2 Теория колец

2.5 Полиномиальные кольца

Основные определения

Определение 1. *Пусть R - коммутативное кольцо $R[X] = \{a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \big| a_i \in R\}, n \in \mathbb{N}$ - кольцо многочленов над R от переменной X.*

Определение 2. *Пусть R - коммутативное кольцо, $f(X), g(X) \in R[X]$ - полиномиальные кольца. Тогда $f(X) \cdot g(X) = c_{m+n}X^{m+n} + ... + c_1X + c_0, f(X) + g(X) = (a_s + b_s)X^s + ... + (a_1 + b_1)X + a_0 + b_0$*

Теорема 1. *Если D - кольцо целостности, то $D[X]$ - кольцо целостности.*

Алгоритм деления

Теорема 2. *Пусть F - поле и $f(X), g(X) \in F[X]$. Тогда $\exists! q(X), r(X) \in F[X] \big| f(X) = g(X) \cdot q(X) + r(X)$. Либо $r(X) = 0$, либо $\deg r < \deg g$.*

Следствие 1. *a - нуль $f(X) \Leftrightarrow (X - a)$ - множитель $f(X)$.*

Следствие 2. *Многочлен степени n, определенный над некоторым полем, имеет не более n нулей с учетом их кратности.*

Определение 3. *Кольцо главных идеалов - кольцо целостности, в котором любой идеал главный.*

Теорема 3. *Пусть F - поле, I - ненулевой идеал в $F[X]$ и $g(X) \in F[X]$. Тогда $I = (g(X)) \Leftrightarrow g(X)$ - ненулевой многочлен минимальной степени в I.*

2.6 Факторизация многочленов

Определение 4. *Пусть D - кольцо целостности. Необратимый ненулевой многочлен $f(X) \in D[X]$ называется неприводимым над D, если $f(X) \neq g(X) \cdot h(X)$, где $g(X) \neq const, h(X) \in D[X]$.*

Теорема 4. *Пусть F - поле. Если $f(X) \in F[X]$ и $\deg f = \left[\begin{array}{l} 2 \\ 3 \end{array} \right.$, то f приводимо над $F \Leftrightarrow f(X)$ имеет ноль в F.*

Определение 5. *Содержание ненулевого многочлена вида $a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$, это НОД$(a_n, a_{n-1}, ..., a_0)$.*
Примитивный многочлен - это многочлен из $\mathbb{Z}[X]$ с содержанием $= 1$.

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

Доказательство. Рассмотрим $f(X)$ и $g(X)$ - примитивные
От противного:
Пусть $f(X) \cdot g(X)$ - не является примитивным многочленом
Пусть простое $p | content(f \cdot g)$
Если $\mathbb{Z}_p[X] = F_p[X] \Rightarrow \overline{f}(X), \overline{g}(X)$ создаются классами $f(X), g(X)$

$\Rightarrow f(X) \cdot g(X) \to \overline{f(X) \cdot g(X)}$
$\mathbb{Z}_p[X]$ - кольцо целостности
$\overline{f}(X) \cdot \overline{g}(X) = \overline{f(X) \cdot g(X)} = 0$
$\Rightarrow \left[\begin{array}{l} \overline{f}(X) = 0 \\ \overline{g}(X) = 0 \end{array} \right.$, так как $F_p[X]$ - кольцо целостности
$\Rightarrow \left[\begin{array}{l} p|content(f) \\ p|content(g) \end{array} \right. \Rightarrow$ противоречие
$\Rightarrow f(X) \cdot g(X)$ - примитивный $\square$

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

Тесты на неприводимость

Теорема 5. *Пусть p - простое и $f(X) \in \mathbb{Z}[X], \deg f \geq 1, f(X) \in \mathbb{Z}_p[X] = F_p[X](mod\ p)$. Если $\overline{f(X)}$ неприводим на F_p и $\deg \overline{f}$, то $f(X)$ - неприводим над $\mathbb{Q}$.*

Замечание 1. *Если $f(X) \in \mathbb{Z}[X]$ и $\overline{f}(X)$ неприводим над F_p, то в обратную сторону выполняется не всегда.*

Теорема 6 (Критерий Эйзенштейна)**.** *Пусть $f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in \mathbb{Z}[X]$. Если $\exists p$ - простое $\big| p \not| a_n, p|a_{n-1}, ..., p|a_0, p^2 \not| a_0$, то f неприводима над $\mathbb{Q}$.*

Доказательство. От противного
Пусть $f(X)$ - приводим над $\mathbb{Q}$
$\Rightarrow \exists g, h \in \mathbb{Z}[X] \big| f(X) = g(X) \cdot h(X)$ и $\deg g, \deg h \geq 1$
По условию $p|a_0, p^2 \not| a_0$
$a_0 = b_0 \cdot c_0 \Rightarrow \left[\begin{array}{l} p|b_0 \\ p|c_0 \end{array} \right.$
По условию $p \not| a_n = b_r \cdot c_s \Rightarrow \left[\begin{array}{l} p \not| b_r \\ p \not| c_s \end{array} \right.$
$\Rightarrow f$ - нериводим, так как противоречие. $\square$

Следствие 3. *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 7. *Пусть F - поле, $f(X) \in F[X]$. Тогда $(f(X))$ - max в $F[X] \Leftrightarrow f(X)$ - неприводим над F.*

Следствие 4. ${}^{F[X]}/_{(f(X))}$ *- поле.*

Следствие 5. *$f(x), g(X), h(X) \in F[X]$. Если f неприводим над F и $f|g \cdot h$, то $\left[\begin{array}{l} f|g \\ f|h \end{array} \right.$*

Теорема 8. *Любой многочлен в $\mathbb{Z}[X]$, не являющимся 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 $s = t, m = n, |b_i| = c_i, |f_j| = g_j$.*