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

АЛГЕБРА И ГЕОМЕТРИЯ

II СЕМЕСТР

Лектор: *Богданов Илья Игоревич*

весна 2026

Оглавление

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)

Напоминание.

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

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.

§1 Корни 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 $P \iff P(a)=0 \iff R=0 \iff (x-a)\mid P$. □

Замечание. В любом случае $R=P(a)$.

Определение 2. 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 $a_1,\ldots,a_d$ — корни P, $k_1,\ldots,k_d$ — их кратности, тогда $(x-a_i)^{k_i} \mid P$. Но $(x-a_i)$ и $(x-a_j)$ взаимно просты при различный $a_i\neq a_j$. Поэтому $Q := \prod\limits_{i=1}^{a}(x-a_i)^{k_i} \mid P$. Значит, $\deg Q = \sum\limits_{i=1}^{d} k_i \leqslant \deg P = n$. □

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

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 $P\in F[x]: P=p_0+p_1x+\ldots+p_nx^n=\sum\limits_i p_ix^i$. Его формальной производной называется $P'=p_1+2p_2x+\ldots+np_nx^{n-1}=\sum\limits_{i\geqslant 1} ip_ix^{i-1}$

Утверждение 1 (Свойства формальной производной)**.**

1. $(\alpha P+\beta Q)' = \alpha\cdot P'+\beta\cdot Q', \quad \alpha,\beta\in F, \quad P,Q\in F[x]$
2. $(PQ)' = P'Q+PQ'$ *и, более того,* $(P_1\ldots P_n)' = P_1'P_2\ldots P_n + P_1P_2'P_3\ldots P_n+\ldots+P_1\ldots P_{n-1}P_n'$
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 $\varphi : F[x] \to F[x]$.

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 $P = x^n, n \geqslant 0$. Аналогично, достаточно рассмотреть случай, когда $Q = x^m, m \geqslant 0$.

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

   Равенство $(P_1, P_2, \ldots, P_n)' = \ldots$ доказывается индукцией по n. База при $n = 2$ уже доказана. Переход: $(P_1, \ldots, P_{n-1}, P_n) = (P_1, \ldots, P_{n-1})' P_n + P_1 \ldots P_{n-1} P_n' = P_1' P_2 \ldots P_n + \ldots + P_1 \ldots P_{n-1}' P_n + P_1 \ldots P_{n-1} P_n'$.

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. *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 $\geqslant k$, то $P(a) = P'(a) = \ldots = P^{(k-1)}(a) = 0$.*

3. *Если $P(a) = \ldots = P^{(k-1)}(a) = 0$, то a — корень p кратности $\geqslant k$ при условии, что $\operatorname{char} F = 0$ или $\operatorname{char} F \geqslant k$.*

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 $t \geqslant 2$, то $P'(a) = 0$.

2. Если a — корень кратности $\geqslant k$ в P, то a — корень кратности $\geqslant k-1$ в $P' \implies \ldots \implies a$ — корень кратности $\geqslant 1$ 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 $\operatorname{char} F = 0$ или $t < \operatorname{char} F$, 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 $t-2 \implies \ldots \implies a$ — корень $P^{(t)}$ кратности 0, то есть, не корень. Таким образом, если $\operatorname{char} F = 0$ или $k \leqslant \operatorname{char} F$, то случай $t < k$ невозможен, иначе $P^{(t)}(a) \neq 0$. Поэтому $t \geqslant k$.

□

Пример. Рассмотрим многочлен $Q = x^p - 1 \in \mathbb{Z}_p[x]$. У него есть корень $a = 1$ кратности $\leqslant p$. С другой стороны, $Q' = px^{p-1} = 0 = Q'' = Q''' = \ldots$ Таким образом, $Q(1) = Q'(1) = Q''(1) = \ldots = 0$. Значит третье утверждение применимо прим $k = p$, следовательно, 1 — корень Q кратности $\geqslant p$. 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_i — это линейное отображение $\varphi : V \to V$, 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 $e = (\vec{e}_1, \ldots, \vec{e}_n)$ — базис в V, то φ однозначно задается свое матрицей в базисе

$$\varphi \underset{e}{\leftrightarrow} A$$

  Такой, что $\varphi(e) = (\varphi(\vec{e}_1), \ldots, \varphi(\vec{e}_n)) = eA$. 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 сопоставление $\varphi \underset{e}{\leftrightarrow} A$ 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 $A' = S^{-1}AS$.

* 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, $\varphi \in \mathcal{L}(V), U \leqslant V$. 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. Это свойство достаточно проверять для базиса в U.

Напоминание.

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

* Образ линейного оператора: $\varphi \in \mathcal{L}(V) \implies \operatorname{Im}\varphi = \varphi(V) \leqslant V$

∗ Ядро линейного оператора: $\operatorname{Ker}\varphi = \varphi^{-1}(\vec{0}) \leqslant V$

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

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

$$\varphi \underset{e}{\leftrightarrow} A = \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array}\right)$$

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

Замечание 1. Если U — φ инвариантно и

$$\varphi \underset{e}{\leftrightarrow} \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array}\right)$$

то $\varphi|_U \underset{(\vec{e}_1, \ldots, \vec{e}_k)}{\longleftrightarrow} B$.

Замечание 2. 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

$$\varphi \underset{e}{\leftrightarrow} A = \left(\begin{array}{c|c} B & 0 \\ \hline 0 & C \end{array}\right)$$

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 $\vec{u} = \vec{u}_1 + \vec{u}_2 \implies \varphi(\vec{u}) = \varphi(\vec{u}_1) + \varphi(\vec{u}_2) \in U_1 + U_2$

□

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

Доказательство. Пусть $\vec{u} \in \operatorname{Ker}\psi$, то есть, $\psi(\vec{u}) = \vec{0}$. Необходимо проверить, что $\varphi(\vec{u}) \in \operatorname{Ker}\psi$, 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 $\vec{u} \in \operatorname{Im}\psi$, то есть, $\vec{u} = \psi(\vec{v}), \vec{v} \in V$. Тогда $\varphi(\vec{u}) = \varphi(\psi(\vec{v})) = \psi(\varphi(\vec{v})) \in \operatorname{Im}\psi$ □

Замечание. Мы будет 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

Определения

Глава 1

Глава 2

Утверждения

Глава 1

Глава 2