Лекция 9

Кольцо многочленов

Содержание лекции:
В настоящей лекции мы кратко рассмотрим основные понятия, связанные с кольцом многочленов и операциями в нем. Данная структура является основополагающей ряда разделов математики и часто служит источником нетривиальных примеров для алгебры и анализа.

Ключевые слова:
Многочлен, коэффициенты многочлена, степень многочлена, сумма и произведение многочленов, ассоциированные многочлены, делимость, остаток от деления, корень многочлена.

Авторы курса:

Трифанов А.И. Москаленко М.А.

Ссылка на ресурсы:

9.1 Основные определения

Nota bene Пусть $\Bbbk$ - некоторое поле.

Многочленом от одной переменной с коэффициентами из поля $\Bbbk$ будем называть бесконечную формальную сумму следующего вида:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots,$$

в которой отличны от нуля только *некоторые* **коэффициенты** $a_0, a_1, a_2, \ldots \in \Bbbk$, а x называется **формальной переменной**.

Nota bene Множество многочленов от переменной x будем обозначать через $\Bbbk[x]$. Пусть далее $p, q \in \Bbbk[x]$, так что

$$p(x) = \sum_{n=0}^{\infty} a_n x^n, \quad q(x) = \sum_{m=0}^{\infty} b_m x^m,$$

Суммой двух многочленов p и q называется такой многочлен $h = p + q$, что

$$h(x) = \sum_{k=0}^{\infty} c_k x^k, \quad c_k = a_k + b_k.$$

Произведением двух многочленов p и q называется такой многочлен $g = p \cdot q$, что

$$g(x) = \sum_{j=0}^{\infty} d_j x^j, \quad d_j = \sum_{i=0}^{j} a_i b_{j-i}.$$

Теорема 9.1. *Множество $\Bbbk[x]$, наделенное операциями сложения и умножения является коммутативным ассоциативным кольцом.*

►

Проверим аксиомы кольца:

- $(\Bbbk[x], +)$ - абелева группа, в которой
$$0(x) = 0, \quad (-p)(x) = -p(x).$$
- $(\Bbbk[x], \cdot)$ - коммутативный моноид, в котором $1(x) = 1$.
- Пусть $p, q, r \in \Bbbk[x]$, проверим дистрибутивность:
$$(p+q) \cdot r = \sum_{k=0} d_k x^k, \quad p \cdot r = \sum_{n=0} \alpha_n x^n, \quad q \cdot r = \sum_{m=0} \beta_m x^m.$$
тогда имеет место
$$d_k = \sum_{i=0}^{k} (a_i + b_i) c_{k-i} = \sum_{i=0}^{k} (a_i c_{k-i}) + \sum_{i=0}^{k} (b_i c_{k-i}) = \alpha_k + \beta_k,$$

◄

Лемма 9.1. *Отображение $\sigma : \Bbbk \to \Bbbk[x]$, так что $\alpha \mapsto \alpha \cdot 1(x)$, является вложением.*

►
Очевидно, что $\sigma \in \mathrm{Hom}(\Bbbk, \Bbbk[x])$ и далее

$$\alpha \in \ker \sigma \quad \Rightarrow \quad \sigma(\alpha) = \alpha \cdot 1(x) = \alpha \cdot 1 + 0 \cdot x + \ldots = 0.$$

◄

Nota bene Под записью $\alpha \cdot p(x), \alpha \in \Bbbk$ понимают многочлен $\sigma(\alpha) \cdot p(x)$.

Два многочлена p и q называются **ассоциированными** (обозначают $p \sim q$), если

$$\exists\, \alpha \in \Bbbk, \quad \alpha \neq 0 : \quad p = \alpha \cdot q.$$

Лемма 9.2. *Ассоциированность - отношение эквивалентности.*

Nota bene Классы в $\Bbbk[x]/_\sim$ по этому отношению составляют многочлены, отличающиеся на скалярный множитель.

9.2 Степень многочлена

Степенью $\deg(p)$ многочлена $p \in \Bbbk[x]$ называется максимальный номер его ненулевого коэффициента. Если $\deg p = n \in \mathbb{N}_0$ то коэффициент a_n называется **старшим коэффициентом** многочлена p.

Nota bene Для нулевого многочлена $0(x)$ положим $\deg(0) = -\infty$.

Лемма 9.3. *Пусть $p, q \in \Bbbk[t]$ тогда имеют место следующие свойства:*

$$\deg(p \cdot q) = \deg(p) + \deg(q), \quad \deg(p+q) \leq \max\{\deg(p), \deg(q)\}.$$

►
Пусть $\deg(p) = n$ и $\deg(q) = m$, и при этом

$$p = \sum_i a_i x^i, \quad q = \sum_j b_j x^j, \quad p \cdot q = \sum_k c_k x^k,$$

тогда будем иметь

$$c_{n+m} = \sum_{i=0}^{n-1} a_i b_{n+m-i} + a_n b_m + \sum_{i=n+1}^{n+m} a_i b_{n+m-i} = a_n b_m \neq 0.$$

При $k > n+m$ имеем $c_k = 0$ и, следовательно, $\deg(p \cdot q) = n+m$.
При $k > \max\{\deg(p), \deg(q)\}$ следует доказательство второго свойства:

$$a_k = b_k = 0 \quad \Rightarrow \quad c_k = a_k + b_k = 0.$$

◄

9.3 Делимость в кольце многочленов

Теорема 9.2. *Пусть $p, q \in \Bbbk[x]$, причем $q \neq 0$, тогда*

$$\exists!\, g, r \in \Bbbk[x]: \quad p = g \cdot q + r, \quad \deg(r) < \deg(q).$$

▶
Пусть $\deg(p) = n$ и $\deg(q) = m$, а также

$$p(x) = a_n x^n + \ldots + a_0, \quad q(x) = b_m x^m + \ldots + b_0.$$

Используем индукцию по n. В качестве базы при $n < m$ подходит $g = 0, \quad r = p$. Пусть теперь $n \geq m$ и для многочленов степени меньшей n утверждеие доказано. Так как

$$\tilde{p}(x) = p(x) - \frac{a_n}{b_m} x^{n-m} q(x), \quad \deg(\tilde{p}) < n,$$

то по индукционному предположению

$$\tilde{p} = g_1 \cdot q + r, \quad \deg(r) < m \quad \Rightarrow \quad p(x) = \left(g_1(x) + \frac{a_n}{b_m} x^{n-m} \right) q(x) + r(x).$$

Теперь докажем единственность. Пусть

$$g_1 q + r_1 = p = g_2 q + r_2, \quad \deg(r_1) < m, \quad \deg(r_2) < m \quad \Rightarrow \quad r_1 - r_2 = q \cdot (g_2 - g_1).$$

При $g_1 \neq g_2$, имеем:

$$\deg\left((g_2 - g_1)q\right) = \deg(g_2 - g_1) + \deg(q) \geq m,$$
$$\deg(r_1 - r_2) \leq \max\left(\deg(r_1), \deg(r_2)\right) < m.$$

Противоречие. Значит $g_1 = g_2$ и $r_1 = r_2$.
◀

Говорят, что многочлен q **делит многочлен** p (пишут $q \,|\, p$), если существует такой многочлен h, что $p = h \cdot q$.

Лемма 9.4. *Свойства делимости в $\Bbbk[x]$:*

1. *Если $q \,|\, p$ и $r \,|\, q$, тогда $r \,|\, p$:*
$$f = pg, \quad g = qh \quad \Rightarrow \quad f = (pq)h.$$
2. *Пусть $r \,|\, p, q$, тогда $\quad \forall g_1, g_2 \in \Bbbk[t] \quad r \,|\, (g_1 p + g_2 q)$:*
$$p = \alpha \cdot r, \quad q = \beta \cdot r, \quad \alpha, \beta \in \Bbbk[x] \quad \Rightarrow \quad g_1 p + g_2 q = (\alpha \cdot g_1 + \beta \cdot g_2) \cdot r.$$
3. *Пусть $q \,|\, p$, причем $p, q \neq 0$, тогда $\deg(p) \geq \deg(q)$:*
$$p = gq, \quad g \in \Bbbk[t], \quad g \neq 0 \quad \Rightarrow \quad \deg(p) = \deg(g) + \deg(q) \geq \deg(g).$$

Лемма 9.5. *Ассоциированность и делимость:*

1. *Пусть $q \,|\, p, \quad p, q \neq 0$ и $\deg(p) = \deg(q)$, тогда $p \sim q$:*
$$\deg(q) = \deg(p) = \deg(g) + \deg(q) \quad \Rightarrow \quad \deg(g) = 0 \quad \Rightarrow \quad g \in \Bbbk.$$
2. *Пусть $q \,|\, p, \quad p, q \neq 0$ и $p \,|\, q$, тогда $p \sim q$:*
$$\deg(p) \geq \deg(q), \quad \deg(q) \geq \deg(p) \quad \Rightarrow \quad \deg(p) = \deg(q).$$

9.4 Корень многочлена

Пусть $p \in \Bbbk[x]$ и $\alpha \in \Bbbk$. Число α называется **корнем** многочлена p степени m, если

$$(x-\alpha)^m \mid (p(x), \quad (x-\alpha)^{m+1} \nmid p(x).$$

Теорема 9.3. *(Безу) Остаток от деления $p \in \Bbbk[x]$ на $(x-\alpha)$ равен $p(\alpha)$*

►

По теореме от делении с остатком имеем:

$$p(x) = (x-\alpha)g(x) + r(x), \quad \deg(r) \leq \deg(x-\alpha) = 1.$$

Следовательно, $r(x) = r \in \Bbbk$ и

$$p(\alpha) = 0 \cdot g(\alpha) + r.$$

◄

Nota bene Если $p \in \Bbbk[x]$ и α - корень $p(x)$, тогда $(x-\alpha) \mid p(x)$.

Теорема 9.4. *(ОТА) Любой многочлен из $\mathbb{C}[x]$ имеет корень из $\mathbb{C}$.*