Алгебра и теория чисел

Курс Жукова И.Б.

Осень 2022 г.

Оглавление

Глава 1

Алгебра линейных операторов

Определение 1.1. V - линейное пространство над полем K. Линейный оператор на V — линейное отображение $V \to V$ (эндоморфизм линейного пространства V)

Определение 1.2. $\operatorname{End} V = \operatorname{Hom}(V, V)$ - множество линейных операторов.

$$\mathcal{A} \in \operatorname{Hom}(V, W) \quad [\mathcal{A}]_{E,F}$$

Имея два пространства V и W, базисы E и F можно выбрать так, что матрица получится окаймленной единичной.

Теперь же мы имеем одно пространство, соответственно, и один базис и все еще хотим, чтобы матрица была наиболее простой.

Определение 1.3. Говорят, что задана алгебра над полем K, если задано множество A, бинарные операции $+$, $\times$ на нем и отбражение $K \cdot A \to A$, т.ч.:

1. $(A, +, \times)$ - кольцо
2. $(A, +, \cdot)$ - линейное пространство над полем K
3. $\forall \alpha \in K\ \forall a, b \in A : \alpha \cdot (a \times b) = (\alpha \cdot a) \times b = a \times (\alpha \cdot b)$

Пример 1.1. $A = M_n(K)$, $A_0 = \{\alpha E_n | \alpha \in K\}$ - подкольцо скалярных матриц, изоморфное полю K.

Пример 1.2. $A = K[x]$

Пример 1.3. Любая ситуация, где поле $K \subset R$ (R - кольцо) $\implies R$ - K-алгебра. В обратную сторону тоже верно, если алгебра содержит единицу. Тогда там найдется подкольцо, которое можно отожествить с полем K.

Почему алгебра с единицей:

Пусть A - алгебра с $1 (\neq 0)$ над полем K. Рассмотрим множество $A_0 = \{\alpha \cdot 1 | \alpha \in K\}$.

$$K \xrightarrow{\varphi} A_0 \quad \alpha \mapsto \alpha_1$$

Идеал в поле либо нулевой, либо все поле. $\varphi(1) \neq 0 \Rightarrow Ker(\varphi) \neq K$. Значит, φ - изоморфизм. A_0 - подкольцо, изоморфное полю K.

Линейные операторы тоже образуют алгебру. Заметим, что в End V есть сложение и композиция операторов, а также умножение на скаляр. (End V,+) - абелева группа. Проверка дистрибутивности операторов:

$$\mathcal{A} \circ (\mathcal{B}_1 + \mathcal{B}_2) = \mathcal{A} \circ \mathcal{B}_1 + \mathcal{A} \circ \mathcal{B}_2$$
$$(\mathcal{A}_1 + \mathcal{A}_2) \circ \mathcal{B} = \mathcal{A}_1 \circ \mathcal{B} + \mathcal{A}_2 \circ \mathcal{B}$$

(End $V, +, \circ$) - линейное пространство над полем K. Наконец, $(\alpha \cdot \mathcal{A}) \circ \mathcal{B} = \mathcal{A} \circ (\alpha \cdot \mathcal{B}) = \alpha \cdot (\mathcal{A} \circ \mathcal{B})$.

Таким образом, (End $V, +, \circ, \cdot$) - алгебра над полем K.

Предложение 1.1. Пусть $\dim V = n$. E - базис V. Тогда отображение End $V \xrightarrow{\lambda_E} M_n(K), \mathcal{A} \mapsto [\mathcal{A}]_E$ - изоморфизм алгебр над полем K (т.е. биекция сохраняет все операции)

Доказательство. Знаем: λ_E - изоморфизм линейных пространств.
$\lambda_E(\mathcal{B} \circ \mathcal{A}) = [\mathcal{B}\mathcal{A}]_E = [\mathcal{B}]_E \cdot [\mathcal{A}]_E = \lambda_E(\mathcal{B})\lambda_E(\mathcal{A})$ ■

Следствие 1.1.1. $\dim \operatorname{End}\ V = (\dim\ V)^2$

lil friendly reminder: $U_E \xrightarrow{\mathcal{A}} V_F \xrightarrow{\mathcal{B}} W_G \quad [\mathcal{B}\mathcal{A}]_{EG} = [\mathcal{B}]_{FG}[\mathcal{A}]_{EF}$

$$U_{EE'} \xrightarrow{\mathcal{A}} V_{FF'}$$
$$[\mathcal{A}]_{EF} = A \quad [\mathcal{A}]_{EF} = ?$$
$$M_{E\to E'} = C \ \ M_{F\to F'} = D$$
$$E' = EC \quad E = (e_1, \dots, e_n) \quad C = c_{ij}$$
$$EC = (c_{11}e_1 + \dots + c_{m1}e_n, c_{12}e_1 + \dots + c_{n2}e_n, \dots)$$

Предложение 1.2. Пусть $\mathcal{A} \in \operatorname{End} V, E$ и E' - базисы, $[\mathcal{A}]_E = A$; $M_{E\to E'} = C$, тогда $[\mathcal{A}]_{E'} = C^{-1}AC$

Доказательство.

$$U_E \xrightarrow{\mathcal{A}} V_F \xrightarrow{\varepsilon_V = \mathrm{id}_V} V'_F \xleftarrow{\mathcal{A}} U'_E \xrightarrow{\varepsilon_U} U_E$$
$$[\mathcal{A}]_{E'F'} = \underbrace{[\varepsilon_V]_{FF'}}_{D^{-1}} \underbrace{[\mathcal{A}]_{EF}}_{A} \underbrace{[\varepsilon_U]_{E'E}}_{C}$$

В нашем случае $(U = V, E = F, E' = F')$ ■

Определение 1.4. Пусть A' эквивалентно A, если $\exists C \in \mathrm{GL}_n(K)$: $A' = C^{-1}AC$. Проверка симметричности и транзитивности:

$$A = (C^{-1})^{-1}A'C^{-1}$$
$$A'' = D^{-1}A'D = D^{-1}C^{-1}A'CD = (DC)^{-1}A'(CD)$$

Глава 2

Инвариантные подпространства

Определение 2.1. V - линейное конечномерное пространство, $A \in \text{End } V$. Пусть $W \subset V$ - линейное подпространство. W - называется инвариантным относительно A, если $\forall w \in W : \mathcal{A}(w) \in W$

Свойства.

1. $0, W$ - A-инвариантны
2. $\text{Ker } \mathcal{A}$ - A-инвариантно
3. $\text{Im } \mathcal{A}$ - A-инвариантен

Пусть W - A-инвариант. Следовательно, $A|_W$ можно рассматривать как элемент $\text{End } W$. Более формально, $\exists\ \mathcal{A}_1 \in \text{End } W\ \forall w \in W : \mathcal{A}_1 w = \mathcal{A} w$

$$W \xrightarrow{\mathcal{A}} W \quad w \mapsto \mathcal{A}w$$

$\mathcal{A}_1$ - оператор индуцированный оператором $\mathcal{A}$ на инвариантном подпространстве W.

$W \subset V, V/W = \{v + w | v \in V\}$ - фактор-пространство. W - A-инвариант. Определим $\mathcal{A}_2$.

$$\mathcal{A}_2 : V/W \to V/W \quad v + W \mapsto \mathcal{A}v + W$$

Проверка корректности: пусть $v_1 + W = v_2 + W$, нужно проверить, что $\mathcal{A}v_1 + W = \mathcal{A}v_2 + W$. Так, $\mathcal{A}v_2 = \mathcal{A}(v_1 + (v_2 - v_1)) = \mathcal{A}v_1 + \mathcal{A}\underbrace{(v_2 - v_1)}_{\in W} \Rightarrow \mathcal{A}v_2 + W = \mathcal{A}v_1 + W$

Предложение 2.1. $\mathcal{A}_2 \in \mathrm{End}\ V/W$

Доказательство. Проверка линейности:
$\mathcal{A}_2((v_1+W)+(v_2+W)) = \mathcal{A}_2((v_1+v_2)+W) = \mathcal{A}(v_1+v_2)+W = \mathcal{A}v_1 + \mathcal{A}v_2 + W = (\mathcal{A}v_1 + W) + (\mathcal{A}v_2 + W)$
$\mathcal{A}_2(\alpha(v+w)) = \mathcal{A}_2(\alpha v + W) = \mathcal{A}(\alpha v) + W = \alpha\mathcal{A}v + W = \alpha(\mathcal{A}v + W) = \alpha\mathcal{A}_2(v+W)$ ■

$\mathcal{A}_2$ - тоже индуцированный оператор

Предложение 2.2. Пусть $\mathcal{A} \in \mathrm{End}\ V, W \subset V, e_1, \dots, e_m$ - базис W, $e_{m+1}, \dots, e_n$ - дополнение до базиса V. Тогда эквивалентны 2 утверждения:

1. W - A-инвариант
2. $[\mathcal{A}]_{e_1,\dots,e_n} = \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right)$, $A_1 \in M_m(K)$

При этом $A_1 = [\mathcal{A}_1]_{e_1,\dots,e_m}$, $A_2 = [\mathcal{A}_2]_{e_{m+1}+W,\dots,e_n+W}$, где $\mathcal{A}_1$ и $\mathcal{A}_2$ соответствуют индуцированные операторы

Доказательство. $1 \Rightarrow 2$: векторы $e_1, \dots, e_n \in W \Rightarrow \mathcal{A}e_1, \dots, \mathcal{A}e_m \in W = \mathrm{Lin}(e_1, \dots, e_m) \Rightarrow [\mathcal{A}]_{e_1,\dots,e_n} = \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right)$
Очевидно, $[\mathcal{A}_1]_{e_1,\dots e_m} = A_1$.
Пусть $[\mathcal{A}]_{e_1,\dots,e_n} = (a_{ij})$.
$\mathcal{A}e_j = \underbrace{a_{1j}e_1 + \dots + a_{mj}e_m}_{\in W} + a_{m+1j}e_{m+1} + \dots + a_{nj}e_n$, $j \geqslant m+1$
$\underbrace{\mathcal{A}e_j + W}_{=\mathcal{A}_2(e_j+W)} = \underbrace{a_{m+1j}e_{m+1} + \dots + a_{nj}e_n + W}_{=a_{m+1j}(e_{m+1}+W)+\dots+a_{nj}(e_n+W)}$ (первые m элементов станут нулевым классом) Таким образом, $[\mathcal{A}_2]_{e_{m+1}+W,\dots,e_n+W} = \begin{pmatrix} a_{m+1m+1} & \dots & a_{m+1n} \\ \vdots & \ddots & \vdots \\ a_{nm+1} & \dots & a_{nn} \end{pmatrix} = A_2$

$2 \Rightarrow 1$: $[\mathcal{A}_1]_{e_1,\dots,e_n} = \left(\begin{array}{c|c} A_1 & B \\ \hline 0 & A_2 \end{array}\right) \Rightarrow \mathcal{A}e_1,\dots,\mathcal{A}e_m \in \operatorname{Lin}(e_1,\dots,e_m) \in W$

Пусть $w \in W \Rightarrow w = \beta_1 e_1 + \dots + \beta_m e_m \Rightarrow \mathcal{A}w = \beta_1 \underbrace{\mathcal{A}_1 e_1}_{\in W} + \dots + \beta_m \underbrace{\mathcal{A}_m e_m}_{\in W} \in W$ ■