

§1. Определение алгебр

Прerequisites: теория колец и модулей

кольца ассоц. с единицей.

линейная алгебра векторные пр-ва (комплексные разн) над полем.

кольца не обязательно комм. Центр кольца A : $Z(A) = \{a \in A : ab = ba \forall b \in A\}$
Гом-мы колец $1 \mapsto 1$

Def: F поле. F -алгебра A это кольцо A вместе с гом-мом колец $s: F \rightarrow Z(A)$.

Пусть A это F -алгебра, $I = \text{Ker}(s)$ идеал в F .

1) $I = F$, т.е. s нулевой. Тогда $0 = 1$ в A и значит $A = 0$: $0 = 0a = 1a = a$

2) $I = 0$, т.е. можно считать, что $F \subset Z(A) \subset A$ подкольцо.

Наоборот, если $F \subset Z(A)$ для кольца A , то A является (ненулевой) F -алгеброй.

Пусть A есть F -алгебра. Тогда A векторное пр-во над F ,

$\dim(A)$ определено.

Гомоморфизмы F -алгебр - это гом-мы колец и вект. пр-в.
Так как $1 \mapsto 1$, то гом-мы тождественны на F . Изоморфизмы = ...

Примеры. 1) Любое комм. кольцо A , содержащее F , является F -алгеброй.

В частности, F явл. F -алгеброй размерности 1.

2) Если A и B две F -алгебры, то $A \times B$ тоже F -алгебра

3) Алгебра матриц $M_n(F)$ является F -алгеброй размерности n^2

$F \hookrightarrow M_n(F) : x \mapsto \text{diag}(x, x, \dots, x)$. Матричные единицы e_{ij}

образуют базис. $e_{ij} \cdot e_{kl} = \begin{cases} e_{il}, & \text{если } j=k \\ 0, & j \neq k \end{cases}, \quad \sum_i e_{ii} = 1$

Более общо: если A это F -алгебра, то $M_n(A)$ тоже F -алгебра

4) Если A это F -алгебра, M - правый A -модуль, то $\text{End}_A(M)$ является F -алгеброй. Например, если $A=F$ поле, а M - вект. пр-во размерности n , то $\text{End}_A(M) \cong M_n(F)$.

Если $M = M_1 \oplus \dots \oplus M_k$, то $\text{End}_A(M) = \{(f_{ij}), f_{ij}: M_j \rightarrow M_i\}$ с матричным умножением

Если $M = N^k$, то $\text{End}_A(M) \cong M_k(\text{End}_A(N))$

5) A^{op} противоположная алгебра: $a^{\text{op}} \cdot b^{\text{op}} = (ba)^{\text{op}}$

§2. Теорема Веддерберна

F -алгебра A называется алгеброй с делением, если все ненулевые элементы обратимы. $A \neq 0$ простой алгеброй, если A не имеет нетривиальных (двусторонних) идеалов.

Примеры. 1. Алгебра с делением проста.

2. Если A простая алгебра, то алгебра $M_n(A)$ также проста. $\neq$

$0 \neq I \subset M_n(A)$ идеал, $0 \neq \sum a_{ij} e_{ij}$, $a_{st} \neq 0$, $a_{ij} \in A \Rightarrow \forall k$,

$$I \ni e_{ks} \cdot \left(\sum a_{ij} e_{ij} \right) e_{tk} = \sum_{s=i, j=t} a_{ij} e_{ks} e_{ij} e_{tk} = a_{st} \cdot e_{kk} \Rightarrow a_{st} = \sum_k a_{st} \cdot e_{kk} \in I.$$

(мы считаем, что $A \hookrightarrow M_n(A)$). Так как A проста, то

$$1 \in A a_{st} A \subset A I A \subset I \Rightarrow I = M_n(A). \square$$

3. $M_n(D)$, где D алгебра с делением, проста.

③

A это F -алгебра.
Заметим, что каждый (правый) A -модуль является вект. пр-вом над F .
Правый A -модуль M называется простым (неприводимым), если $M \neq 0$ и M не имеет нетривиальных подмодулей.

Лемма Шура. Пусть $f: M \rightarrow M'$ гом. простых A -модулей.
Тогда либо $f=0$, либо f изоморфизм.

Док-во. Если $f \neq 0$, то $\text{Ker}(f) \neq M$ and $\text{Im}(f) \neq 0$. Так как M и M' простые, то $\text{Ker}(f)=0$ и $\text{Im}(f)=M'$, т.е. f изоморфизм. $\square$

Следствие. Если M простой A -модуль, то $\text{End}_A(M)$ является
алгеброй с делением. $\square$

Лемма. Пусть N конечномерный A -модуль, являющийся суммой
некоторого числа простых подмодулей. Тогда N является суммой
конечного числа этих подмодулей.

Док-во. Выберем наибольшее число простых подмодулей $N_1, N_2, \dots, N_k$,
таких что сумма $N_1 + N_2 + \dots + N_k$ прямая. Утверждается, что
 $N = N_1 \oplus N_2 \oplus \dots \oplus N_k$. Если $N \neq N_1 \oplus \dots \oplus N_k$, то найдем простой
подмодуль $N' \subset N$, такой что $N' \not\subset N_1 \oplus \dots \oplus N_k$. Так как N' простой,
то $N' \cap (N_1 \oplus \dots \oplus N_k) = 0$, а значит сумма $N' + N_1 \oplus \dots \oplus N_k$ прямая,
противоречие. $\square$

Теорема (Веддерберн). Пусть A — конечномерная простая алгебра.
Тогда $A \cong M_n(D)$, где D — алгебра с делением.

Док-во. Пусть $I \subset A$ — ненулевой правый идеал наименьшей размерности. Значит I — простой правый A -модуль. Заметим, что $aI = 0$ или $aI \cong I \quad \forall a \in A$ (по лемме Шура для $I \xrightarrow{e_a} I$)

Пусть J — сумма всех правых идеалов $(\text{изоморфных } I)$. Тогда $aJ \subset J \quad \forall a \in A$, т.е. J — идеал в A . Так как A — простая алгебра, то $J = A$.

По лемме $A = I_1 \oplus I_2 \oplus \dots \oplus I_n$, где $I_k \cong I \quad \forall k$. Имеем:

$$A = \text{End}_A(A) = \text{End}_A(I_1 \oplus \dots \oplus I_n) \cong \text{End}_A(I^n) = M_n(D), \text{ где}$$

$D = \text{End}_A(I)$ — алгебра с делением по лемме Шура. $\square$

Предложение. Пусть A — конечномерная простая алгебра,
 $I \subset A$ — минимальный правый идеал. Тогда любой простой правый
 A -модуль изоморфен I .

Док-во. Пусть M — простой правый A -модуль. Так как $0 \neq M \cong \text{Hom}_A(A, M)$ и $A \cong I^n$, то имеется ненулевой $I \rightarrow M$, который является изоморфизмом по лемме Шура. $\square$

Пример. Пусть $A = M_n(D)$, где D -алгебра с делением. Тогда правый A -модуль D^n строк длины n над D является простым и $\text{End}_A(D^n) \cong D$. Отсюда следует, что $M_n(D) \cong M_n(D')$, где D и D' алгебры с делением $\Leftrightarrow D \cong D'$ и $n = n'$.

Предложение Пусть M простой правый A -модуль над конечной простой алгеброй A . Тогда любой конечномерный A -модуль изоморфен M^n для некоторого n . Два таких A -модуля N и N' изоморфны $\Leftrightarrow \dim(N) = \dim(N')$.

Док-во. Любой конечномерный A -модуль N конечно порожден и значит является фактор-модулем A^m для нек-го m . Так как A сумма простых модулей, то N также является суммой простых модулей $\Rightarrow$ прямой суммой простых по лемме, значит $N = M^n$.

Заметим, что $n = \frac{\dim N}{\dim M}$. $\square$

§3. Тензорное произведение

6

Пусть U и V конечн. векторные пр-ва над полем F .

Отображение $B: U \times V \rightarrow W$ в пр-ве кон. векторное пр-во W называется билинейным, если

$$1) B(x, u_1 + x_2 u_2, v) = x_1 B(u_1, v) + x_2 B(u_2, v),$$

$$2) B(u, y_1 v_1 + y_2 v_2) = y_1 B(u, v_1) + y_2 B(u, v_2).$$

Если $f: W \rightarrow W'$ линейное отображение, то композиция $f \circ B: U \times V \rightarrow W'$ - билинейное отображение.

Билинейное отображение $B_{U \times V}: U \times V \rightarrow W_{U \times V}$ называется универсальным, если для любого билинейного отображения $B: U \times V \rightarrow W$ найдется единственное линейное отображение $f: W_{U \times V} \rightarrow W$, такое что $B = f \circ B_{U \times V}$.

Предложение. Пусть $B_{U \times V}: U \times V \rightarrow W_{U \times V}$ и $B'_{U \times V}: U \times V \rightarrow W'_{U \times V}$ два универсальных билинейных отображения. Тогда существует единственный линейный изоморфизм $f: W_{U \times V} \rightarrow W'_{U \times V}$, такой что $B'_{U \times V} = f \circ B_{U \times V}$.

Док-во. По определению, существуют единственные линейные отображения $f: W_{U \times V} \rightarrow W'_{U \times V}$ и $g: W'_{U \times V} \rightarrow W_{U \times V}$, такие что $B' = f \circ B$ и $B = g \circ B'$. Тогда $B = (g \circ f) \circ B = \text{Id}_{W_{U \times V}} \circ B$. По единственности $g \circ f = \text{Id}$. Аналогично, $f \circ g = \text{Id}$, т.е. f - изоморфизм. ■

Теорема. Для любых век. пространств U и V существует универсальное линейное отображение $B_{univ} : U \times V \rightarrow W_{univ}$.

Доказ. Пусть $\{u_1, \dots, u_n\}$ и $\{v_1, \dots, v_m\}$ базисы U и V . Рассмотрим векторное пр-во W_{univ} размерности nm с базисом $\{\omega_{ij}\}$, $i=1, \dots, n, j=1, \dots, m$, и линейное отображение $B : U \times V \rightarrow W_{univ}$,

$$B(\sum x_i u_i, \sum y_j v_j) = \sum_{i,j} x_i y_j \omega_{ij} \text{ в частности, } B(u_i, v_j) = \omega_{ij}.$$

Покажем, что B_{univ} универсально. Пусть $B : U \times V \rightarrow W$ линейное отображение. Нужно доказать, что существует единственное линейное отображение $f : W_{univ} \rightarrow W$ такое что $B = f \circ B_{univ}$.

Если так, то $B(u_i, v_j) = f(B_{univ}(u_i, v_j)) = f(\omega_{ij})$, так что f единственно. Зададим f условием $f(\omega_{ij}) = B(u_i, v_j)$. Тогда

$$\begin{aligned} B(\sum x_i u_i, \sum y_j v_j) &= \sum_{i,j} x_i y_j B(u_i, v_j) = \sum_{i,j} x_i y_j f(\omega_{ij}) = f(\sum x_i y_j \omega_{ij}) = \\ &= f(B_{univ}(\sum x_i u_i, \sum y_j v_j)), \text{ т.е., } B = f \circ B_{univ}. \blacksquare \end{aligned}$$

Обозначаем: $W_{univ} = U \otimes_F V$, называем тензорным произведением

$$B_{univ} : U \times V \rightarrow U \otimes_F V, \text{ имеем } u \otimes v = B_{univ}(u, v) \in U \otimes V$$

$$1) (x_1 u_1 + x_2 u_2) \otimes v = x_1 (u_1 \otimes v) + x_2 (u_2 \otimes v), \quad 0 \otimes v = 0$$

$$2) u \otimes (y_1 v_1 + y_2 v_2) = y_1 (u \otimes v_1) + y_2 (u \otimes v_2), \quad u \otimes 0 = 0$$

3) Если $\{u_1, \dots, u_n\}$ базис U , $\{v_1, \dots, v_m\}$ базис V , то

$$\{u_i \otimes v_j\} \text{ базис } U \otimes V. \text{ Поэтому } \dim(U \otimes V) = \dim U \cdot \dim V.$$

Любой элемент $b \in U \otimes V$ имеет вид $\sum x_{ij} (u_i \otimes v_j)$ в частности, $U \otimes V$ порождается векторами $u \otimes v$

4) Если $u_1, u_2, \dots, u_n$ линейно независимы в U и $t_1, t_2, \dots, t_n \in V$ такие что $\sum u_i \otimes t_i = 0$ в $U \otimes V$, то все $t_i = 0$

Пусть $\{v_1, \dots, v_m\}$ базис в V . Запишем $t_i = \sum_j x_{ij} v_j \Rightarrow$

$$0 = \sum_i (u_i \otimes \sum_j x_{ij} v_j) = \sum_{i,j} x_{ij} (u_i \otimes v_j) \Rightarrow x_{ij} = 0 \text{ так как}$$

$u_i \otimes v_j$ линейно независимы $\Rightarrow t_i = 0 \forall i. \square$

5) (Свойство Универсальности) Пусть $B: U \times V \rightarrow W$ ^{двухаргументное} билинейное отображение. Тогда существует единственное линейное отображение $f: U \otimes V \rightarrow W$, такое что $f(u \otimes v) = B(u, v) \forall u, v$.

6) Имеем изоморфизм $U \otimes V \xrightarrow{\sim} V \otimes U, u \otimes v \mapsto v \otimes u$.

7) Имеем изоморфизм $(U \otimes V) \otimes W \xrightarrow{\sim} U \otimes (V \otimes W), (u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$

8) Имеем изоморфизм $F \otimes_F V \xrightarrow{\sim} V, x \otimes v \mapsto xv$.

9) Если $f: U \rightarrow U', g: V \rightarrow V'$ линейные отображения, то

имеем линейное отображение $f \otimes g: U \otimes V \rightarrow U' \otimes V'$,

$(f \otimes g)(u \otimes v) = f(u) \otimes g(v)$. Если f и g инъективны, то $f \otimes g$

также инъективно. Если $U \subset U', V \subset V'$ подпространства,

то $U \otimes V \subset U' \otimes V'$ под-во.

①

$$A \ni a \quad a^3 = x \in F$$

X min-max map $\log$ A ,

$$\begin{array}{ccc} Y(F) & \longrightarrow & F^* \\ \downarrow \text{Gutman?} & & \downarrow \\ X(F) & \longrightarrow & F^x / F^{x^2} \end{array}$$

$$(L, x) : \text{disc}(L) = x \cdot F^{x^2}$$

$$Y \xrightarrow{f} G_m$$

$$1 \longrightarrow 2$$

$$\overline{F[x]} \longrightarrow \overline{F[y]} \longrightarrow \mathbb{Z} \longrightarrow \text{Pic } X$$

$$\downarrow$$

$$X$$

$$\overline{f} \mapsto \overline{2}$$

$$p^{\otimes 2} \simeq A$$

$$\bigoplus_{i \in \mathbb{Z}} p^{\otimes i}$$

$$A[b, t^{\pm 1}]$$

$$\begin{array}{c} \text{G}_m \\ \downarrow \\ X \end{array}$$

$$p^{\otimes 2} \simeq A$$

$$A/2 \hookrightarrow H^1(A, \mu_2) \xrightarrow{\sim} \text{Pic } A$$

$$H^1(A, S_n)$$

$$E S_n \longrightarrow B S_n$$

$$\{ \in H^1(B S_n, S_n) \longrightarrow H^1(B S_n, \mu_2) \}$$

$$\downarrow$$

$$\text{Pic } B G = G^*$$

$$Y$$

$$\text{Pic } B S_n$$

$$X \longrightarrow B S_n \longrightarrow B \mathbb{Z}/2$$

$$\mathbb{Z}/2 \downarrow$$

$$X$$

$$xi+yj+zk \quad ax^2+by^2-abz^2 \neq 0$$

$$\mathbb{P}^2 \supset \mathbb{P}^2 - Q_{\text{red.}}$$

Если A это F -алгебра, то отображение умножения $A \times A \rightarrow A$ задает линейное отображение $A \otimes_F A \rightarrow A$, $a \otimes a' \mapsto aa'$. Обратно, линейное отобр. $A \otimes_F A \rightarrow A$ на векторном пространстве A над F задает дистрибутивное умножение на A .

Пусть A и B две F -алгебры. Имеем линейное отображение $(A \otimes B) \otimes (A \otimes B) \rightarrow A \otimes B$, $(a \otimes b) \otimes (a' \otimes b') \mapsto aa' \otimes bb'$ задает на $A \otimes B$ структуру F -алгебры: $(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'$.

1) $A \otimes B \simeq B \otimes A$

2) $(A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$

3) $F \otimes A \simeq A$.

4) Отображение $M_n(F) \otimes A \rightarrow M_n(A)$, $\sum x_{ij} e_{ij} \otimes a \mapsto \sum x_{ij} a e_{ij}$ является изоморфизмом.

5) Если $A = M_m(F)$, получаем изоморфизм $M_n(F) \otimes M_m(F) \simeq M_{nm}(F)$.

6) $M_n(A) \otimes M_m(B) \simeq M_{nm}(A \otimes B)$

7) $A = A \otimes F \hookrightarrow A \otimes B$ via $a \mapsto a \otimes 1$. Similarly $B \hookrightarrow A \otimes B$ and $ab = ba$ in $A \otimes B$.

8) Положительный факт: пусть $f: A \rightarrow B$ гомоморфизм F -алгебр над F простым и $\dim_F A = \dim_F B$. Тогда f -изоморфизм $\nLeftrightarrow \ker(f)$ ideal в A . $\square$

§4. Центризаторы

Пусть A - F -алгебра, $S \subseteq A$ подалгебра. Множество

$$C_A(S) = \{a \in A : as = sa \ \forall s \in S\}$$

называется центризатором S в A . Ясно, что $C_A(S)$ - подалгебра в A .

Примеры. $C_A(F) = A$, $C_A(A) = Z(A)$ центр A .

Лемма. Пусть A и B две F -алгебры и $S \subseteq A$, $T \subseteq B$ подалгебры

Тогда $C_{A \otimes B}(S \otimes T) = C_A(S) \otimes C_B(T) \subseteq A \otimes B$.

Док-во. $\supset$ очевидно. Пусть $x = \sum a_i \otimes b_i \in C_{A \otimes B}(S \otimes T)$, причем можно считать, что $\{b_i\}$ базис в B . Для любого $s \in S$, имеем $0 = (s \otimes 1) \cdot x - x(s \otimes 1) = \sum (sa_i - a_i s) \otimes b_i$. Так как $\{b_i\}$ - базис, то $sa_i - a_i s = 0$, т.е., $a_i \in C_A(S)$, значит $x \in C_A(S) \otimes B$.

Переменив x , мы можем считать, что $\{a_i\}$ образуют базис в $C_A(S)$. Аналогично, $\forall t \in T$ имеем $0 = (1 \otimes t)x - x(1 \otimes t)$, и как раньше получаем $b_i \in C_B(T)$. $\square$

Следствие. $Z(A \otimes B) = Z(A) \otimes Z(B)$.

(11)

F -алгебра A называется центральной, если $Z(A) = F$.

Пример. F -алгебра $M_n(F)$ центральна. $\Rightarrow Z(M_n(A)) \cong Z(A)$

Следствие. Если F -алгебры A и B центральны, то

$A \otimes_F B$ тоже центральна. $\square$

Тензорное произведение двух простых алгебр не обязательно просто
($\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$).

Предположение. Пусть A и B простые F -алгебры и алгебра A центральна. Тогда алгебра $A \otimes_F B$ проста.

Док-во. Пусть $I \subset A \otimes B$ ненулевой идеал. Выберем

$0 \neq x = \sum_{i=1}^n a_i \otimes b_i \in I$ с минимальным n . Ясно, что все $a_i \neq 0$

и $\{b_i\}$ линейно независимы. Так как A проста, то $Aa_i A = A$,

значит $1 = \sum_{j=1}^m a'_j a_i a''_j$ for some $a'_j, a''_j \in A$. Тогда

$$I \ni \sum_{j=1}^m (a'_j \otimes 1) x (a''_j \otimes 1) = \sum_{i=1}^n \left(\sum_{j=1}^m a'_j a_i a''_j \right) \otimes b_i,$$

так что мы можем считать, что $a_1 = 1$,

$$x = 1 \otimes b_1 + a_2 \otimes b_2 + \dots + a_n \otimes b_n.$$

Для каждой $a \in A$ имеем

$$I \ni (a \otimes 1)x - x(a \otimes 1) = \sum_{i=2}^n (aa_i - a_i a) \otimes b_i$$

Так как n минимально, этот элемент равен нулю, значит

$$aa_i - a_i a = 0 \quad \forall a \in A, \text{ i.e., } a_i \in Z(A) = F.$$

Сл-но, $x = 1 \otimes b$ для $b \in B$. Так как B проста, $B \otimes B = B$,

$\sum_k b'_k \cdot b \cdot b''_k = 1$ для нек-рых $b'_k, b''_k \in B$. Наконец,

$$I \Rightarrow \sum_k (1 \otimes b'_k) x (1 \otimes b''_k) = 1 \otimes 1, \text{ т.е., } I = A \otimes B. \square$$

Следствие. Если A и B у.п.а., то $A \otimes B$ также у.п.а.

§5. Группа Брауэра

Этот класс замкнут относительно $\otimes$ и M_n

Пусть F -поле. Введем отношение эквивалентности на конечномерных у.п. F -алгебрах: мы пишем $A \sim B$, если $M_n(A) \cong M_m(B)$ для некоторых n и m .

1) $A \sim A$

2) $A \sim B \Rightarrow B \sim A$

3) $A \sim B, B \sim C \Rightarrow A \sim C \nparallel M_n(A) \cong M_m(B), M_r(B) \cong M_s(C) \Rightarrow$

$M_{rn}(A) \cong M_{rm}(B) \cong M_{ms}(C). \square$

Обозначим $Br(F)$ множество классов эквивалентности у.п. F -алгебр конечной размерности. Для у.п. F -алгебры A обозначаем $[A]$ ее класс в $Br(F)$.

Предложение. Пусть A и B — у.п. F -алгебры. Затем

$A \cong M_n(D)$, $B \cong M_s(T)$, где D и T — алгебры с делением. Тогда

$$[A] = [B] \iff D \cong T.$$

Док-во. Пусть $A \sim B$, т.е. $M_n(A) \cong M_m(B)$. Тогда

$$M_{nr}(D) \cong M_{ms}(T). \text{ Мы знаем, что } D \cong T. \square$$

Следствие. Каждый класс в $Br(F)$ имеет вид $\{M_n(D)\}_{n \geq 1}$ для единственной (с точностью до изоморфизма) у.п. алгебры с делением D . $\square$

Таким образом имеем биекцию

$$Br(F) \longleftrightarrow \text{Мн-во классов изоморфизмов у.п. F -алгебр с делением}$$

Следствие. Если A и B — у.п. F -алгебры, то $A \cong B \iff [A] = [B]$

$$\text{в } Br(F) \text{ и } \dim(A) = \dim(B).$$

$$\text{Введем операцию в } Br(F): [A] \cdot [B] = [A \otimes_F B]$$

Операция корректно определена: если $A \sim A'$, $M_n(A) \cong M_m(A')$

$$B \sim B', \quad M_r(B) \cong M_s(B'),$$

$$\text{то } M_{nr}(A \otimes_F B) \cong M_{ms}(A' \otimes_F B'), \text{ т.е. } A \otimes B \sim A' \otimes B'.$$

Теорема. Множество $\text{Br}(F)$ с определенной операцией - абелева группа.

Док-во. Ассоц. и комм очевидны. Класс $[F] = \{M_n(F)\}_{n \geq 1}$ является единицей. Пусть A у.н. F -алгебра. Рассмотрим алгебру $\text{End}_F(A)$, где A рассматривается как векторное пространство.

Мы имеем вложения: $A \hookrightarrow \text{End}_F(A)$, $a \mapsto \ell_a$ ($b \mapsto ab$)

$$A^{\text{op}} \hookrightarrow \text{End}_F(A), a \mapsto r_a (b \mapsto ba)$$

A и A^{op} коммутируют поэлементно, поэтому отображение

$$A \otimes A^{\text{op}} \longrightarrow \text{End}_F(A)$$

является гомоморфизмом алгебр. Так как $A \otimes A^{\text{op}}$ проста и

$\dim(A \otimes A^{\text{op}}) = n^2 = \dim \text{End}_F(A)$, где $n = \dim A$, то это

изоморфизм. Получаем: $A \otimes A^{\text{op}} \cong M_n(F)$, т.е. $[A^{\text{op}}] = [A]^{-1}$. $\square$

Замечание. $\text{Br}(F) = 1 \iff F$ единичная у.н. алгебра с делением над $F \iff$ каждая у.н. алгебра с делением над F коммутативна.

Примеры. 1. Если F алгебраически замкнуто, то $\text{Br}(F) = 1$.

Пусть D у.н. алгебра с делением над F . Покажем, что $D = F$.

Пусть $d \in D$. Так как степени d^i линейно зависимы над F , существует непостоянный многочлен $f \in F[t]$ такой что $f(d) = 0$.

Так как F алгебраически замкнуто, $f(t) = x \cdot \prod (t - y_i)$

для некоторых $y_i \in F$. Так как $0 = f(d) = x \cdot \prod (d - y_i)$, то

$d = y_i \in F$ для некоего i .

2. Класс $[H]$ неединичный элемент в $\text{Br}(\mathbb{R})$, поэтому

$\text{Br}(\mathbb{R}) \neq 1$. На самом деле, $\text{Br}(\mathbb{R}) = \{1, [H]\}$ циклическая

группа порядка 2.

Замечание. Пусть A простая конечномерная F -алгебра. Заметим

$A \cong M_n(D)$, где D F -алгебра с делением. Имеем:

$Z(A) = Z(D)$ является полем, поэтому A у.н. алгебра над $Z(D)$.

§6. Две теоремы о простых алгебрах

Теорема (Нётер-Сколем) Пусть A — у.н. F -алгебра, $S, T \subseteq A$ — простые подалгебры. Пусть $f: S \rightarrow T$ — изоморфизм F -алгебр. Тогда существует $a \in A^*$, такой что $f(s) = asa^{-1} \quad \forall s \in S$.

Док-во. Рассмотрим A как правый $A^{\text{op}} \otimes S$ -модуль двумя способами:
 $x \cdot (a^{\text{op}} \otimes s) = axs, \quad x \cdot (a^{\text{op}} \otimes s) = axf(s).$

Алгебра $A^{\text{op}} \otimes S$ проста, поэтому любые два правых $A^{\text{op}} \otimes S$ одинаковой размерности изоморфны. Поэтому имеется линейный изоморфизм

$$g: A \xrightarrow{\sim} A$$

Такой что $g(axs) = a g(x) f(s) \quad \forall a, x \in A, s \in S$.

Положим $x=1=s$: $g(a) = a \cdot g(1)$. В частности, $g(1)$ обратим слева, и значит обратим. (УПР)

Положим $a=1=x$: $g(s) = g(1)f(s)$. Отсюда $f(s) = g(1)^{-1}g(s) = g(1)^{-1} \cdot s \cdot g(1)$.

Следствие. Каждый автоморфизм у.н. алгебры является внутренним.

$\text{Aut}_{F\text{-alg}}(A) = A^*/F^*$. В частности, $\text{Aut}(M_n(F)) = GL_n(F)/F^* = PGL_n(F)$.

Теорема (О глобальном централизаторе) Пусть A - у.н. F -алгебра,

$S \subset A$ простая подалгебра. Тогда

1) Алгебра $C_A(S)$ проста и $Z(C_A(S)) = Z(S)$.

2) $\dim(S) \cdot \dim C_A(S) = \dim(A)$.

3) $C_A(C_A(S)) = S$.

Док-во. Мы рассматриваем S как подалгебру в $B = \text{End}_F(S)$ левых умножений, так что $C_B(S) = S^{\text{op}}$ подалгебра правых умножений. Имеем (УНР)

$$C_{A \otimes B}(S \otimes F) = C_A(S) \otimes B,$$

$$C_{A \otimes B}(F \otimes S) = A \otimes S^{\text{op}} \text{ простая алгебра!}$$

По теореме Гейсера-Сколена, подалгебры $S \otimes F$ и $F \otimes S$ в $A \otimes B$ сопряжены. Сл-но, их централизаторы тоже сопряжены. В частности, они изоморфны: $C_A(S) \otimes B \cong A \otimes S^{\text{op}}$ проста. Значит $C_A(S)$ проста.

Имеем: $\dim C_A(S) \cdot \dim(B) = \dim A \cdot \dim(S^{\text{op}})$, откуда следует 2).

Согласно 2) $\dim(C_A(C_A(S))) = \dim(S)$, а так как $S \subset C_A(C_A(S))$, то $S = C_A(C_A(S))$.

Докажем, что $Z(C_A(S)) = S \cap C_A(S) = Z(S)$. Здесь 4 вложения

Единственное нетривиальное - это $Z(C_A(S)) \subset S \cap C_A(S)$:

$$Z(C_A(S)) \subset C_A(C_A(S)) = S. \quad \square$$

Следствие. Пусть S - ц.п. подалгебра ц.п. алгебры A . Тогда

$$A \cong S \otimes C_A(S).$$

Док-во. Мы имеем естественный гомоморфизм алгебр

$$f: S \otimes C_A(S) \rightarrow A$$

По теореме $C_A(S)$ проста, значит $S \otimes C_A(S)$ проста. По теореме размерности алгебр совпадают, поэтому f - изоморфизм. $\square$

§7. Максимальные подполя

Пусть A - F -алгебра и K/F расширение полей. Тогда

$A_K := A \otimes_F K$ является K -алгеброй. Если (a_i) базис A над F , то

$(a_i \otimes 1)$ базис A_K над K . В частности, $\dim_F(A) = \dim_K(A_K)$.

Если A - ц.п. F -алгебра, то A_K - ц.п. K -алгебра. Если $A \sim A'$,

т.е., $M_n(A) \cong M_m(A')$, то $M_n(A_K) \cong M_m(A'_K)$ над K , т.е., $A_L \sim A'_L$.

Следовательно, мы имеем корректно определенный гом-м

$$i_{K/F}: \text{Br}(F) \rightarrow \text{Br}(K), \quad [A] \mapsto [A_K].$$

Так как $A_K \otimes_K B_K = (A \otimes_F (K \otimes_K B)) \otimes_F K \cong (A \otimes_F B) \otimes_F K = (A \otimes_F B)_K$,

т.е. это отображение - гомоморфизм.

Пусть A у.п.а. над F . Расширение K поля F называется полем расщепления алгебры A , если $[A] \in \text{Ker}(i_{K/F})$, т.е.

$A_K \cong M_n(K)$ для некоторого n . Поля расщепления существуют: можно в качестве K взять алгебраическое замыкание F . Имеем

$$\dim_F(A) = \dim_K(A_K) = \dim_K(M_n(K)) = n^2$$

Число n называется степенью A : $n = \deg(A)$. Ясно, что для любого расширения полей K/F , имеем $\deg(A) = \deg(A_K)$.

Также $\deg(A \otimes B) = \deg A \cdot \deg B$ и $\deg(M_n(A)) = n \cdot \deg A$.

Пусть $A \cong M_m(D)$, где D -алгебра с делением. Число

$$\text{ind}(A) = \deg(D)$$

называется индексом алгебры A . Имеем $\deg(A) = m \cdot \text{ind}(A)$

1) Если $[A] = [B]$, то $\text{ind}(A) = \text{ind}(B)$.

2) $\text{ind}(A) = \deg(A) \iff A$ алгебра с делением

3) $\text{ind}(A) = 1 \iff [A] = 1$, т.е. $A \cong M_n(F)$ расщеплена.

Пусть D -алгебра с делением. Коммутативная подалгебра в D является полем-расширением F . Подполе $K \subset D$ содержащее F называется максимальным подполем в D , если для любого подполя $K \subset K' \subset D$ имеем $K = K'$.

Предложение. Подполе $K \subset D$ является максимальным тогда и только тогда, когда $C_D(K) = K$

Док-во. Ясно что $K \subset C_D(K)$.

$\Rightarrow$: Для любого $x \in C_D(K)$, алгебра $K[x] \subset D$ является полем.

Так как $K \subset K[x]$, то $K' = K[x]$ и $x \in K$.

$\Leftarrow$: Пусть $K \subset K' \subset D$, где K' поле. Тогда $K' \subset C_D(K) = K$, т.е. $K' = K$. $\square$

Следствие. Если $K \subset D$ максимальное подполе, то $[K:F] = \deg(D)$.

Док-во. По теореме о Д.Ц., $\dim_F(K) \cdot \dim_F(C_F(K)) = \dim D = (\deg D)^2$,

Так как $K = C_D(K)$, мы имеем $[K:F] = \dim_F(K) = \deg(D)$. $\square$

Теорема. Пусть A у.н.а. степени n и $K \subset A$ подполе степени n над F (например, A алгебра с делением и $K \subset A$ максимальное подполе). Тогда K поле расщепления алгебры A .

Док-во. Рассмотрим A как ^(правое) векторное пространство над K размерности n . Отображение

$$f: A \otimes_F K \longrightarrow \text{End}_K(A), \quad a \otimes k \longmapsto (x \longmapsto axk)$$

является гомоморфизмом K -алгебр. Алгебра $A_K = A \otimes_F K$ проста

и $\dim_K(A_K) = \dim_F(A) = n^2 = \dim_K \text{End}_K(A)$, сл-но, f -изоморфизм. $\square$

Теорема. Пусть A - у.п.а. над F и K/F конечное расширение полей. Тогда $\text{ind}(A_K) \mid \text{ind}(A) \mid [K:F] \cdot \text{ind}(A_K)$.

Док-во. Мы можем считать, что A - алгебра с делением.

Положим $n := \text{ind}(A) = \deg(A)$. По Теореме Веддерберна $A_K = M_s(B)$, где B - у.п.а. над K . Учен: $\text{ind}(A_K) = \text{ind}(B) = \deg(B)$ и $n = s \cdot m$, так что $m = \text{ind}(A_K)$ делит $n = \text{ind}(A)$.

Пусть $r = [K:F]$. Нужно доказать, что $n \mid r \cdot m$.

Вложим K в $\text{End}_F(K) = M_r(F)$ при помощи (левых) умножений, $K \subset M_r(F)$. Сл-но $A_K \subset A \otimes M_r(F) = M_r(A)$. Поэтому

$$M_s(F) \subset M_s(B) \simeq A_K \subset M_r(A).$$

По Теореме о Д.Ц., $M_r(A) \simeq M_s(F) \otimes T$ для некоторой у.п.а. T/F .

Так как A алгебра с делением, s/r . Сл-но $n = sm \mid rm$. $\square$

Следствие 2. Если K/F конечное поле расщепления у.п.а. A

над F , то $\text{ind}(A) \mid [K:F]$ и $K \hookrightarrow M_k(A)$, где $k = \frac{[K:F]}{\text{ind}(A)}$

Пусть A - у.а. с делением над F . Тогда

Поля расщепления алгебры A минимальной степени

=

Максимальная подполя в A

степень $= \deg A = \text{ind } A$.

Следствие (док-во) 1.

В изоморфна подалгебре в $M_k(A)$, где $k = \frac{r}{s} = \frac{[K:F]}{\text{ind } A}$

Док-во. T - центральный $M_s(F)$ в $M_r(A)$, ирред. $\forall T$ и $T \simeq M_{r/s}(A)$. $\square$

Следствие 3 Если K/F поле расщепления степени $\text{ind}(A)$ то $K \hookrightarrow A$. $\square$

§8. Циклические алгебры

Пусть L/F циклическое расширение полей степени n , $\sigma \in \text{Gal}(L/F)$ - образующая. Выберем $a \in F^\times$. Определяем циклическую алгебру $(L/F, \sigma, a)$ как векторное пространство над L с базисом $1, u, u^2, \dots, u^{n-1}$ с правилами умножения:

$$u^n = a = a \cdot 1$$

$$(lu^i)(l'u^j) = l \sigma^i(l') \cdot u^{i+j}, \quad l, l' \in L.$$

$$(L/F, \sigma, a) = L \cdot 1 \oplus L \cdot u \oplus \dots \oplus L \cdot u^{n-1} \quad \dim(L/F, \sigma, a) = n^2.$$

Пример. $(\mathbb{C}/\mathbb{R}, \sigma, -1) = \mathbb{H}$ над $\mathbb{R}$.

|| Предложение. $(L/F, \sigma, a)$ - ц.п.а. над F .

Док-во. Пусть $x = \sum_{i=0}^{n-1} l_i u^i \in Z(A)$, где $A = (L/F, \sigma, a)$. Для $\forall l' \in L$
 $0 = xl' - l'x = \sum l_i (\sigma^i(l') - l') u_i \Rightarrow l_i = 0$ для $i \neq 0$, т.е. $x = l_0 \cdot 1 = l_0$.
 Так как $0 = ux - xu = \sigma(l_0) - l_0$, мы имеем $x = l_0 \in F$.

Если $I \subset A$ ненулевой идеал, выберем $0 \neq x = \sum l_i u^i$ с наименьшим числом ненулевых l_i . Умножая на некоторую степень u , мы получаем, что $l_0 \neq 0$. Для $\forall l \in L$,

$$I \ni lx - xl = \sum_{i \neq 0} (l l_i - \sigma^i(l) l_i) u_i.$$

По минимальности, $(l - \sigma^i(l)) \cdot l_i = 0 \quad \forall l \in L, i \neq 0$, сл-но $l_i = 0 \quad \forall i \neq 0$.

Значит $x = l_0 \cdot 1$ обратим $\Rightarrow I \ni 1$. $\square$

Отметим, что $LC(L/F, \sigma, a)$ ^{заметим, что $C(L) = L$} ~~подполе степени n~~ . Мы знаем, что алгебра $(L/F, \sigma, a)$ расщепляется над L , т.е.

$$[L/F, \sigma, a] \in \text{Ker}(\text{Br}(F) \xrightarrow{L/F} \text{Br}(L)) =: \text{Br}(L/F)$$

Предложение. Пусть A - ц.п.а. над F степени n , содержащая циклическое расширение L/F степени n с образующей σ группы Галуа. Тогда $A \cong (L/F, \sigma, a)$ для некоторого $a \in F^\times$.

Док-во. По НС, $\sigma: L \rightarrow L$ может быть продолжен до внутреннего автоморфизма $x \mapsto uxu^{-1}$ алгебры A (здесь $u \in A^\times$). Имеем $u^n x = \sigma^n(x) u^n = xu^n$ для $\forall x \in L$, поэтому $u^n \in C_A(L)$. По теореме о ДЦ, $\dim(L) \cdot \dim C_A(L) = \dim A = n^2$, и с учетом $L \subset C_A(L)$ получаем $a := u^n \in C_A(L) = L$. Так как $\sigma(a) = u \cdot u^n u^{-1} = u^n = a$, то $a \in F^\times$. Поэтому мы имеем гомоморфизм $(L/F, \sigma, a) \rightarrow A$, который является изоморфизмом по соображениям размерности. $\square$

Следствие. $\text{Br}(L/F)$ состоит из классов $[L/F, \sigma, a]$, $a \in F^\times$

Док-во. Пусть $[A] \in \text{Br}(L/F)$, мы можем считать, что A - алгебра с делением. Имеем $A \otimes_F L \cong M_m(L)$ для нек-го m , так что $\text{ind}(A) = \deg(A) = m$. По следствию 2, L является подалгеброй в $M_k(A)$, где $k = \frac{n}{m}$. Имеем $\deg M_k(A) = n$. По Предложению $[A] = [M_k(A)] = [L/F, \sigma, a]$ для некоторого $a \in F^\times$. $\square$

Мы доказали, что отображение

$$F^* \longrightarrow \text{Br}(L/F), \quad a \longmapsto [L/F, \sigma, a]$$

является сюръективным. Можно показать, что это — изоморфизм.

Имеются изоморфизмы нормы $N_{L/F} : L^* \longrightarrow F^*$,

$$N_{L/F}(x) = x \cdot \sigma(x) \cdot \sigma^2(x) \cdots \sigma^{n-1}(x).$$

Лемма. $[L/F, \sigma, a] = [L/F, \sigma, b] \iff \frac{b}{a} \in N_{L/F}(L^*)$.

Док-во. $\Rightarrow$: Имеем изоморфизм $f: (L/F, \overset{A}{\sigma}, a) \rightarrow (L/F, \overset{B}{\sigma}, b)$. Так как подполя L и $f(L)$ в $(L/F, \sigma, b)$ изоморфны, то они сопряжены по Теореме НС. Заменяя f на композицию f с внутренним автоморфизмом, мы можем считать, что $f(l) = l \quad \forall l \in L$. Так как $u \cdot u^{-1} = \sigma(l)$ в $(L/F, \overset{A}{\sigma}, a)$, то $f(u) \cdot l \cdot f(u)^{-1} = \sigma(l)$. В алгебре $(L/F, \overset{B}{\sigma}, b)$ имеем $v \cdot l \cdot v^{-1} = \sigma(l)$, где v образующая. Тогда $f(u) \cdot v \in C_B(L) = L$, т.е. $v = f(u)l$ для некоего $l \in L$. Наконец,

$$b = v^n = (f(u)l)^n = f(u^n l^n) = f(N_{L/F}(l) \cdot u^n) = N_{L/F}(l) \cdot a.$$

$\Leftarrow$: Пусть $b = N_{L/F}(l) \cdot a$ для некоторого $l \in L^*$. В алгебре $(L/F, \sigma, a)$

выберем группу образующую $v = l \cdot u$. Тогда по-прежнему

$$vxv^{-1} = \sigma(x) \quad \forall x \in L \quad \text{и} \quad v^n = (lu)^n = N_{L/F}(l) \cdot u^n = b, \text{ т.е.}$$

$$(L/F, \sigma, a) \cong (L/F, \sigma, b). \quad \square$$

Следствие. Гомоморфизм $F^*/N_{L/F}(L^*) \rightarrow Br(L/F)$, переводящий

$a \cdot N_{L/F}(L^*)$ в $[L/F, \sigma, a]$, является изоморфизмом.

Remark. $[L/F, \sigma, a] = 1$
 $\Leftrightarrow a \in N_{L/F}(L^*)$.

Примеры. 1. $Br(\mathbb{R}) = Br(\mathbb{C}/\mathbb{R}) = \mathbb{R}^*/N(\mathbb{C}^*)$ циклическая группа порядка 2, порожденная классом -1 , т.е. $Br(\mathbb{R}) = \{1, [H]\}$.

2. Пусть F конечное поле, L/F конечное расширение. Тогда L/F - циклическое расширение и значит $Br(L/F) = F^*/N_{L/F}(L^*) = 1$, так как норма сюръективна для конечных полей. Значит

$$Br(F) = \bigcup_{L/F} Br(L/F) = 1.$$

3. Пусть $L = \mathbb{Q}(\sqrt{-1})$. Группа $Br(L/\mathbb{Q}) \simeq \mathbb{Q}^*/\{a^2+b^2\}$ бесконечна, поэтому $Br(\mathbb{Q})$ бесконечна.

Экспонента $exp(A)$ ч.п.а. A - это порядок $[A]$ в $Br(F)$. Факт: $exp(A) | ind$

Пример. Так как $(F^*)^n \subset N_{L/F}(L^*)$, то $exp(A) | n$.

Примарное разложение: Если D алгебра с делением степени

$n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, где p_i различные простые, то $D \simeq D_1 \otimes D_2 \otimes \dots \otimes D_s$,

где D_i - алгебра с делением степени $p_i^{k_i} \Rightarrow$ многие вопросы сводятся к примарному случаю.

Не все у.п.а. циклические: например $\otimes$ двух циклических алгебр ^{степени p} может не быть циклической алгеброй степени p^2

Вопрос: Верно ли, что любая у.п.а. простой степени p является циклической? Однако над конечным расширением степени p простой с p алгебра становится циклической

Да, если $p=2$ или $p=3$. Если $p \geq 5$ вопрос открыт.

Случай $p=2$: пусть $\deg A = 2$. Если A не расщеплена, то A -алгебра с делением. Максимальное подполе квадратично и оно циклическое если сепарабельно (всегда можно выбрать).

Вопрос: Верно ли, что любая у.п.а. экспоненты p является $\otimes$ циклических алгебр степени p ?

Верно для степени 2 и 4, но неверно для 8.

Предположим, что поле F содержит первообразный корень ζ_n степени n из единицы. Известно, что любое циклическое расширение L поля F имеет вид $L = F(b^{\frac{1}{n}})$, где $b \in F$. и $\sigma(b^{\frac{1}{n}}) = \zeta_n \cdot b^{\frac{1}{n}}$ Тогда циклическая алгебра $(L/F, \sigma, a)$ порождается элементами u и $v = b^{\frac{1}{n}}$ с соотношениями $u^n = a$, $v^n = b$, и $uv = \zeta_n vu$. Мы обозначаем эту алгебру $(a, b)_{\zeta_n} = (a, b)$.

Свойства: 1) $[a, b]_n \cdot [a', b']_n = [aa', b]_n$

2) $[a, vv']_n = [a, v]_n \cdot [a, v']_n$

3) $[a, 1-a]_n = 1$, так как $1-a = N_{F(a^{\frac{1}{n}})/F}(1-a^{\frac{1}{n}})$. УПР.

Определяем ^(аддитивную) группу $K_2(F)$: образующие $\{a, b\}$, где $a, b \in F^\times$

и соотношения 1), 2), 3). Существует гомоморфизм нормального вычета

$$h_F: K_2(F)/nK_2(F) \longrightarrow \text{Br}(F)[n] := \{[A]: [A]^n = 1\}.$$

$$\{a, b\} + nK_2(F) \mapsto [a, b]_{\mathbb{Z}_n}$$

Теорема (Суслин-М, 1982) Гомоморфизм h_F всегда является
изоморфизмом. $\square$

Следствие. Если $\mathbb{Z}_n \in F$, то группа $\text{Br}(F)[n]$ порождается классами
циклических алгебр $[a, b]_{\mathbb{Z}_n}$, $a, b \in F^\times$. $\square$

Если не предполагать, что $\mathbb{Z}_n \in F$, возникает

Вопрос: Пусть p -простое число. Верно ли что $\text{Br}(F)[p]$
порождается классами циклических алгебр степени p ?

Да, если $p=2, 3$ или 5 . Если $p \geq 7$ вопрос открыт.