Содержание

1 Полилинейная алгебра

1.1 Тензорная алгебра. Тензорное произведение

Тензорное произведение.

$V_1, \ldots, V_n$ — векторные пространства над одним и тем же полем.

Определение 1 *Полилинейное отображение* $\varphi : V_1 \times V_2 \times \ldots \times V_n \to U$

Пространство $\mathrm{Hom}(V_1, \ldots, V_n, U)$. Если все пространства конечномерны, то $\dim \mathrm{Hom}(V_1, \ldots, V_n, U) = \dim V_1 \ldots \dim V_n \cdot \dim U$ Попробуем свести изучение полилинейных отображений к изучению линейных. Для этого потребуются некоторые дополнительные конструкции.

- Пространство M — множество всех финитных функций $V_1 \times \ldots \times V_n \longrightarrow K$ с покоординатным сложением и умножением на скаляры из K. Иными словами

$$M = \{\sum a_{v_1,\ldots,v_n}(v_1, \ldots, v_n) | a_{v_1,\ldots,v_n} \in K\}$$

- M_0 — подпространство M, заданное порождающими

$$M_0 := \langle \begin{pmatrix} (v_1, \ldots, v'_k + v''_k, \ldots, v_n) - (v_1, \ldots, v'_k, \ldots, v_n) - (v_1, \ldots, v''_k, \ldots, v_n) \\ (v_1, \ldots, \alpha v'_k, \ldots, v_n) - \alpha(v_1, \ldots, v_k, \ldots, v_n),\ \alpha \in K \end{pmatrix} \rangle$$

- **Определение 2** *Определим тензорное произведение*

$$V_1 \otimes \ldots \otimes V_n := M/M_0$$
$$v_1 \otimes \ldots \otimes v_n := (v_1, \ldots, v_n) + M_0$$
$$t := V_1 \times \ldots \times V_n \longrightarrow V_1 \otimes \ldots \otimes V_n$$
$$(v_1, \ldots, v_n) \mapsto v_1 \otimes \ldots \otimes v_n.$$

Определение 3 $v_1 \otimes \ldots \otimes v_n$ *— разложимый тензор.*

Лемма 1 *Разложимые тензоры порождают все пространство* $V_1 \otimes \ldots \otimes V_n$

Теорема 1 *1. Отображение* t *полилинейно.*

2. Отображение t *универсально. Т.е.* $\forall s \in \mathrm{Hom}(V_1, \ldots, V_n, U)$ *существует единственное линейное* $f : V_1 \otimes \ldots \otimes V_n \longrightarrow U$ *такое, что* $s = f \circ t$.

Доказательство(см. [4, p262])

1. Нужно проверить, что

$$v_1 \otimes \ldots \otimes (v'_i + v''_i) \otimes \ldots \otimes v_n = v_1 \otimes \ldots \otimes v'_i \otimes \ldots \otimes v_n + \\ + v_1 \otimes \ldots \otimes v''_i \otimes \ldots \otimes v_n$$

   и

$$v_1 \otimes \ldots \otimes \alpha v_i \otimes \ldots \otimes v_n = \alpha v_1 \otimes \ldots \otimes v_i \otimes \ldots \otimes v_n.$$

   Оба равенства следуют из определения M_0.

2. Единственность следует из того, что разложимые тензоры порождают $V_1 \otimes \ldots \otimes V_n$, а равенство $f \circ t = s$ однозначно определяет значение f на разложимых тензорах. Покажем существование f. Рассмотрим линейное отображение

$$g : M \longrightarrow U$$

   заданное на базисных векторах равенством $g(e_1, \ldots, e_n) = s(e_1, \ldots, e_n)$. В силу линейности $M_0 \subseteqq \mathrm{Ker}\, g$, а значит g индуцирует отображение $f : M/M_0 = V_1 \otimes \ldots \otimes V_n \longrightarrow U$.

□

Следствие 1 *1. Отображение*

$$\begin{aligned}\mathrm{Hom}(V_1,\ldots,V_n,U) &\longrightarrow \mathrm{Hom}(V_1\otimes\ldots\otimes V_n,U)\\ s &\mapsto f\end{aligned}$$

является каноническим изоморфизмом векторных пространств.

2. $(V_1\otimes\ldots\otimes V_m)^*\cong\mathrm{Hom}(V_1,\ldots,V_m,K)$*;*

3. $\dim(V_1\otimes\ldots\otimes V_n)=\dim V_1\cdots\dim V_n$.

4. Если $e_1^{(i)},\ldots,e_{k_i}^{(i)}$ *— базис* V_i*, то* $e_{i_1}^{(1)}\otimes\ldots\otimes e_{i_n}^{(n)}$ *— базис* $V_1\otimes\ldots\otimes V_n$.

Доказательство

1. Очевидно, что построенное отображение является гомоморфизмом векторных пространств. Оно сюръективно в силу полилинейности t. Инъективно, т.к. если $f=0$, то $s=f\circ t=0$.

2.

$$\begin{aligned}\dim(V_1\otimes\ldots\otimes V_n)=\dim(V_1\otimes\ldots\otimes V_n)^*=\\ =\dim\mathrm{Hom}(V_1,\ldots,V_n,K)=\dim V_1\cdots\dim V_n\end{aligned}$$

3. $e_{i_1}^{(1)}\otimes\ldots\otimes e_{i_n}^{(n)}$ порождают все разложимые тензоры и их нужное количество.

□

1.1.1 Расширение скаляров.

Комплексификация пространства. Пусть V — векторное пространство над полем $\mathbb{R}$ с базисом $e_1,\ldots,e_n$. Посмотрим на комплексифицированное пространство $V^{\mathbb{C}}$ с новой точки зрения. Поскольку $\mathbb{C}$ — двумерное векторное пространство над полем $\mathbb{R}$, то можно определить $\mathbb{C}\otimes V$. Выше было показано, что $1\otimes e_1\ldots.,1\otimes e_n,i\otimes e_1,\ldots,i\otimes e_n$ — базис $\mathbb{C}\otimes V$. Рассмотрим $\mathbb{R}$-линейное отображение

$$\begin{aligned}\mathbb{C}\otimes V &\longrightarrow V^{\mathbb{C}}\\ 1\otimes e_j &\mapsto e_j\\ i\otimes e_j &\mapsto ie_j.\end{aligned}$$

Оно является изоморфизмом векторных пространств.

Расширение скаляров. Конструкцию, описанную выше можно обобщить. Пусть K и L - поля, причем $K \subset L$. Пусть V — векторное пространство над K. Рассмотрим L как векторное пространство над K и построим $L \otimes V$. На $L \otimes V$ введем структуру векторного пространства над L:

$$\alpha(\beta \otimes v) = \alpha\beta \otimes v,\ \alpha, \beta \in L, v \in V.$$

Непосредственно проверяется, что формула выше корректно определяет структуру векторного пространства на $L \otimes V$. (корректнее сначала ввести $\alpha(\beta, v) = (\alpha\beta, v)$ на множестве M.)

1.1.2 Канонические изоморфизмы

Ассоциативность Пространства $V_1 \otimes V_2 \otimes V_3$ и $(V_1 \otimes V_2) \otimes V_3$ изоморфны. Это позволяет в дальнейшем "игнорировать скобки". Опишем этот изоморфизм.

$$V_1 \times V_2 \times V_3 \longrightarrow (V_1 \otimes V_2) \otimes V_3$$
$$(v_1, v_2, v_3) \mapsto (v_1 \otimes v_2) \otimes v_3$$

Поскольку образ базиса снова базис, получили изоморфизм.
Коммутативность

$$V_1 \times V_2 \longrightarrow (V_2 \otimes V_1)$$
$$(v_1, v_2) \mapsto (v_2 \otimes v_1)$$

Поскольку образ базиса снова базис, получили изоморфизм.
Двойственность

$$V_1^* \otimes \ldots \otimes V_n^* \longrightarrow (V_1 \otimes \ldots \otimes V_n)^*.$$

В силу пункта 2 следствия 1 $(V_1 \otimes \ldots \otimes V_n)^* \cong \mathrm{Hom}(V_1, \ldots, V_n, K)$;

$$V_1^* \times \ldots \times V_n^* \longrightarrow \mathrm{Hom}(V_1, \ldots, V_n, K)$$
$$(f_1, \ldots, f_n) \mapsto ((v_1 \times \ldots \times v_n) \mapsto f_1(v_1) \ldots f_n(v_n))$$

Полученное отображение сюръективно и пространства имеют одинаковую размерность.

$$\mathrm{Hom}(U, V) \longrightarrow U^* \otimes V$$

1.1.3 Тензорная алгебра.

$$T_p^q(V) := \underbrace{V^* \otimes \ldots \otimes V^*}_{p} \otimes \underbrace{V \otimes \ldots \otimes V}_{q}.$$

Примеры:

1. $T_0^0 := K$;
2. $T_1^0 = V^*$;
3. $T_0^1 = V$;
4. $T_1^1 = V^* \otimes V = \mathrm{Hom}(V, V)$;
5. $T_2^0 := V^* \otimes V^* = (V \otimes V)^* = \mathrm{Hom}(v, v; K)$;

Тензорное умножение. **Способ 1.**

$$T_p^q(V) \cong \underbrace{V^* \otimes \ldots \otimes V^*}_{p} \otimes \underbrace{V \otimes \ldots \otimes V}_{q} \cong \mathrm{Hom}(\underbrace{V, \ldots, V}_{p}, \underbrace{V^*, \ldots, V^*}_{q}; K)$$

$$(f \otimes g)(v_!, \ldots, v_p, v'_1, \ldots, v'_{p'}, f_1, \ldots, f_q, f'_1, \ldots, f'_{q'}) = f()g().$$

Замечание 1

$$(af_1 + bf_2) \otimes g = a(f_1 \otimes g) + b(f_2 \otimes g)$$
$$f \otimes (ag_1 + bg_2) = a(f \otimes g_1) + b(f \otimes g_2)$$
$$(f \otimes g) \otimes h = f \otimes (g \otimes h).$$

Способ 2.

Определение 4 *Тензорная алгебра*

$$T(V) := \bigoplus T_p^q(V);$$

Тензоры в координатах. Пусть $e = (e_1, \ldots, e_n)$ базис V, $e' = (e^1, \ldots, e^n)$ дуальный базис V^*. Тогда $\{e^{i_1} \otimes \ldots \otimes e^{i_p} \otimes e_{j_1} \otimes \ldots \otimes e_{j_q} | 1 \leqslant i_k, j_l \leqslant n\}$ — базис $T_p^q(V)$.

$$T = \sum T_{i_1 \ldots i_p}^{j_1 \ldots j_q} e^{i_1} \otimes \ldots \otimes e^{i_p} \otimes e_{j_1} \otimes \ldots \otimes e_{j_q}$$

Изменение координат при замене базиса.

классическое определение

1.1.4 Симметричные тензоры.

Пусть V — конечномерное векторное пространство над полем K нулевой характеристики.

S_q действует на $T_0^q(V)$, причем для $\sigma \in S_q$ и разложимого тензора $v_1 \otimes \ldots \otimes v_q$

$$f_\sigma(v_1 \otimes \ldots \otimes v_q) = v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(q)}.$$

Определим подпространство симметричных тензоров в $T_0^q(V)$

$$S^q(V) = \{T \in T_0^q(V) | f_\sigma T = T, \forall \sigma \in S_q\}$$

Пусть $\operatorname{char} K = 0$ или $\operatorname{char} K \nmid q!$. Положим

$$S := \frac{1}{q!} \sum_{S_q} f_\sigma.$$

Заметим, что при гомоморфизме S образы элементов из одной орбиты относительно действия S_q совпадают.

Предложение 1 *$S^2 = S$ и $\operatorname{Im} S = S^q(V)$, т.е. S — проектор $T_0^q(V)$ на $S^q(V)$.*

Доказательство Ясно, что $\operatorname{Im} S \subseteqq S^q(V)$. Легко видеть, что $S|_{S^q} = \mathrm{id}$, т.е $\operatorname{Im} S = S^q(V)$, $S^2 = S$. □

Предложение 2 *Пусть $e = (e_1, \ldots, e_n)$ базис V, тогда*

1. *$e_{i_1} \ldots e_{i_q} = S(e_{i_1} \otimes \ldots \otimes e_{i_q})$ — базис $S^q(V)$.*
2. *$S^q(V) \cong \{f \in K[x_1, \ldots, x_n] | \deg f = q\}$;*
3. *$\dim S^q(V) = C_q^{n+q-1}$.*

Доказательство Элементы $e_{i_1} \ldots e_{i_q}$ порождают S_q, т.к. являются образами базисных векторов при эпиморфизме $S : T_0^q \longrightarrow S^q$. Элемент $e_{i_1} \ldots e_{i_q}$ не изменится при перестановке индексов, поэтому всякий такой элемент может быть единственным образом записан в виде $e_1^{k_1} \ldots e_n^{k_n}$, $k_1 + \ldots + k_n = q$. Покажем, что тензоры $e_1^{k_1} \ldots e_n^{k_n}$, $k_1 + \ldots + k_n = q$ линейно независимы. Пусть

$$\sum a_{k_1,\ldots,k_n} e_1^{k_1} \ldots e_n^{k_n} = 0.$$

Тогда $S(\sum a_{k_1,\ldots,k_n} e_1^{\otimes k_1} \otimes \ldots \otimes e_n^{\otimes k_n}) = 0$ т.е. $(\sum \sum_{S_q} a_{k_1,\ldots,k_n} f_\sigma e_1^{\otimes k_1} \otimes \ldots \otimes e_n^{\otimes k_n}) = 0$. В последнем выражении при базисных элементах возникают коэффициенты, равные некоторым ненулевым коэффициентам, умноженным на $a_{k_1,\ldots,k_n}$, поэтому все $a_{k_1,\ldots,k_n}$ равны нулю. □
Симметрическая алгебра пространства V

$$S(V) := \bigoplus S^q(V)$$

введем умножение:

$$T_1 T_2 := S(T_1 \otimes T_2)$$

Предложение 3 *$S(V)$ — коммутативная ассоциативная алгебра над K.*

Доказательство Проверим, что

$$S(S(T_1)\otimes T_2) = S(T_1\otimes S(T_2)) = S(T_1\otimes T_2),\ \forall T_1\in T_0^p(V), T_2\in T_0^q(V).$$

Действительно, $S(T_1)\otimes T_2 = \frac{1}{p!}\sum_{S_p} f_\sigma(T_1)\otimes T_2$, откуда

$$S(S(T_1)\otimes T_2) = \frac{1}{p!}\sum_{S_p} S(f_\sigma(T_1)\otimes T_2) = \frac{1}{p!}\sum_{S_p} S(T_1\otimes T_2) = S(T_1\otimes T_2).$$

Отсюда можно получить ассоциативность.

$$(T_1T_2)T_3 = S(S(T_1\otimes T_2)\otimes T_3) = S(T_1\otimes T_2\otimes T_3) = T_1(T_2T_3).$$

Заметим, что

$$(e_1^{k_1}\dots e_n^{k_n})(e_1^{l_1}\dots e_n^{l_n}) = e_1^{k_1+l_1}\dots e_n^{k_n+l_n}.$$

Равенство $S(T_1\otimes T_2) = S(T_2\otimes T_1)$ очевидно для разложимых тензоров и по линейности выполняется для всех тензоров.□

1.1.5 Внешняя алгебра (алгебра Грассмана).

Определим подпространство антисимметричных тензоров в $T_0^q(V)$

$$\Lambda^q(V) = \{T\in T_0^q(V) | f_\sigma T = \mathrm{sgn}(\sigma)T,\ \forall\sigma\in S_q\}$$

Положим

$$A := \frac{1}{q!}\sum_{S_q}\mathrm{sgn}(\sigma)f_\sigma.$$

Предложение 4 $A^2 = A$ *и* $\mathrm{Im}\,A = \Lambda^q(V)$, *т.е.* A *— проектор* $T_0^q(V)$ *на* $\Lambda^q(V)$.

Доказательство

$$f_\sigma(AT) = f_\sigma(\frac{1}{q!}\sum_{S_q}\mathrm{sgn}(\sigma)f_\tau T) = \frac{1}{q!}\sum_{\tau\in S_q}\mathrm{sgn}(\sigma)f_{\sigma\tau}T =$$
$$= \mathrm{sgn}(\sigma)\frac{1}{q!}\sum_{\tau\in S_q}\mathrm{sgn}(\sigma\tau)f_{\sigma\tau}T = \mathrm{sgn}(\sigma)AT$$

Далее

$$A^2 = \frac{1}{(q!)^2}\sum_{\sigma,\tau}\mathrm{sgn}(\sigma\tau)f_{\sigma\tau} = A.$$

□

Пусть $e = (e_1, \ldots, e_n)$ базис V, тогда $e_{i_1} \wedge \ldots \wedge e_{i_q} = A(e_{i_1} \otimes \ldots \otimes e_{i_q})$ — порождают $\Lambda^q(V)$. Заметим, что

$$f_\sigma(e_{i_1} \wedge \ldots \wedge e_{i_q}) = \operatorname{sgn}(\sigma)(e_{i_1} \wedge \ldots \wedge e_{i_q}),$$

поэтому $e_{i_1} \wedge \ldots \wedge e_{i_q} = 0$ при $i_l = i_s$ для некоторых l и s.

Предложение 5 *1. При $q \leqslant n$ тензоры $e_{i_1} \wedge \ldots \wedge e_{i_q}$, $1 \leqslant i_1 < i_2 < \ldots < i_q \leqslant n$ образуют базис пространства $\Lambda^q(V)$.*

2. При $q > n$ $\Lambda^q(V) = 0$.

3. $\dim \Lambda^q(V) = C_n^q$, $\dim \bigoplus_{q=0}^n \Lambda^q(V) = 2^n$.

Доказательство Покажем, что тензоры $e_{i_1} \wedge \ldots \wedge e_{i_q}$ линейно независимы. Пусть

$$\sum a_{i_1,\ldots,i_q} e_{i_1} \wedge \ldots \wedge e_{i_q} = 0.$$

Тогда $A(\sum a_{i_1,\ldots,i_q} e_{i_1} \otimes \ldots \otimes e_{i_q}) = 0$, т.е. $a_{i_1,\ldots,i_q} = 0$. $\square$

$$\Lambda(V) := \bigoplus_{q=0}^{n} \Lambda^q(V)$$

Введем умножение

$$T_1 \wedge T_2 = A(T_1 \otimes T_2); T_1 \in \Lambda^p(V), T_2 \in \Lambda^q(V)$$

Предложение 6 $\Lambda(V)$ — *косокоммутативная(т.е. $T_2 \wedge T_1 = (-1)^{pq} T_1 \wedge T_2$) ассоциативная алгебра над K.*

Доказательство Проверим, что

$$A(A(T_1) \otimes T_2) = A(T_1 \otimes A(T_2)) = A(T_1 \otimes T_2),\ \forall T_1 \in T_0^p(V), T_2 \in T_0^q(V).$$

Действительно,

$$A(T_1) \otimes T_2 = \frac{1}{p!} \sum_{\sigma \in S_p} \operatorname{sgn}(\sigma) f_\sigma(T_1) \otimes T_2,$$

поэтому

$$A(A(T_1) \otimes T_2) = \sum_{\sigma \in S_p} \operatorname{sgn}(\sigma) A(f_\sigma(T_1) \otimes T_2)$$

Замечание 2 *Внешнюю алгебру можно было бы определить и по-другому:*

1.2 Вещественная структура

Пусть V произвольное векторное пространство над $\mathbb{C}$. В некоторых случаях V может быть представлено как комплексификация вещественного пространства. Пусть σ вещественно линейный комплексно антилинейный (т.е. $\sigma(zv) = \bar{z}\sigma(v)$) оператор $V_{\mathbb{R}} \longrightarrow V_{\mathbb{R}}$, причем $\sigma^2 = \mathrm{id}$. Тогда

$$V_{\mathbb{R}} = \mathrm{Ker}(\sigma - 1) \oplus \mathrm{Ker}(\sigma + 1).$$

При этом, т.к. $\sigma(iv) = -i\sigma(v)$, умножение на i — изоморфизм пространств $\mathrm{Ker}(\sigma-1)$ и $\mathrm{Ker}(\sigma+1)$. Таким образом $V_{\mathbb{R}} = W \oplus iW$. Далее, легко проверить, что $(a+ib)\cdot(v_1+iv_2) = (av_1 - bv_2) + i(bv_1 + av_2)$. Из последнего следует, что

$$V = \mathbb{C} \otimes_{\mathbb{R}} W.$$

2 Тело кватернионов

На 4-х мерном пространстве $V = \mathrm{Mat}_2(\mathbb{C})$ рассмотрим вещественно линейный комплексно антилинейный ($\sigma(zA) = \bar{z}\sigma(A)$) оператор σ

$$A \mapsto \overline{Adj(A)}^T$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{d} & -\bar{c} \\ -\bar{b} & \bar{a} \end{pmatrix}$$

Замечание 3 *Заметим, что $\sigma(AB) = \sigma(A)\cdot\sigma(B)$ для $A, B \in \mathrm{Mat}_2(\mathbb{C})$.*

Легко видеть, что $\sigma(zv) = \bar{z}\sigma(v)$ и $\sigma^2 = 1$(т.е.σ — комплексное сопряжение). Рассмотрим σ как эндоморфизм $V_{\mathbb{R}}$, получим $V_{\mathbb{R}} = \mathrm{Ker}(\sigma - 1) \oplus \mathrm{Ker}(\sigma + 1)$. Собственное подпространство $V_{\mathbb{R}}$, соответствующее собственному значению 1 имеет базис

$$1 = e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

$\mathbb{H} := \mathrm{Ker}(\sigma - id)$ — подалгебра в алгебре матриц. Отметим, что

$$i^2 = j^2 = k^2 = -1,$$
$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

Получилась ассоциативная алгебра.

Замечание 4 *Алгебру кватернионов можно было бы определить сразу как вещественное векторное пространство с базисом $1, i, j, k$ и заданным умножением.*

Определение 5 *1.* $\mathbb{R} \subset \mathbb{H}$ *— пространство чисто вещественных кватернионов.*

2. $I = \{x \cdot i + y \cdot j + z \cdot k | x, y, z \in \mathbb{R}\}$ *— пространство чисто мнимых кватернионов.*

На языке матриц $I = \{A \in \mathrm{Mat}_2 \mathbb{C} | \bar{A}^T = -A, \mathrm{tr}\, A = 0\}$. Сопряжение $\overline{a + bi + cj + dk} = a - bi - cj - dk$ или $A^* = \bar{A}^T$.

Скалярное произведение $(u, v) = \mathrm{Re}(u \cdot \bar{v})$. Соответственно $||u|| = u \cdot \bar{u}$.

Лемма 2 *1.* $\forall u \in \mathbb{H}\ u^{-1} = \frac{\bar{u}}{||u||^2}$*;*

2. $\mathrm{Im}(uv) = u \times v\ \forall u, v \in I$*;*

Доказательство(см. [5, p 392])

1. проверяется непосредственно;
2. И правая и левая части — билинейные отображения $I \times I \longrightarrow I$. А на базисных векторах равенство проверяется непосредственно.

3 О расширениях полей.

Определение 6 • *расширение полей*

- *Если* L/K *— расширение полей, то поле* L *можно рассматривать как векторное пространство над* K*. Степенью расширения* L/K *называется* $[L : K] = \dim_K L$*.*
- *Пусть* K *подполе* L*.*
  1. *Элемент* $\alpha \in L$ *называется алгебраическим над* K*, если существует* $f(x) \in K[x]$*,* $f \neq 0$ *такой, что* $f(\alpha) = 0$*.*
  2. *Элемент* $\alpha \in L$ *называется трансцендентным над* K*, если он не является алгебраическим.*
- *Расширение* L/K *алгебраическое, если всякий элемент поля* L *является алгебраическим над* K*.*

Лемма 3 *1. Всякое конечное расширение является алгебраическим.*

2. Пусть $M \subset K \subset L$ *— башня расширений полей. Тогда* $[L : M] = [L : K] \cdot [K : M]$*.*

3.1 Конструкции

Пусть L/K — расширение полей и $\alpha \in L$.

Заметим, что $I_\alpha = \{p(x) \in K[x] | p(\alpha) = 0\}$ — идеал в $K[x]$, а значит имеет вид $(f(x))$, где $f(x)$ многочлен наименьшей степени среди многочленов, имеющих корень α. Если α алгебраический, то $I_\alpha \neq 0$ и многочлен $f(x)$ называется наименьшим многочленом элемента α. Заметим, что $f(x)$ неприводим над K.

Положим $K(\alpha) = \bigcap_{M \subseteqq L,\, \alpha \in M} M$ — наименьшее подполе L, содержащее K и α.

Лемма 4 *Пусть L/K — расширение полей и $\alpha \in L$. Тогда возможен один и только один из двух случаев*

1. $K(\alpha) = K[\alpha] \cong K[x]/(f(x))$, *$\alpha$ алгебраический над K и* $f(\alpha) = 0$.
2. $K(\alpha) \cong K(x) = \operatorname{Quot} K[x]$ *и α трансцендентный над K.*

Доказательство Рассмотрим гомоморфизм колец

$$\theta : K[x] \longrightarrow K[\alpha]$$
$$g(x) \mapsto g(\alpha).$$

По определению $I_\alpha = \operatorname{Ker}\theta$, $K[\alpha] = \operatorname{Im}\theta$, поэтому $K[\alpha] \cong K[x]/I_\alpha$. Если $I_\alpha \neq \{0\}$, то $I_\alpha \neq \{0\} = (f)$, α алгебраический над K и $K[\alpha]$ — поле. Если $I_\alpha = \{0\}$, то α трансцендентный над K. $\square$

Определение 7 *Расширения M/K и L/K эквивалентны, если существует изоморфизм $M \longrightarrow L$ тождественный на K.*

Предложение 7 *Для всякого поля K и неприводимого многочлена $f(x) \in K[x]$ существует одно (с точностью до эквивалентности) простое алгебраическое расширение $K(\alpha)$ такое, что α является корнем многочлена $f(x)$. При этом $[K(\alpha) : K] = \deg f$.*

Доказательство(см.[7, гл VI])Можем считать, что $f(x)$ не является линейным. В кольце главных идеалов $K[x]$, простой идеал $f(x)K[x]$ является максимальным, а значит кольцо вычетов $M := K[x]/(f(x))$ является полем. Имеется вложение

$$K \hookrightarrow M$$
$$a \mapsto \bar{a} = a + (f(x)).$$

В поле M элемент $\bar{x}$ является корнем многочлена $f(x)$. Таким образом M — расширение поля K, содержащее корень многочлена f.

Лемма 5 *1. Конечные расширения и только они получаются присоединением конечного числа элементов.*

2. Если α, β — алгебраические над K, то $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ тоже.

3. Если L/K и K/M алгебраические, то L/M тоже.

Доказательство

1. Конечные расширения и только они получаются присоединением конечного числа элементов.
2. Если α, β — алгебраические над K, то $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ тоже.
3. Если $\alpha \in L$ алгебраичен над K, то $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$ для некоторых $\alpha_i \in K$. Расширения $M(a_0, a_1, \ldots, a_n)/M$ и $M(a_0, a_1, \ldots, a_n)(\alpha)/M(a_0, a_1, \ldots, a_n)$ конечны, а значит $M(a_0, a_1, \ldots, a_n)(\alpha)/M$ конечно, и, следовательно α алгебраичен над M.

Определение 8 *Поле,полученное присоединением всех корней многочлена f назовем полем разложения многочлена f.*

Лемма 6 *Для всякого многочлена существует его поле разложения, причем поля разложения одного многочлена эквивалентны.*

Эквивалентность полей разложения будет обоснована чуть позже.

3.2 Алгебраическое замыкание.

Теорема 2 *Для всякого поля K существует расширение $\bar{K}$ алгебраическое над K и алгебраически замкнутое.*

Доказательство Построим сначала расширение L_1 поля K, в котором всякий многочлен $K[x]$ имеет корень.

Рассмотрим кольцо $R := K[X_f]_{f \in K[X]}$ и идеал I, порожденный многочленами $f(X_f)$. $I \neq R$, действительно, пусть

$$g_1 f_1(X_{f_1}) + \ldots + g_n f_n(X_{f_n}) = 1,\ g_i \in R.$$

Пусть M — конечное расширение поля K, содержащее корни всех многочленов $f_1, \ldots, f_n$. Тогда, подставив, эти корни получаем в поле M соотношение $0 = 1$. Пусть $\mathcal{M}$ — максимальный идеал, содержащий I, тогда $L := R/I$ – поле. Пусть π проекция $R \longrightarrow R/I$. Ясно, что L — расширение $\pi(K)$. Для любого $f \in K[X]$, многочлен f^π имеет корень в R/I.

Построим расширение L поля L_1, в котором любой многочлен имеет корень.

Построим цепочку $L_1 \subsetneqq L_2 \subsetneqq \ldots$, такую, что всякий многочлен $f \in L_n[X]$ степени $\geqslant 1$ имеет корень в L_{n+1}. Положим $L = \cup L_n$. L искомое поле.

Построим $\bar{K}$

Положим $\bar{K}$ — объединение всех подрасширений из L, алгебраических над K.

□

3.3 Продолжения изоморфизмов.

Пусть $\sigma : K \longrightarrow L$ гомоморфизм полей и $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$. Обозначим

$$\sigma(f) = f^\sigma = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n.$$

Замечание 5 *Если α — корень многочлена f поле K, то $\sigma(\alpha)$— корень многочлена f^σ в поле L.*

Предложение 8 *Пусть L/K и L'/K' — расширения полей. $f(x) \in K[x]$.$\varphi : K \longrightarrow K'$ изоморфизм полей.*

1. *Пусть f неприводим, α — корень многочлена f в поле L, α' — корень многочлена f^φ в поле L'. Тогда φ продолжается до изоморфизма $\varphi' : K(\alpha) \longrightarrow K(\alpha')$, при котором α переходит в α'.*
2. *Изоморфизм φ продолжается до изоморфизма полей разложения многочленов f и f^φ соответственно.*

Определение 9 *Пусть $\bar{K}$ —алгебраическое замыкание поля K. Элементы поля $\bar{K}$, лежащие в одной орбите относительно действия группы $\mathrm{Aut}_K \bar{K} = \{\sigma \in \mathrm{Aut}\,\bar{K} | \sigma|_K = \mathrm{id}\}$ называются сопряженными элементами.*

Замечание 6 *Элементы, сопряженные с α — все корни наименьшего многочлена f_α.*

Определение 10 *Алгебраическое расширение L/K называется нормальным, если всякий неприводимый многочлен над K, имеющий корень в L раскладывается в L на линейные множители.*

3.4 Кратные корни

Пусть $f \in K[x]$.

Замечание 7 *1. Многочлен $f(x)$ имеет кратные корни тогда и только тогда, когда $(f, f') \neq K[x]$.*

2. Если неприводимый многочлен f имеет кратные корни, то $f' = 0$.

Лемма 7 *Пусть* $\deg f > 1$ *и f неприводим. Тогда*

1. *Если* $\operatorname{char} K = 0$*, то многочлен f не имеет кратных корней.*
2. *Если* $\operatorname{char} K = p$*, то многочлен f имеет кратные корни тогда и только тогда, когда он имеет вид $f(x) = g(x^p)$, $g \in K[x]$.*

Определение 11 *Пусть* $\operatorname{char} K = p$ *и $f = g(x^{p^e})$ и g не имеет кратных корней. Назовем* $\deg g$ *редуцированной степенью f.*

3.5

Лемма 8 *Пусть $K \subsetneqq L, \alpha \in L$, f — минимальный многочлен элемента α над K причем f раскладывается на линейные множители в L. Пусть m — редуцированная степень f в случае, если* $\operatorname{char} K = p$ *и $m =$* $\deg f$ *если* $\operatorname{char} K = 0$. *Пусть $\sigma : K \longrightarrow L$ — вложение. Тогда существует ровно m продолжений σ до вложения $K(\alpha) \longrightarrow L$.*

Доказательство Каждое продолжение гомоморфизма σ на $K(\alpha)$ переводит α в сопряженный с ним элемент и однозначно определяется образом элемента α. У α ровно m сопряженных и каждый из них определяет продолжение σ. $\square$

Пусть L/K — конечное расширение полей и $\sigma : K \longrightarrow M$ вложение K в алгебраически замкнутое поле M. Пусть $[L : K]_s$ количество продолжения σ до вложения $L \longrightarrow M$

Лемма 9 *1. $[L : K]_s$ не зависит от M.*

2. Если $K - L - M$ башня расширений, то $[M : K]_s = [M : L]_s \cdot [L : K]_s$.

3. $[L : K]_s \leqslant [L : K]$.

Следствие 2 *Пусть L/K — конечное расширение. Тогда* $|\operatorname{Aut}_K L| \leqslant |L : K|$.

3.6 Конечные поля

Напоминание. Было утв.

Предложение 9 *1. Пусть F — конечное поле, тогда $|F| = p^m$, где p — простое число, равное характеристике поля F.*

2. Если F — поле из q элементов, то $a^{q-1} = 1$, $\forall a \in F$.

Так как поле из p^n элементов можно рассматривать как поле разложения многочлена $x^{p^n} - x$ над $\mathbb{F}_p$, то нетрудно получить следующую лемму

Лемма 10 *Конечные поля одного порядка изоморфны.*

Предложение 10 *1. Для всякого простого p и натурального n существует поле из p^n элементов.*

2. Для всякого m с точностью до эквивалентности существует ровно одно расширение поля $\mathbb{F}_q$ степени m и это $\mathbb{F}_{q^m}$.

Доказательство Построим поле разложения многочлена $x^{p^n} - x$ над $\mathbb{F}_p$ и рассмотрим множество корней этого многочлена в нем. Получим искомое поле. В нем p^n элементов, т.к. многочлен $x^{p^n} - x$ не имеет кратных корней. □

Автоморфизмы конечного поля Пусть $q = p^n$.

Определение 12 *Гомоморфизм*

$$\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$$
$$x \mapsto x^p$$

называется гомоморфизмом Фробениуса.

Лемма 11 *φ автоморфизм поля $\mathbb{F}_q$ и $\operatorname{Aut}\mathbb{F}_q = \langle\varphi\rangle$, т.е. $\operatorname{Aut}\mathbb{F}_q$ циклическая группа порядка n.*

Доказательство Т.к. все автоморфизмы сохраняют $\mathbb{F}_p$, то $|\operatorname{Aut}\mathbb{F}_q| \leqslant [\mathbb{F}_q : \mathbb{F}_p] = n$.

В силу конечности поля и инъективности φ, легко видеть, что φ автоморфизм и $\operatorname{ord}\varphi \mid n$. Пусть $\operatorname{ord}\varphi = d$. Тогда $x = \varphi^d(x) = x^{p^d}$, $\forall x \in \mathbb{F}_q$. Но $x^d - x$ имеет не более чем d корней, а значит $n \leqslant d$. □

Список литературы

[1] http://alexei.stepanov.spb.ru/students/temp/conspect.pdf

[2] Кострикин А.И. "Введение в алгебру". Часть II. Линейная алгебра.

[3] Э.Б. Винберг "Курс алгебры"

[4] А.И. Кострикин, Ю.И. Манин "Линейная алгебра и геометрия"

[5] А.Л. Городенцев "Алгебра-1"учебник для студентов-математиков первого курса

[6] Аржанцев И. В. "Базисы Грчбнера и системы алгебраических уравнений". Ч М.: МЦНМО, 2003. Ч 68 с

[7] ван дер Варден "Алгебра"