Центральные простые алгебры

Часть 1. Критерий простоты

Напомним, что радикалом Джекобсона алгебры A называется пресечение всех левых максимальных идеалов в A. Радикал Джекобсона алгебры A обозначается $\mathfrak{R}_A$.

Лемма 1.1. *Радикал Джекобсона является двусторонним идеалом.*

Доказательство: пусть $x \in \mathfrak{R}_A$, $a \in A$ и $xa \notin \mathfrak{R}_A$. Тогда найдется левый максимальный идеал $\mathfrak{m} \subset A$, такой что $xa \notin \mathfrak{m}$. Рассмотрим $I = \{ z \in A \mid za \in \mathfrak{m} \}$. Ясно, что I — левый идеал, $x \notin I$. Отображение $A/I \to A/\mathfrak{m}$, $z \mapsto za$ является вложением левых A-модулей, причем $A/I \neq 0$. Так как $A/\mathfrak{m}$ — простой A-модуль, то $A/I \cong A/\mathfrak{m}$, значит I максимален, и $x \notin \mathfrak{R}_A$. □

Лемма 1.2. *Радикал Джекобсона алгебры $B = A/\mathfrak{R}_A$ равен нулю.*

Доказательство: пусть $f : A \to B$ — проекция. Если $\mathfrak{m} \subset B$ — максимальный левый идеал в B, то $f^{-1}(\mathfrak{m})$ — максимальный идеал в A. Обратно, если $\mathfrak{m} \subset A$ — максимальный левый идеал, то $\mathfrak{R}_A \subset \mathfrak{m}$, поэтому $\mathfrak{m}/\mathfrak{R}_A \subset B$ — максимальный идеал в B. Следовательно, $\mathfrak{R}_A = f^{-1}(\mathfrak{R}_B)$. значит $\mathfrak{R}_B = f(f^{-1}(\mathfrak{R}_B)) = f(\mathfrak{R}_A) = 0$. □

Пусть теперь A — конечномерная алгебра с нулевым радикалом Джекобсона. Тогда пересечение всех левых максимальных идеалов в A равно нулю.

Лемма 1.3. *Пересечению конечного числа левых максимальных идеалов в A равно нулю.*

Доказательство: рассмотрим среди множества конечных пересечений левых максимальных идеалов идеал минимальной размерности над полем k. Ясно, что он лежит в любом левом максимальном идеале (иначе размерность пересечения уменьшилась бы), поэтому он равен нулю. □

Выберем представление $0 = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ с минимально возможным r. Пусть $L_i = \bigcap_{j \neq i} \mathfrak{m}_j$.

Лемма 1.4. *Имеем $\mathfrak{m}_i \cap L_i = 0$, $\mathfrak{m}_i + L_i = A$.*

Доказательство: $\mathfrak{m}_i \cap L_i = \bigcap_j \mathfrak{m}_j = 0$. Кроме того, $\mathfrak{m}_i \subset \mathfrak{m}_i + L_i$, поэтому либо $\mathfrak{m}_i + L_i = A$, либо $\mathfrak{m}_i + L_i = \mathfrak{m}_i$. В последнем случае $L_i \subset \mathfrak{m}_i$, значит $0 = L_i$ и r не было минимальным. □

Следствие 1.5. *Имеем изоморфизм A-модулей $L_i \cong A/\mathfrak{m}_i$.*

Доказательство: гомоморфизм $L_i \to A \to A/\mathfrak{m}_i$ инъективен и сюръективен. □

Следствие 1.6. *Идеал L_i прост.*

Лемма 1.7. *Имеем $A \cong \oplus_{i=1}^r L_i$.*

Доказательство: докажем индукией по k, что $\oplus_{i=1}^k L_i = \bigcap_{j=k+1}^r \mathfrak{m}_j$. База индукции, $k = 0$ очевидна. Пусть случай $k-1$ доказан. Тогда $(\oplus_{i=1}^{k-1} L_i) \cap L_k = (\bigcap_{j=k}^r \mathfrak{m}_j) \cap L_k \subset \mathfrak{m}_k \cap L_k = 0$, значит сумма $\sum_{i=1}^k L_i \subset A$ — прямая. Кроме того, ясно что $\oplus_{i=1}^k L_i \subset \bigcap_{j=k+1}^r \mathfrak{m}_j$, так как каждое из слагаемых в левой части содержится в каждом из пересекаемых идеалов в правой части. Рассмотрим идеал $I = \bigcap_{j=k+1}^r \mathfrak{m}_j$. Мы уже доказали, что морфизм $L_k = (\oplus_{i=1}^k L_i)/(\oplus_{i=1}^{k-1} L_i) \to I/I \cap \mathfrak{m}_k \to A/\mathfrak{m}_k$ является изоморфизмом, а при этом отображение $I/I \cap \mathfrak{m}_k \to A/\mathfrak{m}_k$ — вложение, поэтому $L_k \cong I/I \cap \mathfrak{m}_k$, следовательно $\oplus_{i=1}^k L_i = I$. □

Следствие 1.8. *Алгебра A полупроста.*

Теорема 1.9. *Конечномерная над полем* k *алгебра* A *полупроста* $\iff \mathfrak{R}_A = 0$.

Доказательство: ($\Longleftarrow$) уже доказано, докажем ($\Longrightarrow$). Если A полупроста, то A есть сумма простых левых идеалов, $A = \oplus_{i=1}^{r} L_i$. Ясно, что $\mathfrak{m}_j = \oplus_{i \neq j} L_i = \mathrm{Ker}(A \to L_j)$ является максимальным левым идеалом, и $\bigcap_{j=1}^{r} \mathfrak{m}_j = 0$, поэтому $\mathfrak{R}_A = 0$. $\square$

Следствие 1.10. *Если конечномерная алгебра* A *над полем* k *не имеет нетривиальных двусторонних идеалов, то* A *проста.*

Доказательство: радикал Джекобсона является двусторонним идеалом, поэтому $\mathfrak{R}_A = 0$ и A — полупроста, то есть A есть произведение матричных алгебр над телами. Если сомножителей больше одного, то в A есть двусторонние идеалы. $\square$

Часть 2. Простые алгебры и расширения полей

Лемма 2.1. *Если* D *тело, то все односторонние идеалы в* $D[t]$ *главные.*

Доказательство: элемент минимальной степени в иделе порождает его, так как в $D[t]$ можно делить с остатком (для левых идеалов надо делить справа, а для правых — слева). $\square$

Лемма 2.2. *Пусть* D — *тело,* $K = Z(D)$ — *его центр. Левый идеал* $D[t]f(t) \subset D[t]$ *является двусторонним* $\iff f(t) = ag(t)$, *где* $a \in D^*$, $g(t) \in K[t]$.

Доказательство: пусть a — старший коэффициент f, и $g(t) = a^{-1}f(t)$. Ясно, что идеал $D[t]g(t) = D[t]f(t)$ — двусторонний. Пусть $x \in D^*$. Тогда $g(t)x \in D[t]g(t)$, значит $g(t)x = yg(t)$, где $y \in D^*$. Сравнивая старшие коэффициенты, получаем $y = x$. Значит все коэффициенты многочлена $g(t)$ коммутируют с x. Так как x любое, то $g(t) \in K[t]$. $\square$

Пусть A и B — алгебры над полем K. Рассмотрим тензорное произведение $A \otimes_K B$. Тогда отображение $(A \otimes_K B) \otimes_K (A \otimes_K B) = A \otimes_K B \otimes_K A \otimes_K B = (A \otimes_K A) \otimes_K (B \otimes_K B) \stackrel{m_A \otimes m_B}{\longrightarrow} A \otimes_K B$ задает на $A \otimes_K B$ структуру K-алгебры. Иначе говоря, если $e_1, \ldots, e_m$ — базис A над K, а $f_1, \ldots, f_n$ — базис B над K, то в базисе $e_i \otimes f_j$ умножение задается формулой $(e_i \otimes f_j)(e_k \otimes f_l) = (e_i e_k) \otimes (f_j f_l)$.

Примеры 2.3.
1. $\mathrm{Mat}_{m\times m}(K) \otimes_K \mathrm{Mat}_{n\times n}(K) \cong \mathrm{Mat}_{mn\times mn}(K)$;
2. $\mathrm{Mat}_{n\times n}(K) \otimes_K A \cong \mathrm{Mat}_{n\times n}(A)$;
3. $\mathrm{Mat}_{m\times m}(A) \otimes_K \mathrm{Mat}_{n\times n}(B) \cong \mathrm{Mat}_{mn\times mn}(A \otimes_K B)$.

Лемма 2.4. *Имеем* $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$.

Доказательство: пусть $x \in Z(A \otimes_K B)$. Разложим x по базису $\{ e_i \}$ алгебры A: $x = \sum e_i \otimes x_i$. Для всякого $b \in B$ имеем $(1 \otimes b)x = \sum e_i \otimes (bx_i)$, $x(1 \otimes b) = \sum e_i \otimes (x_i b)$, поэтому $x_i \in Z(B)$, то есть $x \in A \otimes_K Z(B)$. Раскладывая x по базису $Z(B)$ и коммутируя с элементами вида $a \otimes 1$, $a \in A$ получаем, что $x \in Z(A) \otimes_K Z(B)$. $\square$

Определение 2.5. Алгебра A над полем K называется центральной простой алгеброй, если она проста (то есть изоморфна матричной алгебре над полем), а ее центр совпадает с полем K.

Лемма 2.6. *Пусть* D — *тело,* $K = Z(D)$ — *его центр. Если* L/K — *примитивное расширение полей, то* $D \otimes_K L$ — *центральная простая алгебра над* L.

Доказательство: Заметим, что $L \cong K[t]/K[t]f(t)$, где $f(t) = \mathrm{Irr}_\alpha^K(t)$ и $D \otimes_K L \cong D[t]/D[t]f(t)$. Обозначим через $\pi : D[t] \to D \otimes_K L$ — проекцию. Пусть $I \subset D \otimes_K L$ — двусторонний идеал. Тогда $\pi^{-1}(I) \subset D[t]$ — двусторонний идеал в $D[t]$, поэтому $\pi^{-1}(I) = D[t]g(t)$, $g(t) \in K[t]$. Так как $\pi^{-1}(I) \supset \mathrm{Ker}\, \pi = D[t]f(t)$, то $g(t)$ делит $f(t)$, поэтому $g(t) = 1$ или $g(t) = f(t)$, так как $f(t)$ неприводим над K. В первом случае $\pi^{-1}(I) = D[t]$, значит $I = D \otimes_K L$, а во втором случае $\pi^{-1}(I) = D[t]f(t)$, значит $I = 0$. Таким образом, в алгебре $D \otimes_K L$ нет нетривиальных двусторонних идеалов, значит она проста. Остается заметить, что $Z(D \otimes_K L) = Z(D) \otimes_K Z(L) = K \otimes_K L = L$. $\square$

Следствие 2.7. *Если* A — *центральная простая алгебра над* K, *а* L/K — *примитивное расширение полей, то* $A \otimes_K L$ — *центральная простая алгебра над* L.

Доказательство: $A \cong \mathrm{Mat}_{n\times n}(D)$ так как A простая, и $Z(A) = Z(D) = K$, так как A центральная, поэтому $A \otimes_K L \cong \mathrm{Mat}_{n\times n}(D) \otimes_K L \cong \mathrm{Mat}_{n\times n}(K) \otimes_K D \otimes_K L \cong \mathrm{Mat}_{n\times n}(K) \otimes_K \mathrm{Mat}_{m\times m}(D') \cong \mathrm{Mat}_{nm\times nm}(D')$ и $Z(A \otimes_K L) = Z(A) \otimes_K Z(L) = K \otimes_K L = L$. □

Следствие 2.8. *Если A — центральная простая алгебра над K, а L/K — конечное расширение полей, то $A \otimes_K L$ — центральная простая алгебра над L.*

Доказательство: всякое конечное расширение представляется в виде башни примитивных расширений. □

Часть 3. Группа Брауера

Лемма 3.1. *Всякий автоморфизм алгебры $A = \mathrm{Mat}_{n\times n}(K)$ является внутренним.*

Доказательство: пусть $V = K^n$, так что $A = \mathrm{End}_K(V)$. Для всех $f \in V^*$ идеал $L_f = \{ a \in \mathrm{End}_K(V) \mid \mathrm{Ker}\, a \subset \mathrm{Ker}\, f \}$ прост так как $L_f \cong V$ (изоморфизм задается отображением $a \mapsto av$ для любого $v \in V$, такого что $f(v) \neq 0$). Выберем базис $\{ e_i \}$ в V, рассмотрим двойственный базис $\{ f_i \}$ в V^* и пусть $L_1 = L_{f_1}$. Пусть теперь ϕ — автоморфизм A Тогда $\phi(L_1)$ — простой идеал, поэтому $\phi(L_1) = L_f$. Прокомпонировав ϕ с внутренним автоморфизмом можно считать, что $f = f_1$, то есть $\phi(L_1) = L_1$. Зафиксировав изоморфизм $L_1 \cong V$ мы видим, что ϕ индуцирует автоморфизм V. Прокомпонировав ϕ с соответсвтующим внутренним автоморфизмом можно считать, что $\phi_{|L_1} = \mathrm{Id}_{L_1}$. Покажем, что тогда $\phi = \mathrm{Id}$. Действительно, если E_{ij} — матричные единицы, то $\phi(E_{i1}) = E_{i1}$. Соотношение $E_{kj}E_{i1} = \delta_{ji}E_{k1}$ тогда показывает, что $\phi(E_{kj}) = E_{kj}$. □

Лемма 3.2. *Если A — центральная простая алгебра над K, то найдется конечное расширение полей L/K, такое что $A \otimes_K L \cong \mathrm{Mat}_{n\times n}(L)$.*

Доказательство: пусть $A = \mathrm{Mat}_{m\times m}(D)$. Достаточно проверить, что если $D \neq K$, то найдется расширение L/K, такое что $A \otimes_K L \cong \mathrm{Mat}_{m'\times m'}(D')$, и $\dim_K D' < \dim_K D$. Действительно, если $\alpha \in D$, $\alpha \notin K$, то $K(\alpha) \subset D$ — подполе, а $D \otimes K(\alpha)$ имеет делители нуля, поэтому $D \otimes_K K(\alpha) = \mathrm{Mat}_{m''\times m''}(D')$ и $m'' > 1$, поэтому $\dim_K D' < \dim_K D$. □

Расширение L/K, такое что $A \otimes_K L \cong \mathrm{Mat}_{n\times n}(L)$ называется полем разложения алгебры A.

Пусть K — совершенное поле, а L/K — поле разложения алгебры A. Тогда L/K сепарабельно, и расширив L еще немного, можно считать, что L/K — расширение Галуа. Пусть $G = \mathrm{Gal}(L/K)$. Зафиксируем изоморфизм $f_0 : A \otimes_K L \to \mathrm{Mat}_{n\times n}(L)$. Для всякого элемента $g \in G$ отображение $\phi_g = 1 \otimes g : A \otimes_K L \to A \otimes_K L$ является автоморфизмом алгебры $A \otimes_K L$ над K, который на L действует автоморфизмом g. Кроме того, изоморфизм f_0 и действие группы G на $\mathrm{Mat}_{n\times n}(L)$ индуцирует автоморфизм ϕ'_g алгебры $A \otimes_K L$ над K с тем же действием на L. Поэтому композиция $\phi_g \circ {\phi'_g}^{-1}$ является автоморфизмом алгебры $A \otimes_K L$ над L, следовательно найдется элемент $a(g) \in \mathrm{GL}_n(L)$, такой что $\phi_g \circ {\phi'_g}^{-1} = \mathrm{Ad}_{a(g)}$, то есть $\phi_g = \mathrm{Ad}_{a(g)} \circ \phi'_g$. Перемножая эти равенства для $g_1, g_2 \in G$ получаем $\phi_{g_1g_2} = \phi_{g_1} \circ \phi_{g_2} = \mathrm{Ad}_{a(g_1)} \circ \phi'_{g_1} \circ \mathrm{Ad}_{a(g_2)} \circ \phi'_{g_2} = \mathrm{Ad}_{a(g_1)} \circ \mathrm{Ad}_{g_1 a(g_2)} \circ \phi'_{g_1} \circ \phi'_{g_2} = \mathrm{Ad}_{a(g_1)\cdot g_1 a(g_2)} \circ \phi'_{g_1g_2}$, значит $\mathrm{Ad}_{a(g_1)\cdot g_1 a(g_2)} = \mathrm{Ad}_{a(g_1g_2)}$. Следовательно, найдутся элементы $\lambda(g_1, g_2) \in L^*$, такие что $a(g_1g_2) = \lambda(g_1, g_2)a(g_1)g_1a(g_2)$. Тогда $\lambda(g_1g_2, g_3) \cdot \lambda(g_1, g_2) = g_1\lambda(g_2, g_3) \cdot \lambda(g_1, g_2g_3)$, то есть λ — 2-коцикл группы G с коэфициентами в L^*. Можно показать, что произвол в выборе λ сводится к изменению λ на кограницу. Тем самым, всякой центральной простой алгебре A можно сопоставить класс когомлогий $\bar{\lambda} \in H^2(\mathrm{Gal}(L/K), L^*)$. Обратно, если λ — 2-коцикл, представляющий такой клас когомологий, то пространство $L[G]$ с умножением $e_{g_1} * e_{g_2} = \lambda(g_1, g_2)e_{g_1g_2}$, $e_g * \lambda = g(\lambda)e_g$ является центральной простой алгеброй над K. Можно показать, что эти две конструкции взаимно обратны в следующем смысле. Назовем центральные простые K-алгебры A и B подобными, если $\mathrm{Mat}_{n\times n}(A) \cong \mathrm{Mat}_{m\times m}(B)$. Тогда $A \equiv B \Longrightarrow \bar{\lambda}(A) = \bar{\lambda}(B)$, $A_{\bar{\lambda}(A)} \equiv A$, $\bar{\lambda}(A_{\bar{\lambda}}) = \bar{\lambda}$.

Теорема 3.3. *Множество классов подобия центральных простых алгебр над полем K, разлагающихся над полем L изоморфно группе $H^2(\mathrm{Gal}(L/K), L^*)$.*

Легко видеть, что в каждом класе подобия найдется ровно одно тело, поэтому множество тел над полем K, разлагающихся над полем L изоморфно группе $H^2(\mathrm{Gal}(L/K), L^*)$.

Следствие 3.4. *Множество классов изоморфизма всех центральных тел над полем K изоморфно группе $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = \bigcup\limits_{L/K} H^2(\mathrm{Gal}(L/K), L^*)$, которая называется* группой Брауэра *поля K.*