§ 12. Неприводимые многочлены

Б.М.Верников

Уральский федеральный университет,
Институт естественных наук и математики,
кафедра алгебры и фундаментальной информатики

12.1. Общие свойства неприводимых многочленов

В арифметике немаловажную роль играет то обстоятельство, что произвольное натуральное число, отличное от 1, можно *разложить на простые множители*, т. е. представить, причем единственным образом, в виде произведения простых чисел. Аналог этого факта имеет место и в теории многочленов. Это находит многочисленные применения как в алгебре, так и за ее пределами (в частности, в математическом анализе).

Определение

Многочлен f над областью целостности R называется *неприводимым* над R, если $\deg f > 0$ и f нельзя представить в виде произведения двух многочленов из $R[x]$, степень каждого из которых меньше степени f.

- В этом параграфе будут рассматриваться только многочлены над полями и кольцом $\mathbb{Z}$. Поэтому использование приведенного определения неприводимых многочленов всегда будет корректно.

Как мы увидим ниже, неприводимые многочлены как раз и являются аналогом простых чисел.

Неприводимые многочлены (замечание)

В дальнейшем мы многократно будем использовать следующее утверждение, как правило, не упоминая его в явном виде.

Замечание 12.1

Если неприводимый многочлен над полем F разложим в произведение двух многочленов, то один из этих многочленов принадлежит F.

Доказательство. Пусть $f \in F[x]$, f неприводим над F и $f = gh$ для некоторых $g, h \in F[x]$. Ясно, что $\deg g, \deg h \leqslant \deg f$. Случай, когда $\deg g, \deg h < \deg f$, невозможен, поскольку f неприводим. Следовательно, степень одного из многочленов g и h равна степени f. Поскольку $\deg f = \deg g + \deg h$, степень другого из них равна 0. Но тогда этот другой многочлен принадлежит F. □

Неприводимые многочлены (свойство)

Предложение 12.1

Если f — неприводимый многочлен над полем F и f делит произведение некоторых многочленов g и h над F, то f делит один из этих двух многочленов.

Доказательство. Обозначим через d наибольший общий делитель многочленов f и g. Тогда $f = dq$ для некоторого многочлена q. В силу неприводимости f, один из многочленов d и q принадлежит F. Если $d \in F$, то d ассоциирован с 1. Следовательно, 1 является наибольшим общим делителем f и g, т. е. эти два многочлена взаимно просты. По условию $f \mid (gh)$. В силу п. 2) предложения 10.1 получаем, что $f \mid h$. Предположим теперь, что $q \in F$. Ясно, что $q \neq o$ (иначе $f = dq = o$), и потому $d = q^{-1}f$. Из определения многочлена d вытекает, что $g = ds$ для некоторого многочлена s. Следовательно, $g = q^{-1}sf$, и потому $f \mid g$. □

Два замечания

Следующее утверждение немедленно вытекает из следствия из теоремы Безу.

Замечание 12.2

Если f — многочлен над полем F, $\deg f > 1$ и f имеет по крайней мере один корень в поле F, то f приводим над F. □

Посмотрим, что можно сказать о неприводимых многочленах малых степеней. Многочлены степени 1 называются *линейными*. Следующее замечание очевидно.

Замечание 12.3

Произвольный линейный многочлен над любым полем неприводим. □

Связь неприводимости с отсутствием корней у многочленов малых степеней (1)

Предложение 12.2

Многочлен $f(x)$ степени 2 или 3 над произвольным полем F неприводим над F тогда и только тогда, когда он не имеет корней в F.

Доказательство. *Необходимость.* Произвольный многочлен степени > 1, который имеет корень, приводим в силу замечания 12.2.

Достаточность. Предположим, что $2 \leqslant \deg f \leqslant 3$ и f приводим над F. Тогда $f = gh$ для некоторых многочленов g и h над F таких, что $\deg g, \deg h < \deg f$. Если степень одного из многочленов g и h равна 0, то степень другого из них равна степени f. Следовательно, $\deg g, \deg h > 0$. Если $\deg g, \deg h > 1$, то $\deg f = \deg g + \deg h \geqslant 4$. Таким образом, хотя бы один из многочленов g и h линеен. Без ограничения общности можно считать, что $\deg g = 1$. Положим $\alpha = \ell c(g)$. Тогда $g = \alpha(x - a)$ для некоторого $a \in F$. Следовательно, $f = \alpha(x - a)h$, и потому a является корнем многочлена f, лежащим в F. □

Связь неприводимости с отсутствием корней у многочленов малых степеней (2)

Следующий пример показывает, что аналог предложения 12.2 для многочленов степени > 3 места не имеет.

Пример 12.1

Многочлен $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ приводим над полями $\mathbb{R}$ и $\mathbb{Q}$, но не имеет действительных (и, в частности, рациональных) корней.

Теорема о разложении многочлена на неприводимые множители (1)

Перейдем к утверждению, упоминавшемуся в начале параграфа.

Теорема 12.1

Всякий ненулевой многочлен f над полем F представим в виде

$$f = \alpha g_1 g_2 \cdots g_n, \tag{1}$$

где $\alpha \in F$, а $g_1, g_2, \ldots, g_n$ — неприводимые над F унитарные многочлены. Это представление единственно с точностью до порядка следования сомножителей в правой части равенства.

Доказательство. *Существование.* Пусть $f \in F[x]$ и $f \neq o$. Докажем, что f представим в виде (1). Если $\deg f = 0$, то f имеет вид (1), где $\alpha = f$, а $n = 0$. Будем далее считать, что $\deg f > 0$. Если f неприводим над F, то он также представим в виде (1), где, на этот раз, $\alpha = \ell c(f)$, $n = 1$ и $g_1 = \alpha^{-1} f$. Пусть, наконец, f приводим, т. е. $f = gh$, где $\deg g, \deg h < \deg f$. В частности, $\deg f = \deg g + \deg h$. Если степень одного из многочленов g и h равна 0, то степень другого из этих многочленов равна $\deg f$ вопреки сказанному выше. Следовательно, $\deg g, \deg h > 0$. Мы доказали, что если многочлен f приводим, то его можно разложить в произведение многочленов g и h, таких, что $0 < \deg g, \deg h < \deg f$.

Теорема о разложении многочлена на неприводимые множители (2)

Если какой-то из многочленов g и h приводим, представим его в виде произведения многочленов, степени которых > 0 и меньше степени этого многочлена. Будем продолжать этот процесс до тех пор, пока среди получаемых многочленов будут встречаться приводимые. Поскольку на каждом шаге степени новых многочленов уменьшаются, через конечное число шагов этот процесс оборвется, и мы представим многочлен f как произведение неприводимых многочленов $h_1, h_2, \ldots, h_n$. Для всякого $i = 1, 2, \ldots, n$ положим $\ell c(h_i) = \alpha_i$ и $g_i = \alpha_i^{-1} h_i$. Пусть $\alpha = \alpha_1 \alpha_2 \cdots \alpha_n$. Тогда выполнено равенство (1), причем $g_1, g_2, \ldots, g_n$ — неприводимые над F унитарные многочлены.

Единственность. Пусть $f = \alpha g_1 \cdots g_n = \beta h_1 \cdots h_m$, где $\alpha, \beta \in F$, а $g_1, \ldots, g_n, h_1, \ldots, h_m$ — неприводимые над F унитарные многочлены. Ясно, что, с одной стороны, $\ell c(f) = \ell c(\alpha g_1 \cdots g_n) = \alpha$, а с другой — $\ell c(f) = \ell c(\beta h_1 \cdots h_m) = \beta$. Отсюда вытекает, что $\alpha = \beta$, и потому $\alpha g_1 \cdots g_n = \alpha h_1 \cdots h_m$. Разделив обе части последнего равенства на α, получим $g_1 \cdots g_n = h_1 \cdots h_m$. Тогда $g_1 \mid (h_1 \cdots h_m)$. В силу предложения 12.1 $g_1 \mid h_i$ для некоторого $1 \leqslant i \leqslant m$. Не ограничивая общности, можно считать, что $i = 1$ (в противном случае можно переставить сомножители в произведении $h_1 \cdots h_m$). Итак, $h_1 = w g_1$ для некоторого многочлена w. Поскольку многочлен g_1 неприводим, $\deg g_1 > 0$, и потому $g_1 \notin F$.

Теорема о разложении многочлена на неприводимые множители (3)

Следовательно, $w \in F$. Поскольку $\ell c(h_1) = w \cdot \ell c(g_1) = w \cdot 1 = w$, получаем, что $w = 1$, и потому $h_1 = g_1$. Без ограничения общности будем считать, что $n \leqslant m$. Если $n = m = 1$, то все доказано. Случай, когда $n = 1$, а $m > 1$, невозможен, так как в этом случае $\deg h_1 \cdots h_m > \deg h_1 = \deg g_1$ вопреки равенству $g_1 = h_1 \cdots h_m$. Пусть теперь $n > 1$. Тогда $g_1 g_2 \cdots g_n = g_1 h_2 \cdots h_m$, откуда $g_1(g_2 \cdots g_n - h_2 \cdots h_m) = o$. Если $g_2 \cdots g_n - h_2 \cdots h_m \neq o$, то $\deg\big(g_1(g_2 \cdots g_n - h_2 \cdots h_m)\big) \geqslant \deg g_1 > 0$ вопреки равенству $g_1(g_2 \cdots g_n - h_2 \cdots h_m) = o$. Следовательно, $g_2 \cdots g_n = h_2 \cdots h_m$.

Рассуждая так же, как в предыдущем абзаце, получаем, что $g_2 = h_2$. Если $m = n = 2$, то все доказано. Случай, когда $n = 2$, а $m > 2$, невозможен, так как в этом случае $\deg h_2 \cdots h_m > \deg h_2 = \deg g_2$ вопреки равенству $g_2 = h_2 \cdots h_m$. Пусть теперь $n > 2$. Тогда $g_2 g_3 \cdots g_n = g_2 h_3 \cdots h_m$, откуда $g_2(g_3 \cdots g_n - h_3 \cdots h_m) = o$. Как и в предыдущем абзаце, отсюда выводится, что $g_3 \cdots g_n = h_3 \cdots h_m$. Продолжая этот процесс, мы в конце концов получим, что $g_i = h_i$ для всех $i = 1, 2, \ldots, n$. Если $n = m$, то все доказано. Если же $n < m$, то $g_1 \cdots g_n = g_1 \cdots g_n h_{n+1} \cdots h_m$. Но это невозможно, так как $\deg(g_1 \cdots g_n h_{n+1} \cdots h_m) > \deg(g_1 \cdots g_n)$. □

Кратность неприводимого множителя

В силу теоремы 12.1 произвольный многочлен f над полем F единственным образом (с точностью до порядка следования сомножителей) представим в виде

$$f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}, \tag{2}$$

где $\alpha \in F$, а $p_1, p_2, \ldots, p_m$ — попарно различные неприводимые над полем F унитарные многочлены.

Определения

Равенство (2) называется *разложением многочлена f на неприводимые множители*, а многочлены $p_1, p_2, \ldots, p_m$ называются *неприводимыми множителями* многочлена f. Число k_i называется *кратностью* неприводимого множителя p_i. Неприводимый множитель p_i называется *кратным*, если $k_i > 1$, и *простым*, если $k_i = 1$. Чтобы упростить рассуждения, нам будет иногда удобно рассматривать неприводимый многочлен, не являющийся неприводимым множителем многочлена f, как неприводимый множитель f *кратности* 0.

Разложение на неприводимые множители и наибольший общий делитель многочленов

Разложение многочленов на неприводимые множители можно использовать для нахождения наибольшего общего делителя двух многочленов. В самом деле, предположим, что $f = \alpha p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ и $g = \beta q_1^{\ell_1} q_2^{\ell_2} \cdots q_m^{\ell_m}$ — разложения многочленов f и g на неприводимые множители. Если f и g не имеют общих неприводимых множителей, т. е. $\{p_1, p_2, \ldots, p_n\} \cap \{q_1, q_2, \ldots, q_m\} = \varnothing$, то многочлены f и g взаимно просты. В противном случае можно без ограничения общности считать, что $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_r = q_r$ для некоторого $1 \leqslant r \leqslant \min\{n, m\}$, причем r — максимальное число с таким свойством. Ясно, что в этом случае наибольшим общим делителем многочленов f и g является многочлен $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, где $a_i = \min\{k_i, \ell_i\}$ для всякого $i = 1, 2, \ldots, r$. Недостатком изложенного способа нахождения наибольшего общего делителя является то обстоятельство, что он не позволяет найти линейную форму наибольшего общего делителя.

Число неприводимых многочленов (1)

Завершая рассмотрение многочленов, неприводимых над произвольным полем, обсудим вопрос о том, сколько существует таких многочленов. Ясно, что если поле F бесконечно, то уже число линейных многочленов над F бесконечно. В силу замечания 12.3 это означает, что и число неприводимых многочленов над бесконечным полем бесконечно. Оказывается, что аналогичное утверждение верно и для конечных полей. Приводимое ниже доказательство этого факта не использует специфики конечных полей и вполне аналогично классическому доказательству бесконечности множества всех простых чисел, которое приписывается Евклиду.

Предложение 12.3

Для любого поля F существует бесконечно много унитарных многочленов, неприводимых над F.

Доказательство. Предположим, что существует поле F такое, что множество унитарных многочленов, неприводимых над F, конечно. Пусть p_1, p_2, …, p_n — все такие многочлены. Рассмотрим многочлен $p = p_1 p_2 \cdots p_n + 1$. Ясно, что он унитарен и отличен от многочленов p_1, p_2, …, p_n. Предположим, что многочлен p приводим. Тогда $p = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ для некоторых $k_1, k_2, \ldots, k_n \in \mathbb{N} \cup \{0\}$, причем $k_i \neq 0$ для некоторого $i \in \{1, 2, \ldots, n\}$.

Число неприводимых многочленов (2)

Ясно, что $p_i \mid p$. Учитывая, что $p_i \mid p_1 p_2 \cdots p_n$ и $p = p_1 p_2 \cdots p_n + 1$, получаем, что $p_i \mid 1$, и потому $\deg p_i \leqslant 0$ вопреки неприводимости многочлена p_i. Следовательно, многочлен p неприводим. Но это противоречит тому, что множество унитарных многочленов, неприводимых над полем F, исчерпывается многочленами p_1, p_2, …, p_n. □

Из предложения 12.3 и того факта, что, для всякого натурального n, число многочленов степени $\leqslant n$ над произвольным конечным полем конечно, вытекает следующее утверждение.

Следствие 12.1

Для любого натурального числа n и любого конечного поля F существует неприводимый над F унитарный многочлен, степень которого $> n$. □

Как мы увидим ниже, для бесконечных полей аналог следствия 12.1 может как выполняться, причем в усиленном варианте (см. следствие 12.3), так и не выполняться (см. предложения 12.5 и 12.6).

12.2. Отделение кратных множителей

Задача разложения произвольного многочлена f на неприводимые множители в общем случае очень сложна. Опишем один из способов упростить ее решение. Пусть (2) — разложение многочлена f на неприводимые множители. Положим $k = \max\{k_1, k_2, \ldots, k_m\}$. Для всякого $i = 1, 2, \ldots, k$ обозначим через d_i произведение всех неприводимых множителей кратности i многочлена f (если f не имеет неприводимых множителей кратности i, полагаем $d_i = 1$). Если $k > 1$ (т. е. если многочлен f имеет по крайней мере один кратный множитель), то степени многочленов $d_1, d_2, \ldots, d_k$ меньше, чем степень f, и потому разложить их на неприводимые множители проще, чем f. Если это сделать, то разложение f на неприводимые множители находится очень просто, поскольку, очевидно, $f = \alpha d_1 d_2^2 \cdots d_k^k$, где $\alpha = \ell c(f)$. Возникает вопрос: как вычислить многочлены $d_1, d_2, \ldots, d_k$, не разлагая f на неприводимые множители? Мы ответим на этот вопрос для многочленов над произвольным полем характеристики 0.

Производная многочлена

Для того, чтобы ответить на поставленный на предыдущем слайде вопрос, нам понадобится следующее понятие.

Определение

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0$ — многочлен над кольцом R. Если $n > 0$, то *производной* многочлена $f(x)$ называется многочлен $n\alpha_n x^{n-1} + (n-1)\alpha_{n-1} x^{n-2} + \cdots + \alpha_1$, обозначаемый через $f'(x)$. Если $n = 0$ или $f(x) = o$, то, по определению, $f'(x) = o$.

- В случае многочленов над полем $\mathbb{R}$ введенное только что понятие производной многочлена совпадает с понятием производной многочлена как функции от одной переменной, известном из математического анализа.

Степень производной многочлена

Следующий пример показывает, что степень производной многочлена степени n не обязательно равна $n-1$.

Пример 12.2

Рассмотрим многочлен $f(x)=x^p$ над полем F характеристики p, где p — произвольное простое число. Тогда $f'(x)=px^{p-1}=o$, поскольку для произвольного $x\in F$ в поле F выполнено равенство $px=0$. Таким образом, $\deg f(x)=p$, но $\deg f'(x)=-\infty$.

Справедливо, однако, следующее утверждение.

Замечание 12.4

Если f — многочлен над полем характеристики 0, а $\deg f>0$, то $\deg f'=\deg f-1$.

Доказательство. Пусть $\ell m(f)=a_nx^n$. В частности, $a_n\neq 0$ и $\deg f=n$. По условию $n>0$. Коэффициент при x^{n-1} в многочлене f' равен na_n. Если $na_n=0$, то, в силу замечания 4.3а), $nx=0$ для всякого $x\in F$. Но это невозможно, так как $\operatorname{char}F=0$. Следовательно, $na_n\neq 0$, и потому $\deg f'=n-1=\deg f-1$. □

Свойства производной многочлена (1)

Укажем некоторые свойства производной многочлена. Для многочленов над полем $\mathbb{R}$ они известны из курса математического анализа, но для многочленов над произвольным кольцом их надо доказывать.

Лемма 12.1

Если $f(x)$ и $g(x)$ — многочлены над кольцом R, $t \in R$, а m — натуральное число такое, что $m > 1$, то:

1) $(tf)' = tf'$,
2) $(f+g)' = f' + g'$,
3) $(fg)' = f'g + fg'$,
4) $(f^m)' = mf^{m-1}f'$.

Доказательство. 1) Пусть $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$. Тогда:

$$\begin{aligned}(tf)' &= (t\alpha_n x^n + t\alpha_{n-1}x^{n-1} + \cdots + t\alpha_1 x + t\alpha_0)' = \\ &= nt\alpha_n x^{n-1} + (n-1)t\alpha_{n-1}x^{n-2} + \cdots + t\alpha_1 = \\ &= t(n\alpha_n x^{n-1} + (n-1)\alpha_{n-1}x^{n-2} + \cdots + \alpha_1) = \\ &= tf'.\end{aligned}$$

Свойства производной многочлена (2)

2) Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ и $g(x) = \beta_m x^m + \beta_{m-1} x^{m-1} + \cdots + \beta_1 x + \beta_0$. Для определенности будем считать, что $n \geqslant m$. Если $n > m$, то будем записывать $g(x)$ в виде $g(x) = \beta_n x^n + \beta_{n-1} x^{n-1} + \cdots + \beta_1 x + \beta_0$, где $\beta_{m+1} = \cdots = \beta_n = 0$. Тогда:

$$\begin{aligned}(f+g)' &= \big((\alpha_n+\beta_n)x^n + (\alpha_{n-1}+\beta_{n-1})x^{n-1} + \cdots + (\alpha_1+\beta_1)x + (\alpha_0+\beta_0)\big)' = \\ &= n(\alpha_n+\beta_n)x^{n-1} + (n-1)(\alpha_{n-1}+\beta_{n-1})x^{n-2} + \cdots + (\alpha_1+\beta_1) = \\ &= (n\alpha_n x^{n-1} + (n-1)\alpha_{n-1}x^{n-2} + \cdots + \alpha_1) + \\ &+ (n\beta_n x^{n-1} + (n-1)\beta_{n-1}x^{n-2} + \cdots + \beta_1) = \\ &= f' + g'.\end{aligned}$$

3) Предположим сначала, что $f(x) = x^n$, а $g(x) = x^m$ для некоторых n и m. Тогда

$$\begin{aligned}(fg)' = (x^{n+m})' &= (n+m)x^{n+m-1} = nx^{n+m-1} + mx^{n+m-1} = \\ &= nx^{n-1}\cdot x^m + x^n \cdot mx^{m-1} = f'g + fg'.\end{aligned}$$

Если же $f(x)$ и $g(x)$ — произвольные многочлены, то свойство 3) вытекает из доказанного только что равенства и свойств 1) и 2).

Свойства производной многочлена (3)

4) Докажем это свойство индукцией по m.

База индукции. Пусть $m = 2$. Используя свойство 3), имеем $(f^2)' = (f \cdot f)' = f'f + ff' = 2ff'$.

Шаг индукции. Пусть теперь $m > 2$. Используя предположение индукции и свойство 3), имеем

$$(f^m)' = (f^{m-1} \cdot f)' = (f^{m-1})'f + f^{m-1}f' = (m-1)f^{m-2}f'f + f^{m-1}f' =$$
$$= (m-1)f^{m-1}f' + f^{m-1}f' = mf^{m-1}f'.$$

Это завершает доказательство. □

Лемма 12.2

Если p — неприводимый многочлен над полем F характеристики 0, то многочлены p и p' взаимно просты.

Доказательство. Из неприводимости многочлена p вытекает, что $\deg p > 0$. В силу замечания 12.4 $\deg p' = \deg p - 1 \geqslant 0$. В частности, $p' \neq o$. Обозначим через d наибольший общий делитель многочленов p и p'. Тогда $p = dq$ и $p' = dr$ для некоторых многочленов q и r. В силу замечания 12.1 один из многочленов d и q принадлежит F. Если $q \in F$, то $\deg q = 0$ и

$$\deg p = \deg dq = \deg d + \deg q = \deg d \leqslant \deg p' = \deg p - 1.$$

Полученное противоречие показывает, что $q \notin F$. Следовательно, $d \in F$. В частности, d ассоциирован с 1. Учитывая замечание 10.5, мы получаем, что многочлены p и p' взаимно просты. □

Неприводимые множители многочлена и его производной (1)

Как мы уже отмечали (см. замечание 12.3), линейный многочлен над любым полем неприводим. Используя введенные выше термины, лемму 11.3 можно переформулировать так: если f — многочлен над полем $\mathbb{R}$, то его линейный неприводимый множитель кратности k является неприводимым множителем кратности $k-1$ многочлена f'. Как мы увидим ниже, существуют нелинейные многочлены, неприводимые над полем $\mathbb{R}$ (см. предложение 12.6). Но оказывается, что аналог сформулированного только что факта справедлив для всякого неприводимого множителя многочлена над произвольным полем характеристики 0. Напомним, что неприводимый многочлен, не являющийся неприводимым множителем многочлена f, можно рассматривать как неприводимый множитель кратности 0 многочлена f.

Предложение 12.4

Пусть f — многочлен над полем F характеристики 0, а p — неприводимый множитель многочлена f кратности $k \geqslant 1$. Тогда p является неприводимым множителем многочлена f' кратности $k-1$.

Доказательство. Обозначим через g произведение старшего коэффициента многочлена f и всех неприводимых множителей этого многочлена, отличных от p. Тогда $f = p^k g$ и многочлены p и g взаимно просты. В силу леммы 12.2 многочлены p и p' также взаимно просты.

Неприводимые множители многочлена и его производной (2)

Из п. 3) предложения 10.1 вытекает теперь, что и многочлены p и $p'g$ взаимно просты. В частности, p не делит $p'g$. Заметим, что

$$f' = (p^k g)' = (p^k)'g + p^k g' = kp^{k-1}p'g + p^k g' = p^{k-1}(kp'g + pg').$$

Чтобы завершить доказательство, осталось проверить, что p не делит $kp'g + pg'$. Предположим, напротив, что p делит $kp'g + pg'$. Тогда, очевидно, p делит и $kp'g$, т. е. $kp'g = ph$ для некоторого многочлена h. Будем обозначать единицу поля F через e, чтобы отличать ее от числа 1. Положим $a = ke$. Если $a = 0$, то, в силу замечания 4.3а), $kx = 0$ для всякого $x \in F$. Но это невозможно, поскольку $\operatorname{char} F = 0$. Следовательно, $a \neq 0$, и потому существует элемент a^{-1}. Имеем $kp'g = k(ep'g) = (ke)p'g = ap'g$. Следовательно, $ap'g = kp'g = ph$. Умножая обе части равенства $ap'g = ph$ слева на a^{-1}, получаем, что $p'g = a^{-1}(ph) = (a^{-1}h)p$. Это означает, что p делит $p'g$. Но выше было показано, что это не так. □

Переход к многочлену без кратных множителей

Из предложения 12.4 вытекает следующее утверждение.

Следствие 12.2

Пусть f — произвольный многочлен степени > 0 над полем F характеристики 0. Положим $g = \frac{f}{d}$, где d — наибольший общий делитель многочленов f и f'. Тогда многочлены f и g имеют одни и те же неприводимые множители, причем второй из них не имеет кратных неприводимых множителей.

Доказательство. Очевидно, что все неприводимые множители многочлена g являются неприводимыми множителями многочлена f. А в силу предложения 12.4 все неприводимые множители многочлена f являются неприводимыми множителями многочлена g кратности 1. □

Это следствие (при $F = \mathbb{R}$) используется в математическом анализе при интегрировании дробно-рациональных функций.

Отделение кратных множителей: алгоритм

Приведем теперь алгоритм нахождения определенных выше многочленов $d_1, d_2, \ldots, d_k$. Процесс вычисления этих многочленов называется *отделением кратных множителей*.

Алгоритм 12.1 (алгоритм отделения кратных множителей)

Дан многочлен f степени > 0 над произвольным полем характеристики 0. Требуется найти определенные выше многочлены $d_0, d_1, \ldots, d_k$. Полагаем $f_0 = \frac{f}{\ell c(f)}$ и $i = 1$. Обозначаем через f_i наибольший общий делитель многочленов f_{i-1} и f'_{i-1}. Если $\deg f_i > 0$, увеличиваем значение i на единицу и повторяем вычисление многочлена f_i. Продолжаем этот процесс до тех пор, пока не окажется, что $\deg f_i = 0$. В тот момент, когда это равенство оказывается выполненным, полагаем $k = i$, $d_j = \frac{f_{j-1} f_{j+1}}{f_j^2}$ для всех $j = 1, 2, \ldots, k-1$ и $d_k = f_{k-1}$. На этом работа алгоритма завершается.

Обоснование алгоритма отделения кратных множителей. Прежде всего, заметим, что работа алгоритма в любом случае завершится через конечное число шагов, поскольку $\deg f_0 > \deg f_1 > \deg f_2 > \cdots$. Как уже отмечалось выше, $f = \alpha d_1 d_2^2 d_3^3 \cdots d_k^k$, где $\alpha = \ell c(f)$. Следовательно, $f_0 = d_1 d_2^2 d_3^3 \cdots d_k^k$, а из предложения 12.4 вытекает, что $f_1 = d_2 d_3^2 \cdots d_k^{k-1}$, $f_2 = d_3 \cdots d_k^{k-2}$, $\ldots$, $f_{k-1} = d_k$ и $f_k = 1$. Мы доказали, что $d_k = f_{k-1}$. Далее, очевидно, что, для всякого $j = 1, 2, \ldots, k-1$,

$$\frac{f_{j-1}}{f_j} = d_j d_{j+1} \cdots d_k \quad \text{и} \quad \frac{f_j}{f_{j+1}} = d_{j+1} d_{j+2} \cdots d_k,$$

откуда

$$d_j = \frac{d_j d_{j+1} \cdots d_k}{d_{j+1} d_{j+2} \cdots d_k} = \frac{f_{j-1}}{f_j} : \frac{f_j}{f_{j+1}} = \frac{f_{j-1} f_{j+1}}{f_j^2}.$$

□

12.3. Многочлены, неприводимые над полями $\mathbb{C}$ и $\mathbb{R}$

Из следствия 11.4 и замечания 12.3 вытекает

Предложение 12.5

Многочленами, неприводимыми над полем $\mathbb{C}$, являются линейные многочлены и только они. □

Многочлены, неприводимые над полем $\mathbb{R}$ (1)

Предложение 12.6

Многочленами, неприводимыми над полем $\mathbb{R}$, являются линейные многочлены, многочлены второй степени с отрицательными дискриминантами и только они.

Доказательство. Неприводимость линейных многочленов над любым полем очевидна. Как известно из школьного курса математики, квадратные трехчлены с отрицательным дискриминантом действительных корней не имеют. Поэтому их неприводимость над полем $\mathbb{R}$ вытекает из предложения 12.2. Чтобы доказать, что других неприводимых над $\mathbb{R}$ многочленов не существует, надо установить, что любой многочлен степени > 0 над полем $\mathbb{R}$ разлагается на множители с действительными коэффициентами, каждый из которых либо линеен, либо является многочленом второй степени с отрицательным дискриминантом.

Многочлены, неприводимые над полем $\mathbb{R}$ (2)

Пусть $f(x) \in \mathbb{R}[x]$ и $\deg f > 0$. В силу следствия 11.4 $f = \alpha(x-\gamma_1)\cdots(x-\gamma_n)$, где $\alpha, \gamma_1, \ldots, \gamma_n \in \mathbb{C}$. При этом $\alpha \in \mathbb{R}$, поскольку $f \in \mathbb{R}[x]$. Если $\gamma_1, \ldots, \gamma_n \in \mathbb{R}$, то все доказано. Поэтому без ограничения общности можно считать, что $\gamma_1, \ldots, \gamma_m \in \mathbb{R}$ и $\gamma_{m+1}, \ldots, \gamma_n \notin \mathbb{R}$, причем $m < n$. Для всякого $k = m+1, \ldots, n$ положим $\gamma_k = \alpha_k + \beta_k i$. Ясно, что $\beta_k \neq 0$. По лемме 11.2 число $\overline{\gamma_k} = \alpha_k - \beta_k i$ также является корнем многочлена f, причем кратности корней γ_k и $\overline{\gamma_k}$ совпадают. Это означает, что набор чисел $\gamma_{m+1}, \ldots, \gamma_n$ можно (изменив при необходимости порядок перечисления чисел) переписать в виде γ_{m+1}, $\overline{\gamma_{m+1}}$, γ_{m+2}, $\overline{\gamma_{m+2}}$, $\ldots$, $\gamma_{m+\ell}$, $\overline{\gamma_{m+\ell}}$ для некоторого ℓ. Следовательно, для всякого $k = m+1, m+2, \ldots, m+\ell$, многочлен f делится на

$$(x-\gamma_k)(x-\overline{\gamma_k}) = (x-\alpha_k-\beta_k i)(x-\alpha_k+\beta_k i) = \\ = (x-\alpha_k)^2 - (\beta_k i)^2 = x^2 - 2\alpha_k x + \alpha_k^2 + \beta_k^2.$$

Полученный квадратный трехчлен над $\mathbb{R}$ имеет отрицательный дискриминант. В самом деле, $4\alpha_k^2 - 4(\alpha_k^2+\beta_k^2) = -4\beta_k^2 < 0$, поскольку $\beta_k \neq 0$. Таким образом, $f(x)$ является произведением линейных множителей и квадратных трехчленов над $\mathbb{R}$ с отрицательным дискриминантом. $\square$

12.4. Многочлены, неприводимые над полем $\mathbb{Q}$

Простого и удобного для применения критерия неприводимости многочленов над полем $\mathbb{Q}$ не существует. Есть только весьма сильное достаточное условие. Чтобы доказать его, нам понадобятся некоторые вспомогательные понятия и результаты.

Определение

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0$ — многочлен над кольцом $\mathbb{Z}$. Обозначим через $d(f)$ наибольший общий делитель чисел $\alpha_n, \alpha_{n-1}, \ldots, \alpha_0$. Если $d(f) = 1$, то многочлен f называется *примитивным*.

Если в многочлене $f \in \mathbb{Z}[x]$ вынести за скобки наибольший общий делитель всех его коэффициентов, то в скобках будет стоять примитивный многочлен над $\mathbb{Z}$. Таким образом,

!! *произвольный многочлен $f \in \mathbb{Z}[x]$ представим в виде $f = d(f) \cdot f_0$, где f_0 — примитивный многочлен над $\mathbb{Z}$.* □

Лемма 12.3 (лемма Гаусса)

Произведение двух примитивных многочленов над $\mathbb{Z}$ примитивно.

Доказательство. Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ и $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ — многочлены над $\mathbb{Z}$. Предположим, что многочлены f и g примитивны, а их произведение не примитивно. Следовательно, существует простое число p, делящее $d(fg)$. В силу примитивности многочленов f и g, существуют индексы s и t такие, что p не делит a_s и b_t. Пусть s и t — минимальные индексы с такими свойствами. Коэффициент при x^{s+t} в многочлене fg будет равен

$$\begin{aligned} c_{s+t} &= a_s b_t + a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \cdots + \\ &+ a_{s-1} b_{t+1} + a_{s-2} b_{t+2} + \cdots . \end{aligned} \tag{3}$$

В силу выбора индексов s и t, коэффициенты a_{s-i} и b_{t-i} при $i > 0$ делятся на p, а из того, что p делит $d(fg)$, вытекает, что p делит c_{s+t}. Отсюда и из равенства (3) вытекает, что p делит $a_s b_t$. Но тогда, будучи простым, число p делит либо a_s, либо b_t, что противоречит выбору p. □

Эквивалентность неприводимости над $\mathbb{Z}$ и над $\mathbb{Q}$

Предложение 12.7

Многочлен $f \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$ тогда и только тогда, когда он неприводим над $\mathbb{Q}$.

Доказательство. *Достаточность* очевидна. Докажем *необходимость*. Предположим, что f неприводим над $\mathbb{Z}$, но приводим над $\mathbb{Q}$. Пусть $f = gh$, где $g, h \in \mathbb{Q}[x]$ и $\deg g, \deg h < \deg f$. Тогда $\deg g, \deg h > 0$. Обозначим через a наименьшее общее кратное знаменателей всех коэффициентов многочлена g, а через b — наименьшее общее кратное знаменателей всех коэффициентов многочлена h. Тогда $gh = \frac{1}{ab} \cdot g_1 h_1$, где g_1 и h_1 — многочлены над $\mathbb{Z}$. Теперь положим $c = d(g_1)$ и $d = d(h_1)$. Тогда $g_1 = cg_2$ и $h_1 = dh_2$, где g_2 и h_2 — примитивные многочлены над $\mathbb{Z}$. Объединяя сказанное, имеем

$$f = gh = \frac{1}{ab} \cdot g_1 h_1 = \frac{cd}{ab} \cdot g_2 h_2.$$

Все коэффициенты многочлена f являются целыми числами. Следовательно, ab делит все коэффициенты многочлена $cdg_2 h_2$, т. е. ab делит $cd \cdot d(g_2 h_2)$. В силу леммы Гаусса многочлен $g_2 h_2$ примитивен. Это означает, что $d(g_2 h_2) = 1$, и потому ab делит cd. Положим $\frac{cd}{ab} = k$. В силу сказанного выше, k — целое число и $f = (kg_2)h_2$. Это означает, что многочлен f приводим над $\mathbb{Z}$ вопреки его выбору.

Критерий Эйзенштейна: формулировка

Если $f \in \mathbb{Q}[x]$, то умножив многочлен f на наименьшее общее кратное знаменателей всех его коэффициентов, мы получим многочлен g с целыми коэффициентами. Поскольку $g = af$, где $a \in \mathbb{Z}$, многочлен g неприводим над $\mathbb{Q}$ тогда и только тогда, когда f неприводим над $\mathbb{Q}$. Таким образом,

- *при изучении многочленов, неприводимых над $\mathbb{Q}$, можно ограничиться рассмотрением многочленов над $\mathbb{Q}$ с целыми коэффициентами.*

Следующее утверждение дает упомянутое выше достаточное условие неприводимости многочлена над $\mathbb{Q}$, которое по традиции называется критерием Эйзенштейна.

Теорема 12.2 (критерий Эйзенштейна)

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ — многочлен степени > 0 над $\mathbb{Q}$ с целыми коэффициентами и существует простое число p такое, что a_n не делится на p, $a_{n-1}, \ldots, a_0$ делятся на p и a_0 не делится на p^2. Тогда f неприводим над $\mathbb{Q}$.

Критерий Эйзенштейна: комментарий

Как будет показано ниже в данном параграфе, критерий Эйзенштейна не является необходимым условием неприводимости многочлена над $\mathbb{Q}$ (см. пример 12.3). Таким образом, название этого утверждения противоречит общепринятому в математике пониманию слова «критерий» как «необходимое и достаточное условие», и его следовало бы называть не критерием, а признаком Эйзенштейна или даже, скорее, признаком Шёнемана, поскольку оно было впервые доказано Шёнеманом в 1846 г. и переоткрыто Эйзенштейном спустя четыре года. Несмотря на все это, название «критерий Эйзенштейна» общепринято, и потому мы будем им пользоваться.

Критерий Эйзенштейна: доказательство

Доказательство критерия Эйзенштейна. Предположим, что f приводим над $\mathbb{Q}$. Тогда, в силу предложения 12.7, f приводим над $\mathbb{Z}$. Следовательно, f представим в виде $f = gh$, где $g(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_0$ и $h(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_0$ — многочлены степени > 0 над $\mathbb{Z}$. Ясно, что $a_0 = b_0 c_0$. Поскольку a_0 делится на p, но не делится на p^2, из простоты числа p вытекает, что p делит одно из чисел b_0 и c_0, но не оба одновременно. Предположим для определенности, что p делит b_0, но не делит c_0. Если p делит все коэффициенты многочлена g, то оно делит и все коэффициенты многочлена f, включая a_n. Следовательно, существует индекс i такой, что p не делит b_i. Пусть i — минимальный индекс с таким свойством. Ясно, что $\deg g < \deg f$, и потому $i \leqslant k < n$. В частности, p делит a_i. По определению произведения многочленов имеем

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots .$$

Поскольку p делит a_i и b_j для всех $j < i$, из этого равенства вытекает, что p делит $b_i c_0$. Но это невозможно, так как p не делит ни b_i, ни c_0. □

Степени многочленов, неприводимых над полем $\mathbb{Q}$

Критерий Эйзенштейна показывает, что с точки зрения строения неприводимых многочленов поле $\mathbb{Q}$ разительно отличается от полей $\mathbb{R}$ и $\mathbb{C}$. В самом деле, как мы видели выше, всякий неприводимый над $\mathbb{C}$ многочлен линеен, а всякий неприводимый над $\mathbb{R}$ многочлен имеет степень $\leqslant 2$. В то же время, справедлив следующий факт.

Следствие 12.3

Для всякого натурального n существует неприводимый над полем $\mathbb{Q}$ многочлен степени n.

Доказательство. Достаточно учесть, что, в силу критерия Эйзенштейна, неприводимым над $\mathbb{Q}$ является многочлен $x^n + 2$, где n — произвольное натуральное число (он удовлетворяет посылке критерия Эйзенштейна при $p = 2$). □

Иррациональность числа $\sqrt[n]{p}$

В качестве любопытного «побочного» следствия из критерия Эйзенштейна отметим следующий факт, обычно доказываемый средствами элементарной математики.

Следствие 12.4

Для всякого натурального числа $n > 1$ и всякого простого числа p число $\sqrt[n]{p}$ иррационально.

Доказательство. Если число $\sqrt[n]{p}$ рационально, то оно является рациональным корнем многочлена $x^n - p$. В силу замечания 12.2 отсюда вытекает, что многочлен $x^n - p$ приводим над полем $\mathbb{Q}$. Но из критерия Эйзенштейна вытекает, что это не так. $\square$

Критерий Эйзенштейна: пример

Приведем теперь обещанный выше пример, показывающий, что критерий Эйзенштейна не является необходимым условием неприводимости многочлена над $\mathbb{Q}$.

Пример 12.3

Рассмотрим многочлен $f(x) = x^3 + 4$. Пользуясь следствием 11.10, легко проверить, что этот многочлен не имеет рациональных корней. Из предложения 12.2 вытекает теперь, что он неприводим над $\mathbb{Q}$. В то же время, $f(x)$ не удовлетворяет посылке критерия Эйзенштейна, поскольку единственное простое число, которое делит свободный член многочлена $f(x)$ — это число 2, и свободный член $f(x)$ делится на квадрат этого числа.

Алгоритм Кронекера (1)

Отсутствие критерия приводимости многочлена над полем $\mathbb{Q}$ частично компенсируется существованием алгоритмов, позволяющих по произвольному многочлену над $\mathbb{Q}$ установить, приводим он над $\mathbb{Q}$ или нет. Приведем один из таких алгоритмов, называемый *алгоритмом Кронекера*. Отметим, что этот алгоритм впервые был опубликован Шубертом в 1793 г. и переоткрыт Кронекером почти 100 лет спустя — в 1882 г. Его формулировка начинается на этом слайде и завершается на следующем.

Пусть f — многочлен степени > 0 над полем $\mathbb{Q}$. Если не все коэффициенты многочлена f являются целыми числами, умножим f на наименьшее общее кратное знаменателей всех его коэффициентов. Ясно, что на приводимость или неприводимость f это не влияет. Все коэффициенты полученного многочлена являются целыми числами. Поэтому можно считать, что f — многочлен с целыми коэффициентами.

Алгоритм 12.2 (алгоритм Кронекера), начало

Дан многочлен f степени > 0 над полем $\mathbb{Q}$ с целыми коэффициентами. Требуется установить, является ли он приводимым над $\mathbb{Q}$. Если $\deg f = 1$, то алгоритм устанавливает, что f неприводим над $\mathbb{Q}$, и завершает работу. Далее считаем, что $\deg f > 1$. Положим $m = \left[\frac{\deg f}{2}\right]$ (через $[x]$ обозначается целая часть действительного числа x).

Алгоритм 12.2 (алгоритм Кронекера), окончание

Пусть $x_0, x_1, \ldots, x_m$ — произвольные попарно различные целые числа. Вычисляем последовательно числа $f(x_0)$, $f(x_1)$, $\ldots$, $f(x_m)$. Ясно, что все эти числа — целые. Если оказывается, что $f(x_j) = 0$ для некоторого $j \in \{1, 2, \ldots, m\}$, то алгоритм делает вывод, что многочлен f приводим над $\mathbb{Q}$, и завершает работу. Далее считаем, что $f(x_j) \neq 0$ для всех $j = 0, 1, \ldots, m$. Для всякого набора чисел $(d_0, d_1, \ldots, d_m)$ такого, что d_j делит $f(x_j)$ для всех $j = 0, 1, \ldots, m$, обозначим через $g_{(d_0, d_1, \ldots, d_m)}$ интерполяционный многочлен Лагранжа, соответствующий набору пар (x_0, d_0), (x_1, d_1), $\ldots$, (x_m, d_m). Число многочленов вида $g_{(d_0, d_1, \ldots, d_m)}$ конечно, поскольку существует лишь конечное число наборов чисел $(d_0, d_1, \ldots, d_m)$ таких, что d_j делит $f(x_j)$ для всех $j = 0, 1, \ldots, m$. Обозначим эти многочлены через $g_1, g_2, \ldots, g_k$. Перебираем последовательно многочлены $g_1, g_2, \ldots, g_k$. Если найдется $i \in \{1, 2, \ldots, k\}$ такое, что $\deg g_i > 0$ и $g_i \mid f$, то алгоритм устанавливает, что многочлен f приводим над $\mathbb{Q}$, и завершает работу. Если же для всякого $i = 1, 2, \ldots, k$ либо $\deg g_i = 0$, либо g_i не делит f, то алгоритм делает вывод, что многочлен f неприводим над $\mathbb{Q}$, и завершает работу.

Алгоритм Кронекера: примечание

Число многочленов вида $g_{(d_0,d_1,\ldots,d_m)}$, которые надо вычислить в процессе работы алгоритма Кронекера, можно сократить вдвое, если воспользоваться следующим соображением. Пусть $p_0(x)$, $p_1(x)$, …, $p_m(x)$ — многочлены, вычисляемые по формуле (3) из §11. В соответствии с формулой (4) из §11,

$$g_{(-d_0,-d_1,\ldots,-d_m)} = -d_0 p_0(x) - d_1 p_1(x) - \cdots - d_m p_m(x) = \\ = -\bigl(d_0 p_0(x) + d_1 p_1(x) + \cdots + d_m p_m(x)\bigr) = -g_{(d_0,d_1,\ldots,d_m)}.$$

Ясно, что умножение многочлена на -1 не меняет его степень и не влияет на то, делит ли он многочлен f. Поэтому вычислив многочлен $g_{(d_0,d_1,\ldots,d_m)}$, мы можем не вычислять многочлен $g_{(-d_0,-d_1,\ldots,-d_m)}$: ответы на интересующие нас вопросы для этих двух многочленов одинаковы. Это позволяет при выполнении алгоритма Кронекера рассматривать только такие наборы чисел $(d_0, d_1, \ldots, d_m)$, в которых $d_0 > 0$.

Алгоритм Кронекера: обоснование (начало)

Обоснование алгоритма Кронекера. Замечание 12.3 позволяет считать, что $\deg f > 1$. С учетом этого, из замечания 12.2 вытекает, что достаточно рассмотреть случай, когда $f(x_j) \neq 0$ для всех $j = 0, 1, \ldots, m$.

Предположим, что f приводим над $\mathbb{Q}$. В силу предложения 12.7 получаем, что f приводим и над $\mathbb{Z}$. Следовательно, существуют многочлены $g, h \in \mathbb{Z}[x]$ такие, что $f = gh$ и $0 < \deg g, \deg h < \deg f$. Положим $m = \left[\frac{\deg f}{2}\right]$. Если $\deg g, \deg h > m$, то $\deg f = \deg g + \deg h > \deg f$. Поэтому без ограничения общности можно считать, что $\deg g \leqslant m$. Если $g(x_j) = 0$ для некоторого $j \in \{0, 1, \ldots, m\}$, то $f(x_j) = g(x_j) \cdot h(x_j) = 0$. Следовательно, $g(x_j) \neq 0$ для всех $j = 0, 1, \ldots, m$. Поскольку $f(x_j) = g(x_j) \cdot h(x_j)$, получаем, что $g(x_j)$ делит $f(x_j)$ для всех $j = 0, 1, \ldots, m$. Для всякого $j = 0, 1, \ldots, m$ положим $d_j = g(x_j)$. Тогда d_j делит $f(x_j)$ и $g(x_j) = g_{(d_0, d_1, \ldots, d_m)}(x_j)$ для всех $j = 0, 1, \ldots, m$. Из теоремы 11.1 вытекает, что $g = g_{(d_0, d_1, \ldots, d_m)}$. Итак, если f приводим над $\mathbb{Q}$, то один из многочленов вида $g_{(d_0, d_1, \ldots, d_m)}$ делит f и имеет степень > 0. Следовательно, если все многочлены такого вида либо не делят f, либо имеют степень 0, то f неприводим над $\mathbb{Q}$.

Алгоритм Кронекера: обоснование (конец) и комментарий

Обратно, предположим, что существует многочлен g вида $g_{(d_0,d_1,\ldots,d_m)}$ такой, что $g \mid f$ и $\deg g > 0$. Ясно, что $\deg g \leqslant m < \deg f$. Из формул (3) и (4) в § 11 вытекает, что $g \in \mathbb{Q}[x]$. Но тогда и $h = \frac{f}{g} \in \mathbb{Q}[x]$. Ясно, что $\deg h = \deg f - \deg g < \deg f$.Следовательно, многочлен $f = gh$ приводим над $\mathbb{Q}$. □

Если многочлен f приводим над полем $\mathbb{Q}$, то алгоритм Кронекера позволяет не только установить этот факт, но и найти разложение f на неприводимые множители над $\mathbb{Q}$. В самом деле, если f приводим над полем $\mathbb{Q}$, то алгоритм Кронекера находит многочлен g над $\mathbb{Q}$ такой, что $g \mid f$ и $0 < \deg g < \deg f$. Разделив f на g, мы найдем многочлен h над $\mathbb{Q}$ такой, что $f = gh$ и $0 < \deg g, \deg h < \deg f$. Если какой-то из многочленов g и h приводим над $\mathbb{Q}$, то, установив этот факт (с помощью того же алгоритма Кронекера или каким-то иным способом), мы представим этот многочлен в виде произведения многочленов над $\mathbb{Q}$ меньшей степени. Продолжая этот процесс, мы в конце концов получим разложение f на неприводимые множители над полем $\mathbb{Q}$.