Замечание 2. Обычно бывает не слишком просто решить, является ли данный многочлен (скажем, от одной переменной) неприводимым. Например, многочлен X^4+4 приводим над полем рациональных чисел, потому что

$$X^4+4=(X^2-2X+2)(X^2+2X+2).$$

Позже в этой книге мы укажем точный критерий неприводимости многочлена X^n-a. Другие критерии даются в следующем параграфе.

§ 7. Критерии неприводимости

Первый критерий — это критерий Эйзенштейна. *Пусть A — факториальное кольцо, K — его поле частных, $f(X)=a_nX^n+\ldots+a_0$ — многочлен степени $n\geqslant 1$ в $A[X]$ и p — простой элемент в A. Предположим, что*

$$a_n\not\equiv 0 \pmod p,\quad a_i\equiv 0 \pmod p \text{ для всех } i<n,\quad a_0\not\equiv 0 \pmod{p^2}.$$

Тогда $f(X)$ неприводим в $K[X]$.

Доказательство. Выделяя в случае надобности н. о. д. из коэффициентов f, мы можем, не теряя общности, считать, что содержание многочлена f равно 1. Если f разлагается на множители в $K[X]$, то, согласно следствию леммы Гаусса, существует и разложение в $A[X]$, скажем $f(X)=g(X)h(X)$,

$$g(X)=b_dX^d+\ldots+b_0,$$
$$h(X)=c_mX^m+\ldots+c_0,$$

где $d,\ m\geqslant 1$ и $b_dc_m\neq 0$. Пусть σ — канонический гомоморфизм, отображающий A на $A/(p)$. Тогда

$$f^\sigma(X)=g^\sigma(X)h^\sigma(X).$$

Но $f^\sigma(X)=\sigma(a_n)X^n$. Поэтому в силу однозначности разложения на множители в кольце $A/(p)[X]$

$$g^\sigma(X)=\sigma(b_d)X^d \quad\text{и}\quad h^\sigma(X)=\sigma(c_m)X^m,$$

откуда $b_0\equiv 0 \pmod p$ и $c_0\equiv 0 \pmod p$. Следовательно, $a_0=b_0c_0\equiv\equiv 0 \pmod{p^2}$, что противоречит условию.

Пример. Пусть a — отличное от нуля и свободное от квадратов целое число $\neq\pm 1$. Тогда для любого $n\geqslant 1$ многочлен X^n-a неприводим над $\mathbf{Q}$. Многочлены $3X^5-15$, $2X^{10}-21$ неприводимы над $\mathbf{Q}$.

В некоторых случаях многочлен, не удовлетворяющий критерию Эйзенштейна, после простого преобразования начинает ему удовлетворять.

Пример. Пусть p — простое число. Многочлен

$$f(X) = X^{p-1} + \ldots + 1$$

неприводим над $\mathbf{Q}$.

Доказательство. Достаточно доказать, что многочлен $f(X+1)$ неприводим над $\mathbf{Q}$. Заметим, что биномиальные коэффициенты

$$\binom{p}{\nu} = \frac{p!}{\nu!(p-\nu)!}, \quad 1 \leqslant \nu \leqslant p-1,$$

делятся на p (потому что числитель делится на p, знаменатель не делится, а сам коэффициент является целым числом). Имеем

$$f(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \frac{X^p + pX^{p-1} + \ldots + pX}{X},$$

откуда видно, что $f(X+1)$ удовлетворяет критерию Эйзенштейна.

Пример. Пусть E — поле и t — элемент некоторого поля, содержащего E, такой, что t трансцендентен над E. Пусть K — поле частных кольца $E[t]$. Для любого целого $n \geqslant 1$ многочлен $X^n - t$ неприводим в $K[X]$. Это вытекает из того факта, что кольцо $A = E[t]$ факториально и t — простой элемент в нем.

Редукционный критерий. *Пусть* A, B — *целостные кольца,*

$$\sigma\colon A \to B$$

— *гомоморфизм и* K, L — *поля частных для* A *и* B *соответственно. Пусть, далее,* $f \in A[X]$ — *такой многочлен, что* $f^\sigma \neq 0$ *и* $\deg f^\sigma = \deg f$. *Если* f^σ *неприводим в* $L[X]$, *то* f *не обладает разложением* $f(X) = g(X)h(X)$, *в котором*

$$g,\ h \in A[X] \text{ и } \deg g,\ \deg h \geqslant 1.$$

Доказательство. Предположим, что f имеет такое разложение. Тогда $f^\sigma = g^\sigma h^\sigma$. Так как $\deg g^\sigma \leqslant \deg g$ и $\deg h^\sigma \leqslant \deg h$, то из нашего предположения вытекает, что в этих соотношениях для степеней должно иметь место равенство. Следовательно, в силу неприводимости f^σ в $L[X]$ мы заключаем, что либо g, либо h есть элемент из A, что и требовалось установить.

Предположим в предыдущем критерии, что A — локальное кольцо, т. е. кольцо, имеющее единственный максимальный идеал $\mathfrak{p}$, и что $\mathfrak{p}$ служит ядром σ. Тогда из неприводимости f^σ в $L[X]$ заключаем о неприводимости f в $A[X]$. В действительности любой элемент из A, не лежащий в $\mathfrak{p}$, должен быть единицей в A, так что последнее утверждение критерия можно усилить, добавив, что g или h является единицей в A.

Этот критерий можно применять также в тех случаях, когда A факториально, и в этом случае заключать о неприводимости f в $K[X]$.

Пример. Пусть p — простое число. Ниже будет показано, что многочлен $X^p - X - 1$ неприводим над полем $\mathbf{Z}/p\mathbf{Z}$. Следовательно, $X^p - X - 1$ неприводим над $\mathbf{Q}$. Аналогично многочлен

$$X^5 - 5X^4 - 6X - 1$$

неприводим над $\mathbf{Q}$.

§ 8. Производная и кратные корни

Пусть A — коммутативное кольцо. Определим отображение

$$D\colon\ A[X] \to A[X]$$

кольца многочленов в себя. Если $f(X) = a_n X^n + \ldots + a_0$, где $a_i \in A$, то производная $Df \equiv f'$ определяется соотношением

$$Df(X) = f'(X) = \sum_{\nu=1}^{n} \nu a_\nu X^{\nu-1} = n a_n X^{n-1} + \ldots + a_1.$$

Легко проверяется, что для всяких многочленов f, g из $A[X]$

$$(f+g)' = f' + g', \qquad (fg)' = f'g + fg'$$

и для всякого $a \in A$

$$(af)' = af'.$$

Пусть K — поле, f — многочлен из $K[X]$ и a — его корень в K. Тогда

$$f(X) = (X-a)^m g(X),$$

где $g(X)$ — некоторый многочлен, взаимно простой с $X-a$ (и, следовательно, такой, что $g(a) \neq 0$). Мы называем m *кратностью* a в f и говорим, что a — *кратный корень*, если $m > 1$.

Предложение 1. *Пусть K, f обозначают то же, что и выше. Элемент a поля K является кратным корнем многочлена f тогда и только тогда, когда $f'(a) = 0$.*

Доказательство. Взяв для f указанное выше разложение, получаем

$$f'(X) = (X-a)^m g'(X) + m(X-a)^{m-1} g(X).$$

Если $m > 1$, то, очевидно, $f'(a) = 0$. Обратно, если $m = 1$, то $f'(X) = (X-a)g'(X) + g(X)$, откуда $f'(a) = g(a) \neq 0$. Следовательно, если $f'(a) = 0$, то мы должны иметь $m > 1$, что и требовалось доказать.