Лекция №15

2 Теория колец

2.6 Факторизация многочленов

Определение 1. *Пусть R – кольцо целостности. Необратимый ненулевой многочлен $f(X) \in R[X]$ называется неприводимым над R, если $f(X) \neq g(X) \cdot h(X)$, где $g(X) \neq const, h(X) \in R[X]$.*

Теорема 1. *Пусть F – поле. Если $f(X) \in F[X]$ и $\deg f = 2$ или 3. Многочлен f приводим над F тогда и только тогда, когда $f(X)$ имеет ноль в F.*

Определение 2. *Содержанием ненулевого многочлена вида $a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ является НОД$(a_n, a_{n-1}, ..., a_0)$. Примитивным многочленом с коэффициентами из $\mathbb{Z}$ является многочлен с содержанием $= 1$.*

Лемма 1 (Гаусса)**.** *Произведение двух примитивных многочленов есть примитивный многочлен.*

Пусть $f(X) \in \mathbb{Z}[X]$. Если f неприводим над $\mathbb{Q}$, то f неприводим над $\mathbb{Z}$.

Теорема 2. *Пусть p – простое, $f(X) \in \mathbb{Z}[X], \deg f \geq 1$ и $\bar{f}(X) \in \mathbb{Z}_p[X]$ – многочлен, полученный из f редукцией его коэффициентов по модулю p. Если $\bar{f}(X)$ неприводим над F_p и $\deg \bar{f} = \deg f$, то $f(X)$ неприводим над $\mathbb{Q}$.*

Теорема 3 (Критерий Эйзенштейна)**.** *Пусть $f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in \mathbb{Z}[X]$. Если существует простое p, такое, что $p \nmid a_n, p|a_{n-1}, ..., p|a_0, p^2 \nmid a_0$, то f неприводим над $\mathbb{Q}$.*

Следствие 1. *Для любого простого p многочлен, называемый круговым или циклотоническим, $\Phi_p(X) = \frac{X-1}{X+1} = X^{p-1} + X^{p-2} + ... + X + 1$ неприводим над $\mathbb{Q}$.*

Теорема 4. *Пусть F – поле, $f(X) \in F[X]$. Идеал $(f(X))$ является максимальным в $F[X]$ тогда и только тогда, когда $f(X)$ неприводим над F.*

Следствие 2. *Пусть F – поле, $f(X)$ – неприводимый многочлен над F. Тогда $F[X]/(f(X))$ – поле.*

Следствие 3. *Пусть $f(x), g(X), h(X) \in F[X]$. Если f неприводим над F и $f|g \cdot h$, то* $\left[\begin{array}{c} f|g \\ f|h \end{array} \right.$.

Теорема 5. *Любой многочлен в $\mathbb{Z}[X]$, не являющийся ни нулем, ни константой, может быть записан в следующем виде $b_1 \cdot b_2 \cdot ... \cdot b_s \cdot f_1(X) \cdot f_2(X) \cdot ... \cdot f_m(X)$, где $b_i = const$. f_j - неприводимые многочлены. Кроме того, если $b_1 \cdot b_2 \cdot ... \cdot f_1(X) \cdot f_2(X) \cdot ... \cdot f_m(X) = c_1 \cdot c_2 \cdot ... \cdot c_t \cdot g_1(X) \cdot g_2(X) \cdot ... \cdot g_n(X)$, то $s = t, m = n, |b_i| = c_i, |f_j| = g_j$.*