ζ

Лекция 6

Начало алгебры 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:
`mathdep.ifmo.ru/geolin`

6.1 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 6.1. *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 6.1. *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 $\sigma(\alpha) \cdot p(x)$.

6.2 Делимость в кольце многочленов

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 6.2. *Ассоциированность - отношение эквивалентности.*

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

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 **сташим коэффициентом** многочлена p.

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

Лемма 6.3. *Пусть $p, q \in \Bbbk[t]$ тогда имеют место следующие свойства:*

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

▶

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 $k > \max\left\{\deg(p), \deg(q)\right\}$ следует доказательство второго свойства:

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

◀

Теорема 6.2. *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. При $n < m$ в качестве базы подходит

$$g = 0, \quad r = p.$$

Пусть $n \geq m$ и для многочленов степени меньшей n утверждеие доказано. Так как

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

то по индукционному предположению

$$\tilde{p} = g_1 \cdot q + r, \quad \deg(r) < m,$$

но тогда сразу получаем искомое представление:

$$p(t) = \left(g_1(t) + \frac{a_n}{b_m} x^{n-m} \right) q(t) + r(t)$$

Теперь докажем единственность. Пусть

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

Тогда

$$r_1 - r_2 = q \cdot (g_2 - g_1).$$

При $g_1 \neq g_2$, имеем:

$$\deg\left((g_2 - g_1)q\right) = \deg(g_2 - g_1) + \deg(q) \geq m.$$

С другой стороны:

$$\deg(r_1 - r_2) \leq \max\left(\deg(r_1), \deg(r_2)\right) < m.$$

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 6.4. *Если $q \,|\, p$ и $r \,|\, q$, тогда $r \,|\, p$.*
►
Из условия следует, что

$$f = pg, \quad g = qh \quad \Rightarrow \quad f = (pq)h.$$

◄

Лемма 6.5. *Пусть* $f, g \,\vdots\, h$, *тогда*

$$\forall p, q \in K[t] \quad (pf + qg) \,\vdots\, h.$$

▶
Имеем

$$f = \alpha h, \quad g = \beta h, \quad \alpha, \beta \in K[t] \quad \Rightarrow \quad fp + gq = (\alpha p + \beta q)h.$$

◀

Лемма 6.6. *Пусть* $f \,\vdots\, g$, *причем* $f, g \neq 0$, *тогда*

$$\deg(f) \geq \deg(g).$$

▶
Из условия следует, что

$$f = gh, \quad \in K[t], \quad h \neq 0 \quad \Rightarrow \quad \deg(f) = \deg(g) + \deg(h) \geq \deg(g).$$

◀

Лемма 6.7. *Пусть* $f \,\vdots\, g$, $f, g \neq 0$ *и* $\deg(f) = \deg(g)$, *тогда* $f \sim g$.
▶
Из условий следует $f = gh$, $h \in K[t]$ и

$$\deg(g) = \deg(f) = \deg(g) + \deg(h) \quad \Rightarrow \quad \deg(h) = 0 \quad \Rightarrow \quad h \in K.$$

◀

Лемма 6.8. *Пусть* $f \,\vdots\, g$, $f, g \neq 0$ *и* $g \,\vdots\, f$, *тогда* $f \sim g$.
▶
Имеем

$$\deg(f) \geq \deg(g), \quad \deg(g) \geq \deg(f) \quad \Rightarrow \quad \deg(f) = \deg(g).$$

◀

6.3 Корень многочлена

> Пусть $f \in K[t]$ и $\alpha \in K$. Число α называется **корнем** многочлена f степени m, если
> $$f(t) \,\vdots\, (t - \alpha)^m, \quad f(t) \not\vdots\, (t - \alpha)^{m+1}.$$

Лемма 6.9. *Остаток от деления $f \in K[t]$ на $(t-\alpha)$ равен $f(\alpha)$*

▶

По теореме от делении с остатком имеем:

$$f(t) = (t-\alpha)q(t) + r(t), \quad \deg(r) \leq \deg(t-\alpha) = 1$$

Следовательно, $r(t) = r \in K$ и

$$f(\alpha) = 0 \cdot q(t) + r.$$

◀

Nota bene Если $f \in K[t]$ и α - корень $f(t)$, тогда $f(t) \vdots (t-\alpha)$.

Теорема 6.3. *(основная теорема алгебры) Любой многочлен из $\mathbb{C}[t]$ имеет корень из $\mathbb{C}$.*

Nota bene Пусть $f(t) \in \mathbb{C}[t]$, $\deg(f) = n$ и c - старший коэффициент f, тогда

$$f(t) = c(t-\alpha_1)(t-\alpha_2)\ldots(t-\alpha_n), \quad \alpha_j \in \mathbb{C},$$

причем не обязательно все α_j различны.

Nota bene Рассмотрим автоморфизм $\sigma : \mathbb{C}[t] \to \mathbb{C}[t]$, индуцированный операцией комплексного соряжения в $\mathbb{C}$:

$$\sigma(f(t)) = \bar{f}(t) = \bar{a}_n t^n + \ldots + \bar{a}_1 t + \bar{a}_0, \quad f(t) = a_n t^n + \ldots + a_1 t + a_0.$$

Лемма 6.10. *Пусть $f \in \mathbb{C}[t]$ и $\alpha \in \mathbb{C}$ - корень f кратности m. Тогда $\bar{\alpha}$ - корень $\bar{f}$ той же кратности m.*

▶

Из условия леммы имеем:

$$f(t) = (t-\alpha)^m g(t) \quad \Rightarrow \quad \bar{f}(\bar{t}) = (\bar{t}-\bar{\alpha})^m \cdot \bar{g}(\bar{t}).$$

Но это значит, что $\bar{\alpha}$ - корень $\bar{f}$ кратности k не меньшей m. Далее, $\alpha = \bar{\bar{\alpha}}$ - корень $f = \bar{\bar{f}}$ кратности не меньшей k, откуда $k = m$. ◀

Теорема 6.4. *Многочлен $f \in \mathbb{R}[t]$ степени $\deg(f) = n \geq 1$ со старшим коэффициентом c раскладывается в $\mathbb{R}[t]$ на множители:*

$$f(t) = c(t-\alpha_1)^{k_1}\ldots(t-\alpha_s)^{k_s} \cdot (t^2+p_1 t+q_1)^{m_1}\ldots(t^2+p_r t+q_r)^{m_r},$$
$$D(t^2+p_i t+q_i) = p_i^2 - 4q_i < 0, \quad i = 1\ldots r.$$

Лемма 6.11. *Многочлен $f \in \mathbb{R}[t]$ нечетной степени всегда имеет действительный корень.*

▶

Согласно предыдущей теореме, сумма кратностей всех комплексных корней f равна $\deg(f)/2$, а сумма кратностей невещественных корней четна. Следовательно, кратность вещественных корней нечетна и значит такие корни есть.

◀