

Алгебра скалярных полиномов

$\triangleleft K$ — поле, над которым задано множество полиномов $K_\infty[\lambda]$, также обозначается $P_\infty[K]$

$$P_\infty[K] = \{p_n(\lambda) = \sum_{i=1}^n \alpha_i \lambda^i \quad \forall n\}$$

Примечание. $P_\infty[K]$ — линейное пространство:

$$p, q \in P_\infty[K]; \lambda \in K \Rightarrow \begin{cases} (p+q)(\lambda) = p(\lambda) + q(\lambda) \\ (\lambda p)(\lambda) = \alpha p(\lambda) \end{cases} \Rightarrow P_\infty[K] \text{ — линейное пространство}$$

Примечание. $P_\infty[K]$ — коммутативная алгебра

Зададим операцию умножения в $P_\infty[K]$:

$$\forall p, q \in P_\infty[K] \quad (p \cdot q)(\lambda) = p(\lambda)q(\lambda)$$

$$(p \cdot q)(\lambda) = p(\lambda)q(\lambda) = q(\lambda)p(\lambda) = (qp)(\lambda) \Rightarrow \text{коммутативность}$$

$$(p \cdot q) \cdot r = p \cdot (q \cdot r) = p \cdot q \cdot r$$

$$(p+q)r = pr + qr$$

$$(\lambda p)q = p(\lambda q) = \lambda(pq)$$

Нейтральный элемент:

- по сложению: $0(\lambda) = 0$
- по умножению: $1(\lambda) = 1$

Примечание. $\{1, t, t^2 \dots t^n \dots\}$ — базис $P_\infty[K] \Rightarrow \dim P_\infty[K] = \infty$

Определение. Идеалом J алгебры $P_\infty[K]$ называется такое её подпространство, что

$$\forall q \in J \quad \forall p \in P_\infty[K] \quad q \cdot p \in J$$

Пример. Тривиальные идеалы:

- $\{0\}$
- $P_\infty[K]$

Лемма 1. J — линейное подпространство $P_\infty[K]$

Доказательство. $]q_1, q_2 \in J \quad q_1 + q_2 \in J?$

$$q_1, q_2 \in J \Rightarrow \forall p \quad q_1 p, q_2 p \in J$$

$$q_1 = r\tilde{q}_1, q_2 = r\tilde{q}_2 \quad (q_1 + q_2)p = r(\tilde{q}_1 + \tilde{q}_2)p$$

$$(\tilde{q}_1 + \tilde{q}_2)p \in P_\infty[K] \Rightarrow r(\tilde{q}_1 + \tilde{q}_2)p \in J$$

□

Лемма 2. J — подалгебра $P_\infty[K]$

Доказательство.

$$(q_1 \cdot q_2)p = q_1(q_2 p) \in J$$

□

Пример. $J_\alpha = \{p \in P_\infty[K] : p(\alpha) = 0\}$ — идеал

Лемма 3. $]q \in P_\infty[K] \Rightarrow J_q = q \cdot P_\infty[K]$ — идеал в $P_\infty[K]$

Доказательство. $]r \in J_q \Rightarrow \exists p \in P_\infty[K] : r = q \cdot p$

$] \tilde{p} \in P_\infty[K]$

$r\tilde{p} = (qp)\tilde{p} = q(p\tilde{p})$

$p\tilde{p} \in P_\infty[K] \Rightarrow q(p\tilde{p}) \in q \cdot P_\infty[K] = J_q \Rightarrow J_q - \text{идеал}$ □

Определение. Полином $q : J_q = q \cdot P_\infty[K]$ называется **порождающим полиномом идеала** J_q

Примечание. Если идеал содержит $1(\lambda)$, то данный идеал совпадает с $P_\infty[K]$:

$$J_1 = 1 \cdot P_\infty[K] = P_\infty[K]$$

Определение. $]J_1$ и J_2 — идеалы в $P_\infty[K]$

1. Суммой $J_1 + J_2$ называется множество

$$J_s = \{p \in P_\infty[K] : p = p_1 + p_2 \quad p_1 \in J_1, p_2 \in J_2\}$$

2. Пересечением $J_1 \cap J_2$ называется множество:

$$J_r = \{p \in P_\infty[K] : p \in J_1 \wedge p \in J_2\}$$

Лемма 4. J_s и J_r — идеалы в $P_\infty[K]$

Доказательство. $J_s = J_1 + J_2$ — идеал?

$]q \in J_s \Rightarrow q = q_1 + q_2 \quad q_1 \in J_1, q_2 \in J_2$

$]p \in P_\infty[K] \quad qp = (q_1 + q_2)p = q_1p + q_2p$

$q_1p \in J_1, q_2p \in J_2 \Rightarrow q_1p + q_2p \in J_s$

$J_r = J_1 \cap J_2$ — идеал?

$]q \in J_r \Rightarrow q \in J_1; q \in J_2$

$]p \in P_\infty[K] \quad qp \in J_1; qp \in J_2 \Rightarrow qp \in J_r$ □

Определение. Нетривиальный полином минимальной степени, содержащийся в идеале, называется **минимальным полиномом идеала**.

Лемма 5. Любой полином идеала J делится на p_J без остатка:

$$]p \in J \Rightarrow p \mid p_J$$

Доказательство. $] \exists p : p \nmid p_J \Rightarrow p = qp_J + r; \deg r < \deg p_J \Rightarrow r = p - qp_J : \text{min полином — противоречие.}$ □

Примечание. Если p_1 и p_2 — минимальные полиномы $J \Rightarrow p_1 = \alpha p_2; \alpha \in K$

Теорема 1. Минимальный полином идеала является его порождающим полиномом.

Доказательство. $\forall p \in J \quad p \mid p_J \Rightarrow p = p_J \cdot q \in p_J \cdot P_\infty[K]$

$\forall p \in q \cdot P_\infty[K] \Rightarrow p = qr; r \in P_\infty[K] \Rightarrow \forall p \mid q \Rightarrow q = p_J$ □

Лемма 6. Сравнение идеалов:

$$J_1 \subset J_2 \Leftrightarrow p_{J_1} \mid p_{J_2}$$

Доказательство. “ \Rightarrow ”

$J_1 \subset J_2 \Rightarrow p_{J_1} \in J_2 \Rightarrow p_{J_1} \mid p_{J_2}$

“ \Leftarrow ”

$]p_{J_1} \mid p_{J_2} \Rightarrow p_{J_1} = rp_{J_2}$

$\forall q \in J_1 \quad q = \tilde{q}p_{J_1} = \tilde{r}p_{J_2} \Rightarrow q \mid p_{J_2} \Rightarrow J_1 \subset J_2$ □

Лемма 7. О минимальном полиноме пересечения

$$J_1 \leftrightarrow p_{J_1} \quad J_2 \leftrightarrow p_{J_2} \Rightarrow J_r = J_1 \cap J_2 \leftrightarrow r_J = \text{НОК}(p_{J_1}, p_{J_2})$$

Доказательство. $J_r = J_1 \cap J_2 \Rightarrow J_r \subset J_1 \wedge J_r \subset J_2 \Rightarrow r_J \mid p_{J_1} \wedge r_J \mid p_{J_2} \Rightarrow r_J = \text{НОК}(p_{J_1}, p_{J_2})$ \square

Лемма 8. О минимальном полиноме суммы

$$J_s = J_1 + J_2 \Rightarrow S_J = \text{НОД}(p_{J_1}, p_{J_2})$$

Доказательство. $J_s = J_1 + J_2 \Rightarrow J_s \supset J_1 \wedge J_s \supset J_2 \Rightarrow p_{J_1} \mid S_J \wedge p_{J_2} \mid S_J \Rightarrow S_J = \text{НОД}(p_{J_1}, p_{J_2})$ \square

Теорема 2. О взаимно простых полиномах

$[p_1, p_2]$ — взаимно простые, т.е. $\text{НОД}(p_1, p_2) = 1 \Rightarrow \exists q_1, q_2 \in P_\infty[K] : p_1 q_1 + p_2 q_2 = 1$

Доказательство. $p_1 \leftrightarrow J_1 = p_1 P_\infty[K]$

$p_2 \leftrightarrow J_2 = p_2 P_\infty[K]$

$\text{НОД}(p_1, p_2) = 1 \leftrightarrow J_1 + J_2 = P_\infty[K]$

$p_1 q_1 + p_2 q_2 = 1$ \square

Теорема 3. Обобщение

$$p_1 \dots p_k \in P_\infty[K], \text{НОД}(p_1 \dots p_k) = 1 \Rightarrow \exists q_1 \dots q_k : \sum_{i=1}^k p_i q_i = 1$$

Доказательство. Аналогично. \square

Примечание. $[p] = p_1 \cdot p_2 \dots p_k, \{p_i\}$ взаимно простые $\Rightarrow \exists q_1 \dots q_k : p'_1 q_1 + p'_2 q_2 + \dots + p'_k q_k = 1, p'_j = \frac{p}{p_j}$

Алгебра операторных полиномов

$[\varphi : X \rightarrow X]$ — линейный оператор

Определение. Операторным полиномом $p(\varphi)$ называется полином вида:

$$p(\varphi) = \sum_{i=1}^n \alpha_i \varphi^i, \varphi^0 = I$$

Определение. $\mathcal{P}_\varphi = \{p_n(\varphi) \mid \forall n\}$ — множество операторных полиномов

Лемма 9. \mathcal{P}_φ — линейное пространство

Лемма 10. \mathcal{P}_φ — коммутативная алгебра

Доказательство.

$$\forall p(\varphi), q(\varphi) \quad p(\varphi)q(\varphi) = q(\varphi)p(\varphi) \Leftrightarrow \varphi^m \varphi^n = \varphi^n \varphi^m$$

\square

$$\triangleleft S_\varphi : P_\infty[K] \rightarrow \mathcal{P}_\varphi$$

$$p(\lambda) = \sum_{i=1}^n \alpha_i \lambda^i \xrightarrow{S_\varphi} p(\varphi) = \sum_{i=1}^n \alpha_i \varphi^i$$

Лемма 11. S_φ — гомоморфизм алгебр $P_\infty[K]$ и \mathcal{P}_φ

Доказательство.

$$p(\lambda) + q(\lambda) = (p + q)(\lambda) = \sum_{i=1}^n (\lambda_i + \beta_i) \lambda^i \mapsto \sum_{i=1}^n (\lambda_i + \beta_i) \varphi^i = (p + q)(\varphi) = p(\varphi) + q(\varphi)$$

$$\alpha p(\lambda) \mapsto \alpha p(\varphi) \text{ аналогично}$$

$$p(\lambda)q(\lambda) = (pq)(\lambda) = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \beta_j \lambda^{i+j} \mapsto \sum_{i=1}^n \sum_{j=1}^n \alpha_i \beta_j \varphi^{i+j} = (pq)(\varphi) = p(\varphi)q(\varphi)$$

$$1 \mapsto \varphi^0 = I$$

□

Лемма 12. $p_1, p_2 \in P_\infty[K], \text{НОД}(p_1, p_2) = 1 \Rightarrow \exists q_1, q_2 \in P_\infty[K] : p_1(\varphi)q_1(\varphi) + p_2(\varphi)q_2(\varphi) = I$

Доказательство. Применим к обеим частям $p_1(\lambda)q_1(\lambda) + p_2(\lambda)q_2(\lambda) = 1$ отображение S_φ :

$$p_1(\varphi)q_1(\varphi) + p_2(\varphi)q_2(\varphi) = I$$

□

Теорема 4. О сумме ядер.

$$]p = p_1 \cdot p_2, \quad p_1, p_2 \in P_\infty[K]$$

$]p_1, p_2$ — взаимно простые

Тогда

$$\text{Ker } p(\varphi) = \text{Ker } p_1(\varphi) \dot{+} \text{Ker } p_2(\varphi)$$

Т.е., по определению $\dot{+}$:

$$\forall x \in \text{Ker } p(\varphi) \quad \exists! x_1 \in \text{Ker } p_1(\varphi), x_2 \in \text{Ker } p_2(\varphi) \quad x = x_1 + x_2$$

Доказательство. Покажем, что $\text{Ker } p_1(\varphi) + \text{Ker } p_2(\varphi) \subset \text{Ker } p(\varphi)$

$$]x_j \in \text{Ker } p_j(\varphi) \Rightarrow$$

$$p(\varphi)(x) = p(\varphi)(x_1 + x_2) = p_1(\varphi)p_2(\varphi)x_1 + p_1(\varphi)p_2(\varphi)x_2 = 0 + 0 = 0$$

Покажем, что $\text{Ker } p(\varphi) \subset \text{Ker } p_1(\varphi) + \text{Ker } p_2(\varphi)$

$$]x \in \text{Ker } p(\varphi)$$

$$\text{НОД}(p_1, p_2) = 1 \Rightarrow p_1(\varphi)q_1(\varphi) + p_2(\varphi)q_2(\varphi) = I$$

$$x = Ix = p_1(\varphi)q_1(\varphi)x + p_2(\varphi)q_2(\varphi)x$$

$$p_2(\varphi)q_2(\varphi)x \in \text{Ker } p_1(\varphi) \Leftarrow p_1(\varphi)p_2(\varphi)q_2(\varphi)x = p(\varphi)q_2(\varphi)x = 0$$

Покажем, что $\text{Ker } p_1(\varphi) + \text{Ker } p_2(\varphi)$ — прямая сумма

$$\angle \text{Ker } p_1(\varphi) \cap \text{Ker } p_2(\varphi) \ni z$$

$$z = Iz = p_1(\varphi)q_1(\varphi)z + p_2(\varphi)q_2(\varphi)z = 0 + 0 = 0 \Rightarrow \dim \text{Ker } p_1(\varphi) \cap \text{Ker } p_2(\varphi) = 0 \Rightarrow$$

$$\Rightarrow \text{Ker } p_1(\varphi) + \text{Ker } p_2(\varphi) \text{ — прямая сумма}$$

□

Примечание. Пусть $p = p_1 \dots p_k, \{p_k\}$ — взаимно простые \Rightarrow

$$\text{Ker } p(\varphi) = \dot{+} \sum_{j=1}^k \text{Ker } p_j(\varphi)$$