Оглавление

0.1 Кольцо многочленов, деление многочленов с остатком 1
0.1.1 Деление многочленов с остатком 3

Лекция 10

10.11.2023

0.1 Кольцо многочленов, деление многочленов с остатком

Теорема 1. $A[x]$ – является кольцом

Доказательство. Проверим дистрибутивность (остальное – упр):
$(P+Q)R = PR + QR$
$P = (a_0, a_1, \ldots); \quad Q = (b_0, b_1, \ldots)$
$R = (c_0, c_1, \ldots)$
$P + Q = (a_0 + b_0, a_1 + b_1, \ldots)$
$(P+Q)R = (\ldots, (a_0+b_0)c_k + (a_1+b_1)c_{k-1} + \ldots + (a_k+b_k)c_0, \ldots)$
$PR = (\ldots, a_0c_k + a_1c_{k-1} + \ldots + a_kc_0, \ldots)$
$QR = (\ldots, b_0c_k + b_1c_{k-1} + \ldots + b_kc_0, \ldots)$
$PR + QR = (\ldots, a_0c_k + a_1c_{k-1} + \ldots + a_kc_0 + b_0c_k + \ldots + b_kc_0, \ldots)$ □

Обозначение: Пусть $a \in A$. Элемент a отождествляется $(a, 0, 0, \ldots)$
Корректность: $a, b \in A \Rightarrow a + b$ и ab в A и в $A[x]$ согласованны

Свойства. Пусть A – ассоциативное кольцо с 1

1. Пусть $b \in A, P \in A[x]; \quad P = (a_0, a_1, \ldots)$
   Тогда $bP = (ba_0, ba_1, \ldots)$
2. Пусть $P \in A[x], P = (a_0, a_1, \ldots)$
   Тогда $xP = (0, a_0, a_1, \ldots)$
3. $x^n = (0, 0, \ldots, 1_n, 0, \ldots)$

Доказательство.

1. $b = (b, 0, 0, \ldots), P = (a_0, a_1, \ldots)$
   Пусть $bP = (c_0, c_1, \ldots)$
   $c_k = ba_k + 0a_{k-1} + \ldots + 0a_0 = ba_k$
2. Пусть $(0, 1, 0, \ldots)(a_0, a_1, \ldots) = (c_0, c_1, \ldots)$
   $c_0 = 0, a_0 = 0$
   При $k \geq 1 : c_k = 0a_k + 1a_{k-1} + 0a_{k-1} + \ldots = 1a_{k-1} = a_{k-1}$
3. Из (2) (n раз применяем свойство 2)

□

Обозначение: Будем использвать обозначение $P(x) = a_0 + a_1x + \ldots + a_nx^n$ для $P = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$

Определение 1. Пусть $P = (a_0, a_1, \ldots)$ − многочлен не равный 0
Степенью P называют $\max\{k \mid a_k \neq 0\}$
Обозначение: $\deg P$
Если P − нулевой многочлен, считаем $\deg P = -\infty$

Напоминание: Кольцо A называется областью целостности, если оно ассоциативно, коммутативно и если $ab = 0$, то $a = 0$ или $b = 0$

Теорема 2. Пусть A − область целостности
Тогда

1. $\deg(P + Q) \leq \max\{\deg P, \deg Q\}$
2. $\deg(PQ) = \deg P + \deg Q$
3. $A[x]$ − область целостности

Доказательство. Пусть $P = (a_0, a_1, \ldots); \quad Q = (b_0, b_1, \ldots)$

1. Пусть $N = \max\{\deg P, \deg Q\}$
   При $k > N : \quad a_k = 0, b_k = 0 \Rightarrow a_k + b_k = 0$
2. При $P = 0$ или $Q = 0 : -\infty = -\infty + \ldots$
   Считаем $P \neq 0, Q \neq 0$
   Пусть $k = \deg P, m = \deg Q$
   Пусть $PQ = (c_0, c_1, \ldots)$
   $c_{k+m} = \sum\limits_{i+j=k+m} a_ib_i$
   При $i = k, j = m : \quad a_kb_k$
   При $i < k, j > m : \quad a_i * 0 = 0$
   При $i > k, j < m : \quad 0 * b_i = 0$
   Пусть $N > k + m; \quad c_n = \sum\limits_{i+j=N} a_ib_i = 0 + 0 + \ldots = 0$
   Для любого слагаемого $i > k$ или $j > m$
3. Коммутативность − упражнение

Ассоциативность: $P = (a_0, a_1, \ldots); \quad Q = (b_0, b_1, \ldots); \quad R = (c_0, c_1, \ldots)$
Пусть $T - PQ, T = (d_0, d_1, \ldots)$
$S = (PQ)R = (e_0, e_1, \ldots)$

$$e_k = \sum_{i+j=k} d_i c_i = \sum_{i+j=k, l+m=i} a_l b_m c_j = \sum_{l+m+j=k} a_l b_m c_j$$

$$d_i = \sum_{l+m=i} a_l b_m$$

Аналогично $P(QR)$
Если $P \neq 0, Q \neq 0$, то $degPQ = degP + degQ \neq -\infty \Rightarrow PQ \neq 0$

□

Определение 2. Пусть A – коммутативное, ассоциативное кольцо
$P \in A[x], P = (a_0, a_1, , a_2 \ldots)$ и $c \in A$
Значением P в c (или при $x = c$) называется $a_0 + a_1 c + a_2 c^2 + \ldots \in A$
Обозначение: $P(c)$

Свойства. Пусть $P, Q \in A[x], F = P + Q, G = PQ$
Тогда $F(c) = P(c) + Q(c); \quad G(c) = P(c)Q(c)$

0.1.1 Деление многочленов с остатком

Определение 3. Пусть K – поле, $F, G \in K[x], G \neq 0$
Если для $Q, R \in K[x]$ выполнено $F = QG + R, \deg R < \deg G$,
то Q и R назвается неполным частным и остатком от деления F на G

Теорема 3. (Деление многочленов с остатком)
Пусть K – поле, $F, G \in K[x], G \neq 0$
Тогда существует единственные Q, R, такие что $F = QG + R, \deg R < \deg G$

Доказательство. 1. **Существование**
Положим, $A = \{F(x) - T(x)G(x) \mid T \in K[x]\}$
Пусть R – элемент A имеет ctпень $Q : R = F - QG$
Докажем, что $\deg R < \deg G$
Пусть:

$$Q = a_n x^n + a_{n-1} x^{n-1} + \ldots, R(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots$$

$\Rightarrow m \geq n$
Положим $R_1(x) = R(x) - \dfrac{b_n}{a_n} x^{m-n} G(x)$

Тогда

$$R_1(x) \in AR_1(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots - \frac{b_m}{a_n}x^{m-n}a_n x^n - \frac{b_m}{a_n}x^{m-n}a_{n-1}x^{n-1} - \ldots$$

$\deg R_1 < m = \deg R$
Противоречие с выбором R

2. **Единственность**
Пусть: $F = GQ_1 + R_1; \quad F = GQ_2 + R_2; \quad degR_1, degR_2 < degG$
$GQ_1 + R_1 = GQ_2 + R_2$
$G(Q_1 - Q_2) = R_2 - R_1$
$\deg(R_2 - R_1) \leq \max\{degR_1, degR_2\} < \deg G$
$\deg(G(Q_1 - Q_2)) = defG - \deg(Q_1 - Q_2)$
$\Rightarrow Q_1 - Q_2 = 0 \Rightarrow Q_1 = Q_2 \Rightarrow R_1 = R_2$

□

Теорема 4. Безу
Пусть K – поле, $F \in K[x], c \in K$,тогда
Тогда остаток от деления $F(c)$ на $x - c$ равен $F(c)$

Доказательство. Остаток – многочлен степени < 1
$F(x) = (x - c)Q(x) + r$ Подставим $x = c$:
$F(c) = (c - c)Q(c) + r \Rightarrow F(c) = r$ □

Следствие: c – корень $F(x) \Leftrightarrow F(x) \vdots x - c$

Доказательство. $F(x) \vdots x - c \Rightarrow r = 0 \Rightarrow F(c) = 0$ □

Теорема 5. (о количестве корней многочлена)
Пусть K – поле, $F \in K[x], F \neq 0$
Тогда количество корней $F(x)$ не превосходит $\deg F$

Доказательство. Докажем, что у многочлена степени n не более n корней:

По индукции:

- База: $n = 0; \quad F(x) = a_0; \quad a_0 \neq 0 \Rightarrow$ нет корней
- Переход $n \to n + 1$: Пусть $\deg F = n + 1$
Если у F нет корней – верно
Пусть c – корень $F(x) \Rightarrow$ (теорема Безу) $F(x) \vdots x - c \Rightarrow$
$\Rightarrow F(x) = (x - c)Q(x)$
$degF = \deg(x - c) + degQ \Leftrightarrow n + 1 = 1 + degQ \Rightarrow$
$\Rightarrow degQ = n \Rightarrow$ у $Q(x)$ не более n – корней $(x_1, \ldots, x_k); \quad k$
Пусть x_0 – корень $F \Rightarrow 0 = F(x_0) = (x_0 - c)Q(x_0) \Rightarrow$

$\Rightarrow x_0 = c$ или x_0 – корень $Q(x) \Rightarrow$ есть корень $(x_1, \ldots, x_k, c)$

□

Следствие (формальное и функциональное равенство многочлена):
Пусть K – бесконечное поле, $F, G \in K[x]$
Если для любого $c \in K$ выполнено $F(c) = G(c)$ (функциональное), то $F = G$ (формальное)
(функциональное) $\rightarrow$ (формальное) всегда. наоборот не всегда

Доказательство. Пусть $F \neq G, H = F - G \Rightarrow H \neq 0$
$\Rightarrow$ у H не более чем $degH$ корней $\Rightarrow \exists c : H(c) \neq 0$
$\Rightarrow F(c) - G(c) \neq 0 \Rightarrow F(c) \neq G(c)$
Замечание: Верное не всегда
$K = \mathbb{Z}_p, p \in \mathbb{P}$
$F(x) = x^p - p, G(x) = 0$
$F(c) = G(c), F \neq G$ □