$\mathcal{E}$

Лекция 6

Алгебра скалярных полиномов

Содержание лекции:
В настоящей лекции мы кратко обсуждаем структуру алгебры скалярных полиномов. Основной интерес для нас здесь представляют специальные подмножества алгебры - идеалы. Идеал обладает рядом интересных свойств и позволяет очень компактно и изящно выразить некоторые утверждения о подмножествах алгебры полиномов, которыми мы будем пользоваться в дальнейшем.

Ключевые слова:
Пространство полиномов, алгебра, идеал, порождающий полином идеала, пересечение идеалов, сумма идеалов, минимальный полином идеала, НОД и НОК.

Авторы курса:

Трифанов А. И. Москаленко М. А.

Ссылка на ресурсы:
mathdep.ifmo.ru/geolin

6.1 Структуры на множестве полиномов

Nota bene Напомним, что пространством полиномов $\Bbbk[t]$ называется множество формальных сумм следующего вида:

$$\Bbbk[t] = \left\{ p_n(t) = \sum_{k=0}^{n} \alpha_k t^k, \quad \forall n \in \mathbb{N}, \quad \alpha_k \in \Bbbk \right\}$$

Nota bene Следующие операции задают на $\Bbbk[t]$ структуру линейного пространства:

$$(p+q)(t) = p(t) + q(t), \quad (\alpha p)(t) = \alpha \cdot p(t), \quad 0(t) = 0.$$

Nota bene Операция умножения полиномов

$$(p \cdot q)(t) = p(t) \cdot q(t).$$

задает на множестве $\Bbbk[t]$ структуру коммутативного моноида, именно:

1. $p \cdot (q \cdot r) = p \cdot q \cdot r$;
2. $(p \cdot q)(t) = p(t) \cdot q(t) = q(t) \cdot p(t) = (q \cdot p)(t)$.
3. нейтральный по умножению: $1(t) = 1$.

Nota bene Линейные операции и умножение в $\Bbbk[t]$ согласованы:

$$(p+q) \cdot r = p \cdot r + q \cdot r,$$
$$(\alpha p) \cdot q = p \cdot (\alpha q) = \alpha \cdot (pq).$$

Nota bene Введенные законы композиции индуцируют на множестве $\Bbbk[t]$ структуру коммутативной алгебры.

‖ Алгебра $\Bbbk[t]$ называется **алгеброй скалярных полиномов**.

6.2 Идеалы алгебры $\Bbbk[t]$

‖ **Идеалом** $\mathfrak{a}$ алгебры $\Bbbk[t]$ называется такое ее линейное подпространство, что

$$\Bbbk[t] \cdot \mathfrak{a} \subset \mathfrak{a}.$$

Nota bene Так как $1(t) \in \Bbbk[t]$, то $\Bbbk[t] \cdot \mathfrak{a} = \mathfrak{a}$.

Пример 6.1. Примеры идеалов:

- $\{0\}$ и $\Bbbk[t]$ - тривиальные идеалы;
- $\mathfrak{a}(\alpha) = \{p \in \Bbbk[t] \quad | \quad p(\alpha) = 0, \quad \alpha \in \Bbbk\}$;

Лемма 6.1. *Пусть $q \in \Bbbk[t]$, тогда множество $\mathfrak{a}(q) = q \cdot \Bbbk[t]$ является идеалом.*

▶

Пусть $p \in \mathfrak{a}(q)$ и $h \in \Bbbk[t]$, тогда

$$p \cdot h = g \cdot q \cdot h = q \cdot (gh) \in q \cdot \Bbbk[t] = \mathfrak{a}(q).$$

◀

Идеалы вида $\mathfrak{a}(q)$, где $q \in \Bbbk[t]$ называются **главными идеалами** кольца $\Bbbk[t]$. При этом полином q называется **порождающим полиномом идеала** $\mathfrak{a}(q)$.

Nota bene Главные идеалы с порождающим полиномом q обозначают (q).

Теорема 6.1. *Любой идеал в кольце $\Bbbk[t]$ является главным.*

▶

Напомним, что в кольце $\Bbbk[t]$ имеется алгоритм Евклида деления многочленов с остатком. Воспользуемся этим: пусть $\mathfrak{a} \trianglelefteq \Bbbk[t]$ и $q \in \Bbbk[t]$, так что $\deg(q)$ - минимальная степень в идеале $\mathfrak{a}$. Далее, если $p \in \mathfrak{a}$, тогда с помощью алгоритма Евклида находим, что

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

Имеем $p \in \mathfrak{a}$, $q \cdot g \in \mathfrak{a}$, но тогда и $r \in \mathfrak{a}$, а значит $r = 0$.

◀

Минимальным полиномом идеала $\mathfrak{a}$ называется нетривиальный полином p_a наименьшей степени, принадлежащий идеалу $\mathfrak{a}$.

Nota bene Минимальный полином идеала $\mathfrak{a}$ условимся обозначать $\min(\mathfrak{a})$.

Лемма 6.2. *Пусть $p_a = \min(\mathfrak{a})$, тогда*

$$p \in \mathfrak{a} \quad \Leftrightarrow \quad p \,\vdots\, p_a.$$

▶

Доказательство следует из алгоритма Евклида.

◀

Лемма 6.3. *Пусть $\mathfrak{a} = (p)$ и $p_a = \min(\mathfrak{a})$, тогда $p \sim p_a$.*

▶

Прямой проверкой убеждаемся, что

$$\mathfrak{a} = p \cdot \Bbbk[t], \quad p_a \in \mathfrak{a} \quad \Rightarrow \quad \exists\, g \in \Bbbk[t]: \quad p_a = g \cdot p,$$
$$p \in \mathfrak{a} \quad \Rightarrow \quad p \,\vdots\, p_a.$$

◀

Nota bene Будем называть p_a *минимальным порождающим полиномом* идеала $\mathfrak{a}$.

6.3 Арифметика идеалов

Суммой $\mathfrak{a}_1 + \mathfrak{a}_2$ двух идеалов $\mathfrak{a}_1$ и $\mathfrak{a}_2$ называется множество

$$\mathfrak{b} = \{p \in \Bbbk[t] \quad | \quad p = p_1 + p_2, \quad p_1 \in \mathfrak{a}_1, \quad p_2 \in \mathfrak{a}_2\}\,.$$

Лемма 6.4. *Сумма $\mathfrak{b}$ идеалов является идеалом.*

▶

Пусть $p \in \mathfrak{b}$, то есть $p = p_1 + p_2$, $p_1 \in \mathfrak{a}_1$, $p_2 \in \mathfrak{a}_2$, тогда

$$\forall q \in \Bbbk[t] \quad q \cdot p = q(p_1 + p_2) = q \cdot p_1 + q \cdot p_2 \in \mathfrak{b}.$$

◀

Пересечением $a_1 \cap a_2$ двух идеалов называется множество

$$\mathfrak{c} = \{p \in \Bbbk[t] \quad | \quad p \in \mathfrak{a}_1 \quad \wedge \quad p \in \mathfrak{a}_2\}\,.$$

Лемма 6.5. *Пересечение $\mathfrak{c}$ идеалов является идеалом.*

▶

Пусть $p \in \mathfrak{c}$, то есть $p \in \mathfrak{a}_1$ и $p \in \mathfrak{a}_2$, тогда

$$\forall q \in k[t] \quad q \cdot p \in \mathfrak{a}_1, \quad q \cdot p \in \mathfrak{a}_2 \quad \Rightarrow \quad q \cdot p \in \mathfrak{a}_1 \cap \mathfrak{a}_2.$$

◀

Лемма 6.6. *Имеет место следующее свойство*

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \quad \Leftrightarrow \quad p_1 \,\vdots\, p_2.$$

▶

$\Rightarrow$ Необходимость:

$$p_1 \in \mathfrak{a}_1 \quad \Rightarrow \quad p_1 \in \mathfrak{a}_2 \quad \Rightarrow \quad p_1 \,\vdots\, p_2.$$

$\Leftarrow$ Достаточность:

$$p_1 = p_2 \cdot r \quad \Rightarrow \quad \forall g \in \mathfrak{a}_1 \quad g = p_1 \cdot q = p_2 \cdot r \cdot q \in \mathfrak{a}_2.$$

◀

Лемма 6.7. *Пусть $\mathfrak{a}_1 = (p_1)$ и $\mathfrak{a}_2 = (p_2)$, тогда*

$$\mathfrak{a}_1 \cap \mathfrak{a}_2 = (p), \quad p = \langle p_1, p_2 \rangle.$$

▶
Пусть $\tilde{p} = \langle p_1, p_2 \rangle$, тогда

$$p \in \mathfrak{a}_1, \quad p \in \mathfrak{a}_2 \quad \Rightarrow \quad p \;\vdots\; p_1, \quad p \;\vdots\; p_2 \quad \Rightarrow \quad p \;\vdots\; \tilde{p}.$$

С другой стороны

$$\tilde{p} \;\vdots\; p_1, \quad \tilde{p} \;\vdots\; p_2 \quad \Rightarrow \quad \tilde{p} \in \mathfrak{a}_1 \cap \mathfrak{a}_2 \quad \Rightarrow \quad \tilde{p} \;\vdots\; p.$$

◀

Теорема 6.2. *Пусть* $\mathfrak{a}_1 = (p_1)$ *и* $\mathfrak{a}_2 = (p_2)$, *тогда*

$$\mathfrak{a}_1 + \mathfrak{a}_2 = (p), \quad p = (p_1, p_2).$$

▶
Пусть $\tilde{p} = (p_1, p_2)$, тогда

$$p_1, p_2 \in \mathfrak{a}_1 + \mathfrak{a}_2 \quad \Rightarrow \quad p_1 \;\vdots\; p, \quad p_2 \;\vdots\; p \quad \Rightarrow \quad \tilde{p} \;\vdots\; p.$$

С другой стороны

$$\exists\, q_1, q_2 \in \Bbbk[t]: \quad p = q_1 p_1 + q_2 p_2; \quad p_1 \;\vdots\; \tilde{p}, \quad p_2 \;\vdots\; \tilde{p} \quad \Rightarrow \quad p \;\vdots\; \tilde{p}.$$

◀

Теорема 6.3. *Пусть* p_1, p_2 *такие что* $(p_1, p_2) = 1$, *тогда*

$$\exists\, q_1, q_2 \in \Bbbk[t]: \quad p_1 q_1 + p_2 q_2 = 1$$

▶
Пусть $\mathfrak{a}_1 = (p_1)$ и $\mathfrak{a}_2 = (p_2)$, а также $\mathfrak{a}_1 + \mathfrak{a}_2 = (p)$, тогда

$$p = (p_1, p_2) = 1 \quad \Rightarrow \quad \mathfrak{a}_1 + \mathfrak{a}_2 = (1) = \Bbbk[t].$$

◀

Nota bene Пусть $(p_1, p_2, \ldots, p_k) = 1$, тогда

$$\exists\ \{q_i\}_{i=1}^k: \quad \sum_{i=1}^k p_i q_i = 1.$$

Теорема 6.4. *Пусть* $p = p_1, p_2, \ldots, p_k$, где $(p_i, p_{j \neq i}) = 1$ *тогда*

$$\exists\ \{q_i\}_{i=1}^k: \quad \sum_{i=1}^k p'_i q_i = 1, \quad p'_i = p/p_i.$$