвестное x_i на самом деле в его запись не входит.

С другой стороны, если мы назовем *степенью члена*

$$x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$$

число $k_1 + k_2 + \dots + k_n$, т. е. сумму показа степеней при неизвестных, то *степенью многочлена* $f(x_1, x_2, \dots, x_n)$ (т. е. степенью по совокупности неизвестных) будет наивысшая из степеней его членов. В частности, многочленами нулевой степени будут, как и в случае одного неизвестного, лишь отличные от нуля элементы из поля P . С другой стороны, как и в случае многочленов от одного неизвестного, нуль будет единственным многочленом от n неизвестных, степень которого не определена. Понятно, что многочлен в общем случае может содержать несколько членов наивысшей степени и поэтому нельзя говорить о старшем (по степени) члене многочлена.

Для многочленов от n неизвестных над полем P следующим образом определяются операции сложения и умножения. *Суммой* многочленов $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ называется многочлен, коэффициенты которого получаются сложением соответственных коэффициентов многочленов f и g ; если при этом некоторый член входит лишь в один из многочленов f, g , то коэффициент при нем в другом многочлене считается, понятно, равным нулю. Произведение двух «одночленов» определяется следующим равенством:

$$ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n} \cdot bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n} = (ab)x_1^{k_1+l_1}x_2^{k_2+l_2}\dots x_n^{k_n+l_n},$$

после чего *произведение* многочленов $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ определяется как результат почленного перемножения и последующего приведения подобных членов.

При таком определении операций совокупность многочленов от n неизвестных над полем P превращается в коммутативное кольцо, причем это кольцо не содержит делителей нуля. В самом деле, при $n=1$ наши определения совпадают с теми, которые были даны в § 20 для случая многочленов от одного неизвестного. Пусть уже доказано, что многочлены от $n-1$ неизвестных x_1, x_2, \dots, x_{n-1} с коэффициентами из поля P составляют кольцо без делителей нуля. Всякий многочлен от n неизвестных $x_1, x_2, \dots, x_{n-1}, x_n$ можно представить, притом единственным способом, как многочлен от неизвестного x_n с коэффициентами, являющимися многочленами от x_1, x_2, \dots, x_{n-1} ; обратно, всякий многочлен от x_n с коэффициентами из кольца многочленов от x_1, x_2, \dots, x_{n-1} над полем P можно рассматривать, конечно, как многочлен над этим же полем P от всей совокупности неизвестных $x_1, x_2, \dots, x_{n-1}, x_n$. Без труда проверяется, что полученное нами взаимно однозначное соответствие между многочленами от n неизвестных и многочленами от одного неизвестного над кольцом многочленов от $n-1$ неизвестных является изоморфным по отношению к операциям сложения и умножения. Доказываемое утверждение вытекает теперь из того, что многочлены от одного неизвестного над кольцом многочленов от $n-1$ неизвестных сами составляют кольцо, причем оно как кольцо многочленов от одного неизвестного над кольцом без делителей нуля само не содержит делителей нуля (см. § 47).

Мы доказали, следовательно, существование *кольца многочленов от n неизвестных над полем P* ; это кольцо обозначается символом $P[x_1, x_2, \dots, x_n]$.

Следующие рассмотрения позволяют посмотреть на кольцо многочленов от n неизвестных с несколько иной точки зрения. Пусть поле P содержится в некотором коммутативном кольце L в качестве подкольца. Возьмем в L n элементов $\alpha_1, \alpha_2, \dots, \alpha_n$ и найдем минимальное подкольцо L' кольца L , содержащее эти элементы и все поле P , т. е. подкольцо, получающееся в результате *присоединения*

к полю P элементов $\alpha_1, \alpha_2, \dots, \alpha_n$. Подкольцо L' состоит из всех элементов кольца L , которые выражаются через элементы $\alpha_1, \alpha_2, \dots, \alpha_n$ и элементы поля P при помощи сложения, вычитания и умножения. Легко видеть, что это будут в точности те элементы кольца L , которые можно записать (при помощи операций, имеющих место в L) в виде многочленов от $\alpha_1, \alpha_2, \dots, \alpha_n$ с коэффициентами из P , причем эти элементы будут как элементы кольца L между собой складываться и умножаться как раз по указанным выше правилам сложения и умножения многочленов от n неизвестных.

Конечно, данный элемент β из подкольца L' будет, вообще говоря, обладать многими различными записями в виде многочлена от $\alpha_1, \alpha_2, \dots, \alpha_n$ с коэффициентами из поля P . Если для всякого β из L' такая запись однозначна, т. е. если различные многочлены от $\alpha_1, \alpha_2, \dots, \alpha_n$ будут различными элементами кольца L' (и, следовательно, кольца L), то система элементов $\alpha_1, \alpha_2, \dots, \alpha_n$ называется *алгебраически независимой* над полем P , в противном случае — *алгебраически зависимой*¹⁾. Отсюда можно вывести такое заключение:

Если поле P является подкольцом коммутативного кольца L и если система элементов $\alpha_1, \alpha_2, \dots, \alpha_n$ из L алгебраически независима над P , то подкольцо L' кольца L , порожданное присоединением к полю P элементов $\alpha_1, \alpha_2, \dots, \alpha_n$, изоморфно кольцу многочленов $P[x_1, x_2, \dots, x_n]$.

Из других свойств кольца многочленов от n неизвестных $P[x_1, x_2, \dots, x_n]$ укажем на следующее: это кольцо можно включить в поле рациональных дробей $P(x_1, x_2, \dots, x_n)$ от n неизвестных над полем P . Всякий элемент этого поля может быть записан в виде $\frac{f}{g}$, где f и g — многочлены из кольца $P[x_1, x_2, \dots, x_n]$, причем тогда и только тогда $\frac{f}{g} = \frac{\varphi}{\psi}$, если $f\varphi = g\psi$. Сложение и умножение этих рациональных дробей производятся по правилам, которые, как было указано в § 45, справедливы для частных во всяком поле. Доказательство существования поля $P(x_1, x_2, \dots, x_n)$ проводится так же, как это делалось в § 50 для случая $n=1$.

Для многочленов от нескольких неизвестных можно построить теорию делимости, обобщающую ту теорию делимости для многочленов от одного неизвестного, которую мы изучали в гл. 5 и 10. Так как, однако, детальное изучение кольца многочленов от нескольких неизвестных не входит в наши задачи, то мы ограничимся только вопросом о разложении многочлена на неприводимые множители.

Введем сначала следующее понятие: если все члены многочлена $f(x_1, x_2, \dots, x_n)$ имеют одну и ту же степень s , то такой многочлен называется *однородным многочленом* или, короче, *формой* s -й степени; нам

¹⁾ Соответствующие понятия для случая $n=1$ были уже введены в § 47: элемент α , алгебраически независимый над полем P в смысле только что данного определения, был назван там трансцендентным над P , в противном случае — алгебраическим над P .

уже известны линейные и квадратичные формы, можно рассматривать, далее, кубичные формы, все члены которых имеют по совокупности неизвестных степень 3, и т. д. Всякий многочлен от n неизвестных однозначно представим в виде суммы нескольких форм от этих неизвестных, притом имеющих разные степени: достаточно объединить вместе все члены, имеющие одну и ту же степень, чтобы получить искомое представление. Так, многочлен четвертой степени $f(x_1, x_2, x_3) = 3x_1x_2^2 - 7x_1^2x_3^2 + x_2 - 5x_1x_2x_3 + x_1^4 - 2x_3 - 6 + x_3^3$ будет суммой формы четвертой степени $x_1^4 - 7x_1^2x_3^2$, кубичной формы $3x_1x_2^2 - 5x_1x_2x_3 + x_3^3$, линейной формы $x_2 - 2x_3$ и свободного члена (формы нулевой степени) -6 .

Докажем теперь следующую теорему:

Степень произведения двух отличных от нуля многочленов от n неизвестных равна сумме степеней этих многочленов.

Предположим сначала, что нам даны формы $\varphi(x_1, x_2, \dots, x_n)$ степени s и $\psi(x_1, x_2, \dots, x_n)$ степени t . Произведение любого члена формы φ на любой член формы ψ будет, очевидно, иметь степень $s+t$, а потому произведение $\varphi\psi$ будет формой степени $s+t$, так как приведение подобных членов не может сделать все коэффициенты этого произведения равными нулю ввиду отсутствия в кольце $P[x_1, x_2, \dots, x_n]$ делителей нуля.

Если теперь даны произвольные многочлены $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ соответственно степеней s и t , то, представляя каждый из них в виде суммы форм разных степеней, мы получим:

$$f(x_1, x_2, \dots, x_n) = \varphi(x_1, x_2, \dots, x_n) + \dots,$$

$$g(x_1, x_2, \dots, x_n) = \psi(x_1, x_2, \dots, x_n) + \dots,$$

где φ и ψ будут соответственно формами степеней s и t , а многоточия заменяют суммы форм меньших степеней. Тогда

$$fg = \varphi\psi + \dots;$$

форма $\varphi\psi$ имеет, по доказанному, степень $s+t$, а так как все члены, замененные многоточием, имеют меньшую степень, то степень произведения fg будет равна $s+t$. Теорема доказана.

Многочлен φ называется *делителем* многочлена f , а f — *делящимся на φ* , если в кольце $P[x_1, x_2, \dots, x_n]$ существует такой многочлен ψ , что $f = \varphi\psi$. Легко видеть, что свойства делимости I—IX из § 21 сохраняются и в рассматриваемом сейчас общем случае. Многочлен f степени k , $k \geq 1$, называется *приводимым* над полем P , если он разлагается в произведение многочленов из кольца $P[x_1, x_2, \dots, x_n]$, степени которых меньше k , и *неприводимым* — в противоположном случае.

Всякий многочлен из кольца $P[x_1, x_2, \dots, x_n]$, имеющий степень, отличную от нуля, разлагается в произведение *неприводимых множителей*. Это разложение однозначно с точностью до множителей нулевой степени.

Эта теорема обобщает соответствующие результаты из § 48, относящиеся к многочленам от одного неизвестного. Ее первое утверждение доказывается дословным повторением рассуждений из указанного параграфа. Доказательство второго утверждения представляет уже значительные трудности. Прежде чем проводить его, мы заметим, что из второго утверждения этой теоремы вытекает такое следствие: *если произведение двух многочленов f и g из кольца $P[x_1, x_2, \dots, x_n]$ делится на неприводимый многочлен p , то хотя бы один из этих многочленов делится на p .* Действительно, в противном случае мы получили бы для произведения fg два разложения на неприводимые множители, одно из которых p не содержит, а другое содержит.

Пусть теорема уже доказана для многочленов от n неизвестных, и мы хотим доказать ее для многочлена от $n+1$ неизвестных x, x_1, x_2, \dots, x_n . Запишем этот многочлен в виде $\phi(x)$; его коэффициенты будут, следовательно, многочленами от x_1, x_2, \dots, x_n . Для этих коэффициентов теорема уже доказана, т. е. каждый из них однозначно разлагается в произведение неприводимых множителей. Назовем многочлен $\phi(x)$ примитивным (точнее, примитивным над кольцом $P[x_1, x_2, \dots, x_n]$), если его коэффициенты не содержат ни одного общего неприводимого множителя, т. е. в совокупности взаимно просты, и докажем следующую лемму Гаусса:

Произведение двух примитивных многочленов само есть примитивный многочлен.

В самом деле, пусть даны примитивные многочлены

$$\begin{aligned} f(x) &= a_0x^k + a_1x^{k-1} + \dots + a_ix^{k-i} + \dots + a_k, \\ g(x) &= b_0x^l + b_1x^{l-1} + \dots + b_jx^{l-j} + \dots + b_l \end{aligned}$$

с коэффициентами из кольца $P[x_1, x_2, \dots, x_n]$ и пусть

$$f(x)g(x) = c_0x^{k+l} + c_1x^{k+l-1} + \dots + c_{i+j}x^{k+l-(i+j)} + \dots + c_{k+l}.$$

Если это произведение не примитивно, то коэффициенты c_0, c_1, \dots, c_{k+l} будут обладать общим неприводимым множителем $p = p(x_1, x_2, \dots, x_n)$. Так как все коэффициенты примитивного многочлена $f(x)$ не могут делиться на p , то пусть коэффициент a_i будет первым, на p не делящимся; аналогично через b_j мы обозначим первый коэффициент многочлена $g(x)$, не делящийся на p . Перемножая почленно $f(x)$ и $g(x)$ и собирая члены, содержащие $x^{k+l-(i+j)}$, мы получим:

$$c_{i+j} = a_ib_j + a_{i-1}b_{j+1} + a_{i-2}b_{j+2} + \dots + a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \dots$$

Левая часть этого равенства делится на неприводимый многочлен p . На него заведомо делятся также все слагаемые правой части, кроме первого; действительно, ввиду условий, наложенных на выбор i и j , все коэффициенты a_{i-1}, a_{i-2}, \dots , а также b_{j-1}, b_{j-2}, \dots делятся на p . Отсюда следует, что произведение a_ib_j также делится на p , а поэтому, как отмечено выше, на p должен делиться хотя бы один из многочленов a_i, b_j , что, однако, не имеет места. Этим заканчивается доказательство леммы в предположении справедливости основной теоремы для многочленов от n неизвестных.

Кольцо $P[x_1, x_2, \dots, x_n]$ содержится, как мы знаем, в поле рациональных дробей $P(x_1, x_2, \dots, x_n)$, которое мы обозначим через Q :

$$Q = P(x_1, x_2, \dots, x_n).$$

Рассмотрим кольцо многочленов $Q[x]$. Если многочлен $\phi(x)$ принадлежит к этому кольцу, то каждый его коэффициент представим в виде частного многочленов из кольца $P[x_1, x_2, \dots, x_n]$. Вынося за скобки общий знаменатель этих частных, а затем и общие множители из числителей, можно представить $\phi(x)$ в виде

$$\phi(x) = \frac{a}{b} f(x).$$

Здесь a и b являются многочленами из кольца $P[x_1, x_2, \dots, x_n]$, а $f(x)$ — многочленом от x с коэффициентами из $P[x_1, x_2, \dots, x_n]$, причем даже примитивным многочленом, так как его коэффициенты уже не имеют общих множителей.

Этим путем всякому многочлену $\phi(x)$ из кольца $Q[x]$ поставлен в соответствие примитивный многочлен $f(x)$. Для данного $\phi(x)$ многочлен $f(x)$

определен однозначно с точностью до отличного от нуля множителя из поля P . Действительно, пусть

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x),$$

где $g(x)$ — снова примитивный многочлен. Тогда

$$adf(x) = bcg(x).$$

Таким образом, ad и bc получены вынесением всех общих множителей из коэффициентов одного и того же многочлена над кольцом $P[x_1, x_2, \dots, x_n]$. Отсюда вытекает, ввиду справедливости в этом кольце (по предположению индукции) теоремы об однозначности разложения, что ad и bc могут отличаться друг от друга лишь множителем нулевой степени. Таким же множителем, следовательно, отличаются друг от друга примитивные многочлены $f(x)$ и $g(x)$.

Произведению двух многочленов из кольца $Q[x]$ соответствует произведение соответствующих им примитивных многочленов. В самом деле, если

$$\varphi(x) = \frac{a}{b} f(x), \quad \psi(x) = \frac{c}{d} g(x),$$

где $f(x)$ и $g(x)$ — примитивные многочлены, то

$$\varphi(x) \psi(x) = \frac{ac}{bd} f(x) g(x).$$

Но, как доказано выше, произведение $f(x) g(x)$ является примитивным многочленом.

Отметим, далее, что если многочлен $\varphi(x)$ из кольца $Q[x]$ неприводим над полем Q , то соответствующий ему примитивный многочлен $f(x)$, рассматриваемый как многочлен от x, x_1, x_2, \dots, x_n , также будет неприводимым, и обратно. В самом деле, если многочлен f приводим, $f = f_1 f_2$, то оба множителя должны содержать неизвестное x , так как иначе многочлен f не был бы примитивным. Отсюда вытекает разложение многочлена $\varphi(x)$ над полем Q :

$$\varphi(x) = \frac{a}{b} f(x) = \left(\frac{a}{b} f_1 \right) f_2.$$

Обратно, если многочлен $\varphi(x)$ приводим над Q , $\varphi(x) = \varphi_1(x) \varphi_2(x)$, то примитивные многочлены $f_1(x)$ и $f_2(x)$, соответствующие многочленам $\varphi_1(x)$ и $\varphi_2(x)$, будут оба содержать x , но их произведение, как доказано выше, равно $f(x)$ (с точностью до множителя из поля P).

Возьмем теперь примитивный многочлен f и разложим его на неприводимые множители, $f = f_1 \cdot f_2 \cdots f_k$. Все эти множители не только должны содержать неизвестное x , но даже будут примитивными многочленами, так как иначе многочлен f не был бы примитивным. Это разложение примитивного многочлена f будет однозначным с точностью до множителей из поля P . В самом деле, ввиду предшествующей леммы, можно смотреть на это разложение как на разложение $f(x)$ на неприводимые множители над полем Q , но для многочленов от одного неизвестного над некоторым полем однозначность разложения нам уже известна; эта однозначность имеет место с точностью до множителей из Q ; однако в нашем случае, благодаря примитивности всех множителей f_i , она будет с точностью до множителей из P .

После этих лемм, справедливость которых нами доказана, исходя из индуктивного предположения, доказательство нашей основной теоремы проходит без всяких затруднений. В самом деле, всякий неприводимый многочлен из кольца $P[x, x_1, x_2, \dots, x_n]$ будет или неприводимым многочленом

из кольца $P[x_1, x_2, \dots, x_n]$, или же неприводимым примитивным многочленом. Отсюда следует, что если нам дано некоторое разложение многочлена $\Phi(x, x_1, x_2, \dots, x_n)$ на неприводимые множители, то, объединяя множители, мы представим Φ в виде

$$\Phi(x, x_1, x_2, \dots, x_n) = a(x_1, x_2, \dots, x_n) f(x, x_1, x_2, \dots, x_n),$$

где a от x не зависит, а f является примитивным многочленом. Мы знаем, однако, что это разложение для Φ однозначно с точностью до множителей из P . Так как, с другой стороны, однозначность разложения на неприводимые множители для многочлена a от n неизвестных имеет место по предположению индукции, а для примитивного многочлена f доказана в предшествующей лемме, то наша теорема для случая $n+1$ неизвестных также полностью доказана.

Из доказанных выше лемм вытекает еще одно интересное следствие: если многочлен $\Phi(x)$ с коэффициентами из $P[x_1, x_2, \dots, x_n]$ приводим над полем $Q = P(x_1, x_2, \dots, x_n)$, то он может быть разложен на множители, зависящие от x и имеющие коэффициентами многочлены из кольца $P[x_1, x_2, \dots, x_n]$. Действительно, если многочлену $\Phi(x)$ соответствует примитивный многочлен $f(x)$, т. е. $\Phi(x) = af(x)$, то, как мы знаем, из разложимости $\Phi(x)$ следует разложимость $f(x)$; последнее приводит, однако, к разложению $\Phi(x)$ над кольцом $P[x_1, x_2, \dots, x_n]$.

В отличие от случая многочленов от одного неизвестного, которые, как мы знаем из § 49, могут быть разложены на линейные множители над соответственно подобранным расширением рассматриваемого основного поля, над любым полем P существуют абсолютно неприводимые многочлены произвольной степени от нескольких (двух или более) неизвестных, т. е. многочлены, которые остаются неприводимыми при любом расширении этого поля.

Таков, например, многочлен

$$f(x, y) = \Phi(x) + y,$$

где $\Phi(x)$ — произвольный многочлен от одного неизвестного над полем P . Действительно, если бы в некотором расширении \bar{P} поля P существовало разложение

$$f(x, y) = g(x, y) h(x, y),$$

то, записывая g и h по степеням y , мы получили бы, что, например,

$$g(x, y) = a_0(x)y + a_1(x), \quad h(x, y) = b_0(x),$$

т. е. h не зависит от y , а затем, ввиду $a_0(x)b_0(x) = 1$, что $b_0(x)$ имеет степень 0, т. е. h не зависит и от x .

Лексикографическое расположение членов многочлена. Для многочленов от одного неизвестного мы имеем два естественных способа расположения членов — по убывающим и по возрастающим степеням неизвестного. В случае многочленов от нескольких неизвестных такие способы уже отсутствуют: если дан многочлен пятой степени от трех неизвестных

$$f(x_1, x_2, x_3) = x_1 x_2^2 x_3^2 + x_1^4 x_3 + x_2^3 x_3^2 + x_1^2 x_2 x_3^2,$$

то его можно было бы записать и в виде

$$f(x_1, x_2, x_3) = x_1^4 x_3 + x_1^2 x_2 x_3^2 + x_1 x_2^2 x_3^2 + x_2^3 x_3^2,$$

и нет оснований одну из этих записей предпочтеть другой. Существует, однако, способ вполне определенного расположения членов многочлена от нескольких неизвестных, зависящий, впрочем, от выбора нумерации неизвестных; для многочленов от одного неизвестного он приводит к расположению членов по убывающим степеням неизвестного. Этот способ, называемый *лексикографическим*, подсказан обычным приемом расположения слов в словарях («лексиконах»): считая буквы упорядоченными так, как это принято в алфавите, мы определяем взаимное положение двух данных слов в словаре по их первым буквам, если же эти буквы совпадают, то по вторым буквам и т. д.

Пусть дан многочлен $f(x_1, x_2, \dots, x_n)$ из кольца $P[x_1, x_2, \dots, x_n]$ и в нем два различных члена:

$$x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \quad (1)$$

$$x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}, \quad (2)$$

коэффициенты которых являются некоторыми отличными от нуля элементами из P . Так как члены (1) и (2) различны, то хотя бы одна из разностей показателей при неизвестных

$$k_i - l_i, \quad i = 1, 2, \dots, n,$$

отлична от нуля. Член (1) будет считаться *выше* члена (2) (а член (2) — *ниже* члена (1)), если первая из этих разностей, отличная от нуля, положительна, т. е. если существует такое i , $1 \leq i \leq n$, что

$$k_1 = l_1, \quad k_2 = l_2, \dots, k_{i-1} = l_{i-1}, \quad \text{но } k_i > l_i.$$

Иными словами, член (1) будет выше члена (2), если показатель при x_1 в (1) больше, чем в (2), или если эти показатели равны, но показатель при x_2 в (1) больше, чем в (2), и т. д. Легко видеть, что из того, что член (1) выше члена (2), не следует, что степень первого по совокупности неизвестных больше степени второго: из членов

$$x_1^3 x_2 x_3, \quad x_1 x_2^5 x_3^2$$

первый выше, хотя имеет меньшую степень.

Очевидно, что из любых двух различных членов многочлена $f(x_1, x_2, \dots, x_n)$ один будет выше другого. Легко проверить также, что если член (1) выше члена (2), а член (2), в свою очередь, выше члена

$$x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}, \quad (3)$$

т. е. существует такое j , $1 \leq j \leq n$, что

$$l_1 = m_1, \quad l_2 = m_2, \dots, l_{j-1} = m_{j-1}, \quad \text{но } l_j > m_j,$$

то, независимо от того, будет ли i больше, равно или меньше j , член (1) будет выше члена (3). Таким образом, ставя раньше тот

из двух членов, который выше, мы получим вполне определенное упорядочение членов многочлена $f(x_1, x_2, \dots, x_n)$, которое и называется лексикографическим.

Так, многочлен

$$f(x_1, x_2, x_3, x_4) = x_1^4 + 3x_1^2x_2^3x_3 - x_1^2x_2^3x_4^2 + 5x_1x_3x_4^2 + 2x_2 + x_3^3x_4 - 4$$

расположен лексикографически.

При лексикографической записи многочлена $f(x_1, x_2, \dots, x_n)$ один из его членов будет стоять на первом месте, т. е. будет выше всех других членов. Этот член называется *высшим членом многочлена*; в предшествующем примере высшим членом будет член x_1^4 . Относительно высших членов мы докажем лемму, которая будет использована при доказательстве основной теоремы следующего параграфа:

Высший член произведения двух многочленов от n неизвестных равен произведению высших членов сомножителей.

В самом деле, пусть перемножаются многочлены $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$. Если

$$ax_1^{k_1}x_2^{k_2} \dots x_n^{k_n} \quad (4)$$

будет высший член многочлена $f(x_1, x_2, \dots, x_n)$, а

$$a'x_1^{s_1}x_2^{s_2} \dots x_n^{s_n} \quad (5)$$

— любой другой член этого многочлена, то существует такое i , $1 \leq i \leq n$, что

$$k_1 = s_1, \dots, k_{i-1} = s_{i-1}, \quad k_i > s_i.$$

Если, с другой стороны,

$$bx_1^{l_1}x_2^{l_2} \dots x_n^{l_n}, \quad (6)$$

$$b'x_1^{t_1}x_2^{t_2} \dots x_n^{t_n} \quad (7)$$

будут высший и любой другой члены многочлена $g(x_1, x_2, \dots, x_n)$, то существует такое j , $1 \leq j \leq n$, что

$$l_1 = t_1, \dots, l_{j-1} = t_{j-1}, \quad l_j > t_j.$$

Перемножая члены (4) и (6), а также члены (5) и (7), мы получаем:

$$abx_1^{k_1+l_1}x_2^{k_2+l_2} \dots x_n^{k_n+l_n}, \quad (8)$$

$$a'b'x_1^{s_1+t_1}x_2^{s_2+t_2} \dots x_n^{s_n+t_n}. \quad (9)$$

Легко видеть, однако, что член (8) выше члена (9); если, например, $i \leq j$, то

$$k_1 + l_1 = s_1 + t_1, \dots, k_{i-1} + l_{i-1} = s_{i-1} + t_{i-1}, \quad \text{но} \quad k_i + l_i > s_i + t_i,$$

так как $k_i > s_i$, $l_i \geq t_i$. Так же проверяется, что член (8) будет выше произведения членов (4) и (7), а также выше произведения

членов (5) и (6). Таким образом, член (8) — произведение высших членов многочленов f и g — будет выше всех других членов, получающихся в результате почленного перемножения многочленов f и g , а потому этот член не уничтожается при приведении подобных членов, т. е. остается высшим членом в произведении fg .

§ 52. Симметрические многочлены

Среди многочленов от нескольких неизвестных выделяются те, которые не меняются ни при какой перестановке неизвестных. В такие многочлены все неизвестные входят, следовательно, вполне симметричным образом, и поэтому эти многочлены называются *симметрическими многочленами* (или *симметрическими функциями*). Простейшими примерами будут: сумма всех неизвестных $x_1 + x_2 + \dots + x_n$, сумма квадратов неизвестных $x_1^2 + x_2^2 + \dots + x_n^2$, произведение неизвестных $x_1 x_2 \dots x_n$ и т. д. Ввиду представимости всякой подстановки n символов в виде произведения транспозиций (см. § 3), при доказательстве симметричности некоторого многочлена достаточно проверить, что он не меняется ни при какой транспозиции двух неизвестных.

Мы будем рассматривать дальше симметрические многочлены от n неизвестных с коэффициентами из некоторого поля P . Легко видеть, что *сумма, разность и произведение двух симметрических многочленов сами будут симметрическими*, т. е. симметрические многочлены составляют подкольцо в кольце $P[x_1, x_2, \dots, x_n]$ всех многочленов от n неизвестных над полем P , называемое *кольцом симметрических многочленов от n неизвестных над полем P*. К этому кольцу принадлежат все элементы из P (т. е. все многочлены нулевой степени, а также нуль), так как они заведомо не меняются ни при какой перестановке неизвестных. Всякий другой симметрический многочлен непременно содержит все n неизвестных и даже имеет по ним одну и ту же степень: если симметрический многочлен $f(x_1, x_2, \dots, x_n)$ обладает членом, в который неизвестное x_i входит с показателем k , то обладает и членом, получающимся из него транспозицией неизвестных x_i и x_j , т. е. содержащим неизвестное x_j в той же степени k .

Следующие n симметрических многочленов от n неизвестных называются *элементарными симметрическими многочленами*:

$$\left. \begin{aligned} \sigma_1 &= x_1 + x_2 + \dots + x_n, \\ \sigma_2 &= x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n, \\ \sigma_3 &= x_1 x_2 x_3 + x_1 x_2 x_4 + \dots + x_{n-2} x_{n-1} x_n, \\ &\dots \\ \sigma_{n-1} &= x_1 x_2 \dots x_{n-1} + x_1 x_2 \dots x_{n-2} x_n + \dots + x_2 x_3 \dots x_n, \\ \sigma_n &= x_1 x_2 \dots x_n. \end{aligned} \right\} \quad (1)$$

Эти многочлены, симметричность которых очевидна, играют в теории симметрических многочленов очень большую роль. Они подсказаны формулами Вьета (см. § 24), и поэтому можно сказать, что *коэффициенты многочлена от одного неизвестного, имеющего старшим коэффициентом единицу, будут, с точностью до знака, элементарными симметрическими многочленами от его корней.* Эта связь элементарных симметрических многочленов с формулами Вьета будет весьма существенна для тех применений симметрических многочленов к теории многочленов от одного неизвестного, ради которых мы сейчас их изучаем.

Так как симметрические многочлены от n неизвестных x_1, x_2, \dots, x_n над полем P составляют кольцо, то очевидны следующие утверждения: симметрическим многочленом будет всякая целая положительная степень любого из элементарных симметрических многочленов, а также произведение таких степеней, притом взятое с любым коэффициентом из P , и, наконец, всякая сумма указанных произведений. Иными словами, *всякий многочлен от элементарных симметрических многочленов $\sigma_1, \sigma_2, \dots, \sigma_n$ с коэффициентами из P , рассматриваемый как многочлен от неизвестных x_1, x_2, \dots, x_n , будет симметрическим.* Так, положим $n=3$ и возьмем многочлен $\sigma_1\sigma_2 + 2\sigma_3$. Заменяя σ_1, σ_2 и σ_3 их выражениями, мы получим:

$$\sigma_1\sigma_2 + 2\sigma_3 = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2 + 5x_1x_2x_3;$$

справа стоит, очевидно, симметрический многочлен от x_1, x_2, x_3 .

Обращением этого результата является следующая основная теорема о симметрических многочленах:

Всякий симметрический многочлен от неизвестных x_1, x_2, \dots, x_n над полем P является многочленом от элементарных симметрических многочленов $\sigma_1, \sigma_2, \dots, \sigma_n$ с коэффициентами, принадлежащими к полю P .

Пусть, в самом деле, дан симметрический многочлен

$$f(x_1, x_2, \dots, x_n)$$

и пусть в его лексикографической записи высшим будет член

$$a_0 x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}. \quad (2)$$

Показатели при неизвестных в этом члене должны удовлетворять неравенствам

$$k_1 \geq k_2 \geq \dots \geq k_n. \quad (3)$$

Действительно, пусть при некотором i будет $k_i < k_{i+1}$. Многочлен $f(x_1, x_2, \dots, x_n)$, будучи симметрическим, должен содержать, однако, член

$$a_0 x_1^{k_1} x_2^{k_2} \dots x_i^{k_{i+1}} x_{i+1}^{k_i} \dots x_n^{k_n}, \quad (4)$$

получающийся из члена (2) транспозицией неизвестных x_i и x_{i+1} . Это приводит нас к противоречию, так как член (4) в смысле лексикографического расположения выше члена (2): показатели при x_1, x_2, \dots, x_{i-1} в обоих членах совпадают, но показатель при x_i в члене (4) больше, чем в члене (2).

Возьмем теперь следующее произведение элементарных симметрических многочленов (ввиду неравенств (3) все показатели будут неотрицательными):

$$\varphi_1 = a_0 \sigma_1^{k_1-k_2} \sigma_2^{k_2-k_3} \dots \sigma_{n-1}^{k_{n-1}-k_n} \sigma_n^{k_n}. \quad (5)$$

Это будет симметрический многочлен от неизвестных x_1, x_2, \dots, x_n , причем его высший член равен члену (2). Действительно, высшие члены многочленов $\sigma_1, \sigma_2, \sigma_3, \dots, \sigma_n$ равны соответственно $x_1, x_1x_2, x_1x_2x_3, \dots, x_1x_2 \dots x_n$, а так как в конце предыдущего параграфа доказано, что высший член произведения равен произведению высших членов сомножителей, то высшим членом многочлена φ_1 будет $a_0 x_1^{k_1-k_2} (x_1x_2)^{k_2-k_3} (x_1x_2x_3)^{k_3-k_4} \dots$

$$\dots (x_1x_2 \dots x_{n-1})^{k_{n-1}-k_n} (x_1x_2 \dots x_n)^{k_n} = a_0 x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}.$$

Отсюда следует, что при вычитании φ_1 из f высшие члены этих многочленов взаимно уничтожаются, т. е. высший член симметрического многочлена $f - \varphi_1 = f_1$ будет ниже члена (2), высшего в многочлене f . Повторяя для многочлена f_1 , коэффициенты которого принадлежат, очевидно, к полю P , этот же прием, мы придем к равенству

$$f_1 = \varphi_2 + f_2,$$

где φ_2 есть произведение степеней элементарных симметрических многочленов с некоторым коэффициентом из поля P , а f_2 — симметрический многочлен, высший член которого ниже, чем высший член в f_1 . Отсюда вытекает равенство

$$f = \varphi_1 + \varphi_2 + f_2.$$

Продолжая этот процесс, мы для некоторого s получим $f_s = 0$ и поэтому придем к выражению для f в виде многочлена от $\sigma_1, \sigma_2, \dots, \sigma_n$ с коэффициентами из P :

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^s \varphi_i = \varphi(\sigma_1, \sigma_2, \dots, \sigma_n).$$

В самом деле, если бы этот процесс был бесконечным¹⁾, то мы получили бы бесконечную последовательность симметрических многочленов

$$f_1, f_2, \dots, f_s, \dots, \quad (6)$$

¹⁾ Следует учесть, что многочлен φ_s содержит, вообще говоря, и такие члены, каких нет в многочлене f_{s-1} , и поэтому переход от f_{s-1} к $f_s = f_{s-1} - \varphi_s$ связан не только с уничтожением некоторых членов из f_{s-1} , но и с появлением новых членов. Здесь $s=1, 2, \dots$

причем высший член каждого из них был бы ниже, чем высшие члены предшествующих многочленов, и тем более ниже, чем (2). Однако, если

$$bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n} \quad (7)$$

есть высший член многочлена f_s , то из симметричности этого многочлена следуют неравенства

$$l_1 \geq l_2 \geq \dots \geq l_n, \quad (8)$$

подобные неравенствам (3). С другой стороны, так как член (2) выше члена (7), то

$$k_1 \geq l_1. \quad (9)$$

Легко видеть, однако, что системы целых неотрицательных чисел l_1, l_2, \dots, l_n удовлетворяющих неравенствам (8) и (9), можно выбрать лишь конечным числом способов. Действительно, если даже отказаться от требования (8) и лишь предполагать, что все $l_i, i = 1, 2, \dots, n$, не больше k_1 , то все равно выбор чисел l_i будет возможен лишь $(k_1 + 1)^n$ способами. Отсюда следует, что последовательность многочленов (6) со строго поникающимися высшими членами не может быть бесконечной.

Доказательство теоремы закончено.

Отмеченная выше связь элементарных симметрических многочленов с формулами Вьета позволяет вывести такое важное следствие из основной теоремы о симметрических многочленах:

Пусть $f(x)$ есть многочлен от одного неизвестного над полем P , имеющий старшим коэффициентом единицу. Тогда всякий симметрический многочлен (с коэффициентами из P) от корней многочлена $f(x)$, принадлежащих к некоторому полю разложения многочлена $f(x)$ над P , будет многочленом (с коэффициентами из P) от коэффициентов многочлена $f(x)$ и поэтому будет элементом поля P .

Изложенное выше доказательство основной теоремы дает заодно и метод для практического разыскания выражений симметрических многочленов через элементарные. Предварительно введем следующее обозначение: если

$$ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n} \quad (10)$$

есть некоторое произведение степеней неизвестных x_1, x_2, \dots, x_n (причем среди показателей могут быть и равные нулю), то через

$$S(ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}) \quad (11)$$

будет обозначаться сумма всех членов, получающихся из (10) при всевозможных перестановках неизвестных. Очевидно, что это будет симметрический многочлен, притом однородный, и что всякий симметрический многочлен от n неизвестных, содержащий член (10), будет содержать и все остальные члены многочлена (11). Например, $S(x_1) = \sigma_1$, $S(x_1x_2) = \sigma_2$, $S(x_1^2)$ есть сумма квадратов всех неизвестных и т. д.

Пример. Симметрический многочлен $f = S(x_1^2 x_2)$ от n неизвестных выразить через элементарные симметрические многочлены.

Здесь высший член $x_1^2 x_2$ и поэтому $\varphi_1 = \sigma_1^{2-1} \sigma_2 = \sigma_1 \sigma_2$, т. е.

$$\begin{aligned}\varphi_1 &= (x_1 + x_2 + \dots + x_n)(x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n) = \\ &= S(x_1^2 x_2) + 3S(x_1 x_2 x_3),\end{aligned}$$

откуда

$$f_1 = f - \varphi_1 = -3S(x_1 x_2 x_3) = -3\sigma_3.$$

Поэтому $f = \varphi_1 + f_1 = \sigma_1 \sigma_2 - 3\sigma_3$.

В более сложных примерах целесообразнее предварительно установить, какие члены могут войти в выражение данного многочлена через элементарные, а затем найти коэффициенты этих членов методом неопределенных коэффициентов.

Примеры. 1. Найти выражение для симметрического многочлена $f = S(x_1^2 x_2^2)$.

Мы знаем (см. доказательство основной теоремы), что члены искомого многочлена $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ определяются через высшие члены симметрических многочленов f_1, f_2, \dots , причем эти высшие члены ниже высшего члена данного многочлена f , т. е. ниже $x_1^2 x_2^2$. Найдем все произведения $x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$, удовлетворяющие следующим условиям: 1) они ниже члена $x_1^2 x_2^2$, 2) они могут служить высшими членами симметрических многочленов, т. е. удовлетворяют неравенствам $l_1 \geq l_2 \geq \dots \geq l_n$, 3) по совокупности неизвестных они имеют степень 4 (так как все многочлены f_1, f_2, \dots имеют, как мы знаем, ту же степень, что и однородный многочлен f). Выписывая лишь соответствующие комбинации показателей и указывая рядом те произведения степеней σ , которые ими определяются, мы получаем следующую таблицу:

$$\begin{aligned}22000. . . \sigma_1^{2-2} \sigma_2^{2-0} &= \sigma_2^2, \\ 21100. . . \sigma_1^{2-1} \sigma_2^{1-1} \sigma_3^{1-0} &= \sigma_1 \sigma_3, \\ 11110. . . \sigma_1^{1-1} \sigma_2^{1-1} \sigma_3^{1-1} \sigma_4^{1-0} &= \sigma_4.\end{aligned}$$

Таким образом, многочлен f имеет вид

$$f = \sigma_2^2 + A\sigma_1\sigma_3 + B\sigma_4.$$

Коэффициент при σ_2 мы положили равным единице, так как этот член определен высшим членом многочлена f и имеет, как мы знаем из доказательства основной теоремы, такой же коэффициент. Коэффициенты A и B мы найдем следующим образом.

Положим $x_1 = x_2 = x_3 = 1$, $x_4 = \dots = x_n = 0$. Легко видеть, что при этих значениях неизвестных многочлен f получает значение 3, а многочлены $\sigma_1, \sigma_2, \sigma_3$ и σ_4 — соответственно значения 3, 3, 1 и 0. Поэтому

$$3 = 9 + A \cdot 3 \cdot 1 + B \cdot 0,$$

откуда $A = -2$. Положим теперь $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = \dots = x_n = 0$. Значения многочленов $f, \sigma_1, \sigma_2, \sigma_3$ и σ_4 будут равны соответственно 6, 4, 6, 4, 1. Поэтому

$$6 = 36 - 2 \cdot 4 \cdot 4 + B \cdot 1,$$

откуда $B = 2$. Таким образом, искомое выражение для f будет

$$f = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4.$$

2. Найти сумму кубов корней многочлена

$$f(x) = x^4 + x^3 + 2x^2 + x + 1.$$

Для решения этой задачи найдем выражение через элементарные симметрические многочлены для симметрического многочлена $S(x_1^3)$. Применяя тот же метод, как и в предыдущем примере, мы получим таблицу

$$3000 \dots \sigma_1^3,$$

$$2100 \dots \sigma_1\sigma_2,$$

$$1110 \dots \sigma_3,$$

а поэтому

$$S(x_1^3) = \sigma_1^3 + A\sigma_1\sigma_2 + B\sigma_3.$$

Полагая сперва $x_1 = x_2 = 1$, $x_3 = \dots = x_n = 0$, а затем $x_1 = x_2 = x_3 = 1$, $x_4 = \dots = x_n = 0$, мы получим $A = -3$, $B = 3$, т. е.

$$S(x_1^3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \quad (12)$$

Для нахождения суммы кубов корней данного нам многочлена $f(x)$ нужно, ввиду формул Вьета, в найденном выше выражении заменить σ_1 через коэффициент при x^3 с обратным знаком, т. е. через -1 , заменить σ_2 через коэффициент при x^2 , т. е. через 2 , и, наконец, заменить σ_3 через коэффициент при x с обратным знаком, т. е. через -1 . Таким образом, интересующая нас сумма кубов корней равна

$$(-1)^3 - 3 \cdot (-1) \cdot 2 + 3 \cdot (-1) = 2.$$

Читатель может проверить этот результат, если учитет, что $f(x)$ имеет корнями числа i , $-i$, $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ и $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$. Очевидно также, что формула (12) не зависит от заданного многочлена $f(x)$ и позволяет находить сумму кубов корней любого многочлена.

Метод для выражения симметрического многочлена f через элементарные, полученный при доказательстве основной теоремы, приводит к вполне определенному многочлену от $\sigma_1, \sigma_2, \dots, \sigma_n$. Оказывается, что никаким способом нельзя получить для f иного выражения через $\sigma_1, \sigma_2, \dots, \sigma_n$. Это показывает следующая теорема единственности:

Всякий симметрический многочлен обладает лишь единственным выражением в виде многочлена от элементарных симметрических многочленов.

Докажем эту теорему. Если бы симметрический многочлен $f(x_1, x_2, \dots, x_n)$ на поле P обладал двумя различными выражениями через $\sigma_1, \sigma_2, \dots, \sigma_n$:

$$f(x_1, x_2, \dots, x_n) = \Phi(\sigma_1, \sigma_2, \dots, \sigma_n) = \Psi(\sigma_1, \sigma_2, \dots, \sigma_n),$$

то разность

$$\chi(\sigma_1, \sigma_2, \dots, \sigma_n) = \Phi(\sigma_1, \sigma_2, \dots, \sigma_n) - \Psi(\sigma_1, \sigma_2, \dots, \sigma_n)$$

была бы отличным от нуля многочленом от $\sigma_1, \sigma_2, \dots, \sigma_n$, т. е. не все его коэффициенты были бы равны нулю, в то время как замена в этом многочлене $\sigma_1, \sigma_2, \dots, \sigma_n$ их выражениями через x_1, x_2, \dots, x_n приводила бы к нулю кольца $P[x_1, x_2, \dots, x_n]$. Нам остается поэтому доказать, что если многочлен $\chi(\sigma_1, \sigma_2, \dots, \sigma_n)$ отличен от нуля, т. е. обладает хотя бы одним отличным от нуля коэффициентом, то и многочлен $g(x_1, x_2, \dots, x_n)$, полученный из χ заменой $\sigma_1, \sigma_2, \dots, \sigma_n$ их выражениями через x_1, x_2, \dots, x_n :

$$\chi(\sigma_1, \sigma_2, \dots, \sigma_n) = g(x_1, x_2, \dots, x_n), \quad (13)$$

также отличен от нуля.

Если $a\sigma_1^{k_1}\sigma_2^{k_2} \dots \sigma_n^{k_n}$ — один из членов многочлена χ , причем $a \neq 0$, то после замены всех σ их выражениями (1) мы получим многочлен от x_1, x_2, \dots, x_n , высшим членом которого (в смысле лексикографического расположения) будет, как мы уже знаем из доказательства основной теоремы, член

$$ax_1^{l_1}(x_1x_2)^{k_2} \dots (x_1x_2 \dots x_n)^{k_n} = ax_1^{l_1}x_2^{l_2} \dots x_n^{l_n},$$

где

$$\begin{aligned} l_1 &= k_1 + k_2 + \dots + k_n, \\ l_2 &= \quad k_2 + \dots + k_n, \\ &\vdots \\ l_n &= \quad k_n. \end{aligned}$$

Отсюда

$$k_i = l_i - l_{i+1}, \quad k_n = l_n, \quad i = 1, 2, \dots, n-1,$$

т. е. по показателям l_1, l_2, \dots, l_n можно восстановить показатели k_1, k_2, \dots, k_n исходного члена многочлена χ . Таким образом, различные члены многочлена χ , рассматриваемые как многочлены от x_1, x_2, \dots, x_n , обладают различными высшими членами.

Рассмотрим теперь все члены многочлена χ ; для каждого из них найдем высший член его представления в виде многочлена от x_1, x_2, \dots, x_n и отберем тот из этих высших членов, который будет наивысшим в смысле лексикографического расположения. Как сказано выше, этот член не имеет подобных среди высших членов, получающихся из других членов многочлена χ , а так как он, по условию, выше каждого из этих высших членов, то тем более он выше других членов, получающихся при замене в членах многочлена χ элементов $\sigma_1, \sigma_2, \dots, \sigma_n$ их выражениями (1). Мы нашли, следовательно, такой член, который при переходе от $\chi(\sigma_1, \sigma_2, \dots, \sigma_n)$ к $g(x_1, x_2, \dots, x_n)$ появляется (с отличным от нуля коэффициентом) только один раз и поэтому ни с чем не может сократиться. Отсюда следует, что не все коэффициенты многочлена $g(x_1, x_2, \dots, x_n)$ равны нулю, т. е. этот многочлен не является нулем кольца $P[x_1, x_2, \dots, x_n]$, что и требовалось доказать.

Доказанную теорему можно также, очевидно, сформулировать следующим образом:

Система элементарных симметрических многочленов $\sigma_1, \sigma_2, \dots, \sigma_n$, рассматриваемых как элементы кольца многочленов $P[x_1, x_2, \dots, x_n]$, алгебраически независима над полем P .

§ 53*. Дополнительные замечания о симметрических многочленах

Замечания к основной теореме. Доказательство основной теоремы о симметрических многочленах, проведенное в предшествующем параграфе, позволяет сделать несколько существенных добавлений к формулировке теоремы, которыми мы ниже воспользуемся. Прежде всего, коэффициенты того многочлена $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$, который найден нами в качестве выражения для симметрического многочлена $f(x_1, x_2, \dots, x_n)$ через элементарные симметрические многочлены, не только принадлежат к полю P , но даже выражаются через коэффициенты многочлена f при помощи сложения и вычитания, т. е. принадлежат к кольцу L , порождаемому коэффициентами многочлена f внутри поля P .

В самом деле, все коэффициенты многочлена φ_1 (см. формулу (5) предшествующего параграфа) относительно неизвестных x_1, x_2, \dots, x_n суть, как легко видеть, целые кратные от коэффициента a_0 при высшем члене многочлена f и поэтому принадлежат к кольцу L . Пусть уже доказано, что к L принадлежат все коэффициенты (относительно x_1, x_2, \dots, x_n) многочленов $\varPhi_1, \varPhi_2, \dots, \varPhi_t$. Тогда коэффициенты многочлена $f_1 = f - \varPhi_1 - \varPhi_2 - \dots - \varPhi_t$ также будут принадлежать к L , а поэтому в L лежат и все коэффициенты многочлена \varPhi_{t+1} относительно x_1, x_2, \dots, x_n .

С другой стороны, степень многочлена $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ по совокупности $\sigma_1, \sigma_2, \dots, \sigma_n$ равна степени, которую имеет многочлен $f(x_1, x_2, \dots, x_n)$ по каждому из неизвестных x_i . В самом деле, так как (2) из предшествующего параграфа есть высший член многочлена f , то k_1 будет степенью f относительно неизвестного x_1 , а поэтому, ввиду симметричности, и относительно любого другого из неизвестных x_i . Однако степень \varPhi_1 по совокупности σ равна, по (5) из предшествующего параграфа, числу

$$(k_1 - k_2) + (k_2 - k_3) + \dots + (k_{n-1} - k_n) + k_n = k_1.$$

Далее, так как старший член многочлена f_1 ниже старшего члена многочлена f , то степень f_1 по каждому из x_i будет не выше чем степень f по каждому из этих неизвестных. Однако многочлен \varPhi_2 играет для f_1 такую же роль, как \varPhi_1 для f , поэтому степень \varPhi_2 по совокупности σ равна степени f_1 по каждому из x_i , т. е. она не больше чем k_1 и т. д. Таким образом, и степень $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ не выше чем k_1 . Поскольку же никакое \varPhi_i с $i > 1$ не может содер-

жать все $\sigma_1, \sigma_2, \dots, \sigma_n$ в тех же степенях, что и φ_1 , то степень $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ в точности равна k_1 . Тем самым наше утверждение доказано.

Наконец, пусть $a\sigma_1^{l_1}\sigma_2^{l_2}\dots\sigma_n^{l_n}$ будет один из членов многочлена $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$. Назовем *весом* этого члена число

$$l_1 + 2l_2 + \dots + nl_n,$$

т. е. сумму показателей, умноженных на индексы соответствующих σ_i . Это будет, иными словами, степень взятого нами члена по совокупности неизвестных x_1, x_2, \dots, x_n , как вытекает из доказанной в § 51 теоремы о степени произведения многочленов. Тогда справедливо следующее утверждение:

Если однородный симметрический многочлен $f(x_1, x_2, \dots, x_n)$ имеет по совокупности неизвестных степень s , то все члены его выражения $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ через σ будут одного и того же веса, равного s .

Действительно, если (2) из предшествующего параграфа есть высший член однородного многочлена f , то

$$s = k_1 + k_2 + \dots + k_n.$$

Однако вес члена φ_1 равен, по (5) из предшествующего параграфа,

$$(k_1 - k_2) + 2(k_2 - k_3) + \dots + (n-1)(k_{n-1} - k_n) + nk_n = \\ = k_1 + k_2 + k_3 + \dots + k_n,$$

т. е. также равен s . Далее, многочлен $f_1 = f - \varphi_1$ как разность двух однородных многочленов степени s сам будет однородным степени s , а поэтому и член φ_2 многочлена φ будет веса s и т. д.

Симметрические рациональные дроби. Основная теорема о симметрических многочленах может быть распространена на случай рациональных дробей. Назовем рациональную дробь $\frac{f}{g}$ от n неизвестных x_1, x_2, \dots, x_n *симметрической*, если она остается равной самой себе при любой перестановке неизвестных. Легко показать, что это определение не зависит от того, берем ли мы дробь $\frac{f}{g}$ или равную ей дробь $\frac{f_0}{g_0}$. Действительно, если ω есть некоторая перестановка наших неизвестных, а φ — произвольный многочлен от этих неизвестных, то условимся через φ^ω обозначать тот многочлен, в который переводится φ перестановкой ω . По предположению, при любом ω

$$\frac{f}{g} = \frac{f^\omega}{g^\omega},$$

т. е. $fg^\omega = gf^\omega$. С другой стороны, из

$$\frac{f}{g} = \frac{f_0}{g_0}$$

следует $fg_0 = gf_0$, откуда $f^\omega g_0^\omega = g^\omega f_0^\omega$. Умножая обе части последнего равенства на f , мы получаем:

$$ff^\omega g_0^\omega = fg^\omega f_0^\omega = gf^\omega f_0^\omega,$$

откуда после сокращения на f^ω следует: $fg_0^\omega = gf_0^\omega$, т. е.

$$\frac{f_0^\omega}{g_0^\omega} = \frac{f}{g} = \frac{f_0}{g_0}.$$

Справедлива следующая теорема:

Всякая симметрическая рациональная дробь от неизвестных x_1, x_2, \dots, x_n с коэффициентами из поля P представима в виде рациональной дроби от элементарных симметрических многочленов $\sigma_1, \sigma_2, \dots, \sigma_n$ с коэффициентами, снова принадлежащими к P .

Действительно, пусть дана симметрическая рациональная дробь

$$\frac{f(x_1, x_2, \dots, x_n)}{g(x_1, x_2, \dots, x_n)}.$$

Предполагая ее несократимой, можно было бы доказать, что и f и g будут симметрическими многочленами. Следующий путь будет, однако, более простым. Если многочлен g не является симметрическим, то умножаем числитель и знаменатель на произведение всех $n! - 1$ многочленов, получающихся из g при всевозможных нетождественных подстановках неизвестных. Легко проверить, что знаменатель будет теперь симметрическим многочленом. Ввиду симметричности всей дроби отсюда следует, что числитель теперь также будет симметрическим, а поэтому для доказательства теоремы остается выразить числитель и знаменатель через элементарные симметрические многочлены.

Степенные суммы. В приложениях часто встречаются симметрические многочлены

$$s_k = x_1^k + x_2^k + \dots + x_n^k, \quad k = 1, 2, \dots,$$

т. е. суммы k -х степеней неизвестных x_1, x_2, \dots, x_n . Эти многочлены, называемые *степенными суммами*, должны выражаться, по основной теореме, через элементарные симметрические многочлены. Разыскание этих выражений является, однако, при больших k весьма затруднительным, и поэтому представляет интерес та связь между многочленами s_1, s_2, \dots и $\sigma_1, \sigma_2, \dots, \sigma_n$, которая будет сейчас установлена.

Прежде всего $s_1 = \sigma_1$. Далее, если $k \leq n$, то легко проверить справедливость равенств

$$\left. \begin{aligned} s_{k-1}\sigma_1 &= s_k + S(x_1^{k-1}x_2)^1, \\ s_{k-2}\sigma_2 &= S(x_1^{k-1}x_2) + S(x_1^{k-2}x_2x_3), \\ &\dots \\ s_{k-i}\sigma_i &= S(x_1^{k-i+1}x_2 \dots x_i) + S(x_1^{k-i}x_2 \dots x_i x_{i+1}), \\ &\quad 2 \leq i \leq k-2, \\ &\dots \\ s_1\sigma_{k-1} &= S(x_1^2 x_2 \dots x_{k-1}) + k\sigma_k. \end{aligned} \right\} \quad (1)$$

Беря альтернирующую сумму этих равенств (т. е. сумму с чередующимися знаками), а затем перенося все члены в одну часть равенства, мы получим следующую формулу:

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^kk\sigma_k = 0 \quad (2) \quad (k \leq n).$$

Если же $k > n$, то система равенств (1) примет вид

$$\left. \begin{aligned} s_{k-1}\sigma_1 &= s_k + S(x_1^{k-1}x_2), \\ s_{k-2}\sigma_2 &= S(x_1^{k-1}x_2) + S(x_1^{k-2}x_2x_3), \\ &\dots \\ s_{k-i}\sigma_i &= S(x_1^{k-i+1}x_2 \dots x_i) + S(x_1^{k-i}x_2 \dots x_i x_{i+1}), \quad 2 \leq i \leq n-1, \\ &\dots \\ s_{k-n}\sigma_n &= S(x_1^{k-n+1}x_2 \dots x_n), \end{aligned} \right.$$

откуда вытекает формула

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^n s_{k-n}\sigma_n = 0 \quad (k > n). \quad (3)$$

Формулы (2) и (3) называются *формулами Ньютона*. Они связывают степенные суммы с элементарными симметрическими многочленами и позволяют последовательно находить выражения для s_1, s_2, s_3, \dots через $\sigma_1, \sigma_2, \dots, \sigma_n$. Так, мы знаем, что $s_1 = \sigma_1$, что вытекает и из формулы (2). Если, далее, $k = 2 \leq n$, то, по (2), $s_2 - s_1\sigma_1 + 2\sigma_2 = 0$, откуда

$$s_2 = \sigma_1^2 - 2\sigma_2.$$

Далее, при $k = 3 \leq n$ будет $s_3 - s_2\sigma_1 + s_1\sigma_2 - 3\sigma_3 = 0$, откуда, используя найденные уже выражения для s_1 и s_2 , получаем:

$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3,$$

¹⁾ См. (11) предшествующего параграфа.

что нам уже известно (см. (12) из предшествующего параграфа). Если же $k=3$, но $n=2$, то, по (3), $s_3-s_2\sigma_1+s_1\sigma_2=0$, откуда $s_3=\sigma_1^3-3\sigma_1\sigma_2$. Пользуясь формулами Ньютона, можно получить общую формулу, выражающую s_k через $\sigma_1, \sigma_2, \dots, \sigma_n$. Эта формула, впрочем, весьма громоздка и мы не будем ее приводить.

Если основное поле P имеет характеристику 0 и поэтому деление на любое натуральное число n имеет смысл¹⁾, то формула (2) дает возможность последовательно выразить элементарные симметрические многочлены $\sigma_1, \sigma_2, \dots, \sigma_n$ через первые n степенных сумм s_1, s_2, \dots, s_n . Так, $\sigma_1=s_1$, а поэтому

$$\sigma_2 = \frac{1}{2} (s_1\sigma_1 - s_2) = \frac{1}{2} (s_1^2 - s_2),$$

$$\sigma_3 = \frac{1}{3} (s_3 - s_2\sigma_1 + s_1\sigma_2) = \frac{1}{6} (s_1^3 - 3s_1s_2 + 2s_3)$$

и т. д. Отсюда и из основной теоремы вытекает следующий результат:

Всякий симметрический многочлен от n неизвестных x_1, x_2, \dots, x_n над полем P характеристики нуль представим в виде многочлена от степенных сумм s_1, s_2, \dots, s_n с коэффициентами, принадлежащими к полю P .

Многочлены, симметрические по двум системам неизвестных. В следующем параграфе, а также в § 58 будет использовано одно обобщение понятия симметрического многочлена. Пусть даны две системы неизвестных x_1, x_2, \dots, x_n и y_1, y_2, \dots, y_r , причем их объединение

$$x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_r \quad (4)$$

алгебраически независимо над полем P . Многочлен над полем P $f(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_r)$ называется *симметрическим по двум системам неизвестных*, если он не меняется при любых перестановках неизвестных x_1, x_2, \dots, x_n между собой и неизвестных y_1, y_2, \dots, y_r между собой. Если для элементарных симметрических многочленов от x_1, x_2, \dots, x_n мы сохраним обозначения $\sigma_1, \sigma_2, \dots, \sigma_n$, а элементарные симметрические многочлены от y_1, y_2, \dots, y_r обозначим через $\tau_1, \tau_2, \dots, \tau_r$, то основная теорема обобщается следующим образом.

Всякий многочлен $f(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_r)$ над полем P , симметрический по системам неизвестных x_1, x_2, \dots, x_n и y_1, y_2, \dots, y_r , представим в виде многочлена (с коэффициентами из P) от элементарных симметрических многочленов по этим двум системам неизвестных:

$$f(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_r) = \varPhi(\sigma_1, \sigma_2, \dots, \sigma_n, \tau_1, \tau_2, \dots, \tau_r).$$

¹⁾ В поле характеристики p выражение $\frac{a}{p}$ не имеет смысла при $a \neq 0$, так как в этом поле при любом x будет $px=0$.

В самом деле, многочлен f можно рассматривать как многочлен $\bar{f}(y_1, y_2, \dots, y_r)$ с коэффициентами, являющимися многочленами от x_1, x_2, \dots, x_n . Так как f не меняется при перестановках неизвестных x_1, x_2, \dots, x_n , то коэффициенты многочлена \bar{f} будут симметрическими многочленами от x_1, x_2, \dots, x_n и поэтому, по основной теореме, представимы в виде многочленов (с коэффициентами из P) от $\sigma_1, \sigma_2, \dots, \sigma_n$. С другой стороны, многочлен $\bar{f}(y_1, y_2, \dots, y_r)$, рассматриваемый над полем $P(x_1, x_2, \dots, x_n)$, будет симметрическим относительно y_1, y_2, \dots, y_r и поэтому представим в виде многочлена $\Phi(\tau_1, \tau_2, \dots, \tau_r)$. Коэффициенты многочлена Φ будут, как показано в начале настоящего параграфа, выражаться через коэффициенты многочлена \bar{f} при помощи сложения и вычитания, а поэтому они также будут многочленами от $\sigma_1, \sigma_2, \dots, \sigma_n$. Это приводит, очевидно, к искомому выражению для f через $\sigma_1, \sigma_2, \dots, \sigma_n, \tau_1, \tau_2, \dots, \tau_r$.

Пример. Многочлен

$$\begin{aligned} f(x_1, x_2, x_3, y_1, y_2) = & x_1x_2x_3 - x_1x_2y_1 - x_1x_2y_2 - x_1x_3y_1 - \\ & - x_1x_3y_2 - x_2x_3y_1 - x_2x_3y_2 + x_1y_1y_2 - x_2y_1y_2 + x_3y_1y_2 \end{aligned}$$

симметричен как по неизвестным x_1, x_2, x_3 , так и по неизвестным y_1, y_2 , но не будет симметрическим по всей совокупности пяти неизвестных, как обнаруживается хотя бы при транспозиции неизвестных x_1 и y_1 . Найдем выражение для f через $\sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2$:

$$\begin{aligned} f = & x_1x_2x_3 - (x_1x_2 + x_1x_3 + x_2x_3)y_1 - (x_1x_2 + x_1x_3 + x_2x_3)y_2 + \\ & + (x_1 + x_2 + x_3)y_1y_2 = \sigma_3 - \sigma_2y_1 - \sigma_2y_2 + \sigma_1y_1y_2 = \sigma_3 - \sigma_2\tau_1 + \sigma_1\tau_2. \end{aligned}$$

Доказанная сейчас теорема распространяется, понятно, также на случай трех и большего числа систем неизвестных.

Для многочленов, симметрических по двум системам неизвестных, справедлива также теорема единственности представления через элементарные симметрические многочлены. Иными словами, справедлива следующая теорема:

Объединенная система

$$\sigma_1, \sigma_2, \dots, \sigma_n, \tau_1, \tau_2, \dots, \tau_r$$

элементарных симметрических многочленов от заданных систем неизвестных x_1, x_2, \dots, x_n и y_1, y_2, \dots, y_r алгебраически независима над полем P .

Пусть, в самом деле, существует многочлен

$$\Phi(\sigma_1, \sigma_2, \dots, \sigma_n, \tau_1, \tau_2, \dots, \tau_r)$$

над полем P , равный нулю, хотя не все его коэффициенты нули. Этот многочлен можно рассматривать как многочлен $\Psi(\tau_1, \tau_2, \dots, \tau_r)$ с коэффициентами, являющимися многочленами от $\sigma_1, \sigma_2, \dots, \sigma_n$.

Можно считать, следовательно, что ψ — многочлен от $\tau_1, \tau_2, \dots, \tau_r$ над полем рациональных дробей

$$Q = P(x_1, x_2, \dots, x_n).$$

Система y_1, y_2, \dots, y_r остается алгебраически независимой над полем Q : если бы для этой системы существовала алгебраическая зависимость с коэффициентами из Q , то, освобождаясь от знаменателей, мы получили бы алгебраическую зависимость в системе (4) против предположения. Опираясь на теорему единственности из предыдущего параграфа, мы получаем теперь, что система $\tau_1, \tau_2, \dots, \tau_r$, также должна быть алгебраически независимой над полем Q , а поэтому все коэффициенты многочлена ψ равны нулю. Эти коэффициенты являются, однако, многочленами от $\sigma_1, \sigma_2, \dots, \sigma_n$, а поэтому, снова на основании теоремы единственности для случая одной системы неизвестных (на этот раз системы x_1, x_2, \dots, x_n), все коэффициенты этих последних многочленов сами равны нулю. Этим доказано, что в противоречие с предположением все коэффициенты многочлена ψ должны быть равными нулю.

§ 54*. Результант. Исключение неизвестного. Дискриминант

Если дан многочлен $f(x_1, x_2, \dots, x_n)$ из кольца $P[x_1, x_2, \dots, x_n]$, то его *решением* называется такая система значений для неизвестных

$$x_1 = \alpha_1, \quad x_2 = \alpha_2, \quad \dots, \quad x_n = \alpha_n,$$

взятых в поле P или в некотором расширении \bar{P} этого поля, которая обращает многочлен f в нуль:

$$f(\alpha_1, \alpha_2, \dots, \alpha_n) = 0.$$

Всякий многочлен f , степень которого больше нуля, обладает решениями: если неизвестное x_1 входит в запись этого многочлена, то в качестве $\alpha_2, \dots, \alpha_n$ можно взять по существу произвольные элементы из поля P , лишь бы степень многочлена $f(x_1, \alpha_2, \dots, \alpha_n)$ оставалась строго положительной, а затем, используя теорему о существовании корня (§ 49), взять такое расширение \bar{P} поля P , в котором многочлен $f(x_1, \alpha_2, \dots, \alpha_n)$ от одного неизвестного x_1 обладает корнем α_1 . Мы видим вместе с тем, что свойство многочлена степени n от одного неизвестного обладать во всяком поле не более чем n корнями для многочленов от нескольких неизвестных перестает быть справедливым.

Если дано несколько многочленов от n неизвестных, то можно поставить вопрос о разыскании решений, общих для всех этих многочленов, т. е. решений той системы уравнений, которая получается в результате приравнивания заданных многочленов нулю. Частный случай этой задачи, а именно случай систем линейных уравнений,

уже был подвергнут во второй главе детальному рассмотрению. Однако для противоположного частного случая одного уравнения от одного неизвестного, но имеющего произвольную степень, мы не знаем о корнях ничего, кроме того, что они существуют в некотором расширении основного поля. Разыскание и изучение решений произвольной нелинейной системы уравнений от нескольких неизвестных является, понятно, еще более сложной задачей, выходящей, впрочем, за рамки нашего курса и составляющей предмет особой математической науки — алгебраической геометрии. Мы же здесь ограничимся лишь случаем системы двух уравнений произвольной степени от двух неизвестных и покажем, что этот случай может быть сведен к случаю одного уравнения от одного неизвестного.

Займемся сперва вопросом о существовании общих корней у двух многочленов от одного неизвестного. Пусть даны многочлены

$$\left. \begin{aligned} f(x) &= a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n, \\ g(x) &= b_0 x^s + b_1 x^{s-1} + \dots + b_{s-1} x + b_s \end{aligned} \right\} \quad (1)$$

над полем P , причем $a_0 \neq 0$, $b_0 \neq 0$.

Из результатов предшествующей главы без труда вытекает, что многочлены $f(x)$ и $g(x)$ тогда и только тогда обладают общим корнем в некотором расширении поля P , если они не являются взаимно простыми. Таким образом, вопрос о существовании общих корней у данных многочленов может быть решен применением к ним алгоритма Евклида.

Сейчас мы укажем другой метод для получения ответа на этот вопрос. Пусть \bar{P} будет некоторое такое расширение поля P , в котором $f(x)$ имеет n корней $\alpha_1, \alpha_2, \dots, \alpha_n$, а $g(x)$ имеет s корней $\beta_1, \beta_2, \dots, \beta_s$; в качестве \bar{P} можно взять поле разложения для произведения $f(x)g(x)$. Элемент

$$R(f, g) = a_0^s b_0^n \prod_{i=1}^n \prod_{j=1}^s (\alpha_i - \beta_j) \quad (2)$$

поля \bar{P} называется *результатантом* многочленов $f(x)$ и $g(x)$. Очевидно, что $f(x)$ и $g(x)$ тогда и только тогда обладают в \bar{P} общим корнем, если $R(f, g) = 0$. Так как

$$g(x) = b_0 \prod_{j=1}^s (x - \beta_j)$$

и поэтому

$$g(\alpha_i) = b_0 \prod_{j=1}^s (\alpha_i - \beta_j),$$

то результатант $R(f, g)$ может быть записан также в виде

$$R(f, g) = a_0^s \prod_{i=1}^n g(\alpha_i). \quad (3)$$

Многочлены $f(x)$ и $g(x)$ используются в определении результанта не симметричным образом. Действительно,

$$R(g, f) = b_0^n a_0^s \prod_{j=1}^s \prod_{i=1}^n (\beta_j - \alpha_i) = (-1)^{ns} R(f, g). \quad (4)$$

В соответствии с (3) $R(g, f)$ можно записать в виде

$$R(g, f) = b_0^n \prod_{j=1}^s f(\beta_j). \quad (5)$$

Выражение (2) для результанта требует знания корней многочленов $f(x)$ и $g(x)$ и поэтому практически бесполезно для решения вопроса о существовании у этих двух многочленов общего корня. Оказывается, однако, что *результатант $R(f, g)$ может быть представлен в виде многочлена от коэффициентов $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_s$ многочленов $f(x)$ и $g(x)$.*

Возможность такого представления легко вытекает из результатов предшествующего параграфа. В самом деле, формула (2) показывает, что результант $R(f, g)$ является симметрическим многочленом от двух систем неизвестных: системы $\alpha_1, \alpha_2, \dots, \alpha_n$ и системы $\beta_1, \beta_2, \dots, \beta_s$. Он представим поэтому, как доказано в конце предшествующего параграфа, в виде многочлена от элементарных симметрических многочленов по этим двум системам неизвестных, т. е., ввиду формул Вьета, в виде многочлена от частных $\frac{a_i}{a_0}$, $i = 1, 2, \dots, n$, и $\frac{b_j}{b_0}$, $j = 1, 2, \dots, s$; множитель $a_0^s b_0^n$, включенный в (2), освобождает полученное выражение от a_0 и b_0 в знаменателях. Впрочем, было бы затруднительным разыскивать выражение результанта через коэффициенты при помощи методов, изложенных в предшествующих параграфах, и мы воспользуемся иным приемом.

Выражение для результанта многочленов (1), которое мы найдем, будет годно для любой пары таких многочленов. Мы будем считать, точнее говоря, что система корней

$$\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_s \quad (6)$$

многочленов (1) является системой $n+s$ независимых неизвестных, т. е. системой $n+s$ элементов, алгебраически независимых над полем P в смысле § 51.

Мы получим выражение для результанта, которое, рассматриваемое как многочлен от неизвестных (6) (после замены по формулам Вьета коэффициентов через корни), будет равно правой части равенства (2), также рассматриваемой как многочлен от неизвестных (6).

Понимая равенство именно в смысле такого тождественного равенства относительно системы неизвестных (6), мы докажем, что

результатант $R(f, g)$ многочленов (1) равен следующему определителю порядка $n+s$:

$$D = \begin{vmatrix} a_0 & a_1 & \dots & a_n \\ a_0 & a_1 & \dots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_s \\ b_0 & b_1 & \dots & b_s \\ \vdots & \vdots & \ddots & \vdots \\ b_0 & b_1 & \dots & b_s \end{vmatrix} \left. \begin{array}{l} s \text{ строк} \\ n \text{ строк} \end{array} \right\} \quad (7)$$

(на свободных местах стоят нули). Строение этого определителя достаточно ясно; мы отметим лишь, что на его главной диагонали стоит s раз коэффициент a_0 и затем n раз коэффициент b_s .

Для доказательства нашего утверждения мы двумя способами вычислим произведение $a_0^s b_0^n DM$, где M есть следующий вспомогательный определитель порядка $n+s$:

$$M = \begin{vmatrix} \beta_1^{n+s-1} & \beta_2^{n+s-1} & \dots & \beta_s^{n+s-1} & \alpha_1^{n+s-1} & \alpha_2^{n+s-1} & \dots & \alpha_n^{n+s-1} \\ \beta_1^{n+s-2} & \beta_2^{n+s-2} & \dots & \beta_s^{n+s-2} & \alpha_1^{n+s-2} & \alpha_2^{n+s-2} & \dots & \alpha_n^{n+s-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_1^2 & \beta_2^2 & \dots & \beta_s^2 & \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \beta_1 & \beta_2 & \dots & \beta_s & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \end{vmatrix}.$$

M является определителем Вандермонда и поэтому равен, как указано в § 6, произведению разностей элементов его предпоследней строки, причем из всякого предшествующего элемента вычитается любой следующий элемент. Таким образом,

$$M = \prod_{1 \leq i < j \leq s} (\beta_i - \beta_j) \cdot \prod_{j=1}^s \prod_{i=1}^n (\beta_j - \alpha_i) \cdot \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

и поэтому, виду (4),

$$a_0^s b_0^n DM = D \cdot R(g, f) \cdot \prod_{1 \leq i < j \leq s} (\beta_i - \beta_j) \cdot \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j). \quad (8)$$

Вычислим, с другой стороны, произведение DM на основании теоремы об определителе произведения матриц. Перемножая соответствующие матрицы и учитывая, что все α являются корнями

для $f(x)$, а все β — корнями для $g(x)$, мы получим:

$$DM = \begin{vmatrix} \beta_1^{s-1} f(\beta_1) & \beta_2^{s-1} f(\beta_2) & \dots & \beta_s^{s-1} f(\beta_s) & 0 & 0 & \dots & 0 \\ \beta_1^{s-2} f(\beta_1) & \beta_2^{s-2} f(\beta_2) & \dots & \beta_s^{s-2} f(\beta_s) & 0 & 0 & \dots & 0 \\ \dots & \dots \\ \beta_1 f(\beta_1) & \beta_2 f(\beta_2) & \dots & \beta_s f(\beta_s) & 0 & 0 & \dots & 0 \\ f(\beta_1) & f(\beta_2) & \dots & f(\beta_s) & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \alpha_1^{n-1} g(\alpha_1) & \alpha_2^{n-1} g(\alpha_2) & \dots & \alpha_n^{n-1} g(\alpha_n) \\ 0 & 0 & \dots & 0 & \alpha_1^{n-2} g(\alpha_1) & \alpha_2^{n-2} g(\alpha_2) & \dots & \alpha_n^{n-2} g(\alpha_n) \\ \dots & \dots \\ 0 & 0 & \dots & 0 & \alpha_1 g(\alpha_1) & \alpha_2 g(\alpha_2) & \dots & \alpha_n g(\alpha_n) \\ 0 & 0 & \dots & 0 & g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \end{vmatrix}$$

Применяя теорему Лапласа, вынося затем общие множители из столбцов определителей и вычисляя остающиеся определители как определители Вандермонда, мы получим:

$$a_0^s b_0^n DM = a_0^s b_0^n \prod_{j=1}^s f(\beta_j) \cdot \prod_{1 \leq i < j \leq s} (\beta_i - \beta_j) \cdot \prod_{i=1}^n g(\alpha_i) \cdot \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

или, используя (3) и (5),

$$a_0^s b_0^n DM = R(f, g) R(g, f) \cdot \prod_{1 \leq i < j \leq s} (\beta_i - \beta_j) \cdot \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j). \quad (9)$$

Мы получаем, что правые части равенств (8) и (9), рассматриваемые как многочлены от неизвестных (6), равны между собой. Обе части полученного равенства можно сократить на общие множители, не равные тождественно нулю. Общий множитель $R(g, f)$ не равен нулю: так как $a_0 \neq 0$ и $b_0 \neq 0$ по условию, то достаточно подобрать для неизвестных (6) не равные друг другу значения (в основном поле или в некотором его расширении), чтобы из (4) получить отличное от нуля значение для многочлена $R(g, f)$. Так же доказывается, что и другие два общих множителя отличны от нуля. Сокращая на все эти общие множители, мы приходим к равенству

$$R(f, g) = D, \quad (10)$$

которое и требовалось доказать.

Откажемся теперь от требования, чтобы старшие коэффициенты многочленов (1) были отличны от нуля¹⁾. Об истинных степенях этих многочленов, можно, следова-

¹⁾ Этот временный отказ от того условия о старшем коэффициенте многочлена, которому мы следовали до сих пор, обусловлен дальнейшими приложениями: мы хотим рассматривать системы многочленов от двух неизвестных и будем одно из этих неизвестных относить к коэффициенты. Старший коэффициент может, следовательно, обратиться в нуль при частных значениях этого неизвестного.

тельно, лишь утверждать, что они не больше их «формальных» степеней n и, соответственно, s . Выражение (2) для результанта не имеет теперь смысла, так как рассматриваемые многочлены имеют, возможно, меньше корней, чем n или s . С другой стороны, определитель (7) и теперь может быть написан, и так как уже доказано, что при $a_0 \neq 0$, $b_0 \neq 0$ этот определитель равен результанту, то и в нашем общем случае назовем его *результатом* многочленов $f(x)$ и $g(x)$ и обозначим через $R(f, g)$.

Теперь уже нельзя, однако, рассчитывать на то, что равенство результанта нулю равносильно существованию у наших многочленов общего корня. Действительно, если $a_0 = 0$ и $b_0 = 0$, то $R(f, g) = 0$ независимо от того, обладают ли многочлены f и g общими корнями или нет. Оказывается, однако, что этот случай будет единственным, когда из равенства результанта нулю нельзя вывести заключение о существовании у данных многочленов общих корней¹⁾. Именно, справедлива следующая теорема:

Если даны многочлены (1) с произвольными старшими коэффициентами, то результатант (7) этих многочленов тогда и только тогда равен нулю, если эти многочлены обладают общим корнем или же если их старшие коэффициенты оба равны нулю.

Доказательство. Случай $a_0 \neq 0$, $b_0 \neq 0$ уже рассматривался выше, а случай $a_0 = b_0 = 0$ предусмотрен в формулировке теоремы. Нам остается рассмотреть случай, когда один из старших коэффициентов многочленов (1), например a_0 , отличен от нуля, а b_0 равно нулю.

Если $b_i = 0$ для всех i , $i = 0, 1, \dots, s$, то $R(f, g) = 0$, так как определитель (7) содержит нулевые строки. В этом случае, однако, многочлен $g(x)$ равен нулю тождественно и поэтому имеет общие корни с $f(x)$. Если же

$$b_0 = b_1 = \dots = b_{k-1} = 0, \quad \text{но} \quad b_k \neq 0, \quad k \leqslant s,$$

и если

$$\bar{g}(x) = b_k x^{s-k} + b_{k+1} x^{s-k-1} + \dots + b_{s-1} x + b_s,$$

то, заменяя в определителе (7) элементы b_0, b_1, \dots, b_{k-1} нулями и применяя теорему Лапласа, мы придем, очевидно, к равенству

$$R(f, g) = a_0^k R(f, \bar{g}). \quad (11)$$

Так как, однако, старшие коэффициенты обоих многочленов f и \bar{g} отличны от нуля, то, по доказанному выше, равенство $R(f, \bar{g}) = 0$ необходимо и достаточно для существования общего корня у многочленов f и \bar{g} . С другой стороны, по (11), равенства $R(f, g) = 0$ и $R(f, \bar{g}) = 0$ равносильны, а так как многочлены g и \bar{g} имеют,

¹⁾ Определитель (7) равен нулю, конечно, и при $a_n = b_s = 0$. В этом случае, однако, многочлены (1) имеют общий корень 0.

понятно, одинаковые корни, то мы получаем, что и в рассматриваемом случае равенство нулю результанта $R(f, g)$ равносильно существованию общего корня у многочленов $f(x)$ и $g(x)$. Этим теорема доказана.

Найдем результант двух квадратных многочленов

$$f(x) = a_0x^2 + a_1x + a_2, \quad g(x) = b_0x^2 + b_1x + b_2.$$

По (7)

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix},$$

или, вычисляя определитель разложением по первой и третьей строкам,

$$R(f, g) = (a_0b_2 - a_2b_0)^2 - (a_0b_1 - a_1b_0)(a_1b_2 - a_2b_1). \quad (12)$$

Так, если даны многочлены

$$f(x) = x^2 - 6x + 2, \quad g(x) = x^2 + x + 5,$$

то, по (12), $R(f, g) = 233$, и потому эти многочлены не имеют общих корней. Если же даны многочлены

$$f(x) = x^2 - 4x - 5, \quad g(x) = x^2 - 7x + 10,$$

то $R(f, g) = 0$, т. е. эти многочлены обладают общим корнем; этим корнем является число 5.

Исключение неизвестного из системы двух уравнений с двумя неизвестными. Пусть даны два многочлена f и g от двух неизвестных x и y с коэффициентами из некоторого поля P . Мы запишем эти многочлены по убывающим степеням неизвестного x :

$$\left. \begin{aligned} f(x, y) &= a_0(y)x^k + a_1(y)x^{k-1} + \dots + a_{k-1}(y)x + a_k(y), \\ g(x, y) &= b_0(y)x^l + b_1(y)x^{l-1} + \dots + b_{l-1}(y)x + b_l(y); \end{aligned} \right\} \quad (13)$$

коэффициенты будут многочленами из кольца $P[y]$. Найдем результант многочленов f и g , рассматриваемых как многочлены от x , и обозначим его через $R_x(f, g)$; он будет, ввиду (7), многочленом от одного неизвестного y с коэффициентами из поля P :

$$R_x(f, g) = F(y). \quad (14)$$

Пусть система многочленов (13) обладает в некотором расширении поля P общим решением $x = \alpha$, $y = \beta$. Подставляя в (13) вместо y значение β , мы получим два многочлена $f(x, \beta)$ и $g(x, \beta)$ от одного неизвестного x . Эти многочлены обладают общим корнем α , а поэтому их результант, равный, ввиду (14), $F(\beta)$, должен быть равным нулю, т. е. β должно быть корнем результанта $R_x(f, g)$. Обратно, если результант $R_x(f, g)$ многочленов (13) обладает корнем β , то результант многочленов $f(x, \beta)$ и $g(x, \beta)$ равен нулю, т. е. либо

эти многочлены обладают общим корнем, либо же оба их старших коэффициента равны нулю,

$$a_0(\beta) = b_0(\beta) = 0.$$

Этим путем разыскание общих решений системы многочленов (13) сведено к разысканию корней одного многочлена (14) от одного неизвестного y , т. е., как принято говорить, *неизвестное исключено из системы многочленов* (13).

Следующая теорема отвечает на вопрос о степени того многочлена, который мы получаем после исключения одного неизвестного из системы двух многочленов с двумя неизвестными:

Если многочлены $f(x, y)$ и $g(x, y)$ имеют по совокупности неизвестных соответственно степени n и s , то степень многочлена $R_x(f, g)$ по неизвестному y не больше произведения ns , если, конечно, этот многочлен не равен нулю тождественно.

Прежде всего, если мы рассматриваем два многочлена от одного неизвестного со старшими коэффициентами, равными единице, то, по (2), их результатант $R(f, g)$ является однородным многочленом от $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_s$ степени ns . Отсюда следует, что если в выражение результанта через коэффициенты $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_s$ входит член

$$a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} b_1^{l_1} b_2^{l_2} \cdots b_s^{l_s}$$

и если весом этого члена будет названо число

$$k_1 + 2k_2 + \dots + nk_n + l_1 + 2l_2 + \dots + sl_s,$$

то все члены выражения $R(f, g)$ через коэффициенты имеют один и тот же вес, равный ns . Это утверждение справедливо и в общем случае, для членов результанта (7), если весом члена $a_0^{k_0} a_1^{k_1} \cdots a_n^{k_n} b_0^{l_0} b_1^{l_1} \cdots b_s^{l_s}$ будет названо число

$$0 \cdot k_0 + 1 \cdot k_1 + \dots + nk_n + 0 \cdot l_0 + 1 \cdot l_1 + \dots + sl_s. \quad (15)$$

Действительно, заменяя в членах определителя (7) множители a_0 и b_0 единицей, мы приходим к уже рассмотренному случаю, однако показатели при этих множителях входят в (15) с коэффициентами 0.

Запишем теперь многочлены f и g в следующем виде:

$$\begin{aligned} f(x, y) &= a_0(y)x^n + a_1(y)x^{n-1} + \dots + a_n(y), \\ g(x, y) &= b_0(y)x^s + b_1(y)x^{s-1} + \dots + b_s(y). \end{aligned}$$

Так как n есть степень $f(x, y)$ по совокупности неизвестных, то степень коэффициента $a_r(y)$, $r=0, 1, 2, \dots, n$, не может превосходить его индекс r ; это же верно и для $b_r(y)$. Отсюда следует, что степень каждого члена результанта $R_x(f, g)$ не больше веса этого члена, т. е. она не больше числа ns , что и требовалось доказать.

При м'єры.

1. Найти общие решения системы многочленов

$$f(x, y) = x^2y + 3xy + 2y + 3,$$

$$g(x, y) = 2xy - 2x + 2y + 3.$$

Исключим из этой системы неизвестное x , для чего перепишем ее в виде

$$\left. \begin{array}{l} f(x, y) = y \cdot x^2 + (3y) \cdot x + (2y + 3), \\ g(x, y) = (2y - 2)x + (2y + 3); \end{array} \right\} \quad (16)$$

тогда

$$R_x(f, g) = \begin{vmatrix} y & 3y & 2y + 3 \\ 2y - 2 & 2y + 3 & 0 \\ 0 & 2y - 2 & 2y + 3 \end{vmatrix} = 2y^2 + 11y + 12.$$

Корнями результанта будут числа $\beta_1 = -4$, $\beta_2 = -\frac{3}{2}$. При этих значениях неизвестного y старшие коэффициенты многочленов (16) не обращаются в нуль, поэтому каждое из них вместе с некоторым значением для x составляет решение заданной системы многочленов. Многочлены

$$\begin{aligned} f(x, -4) &= -4x^2 - 12x - 5, \\ g(x, -4) &= -10x - 5 \end{aligned}$$

обладают общим корнем $a_1 = -\frac{1}{2}$. Многочлены

$$\begin{aligned} f\left(x, -\frac{3}{2}\right) &= -\frac{3}{2}x^2 - \frac{9}{2}x, \\ g\left(x, -\frac{3}{2}\right) &= -5x \end{aligned}$$

имеют общий корень $a_2 = 0$. Таким образом, заданная система многочленов имеет два решения:

$$a_1 = -\frac{1}{2}, \quad \beta_1 = -4 \quad \text{и} \quad a_2 = 0, \quad \beta_2 = -\frac{3}{2}.$$

2. Исключить одно неизвестное из системы многочленов

$$\begin{aligned} f(x, y) &= 2x^3y - xy^2 + x + 5, \\ g(x, y) &= x^2y^2 + 2xy^2 - 5y + 1. \end{aligned}$$

Так как оба многочлена имеют по неизвестному y степень 2, тогда как у одного из них по неизвестному x степень 3, то целесообразно исключить y . Перепишем систему в виде

$$\left. \begin{array}{l} f(x, y) = (-x) \cdot y^2 + (2x^3) \cdot y + (x + 5), \\ g(x, y) = (x^2 + 2x) y^2 - 5y + 1 \end{array} \right\} \quad (17)$$

и найдем ее результант, применяя формулу (12):

$$\begin{aligned} R_y(f, g) &= [(-x) \cdot 1 - (x + 5)(x^2 + 2x)]^2 - \\ &- [(-x)(-5) - 2x^3(x^2 + 2x)] [2x^3 \cdot 1 - (x + 5)(-5)] = \\ &= 4x^8 + 8x^7 + 11x^6 + 84x^5 + 161x^4 + 154x^3 + 96x^2 - 125x. \end{aligned}$$

Одним из корней результанта является 0. Однако при этом значении неизвестного x оба старших коэффициента многочленов (17) обращаются в нуль, причем, как легко видеть, многочлены $f(0, y)$ и $g(0, y)$ не имеют общих корней. У нас нет способа найти другие корни результанта. Можно утверждать лишь, что если бы мы их нашли (например, в поле разложения для $R_y(f, g)$), то ни один из них не обращал бы в нуль оба старших коэффициента многочленов (17) и поэтому каждый из этих корней вместе с некоторым значением для y (одним или даже несколькими) составлял бы решение заданной системы многочленов.

Существуют методы, позволяющие последовательно исключать неизвестные и из систем с произвольным числом многочленов и неизвестных. Эти методы, однако, слишком громоздки и поэтому не могут быть включены в наш курс.

Дискриминант. По аналогии с вопросом, который привел нас к понятию результанта, можно поставить вопрос об условиях, при которых многочлен $f(x)$ степени n из кольца $P[x]$ обладает кратными корнями. Пусть

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n, \quad a_0 \neq 0,$$

и пусть в некотором расширении поля P этот многочлен имеет корни $\alpha_1, \alpha_2, \dots, \alpha_n$. Очевидно, что среди этих корней тогда и только тогда будут равные, если равно нулю произведение

$$\begin{aligned} \Delta &= (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1) \dots (\alpha_n - \alpha_1) \times \\ &\quad \times (\alpha_3 - \alpha_2)(\alpha_4 - \alpha_2) \dots (\alpha_n - \alpha_2) \times \\ &\quad \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \\ &\quad \times (\alpha_n - \alpha_{n-1}) = \prod_{n \geq i > j \geq 1} (\alpha_i - \alpha_j) \end{aligned}$$

или, что же, если равно нулю произведение

$$D = a_0^{2n-2} \prod_{n > i > j > 1} (\alpha_i - \alpha_j)^2,$$

называемое *дискриминантом* многочлена $f(x)$.

В отличие от произведения Δ ,ющего менять знак при перестановке корней, дискриминант D симметричен относительно $\alpha_1, \alpha_2, \dots, \alpha_n$ и поэтому может быть выражен через коэффициенты многочлена $f(x)$. Для разыскания этого выражения в предположении, что поле P имеет характеристику нуль, можно воспользоваться связью, существующей между дискриминантом многочлена $f(x)$ и результантом этого многочлена и его производной. Наличие такой связи естественно ожидать: мы знаем из § 49, что многочлен тогда и только тогда обладает кратными корнями, если у него есть общие корни с производной $f'(x)$, а поэтому тогда и только тогда $D = 0$, если $R(f, f') = 0$.

По формуле (3) настоящего параграфа

$$R(f, f') = a_0^{n-1} \prod_{i=1}^n f'(\alpha_i).$$

Дифференцируя равенство

$$f(x) = a_0 \prod_{k=1}^n (x - \alpha_k),$$

мы получаем:

$$f'(x) = a_0 \sum_{k=1}^n \prod_{j \neq k} (x - \alpha_j).$$

После подстановки сюда α_i вместо x все слагаемые, кроме i -го, обращаются в нуль и поэтому

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j),$$

откуда

$$R(f, f') = a_0^{n-1} \cdot a_0^n \prod_{i=1}^n \prod_{j \neq i} (\alpha_i - \alpha_j).$$

В это произведение для любых i и j , $i > j$, входят два множителя: $\alpha_i - \alpha_j$ и $\alpha_j - \alpha_i$. Их произведение равно $(-1) \cdot (\alpha_i - \alpha_j)^2$, а так как существует $\frac{n(n-1)}{2}$ пар индексов i, j , удовлетворяющих неравенствам $n \geq i > j \geq 1$, то

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} \prod_{n \geq i > j \geq 1} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_0 D.$$

Пример. Найдем дискриминант квадратного трехчлена

$$f(x) = ax^2 + bx + c.$$

Так как $f'(x) = 2ax + b$, то

$$R(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(-b^2 + 4ac).$$

В нашем случае $\frac{n(n-1)}{2} = 1$ и поэтому

$$D = -a^{-1} R(f, f') = b^2 - 4ac.$$

Это совпадает с тем, что в школьной алгебре называют обычно дискриминантом квадратного уравнения.

Другой способ разыскания дискриминанта состоит в следующем. Составим определитель Вандермонда из степеней корней $\alpha_1, \alpha_2, \dots, \alpha_n$. Как доказано в § 6,

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \dots & \dots & \dots & \dots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} = \prod_{n \geq i > j \geq 1} (\alpha_i - \alpha_j) = \Delta,$$

а поэтому дискриминант равен квадрату этого определителя, умноженному на a_0^{2n-2} . Умножая этот определитель на его транспониро-

ванный по правилу умножения матриц и вспоминая определенные в предыдущем параграфе степенные суммы, мы получим:

$$D = a_0^{2n-2} \begin{vmatrix} n & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix}, \quad (18)$$

где s_k есть сумма k -х степеней корней $\alpha_1, \alpha_2, \dots, \alpha_n$.

Пример. Найдем дискриминант кубического многочлена $f(x) = x^3 + ax^2 + bx + c$. По (18)

$$D = \begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}.$$

Как мы знаем из предыдущего параграфа,

$$s_1 = \sigma_1 = -a,$$

$$s_2 = \sigma_1^2 - 2\sigma_2 = a^2 - 2b,$$

$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = -a^3 + 3ab - 3c.$$

Пользуясь формулой Ньютона, мы найдем также, ввиду $\sigma_4 = 0$, что

$$s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 = a^4 - 4a^2b + 4ac + 2b^2.$$

Отсюда

$$\begin{aligned} D &= 3s_2s_4 + 2s_1s_2s_3 - s_2^3 - s_1^2s_4 - 3s_3^2 = \\ &= a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2. \end{aligned} \quad (19)$$

В частности, при $a = 0$, т. е. для неполного кубического многочлена, мы получаем

$$D = -4b^3 - 27c^2$$

в полном соответствии с тем, что было сказано в § 38.

§ 55*. Второе доказательство основной теоремы алгебры комплексных чисел

Доказательство основной теоремы, приведенное в § 23, было совершенно неалгебраическим. Мы хотим изложить сейчас другое доказательство, использующее большой алгебраический аппарат — так, в нем существенно используется основная теорема о симметрических многочленах (§ 52), а также теорема о существовании поля разложения для всякого многочлена (§ 49), — в то время как неалгебраическая часть этого доказательства является минимальной и сведена к одному весьма простому утверждению.

Заметим сначала, что в § 23 доказана лемма о модуле старшего члена многочлена. Считая коэффициенты многочлена $f(x)$ действи-

тельными и полагая $k=1$, мы получаем из этой леммы такое следствие:

При действительных значениях x , достаточно больших по абсолютной величине, знак многочлена $f(x)$ с действительными коэффициентами совпадает со знаком его старшего члена.

Отсюда вытекает следующий результат:

Многочлен нечетной степени с действительными коэффициентами имеет хотя бы один действительный корень.

В самом деле, пусть

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

причем все коэффициенты действительны. Ввиду нечетности n старший член a_0x^n имеет при положительных и отрицательных значениях x разные знаки, а потому, как доказано выше, при положительных и отрицательных значениях x , достаточно больших по абсолютной величине, многочлен $f(x)$ также будет иметь разные знаки. Существуют, следовательно, такие действительные значения x , например a и b , что

$$f(a) < 0, \quad f(b) > 0.$$

Из курса анализа известно, однако, что многочлен (т. е. целая рациональная функция) $f(x)$ является функцией непрерывной, а поэтому, ввиду одного из основных свойств непрерывных функций, при некоторых действительных значениях x , заключенных между a и b , $f(x)$ принимает любое заданное значение, промежуточное между $f(a)$ и $f(b)$. Существует, в частности, такое α , лежащее между a и b , что $f(\alpha)=0$.

Опираясь на этот результат, мы докажем теперь следующее утверждение:

Всякий многочлен произвольной степени с действительными коэффициентами имеет хотя бы один комплексный корень.

Пусть, в самом деле, дан многочлен $f(x)$ с действительными коэффициентами, имеющий степень $n = 2^k q$, где q — нечетное число. Так как случай $k=0$ уже рассмотрен выше, мы будем полагать $k > 0$, т. е. считать n четным числом, и будем вести доказательство индукцией по k , предполагая, что наше утверждение уже доказано для всех многочленов с действительными коэффициентами, степень которых делится на 2^{k-1} , но не делится на 2^k).

Пусть P будет полем разложения для многочлена $f(x)$ над полем комплексных чисел (см. § 49) и пусть $\alpha_1, \alpha_2, \dots, \alpha_n$ будут корни $f(x)$, содержащиеся в поле P . Выберем произвольное действительное число c и возьмем элементы поля P , имеющие вид

$$\beta_{ij} = \alpha_i \alpha_j + c (\alpha_i + \alpha_j), \quad i < j. \quad (1)$$

¹⁾ Эта степень может, следовательно, быть даже больше n .

Число элементов β_{ij} равно, очевидно,

$$\frac{n(n-1)}{2} = \frac{2^k q (2^k q - 1)}{2} = 2^{k-1} q (2^k q - 1) = 2^{k-1} q', \quad (2)$$

где q' есть нечетное число.

Построим теперь многочлен $g(x)$ из кольца $P[x]$, имеющий свойствами корнями все эти элементы β_{ij} и только их:

$$g(x) = \prod_{i, j, i < j} (x - \beta_{ij}).$$

Коэффициенты этого многочлена являются элементарными симметрическими многочленами от β_{ij} . Они будут, следовательно, ввиду (1), многочленами от $\alpha_1, \alpha_2, \dots, \alpha_n$ с действительными коэффициентами (так как число c действительное), причем даже симметрическими многочленами. В самом деле, транспозиция любых двух α , например α_k и α_l , влечет за собой лишь перестановку в системе всех β_{ij} : всякое β_{kj} , где j отлично от k и от l , превращается в β_{lj} и обратно, в то время как β_{kl} и все β_{ij} при i и j , отличных от k и l , остаются на месте. Однако коэффициенты многочлена $g(x)$ не меняются при перестановке его корней.

Отсюда следует, ввиду основной теоремы о симметрических многочленах, что коэффициенты многочлена $g(x)$ будут многочленами (с действительными коэффициентами) от коэффициентов заданного многочлена $f(x)$ и поэтому сами будут действительными числами. Степень этого многочлена, равная числу корней β_{ij} , делится, по (2), на 2^{k-1} , но не делится на 2^k . Поэтому, по предположению индукции, хотя бы один из корней β_{ij} многочлена $g(x)$ должен быть комплексным числом.

Таким образом, при всяком выборе действительного числа c можно указать такую пару индексов i, j , где $1 \leq i \leq n, 1 \leq j \leq n$, что элемент $\alpha_i \alpha_j + c(\alpha_i + \alpha_j)$ является комплексным числом — напомним, что поле P содержит поле комплексных чисел в качестве подполя. Понятно, что при другом выборе числа c ему будет соответствовать в указанном смысле, вообще говоря, другая пара индексов. Однако существует бесконечно много различных действительных чисел c , в то время как в нашем распоряжении находится лишь конечное число различных пар i, j . Отсюда следует, что можно выбрать такие два различных действительных числа c_1 и c_2 , $c_1 \neq c_2$, что им соответствует одна и та же пара индексов i, j , для которых

$$\left. \begin{aligned} \alpha_i \alpha_j + c_1 (\alpha_i + \alpha_j) &= a, \\ \alpha_i \alpha_j + c_2 (\alpha_i + \alpha_j) &= b \end{aligned} \right\} \quad (3)$$

являются комплексными числами.

Из равенств (3) вытекает:

$$(c_1 - c_2)(\alpha_i + \alpha_j) = a - b,$$

откуда следует:

$$\alpha_i + \alpha_j = \frac{a - b}{c_1 - c_2},$$

т. е. эта сумма оказывается комплексным числом. Отсюда и хотя бы из первого из равенств (3) следует, что произведение $\alpha_i \alpha_j$ также будет комплексным числом. Таким образом, элементы α_i и α_j оказываются корнями квадратного уравнения

$$x^2 - (\alpha_i + \alpha_j)x + \alpha_i \alpha_j = 0$$

с комплексными коэффициентами и поэтому, как вытекает из формулы для решения квадратного уравнения с комплексными коэффициентами, выведенной в § 38, они сами должны быть комплексными числами. Мы нашли, следовательно, среди корней многочлена $f(x)$ даже два комплексных корня и этим доказали наше утверждение.

Для полного доказательства основной теоремы остается рассмотреть случай многочлена с произвольными комплексными коэффициентами. Пусть

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$$

будет такой многочлен. Возьмем многочлен

$$\bar{f}(x) = \bar{a}_0 x^n + \bar{a}_1 x^{n-1} + \dots + \bar{a}_n,$$

полученный из $f(x)$ заменой всех коэффициентов сопряженными комплексными числами, и рассмотрим произведение

$$F(x) = f(x) \bar{f}(x) = b_0 x^{2n} + b_1 x^{2n-1} + \dots + b_k x^{2n-k} + \dots + b_{2n},$$

где, очевидно,

$$b_k = \sum_{i+j=k} a_i \bar{a}_j, \quad k = 0, 1, 2, \dots, 2n.$$

Опираясь на известные нам из § 18 свойства сопряженных комплексных чисел, мы получаем, что

$$\bar{b}_k = \sum_{i+j=k} \bar{a}_i a_j = b_k,$$

т. е. все коэффициенты многочлена $F(x)$ оказываются действительными.

Отсюда, как доказано выше, следует, что многочлен $F(x)$ обладает хотя бы одним комплексным корнем β ,

$$F(\beta) = f(\beta) \bar{f}(\beta) = 0,$$

т. е. или $f(\beta) = 0$, или же $\bar{f}(\bar{\beta}) = 0$. В первом случае теорема доказана. Если же имеет место второй случай, т. е.

$$\bar{a}_0\beta^n + \bar{a}_1\beta^{n-1} + \dots + \bar{a}_n = 0,$$

то, заменяя все входящие сюда комплексные числа им сопряженнымими (что, как мы знаем, не нарушает равенства), мы получим:

$$f(\bar{\beta}) = a_0\bar{\beta}^n + a_1\bar{\beta}^{n-1} + \dots + a_n = 0,$$

т. е. $f(x)$ имеет своим корнем комплексное число $\bar{\beta}$. Доказательство основной теоремы закончено.

ГЛАВА ДВЕНАДЦАТАЯ МНОГОЧЛЕНЫ С РАЦИОНАЛЬНЫМИ КОЭФФИЦИЕНТАМИ

§ 56*. Приводимость многочленов над полем рациональных чисел

Третьим числовым полем, которое наряду с полями действительных и комплексных чисел представляет для нас особый интерес, является поле рациональных чисел; обозначим его через R . Оно является самым малым среди числовых полей: как доказано в § 43, поле R содержится целиком во всяком числовом поле. Мы будем интересоваться сейчас вопросом о приводимости многочленов над полем рациональных чисел, а в следующем параграфе — вопросом о рациональных (целых и дробных) корнях многочленов с рациональными коэффициентами. Еще раз подчеркнем, что это два разных вопроса: многочлен

$$x^4 + 2x^2 + 1 = (x^2 + 1)^2$$

приводим над полем рациональных чисел, хотя не имеет ни одного рационального корня.

Что можно сказать о приводимости многочленов над полем R ? Заметим, прежде всего, что если дан многочлен $f(x)$, коэффициенты которого рациональны, но не все целые, то, приводя коэффициенты к общему знаменателю и умножая $f(x)$ на этот знаменатель, равный, например, k , мы получим многочлен $kf(x)$, все коэффициенты которого будут уже целыми числами. Очевидно, что многочлены $f(x)$ и $kf(x)$ имеют одинаковые корни; с другой стороны, они одновременно будут приводимыми или неприводимыми над полем R .

Мы, однако, пока не получили права ограничиться в дальнейшем рассмотрением многочленов с целыми коэффициентами. В самом деле, пусть целочисленный многочлен $g(x)$ (т. е. многочлен с целыми коэффициентами) приводим над полем рациональных чисел, т. е. разложим на множители меньшей степени с рациональными (вообще говоря, дробными) коэффициентами. Следует ли отсюда разложимость $g(x)$ на множители с целыми коэффициентами? Иными словами, не может ли многочлен с целыми коэффициентами, приводимый над полем рациональных чисел, оказаться неприводимым над кольцом целых чисел?