

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 Корни многочленов	3
2 Линейные преобразования	7
§1 Инвариантные подпространства	7
Приложения	
Предметный указатель	9

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

\hookrightarrow – выполняется;

$:$ – такой (ая, ое), что.

Глава 1

Многочлены

Лекция 1 (04.02.2026)

§1 Корни многочленов

Напоминание.

- * Многочлен над полем F единственным образом представляется в виде $P = p_0 + p_1x + \dots + p_nx^n$, причем единственным образом. Все многочлены над полем F образуют кольцо, обозначаемое $F[x]$, а также алгебру над F .
- * Базис $F[x]$ — это $(1, x, x^2, \dots)$
- * Значения многочлена: Если A — произвольная алгебра над F , $a \in A$, то $P(a) = p_0 \cdot 1 + p_1 \cdot a + p_2 \cdot a^2 + \dots + p_n a^n \in A$
- * $P(a) + Q(a) = (P + Q)(a)$
- * $(PQ)(a) = P(a) \cdot Q(a)$

Напоминание.

- * A делим на $B \neq 0$:

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

- * У многочленов A и B существует наибольший общий делитель:

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

- * Основная теорема арифметики: любой ненулевой многочлен единственным образом раскладывается в произведение неприводимых многочленов.

Определение 1 (Корень многочлена). 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 $P \iff P(a) = 0 \iff R = 0 \iff (x - a) \mid P$. \square

Замечание. В любом случае $R = P(a)$.

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

Теорема 2 (О сумме кратностей корней). 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_d — корни P , k_1, \dots, k_d — их кратности, тогда $(x - a_i)^{k_i} \mid P$. Но $(x - a_i)$ и $(x - a_j)$ взаимно просты при различных $a_i \neq a_j$. Поэтому $Q := \prod_{i=1}^d (x - a_i)^{k_i} \mid P$. Значит, $\deg Q = \sum_{i=1}^d k_i \leq \deg P = n$. \square

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

Определение 3 (Линейно факторизуемый многочлен). Такой многочлен называется линейно факторизуемым.

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

Замечание. Поля с таким же свойством называются алгебраически замкнутыми.

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

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

Утверждение 1 (Свойства формальной производной).

1. $(\alpha P + \beta Q)' = \alpha \cdot P' + \beta \cdot Q'$, $\alpha, \beta \in F$, $P, Q \in F[x]$
2. $(PQ)' = P'Q + PQ'$ и, более того, $(P_1 \dots P_n)' = P_1'P_2 \dots P_n + P_1P_2'P_3 \dots P_n + \dots + P_1 \dots P_{n-1}P_n'$
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 $(\alpha P + \beta Q)' = \left(\sum_i (\alpha p_i + \beta q_i) x^i \right)' = \sum_i (\alpha p_i + \beta q_i) \cdot i \cdot x^{i-1} = \alpha \cdot \sum_i i p_i x^{i-1} + \beta \cdot \sum_i i q_i x^{i-1} = \alpha P' + \beta Q'$.

Замечание. Мы доказали, что взятие производной от многочлена — это линейное преобразование $\varphi : F[x] \rightarrow F[x]$.

2. При фиксированном многочлене Q обе части равенства являются линейными операторами, зависящими от P . Линейный оператор однозначно задается значениями этого оператора на базисе, следовательно достаточно проверить равенство 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 $n = 2$ уже доказана. Переход: $(P_1, \dots, P_{n-1}, P_n) = (P_1, \dots, P_{n-1})'P_n + P_1 \dots P_{n-1}P'_n = P'_1P_2 \dots P_n + \dots + P_1 \dots P'_{n-1}P_n + P_1 \dots P_{n-1}P'_n$.

3. Опять же, левая и правая части линейны по P , а значит достаточно проверить равенство при $P = x^n$. Тогда $(P(Q))' = (Q^n)' = nQ^{n-1}Q' = P'(Q) \cdot Q'$

□

Теорема 4 (Условия кратности корня). 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 $P(a) = P'(a) = \dots = P^{(k-1)}(a) = 0$.
3. Если $P(a) = \dots = P^{(k-1)}(a) = 0$, то a — корень 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 $P' = ((x-a)^t)'Q + (x-a)^t Q' = t(x-a)^{t-1}Q + (x-a)^t Q' = (x-a)^{t-1}(tQ + (x-a)Q')$.

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

Замечание. Подставляя во вторую скобку a , получаем $tQ(a) + 0 = tQ(a)$, что будет нулем в случае, если $p \mid t$.

3. Заметим, что при $\text{char } F = 0$ или $t < \text{char } F$, корень a многочлена P' имеет кратность $t-1$, так как $tQ(a) \neq 0$. 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, иначе $P^{(t)}(a) \neq 0$. Поэтому $t \geq k$.

□

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

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

Глава 2

Линейные преобразования

§1 Инвариантные подпространства

Напоминание.

- * Линейное преобразование пространства V — это линейное отображение $\varphi : V \rightarrow V$, то есть такое, что

1. $\varphi(\vec{v}_1 + \vec{v}_2) = \varphi(\vec{v}_1) + \varphi(\vec{v}_2)$
2. $\varphi(\alpha\vec{v}) = \alpha \cdot \varphi(\vec{v}), \quad \alpha \in F$

(Считаем, что V — конечномерное пространство над полем F)

- * Если $e = (\vec{e}_1, \dots, \vec{e}_n)$ — базис в V , то φ однозначно задается своей матрицей в базисе $\varphi \xleftrightarrow{e} A$. Причем такой, что $\varphi(e) = (\varphi(\vec{e}_1), \dots, \varphi(\vec{e}_n)) = eA$. Если $\varphi \xleftrightarrow{e} A, \vec{v} \xleftrightarrow{e} \alpha$, то $\varphi(\vec{v}) \xleftrightarrow{e} A\alpha$.
- * $\mathcal{L}(V)$ — множество всех линейных преобразований V — линейное пространство над F , а также кольцо, то есть алгебра над F . Для фиксированного базиса e сопоставление $\varphi \xleftrightarrow{e} A$ дает изоморфизм алгебр $\mathcal{L}(V) \cong M_n(F)$.
- * Если e, e' — базисы в V , $e' = eS$, причем $\varphi \xleftrightarrow{e} A, \varphi \xleftrightarrow{e'} A'$, то $A' = S^{-1}AS$.
- * Матрицы $A, A' \in M_n(F)$ подобны, если $\exists S \in GL_n(F) : A' = S^{-1}AS$.

Определение 1 (Инвариантное подпространство). Пусть V — линейное пространство над F , $\varphi \in \mathcal{L}(V), U \leq V$. 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. Это свойство достаточно проверять для базиса в U .

Напоминание.

- * Если U подпространство в V , то $\varphi(U)$ тоже подпространство в V .
- * Образ линейного оператора: $\varphi \in \mathcal{L}(V) \implies \text{Im } \varphi = \varphi(V) \leq V$
- * Ядро линейного оператора: $\text{Ker } \varphi = \varphi^{-1}(\vec{0}) \leq V$

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

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

$$\varphi \xleftrightarrow[e]{\quad} A = \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array} \right)$$

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

Замечание 1. Если U — φ инвариантно и

$$\varphi \xleftrightarrow[e]{\quad} \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array} \right)$$

то $\varphi|_U \xleftrightarrow[(\vec{e}_1, \dots, \vec{e}_k)]{\quad} B$.

Замечание 2. Если $V = U_1 \oplus U_2$, где U_1, U_2 — φ -инвариантны, то в базисе, согласованном с U_1 и U_2 , имеем

$$\varphi \xleftrightarrow[e]{\quad} A = \left(\begin{array}{c|c} B & 0 \\ \hline 0 & C \end{array} \right)$$

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

\square

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, $\psi(\varphi(\vec{u})) = \psi\varphi(\vec{u}) = \varphi\psi(\vec{u}) = \varphi(\psi(\vec{u})) = \varphi(\vec{0}) = \vec{0}$.

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

Замечание. Мы будем применять это утверждение в случае $\varphi = P(\psi)$, где P — это некоторый многочлен, ведь любой такой многочлен коммутирует с φ .

Предметный указатель

Теоремы

Глава 1

Теорема 1. Безу	3
Теорема 2. О сумме кратностей корней ...	4
Теорема 3. Основная теорема алгебры	4
Теорема 4. Условия кратности корня	5

Определения

Глава 1

Определение 1. Корень многочлена	3
Определение 2. Кратность корня	4
Определение 3. Линейно факторизуемый многочлен	4
Определение 4. Кратный корень	4

Определение 5. Формальная производная многочлена	4
---	---

Глава 2

Определение 1. Инвариантное подпространство	7
--	---

Утверждения

Глава 1

Утверждение 1. Свойства формальной производной	4
---	---

Глава 2

Утверждение 1	8
Утверждение 2	8
Утверждение 3	8