1.3. Разложение полинома на множители

Определение 1.3.1. *Алгебраическим уравнением* n*-й степени одной переменной* x называется уравнение вида

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0,$$

где $n \geq 1$, $a_0 \neq 0$, a_k, $k = \overline{0,n}$ — комплексные числа.

Теорема 1.3.1 (основная Теорема высшей алгебры). *Любое алгебраическое уравнение имеет, по крайней мере, один корень (вещественный или комплексный).*

Доказательство теоремы приведено в работе [А.Г.Курош «Курс высшей алгебры»].

Теорема 1.3.2. Любой полином $f(x)$, $\deg f(x) = n \geq 1$, с любыми числовыми коэффициентами имеет ровно n корней, если каждый корень считать столько раз какова его кратность.

Доказательство. Пусть $x = x_1$ является корнем полинома $f(x)$. Это означает, что $f(x) = (x - x_1) f_1(x)$, где $f_1(x)$ — полином степени n— 1. Если $n - 1 \geq 1$, то в соответствии с основной теоремой высшей алгебры полином $f_1(x)$ имеет хотя бы один корень, например, $x = x_2$. Тогда полином $f_1(x) = (x - x_2) f_2(x)$, следовательно, $f(x) = (x - x_1)(x - x_2) f_2(x)$. Продолжая подобные рассуждения, окончательно получаем, что $f(x) = a_0 (x - x_1)(x - x_2) \cdots (x - x_n)$. Заметим, что все числа x_i, $i = \overline{1,n}$, являются корнями полинома $f(x)$, так как для любого $i = \overline{1,n}$ справедливо равенство $f(x_i) = 0$.

Докажем теперь, что разложение полинома $f(x)$ на множители определяется однозначно с точностью до порядка сомножителей. Доказательство этого факта проведем от противного.

Пусть существует другое *разложение полинома* $f(x)$ *на множители*, т. е. $f(x) = a_0 (x - x_1')(x - x_2') \cdots (x - x_n')$. Допустим, что среди корней x_i, $i = \overline{1,n}$, существует такой корень x_k, что $x_k \neq x_j'$, для любого $j = \overline{1,n}$. Подставляя x_k в очевидное равенство $(x - x_1)(x - x_2) \cdots (x - x_n) = (x - x_1')(x - x_2') \cdots (x - x_n')$, получаем, что выражение слева обращается в нуль, а справа стоит произведение, отличное от нуля. Таким образом, для любого $i = \overline{1,n}$ существует такое $j = \overline{1,n}$, что $x_i = x_j'$. Однако, из этого еще не следует, что разложение полинома $f(x)$ на множители определяется однозначно, так как корни x_i для различных $i = \overline{1,n}$ могут совпадать.

Допустим, что среди корней x_i существует ровно m, равных x_1, в то время как среди корней x_j' имеется только l, равных x_1. Предположим, что $m > l$. Приравнивая различные разложения полинома $f(x)$, получаем равенство $(x - x_1)^m f_m(x) = (x - x_1)^l f_l(x)$, причем $f_m(x_1) \neq 0$, $f_l(x_1) \neq 0$. Сокращая обе части этого соотношения на общий множитель $(x - x_1)^l$, получаем $(x - x_1)^{m-l} f_m(x) = f_l(x)$. Заметим, что при подстановке в последнее равенство $x = x_1$ левая часть обращается в нуль, в то время как правая отлична от нуля. Отсюда следует, что $m = l$.

Если объединить сомножители, отвечающие совпадающим корням, то полином

$$f(x) = a_0 (x - x_1)^{k_1} (x - x_2)^{k_2} \cdots (x - x_s)^{k_s},$$

где $k_1 + k_2 + ... + k_s = n$, а $x_1, x_2, ..., x_s$ — различные корни полинома $f(x)$.

Таким образом, полином степени n не может иметь более чем n корней.

Теорема 1.3.3. *Если полиномы* $f(x)$, $\deg f(x) \le n$ и $g(x)$, $\deg g(x) \le n$ *имеют совпадающие значения в более чем* n *различных точках, то* $f(x) = g(x)$.

<u>Доказательство.</u> Рассмотрим полином $h(x) = f(x) - g(x)$. Очевидно, что $\deg h(x) \le n$. Но по условию теоремы полином $h(x)$ обращается в нуль в более чем n различных точках. Однако у этого полинома не может быть корней больше чем n. Поэтому $h(x) \equiv 0$, т. е. $f(x) \equiv g(x)$.