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?

Ответ на эти вопросы может быть получен при помощи рассмотрений, аналогичных проведенным в § 51. Назовем многочлен $f(x)$ с целыми коэффициентами *примитивным*, если его коэффициенты в совокупности взаимно просты, т. е. не имеют общих делителей, отличных от 1 и —1. Если дан произвольный многочлен $\varphi(x)$ с рациональными коэффициентами, то его можно, притом однозначным образом, представить в виде произведения несократимой дроби на некоторый примитивный многочлен:

$$\varphi(x) = \frac{a}{b} f(x); \tag{1}$$

для этого нужно вынести за скобки общий знаменатель всех коэффициентов многочлена $\varphi(x)$, а затем и общие множители из числителей этих коэффициентов; заметим, что степень $f(x)$ равна степени $\varphi(x)$. Однозначность (с точностью до знака) представления (1) доказывается следующим образом. 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 целочисленного многочлена, а поэтому могут отличаться друг от друга лишь знаком. Отсюда следует, что и примитивные многочлены $f(x)$ и $g(x)$ также могут отличаться друг от друга лишь знаком.

Для целочисленных примитивных многочленов остается справедливой лемма Гаусса:

Произведение двух целочисленных примитивных многочленов само есть примитивный многочлен.

В самом деле, пусть даны примитивные целочисленные многочлены

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

и пусть

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

Если это произведение не примитивно, то существует такое простое число p, которое служит общим делителем для всех коэффициентов $c_0, c_1, \ldots, c_{k+l}$. 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:

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

Левая часть этого равенства делится на 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}, ..., а также b_{j-1}, b_{j-2}, ..., делятся на p. Отсюда следует, что произведение a_ib_j также делится на p, а поэтому, ввиду простоты числа p, на p должен делиться хотя бы один из коэффициентов a_i, b_j, что, однако, не имеет места. Этим заканчивается доказательство леммы.

Переходим к ответу на поставленные выше вопросы. Пусть многочлен $g(x)$ степени n с целыми коэффициентами приводим над полем рациональных чисел:

$$g(x)=\varphi_1(x)\,\varphi_2(x),$$

где $\varphi_1(x)$ и $\varphi_2(x)$ — многочлены с рациональными коэффициентами и их степени меньше n. Тогда

$$\varphi_i(x)=\frac{a_i}{b_i}f_i(x),\quad i=1,\ 2,$$

где $\frac{a_i}{b_i}$ — несократимая дробь, $f_i(x)$ — примитивный многочлен. Отсюда

$$g(x)=\frac{a_1a_2}{b_1b_2}[f_1(x)f_2(x)].$$

Левая часть этого равенства является целочисленным многочленом, поэтому знаменатель b_1b_2 в правой части должен сократиться. Однако многочлен, стоящий в квадратных скобках, будет, по лемме Гаусса, примитивным, поэтому всякий простой множитель из b_1b_2 может сократиться лишь с некоторым простым множителем из a_1a_2, а так как a_i и b_i взаимно просты, $i=1,\ 2$, то число a_2 должно нацело делиться на b_1, a_1 — на b_2;

$$a_2=b_1a_2',\quad a_1=b_2a_1'.$$

Отсюда

$$g(x)=a_1'a_2'f_1(x)f_2(x).$$

Присоединив коэффициент $a_1'a_2'$ к любому из множителей $f_1(x)$, $f_2(x)$, мы получим разложение многочлена $g(x)$ на множители меньшей степени с целыми коэффициентами. Этим доказана следующая теорема:

Многочлен с целыми коэффициентами, неприводимый над кольцом целых чисел, будет неприводимым и над полем рациональных чисел.

Теперь мы получили, наконец, право ограничиваться в вопросах, относящихся к приводимости многочленов над полем рациональных чисел, рассмотрением разложений целочисленных многочленов на множители, все коэффициенты которых также целые.

Мы знаем, что над полем комплексных чисел приводим всякий многочлен, степень которого больше единицы, а над полем действительных чисел — всякий многочлен (с действительными коэффициентами), степень которого больше двух. Совсем иное положение в случае поля рациональных чисел: *для любого n можно указать многочлен n-й степени с рациональными (даже целыми) коэффициентами, неприводимый над полем рациональных чисел.* Доказательство этого утверждения основано на следующем достаточном признаке неприводимости многочлена над полем R, называемом критерием Эйзенштейна:

Пусть дан многочлен

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

с целыми коэффициентами. Если хотя бы одним способом можно подобрать простое число p, удовлетворяющее следующим требованиям:

1) *старший коэффициент a_0 не делится на p,*

2) *все остальные коэффициенты делятся на p,*

3) *свободный член, делясь на p, не делится на p^2,*

то многочлен $f(x)$ неприводим над полем рациональных чисел.

В самом деле, если многочлен $f(x)$ приводим над полем R, то он разлагается на два множителя меньшей степени с целыми коэффициентами:

$$f(x)=(b_0x^k+b_1x^{k-1}+\ldots+b_k)(c_0x^l+c_1x^{l-1}+\ldots+c_l),$$

где $k<n$, $l<n$, $k+l=n$. Отсюда, сравнивая коэффициенты в обеих частях этого равенства, получаем:

$$\left.\begin{aligned} a_n&=b_kc_l,\\ a_{n-1}&=b_kc_{l-1}+b_{k-1}c_l,\\ a_{n-2}&=b_kc_{l-2}+b_{k-1}c_{l-1}+b_{k-2}c_l,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ a_0&=b_0c_0. \end{aligned}\right\} \qquad (2)$$

Из первого из равенств (2) следует, так как a_n делится на p, а число p простое, что один из множителей b_k, c_l должен делиться на p. Они оба не могут одновременно делиться на p, так как a_n, по условию, не делится на p^2. Пусть, например, b_k делится на p и поэтому c_l взаимно просто с p. Переходим теперь ко второму из равенств (2). Его левая часть, а также первое слагаемое правой части делятся на p, поэтому на p делится и произведение $b_{k-1}c_l$;

так как, однако, c_l на p не делится, то на p будет делиться b_{k-1}. Подобным же образом из третьего равенства (2) мы получим, что b_{k-2} делится на p, и т. д. Наконец, из $(k+1)$-го равенства будет получено, что на p делится b_0; но тогда из последнего из равенств (2) вытекает, что на p делится a_0, что противоречит предположению.

Весьма легко для любого n написать целочисленные многочлены n-й степени, удовлетворяющие условиям критерия Эйзенштейна и, следовательно, неприводимые над полем рациональных чисел. Таков, например, многочлен x^n+2; к нему применим критерий Эйзенштейна при $p=2$.

Критерий Эйзенштейна является лишь достаточным условием неприводимости над полем R, но отнюдь не необходимым: если для данного многочлена $f(x)$ нельзя подобрать такого простого числа p, чтобы выполнялись условия критерия Эйзенштейна, то он может быть приводимым, как x^2-5x+6, но может быть и неприводимым, как x^2+1. Существует, помимо критерия Эйзенштейна, много других достаточных критериев неприводимости многочленов над полем R, впрочем менее значительных. Существует также метод, принадлежащий Кронекеру и позволяющий о любом многочлене с целыми коэффициентами решить, приводим ли он над полем R или нет. Этот метод, однако, очень громоздок и практически почти неприменим.

Пример. Рассмотрим многочлен

$$f_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\ldots+x+1,$$

где p — простое число. Корнями этого многочлена служат корни p-й степени из единицы, отличные от самой единицы; так как эти корни вместе с 1 делят единичный круг комплексной плоскости на p равных частей, то многочлен $f_p(x)$ называется *многочленом деления круга*.

К этому многочлену не может быть непосредственно применен критерий Эйзенштейна. Совершим, однако, замену неизвестного, положив $x=y+1$. Мы получим:

$$g(y)=f_p(y+1)=\frac{(y+1)^p-1}{(y+1)-1}=$$
$$=\frac{1}{y}\left[y^p+py^{p-1}+\frac{p(p-1)}{2!}y^{p-2}+\ldots+py\right]=$$
$$=y^{p-1}+py^{p-2}+\frac{p(p-1)}{2!}y^{p-3}+\ldots+p.$$

Коэффициенты многочлена $g(y)$ являются биномиальными коэффициентами и поэтому все, кроме старшего, делятся на p, причем свободный член не делится на p^2. Таким образом, согласно критерию Эйзенштейна многочлен $g(y)$ неприводим над полем R. Отсюда следует *неприводимость над полем R многочлена деления круга* $f_p(x)$. В самом деле, если

$$f_p(x)=\varphi(x)\psi(x),$$

или

$$g(y)=\varphi(y+1)\psi(y+1).$$