

**Московский физико-технический институт
Физтех-школа прикладной математики и информатики**

АЛГЕБРА И ГЕОМЕТРИЯ

II СЕМЕСТР

Лектор: *Богданов Илья Игоревич*

весна 2026

Оглавление

Предисловие	2
1 Многочлены	3
§1 Многочлены	3
2 Линейные преобразования	6
Приложения	
Предметный указатель	8

Предисловие

В конспекте могут быть ошибки и/или неточности.

Предметный указатель

Для удобства поиска, скажем, теорем, в конце конспекта находится [предметный указатель](#), с помощью которого можно быстро найти нужную теорему.

Используемые обозначения

↪ – выполняется;
: – такой (ая, ое), что.

Глава 1

Многочлены

§1 Многочлены

Конспект лекции пока не доделан, формулы и определения могут быть с ошибками (вообще говоря, и так могли, но здесь вероятность наткнуться на них сильно выше). Значок \bullet означает пропуск.

Лекция 1 (04.02.2026)

Напоминание. Многочлен над полем F единственным образом представляется в виде $P = p_0 + p_1x + \dots + p_nx^n$. Они образуют кольцо, обозначаемым $F[x]$

Базис $F[x]$ — это $(1, x, x^2, \dots)$

Напоминание. Значения многочлена: Если A — алгебра над F , то $P(a) = p_0 \cdot 1 + p_1 \cdot a + p_2 \cdot a^2 + \dots + p_na^n \in A$

$$P(a) + Q(a) = (p + \bullet) \bullet$$

Напоминание. Делимость, деление с остатком

$A \bullet$ на $B \bullet$

$$A = QB + R, \deg R = \deg B$$

$$\text{НОД}(P, Q) = AP + BQ, A, B \in F[x]$$

Основная теорема арифметики.

Определение 1. Пусть $D \in F[x]$, (F — поле), $a \in F$. Тогда a — корень многочлена P , если $P(a) = 0$.

Теорема 1 (Безу). *Пусть $P \in F[x]; a \in F$. Тогда a — корень P тогда и только тогда, когда $x - a \mid P$.*

Доказательство. Разделим P на $x - a$ с остатком. $D = Q \cdot (x - a) + R$, где $\deg R < \deg(x - a) = 1$, то есть R — константа. Подставим a в P : $P(a) = Q(a) \cdot (a - a) + R = R$. a — корень $P \iff P(a) = a \iff R = 0 \iff (x - a) \mid P$. \square

Замечание. И любом случае $R = P(0)$.

Определение 2. Пусть a — корень многочлена $P \in F[x] : P \neq 0$. Его кратность — это наибольшее натуральное число k такое, что $(x - k)^k \mid P$.

Теорема 2. Пусть $P \in F[x] : P \neq 0, \deg P = n$. Тогда сумма кратностей всех его корней, не превосходит n .

Доказательство. Пусть a_1, \dots, a_k — корни P , k_1, \dots, k_k — их кратности, тогда $(x-a_i)_{k_i} | P$.

Но $x - a_i, x - a_j (a_i \neq a_j)$ взаимно просты. Поэтому $\prod_{i=1}^k (x - a_i)^{k_i} | P$.

•

$$\deg Q \subseteq \deg P = n$$

$$\deg Q = \sum$$

□

Замечание. Если $2k_i = n$, то это означает, что $P = \alpha \prod_{i=1}^d (x - a_i)$, $\alpha \in F$

Определение 3. Такой многочлен называется линейно факторизуемым.

Теорема 3 (Основная теорема Алгебра). Любой многочлен над полем комплексных чисел линейно факторизуем.

Замечание. Такие поля называются алгебраически замкнутыми.

Определение 4. Корень $a \in F$ многочлена $P \in F[x]$ называется кратным корнем, если его кратность > 1 , иначе он называется простым.

Определение 5 (Формальная производная). Пусть $P \in F[x]$, $P = p_0 + p_1x + \dots + p_nx^n = \sum_i p_i x^i$. Его формальной производной называется $P' = p_1 + 2p_2x + \dots + np_nx^{n-1} = \sum_{i \geq 1} ip_i x^{i-1}$

Утверждение 1 (Линейность формальной производной).

1. $(\alpha + \beta Q)' = \alpha \cdot P' + \beta \cdot Q'$, $\alpha, \beta \in F$, $P, Q \in F[x]$
2. $(PQ)' = P'Q + PQ'$ и, более того, $(p_1, \dots, p_n)' = p'_1 p_2 \dots p_n + p_1 p'_2 p_3 \dots p_n + \dots + p_1 \dots p_{n-1} p'_n$
3. $(P(Q))' = P'(Q) \cdot Q'$

Доказательство.

1. Если $P = \sum_i p_i x^i$, $Q = \sum_i q_i x^i$, то $(\alpha P + \beta Q)' = \left(\sum_i (\alpha p_i + \beta q_i) x^i \right)' = \sum_i i(\alpha p_i + \beta q_i) x^{i-1} = \alpha \cdot \sum_i ip_i x^{i-1} + \beta \cdot \sum_i iq_i x^{i-1} = \alpha P' + \beta Q'$.

При фиксированном ● части расv... ● — линейным операторами от P . Линейном однозначно задается значениями на базисе \Rightarrow достаточно проверить для $P = x^n$, $n \geq 0$. Аналогично, достаточно рассмотреть случай, когда $Q = x^m$, $m \geq 0$.

$$P'Q + Q'P = nx^{n-1} \cdot x^m + mx^{m-1} \cdot x^n = (n+m)x^{n+m-1} = (x^{n+m})' = (PQ)'.$$

Равенство $(P_1, P_2, \dots, P_n)' = \dots$ доказывается индукцией по n . База при $n = z$ ●

Для перехода: $(P_1, \dots, P_{n-1}, P_n) = (P_1, \dots, P_{n-1})' P_n + P_1 \dots P_{n-1} P'_n = P'_1 P_2 \dots P_n + \dots + P_1 \dots P'_{n-1} P_n + P_1 \dots P_{n-1} P'_n$.

- левая и правая части .. по $P \implies$ достаточно проверить равенство при $P = x^n$. Тогда $(P(Q))' = (Q^n)' = nQ^{n+1}Q' = P'(Q) \cdot Q'$ \square

Теорема 4. Пусть $P \in F[x]$, $a \in F$.

1. *a является кратным корнем многочлена P тогда и только тогда, когда $P(a) = P'(a) = 0$.*
2. *Если a – корень кратности $\geq k$, то $P(a) = P'(a) = \dots = P^{(\bullet)}(a) = 0$.*
3. *Если $P(a) = \dots = P^{(n-1)}(a) = 0$, то a – корень p кратности $\geq k$ при условии, что $\text{char } F = 0$ или $\text{char } F \geq k$.*

Доказательство. Пусть t – кратность корня a , то есть, $P = (x - a)^t Q$, где $Q(a) \neq 0$. Тогда $P' = ((x - a)^t)Q + (x - a)^t Q' = (x - a)^{t-1}Q + (X - a)^t Q' = (x - a)^{t-1}(tQ + (x - a)Q')$.

1. Если $t = 1$, то $P'(a) = tQ(a) + 0 = Q(a) \neq 0$. Если $t \geq 2$, то $P'(a) = 0$.
2. a – корень кратности $\geq k$ в $P \implies a$ – корень кратности $\geq k-1$ в $P' \implies \dots \implies a$ – корень кратности ≥ 1 в $P^{(k-1)}$.

Замечание 1. Подставляя во вторую скобку a , получаем $tQ(a) + 0 = tQ(a) \neq 0$

3. Заметим, что при $\sum \text{char } F = 0$ или $t < \text{char } F$, корень a многочлена P' имеет кратность $t - q : tQ(a) \neq 0$. Значит, a – корень P кратности $t \implies a$ – корень P' кратности $t - 1 \implies a$ – корень P'' кратности $t - 2 \implies \dots \implies a$ – корень $P^{(t)}$ кратности 0, то есть, не корень. Таким образом, если $\text{char } F = 0$ или $k \leq \text{char } F$, то случай $t < k$ невозможен: $P^{(t)}(a) \neq 0$. Поэтому $t \geq k$.

□

Пример 1. При $F = \mathbb{Z}_p$. Рассмотрим многочлен $Q = x^p - q \in \mathbb{Z}_p[x]$. У него есть корень $a = 1$ кратности $\leq p$. С другой стороны, $Q' = px^{p-1} = 0 = Q'' = Q''' = \dots$. Таким образом, $Q(q) = Q'(q) = Q''(1) = \dots = 0$. Значит третье утверждение применимо для $k = p$, следовательно, 1 – корень Q кратности $\geq p$. Значит, $Q = \alpha(x - 1)^p = (x - 1)^p$.

Замечание 2. С некоторыми изменениями, тот же метод работает для выяснения на какую степень неприводимого многочлена Q делится P .

Глава 2

Линейные преобразования

Определение 1. Линейное преобразование пространства V_i — это линейное отображение $\varphi : V \rightarrow V$.

•

(V -)

e — базис в V

$\varphi \underset{e}{\leftrightarrow} A$ — матрица φ в базисе e : $\varphi(e) = (\varphi(\vec{e}_1), \dots, \varphi(\vec{e}_n)) = eA$

Если $\varphi \underset{e}{\leftrightarrow} A, \vec{v} \underset{e}{\leftrightarrow} \alpha$, то $\varphi(\vec{v}) \underset{e}{\leftrightarrow} A\alpha$.

$\mathcal{L}(V)$ — множество всех линейных преобразований V — линейное пространство над F , а также кольцо, то есть алгебра над F . Для фиксированного базиса e сопоставления $\varphi \underset{e}{\leftrightarrow} A$ дает изоморфизм алгебр $\mathcal{L}(V) \cong M_n(F)$.

Если e, e' — базисы в V , $e' = eS$, причем $\varphi \underset{e}{\leftrightarrow} A, \varphi \underset{e'}{\leftrightarrow} A'$, то $A' = S^{-1}AS$.

Напоминание 1. Матрицы $A, A' \in M_n(F)$, если $\exists S \in GL_n(F) : A' = S^{-1}AS$.

Определение 2 (Инвариантное подпространство). Пусть V — линейное пространство над F , $\varphi \in \mathcal{L}(V)$, $U \leqslant V$. Подпространство U называется инвариантным относительно φ (или φ -инвариантным), если $\varphi(U) \subseteq U$ (то есть, $\forall \vec{u} \in U \hookrightarrow \varphi(\vec{u}) \in U$).

Замечание 3. Это евклидово • .

Напоминание 2. Если U подпространство в V , то $\varphi(U)$ тоже подпространство в V .

$\varphi \in \mathcal{L}(V) \implies \text{Im } \varphi = \varphi(V) \leqslant V$

$\text{Ker } \varphi = \varphi^{-1}(\vec{0}) \leqslant V$

Замечание 4. Если U — φ -инвариантное подпространство, то $\varphi|_u \in \mathcal{L}(U)$.

Утверждение 1. Пусть $\varphi \in \mathcal{L}(V)$, $U \leqslant V$, $u \in e = (\vec{e}_1, \dots, \vec{e}_n)$ — базис в V такой, что его префикс $(\vec{e}_1, \dots, \vec{e}_k)$ — базис в V . Тогда U — φ -инвариантное подпространство V тогда и только тогда, когда

$$\varphi \underset{e}{\leftrightarrow} A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

Доказательство. U — φ -инвариантное подпространство $\iff \forall \vec{u} \in U \hookrightarrow \varphi(\vec{u}) \in U \iff \forall i = 1, \dots, k \hookrightarrow \varphi(\vec{e}_i) \in U \iff \forall i = 1, \dots, k \hookrightarrow \varphi(\vec{e}_i) \in \langle \vec{e}_1, \dots, \vec{e}_k \rangle$. \square

Замечание 5. Если $U - \varphi$ инвариантно и

$$\varphi \underset{e}{\leftrightarrow} \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

то $\varphi|_u \underset{(\vec{e}_1, \dots, \vec{e}_k)}{\leftrightarrow} B$.

Замечание 6. Если $V = U_1 \oplus U_2$, где U_1, U_2 — φ -инвариантны, то в базисе, согласованным с U_1 и U_2 , имеем

$$\varphi \underset{e}{\leftrightarrow} A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

Утверждение 2. Пусть U_1, U_2 — φ -инвариантные подпространства, тогда $U_1 \cap U_2$ и $U_1 + U_2$ также φ -инвариантны.

Доказательство.

1. $\vec{u} \in U_1 \cap U_2 \implies \varphi(\vec{u})$
2. Если $\vec{u} \in U_1 + U_2$, то $\vec{u} = \vec{u}_1 + \vec{u}_2 \implies \varphi(\vec{u}) = \varphi(\vec{u}_1) + \varphi(\vec{u}_2) \in U_1 + U_2$

□

Утверждение 3. Пусть $\varphi, \psi \in \mathcal{L}(V)$, причем $\varphi\psi = \psi\varphi$. Тогда $\text{Ker } \psi$ и $\text{Im } \psi$ инвариантны относительно φ .

Доказательство. Пусть $\vec{u} \in \text{Ker } \psi$, то есть, $\psi(\vec{u}) = \vec{0}$. Необходимо проверить, что $\varphi(\vec{u}) \in \text{Ker } \psi$, то есть, $\psi(\varphi(\vec{u})) = \psi\varphi(\vec{u}) = \varphi(\vec{0}) = \vec{0}$.

Пусть $\vec{u} \in \text{Im } \psi$, то есть, $\vec{u} = \psi(\vec{v}), \vec{v} \in V$. Тогда $\varphi(\vec{u}) = \varphi(\psi(\vec{v})) = \psi(\varphi(\vec{v}))$

□

Замечание 7. • • •

Предметный указатель

Теоремы

Глава 1 §1

Теорема 1. Безу	3
Теорема 2	4
Теорема 3. Основная теорема Алгебра	4
Теорема 4	5

Определения

Глава 1 §1

Определение 1	3
Определение 2	3
Определение 3	4
Определение 4	4
Определение 5. Формальная	

производная

4

Глава 2 §0

Определение 1	6
Определение 2. Инвариантное подпространство	6

Утверждения

Глава 1 §1

Утверждение 1. Линейность формальной производной	4
Глава 2 §0	
Утверждение 1	6
Утверждение 2	7
Утверждение 3	7