Доказательство

Пусть $p(x)$ – неприводим над $\mathbb{R}$ и $\deg p(x) > 2$ По теореме Гаусса существует $x_0 \in \mathbb{C}$ – корень $p(x)$ По лемме $\overline{x}_0$ – также корень $p(x)$ Имеем

$$p(x) = (x - x_0)(x - \overline{x}_0)q(x),$$

где $\deg q(x) > 0$

Ясно, что $q(x) \in \mathbb{R}[x]$, т к $p(x) \in \mathbb{R}[x]$ и $(x - x_0)(x - \overline{x}_0) = \; = x^2 - (x_0 + \overline{x}_0)x +$
$+|x_0|^2 \in \mathbb{R}[x]$

Но равенство

$$p(x) = (x^2 - \; -(x_0 + \overline{x}_0)x + |x_0|^2)q(x)$$

противоречит неприводимости многочлена $p(x)$

Осталось заметить, что многочлены $ax^2 + bx + c$, $a \neq 0$, $b^2 - 4ac \geq 0$ не могут быть неприводимыми, т к имеют хотя бы один вещественный корень

Замечание

Если $f(x) \in F[x]$, $\deg f(x) = 2$ или 3, то вопрос о неприводимости $f(x)$ эквивалентен вопросу об отсутствии корней $f(x)$ в поле F

В общем случае это утверждение неверно

Пример

$F = \mathbb{R}$, $f(x) = x^4 + 4 = \; = (x^4 + 4x^2 + 4) - 4x^2 = \; = (x^2 + 2)^2 - 4x^2 = \; = (x^2 - 2x + 2)$
$(x^2 + 2x + 2)$

Следствие 4

Всякий многочлен $f(x) \in \mathbb{R}[x]$, $\deg f(x) > 0$ представим в виде

$$f(x) = a(x - x_1)^{k_1} \quad (x - x_s)^{k} \; p_1(x)^{l_1} \quad p_t(x)^{l},$$

Где $x_1, \quad , x_s \in \mathbb{R}$ – попарно различные вещественные корни $f(x)$ кратности $k_1, \quad , k_s$ соответственно, $p_i(x) = x^2 + c_i x + \quad + d_i \in \mathbb{R}[x]$ – попарно различные многочлены $c_i^2 - 4d_i < 0$ $(i = 1, \quad , t)$

Пусть $F = \mathbb{Q}$ Можно доказать, что неприводимыми над $\mathbb{Q}$ могут быть многочлены любой степени Например, многочлен $p(x) = x^n - 2$, неприводим при любом $n \geq 1$ Для доказательства этого утверждения и других подобных обычно применяют признаки (достаточные условия) неприводимости Наиболее известным из них является так называемый признак Эйзенштейна

Теорема 13 (критерий Эйзенштейна)

Пусть $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \; + \quad + a_1 x + a_0$

Предположим, что существует такое простое число p что

1 a_n не делится на p

2 $a_{n-1}, \quad , a_1, a_0$ делятся на p

3 a_0 не делится на p^2

Тогда $f(x)$ неприводим над $\mathbb{Q}$

Доказательство этой теоремы опирается на нижеследующие леммы Гаусса

Лемма 1

Если $f(x) \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$ (т е $f(x) \neq f_1(x) f_2(x)$, где $f_i(x) \in \mathbb{Z}[x]$ $\deg f_i(x) > 0$, $i = 1, 2$), то $f(x)$ неприводим и над $\mathbb{Q}$

Опр Содержанием многочлена f (x) называется НОД всех его коэффициентов

Обозначение cont ($f(x)$)

Лемма 2

Пусть $f(x), g(x) \in \mathbb{Z}[x]$
Тогда cont ($f(x)\, g(x)$) = cont ($f(x)$) cont ($g(x)$)

Q Как найти корни многочлена? (и тем самым частично найти его каноническое разложение)

A Для поля $\mathbb{Q}$ ответ в следующей теореме

Теорема 14

Пусть $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + \quad + \ + a_1 x + a_0$

Если $p/q \in \mathbb{Q}$ – корень $f(x)$, причем НОД (p, q) = 1, то p – делитель a_0 q – делитель a_n

Замечание

Эта теорема дает очевидный алгоритм поиска всех рациональных корней данного многочлена $f(x) \in \mathbb{Q}[x]$

Доказательство

Имеем $f\left(p/q\right) = 0$, т е

$$a_n\left(p/q\right)^n + \quad + \ + a_1\left(p/q\right) + a_0 = 0$$

Избавимся от знаменателей

$$a_n p^n + a_{n-1} p^{n-1} q + \qquad + a_1 p q^{n-1} + \ + a_0 q^n = 0$$

Или

$$a_n p^n = q(-a_{n-1} p^{n-1} - \qquad - a_1 p q^{n-2} - a_0 q^{n-1})$$

Следовательно, $a_n p^n$ делится на q Т к $НОД\left(p^n, q\right) = 1$ (это – следствие взаимной простоты p и q), то a_n делится на q (по соответствующему свойству взаимно простых чисел)

Аналогично доказывается, что a_0 делится на p