Центральные простые алгебры. Сводка результатов.

Следующий далее текст не претендует на полное и/или последовательное изложение теории центральных простых алгебр. Здесь собраны определения, примеры, формулировки утверждений, которые в разные моменты появлялись на лекциях. Возможно, этот текст поможет слушателям восстановить логику рассуждения в некоторых местах. Доказательства в большинстве своём проводятся достаточно прямолинейно и в тексте не приводятся.

Теорема 1. Конечномерная простая алгебра — алгебра матриц над некоторым телом D. Все минимальные левые идеалы центральной простой алгебры изоморфны. Тело D определено однозначно с точностью до изоморфизма и изоморфно телу A-эндоморфизмов любого минимального левого идеала.

Определение 1. Алгебра A над полем K называется центральной, если её центр $Z(A)$ совпадает с K.

Лемма 1. $Z(A \otimes B) \simeq Z(A) \otimes Z(B)$.

Теорема 2. Тензорное произведение двух простых алгебр — простая алгебра, если хотя бы одна из этих алгебр центральна. Тензорное произведение центральных простых алгебр — центральная простая алгебра.

Замечание 1. Тензорное произведение двух простых алгебр — простая алгебра, если хотя бы один из сомножителей централен.

Теорема 3. Если A — центральная простая алгебра, то $A \otimes A^{opp} \simeq \mathrm{End}(A)$.

Определение 2. Зададим на множестве центральных простых алгебр над полем F отношение эквивалентности: $A \sim B$, если $A \otimes \mathrm{Mat}_n(F) \simeq B \otimes \mathrm{Mat}_m(F)$ для некоторых m и n (т.е. если эти алгебры — матричные над одним и тем же телом). Тензорное произведение согласовано с эквивалентностью и задаёт на множестве классов эквивалентности структуру абелевой группы (наличие обратного следует из предыдущей теоремы). Эта группа называется группой Брауэра поля F и обозначается $\mathrm{Br}(F)$.

Пример 1. Если поле F алгебраически замкнуто, то $\mathrm{Br}(F) = \{e\}$.

Теорема 4. Все неприводимые представления центральной простой алгебры изоморфны представлению в эндоморфизмах минимального левого идеала. Любое конечномерное представление вполне приводимо (есть сумма нескольких экземпляров этого неприводимого).

Следствие. Пусть A — конечномерная простая алгебра над полем F, φ, ψ — два гомоморфизма A в алгебру матриц $n \times n$. Тогда существует обратимая матрица f, для которой выполнено $\varphi(x) = f^{-1}\psi(x)f$ при всех $x \in A$.

Теорема 5. (Сколем–Нётер) Пусть A — центральная простая алгебра, B — её простая подалгебра. Любое вложение χ алгебры B в A продолжается до внутреннего автоморфизма алгебры A, т.е. существует обратимый элемент $f \in A$, для которого $\chi(b) = f^{-1}bf$ при всех $b \in B$.

Определение 3. Пусть A — алгебра, B — её подалгебра. Централизатор B в A состоит из всех элементов $z \in A$, для которых $zb = bz$ при всех $b \in B$. Централизатор — подалгебра в A, обозначаемая $Z_A(B)$.

Теорема 6. (Теорема о бикоммутанте для центральных простых алгебр) Пусть A — центральная простая алгебра, B — её простая подалгебра. Тогда

- алгебра $Z_A(B)$ проста;
- $\dim B \cdot \dim Z_A(B) = \dim A$;
- $Z_A(Z_A(B)) = B$;
- если алгебра B центральна, то алгебра $Z_A(B)$ тоже центральна и $A = B \otimes Z_A(B)$.

Следствие. (Веддербёрн) Конечное тело коммутативно. (Таким образом, $\mathrm{Br}(\mathbb{F}_q) \simeq \{e\}$.)

Теорема 7. Пусть D — центральное тело, E — его максимальное (по включению) подполе. Тогда $\dim D = (\dim E)^2$.

Следствие. (Фробениус) Алгебры с делением над $\mathbb{R}$ суть $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$. (Центральные тела суть $\mathbb{R}$ и $\mathbb{H}$. Таким образом, $\mathrm{Br}(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$.)

Определение 4. Пусть A — центральная простая алгебра над полем F. Расширение E поля F называется полем расщепления для A, если $A \otimes E$ — алгебра матриц над E.

Замечание 2. У любой центральной простой алгебры существует поле расщепления (например, алгебраическое замыкание основного поля).

Замечание 3. Если A, B — представители одного класса группы Брауэра, то любое поле расщепления для одной из этих алгебр будет и полем расщепления для другой.

Лемма 2. Пусть A — центральная простая алгебра, E — подполе в A. Тогда $Z_A(E)$ — центральная простая алгебра над E, класс которой в $\mathrm{Br}(E)$ совпадает с классом $A \otimes E$.

Теорема 8. Пусть D — центральное тело, E — его максимальное подполе. Тогда E — поле расщепления для D.

Определение 5. Подполе E центральной простой алгебры A называется строго максимальным, если $\dim A = (\dim E)^2$.

Лемма 3. Пусть E — строго максимальное подполе центральной простой алгебры A. Тогда

- E — поле расщепления для A;
- $Z_A(E) = \mathrm{Mat}_k(E)$, где $(k \dim E)^2 = \dim A$.

Лемма 4. Если E — поле расщепления центральной простой алгебры, то E вкладывается в качестве подполя в некоторую алгебру из того же класса группы Брауэра.

Теорема 9. Любое поле расщепления центральной простой алгебры вкладывается в качестве строго максимального подполя в некоторую алгебру из того же класса в группе Брауэра.

Теорема 10. Любая центральная простая алгебра обладает полем расщепления, являющимся расширением Галуа.

Замечание 4. Реально в предыдущей теореме (не доказанной в курсе) нетривиальна лишь сепарабельность (нормальности легко добиться — достаточно взять поле разложения минимального многочлена примитивного элемента).

Определение 6. Пусть E — расширение основного поля F, $G = \mathrm{Gal}(E : F)$. Скрещённое произведение G и E — это пространство $F[G] \otimes_F E$, снабжённое необычной операцией умножения. Именно, фиксируется набор элементов $c_{g,h} \in E^*$, и закон умножения определяется формулами

$$\begin{aligned}
(g \otimes 1)(h \otimes 1) &= gh \otimes c_{g,h},\\
(g \otimes 1)(1 \otimes l) &= g \otimes l,\\
(1 \otimes l)(g \otimes 1) &= g \otimes g^{-1}(l),\\
(1 \otimes l)(1 \otimes l') &= 1 \otimes ll'.
\end{aligned}$$

Здесь нужно предположить, что выполнены условия («уравнение коцикла»)

$$c_{fg,h}h^{-1}(c_{f,g}) = c_{f,gh}c_{g,h}.$$

В этом случае набор элементов $c_{g,h}$ называется (нётеровой) системой факторов.

Теорема 11. Скрещённое произведение — центральная простая алгебра для любого выбора системы факторов, E — строго максимальное подполе в ней.

Теорема 12. Пусть A — центральная простая алгебра, E — расширение Галуа, которое её расщепляет. Рассмотрим алгебру из того же класса группы Брауэра, в которой E — строго максимальное подполе. Тогда эта алгебра изоморфна скрещённому произведению поля E с его группой Галуа (для некоторой системы факторов).

Теорема 13. Две системы факторов $\{c_{g,h}\}$ и $\{d_{g,h}\}$ задают изоморфные алгебры, если и только если существует набор $a_h \in L^*$, для которого

$$d_{g,h} = \frac{h^{-1}(a_g)a_h}{a_{gh}} c_{g,h}.$$

Следствие. Профакторизуем множество систем факторов, которые удовлетворяют уравнению коцикла, по такому отношению эквивалентности. Тогда полученное множество с помощью конструкции скрещённого произведения биективно отображается на подгруппу группы Брауэра, которая состоит из классов алгебр, расщепляющихся над E.

Замечание 5. На множестве классов эквивалентности систем факторов есть групповой закон (покомпонентное умножение). Группа классов систем факторов с такой операцией называется второй группой когомологий группы $G = \mathrm{Gal}(E : F)$ с коэффициентами в E^* и обозначается $H^2(G, E^*)$. Подробно такие когомологии изучает «теория полей классов».

Теорема 14. (Теорема о произведении) Биекция между $\mathrm{Br}_E(F)$ (подгруппой группы Галуа, состоящей из классов, расщепляющихся над E) и $H^2(G, E^*)$, описанная в предыдущем следствии, есть изоморфизм групп.

Эту теорему можно доказывать по-разному. Мы докажем её в очень специальном частном случае, доказательство общего случая можно прочесть в книге Пирса (более явное; в тензорном произведении двух скрещённых произведений явно выделяется нужная подалгебра) и в книге Ван дер Вардена (где предлагается другая параметризация группы когомологий — «брауэровы системы факторов»).

Следствие. Группа Брауэра любого поля F периодична, то есть все её элементы имеют конечный порядок. Если A расщепляется над E, то её порядок делит $[E : F]$.

Определение 7. Алгебра A называется циклической, если она содержит строго максимальное подполе, являющееся циклическим расширением Галуа основного поля.

Пример 2. Если основное поле содержит примитивный корень ξ степени n из 1, а его характеристика не делит n, то всякая циклическая алгебра размерности n^2 изоморфна алгебре с образующими x, y и соотношениями $x^n = a$, $y^n = b$, $yx = \xi xy$. Эта алгебра обозначается $A_\xi(a, b)$.

Лемма 5. Пусть A — центральная простая алгебра размерности n^2. Предположим, что минимальный многочлен некоторого её элемента имеет степень n, причём все его корни принадлежат основному полю и различны. Тогда алгебра A изоморфна алгебре $\mathrm{Mat}_n(F)$.

Следствие. $A_\xi(a^n, b) \simeq \mathrm{Mat}_n(F)$.

Теорема 15. Пусть $a_\xi(a, b)$ — класс алгебры $A_\xi(a, b)$ в $\mathrm{Br}(F)$. Тогда выполнены равенства

- $a_\xi(a, b)a_\xi(b, a) = 1$;
- $a_\xi(a, b)a_\xi(a, b') = a_\xi(a, bb')$;
- $a_\xi(a, 1 - a) = 1$.

Замечание 6. Второе из соотношений является частным случаем «теоремы о произведении».

Теорема 16. Для циклического расширения E поля F имеет место изоморфизм $\mathrm{Br}_E(F) \simeq F^*/N_{E/F}(E^*)$. В частности, $a_\xi(a, b) = 1$ если и только если a является нормой элемента из $F(\sqrt[n]{b})$.

Следствие. Пусть $a, b \in F$. Тогда a является нормой элемента из $F(\sqrt[n]{b})$ если и только если b является нормой элемента из $F(\sqrt[n]{a})$.

Определение 8. Пусть K — расширение основного поля, $\rho\colon A \to \mathrm{Mat}_n(F)$ — гомоморфизм. Характеристический многочлен, норма, след элемента алгебры A в этом представлении — это характеристический многочлен, определитель и след соответствующего оператора.

Определение 9. Пусть E — поле расщепления алгебры A. Тогда расщепляющее представление — это вложение в алгебру матриц $\mathrm{Mat}_m(E)$, где $\dim A = m^2$ (такое вложение есть по определению поля расщепления).

Лемма 6. Пусть ρ_E — расщепляющее представление, ρ — какое-то представление над E. Тогда размерность представления ρ делится на размерность представления ρ_E, и характеристический многочлен в представлении ρ является степенью характеристического многочлена в представлении ρ_E.

Определение 10. Норма, след, характеристический многочлен в расщепляющем представлении называются приведённой нормой, приведённым следом и приведённым характеристическим многочленом.

Теорема 17. Это определение корректно, т. е. не зависит от выбора расщепляющего представления.

Теорема 18. Коэффициенты приведённого характеристического многочлена лежат в основном поле.

Лемма 7. (Теорема Гамильтона – Кэли для центральных простых алгебр) Пусть a — элемент центральной простой алгебры a. Подставим a в его приведённый характеристический многочлен. Тогда получившийся элемент алгебры A равен нулю.

Теорема 19. Элемент центральной простой алгебры обратим тогда и только тогда, когда его приведённая норма отлична от нуля. Центральная простая алгебра является телом тогда и только тогда, когда приведённые нормы всех ненулевых элементов не равны нулю.

Замечание 7. Норма в координатах является однородным многочленом степени $\sqrt{\dim A}$. Использование предыдущей теоремы и теоремы Шевалле – Варнинга даёт теорему о коммутативности конечного тела. Кроме того, так же можно доказать теорему Тзена о тривиальности группы Брауэра $\mathbb{C}(t)$.

Определение 11. Пусть p — простое число. Поле p-адических чисел $\mathbb{Q}_p$ — это пополнение поля рациональных чисел по норме $||\cdot||_p$, сопоставляющей числу $z = p^k a/b$, где $a, b \in \mathbb{Z}$, $(ab, p) = 1$, число $||z|| = 1/p^k$. (Число тем «меньше», чем на бо́льшую степень p оно делится.)

Поле p-адических чисел используется для описания группы Брауэра поля $\mathbb{Q}$. Мы не будем доказывать соответствующие теоремы, а ограничимся формулировками.

Теорема 20. (Алберт – Брауэр – Хассе – Нётер) Пусть A — центральная простая $\mathbb{Q}$-алгебра. Тогда A является матричной алгеброй тогда и только тогда, когда она расщепляется над всеми $\mathbb{Q}_p$ и над $\mathbb{R}$.

Замечание 8. Во многих ситуациях работает «принцип Хассе», который гласит, что разнообразные факты для поля рациональных чисел достаточно проверять лишь «локально», т. е. в его всевозможных пополнениях. Так, например, для того, чтобы квадратичная форма «представляла нуль», необходимо и достаточно, чтобы это было верно над всеми пополнениями; класс простой алгебры в группе Брауэра тоже задаётся соответствующими классами в группах Брауэра пополнений. В разных других случаях (скажем, при изучении вопроса о представлении чисел формами высших степеней) этот принцип неверен.

Теорема 21. Для любого простого числа p имеет место изоморфизм $\mathrm{Br}(\mathbb{Q}_p) \simeq \mathbb{Q}/\mathbb{Z}$. Любая центральная простая алгебра над полем $\mathbb{Q}_p$ является циклической. Образ группы $\mathrm{Br}(\mathbb{Q})$ в группе $\mathrm{Br}(\mathbb{R}) \oplus \bigoplus_p \mathrm{Br}(\mathbb{Q}_p) \simeq (1/2\mathbb{Z}/\mathbb{Z}) \oplus \bigoplus_p \mathbb{Q}/\mathbb{Z}$ задаётся уравнением $t_\infty + \sum_p t_p = 0$, где $t_\infty \in (1/2\mathbb{Z})/\mathbb{Z}$, t_p принадлежит p-ому слагаемому $\mathbb{Q}/\mathbb{Z}$. Любая центральная простая алгебра над $\mathbb{Q}$ является циклической.