Неприводимость над $\mathbb{R}$

Лемма. Пусть $f(x) \in \mathbb{R}[x]$. Если число $z \in \mathbb{C}$ является корнем $f(x)$, то и сопряжённое ему число $\overline{z}$ тоже является корнем $f(x)$.

Доказательство. $f(x) = a_n x^n + ... + a_0, a_i \in \mathbb{R}$
z - корень $\Rightarrow f(z) = a_n z^n + ... + a_1 z + a_0 = 0$.
Возьмём комплексное сопряжённое от обеих частей. Получим $\overline{f(z)} = \overline{a_n z^n + ... + a_1 z + a_0} = \overline{0}$
$\overline{a_n}(\overline{z^n}) + (\overline{a_{n-1}})(\overline{z^{n-1}}) + ... + \overline{a_1}\overline{z} + \overline{a_0} = 0$
$a_i \in \mathbb{R}$
$a_n(\overline{z^n}) + a_{n-1}(\overline{z^{n-1}}) + ... + a_1\overline{z} + a_0 = 0 \Rightarrow f(\overline{z}) = 0$ чтд.

Теорема. Над $\mathbb{R}$ неразложимимы являются многочлены только первой и второй степени (с отрицательным дискриминантом)

Доказательство.
$\mathbb{R} \subseteq \mathbb{C} \Rightarrow f(x) \in \mathbb{R}[x]$ имеет в точности n корней над полем $\mathbb{C}$.
Множество корней можно разбить на два типа:

1. $a_1, ..., a_k$ - вещественные корни

2. $z_1, \overline{z_1}, z_2, \overline{z_2}, ..., z_m$ - комплексные корни, у каждого из которых есть сопряженная пара (смотри предыдущую лемму)

n - степень $f(x) \Rightarrow k + 2m = n$
$f(x) = (x - a_1)...(x - a_k)(x - z_1)(x - \overline{z_1})...(x - z_m)(x - \overline{z_m})$
Перемножим пары скобок, которые содержат сопряжённые числа.
$(x - z_i)(x - \overline{z_i}) = x^2 - x(z_i + \overline{z_i}) + z_i\overline{z_i} = x^2 - 2c_i + (x_i^2 + d_i^2), (z_i = c_i + id_i, z_i + \overline{z_i} = 2c_i, z_i\overline{z_i} = c_i^2 + d_i^2$
Для каждого $i = 1, ..., m$ получаем многочлен второй степени $f_i(x) = x^2 - 2c_i + (x_i^2 + d_i^2)$

Следствие. Любой многочлен над $\mathbb{R}$, имеющий нечётную степень, имеет вещественный корень.

Разложение многочленов над $\mathbb{Q}$ и $\mathbb{Z}$

Теорема. Пусть $f(x) \in \mathbb{Z}[x]$. Многочлен разложим над $\mathbb{Z}[x] \Leftrightarrow$ он разложим над $\mathbb{Q}[x]$.

Доказательство. Пусть $f(x) \in \mathbb{Z}[x]$.
Пусть $f(x)$ разложим над $\mathbb{Q}[x]$.
$f(x) = a_n x^n + ... + a_1 x + a_0, a_i \in \mathbb{Z}, i = 0, ..., n$
$f(x) = g(x)h(x), g(x), h(x) \in \mathbb{Q}[x]$
Рассмотрим $g(x)h(x)$.
$g(x) = \frac{c_1}{b_1} g_1(x)$
$h(x) = \frac{c_2}{b_2} h_1(x)$
b_1 - общий знаменатель, c_1 - общий множитель в числителе.

Определение. Многочлен называется **примитивным**, если НОД его коэффициентов равен 1.

$g_1(x)$ и $h_1(x) \in \mathbb{Z}[x]$ (примитивные)

$f(x) = a_nx^n + ... + a_1x + a_0 = g(x)h(x) = \dfrac{c_1c_2}{b_1b_2}(g_1(x)h_1(x))$
$g_1(x)h_1(x)$ - примитивный многочлен с целыми коэффициентами.
Если $\dfrac{c_1c_2}{b_1b_2} = \dfrac{p}{q}$, то $\dfrac{p}{q}f_1(x)$ - многочлен, в котором есть рациональная дробь (поскольку он примитивный, то НОД коэффициентов равен 1 и при $q \neq 1$ остаётся коэффициент, не являющийся целым числом)

Лемма Гаусса. Произведение примитивных многочленов является примитивным многочленом.

Доказательство. Пусть $g(x) = b_kx^k+...+b_1x+b_0(b_i \in \mathbb{Z}), h(x) = c_mx^m+...+c_1x+c_0(c_i \in \mathbb{Z}) \in \mathbb{Z}[x]$ являются примитивными.
$f(x) = a_nx^n + ... + a_1x + a_0 = (b_kx^k + ... + b_1x + b_0)(c_mx^m + ... + c_1x + c_0)$
$a_n = c_mb_{n-m}$
$a_{n-1} = c_{m-1}b_{n-m-1} + c_{m-1}b_{n-m}$
...
$a_i = c_0b_i + c_1b_{i-1} + ... + c_ib_{k-i}$
Пусть $f(x)$ непримитивный $\Rightarrow \exists d \neq 1$ такое, что d делит любой коэффициент $f(x)$ (будем считать, что d - простое).
Возьмём наименьший индекс i_0 такой, что c_{i_0} не делится на d (если все коэффициенты $h(x)$ делятся на d, то $h(x)$ непримитивный)
Возьмём наименьший индекс j_0 такой, что b_{j_0} не делится на d (если все коэффициенты $h(x)$ делятся на d, то $h(x)$ непримитивный)
Рассмотрим коэффициент $a_{i_0+j_0}$ при степени $x^{i_0+j_0}$:
$a_{i_0+j_0} = c_0b_{i_0+j_0} + c_1b_{i_0+j_0-1} + ... + c_{i_0}b_{j_0} + c_{i_0+1}b_{j_0-1} + ... + c_{i_0+j_0}b_0$
Все члены до и после $c_{i_0}b_{j_0}$ делятся на d, а $c_{i_0}b_{j_0}$ на d не делится. Пришли к противоречию. чтд

Теорема (Критерий Эйзенштейна. Пусть $f(x) \in \mathbb{Z}[x], f(x) = a_nx^n + ... + ax_1 + a_0$. Если существует простое число p такое, что

1. p не делит a_n
2. p делит все остальные $a_i(i = 0, ..., n-1)$
3. p^2 не делит a_0

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

Доказательство. $f(x) \in \mathbb{Z}[x]$ и пусть выполняется условия критерия Эйзенштейна, то есть существует p, для которого выполняются условия 1) - 3) и при этом $f(x) = g(x)h(x), (f(x), g(x) \in \mathbb{Z}[x])$
$g(x) = b_kx^k + ... + b_1x + b_0(b_i \in \mathbb{Z}), h(x) = c_mx^m + ... + c_1x + c_0(c_i \in \mathbb{Z}) \in \mathbb{Z}[x]$
$a_0 = b_0c_0$
p^2 не делит $a_0 \Rightarrow$ либо $p|b_0$ b p не делит c_0 либо наоборот.
Пусть $p|c_0$ и p не делит b_0 (второй случай рассматривается аналогично).
$a_1 = b_1c_0 + c_1b_0$. Отсюда получаем, что так как $p|a_1$, то $p|c_1$.
$a_2 = b_2c_0 + c_1b_1 + c_2b_0$. Отсюда получаем, что $p|c_2$
...
$a_m = b_mc_0 + ... + b_0c_m \Rightarrow p|c_m$
Берём старший коэффициент $a_n = b_kc_m$
$p|c_m$ а значит $p|a_n$. Противоречие.

Теорема (о виде рациональных корней многочлена над $\mathbb{Z}$. Если $\frac{p}{q}$ является корнем многочлена $f(x) = a)nx^n + ... + a_1x + a_0$, то $q|a_n$ и $p|a_0$.

Доказательство. Пусть $\frac{p}{q}$ является корнем, p и q взаимно просты.
Просто подставляем: $f(\frac{p}{q}) = a_n(\frac{p}{q})^n + ... + a_q(\frac{p}{q}) + a_0 = 0$
$a_np^n + a_{n-1}p^{n-1}q + ... + a_1pq^{n-1} + a_0q^n = 0$
$a_np^n = -a_{n-1}p^{n-1}q - ... - a_1pq^{n-1} - a_0q^n$
$q|(a_np^n) \Rightarrow q|a_n$
$a_np^n + a_{n-1}p^{n-1}q + ... + a_1pq^{n-1} = -a_0q^n \Rightarrow p|a_0$
Противоречие. Чтд.