А. П. Пожидаев

Лекции по теории колец

Новосибирск

2012

Оглавление

Глава 1

Часть I

Мы начинаем изложение с общих теорем о гомоморфизмах и тензорном произведении, после чего переходим к построению структурной теории колец, в основе которой лежит понятие радикала Джекобсона. А цель любой структурной теории — описать общие объекты через простые.

§1 Ω-алгебры, теоремы о гомоморфизмах

Ω-Алгеброй над полем Φ называется линейное пространство A над Φ, на котором задана система полилинейных алгебраических операций $\Omega = \{\omega_i : |\omega_i| = n_i \in N,\ i \in I\}$, где символом $|\omega_i|$ обозначена арность операции ω_i.

Подпространство B Ω-алгебры A называется *подалгеброй*, если $\omega(b_1, \ldots, b_n) \in B$ для любых $b_1, \ldots, b_n \in B$ и $\omega \in \Omega$, $|\omega| = n$.

Подалгебра I Ω-алгебры A называется *идеалом*, если $\omega(a_1, \ldots, a_{i-1}, c, a_{i+1}, \ldots, a_n) \in I$ для любых $a_1, \ldots, a_n \in A$, $c \in I$, $\omega \in \Omega$ ($|\omega| = n$) и любого $1 \leq i \leq n$.

Если I — идеал в A, то мы можем рассмотреть фактор-пространство $A/I := \{a + I : a \in A\}$ и определить на нём операции правилом:

$$\omega(a_1 + I, \ldots, a_n + I) = \omega(a_1, \ldots, a_n) + I$$

для любых $a_i \in A$ и $\omega \in \Omega$, $|\omega| = n$. Легко проверить, что данные операции определены корректно и относительно них A/I становится Ω-алгеброй, которую называют *фактор-алгеброй* алгебры A по идеалу I (напомним, что $a_1 + I = a_2 + I \iff a_1 - a_2 \in I$).

Пусть A и B — Ω-алгебры с одной и той же системой операций Ω. Линейное отображение $\phi : A \mapsto B$ называется *гомоморфизмом* из A в B, если

$$\phi\left(\omega(a_1, \dots, a_n)\right) = \omega(\phi(a_1), \dots, \phi(a_n))$$

для любых $a_i \in A$ и $\omega \in \Omega$, $|\omega| = n$. Гомоморфизм $\phi : A \mapsto B$ называется *эпиморфизмом*, если его образ совпадает с B, т.е. $\operatorname{Im}\phi = B$. Множество $\operatorname{Ker}\phi := \{x \in A : \phi(x) = 0\}$ называется *ядром* гомоморфизма ϕ. Если $\operatorname{Ker}\phi = 0$, то такой гомоморфизм называется *мономорфизмом*. Гомоморфизм, являющийся мономорфизмом и эпиморфизмом, называется *изоморфизмом*.

Теорема 1. *Пусть A, B — Ω-алгебры над F и $\phi \in \operatorname{Hom}_F(A, B)$. Тогда $\operatorname{Ker}\phi \trianglelefteq A$ и $A/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$.*

Доказательство. Пусть $a \in \operatorname{Ker}\phi$. Тогда для любых $x_i \in A, \omega \in \Omega$ имеем

$$\phi(\omega(x_1, \dots, a, \dots, x_n)) = \omega_\phi(\phi(x_1), \dots, \phi(a), \dots, \phi(x_n)) = 0.$$

Следовательно, $\omega(x_1, \dots, a, \dots, x_n) \in \operatorname{Ker}\phi$.

Определим $\psi : A/\operatorname{Ker}\phi \mapsto \operatorname{Im}\phi$ правилом: $\psi(a + I) = \phi(a)$.

Корректность: $a + I = a_1 + I \Rightarrow a - a_1 \in I, \psi(a_1 + I) = \phi(a_1), \phi(a) = \phi(a_1)$.

Биективность ψ очевидна.

Гомоморфность: $\psi(\omega(x_1 + I, \dots, x_n + I)) = \psi(\omega(x_1, \dots, x_n) + I) = \phi(\omega(x_1, \dots, x_n)) = \omega_\phi(\phi(x_1), \dots, \phi(x_n)) = \omega_\phi(\psi(x_1 + I), \dots, \psi(x_n + I))$. □

Теорема 2. *Пусть A, B — Ω-алгебры над F и $\phi \in \operatorname{Hom}_F(A, B)$, $I := \operatorname{Ker}\phi, \operatorname{Im}\phi = B$. Тогда идеалы из A, содержащие I, находятся во взаимно однозначном соответствии с идеалами из B.*

Доказательство. Пусть $J \trianglelefteq A, I \subseteq J$. Покажем, что $\phi(J) \trianglelefteq B$. Пусть $b \in \phi(J)$. Тогда $b = \phi(a), a \in J$. Имеем

$$\omega_\phi(y_1, \dots, b, \dots, y_n) = \omega_\phi(\phi(x_1), \dots, \phi(a), \dots, \phi(x_n)) =$$

$$\phi(\omega(x_1, \dots, a, \dots, x_n)) \in \phi(J).$$

Определим отображение ψ_1, ставящее в соответствие идеалу J идеал $\phi(J)$.

Определим отображение ψ_2, ставящее в соответствие идеалу $H \trianglelefteq B$ идеал $\psi_2(H) := \{x \in A : \phi(x) \in H\}$. Покажем, что $\psi_2(H)$ — действительно идеал в A. Пусть $a \in \psi_2(H)$, т.е. $\phi(a) \in H$. Тогда $\phi(\omega(x_1, \ldots, a, \ldots, x_n)) = \omega_\phi(\phi(x_1), \ldots, \phi(a), \ldots, \phi(x_n)) \in \omega_\phi(\phi(x_1), \ldots, H, \ldots, \phi(x_n)) \subseteq H$. Следовательно, $\omega(x_1, \ldots, a, \ldots, x_n) \in \psi_2(H)$. Покажем взаимно однозначность, т.е. докажем, что
1). $\psi_2\psi_1(J) = J$;
2). $\psi_1\psi_2(H) = H$.

1). $\psi_1(J) = \phi(J) \Rightarrow \psi_2\psi_1(J) = \psi_2\phi(J) = \{x \in A : \phi(x) \in \phi(J)\}$.

Покажем, что $\psi_2\phi(J) = J$.

a). Если $a \in J$, то $a \in \psi_2\phi(J)$, т.е. $J \subseteq \psi_2\phi(J)$.

b). Если $b \in \psi_2\phi(J)$, то $\phi(b) \in \phi(J)$, т.е. $\phi(b) = \phi(j)$ для некоторого $j \in J$. Тогда $\phi(b - j) = 0$, т.е. $b - j \in I$ и $b \in J$.

2). $\psi_1\psi_2(H) = \phi\psi_2(H) = \phi(\{x \in A : \phi(x) \in H\}) \subseteq H$.

Пусть $b \in H$, тогда существует $a \in A$ такой, что $b = \phi(a) \in H$. Следовательно, $a \in \psi_2(H)$, а потому $b \in \phi\psi_2(H)$. □

Теорема 3. *Пусть $A, B \trianglelefteq C$ — Ω-алгебры над F. Тогда* $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

Доказательство. $A \cap B \trianglelefteq C, A \cap B \trianglelefteq B$. Пусть $\phi : A + B \mapsto \frac{B}{A \cap B}$ такое, что $\phi(a + b) = b + I$, где $I := A \cap B$.

1). *Корректность.* $a + b = a' + b' \Rightarrow a - a' = b' - b \in I$.

2). $\phi \in \mathrm{Hom}_F(A + B, B/I)$:

$$\phi(\omega(a_1 + b_1, \ldots, a_n + b_n)) = \phi(a + \omega(b_1, \ldots, b_n)) =$$

$$\omega(b_1, \ldots, b_n) + I = \omega(b_1 + I, \ldots, b_n + I) =$$

$$\omega(\phi(a_1 + b_1), \ldots, \phi(a_n + b_n)).$$

3). *Сюрьективность* очевидна.

4). $\mathrm{Ker}\,\phi = A : x \in A \Rightarrow \phi(x + 0) = 0 + I \Rightarrow x \in \mathrm{Ker}\,\phi$. Обратно, $x \in \mathrm{Ker}\,\phi, x = a + b \Rightarrow \phi(x) = b + I = 0 + I \Rightarrow b \in I \Rightarrow x \in A$. По теореме 1, $\frac{A+B}{A} \cong \frac{B}{A \cap B}$. □

Теорема 4. *Пусть $I, J \trianglelefteq A$, $I \trianglelefteq J$. Тогда* $\frac{A}{I}/\frac{J}{I} \cong \frac{A}{J}$.

Доказательство. Определим $\psi : \frac{A}{I} \mapsto \frac{A}{J}$ правилом $\psi(a + I) = a + J$.

1). *Корректность* очевидна.

2). *Гомоморфность*:

$$\psi(\omega(\bar{x}_1, \ldots, \bar{x}_n)) = \psi(\omega(x_1, \ldots, x_n) + I) =$$

$$\omega(x_1, \dots, x_n) + J = \omega(\psi(x_1), \dots, \psi(x_n)).$$

3). $\operatorname{Ker}\psi = J/I$. □

§2 Тензорное произведение пространств

Теорема 1. *Для любых векторных пространств* $V_1, \dots, V_m$ *над полем* F *существуют единственные (с точностью до изоморфизма) векторное пространство* T *и полилинейное отображение* $\tau : V_1 \times \dots \times V_m \mapsto T$*, такие что*: 1). $\operatorname{Im}\tau$ *порождает* T; 2). *для всякого полилинейного отображения* $\phi : V_1 \times \dots \times V_m \mapsto W$ *в векторное пространство* W *над* F *существует линейное отображение* $\phi_0 : T \mapsto W$ *такое, что* $\phi = \tau\phi_0$.

Доказательство. Пусть $T = L^*$, где $L = \{f : V_1 \times \dots \times V_m \mapsto F : f$ полилинейно и $\dim\langle Supp\, f\rangle < \infty\}$, где $Supp\, f := \{v_1 + \dots + v_m \in V_1 \oplus \dots \oplus V_m : f(v_1, \dots, v_m) \neq 0\}$.

Для $v_i \in V_i$ обозначим через $v_1 \otimes \dots \otimes v_m$ отображение из L в F такое, что

$$v_1 \otimes \dots \otimes v_m(f) = f(v_1, \dots, v_m).$$

Это отображение линейно. Положим $\tau(v_1, \dots, v_m) = v_1 \otimes \dots \otimes v_m$. Очевидно, что τ полилинейно. Проверим 1). Пусть $\{e_i^{(k)}\}$ — база V_k. Достаточно показать, что $\{e_{i_1}^{(1)} \otimes \dots \otimes e_{i_m}^{(m)}\}$ — база T. Легко видеть, что $\{e^*_{i_1 \dots i_m}\}$ — база в L, где

$$e^*_{i_1 \dots i_m}(e_{j_1}^{(1)}, \dots, e_{j_m}^{(m)}) = \delta_{i_1, j_1} \cdot \ldots \cdot \delta_{i_m, j_m} = e_{j_1}^{(1)} \otimes \dots \otimes e_{j_m}^{(m)}(e^*_{i_1 \dots i_m}),$$

где δ_{ij} — символ Кронекера, откуда следует, что $\{e_{i_1}^{(1)} \otimes \dots \otimes e_{i_m}^{(m)}\}$ — дуальная база к $\{e^*_{i_1 \dots i_m}\}$.

Докажем 2). Пусть такое ϕ задано. Возьмём в T базу $\{e_{i_1}^{(1)} \otimes \dots \otimes e_{i_m}^{(m)}\}$. Мы должны положить

$$\phi_0(e_{i_1}^{(1)} \otimes \dots \otimes e_{i_m}^{(m)}) = \phi(e_{i_1}^{(1)}, \dots, e_{i_m}^{(m)}).$$

Продолжим далее ϕ_0 по линейности на T. Тогда для любых $v_i \in V_i$ имеем

$$\phi(v_1, \dots, v_m) = \phi\left(\sum_i \alpha_{1i} e_i^{(1)}, \dots, \sum_j \alpha_{mj} e_j^{(m)}\right) =$$

$$\sum_i \dots \sum_j \alpha_{1i} \dots \alpha_{mj} \phi(e_i^{(1)}, \dots, e_j^{(m)}) =$$

$$= \sum_i \dots \sum_j \alpha_{1i} \dots \alpha_{mj} \phi_0(e_i^{(1)} \otimes \dots \otimes e_j^{(m)}) =$$

$$\sum_i \dots \sum_j \alpha_{1i} \dots \alpha_{mj} \phi_0(\tau(e_i^{(1)}, \dots, e_j^{(m)})) = \tau \circ \phi_0(v_1, \dots, v_m),$$

откуда $\phi = \tau \circ \phi_0$.

Докажем единственность. Пусть T', τ' — другая пара со свойствами 1) и 2). Возьмём вместо ϕ отображение τ'. Тогда существует линейное отображение $\tau_0' : T \mapsto T'$ такое, что

$$\tau \tau_0' = \tau'. \tag{1}$$

Аналогично, существует линейное отображение $\tau_0 : T' \mapsto T$ такое, что

$$\tau' \tau_0 = \tau. \tag{2}$$

Следовательно, $\tau' \tau_0 \tau_0' = \tau'$. Так как $\operatorname{Im} \tau' = T'$, то $\tau_0 \tau_0' = 1_{T'}$. Аналогично, $\tau_0' \tau_0 = 1_T$, т.е. τ_0 и τ_0' взаимно обратны и $T \cong T'$. □

Пространство T, построенное в теореме 1, называется *тензорным произведением* пространств $V_1, \dots, V_m$ и обозначается через $V_1 \otimes_F \dots \otimes_F V_m$, или просто $V_1 \otimes \dots \otimes V_m$.

Следствие. *Пусть* $\{e_i^{(k)}\}$ *— база* V_k, $k = 1, \dots, m$. *Тогда* $\{e_{i_1}^{(1)} \otimes \dots \otimes e_{i_m}^{(m)}\}$ *— база* $V_1 \otimes \dots \otimes V_m$.

Рассмотрим ещё один подход к построению тензорного произведения пространств.

Пусть V, U, W — линейные пространства над полем F. Рассмотрим множество $V \times_s U$ формальных сумм $\sum_i \alpha_i(v_i, u_i)$, где $(v_i, u_i) \in V \times U$ ($V \times U$ — декартово произведение V и U как множеств), $\alpha_i \in F$. Тогда множество $V \times_s U$ является линейным пространством над F.

Отображение f из $V \times_s U$ в пространство W называется *сбалансированным*, если выполнены следующие условия:

$$f(\sum \alpha_i(v_i, u_i)) = \sum \alpha_i f(v_i, u_i),$$

$$f(v_1 + v_2, u) = f(v_1, u) + f(v_2, u),$$

$$f(v, u_1 + u_2) = f(v, u_2) + f(v, u_2),$$

$$f(\alpha(v, u)) = f(\alpha v, u) = f(v, \alpha u),$$

здесь $v, v_1, v_2 \in V$, $u, u_1, u_2 \in U$ и $\alpha \in F$.

Пусть $f : V \times_s U \mapsto W$ и $g : V \times_s U \mapsto Z$ — сбалансированные отображения в пространства W и Z. Будем говорить, что отображение f *факторизуемо* с помощью пространства Z, если найдётся такое линейное отображение $h : Z \mapsto W$, что $f = hg$, т.е. $f(v, u) = h(g(v, u))$.

В пространстве $V \times_s U$ рассмотрим подпространство T, порождённое элементами

$$(v_1 + v_2, u) - (v_1, u) - (v_2, u),$$

$$(v, u_1 + u_2) - (v, u_1) - (v, u_2),$$

$$(\alpha v, u) - (v, \alpha u), \quad \alpha(v, u) - (\alpha v, u),$$

где $\alpha \in F$. Пусть $V \otimes U$ — фактор-пространство $V \times_s U$ по подпространству T. Обозначим через $v \otimes u$ образ элемента (v, u) в пространстве $V \otimes U$.

Легко показать, что отображение $f : V \times_s U \mapsto V \otimes U$ $(f(\sum(v_i, u_i)) = \sum v_i \otimes u_i)$ является сбалансированным и для любого $\alpha \in F$ выполняется

$$\alpha(v \otimes u) = \alpha v \otimes u = v \otimes \alpha u.$$

Каждый элемент пространства $V \otimes U$ имеет вид $\sum v_i \otimes u_i$, где $v_i \in V$, $u_i \in U$, а любое сбалансированное отображение из $V \times_s U$ в произвольное пространство Z факторизуемо с помощью $V \otimes U$.

Заметим, что для любого билинейного отображения t из $V \times U$ в произвольное пространство Z найдётся такое линейное отображение $g : V \otimes U \mapsto Z$, что $t(v, u) = g(f(v, u))$.

Пространство $V \otimes U$ называется *тензорным произведением* пространств V и U над полем F и обозначается как $V \otimes_F U$.

Теорема 2. *Справедливы следующие утверждения.*

1). Пространство $V \otimes_F F$ изоморфно V.

2). Пусть $V = V_1 \oplus V_2$, где V_1, V_2 — подпространства в V, и U — произвольное пространство. Тогда пространство $V \otimes_F U$ изоморфно пространству $V_1 \otimes_F U \oplus V_2 \otimes_F U$.

3). Пусть $v_1, \ldots, v_k$ — линейно независимые элементы пространства V. Тогда равенство $\sum_{i=1}^k v_i \otimes u_i = 0$ влечёт $u_i = 0$.

4). Пусть $v_1, \ldots, v_k$ — базис пространства V и $u_1, \ldots, u_n$ — базис пространства U. Тогда $v_i \otimes u_j$ — базис пространства $V \otimes U$.

5). *Отображение $\phi : V \otimes_F U \mapsto U \otimes_F V$, заданное правилом $\phi(v \otimes u) = u \otimes v$, является изоморфизмом пространств.*

6). *Отображение $\phi : (V \otimes_F U) \otimes_F W \mapsto V \otimes_F (U \otimes_F W)$, заданное правилом $\phi((v \otimes u) \otimes w) = v \otimes (u \otimes w)$, является изоморфизмом пространств.*

Упражнение. Доказать теорему 2.

§3 Модули

Пусть R — ассоциативное кольцо. Абелева группа M называется R-*модулем*, если определено отображение $M \times R \mapsto M$ (переводящее (m, r) в mr) такое, что
1). $m(a + b) = ma + mb$;
2). $(m_1 + m_2)a = m_1 a + m_2 a$;
3). $(ma)b = m(ab)$
для любых $m, m_1, m_2 \in M, a, b \in R$.

Если $1 \in R$ и $m1 = m$ для любого $m \in M$, то M называется *унитарным* (унитальным).

Примеры. 1). R — кольцо, $\rho \trianglelefteq_r R$. Тогда R действует справа на ρ, т.е. ρ — правый R-модуль.

2). Пусть $(R/\rho; +)$ — фактор-группа. Положим $(x + \rho)r = xr + \rho$.

3). $M = V$ — векторное пространство над полем F, $R = F$. При этом $v\alpha = 0 \Leftrightarrow v = 0$ или $\alpha = 0$. Над произвольным кольцом это не так.

Говорим, что M — точный R-модуль, если $Mr = 0 \Leftrightarrow r = 0$.

Определим $A(M) := \{x \in R : Mx = 0\}$.

Лемма 1. *$A(M) \trianglelefteq R$ и M — точный $(R/A(M))$-модуль.*

Доказательство. Положим $m(r + A(M)) = mr$. Корректность очевидна. Если $m(r + A(M)) = 0$ для любого $m \in M$, то $Mr = 0$. □

Для $a \in R$ положим: $T_a : M \mapsto M$, $mT_a = ma$. Тогда $T_a \in E(M)$, где $E(M)$ — кольцо всех аддитивных отображений на M. Рассмотрим отображение $T : R \mapsto E(M)$, $a \mapsto T_a$. Имеем $T(a + b) = T(a) + T(b)$, $T(ab) = T(a)T(b)$, т.е. $T \in \mathrm{Hom}\,(R, E(M))$, $\mathrm{Ker}\, T = A(M)$. Таким образом, нами доказана

Лемма 2. $R/A(M) \cong B \leq E(M)$.

Следовательно, если M — точный R-модуль, то мы можем рассматривать R как подкольцо в $E(M)$. Как расположено это подкольцо в $E(M)$?

Централизатором кольца R на M называется кольцо

$$C(M) = \{\psi \in E(M) : T_a\psi = \psi T_a \forall a \in R\}.$$

Таким образом, если $\psi \in C(M)$, то $(m\psi)a = (ma)\psi$ и $C(M)$ — гомоморфизмы в себя как R-модуля, т.е. $C(M)$ — кольцо всех модульных эндоморфизмов M.

R-модуль M называется *неприводимым*, если $MR \neq 0$ и единственными подмодулями в M являются 0 и M.

Централизатор на неприводимом модуле имеет особое строение.

Теорема 1 (*лемма Шура*). *M — неприводим $\Rightarrow C(M)$ — тело.*

Доказательство. Покажем, что для любого ненулевого $\theta \in C(M)$ существует $\theta^{-1} \in C(M)$. Достаточно найти $\theta^{-1} \in E(M)$. Действительно, если существует $\theta^{-1} \in E(M)$, то из $\theta T_a = T_a\theta$ следует $\theta^{-1}T_a = T_a\theta^{-1}$.

Пусть $\theta \in C(M), \theta \neq 0$. Если $M\theta = W$, то для любого $r \in R$ имеем

$$Wr = WT_r = (M\theta)T_r = (MT_r)\theta \subseteq M\theta = W.$$

Следовательно, W — подмодуль в M, а потому $M\theta = M$. Аналогично, $\operatorname{Ker}\theta = 0$. Следовательно, θ — изоморфизм и существует $\theta^{-1} \in E(M)$.$\square$

Примеры. 1). F — поле, $M_n(F)$ — алгебра матриц, F_n — пространство строк. Для $A \subseteq M_n(F)$ через $\bar{A} = alg\,\langle A\rangle$ обозначим подалгебру в $M_n(F)$, порождённую A. Тогда F_n — точный неприводимый модуль над $M_n(F)$, а потому F_n — точный модуль над $\bar{A}$, F_n — унитарный неприводимый модуль над $M_n(F)$.

Множество матриц A называется неприводимым, если F_n неприводим как $\bar{A}$-модуль. В матричных терминах это равносильно тому, что не существует такой $S \in M_n(F)$, что

$$S^{-1}aS = \begin{pmatrix} a_1 & 0 \\ * & a_2 \end{pmatrix}$$

для любой $a \in A$.

Централизатором множества A $(\bar{A})$ на F_n называется множество всех матриц из $M_n(F)$ перестановочных с каждой матрицей из A.

Центром кольца R называется множество $Z(R)$ элементов кольца R, перестановочных со всеми элементами кольца. Если F — алгебраически замкнутое поле, то единственным телом, содержащим F в своём центре и конечномерным над F, является F (это мы покажем позже), поэтому централизатор неприводимого множества матриц в этом случае состоит только из скалярных матриц, т.е. справедлива

Теорема (классическая лемма Шура). *Если F — алгебраически замкнутое поле, то централизатор неприводимого множества матриц состоит только из скалярных матриц.*

2). *Упражнение.* Пусть $F = \mathbb{R}$, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; $\{A\}$ — неприводимо, а его централизатор — тело, изоморфное $\mathbb{C}$.

3). *Упражнение.* $A = -e_{12} + e_{21} - e_{34} + e_{43}$, $B = -e_{13} + e_{31} + e_{24} - e_{42}$. $\{A, B\}$ — неприводимо, а его централизатор — тело, изоморфное телу кватернионов.

Лемма 3. *Если M — неприводимый R-модуль, то $M \cong R/\rho$ для некоторого максимального правого идеала $\rho \trianglelefteq^r_{max} R$. Далее, существует $a \in R$ такой, что $x - ax \in \rho$ для любого $x \in R$. Обратно, если $\rho \trianglelefteq^r_{max} R$ и существует $a \in R$ такой, что $x - ax \in \rho$ для любого $x \in R$, то R-модуль R/ρ неприводим.*

Доказательство. 1). $MR \neq 0$. 2). $S = \{m \in M : mR = 0\} \trianglelefteq M \Rightarrow S = 0$. Таким образом, если $m \in M$, $m \neq 0$, то $mR \neq 0$. Но $mR \trianglelefteq M$, а потому $mR = M$. Определим $\psi : R \mapsto M$ правилом $\psi(r) = mr$. Тогда $\psi \in \mathrm{Hom}\,(R, M)$, $\rho = \mathrm{Ker}\,\psi = \{x \in R : mx = 0\} \trianglelefteq_r R$. Следовательно, по теореме о гомоморфизмах $M \cong R/\rho$.

Если $I \trianglelefteq_r R$ и $\rho \subseteq I$, то $\psi(I) \trianglelefteq M \Rightarrow \rho \trianglelefteq^{max}_r R$. Далее, $mR = M$, а значит существует $a \in R$ такой, что $ma = m$. Следовательно, для любого $x \in R$ имеем $max = mx$, $m(x - ax) = 0 \Rightarrow x - ax \in \rho$. $\square$

Упражнение. Доказать обратное утверждение.

§4 Радикал Джекобсона

Радикалом Джекобсона кольца называется совокупность элементов из R, которые аннулируют все неприводимые R-модули и само кольцо, если неприводимых модулей не существует. Обозначение: $J(R)$ — радикал Джекобсона.

Пусть $\mathfrak{M}$ — множество всех неприводимых правых R-модулей. По определению, $J(R) = \bigcap\limits_{M \in \mathfrak{M}} A(M)$. Так как $A(M) \trianglelefteq R$, то $J(R) \trianglelefteq R$.

Из леммы 3 §3 следует определение: правый идеал ρ в R называется *регулярным*, если существует $a \in R$ такой, что $x - ax \in \rho$ для любого $x \in R$. Обозначение: $\rho \trianglelefteq_{reg} R$ или $\rho \trianglelefteq^{reg} R$.

Если в кольце есть (левая) единица, то любой правый идеал кольца будет регулярным.

Пусть $\rho \trianglelefteq^r R$. Положим

$$(\rho : R) := \{x \in R : Rx \subseteq \rho\}.$$

Теорема 1. *$J(R) = \bigcap\limits_{\rho \trianglelefteq^{r,reg}_{max} R} (\rho : R)$, а $(\rho : R)$ — наибольший идеал кольца R, лежащий в ρ.*

Доказательство. Имеем $J(R) = \bigcap\limits_{M \cong R/\rho, \rho \trianglelefteq^{max}_{r,reg} R} A(M)$. Далее,

$$x \in A(M) \iff Mx = 0 \iff (x + \rho)x = \rho \ \forall r \in R$$

$$\iff Rx \subseteq \rho \iff x \in (\rho : R).$$

Следовательно, $(\rho : R) = A(M)$.

Если $x \in (\rho : R)$, $x - ax \in \rho \Rightarrow ax \in \rho \Rightarrow x \in \rho$. Если $(\rho : R) \subseteq S \subseteq \rho, S \trianglelefteq R$, то $S \subseteq (\rho : R)$. Значит, $(\rho : R)$ — наибольший двусторонний идеал кольца R, лежащий в ρ. $\square$

Лемма 1. *Если $\rho \trianglelefteq^{reg}_r R$, то ρ содержится в некотором максимальном правом идеале, который также регулярен.*

Доказательство. Пусть $a \in R$ такой, что $x - ax \in \rho$ для любого $x \in R$. Пусть $\mathcal{M}$ — множество всех собственных правых идеалов из R, содержащих ρ. Если $\rho' \in \mathcal{M}$, то $a \notin \rho'$, иначе $ax \in \rho'$, $x - ax \in \rho \subseteq \rho' \Rightarrow \rho' = R$. В частности, $a \notin \rho$. Следовательно, к $\mathcal{M}$ можно применить лемму Цорна. Пусть ρ_0 — максимальный элемент из $\mathcal{M}$, тогда он и является искомым. $\square$

Теорема 2. $J(R) = \bigcap\limits_{\rho \trianglelefteq^{r,reg}_{max} R} \rho.$

Доказательство. По теореме 1, $J(R) = \bigcap\limits_{\rho \trianglelefteq^{r,reg}_{max} R} (\rho : R)$, а так как $(\rho : R) \subseteq \rho$, то $J(R) \subseteq \bigcap\limits_{\rho \trianglelefteq^{r,reg}_{max} R} \rho$. С другой стороны, пусть $\bigcap\limits_{\rho \trianglelefteq^{r,reg}_{max} R} \rho = \tau$ и $x \in \tau$. Покажем, что $I = \{xy + y : y \in R\} = R$. Действительно, если это не так, то $I \trianglelefteq^{r,reg} R$ $(a = -x) \Rightarrow I \subseteq \rho_0$, где $\rho_0 \trianglelefteq^{r,reg}_{max} R$. Так как $x \in \bigcap\limits_{\rho \trianglelefteq^{r,reg}_{max} R} \rho \Rightarrow x \in \rho_0 \Rightarrow xy \in \rho_0 \Rightarrow y \in \rho_0$ для любого $y \in R$.

Следовательно, существует $w \in R$ такой, что $xw + w = -x$, т.е. $x + w + xw = 0$. Если $\tau \not\subseteq J(R)$, то существует неприводимый R-модуль M такой, что $M\tau \neq 0$. Значит, $m\tau \neq 0$ для некоторого $m \in M$. Так как $m\tau \trianglelefteq M$, то $m\tau = M$. Следовательно, существует $t \in \tau$ такой, что $mt = -m$. По доказанному, существует $s \in R$ такой, что $t + s + ts = 0$. Имеем $0 = m(s+t+st) = ms+mt+mts = -m$. Получили противоречие. $\square$

При доказательстве мы обнаружили, что для любого $x \in J(R)$ существует $y \in R$ такой, что $x + y + xy = 0$.

Элемент $a \in R$ называется *право-квазирегулярным элементом*, если существует $b \in R$ такой, что $a + b + ab = 0$. Элемент b называется *правым-квазиобратным* для a. Идеал I (левый, правый, двусторонний) называется *право-квазирегулярным*, если все его элементы право-квазирегулярны (обозначение: $I \trianglelefteq_{qr} R$.).

Упражнение. Если $1 \in R$, то a — право-квазирегулярный элемент $\Leftrightarrow$ $1 + a$ обратим справа в R.

В ходе доказательства теоремы 2 мы установили, что

1). $J(R)$ — правый квазирегулярный идеал в R;

2). если ρ — правый квазирегулярный идеал в R, то $\rho \subseteq J(R)$.

Таким образом, нами доказана

Теорема 3. *$J(R)$ — единственный максимальный право-квазирегулярный идеал в R.*

Упражнение. Показать, что если a имеет и левый и правый квазиобратный, то они совпадают. Доказать, что $J(R) \trianglelefteq^{l}_{qr} R$.

Аналогично определяется лево-квазирегулярный идеал и показывается, что $J(R)$ — лево-квазирегулярный идеал. Таким образом, нет различий между левым и правым радикалом.

Элемент $a \in R$ называется *ниль-элементом* (*нильпотентным*), если $a^n = 0$ для некоторого $n \in \mathbb{N}_0$ (здесь и далее $\mathbb{N}_0$ обозначает множество натуральных чисел с нулём); идеал (левый, правый, двусторонний) называется *ниль-идеалом*, если каждый его элемент является нильпотентным.

Если I, J — идеалы в R (левый, правый, двусторонний), то через IJ обозначается абелева подгруппа в R, порождённая элементами ab, где $a \in I, b \in J$. Тогда IJ — идеал в R (левый, правый, двусторонний). Идеал I (левый, правый, двусторонний) называется *нильпотентным*, если $I^m = 0$ для некоторого $m \in \mathbb{N}_0$. Заметим, что нильпотентный идеал (левый, правый, двусторонний) является ниль-идеалом, но обратное не верно в общем случае.

Лемма 2. *Каждый правый ниль-идеал лежит в* $J(R)$.

Доказательство. Пусть $a^m = 0$, положим $b = -a + a^2 - a^3 + \ldots + (-1)^{m-1}a^{m-1}$. Тогда $a + b + ab = 0$. $\square$

Теорема 4. $J(R/J(R)) = 0$.

Доказательство. Пусть $\bar{R} = R/J(R)$. Если $\bar{\rho}$ — максимальный правый идеал в $\bar{R}$, то $\bar{\rho} = \rho + J(R)$ для некоторого максимального регулярного правого идеала ρ из R. Таким образом,

$$\bigcap_{\bar{\rho} \trianglelefteq^{r,reg}_{max} \bar{R}} \bar{\rho} = \bigcap_{\rho \trianglelefteq^{r,reg}_{max} R} \rho + J(R) = \bar{0},$$

что и доказывает теорему. $\square$

Кольцо R называется *полупростым*, если $J(R) = 0$, и *радикальным*, если $J(R) = R$.

Лемма 3. *Идеалы полупростого кольца полупросты.*

Доказательство. Пусть $A \trianglelefteq R$, но $J(A) \neq 0$. Тогда $J(A)R \trianglelefteq^r R$ и $I_1 = J(A)R \neq 0$, так как иначе $J(A) \trianglelefteq^r R$ и $J(A)$ нильпотентен. Также $I_1^2 \neq 0$, но $I_1^2 = J(A)RJ(A)R \subseteq J(A)A \subseteq J(A)$. Следовательно, для любого $x \in I_1^2$ существует правый квазиобратный и $I_1^2 \trianglelefteq^r R$, что противоречиво. $\square$

Теорема 5. $A \trianglelefteq R \Rightarrow J(A) = J(R) \cap A$.

Доказательство. Пусть $J = J(R)$. Если $a \in J \cap A$, то a право-квазирегулярен. Если b — квазиобратный к a, то $b = a - ab \in A$, так как $A \trianglelefteq R$. Следовательно, $J \cap A \trianglelefteq^{qr}_r A$, а потому $J \cap A \subseteq J(A)$.

Рассмотрим эпиморфизм $\phi : R \mapsto \bar{R} := R/J$. Тогда $\phi(A) = A/J$. Кольцо $\bar{R}$ полупросто, т.е. идеал A/J полупрост. Далее, $A/J = (A+J)/J \cong A/(A\cap J)$, т.е. $A/(A\cap J)$ полупросто. Рассмотрим эпиморфизм $A \mapsto A/(J\cap A)$. Образ квазирегулярного идеала — квазирегулярный идеал, но $A/(J\cap A)$ полупросто, т.е. $J(A) \subseteq J\cap A$. $\square$

Утверждение становится неверным, если A — односторонний идеал.

Упражнение. Пусть $R = M_2(F)$. Показать, что в R нет собственных идеалов, откуда $J(R) = 0$. Далее, показать, что

$$\rho = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \right\} \trianglelefteq_r M_2(F),\ \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \in J(\rho),$$

т.е. $J(\rho) \neq 0 = \rho \cap J(R)$.

Далее в этом параграфе обозначаем через R_n кольцо матриц с элементами из кольца R.

Упражнение. Пусть M — неприводимый R-модуль, тогда $M^{(n)} = \{(m_1,\ldots,m_n) : m_i \in M\}$ — неприводимый R_n-модуль.

Теорема 6. $J(R_n) = J(R)_n$.

Доказательство. Пусть M — неприводимый R-модуль. Тогда для любого $(m_1,\ldots,m_n) \in M^{(n)}$ и для любой $(a_{ij}) \in J(R_n)$ имеем

$$(m_1,\ldots,m_n)(a_{ij}) = 0 \Rightarrow Ma_{ij} = 0 \Rightarrow a_{ij} \in J(R),$$

т.е. $J(R_n) \subseteq J(R)_n$.

Покажем, что $J(R)_n$ — квазирегулярный идеал в R_n. Пусть $\rho_i = \{\alpha_{i1}e_{i1} + \ldots + \alpha_{in}e_{in} : \alpha_{ij} \in J(R)\}$. Если $x = \alpha_{11}e_{11} + \ldots + \alpha_{1n}e_{1n}$ и $y = \alpha'_{11}e_{11}$, где $\alpha_{11} + \alpha'_{11} + \alpha_{11}\alpha'_{11} = 0$, то $w = x + y + xy$ — треугольная матрица с нулевой диагональю. Следовательно, $w^n = 0$, а потому w квазирегулярен. Пусть $w + z + wz = 0$. Тогда

$$0 = x + y + z + xy + xz + yz + xyz = x + (y + z + yz) + x(y + z + yz).$$

Следовательно, x квазирегулярен и ρ_1 — правый квазирегулярный идеал в R_n, т.е. $\rho_1 \subseteq J(R_n)$. Аналогично, $\rho_i \subseteq J(R_n)$. Так как $J(R)_n = \rho_1 + \ldots + \rho_n$ и идеал $J(R_n)$ замкнут относительно сложения, то $J(R)_n \subseteq J(R_n)$. $\square$

§5 Артиновы кольца

Кольцо называется *артиновым* (справа), если любое непустое множество его правых идеалов имеет минимальный элемент.

Утверждение 1. *Кольцо R артиново $\iff$ любая убывающая цепь правых идеалов $\rho_1 \supseteq \rho_2 \supseteq \ldots \supseteq \rho_n \ldots$ обрывается.*

Доказательство. очевидно. □

Примеры. 1). Тело.

2). $M_n(T)$, где T — тело.

3). *Упражнение.* Если кольцо R артиново, то и $M_n(R)$ артиново.

4). $R_1 \oplus \ldots \oplus R_k$ артиново, если все R_i артиновы.

5). Если A — конечномерная алгебра над полем, то A артинова как алгебра. Как кольцо это может быть не артиново кольцо. Пример: $\mathbb{R}u, u^2 = 0$.

Теорема 1. *Если кольцо R артиново, то $J(R)$ — нильпотентный идеал.*

Доказательство. Пусть $J = J(R)$. Рассмотрим $J \supseteq J^2 \supseteq \ldots \supseteq J^n \ldots$. Существует такое $n \in \mathbb{N}$, что $J^n = \ldots = J^{2n}$. Рассмотрим $W = \{x \in R : xJ^n = 0\} \trianglelefteq R$. Если $W \supseteq J^n$, то $J^{2n} = 0$. Пусть $W \not\supseteq J^n$. Рассмотрим $\bar{R} = R/W$; при гомоморфизме $\phi : R \mapsto \bar{R}$ имеем

$$\phi(J^n) = \bar{J}^n \neq 0, \; \bar{J}^n \trianglelefteq \bar{R}, \; \bar{J}^n \subseteq J(\bar{R}).$$

Так как $\bar{R}$ артиново, то существует минимальный $\bar{\rho} \trianglelefteq_r \bar{R}$ такой, что $\bar{\rho} \subseteq \bar{J}^n$. Рассматривая $\bar{\rho}$ как модуль над $\bar{R}$, замечаем, что либо $\bar{\rho}$ неприводим, либо $\bar{\rho}\bar{R} = 0$. В обоих случаях $\bar{\rho}\bar{J}^n = 0$. Переходя к прообразам в R, имеем

$$\rho J^n \subseteq W, \rho J^n J^n = \rho J^{2n} = 0 \Rightarrow \rho J^n = 0 \Rightarrow \rho \subseteq W \Rightarrow \bar{\rho} = 0.$$

Полученное противоречие доказывает теорему. □

Следствие (*Гопкинс*). *Если кольцо R артиново, то любой его ниль-идеал нильпотентен.*

Пусть R — кольцо, $\rho \neq 0$ — нильпотентный правый идеал в R. Если $R\rho \neq 0$ и $\rho^m = 0$, то $R\rho \trianglelefteq R$ и $(R\rho)^m = \underbrace{R\rho \ldots R\rho}_{n}$. Следовательно, в R существует двусторонний нильпотентный идеал.

Гипотеза (*Кёте*). Если $I \trianglelefteq_r R$, I — ниль, то в R существует двусторонний ниль-идеал.

Ненулевой элемент $e \in R$ называется *идемпотентом*, если $e^2 = e$.

Лемма 1. *Пусть R — кольцо без нильпотентных идеалов, $\rho \trianglelefteq_r^{min} R$. Тогда $\rho = eR$.*

Доказательство. Так как $\rho^2 \neq 0$, то существует $x \in \rho$ такой, что $x\rho \neq 0$. Поскольку $x\rho \trianglelefteq_r R$ и $x\rho \subseteq \rho$, то $x\rho = \rho$, т.е. $x = xe$. Следовательно, $xe^2 = xe$, $x(e-e^2) = 0$. Пусть $\rho_0 = \{a \in \rho : xa = 0\}$. Тогда $\rho_0 \trianglelefteq_r R$, $\rho_0 \subseteq \rho$, $\rho_0 \neq \rho$. Значит, $\rho_0 = 0$ и $e = e^2$. Далее, имеем $eR \subseteq \rho$, $eR \neq 0$, а потому $eR = \rho$. □

Лемма 2. *Пусть R — кольцо, $a^2 - a$ — нильпотентный элемент из R. Тогда либо a — нильпотентный элемент из R, либо существует $p(x) \in \mathbb{Z}[x]$ такой, что $e = ap(a)$ — идемпотент.*

Доказательство. Пусть $(a^2-a)^k = 0$. Тогда $a^k = a^{k+1}p(a)$, откуда $a^k = a^k ap(a) = a^k[ap(a)]^2$. Следовательно, $a^k = a^k[ap(a)]^k = a^{2k}p(a)^k$. Если $a^k \neq 0$, то $e = a^k p(a)^k \neq 0$ и $e^2 = [a^{2k}p(a)^k]p(a)^k = a^k p(a)^k = e$. □

Теорема 2. *Пусть R — артиново кольцо, ρ — ненулевой ненильпотентный правый идеал в R. Тогда ρ содержит ненулевой идемпотент.*

Доказательство. Так как ρ — ненулевой ненильпотентный правый идеал в R, то по теореме 1 получаем $\rho \not\subseteq J(R)$. Пусть $\phi : R \mapsto \bar{R} = R/J(R)$. Так как $\bar{R}$ полупросто, то в $\bar{R}$ нет нильпотентных идеалов. Пусть $\bar{\rho}$ — образ ρ в $\bar{R}$. Так как $\bar{\rho} \neq 0$, то в $\bar{\rho}$ существует минимальный правый идеал $\bar{\rho}_0$ из $\bar{R}$. По лемме 1, $\bar{\rho}_0 = \bar{e}\bar{R}$, где $\bar{e}$ — идемпотент из $\bar{\rho}_0$. Пусть $\phi(a) = \bar{e}$. Тогда $\phi(a^2 - a) = \bar{0}$, откуда $a^2 - a \in J(R)$ и $a^2 - a$ — нильпотентный элемент. Так как $\phi(a^k) = \bar{e}^k = \bar{e} \neq 0$ для любого $k \in \mathbb{N}$, то a — ненильпотентный элемент. Следовательно, по лемме 2, ρ содержит ненулевой идемпотент. □

§6 Полупростые артиновы кольца

Пусть F — поле, G — конечная группа. Групповой алгеброй $F(G)$ группы G над F называется совокупность элементов вида $\sum \alpha_i g_i$ с естественными операциями сложения и умножения.

Теорема 1 (*Машке*). *Пусть G — конечная группа, а F — поле характеристики 0 или характеристики $p > 0$, которая не делит порядок группы G. Тогда $F(G)$ — полупростая алгебра.*

Доказательство. Определим отображение $T_a : F(G) \mapsto F(G)$ правилом $xT_a = xa$. Тогда $\psi : a \mapsto T_a$ — изоморфное вложение $F(G)$

в алгебру $\mathrm{End}_F F(G)$. Элементы из G рассмотрим как базис $F(G)$. Если g — неединичный элемент из G, то $\mathrm{tr}\, T_g = 0, \mathrm{tr}\, T_1 = |G|$.

Пусть $J = J(F(G))$. Так как $F(G)$ конечномерна над F, то она артинова как алгебра и её радикал нильпотентен. Пусть $x = \sum \alpha_i g_i$ — ненулевой элемент из J. Так как $J \trianglelefteq F(G)$, то можно считать, что $g_1 = 1$ и $\alpha_1 \neq 0$. Поскольку x нильпотентен, то T_x — нильпотентное линейное преобразование и $\mathrm{tr}\, T_x = 0$, но

$$\mathrm{tr}\, T_x = \alpha_1 \mathrm{tr}\, T_1 + \ldots + \alpha_n \mathrm{tr}\, T_{g_n} = \alpha_1 \mathrm{tr}\, T_1 = \alpha_1 |G|.$$

Полученное противоречие завершает доказательство теоремы. $\square$

Пример. Если характеристика p поля делит порядок группы G, то $F(G)$ не является полупростой. Действительно, рассмотрим $a = \sum_{g \in G} g$, $a \neq 0$. Тогда $xa = ax = a$ для любого $x \in G$. Следовательно, $a \in Z(F(G))$. Далее, $a^2 = a \sum_{g \in G} g = |G|a = 0$, $I = F(G)a \trianglelefteq F(G)$ и $I^2 = 0$, т.е. $F(G)$ не является полупростой.

Теорема 2. *Пусть R — полупростое артиново кольцо, ρ — ненулевой правый идеал в R. Тогда $\rho = eR$ для некоторого идемпотента $e \in \rho$.*

Доказательство. Так как ρ не является нильпотентным, то в ρ существует идемпотент. Для любого идемпотента $e \in \rho$ рассмотрим $A(e) = \{x \in \rho : ex = 0\} \trianglelefteq_r R$. Множество таких идеалов непусто. Следовательно, оно имеет минимальный элемент $A(e_0)$.

Если $A(e_0) = 0$, то из того, что $e_0(x - e_0 x) = 0$ для любого $x \in \rho$, следует $x = e_0 x$. Тогда $\rho = e_0 \rho \subseteq e_0 R \subseteq \rho$, а потому $\rho = e_0 R$.

Предположим, что $A(e_0) \neq 0$. Существует идемпотент $e_1 \in A(e_0)$ такой, что $e_1 \in \rho$ и $e_0 e_1 = 0$. Элемент $e = e_0 + e_1 - e_1 e_0$ является идемпотентом в ρ. Так как $ee_1 = e_1 \neq 0$, то $e \neq 0$. Если $ex = 0$ для некоторого $x \in \rho$, то

$$e_0 ex = 0,\ e_0 e = e_0 \Rightarrow e_0 x = 0 \Rightarrow x \in A(e_0) \Rightarrow A(e) \subseteq A(e_0).$$

Так как $e_1 \in A(e_0)$ и $e_1 \notin A(e)$, то $A(e) \subset A(e_0)$, что противоречит минимальности $A(e_0)$. $\square$

Следствие 1. *Пусть R — полупростое артиново кольцо, A — ненулевой идеал в R. Тогда $A = eR = Re$, где e — идемпотент из центра кольца R.*

Доказательство. Так как $A \trianglelefteq_r R$, то $A = eR$. Рассмотрим $B = \{x - xe : x \in A\} \trianglelefteq_l R$. Так как $Be = 0, eA = A$, то $B^2 \subseteq BA = BeA =$

$0 \Rightarrow B = 0 \Rightarrow x = xe$ для любого $x \in A$, и e — двусторонняя единица в A. Далее, $A = Ae \subseteq Re \subseteq A \Rightarrow A = Re$. Если $x \in R$, то $ex \in A$, $xe \in A$, и так как e — правая единица в A, то $ex = exe$, а поскольку e — левая единица в A, то $xe = exe$. Следовательно, $ex = xe$. $\square$

Следствие 2. *Полупростое артиново кольцо имеет единицу.*

Кольцо R называется *кольцом без кручения* (кольцом характеристики 0), если из равенства $nx = 0$ для некоторого $n \in \mathbb{N}$ и $x \in R$ следует $x = 0$.

Справедлива следующая теорема, доказательство которой мы опустим.

Теорема. *Артиново справа кольцо без кручения имеет правую единицу.*

Лемма 1. *Любой идеал полупростого артинова кольца — полупростое артиново кольцо.*

Доказательство. Пусть $A \trianglelefteq R$. Тогда $A = eR = Re$ для некоторого идемпотента $e \in R$. Пусть 1 — единица кольца R. Если $x \in R$, то $x = xe + x(1-e)$ и $R = Re + R(1-e)$ — пирсовское разложение кольца относительно e. Так как $1 - e \in Z(R)$, то $R(1-e) \trianglelefteq R$. Кроме того $Re \cap R(1-e) = 0$, так как если $x \in Re \cap R(1-e)$, то $xe = x$ и $xe = 0$. Следовательно, $R = Re \oplus R(1-e)$ и $A = Re \cong R/R(1-e)$, а потому A — артиново кольцо и, по лемме 3 §4, A — полупростое кольцо. $\square$

Кольцо R называется *простым*, если единственные идеалы в R — это 0 и R.

Теорема 3 (*Веддербарн*). *Полупростое артиново кольцо есть прямая сумма конечного числа простых артиновых колец.*

Доказательство. Пусть $A_0 \trianglelefteq_{min} R$. Тогда A_0 — простое кольцо. Действительно, $A_0^2 \neq 0$ и если $B \trianglelefteq A_0$, то $A_0BA_0 \subseteq B$ и $A_0BA_0 \trianglelefteq R$, а так как $1 \in A_0$, то $A_0BA_0 \neq 0$. Поскольку $A_0 \supseteq B \supseteq A_0BA_0$ и $A_0 \trianglelefteq_{min} R$, то $A_0 = B$.

Из леммы 1 следует, что $R = A_0 \oplus T_0$, где T_0 — полупростое артиново кольцо. Выбирая в T_0 минимальный идеал A_1, получаем $T_0 = A_1 \oplus T_1$. Далее, для некоторого $k \in \mathbb{N}$ имеем $R = A_0 \oplus \ldots \oplus A_k$. В противном случае $R_0 = A_0 \oplus A_1 \oplus \ldots,\ R_1 = A_1 \oplus A_2 \oplus \ldots, R_m = A_m \oplus A_{m+1} \oplus \ldots,\ \ldots$ — бесконечная строго убывающая цепь идеалов. $\square$

Упражнение. Пусть R — кольцо полиномов $\{\sum \alpha_{ij}x^iy^j,\ \alpha_{ij} \in F,\ xy - yx = 1\}$ над полем F характеристики ноль. Показать, что R — простая ассоциативная алгебра без делителей нуля, которая не является телом.

Лемма 2. *Пусть R — полупростое артиново кольцо, $R = A_1 \oplus \ldots \oplus A_k$, где $A_1, \ldots, A_k$ — простые кольца. Тогда $\{A_1, \ldots, A_k\}$ — это множество всех минимальных идеалов кольца R.*

Доказательство. Пусть B — ненулевой минимальный идеал в R. Так как $1 \in R$, то $RB \neq 0$, но $RB = A_1B \oplus \ldots \oplus A_kB$. Следовательно, $A_iB \neq 0$ для некоторого i. Тогда $A_iB \trianglelefteq R, A_iB \subseteq B, A_iB \subseteq A_i$. В итоге, $A_i = B$. $\square$

Кольцо называется *нётеровым справа*, если любое непустое множество его правых идеалов содержит максимальный элемент.

Примеры. 1). Кольцо $\mathbb{Z}$ является нётеровым, так как любой идеал в $\mathbb{Z}$ главный.

2). Приведём пример кольца, которое является нётеровым справа, но не слева. Рассмотрим кольцо R, образованное матрицами вида $\begin{pmatrix} n & a \\ 0 & b \end{pmatrix}$, где $n \in \mathbb{Z},\ a, b \in \mathbb{Q}$, с обычными операциями.

Упражнение. Показать, что R нётерово справа, но не слева (при этом рассмотреть левые идеалы вида $\begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}$, где M — подмодуль $\mathbb{Z}$-модуля $\mathbb{Q}$, и заметить, что $\mathbb{Q}$ не является конечнопорождённым $\mathbb{Z}$-модулем).

Теорема (*Левицкий*). *Пусть A — односторонний ниль-идеал в нётеровом справа кольце. Тогда A нильпотентен.*

§7 Простое радикальное кольцо

Влечёт ли простота кольца R его полупростоту? Если $1 \in R$, то ответ положителен, если R артиново, то ответ также положителен. Однако польский математик Е. Сансяда доказал, что существует простое радикальное кольцо (*Sansiada E., Cohn P.M.*, J. of Alg., 1967).

Лемма 1 (*Андрунакиевич*). *Пусть $\rho \trianglelefteq_{min} R,\ \rho^2 \neq 0$. Тогда ρ — простое кольцо.*

Доказательство. Из минимальности получаем $\rho^2 = \rho$. Далее $Ann_r\, \rho \trianglelefteq R, \rho \not\subseteq Ann_r\, \rho$, т.е. $Ann_r\, \rho \cap \rho = 0 \Rightarrow \rho x \neq 0$ для любого ненулевого $x \in \rho$. Аналогично, $x\rho \neq 0$. Если $0 \neq x \in \rho$, то $\rho x \rho \neq 0 \Rightarrow \rho x \rho = \rho$ для любого ненулевого $x \in \rho$. $\square$

Пусть $R = F[[x, y]]$ — алгебра формальных рядов со свободными членами от двух некоммутирующих переменных x, y над полем F.

Обозначим через $R^0 := F^0[[x,y]]$ подалгебру в R, состоящую из рядов без свободных членов, $R^1 := F^1[[x,y]]$ — множество рядов со свободными членами 1. Рассмотрим в R идеал S, порождённый элементом $u = x - yx^2y$.

Теорема 1. (*Сансяда*) $x \notin S$.

Построим, исходя из этой леммы, пример Сансяды. Рассмотрим множество всех идеалов кольца R^0, содержащих u, но не содержащих x. По лемме Цорна существует максимальный идеал S_0 с этим свойством. Пусть $Q = R^0/S^0$. В Q любой ненулевой идеал содержит ненулевой элемент $\bar{x} = x + S_0$. Следовательно, *сердцевина* $H = H(Q)$ (пересечение всех ненулевых идеалов) не равна нулю и $H = \langle \bar{x} \rangle$. Далее, $H^2 \neq 0$, так как $\bar{x} = (\bar{y}\bar{x})(\bar{x}\bar{y})$. Тогда по лемме 1 H является простым. Так как R^0 радикально, то

$$(1-f)^{-1} = 1 + f + f^2 + \dots,\ f \in R^0$$

и H является гомоморфным образом идеала из R^0, то H радикально.

Доказательство *теоремы Сансяды* основывается на нижеследующих леммах. Все леммы далее относятся к R.

Лемма 1. *Пусть $c = \sum_{i=1}^{n} a_i u b_i$, где b_1 — обратимый элемент из R. Тогда*

$$c = a_1' u b_1' + \sum_{i=2}^{n} a_i u b_i',\ b_1' \in R^1,\ b_i' \in R^0.$$

Доказательство. Пусть $b_1 = \beta b_1'$, где $0 \neq \beta \in F, b_1' \in R^1$. Пусть β_i — свободные члены элементов $b_i,\ 2 \le i \le n$. Тогда

$$c = (\beta a_1 + \sum_{i=2}^{n} \beta_i a_i) u b_1' + \sum_{i=2}^{n} a_i u (b_i - \beta_i b_1') = a_1' u b_1' + \sum_{i=2}^{n} a_i u b_i'. \qquad \square$$

Лемма 2. *Пусть $cx + dy = \sum_{i=1}^{n} a_i u b_i$, где b_1 — обратимый элемент из R. Тогда*

$$cx + dy = cu(1 + b_1^*) + \sum_{i=2}^{n} a_i u b_i^*, \tag{$*$}$$

где $b_1^* \in R^0$.

Доказательство. По лемме 1 можно считать, что $b_1 \in R^1, b_i \in R^0, i \ge 2$. Тогда $b_1 = 1 + b_1' x + b_1'' y, b_i = b_i' x + b_i'' y,\ i > 1$. Приравняем в

$(*)$ элементы, оканчивающиеся на x (вспомним, что $u = x - yx^2y$):

$$c = a_1 + a_1ub_1' + \sum_{i=2}^{n} a_iub_i'.$$

Умножив справа на $(1 + ub_1')^{-1} = 1 + uq$, получим

$$c(1 + uq) = a_1 + \sum_{i=2}^{n} a_iud_i.$$

Подставляя a_1 из этого равенства в $(*)$, приходим к требуемому равенству

$$cx + dy = c(1 + uq)ub_1 + \sum_{i=2}^{n} a_iub_i^* = cu(1 + b_1^*) + \sum_{i=2}^{n} a_iub_i^*. \qquad \square$$

Следствие 1. *Пусть* $dy = \sum_{i=1}^{n} a_iub_i$ *и* n *— минимальное из возможных для данного элемента* dy. *Тогда все* $b_i \in R^0$.

Доказательство. Если, например, $b_1 \notin R^0$, то по лемме 2 при $c = 0$ элемент dy обладает более коротким представлением. $\square$

Лемма 3. *Идеал* $\langle u \rangle$ *в* R, *порождённый элементом* u, *не содержит одночленов.*

Доказательство. Предположим противное. Пусть

$$c = \sum_{i=1}^{n} a_iub_i \in \langle u \rangle, \tag{1}$$

— одночлен от x, y. Выберем одно из равенств (1) (одночлен c не фиксирован) с минимально возможным n, а среди них — равенство, для которого минимальна степень c. Если $c = c_1y$, то по следствию 1 $b_i \in R^0$, т.е. $c_1 = \sum_{i=1}^{n} a_iub_i'$, что противоречит минимальности степени c. Следовательно, $c = c_1x$ и

$$c_1x = \sum_{i=1}^{n} a_iub_i \in \langle u \rangle, \tag{2}$$

где не все $b_i \in R^0$. Это равенство будет основанием для следующей индукции: для любого r существуют одночлены $p_1, \ldots, p_r$ степени больше нуля такие, что

$$c_1p_1\dots p_rx=\sum_{i=1}^{r}c_1p_1\dots p_{i-1}ud_i+\sum_{j=r+1}^{n}a_jud_j, \qquad (3)$$

где $d_i\notin R^0$ для некоторого $i,\ 1\le i\le n$.

При $r=0$ (3) превращается в (2). Пусть $r<n$ и имеет место (3). Докажем аналогичное равенство для $r+1$. Рассмотрим два случая.

1). Пусть $d_j\in R^0$ при $j\ge r+1$. Тогда существует $k\le r$ такое, что $d_k\notin R^0$. Пусть $d_i=\lambda_i+d'_ix+d''_iy,\ \lambda_i\in F,\ 1\le i\le n$. Приравняем в (3) элементы, оканчивающиеся на x:

$$c_1p_1\dots p_r=\sum_{i=1}^{r}c_1p_1\dots p_{i-1}\lambda_i+\sum_{i=1}^{r}c_1p_1\dots p_{i-1}ud'_i+\sum_{j=r+1}^{n}a_jud'_j.$$

Пусть $s=min_{i\le r}\{i:\lambda_i\ne 0\}$. Тогда

$$c_1p_1\dots p_{s-1}(1+f)\lambda_s=\sum_{i=1}^{r}c_1p_1\dots p_{i-1}ud'_i+\sum_{j=r+1}^{n}a_jud'_j,$$

где $f\in R^0$. Перенося теперь s-ый член первой суммы правой части в левую часть и умножая обе части получившегося равенства на $((1+f)\lambda_s-ud'_s)^{-1}$, получим представление типа (1) с меньшим числом n.

Замечание. Эти рассуждения показывают, что при $r=n$ равенство (3) невозможно.

2). Пусть, например, $d_{r+1}\notin R^0$. Применим к (3) лемму (2) (при $d=0$):

$$c_1p_1\dots p_rx=\sum_{i=1}^{r}c_1p_1\dots p_{i-1}ud^*_i+c_1p_1\dots p_ru(1+d^*_{r+1})+\sum_{j=r+2}^{n}a_jud^*_j,$$

где $d^*_{r+1}\in R^0$. Из этого равенства имеем

$$c_1p_1\dots p_ryx^2y=\sum_{i=1}^{r}c_1p_1\dots p_{i-1}ud^*_i+c_1p_1\dots p_rud^*_{r+1}+\sum_{j=r+2}^{n}a_jud^*_j,\ (4).$$

В силу следствия 1 все элементы d^*_i лежат в R^0, поэтому (4) можно сократить справа на y. Если в полученном равенстве не все элементы

"d_i^*" лежат в R^0, то индуктивный переход завершён ($p_{r+1} = yx$). Если же "d_i^*" лежит в R^0, то (4) можно сократить на xy, не меняя вида этого равенства. Если теперь все "d_i^*" лежат в R^0, то снова сокращая на x, мы оказываемся в условиях следствия 1, откуда следует возможность сокращения на y. Таким образом, (4) можно сократить на yx^2y, не меняя его вида, но тогда перенося $c_1p_1 \dots p_r ud_{r+1}^*$ влево и домножая полученное на $(1 - ud_{r+1}^*)^{-1}$, получим для $c_1p_1 \dots p_r$ более короткое представление. Противоречие показывает, что после сокращения (4) справа на xy не все полученные элементы лежат в R^0, т.е. в качестве p_{r+1} можно взять y.□

§8 Примитивные кольца. Теорема плотности

Кольцо R называется *примитивным*, если оно обладает точным неприводимым модулем. Стоит говорить о примитивности справа, так как Бергман построил пример кольца примитивного справа, но не слева.

Если M — неприводимый R-модуль, то кольцо $R/A(M)$ примитивно. Если $\rho \trianglelefteq_{max}^{r,reg} R$ и $M = R/\rho$, то $A(M) = (\rho : R)$ и $R/(\rho : R)$ примитивно. Если R содержит максимальный регулярный правый идеал ρ, в котором нет двусторонних идеалов из R, то R примитивно. Верно и обратное.

Кольцо R примитивно, значит R полупросто. Действительно, $J(R) = \cap(\rho : R) = 0$.

Теорема 1. *Кольцо R примитивно $\iff$ в R существует максимальный регулярный правый идеал ρ такой, что $(\rho : R) = 0$. В этом случае R полупросто. Если R, кроме того, коммутативно, то R — поле.*

Упражнение. Доказать последнюю часть теоремы 1, т.е. показать, что если R примитивно, полупросто и коммутативно, то R является полем.

Пример. Кольцо $\mathbb{Z}$ полупросто и коммутативно, но не примитивно.

Пусть R — примитивное кольцо и M — точный неприводимый R-модуль. Если $\Delta = C(M)$ — централизатор R на M, то по лемме Шура Δ — это тело. Рассмотрим M как правое векторное пространство над Δ: $m\alpha = \alpha(m)$.

Говорят, что R действует *плотно* на M, если для любых $n \in \mathbb{N}$ и $v_1, \dots, v_n \in M$ таких, что $\dim \langle v_1, \dots, v_n \rangle = n$, и любых $w_i \in M$ существует $r \in R$ такой, что $v_i r = w_i$.

Упражнение. Если $\dim_\Delta M = n$, а R действует точно и плотно на M, то $R \cong \mathrm{Hom}_\Delta(M, M)$, что также изоморфно кольцу Δ'_n, где Δ' — тело, антиизоморфное телу Δ.

Теорема 2 (*плотности*). *Пусть R — примитивное кольцо, M — точный неприводимый R-модуль, а $\Delta = C(M)$ — централизатор R на M. Тогда R — плотное кольцо линейных преобразований M над Δ.*

Доказательство. Достаточно показать, что если V — конечномерное подпространство в M и $m \in M \setminus V$, то существует $r \in R$ такой, что $Vr = 0$ и $mr \neq 0$.

Пусть $v_1, \ldots, v_n \in M$ линейно независимы над Δ. Обозначим $V_i = \langle v_1, \ldots, \widehat{v}_i, \ldots, v_n \rangle_\Delta$. Имеем $mrR \neq 0$ и $mrR = M$. Значит поскольку $v_i \notin V_i$, то существуют $t_i \in R$ такие, что $v_i t_i = w_i,\ v_j t_j = 0$ при $j \neq i$. Следовательно, при $t = t_1 + \ldots + t_n$ имеем $v_i t = w_i$.

Докажем это утверждение индукцией по $\dim_\Delta V$. Утверждение тривиально, если $\dim_\Delta V = 0$. Пусть $V = V_0 + w\Delta$ и $A(V_0) = \{x \in R : V_0 x = 0\}$. Тогда для любого $m \notin V_0$ существует $r \in A(V_0)$ такой, что $mr \neq 0$, т.е. если $mA(V_0)$, то $m \in V_0$. Так как $A(V_0) \trianglelefteq_r R,\ w \notin V_0$, то $wA(V_0) \neq 0$, а потому $wA(V_0) = M$.

Предположим, что существует $m \in M \setminus V$ такой, что $Vr = 0$ влечёт $mr = 0$.

Определим $\tau : M \mapsto M$ правилом $x\tau = ma$, если $x = wa,\ a \in A(V_0)$.

Корректность: если $wa = 0$, где $a \in A(V_0)$, то $Va = 0$, т.е. $ma = 0$.

По определению, $\tau \in E(M)$. Далее, если $x = wa$, где $a \in A(V_0)$, то для любого $r \in R$ имеем $ar \in A(V_0)$, а также

$$xr = (wa)r = w(ar),\ (xr)\tau = m(ar) = (a\tau)r.$$

Следовательно, $\tau \in \Delta$ и для любого $a \in A(V_0)$ справедливо

$$ma = (wa)\tau = (w\tau)a \Rightarrow (m - w\tau)a = 0.$$

Теперь по предположению индукции получаем $m - w\tau \in V_0$ и $m \in V$, что противоречиво. $\square$

Справедливо и обращение теоремы. Более того, справедливо следующее

Утверждение. *Пусть V — векторное пространство над телом D, R — транзитивное кольцо линейных преобразований пространства V (т.е. для любого ненулевого $v \in V$ и любого $w \in V$ существует $r \in R$ такой, что $vr = w$). Тогда R примитивно.*

Доказательство. Так как R — кольцо линейных преобразований, то V — точный R-модуль. Из транзитивности следует неприводимость V, т.е. R примитивно. □

Централизатор кольца R на V может не совпадать с D. Включение $D \subseteq C(V)$ всегда имеет место, но оно может быть и строгим, что мы уже видели ранее.

Теорема 3. *Пусть R — дважды транзитивное кольцо линейных преобразований векторного пространства V над телом D. Тогда R плотно на V и $C(V) = D$.*

Доказательство. Как и в утверждении выше, R примитивно. Пусть $\Delta = C(V)$, $D \subset \Delta$, $\tau \in \Delta \setminus D$ и $0 \neq v \in V$. Если v и $v\tau$ линейно зависимы над D, то

$$v\tau = v\alpha, \alpha \in D \Rightarrow v(\tau - \alpha) = 0 \Rightarrow \tau = \alpha \in D,$$

что противоречиво. Следовательно, v и $v\tau$ линейно зависимы над D и существует $r \in R$ такой, что $vr = 0, (v\tau)r \neq 0$. Получили противоречие. По теореме плотности, R — плотное кольцо. □

Теорема 4. *Пусть R — примитивное кольцо. Тогда существует тело Δ' такое, что либо $R \cong M_n(\Delta')$, либо для любого $m \in \mathbb{N}$ в R существует подкольцо S_m, гомоморфно отображающееся на $M_m(\Delta')$.*

Доказательство. Кольцо R действует как плотное кольцо линейных преобразований на некотором векторном пространстве V над телом Δ. Если $\dim_\Delta V = n$, то всё доказано. Если $\dim_\Delta V = \infty$, то для любого $m \in \mathbb{N}$ существуют элементы $v_1, \ldots, v_m \in V$ линейно независимые над Δ. Пусть $V_m = v_1\Delta + \ldots + v_m\Delta$ и $S_m = \{x \in R : V_m x \subseteq V_m\}$. Тогда по теореме плотности любое Δ-линейное преобразование пространства V_m индуцируется некоторым элементом из S_m. Пусть $W_m = \{x \in S_m : V_m x = 0\}$. Тогда $S_m/W_m \cong \mathrm{Hom}_\Delta(V_m, V_m) \cong M_m(\Delta')$. □

Кольцо R называется *первичным*, если aRb влечёт, что либо $a = 0$, либо $b = 0$.

Если $S \subseteq R$, то *правым аннулятором* множества S называется следующее множество $A_r(S) = \{x \in R : Sx = 0\}$. Аналогично определяется *левый аннулятор* $A_l(S)$.

Лемма 1. *Кольцо R первично $\iff$ R удовлетворяет одному из следующих условий*:

1). $0 \neq I \trianglelefteq^r R \Rightarrow A_r(I) = 0$;
2). $0 \neq I \trianglelefteq^l R \Rightarrow A_l(I) = 0$;
3). $A, B \trianglelefteq R, AB = 0 \Rightarrow A = 0$ *или* $B = 0$.

Упражнение. Доказать лемму.

Лемма 2. *Примитивное кольцо первично.*

Доказательство. Пусть ρ — ненулевой правый идеал в R и $\rho a = 0$ для некоторого $a \in R$. Кольцо R примитивно, значит существует точный неприводимый R-модуль M. Значит, $M\rho \neq 0$ и $M\rho = M$. Следовательно, $Ma = M\rho a = 0$, а потому $a = 0$. □

Лемма 3. *Пусть кольцо R первично, $0 \neq a \in Z(R)$. Тогда a не является делителем нуля в R. В частности, центр первичного (примитивного) кольца — область целостности.*

Доказательство. Если $ab = 0$, $0 \neq b \in R$, то $0 = Rab = aRb$. Следовательно, $a = 0$. □

Пусть R — кольцо, $E(R)$ — кольцо эндоморфизмов аддитивной группы R^+ кольца R, $R_a, L_a \in E(R)$. Обозначим через $B(R)$ подкольцо в $E(R)$, порождённое отображениями R_a, L_a, когда a пробегает R. Тогда $B(R)$ называется кольцом умножений кольца R. Заметим, что R^+ — модуль над $B(R)$, а идеалы в R — это в точности $B(R)$-подмодули; при этом R^+ — неприводимый модуль $\iff$ R — простое кольцо.

Центроидом кольца R называется множество элементов из $E(R)$, перестановочных со всеми элементами из $B(R)$.

Лемма 4. *Если $R^2 = R$, то центроид $C(R)$ кольца R коммутативен.*

Доказательство. Пусть $\sigma, \tau \in C(R)$. Тогда для любых $x, y \in R$ имеем

$$(xy)\sigma = xR_y\sigma = x\sigma R_y = (x\sigma)y = (yL_x)\sigma = x(y\sigma);$$

$$(xy)(\sigma\tau) = ((x\sigma)y)\tau = (x\sigma)(y\tau) = (x(y\tau))\sigma = (xy)(\tau\sigma).$$

Следовательно, $\sigma\tau - \tau\sigma = 0$. □

Теорема 5. *Если R просто, то центроид $C(R)$ кольца R — поле, а R можно рассматривать как алгебру над $C(R)$. Если $Z(R) \neq 0$, то $Z(R) \cong C(R)$.*

Доказательство. По лемме Шура, $C(R)$ — тело. Если $z \in Z^*$, то $Rz \trianglelefteq R$. Следовательно, $Rz = R$ и $1 \in R$. Отображение $z \mapsto T_z$ — это изоморфизм на некоторое подкольцо в $E(R)$. Если $\sigma \in C(R)$, то

$$r\sigma = (1r)\sigma = (r1)\sigma = (1\sigma)r = r(1\sigma).$$

Если $1\sigma = a$, то $a \in Z$, $\sigma = T_a$. Следовательно, $Z \cong C(R)$. □

Теорема 6 (*Веддербарн-Артин*). *Пусть R — простое артиново кольцо. Тогда $R \cong M_n(D)$. При этом n определено однозначно, а тело D — с точностью до изоморфизма. Обратно, $M_n(D)$ — простое артиново кольцо для любого тела D.*

Доказательство. Заметим, что R примитивно. Действительно, так как R артиново, то $J(R)$ — нильпотентный идеал в R. Поскольку $R^2 = R$, то $J(R) \neq R$, а потому $J(R) = 0$. Так как R просто и полупросто, то R примитивно.

Пусть M — точный неприводимый модуль над R. Тогда M — векторное пространство над телом $D = C(M)$. Докажем, что $\dim_D M < \infty$. Если $v_1, \ldots, v_m, \ldots$ линейно независимы, то $\rho_m = \{x \in R : v_i x = 0, i = 1, \ldots, m\} \trianglelefteq_r R$ и $\rho_1 \supseteq \rho_2 \supseteq \ldots \supseteq \rho_m \supseteq \ldots$. По теореме плотности эти включения строгие. Противоречие с артиновостью. Следовательно, $R \cong M_n(D')$, где $n = \dim_D M$.

Докажем единственность. Докажем, что если $A := M_m(D) \cong B := M_n(\Delta)$, то $m = n$, а $D \cong \Delta$.

Пусть $e = e_{11} \in A$, $\phi : A \mapsto B$ — изоморфизм, и $f = \phi(e)$. Так как $eA \trianglelefteq_r^{min} A$, то $fB \trianglelefteq_r^{min} B$.

Упражнение. Пусть D — тело, а e — идемпотент из D. Показать, что существует автоморфизм кольца $M_n(D)$, переводящий e в диагональную идемпотентную матрицу (т.е. с 0 и 1 на диагонали).

В силу этого упражнения, можно считать, что f также имеет вид e_{11}. Тогда

$$D \cong eAe \cong fBf \cong \Delta.$$

Так как $\dim_D A = m$, $\dim_\Delta B = n$, то $m = n$.

Упражнение. Доказать обращение теоремы. □

Теорема 7. *Пусть R — полупростое артиново кольцо. Тогда $R \cong \Delta^{(1)}_{n_1} \oplus \ldots \oplus \Delta^{(k)}_{n_k}$, где $\Delta^{(i)}$ — тело, $i = 1, \ldots, k$.*

Пусть A — алгебра над полем F. Элемент $a \in A$ называется *алгебраическим элементом* над F, если существует ненулевой $p(x) \in F[x]$ такой, что $p(a) = 0$. Алгебра называется *алгебраической*, если каждый её элемент является алгебраическим.

Пример. 1). $\mathbb{C}$ — алгебра над $\mathbb{R}$. Если $a = b + di$, то $p(x) = x^2 - 2bx + (b^2 + d^2)$.

2). *Упражнение.* Если A — алгебра над полем F, $\dim_F A = n$, то A — алгебраическая алгебра.

Лемма 5. *Пусть F — алгебраически замкнутое поле, D — тело, являющееся алгебраической алгеброй над F. Тогда $D = F$.*

Доказательство. Имеем $F \subseteq Z(D)$. Пусть $a \in D$, $p(a) = 0$ и $p(x) = \prod(x - \lambda_i)$, $\lambda_i \in F$. Тогда $p(a) = \prod(a - \lambda_i) = 0 \Rightarrow a - \lambda_i = 0$. Следовательно, $D = F$. □

Теорема 8. *Пусть F — алгебраически замкнутое поле, A — конечномерная полупростая алгебра над F. Тогда $A \cong F_{n_1} \oplus \ldots \oplus F_{n_k}$.*

Заметим, что центр прямой суммы — прямая сумма центров; $Z(M_n(F))$ одномерен. Следовательно, в условиях теоремы 8, $k = \dim_F Z(A)$.

Теорема 9. *Пусть G — конечная группа, F — алгебраически замкнутое поле характеристики ноль или p (p не делит $|G|$). Тогда $F(G) \cong F_{n_1} \oplus \ldots \oplus F_{n_k}$.*

§9 Подпрямая сумма

Прямым произведением (полной прямой суммой) колец R_γ ($\gamma \in I$) называется множество

$$\prod_{\gamma \in I} R_\gamma = \{f : I \mapsto \cup_{\gamma \in I} R_\gamma : f(\gamma) \in R_\gamma\}.$$

Операции: $(f + g)(\gamma) = f(\gamma) + g(\gamma),\ (fg)(\gamma) = f(\gamma)g(\gamma)$.

Обозначим через π_γ проекцию кольца $\prod_{\gamma \in I} R_\gamma$ на R_γ.

Кольцо R называется *подпрямой суммой* колец R_γ ($\gamma \in I$), если существует мономорфизм $\psi : R \mapsto \prod_{\gamma \in I} R_\gamma$ такой, что $R\psi\pi_\gamma = R_\gamma$ для любого $\gamma \in I$.

Лемма 1. *Пусть R — кольцо, $\psi_\gamma : R \mapsto R_\gamma$ — эпиморфизмы, $\psi : R \mapsto \prod R_\gamma$ составлен из ψ_γ. Пусть $U_\gamma = \mathrm{Ker}\ \psi_\gamma$. Тогда ψ — мономорфизм (т.е. R — подпрямая сумма колец R_γ) $\iff \cap U_\gamma = 0$.*

Упражнение. Доказать лемму.

Кольцо называется *подпрямо неразложимым*, если пересечение всех его ненулевых идеалов отлично от нуля (т.е. кольцо не допускает нетривиального представления в виде подпрямого произведения).

Примеры. 1). $\mathbb{Z}$ — подпрямая сумма колец Z_{p^k};

2). $\mathbb{Z}$ — подпрямая сумма полей Z_p, где p пробегает бесконечное множество простых чисел.

Лемма 2. *Любое кольцо представимо как подпрямая сумма подпрямо неразложимых колец.*

Доказательство. Пусть $0 \neq a \in R$. Обозначим через U_a идеал в R максимальный по отношению к свойству не содержать элемент a. Он существует по лемме Цорна. Так как $\cap_{a\neq 0} U_a = 0$, то R — подпрямая сумма колец R/U_a. Кольцо R/U_a подпрямо неразложимо: элемент $a + U_a \in R/U_a$ является ненулевым и лежит во всех ненулевых идеалах из R/U_a. $\square$

Лемма 3. *Пусть R — кольцо без ниль-идеалов, тогда R — подпрямая сумма первичных колец.*

Доказательство. Пусть a — ненильпотентный элемент из R и $U_a \trianglelefteq R$ максимальный по отношению к свойству не содержать степеней элемента a. Если $A, B \trianglelefteq R$, $U_a \subseteq A$, $U_a \subseteq B$ и $AB \subseteq U_a$, то $a^n \in A, a^k \in B \Rightarrow a^{n+k} \in U_a$, что невозможно. Следовательно, $R_a = R/U_a$ первично. Если N — множество всех ненильпотентных элементов из R, то $\cap_{a\in N} U_a$ — ниль-идеал, а потому он равен нулю. Значит, R — подпрямая сумма колец R_a. $\square$

Заметим, что R_a обладает дополнительным свойством: если $\bar{a}$ — образ элемента a в R_a и $\bar{U} \trianglelefteq R_a$, то $a^{n(\bar{U})} \in \bar{U}$, т.е. степени элемента a попадают во все ненулевые идеалы кольца R_a.

Теорема 1. *Кольцо R полупросто $\iff$ R — подпрямая сумма примитивных колец.*

Доказательство. Имеем $J(R) = \bigcap\limits_{\rho \trianglelefteq^{r,reg}_{max} R} (\rho : R) = 0$. Тогда R — подпрямая сумма колец $R/(\rho : R)$ по лемме 1. Как следует из §6, кольцо $R/(\rho : R)$ примитивно.

Обратно, пусть R — подпрямая сумма колец $R_\lambda := R/U_\lambda$, где $\cap U_\lambda = 0$. Кольцо R_λ примитивно, значит оно полупросто. Пусть $\psi_\lambda : R \mapsto R_\lambda$ — естественный гомоморфизм колец. Тогда $\psi_\lambda(J(R))$ — квазирегулярный идеал в R_λ. Следовательно, $J(R) \subseteq U_\lambda$ для любого λ, а потому $J(R) = 0$. $\square$

Следствие. *Коммутативное полупростое кольцо — подпрямая сумма полей.*

Схема. *Есть утверждение.* 1). *Доказать его для тел*; 2). *Доказать его для примитивных колец (сводя к матричным над телом)*; 3). *Доказать его для полупростых колец*; 4). *Доказать его для радикала.*

Утверждение. *Пусть R — кольцо, такое что*

$$(ab - ba)^3 = ab - ba \tag{$*$}$$

для любых $a, b \in R$. Тогда R коммутативно.

Доказательство. 1). Пусть R — тело. Если $\alpha = ab - ba \neq 0$, то $\alpha^2 = 1$. Тогда $\alpha \in Z(R) \Rightarrow a(ab) - (ab)a \in Z(R) \Rightarrow a\alpha \in Z(R) \Rightarrow a \in Z \Rightarrow \alpha = 0$.

2). Пусть R примитивно и $M_n(D)$, где D — тело, является эпиморфным образом подкольца из R. Тогда $(*)$ выполняется в $M_n(D)$. Возьмём $a = e_{11}, b := e_{12}$. Тогда $ab - ba = b,\ b^2 = 0 \Rightarrow 0 = (ab - ba)^3 \neq ab - ba$.

3). Пусть R полупросто. Значит R — подпрямая сумма примитивных колец R_ψ, которые являются гомоморфными образами кольца R. Следовательно, $(*)$ верно в R_ψ, а потому каждое R_ψ коммутативно. В итоге R коммутативно как подкольцо коммутативного кольца.

4). Пусть R произвольно. Тогда $R/J(R)$ полупросто, а потому $R/J(R)$ коммутативно. Следовательно, $x = ab - ba \in J(R)$ для любых $a, b \in R$ и $x^3 = x$. Следовательно, $x = 0$: действительно, если $uy = u, y \in J$, то $u = 0$, поскольку $-y + z - yz = 0$ влечёт $-uy + uz - uyz = -u = 0$. $\square$

§10 Тензорное произведение алгебр

Пусть A и B — алгебры над полем F. Рассмотрим тензорное произведение $A \otimes_F B$ пространств A и B над полем F. Определим на пространстве $A \otimes_F B$ умножение, полагая

$$\left(\sum_i a_i \otimes b_i\right)\left(\sum_j c_j \otimes d_j\right) = \sum_{ij} a_i c_j \otimes b_i d_j,$$

где $a_i, c_j \in A, b_i, d_j \in B$.

Теорема 1. *$A \otimes_F B$, с определённым выше умножением, является алгеброй. Пусть 1_A и 1_B — единицы алгебр A и B, соответственно.*

Тогда подпространства $A\otimes 1_B$ и $1_A\otimes B$ — подалгебры в $A\otimes_F B$, причём A изоморфна $A\otimes 1_B$, а B изоморфна $1_A\otimes B$.

Упражнение. Доказать теорему 1.

Теорема 2. *Пусть A — конечномерная алгебра над полем F с базисом из нильпотентных элементов. Тогда A нильпотентна.*

Доказательство. Можно считать, что поле F алгебраически замкнуто. Действительно, пусть $\bar F$ — алгебраическое замыкание поля F и $\bar A = A\otimes_F \bar F$. Тогда $\bar A$ имеет базис $\{u_i\otimes 1\}$ над $\bar F$, где $\{u_i\}$ — база A над F. Каждый из элементов $u_i\otimes 1$ нильпотентен и если $\bar A$ нильпотентна, то A нильпотентна, так как $A\cong A\otimes 1$.

Воспользуемся индукцией по $\dim A$. Если $\dim A{=}1$, то всё очевидно. Пусть $\dim A = n$. Если $J(A) = A$, то A нильпотентна и всё доказано. Если $J(A)\neq 0$, то $A/J(A)$ нильпотентна, но она полупроста. Следовательно, $J(A) = 0$ и $A = A_1\oplus\ldots\oplus A_n$, где A_i — проста, $i = 1,\ldots,n$. Но тогда след любого элемента алгебры нулевой, что противоречиво. $\square$

Алгебра A с единицей над полем F называется *центральной*, если $Z(A) = F$.

Теорема 3. *Пусть A — центральная простая алгебра над полем F, B — простая алгебра, содержащая F в своём центре. Тогда $A\otimes_F B$ проста.*

Доказательство. Пусть $0\neq U\trianglelefteq A\otimes_F B$. Если $0\neq u\in U$, то $u=\sum a_i\otimes b_i$, где можно считать, что b_i линейно независимы. Назовём число ненулевых a_i длиной элемента u. Пусть $u\in U$ — ненулевой элемент минимальной длины. Если $r,s\in A$, то $(r\otimes 1)u(s\otimes 1) = \sum ra_is\otimes b_i\in U$. Так как A проста, то $Aa_1A = A$. Следовательно, можно считать, что $a_1 = 1$. Для любого $a\in A$ имеем $(a\otimes 1)u - u(a\otimes 1)\in U$. Значит, $\sum[a,a_i]\otimes b_i\in U$, где $[a,a_i] = aa_i - a_ia$. Длина полученного элемента меньше, а потому это ноль. Так как b_i линейно независимы, то $[a,a_i] = 0$ для любого i, т.е. $a_i\in Z(A) = F$. Пусть $a_i = \alpha_i\in F$. Тогда $u = 1\otimes (b_1+\sum_{i=2}^n\alpha_ib_i) = 1\otimes b$, где $b\neq 0$, так как b_i линейно независимы. Следовательно, $U\supseteq(1\otimes B)(1\otimes b)(1\otimes B) = 1\otimes BbB = 1\otimes B$, а потому $U\supseteq (A\otimes 1)(1\otimes B) = A\otimes B$. $\square$

Теорема 4. *Пусть A, B — центральные простые алгебры над полем F. Тогда $A\otimes_F B$ центральная простая алгебра над полем F.*

Доказательство. Пусть $z=\sum a_i\otimes b_i\in Z(A\otimes_F B)$, где b_i линейно независимы. Следовательно, для любого $a\in A$ имеем

$$0 = (a\otimes 1)z - z(a\otimes 1) = \sum[a,a_i]\otimes b_i.$$

Тогда $[a, a_i] = 0$ и $a_i = \alpha_i \in F$. Значит $z = 1 \otimes \sum \alpha_i b_i = 1 \otimes b$, а потому для любого $x \in B$ выполняется

$$0 = z(1 \otimes x) - (1 \otimes x)z = 1 \otimes [b, x],$$

т.е. $[b, x] = 0$ и $b = \beta \in F$. Следовательно, $z = \beta(1 \otimes 1)$. □

§11 Группа Брауэра

Теорема 1. *Пусть D — алгебра с делением, конечномерная над своим центром Z. Тогда* $\dim[D : Z] = n^2$, $n \in \mathbb{N}$.

Доказательство. Пусть $\bar{Z}$ — алгебраическое замыкание поля Z. Так как D — центральная простая алгебра над Z, то $\bar{D} = D \otimes_Z \bar{Z}$ — простая алгебра над $\bar{Z}$ и $\dim_Z D := [D : Z] = [\bar{D} : \bar{Z}]$. Так как $\bar{D}$ — простая конечномерная алгебра над алгебраически замкнутым полем $\bar{Z}$, то $\bar{D} \cong M_n(\bar{Z})$ и $[\bar{D} : \bar{Z}] = n^2$. □

Теорема 2. *Если A — конечномерная центральная простая алгебра над $Z = Z(A)$, то* $\dim [A : Z] = n^2$, $n \in \mathbb{N}$.

Доказательство. Так как $A \cong M_m(D)$, где D — конечномерная алгебра с делением над Z и $Z(D) = Z$. Следовательно, $[D : Z] = n^2$, а потому $[A : Z] = (mn)^2$. □

Пусть R' — кольцо *взаимное* к R (*антиизоморфное*; $\phi(xy) = \phi(y)\phi(x)$).

Теорема 3. *Если A — конечномерная центральная простая алгебра над F, то $A \otimes A' \cong M_n(F)$, где $n = \dim_F A$.*

Доказательство. Рассматривая A как векторное пространство, имеем $L_F(A, A) := End_F(A) := L(A) \cong M_n(F)$. Пусть $A_r := \{R_a : a \in A\}$, $A_l := \{L_a : a \in A\}$. Тогда $A_r, A_l \leq L(A)$ и $A_r \cong A, A_l \cong A'$. Следовательно, $A \otimes_F A' \cong A_r \otimes_F A_l$ — центральная простая алгебра. Пусть $\phi : A_r \otimes_F A_l \mapsto A_r A_l \subseteq L(A)$ такое, что $\phi(\sum R_a \otimes L_b) = \sum R_a L_b$. Заметим, что A_r и A_l взаимно коммутируют, а ϕ является эпиморфизмом. В итоге, $A_r \otimes_F A_l \cong A_r A_l$ и $\dim_F(A_r \otimes_F A_l) = \dim_F(A_r A_l) = n^2$. Следовательно, $A_r A_l = L(A) = M_n(F)$, а потому $A \otimes A' \cong M_n(F)$. □

Если A и B — конечномерные центральные простые алгебры над полем F, то говорим, что A и B *эквивалентны* ($A \sim B$), если для некоторых $m, n \in \mathbb{N}$ выполняется

$$A \otimes_F M_n(F) \cong B \otimes_F M_m(F).$$

Если $A \cong D_1 \otimes_F M_n(F)$, а $B \cong D_2 \otimes_F M_m(F)$, где D_1, D_2 — конечномерные над F тела с центром F, то $A \sim B \iff D_1 \cong D_2$.

Упражнение. Доказать, что $\sim$ является отношением эквивалентности.

Пусть $B(F)$ — множество классов эквивалентности конечномерных центральных простых алгебр над полем F. Обозначим через $[A]$ класс, содержащий A, и определим произведение в $B(F)$:

$$[A][B] = [A \otimes_F B].$$

Теорема 4. *$B(F)$ — абелева группа.*

Упражнение. Доказать теорему.

Группа $B(F)$ называется *группой Брауэра* поля F, она перечисляет все алгебры с делением над F, содержащие F как центр.

§12 Максимальные подполя

Пусть D — тело, $S \subseteq D$. *Централизатором* S в D называется множество

$$C_D(S) := C(S) = \{x \in D : xs = sx \ \forall s \in S\}.$$

Легко видеть, что $C(S)$ — подтело в D.

Максимальным подполем тела D называется поле $K \subseteq D$ такое, что K не содержится ни в каком большем поле из D.

Максимальное подполе K содержит центр Z тела D, так как иначе, присоединяя к K элементы из Z, получим большее тело.

Лемма 1. *Если D — тело и K — подполе в D, то K максимально $\iff C(K) = K$.*

Доказательство. Если $K = C(K)$ и $L \supseteq K$ — подполе в D, то $L \subseteq C(K) = K$.

Если K максимально и $a \in C(K) \setminus K$, то $K(a) \supsetneq K$ — большее поле. □

Теорема 1. *Пусть D — тело с центром F и K — максимальное подполе в D. Тогда $D \otimes_F K$ — плотное кольцо линейных преобразований D, рассматриваемого как векторное пространство над K.*

Доказательство. Пусть $E(D)$ — кольцо эндоморфизмов аддитивной группы тела D, $D_r := \{R_a : a \in D\}$, $K_l := \{L_k : k \in K\}$. Тогда $[D_r, K_l] = 0$. Так как D — тело, то $dD_r = D$ для любого $d \in D^*$, т.е. D_r неприводимо. Следовательно, D_rK_l неприводимо. Так как D_rK_l — алгебра линейных преобразований, то D_rK_l точно на D.

Пусть Δ — централизатор кольца D_rK_l на D (в $E(D)$). Так как Δ централизует D_r, то $\Delta \subseteq D_l$ (если $\delta \in \Delta$, то $m\delta = (1m)\delta = \delta(1)m = mL_{\delta(1)}$). Кроме того, Δ централизует K_l. Так как K_l — максимальное подполе в D_l, то $\Delta \subseteq K_l$. С другой стороны, $K_l \subseteq \Delta$, а потому $K_l = \Delta$. Таким образом, D_rK_l — плотное кольцо линейных преобразований пространства D над K_l.

Поскольку $K \cong K_l$, то $D \otimes_F K$ — простая алгебра. Отображение $\phi : D \otimes_F K \mapsto D_rK_l$, действующее по правилу $\phi(\sum a_i \otimes k_i) = \sum R_{a_i} L_{k_i}$, — изоморфизм. Значит, $D \otimes_F K \cong D_rK_l$ и $D \otimes_F K$ является плотным кольцом K-линейных преобразований пространства D. □

Следствие 1. *Если $[D : Z(D)] < \infty$ и K — максимальное подполе в D, то $D \otimes_Z K \cong K_n$, где $n = [D : K]$.*

Доказательство. Плотность $D \otimes_Z K$ на пространстве D над K означает, что $D \otimes_Z K \cong K_n$. □

Теорема 2. *Если D — алгебра с делением, а Z — центр тела D, и $[D : Z] < \infty$, то для любого максимального подполя K справедливо*

$$[D : K] = [K : Z] = \sqrt{[D : Z]}.$$

Доказательство. Имеем $[D \otimes_Z K : K] = [D : Z]$. Так как $D \otimes_Z K \cong K_n$, то $[D \otimes_Z K : K] = n^2$. Следовательно, $[D : Z] = n^2$, а потому $[D : K] = [K : Z] = n$. □

Следствие 2. *Пусть D — конечномерная центральная некоммутативная алгебра с делением над $\mathbb{R}$. Тогда $\mathbb{C}$ — максимальное подполе в D и $[D : \mathbb{R}] = 4$.*

Доказательство. $\mathbb{C}$ — единственное конечное расширение поля $\mathbb{R}$. □

Следствие 3. *Тензорное произведение артиновых колец может быть не артиновым.*

Доказательство. Если D — алгебра с делением и $[D : K] = \infty$, то $D \otimes_F K$ — не артинова ($F = Z(D)$), иначе $D \otimes_F K \cong K_n$, что противоречит бесконечномерности $D \otimes_F K$ над K. □

§13 Модули над полупростыми артиновыми кольцами

Теорема 1. *Пусть R — полупростое артиново кольцо, M — унитарный модуль над R. Тогда M — прямая сумма неприводимых R-модулей.*

Доказательство. Так как R — полупростое артиново кольцо, то $R = R_1 \oplus \ldots \oplus R_k$, где R_i — простое артиново кольцо и e_i — идемпотент из $Z(R)$. Поскольку $1 = e_1 + \ldots + e_k$, то $M = Me_1 \oplus \ldots \oplus Me_k$. Далее, Me_i — унитарный R_i-модуль и $Me_iR_j = 0,\ i \neq j$. Следовательно, наше утверждение достаточно доказать, когда R — простое кольцо.

Если R — простое артиново кольцо, то $R \cong M_n(D)$. Пусть $\rho_i = e_{ii}R$. Тогда $R = \rho_1 \oplus \ldots \oplus \rho_n$, где $\rho_i \trianglelefteq^r_{min} R$. Значит, ρ_i — неприводимый R_i-модуль. Если $m \in M$, то $m = m_1 + \ldots + m_n$, где $m_i = me_{ii} \in m\rho_i$. Имеем либо $m\rho_i = 0$, либо $m\rho_i$ — неприводимый R-модуль. Следовательно, m содержится в сумме неприводимый R-модулей. Тогда M — сумма неприводимых R-модулей. Рассмотрим такие подмодули в M, которые являются прямыми суммами неприводимых R-модулей. По лемме Цорна выберем среди них максимальный — T_0. Тогда $T_0 = M$. Если $M_j \not\subseteq T_0$ для некоторого неприводимого подмодуля M_j, то $M_j \cap T_0 = 0$ и модуль $M_j \oplus T_0$ больше, чем T_0. Следовательно, $T_0 = M$. □

Теорема 2. *Пусть R — полупростое артиново кольцо, M — неприводимый модуль над R. Тогда $M \cong \rho$, где $\rho \trianglelefteq^r_{min} R$. Если R — простое артиново кольцо, то все неприводимые R-модули изоморфны.*

Доказательство. Имеем $M \cong R/\rho$, где $\rho \trianglelefteq^r_{max} R$. Существует такой $e \in R$, что $\rho = eR$. Тогда $R = eR \oplus (1-e)R$ и $M \cong R/\rho \cong R/eR \cong (1-e)R$. Так как M неприводим, то $(1-e)R \trianglelefteq^r_{min} R$.

Если R — простое артиново кольцо, то $R \cong M_n(D)$. Если $\rho \trianglelefteq^r_{min} R$, то $\rho = eR$, где $e^2 = e$. Подходящим автоморфизмом кольца R матрицу e можно привести к диагональному виду. Из минимальности ρ следует, что $e = e_{11}$, а потому $\rho \cong \rho_1$, где $\rho_1 = \{\sum_{i=1}^n \alpha_{1i}e_{1i}\} \trianglelefteq_r M_n(D)$. □

Глава 2

Часть II

§1 Автоморфизмы и дифференцирования

Теорема 1 (*Нётер-Сколем*). *Пусть R — простое артиново кольцо с центром F. Предположим, что A и B — простые подалгебры в R, которые содержат F и имеют конечную размерность над F. Если ϕ — изоморфизм A и B, и $\phi(\alpha) = \alpha$ для любого $\alpha \in F$, то существует $x \in R$ такой, что $\phi(a) = x^{-1}ax$ для любого $a \in A$.*

Доказательство. Заметим, что $R_l \otimes A_r$ — простое артиново кольцо, изоморфное R_lA_r, а $R_l \otimes B_r \cong R_lB_r$. Пусть $\psi : R_l \otimes A_r \mapsto R_l \otimes B_r$ такое, что $\psi(L_u \otimes R_a) = L_u \otimes R_{\phi(a)}$. Тогда ψ — изоморфизм, а кольцо R — модуль над $R_l \otimes A_r$: $x(L_u \otimes R_a) = uxa$ для любого $x \in R$. Аналогично, кольцо R — модуль над $R_l \otimes B_r$: $x(L_u \otimes R_{\phi(a)}) = ux\phi(a)$ для любого $x \in R$.

Кольцо R является прямой суммой неприводимых $R_l \otimes A_r$-модулей V_i ($V_i \cong V_j$), а также R является прямой суммой неприводимых $R_l \otimes B_r$-модулей U_i ($U_i \cong U_j$). Так как $R_l \otimes A_r \cong R_l \otimes B_r$, то $V_i \cong U_j$.

Пусть $R = V_1 \oplus \ldots \oplus V_n$ и $R = U_1 \oplus \ldots \oplus U_m$, $n \leq m$. Тогда существует изоморфизм $\sigma_i : V_i \mapsto U_i$ такой, что $\sigma_i(v_iL_uR_a) = \sigma_i(v_i)L_uR_{\phi(a)}$. Пусть $\sigma = \sum \sigma_i$. Тогда σ — мономорфизм из R в R такой, что $\sigma(vL_uR_a) = \sigma(v)L_uR_{\phi(a)}$.

Если $v = 1, a = 1$, то для любого $u \in R$ имеем $\sigma(u) = u\sigma(1) = ux$, где $x = \sigma(1)$. В частности, при $u = a$ получаем $\sigma(a) = ax$.

Если $v = u = 1$, то для любого $a \in A$ имеем $\sigma(a) = \sigma(1)\phi(a) = x\phi(a)$, т.е. $x\phi(a) = ax$ для любого $a \in A$.

Докажем, что x обратим в R. Если $ux = 0$ для некоторого $u \in R$, то $\sigma(u) = 0$ и поскольку σ — это мономорфизм, то $u = 0$. Следовательно, x не является правым делителем нуля в R.

Так как R — кольцо матриц над некоторым телом, то R артиново слева.

Покажем, что если R артиново слева, а x не является правым делителем нуля, то $R = Rx$. Действительно, пусть $I_0 = R$ и $I_1 = Rx$. Если $I_1 \neq I_0$, то положим $I_2 = I_1 x$. Тогда $I_2 \subseteq I_1$ и если $I_2 = I_1$, то $I_1 x = Rx$, противоречие с тем, что x не является правым делителем нуля. Пусть мы уже построили $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots \supseteq I_k$, где все включения строгие и $I_s = I_{s-1}x$. Положим $I_{k+1} = I_k x$. Тогда $I_{k+1} = I_k x \subseteq I_{k-1}x = I_k$. Если $I_{k+1} = I_k x = I_{k-1}x = I_k$, то как и выше получаем противоречие. В итоге, противоречие с артиновостью слева.

Таким образом, x обратим и $\phi(a) = x^{-1}ax$. $\square$

Следствие. *Пусть A — простая алгебра, конечномерная над своим центром. Тогда любой автоморфизм A является внутренним.*

Аддитивное (линейное) отображение δ кольца (алгебры) R называется *дифференцированием*, если

$$\delta(xy) = \delta(x)y + x\delta(y)$$

для любых $x, y \in R$. При этом дифференцирование δ называется *внутренним*, если $\delta(x) = xc - cx$ для некоторого $c \in R$.

Теорема 2. *Пусть A — простая алгебра, конечномерная над своим центром F. Тогда любое дифференцирование A является внутренним.*

Доказательство. Алгебра $M_2(A)$ является простой, её центр изоморфен F и она является конечномерной над F. Пусть

$$B = \left\{ \begin{pmatrix} a & \delta(a) \\ 0 & a \end{pmatrix} : a \in A \right\},\ C = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in A \right\}.$$

Если $\alpha \in F$, то $\delta(a) = 0$. Следовательно, B — подалгебра в $M_2(A)$, содержащая центр алгебры $M_2(A)$. Отображение $\psi : C \mapsto B$, определённое правилом

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mapsto \begin{pmatrix} a & \delta(a) \\ 0 & a \end{pmatrix},$$

— это изоморфизм C на B, при котором элементы из F неподвижны и $C \cong A$. Следовательно, существует обратимая матрица $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(A)$ такая, что

$$\begin{pmatrix} a & \delta(a) \\ 0 & a \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Значит $ax + \delta(a)z = xa$, $ay + \delta(a)w = ya, az = za, aw = wa$. Следовательно, $z, w \in F$. Так как $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ обратима, то можно считать, что $z \neq 0$. Полагая $u = -xz^{-1}$, получаем $\delta(a) = au - ua$. $\square$

§2 Теорема Фробениуса и теорема о двойном централизаторе

Теорема 1 (*Фробениус*). *Пусть D — некоммутативная алгебра с делением, конечномерная над $\mathbb{R}$. Тогда D изоморфна алгебре кватернионов.*

Доказательство. По следствию 2, $[D : \mathbb{R}] = 4$. Пусть K — максимальное подполе в D. Тогда $K \cong \mathbb{C}$. Рассмотрим автоморфизм в $\mathbb{C}$, переводящий элементы в комплексно сопряженные. Тогда он оставляет элементы из $\mathbb{R}$ неподвижными. Следовательно, существует $x \in D$ такой, что $\alpha - \beta i = x^{-1}(\alpha + \beta i)x$. Тогда $x^{-1}ix = -i$, откуда $x^2 i = ix^2$ и $x^2 \in \mathbb{C}$. Так как $x^2 \in \{a \in \mathbb{C} : \bar{a} = a\}$, то $x^2 \in \mathbb{R}$, но $x \notin \mathbb{R}$. Тогда $x^2 = -\alpha^2$, $\alpha \in \mathbb{R}$. Пусть $j = x/\alpha$. Имеем $j^2 = -1, ji = -ij$ и элементы $1, i, j, ij = k$ линейно независимы над $\mathbb{R}$, а поскольку $[D : \mathbb{R}] = 4$, то это базис D над $\mathbb{R}$. $\square$

Рассмотрим централизатор $C_R(S)$ подмножества S кольца R. Легко видеть, что $C_R(S)$ — подкольцо в R и $S \subseteq C_R(C_R(S))$. В случае, когда R — простое артиново кольцо, о (двойном) централизаторе можно сказать большее.

Теорема 2 (*о двойном централизаторе*). *Пусть R — простое артиново кольцо с центром F, и пусть $A \subseteq R$ — конечномерная простая подалгебра над F, содержащая F. Тогда $C_R(A)$ — простое кольцо и $A = C_R(C_R(A))$.*

Доказательство. Рассмотрим A как кольцо линейных преобразований, действующих на A. Если $\dim_F A = n$, то A

изоморфно вкладывается в $M_n(F)$ ($A \cong A_r$). Мы видели, что $C_{M_n(F)}(A_r) = A_l$, а потому $C_{M_n(F)}(C_{M_n(F)}(A_r)) = C_{M_n(F)}(A_l) = A_r$. Алгебра A_l антиизоморфна алгебре A. Следовательно, A_l проста и наше утверждение справедливо, если $R = M_n(F)$.

Кольцо $S := R \otimes_F M_n(F)$ является простым артиновым кольцом с центром F. Так как $A \subseteq M_n(F)$ и $A \subseteq R$, то кольца $A \otimes 1$ и $1 \otimes A$ лежат в S, являются конечномерными над F, простыми и изоморфными. При изоморфизме элементы из $F = F(1 \otimes 1)$ неподвижны. По теореме Нётер-Сколема кольца $A \otimes 1$ и $1 \otimes A$ сопряжены, а потому и их централизаторы в S сопряжены тем же самым элементом. Имеем

$$C_S(A \otimes 1) = C_R(A) \otimes M_n(F),\ C_S(1 \otimes A) = R \otimes C_{M_n(F)}(A).$$

Так как кольца $C_R(A) \otimes M_n(F)$ и $R \otimes C_{M_n(F)}(A)$ сопряжены в S то сопряжены их централизаторы:

$$C_S(C_R(A) \otimes M_n(F)) = C_R(C_R(A)) \otimes F \cong C_R(C_R(A)),$$

$$C_S(R \otimes C_{M_n(F)}(A)) = F \otimes C_{M_n(F)}(C_{M_n(F)}(A)) = F \otimes A \cong A.$$

Следовательно, $C_R(C_R(A)) \cong A$, т.е. они имеют одинаковую размерность над F. Так как $A \subseteq C_R(C_R(A))$, то $A = C_R(C_R(A))$.

Алгебры $C_R(A) \otimes M_n(F)$ и $R \otimes C_{M_n(F)}(A)$ сопряжены, а потому они изоморфны. Поскольку $C_{M_n(F)}(A)$ изоморфна A' и антиизоморфна алгебре A, то $R \otimes C_{M_n(F)}(A) \cong R \otimes A'$ — простое кольцо. Следовательно, $C_R(A) \otimes M_n(F)$ просто и $C_R(A)$ просто. □

§3 О радикале кольца $R[t]$

Упражнение. Пусть R — ассоциативное коммутативное кольцо с единицей. Показать, что полином $a_0 + a_1 t + \ldots + a_n t^n \in R[t]$ обратим $\iff$ a_0 обратим в R, а $a_1, \ldots, a_n$ нильпотентны в R.

Теорема 1. *Если R не имеет ненулевых ниль-идеалов, то кольцо $R[t]$ полупросто.*

Доказательство. Пусть $0 \neq J$ — радикал в $R[t]$. Пусть

$$r = a_0 t^{n_0} + \ldots + a_k t^{n_k} \quad (n_0 < \ldots < n_k)$$

— ненулевой элемент из J с наименьшим числом ненулевых коэффициентов a_i. Так как $a_i r - r a_i$ лежит в J и имеет меньше ненулевых коэффициентов, то он должен быть равен нулю, откуда $a_i a_j = a_j a_i$ для всех i, j.

Покажем, что все $a_0, \ldots, a_k$ нильпотентны. Элемент $r_1 = ra_i t$ лежит в J, поэтому существует s такой, что $r_1 + s + r_1 s = 0$, откуда

$$s = -r_1 - r_1 s = -r_1 + r_1(r_1 + r_1 s) = -r_1 + r_1^2 + r_1^2 s.$$

Продолжая далее по индукции, получаем

$$s = -r_1 + r_1^2 - r_1^3 + \ldots + (-1)^n r_1^n + (-1)^n r_1^n s.$$

для любого $n \in \mathbb{N}$. Пусть n больше степени элемента s. Сравнивая коэффициенты при одинаковых степенях t, обнаруживаем, что коэффициенты полинома s суть полиномы от $a_0, \ldots, a_k$. Обозначим через R_0 подкольцо в R, порождённое $a_0, \ldots, a_k$, и через R_0' — кольцо, полученное из R_0 формальным присоединением единицы 1. Тогда $r_1, s \in R_0'[t]$ и $(1 + r_1)(1 + s) = 1$. Так как R_0' коммутативно, то по упражнению выше получаем, что все коэффициенты многочлена $r_1 = ra_i t$ нильпотентны. В частности, a_i нильпотентен.

Обозначим через U множество таких элементов $a \in R$, что $r = at^{n_0} + b_1 t^{n_1} + \ldots + b_k t^{n_k} \in J$ для некоторых $b_1, \ldots, b_k$. Тогда U — ниль-идеал в R и $0 \neq a_0 \in U$. Противоречие. $\square$

§4 Стандартные тождества

Далее рассматриваем алгебры над полем F. Говорят, что алгебра A над полем F удовлетворяет *полиномиальному тождеству*, если для некоторого $d > 0$ существует ненулевой полином $f \in F[x_1, \ldots, x_d]$ от некоммутативных переменных $x_1, \ldots, x_d$ над F, такой что

$$f(a_1, \ldots, a_d) = 0$$

для всех $a_1, \ldots, a_d \in A$. Алгебру с полиномиальным тождеством будем называть *PI-алгеброй.*

Примеры. 1) Любая коммутативная алгебра является PI-алгеброй, так как удовлетворяет тождеству $f(x_1, x_2) = x_1 x_2 - x_2 x_1$.

2) Алгебра $M_2(F)$ удовлетворяет полиному

$$f(x_1, x_2, x_3) = (x_1 x_2 - x_2 x_1)^2 x_3 - x_3 (x_1 x_2 - x_2 x_1)^2.$$

Лемма 1. *Если $d \in \mathbb{N}$ и $0 \neq f \in F[x_1, \ldots, x_d]$, то существует $n \in \mathbb{N}$ такое, что $M_n(F)$ не удовлетворяет f.*

Доказательство. Пусть степень f равна k и M — идеал в $F[x_1, \ldots, x_d]$, порожденный всеми одночленами степени, большей k. Тогда алгебра $A = F[x_1, \ldots, x_d]/M$ конечномерна над F. Используя регулярное представление алгебры A, мы можем представить её как подалгебру полной матричной алгебры $M_n(F)$, где $n = \dim_F A$. Так как $f \notin M$, то образ $\bar{f}$ элемента f в алгебре A отличен от нуля. Следовательно, существуют такие $a_1, \ldots, a_d \in M_n(F)$, что $f(a_1, \ldots, a_d) \neq 0$. $\square$

Стандартным полиномом степени n в алгебре $F[x_1, \ldots, x_n]$ $(n \geq 2)$ называется полином

$$[x_1, \ldots, x_n] := \sum_{\sigma \in \mathbb{S}_n} (-1)^\sigma x_{\sigma(1)} \ldots x_{\sigma(1)}.$$

Говорят, что алгебра A удовлетворяет стандартному тождеству, если для некоторого n полином $[x_1, \ldots, x_n]$ равен нулю на A.

Лемма 2. *Если A — алгебра размерности n над F, то A удовлетворяет полиному $[x_1, \ldots, x_{n+1}]$.*

Доказательство. Из определения стандартного полинома следует, что он полилинеен и кососимметричен по всем аргументам. Расписывая элементы по базису $e_1, \ldots, e_n$ и пользуясь полилинейностью и кососимметричностью, получаем представление $[x_1, \ldots, x_{n+1}]$ как сумму элементов вида $[e_{i_1}, \ldots, e_{i_{n+1}}]$, где два базисных элемента совпадают, что дает равенство нулю. $\square$

Следствие 1. *Алгебра $M_n(F)$ удовлетворяет полиному $[x_1, \ldots, x_{n^2+1}]$.*

Следствие 2. *Если A — коммутативная алгебра над полем F, то алгебра $M_n(A)$ удовлетворяет полиному $[x_1, \ldots, x_{n^2+1}]$.*

Алгебра A называется *алгебраической алгеброй ограниченной степени* над полем F, если существует такое $n \in \mathbb{N}$, что для любого $a \in A$ существует полином вида $x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n \in F[x]$, корнем которого является α.

Лемма 3. *Если A — алгебраическая алгебра ограниченной степени над полем F, то A является PI-алгеброй.*

Доказательство. Пусть каждый $a \in A$ удовлетворяет полиному вида $x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n \in F[x]$, где n — фиксированное число. Если

b — произвольный элемент из A, то, коммутируя его с обеими частями равенства

$$a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0,$$

получим

$$[a^n, b] + \alpha_1 [a^{n-1}, b] + \ldots + \alpha_{n-1}[a, b] = 0.$$

Коммутируя это равенство с элементом $[a, b]$, получим

$$[[a^n, b], [a, b]] + \alpha_1[[a^{n-1}, b], [a, b]] + \ldots + \alpha_{n-2}[[a^2, b], [a, b]] = 0.$$

Прокоммутируем это равенство с элементом $[[a^2, b], [a, b]]$ и т.д. (n раз). В итоге получим специфическое тождество, которому удовлетворяет A. □

Лемма 4. *Если алгебра A удовлетворяет полиномиальному тождеству степени d, то она удовлетворяет полилинейному тождеству степени $\leq d$.*

Доказательство. Пусть A удовлетворяет полиномиальному тождеству $f(x_1, \ldots, x_n) = 0$ степени d. Тогда она удовлетворяет также тождеству

$$g(x_1, \ldots, x_n, x_{n+1}) = f(x_1 + x_{n+1}, x_2, \ldots, x_n)$$

$$-f(x_1, \ldots, x_n) - f(x_{n+1}, x_2, \ldots, x_n) = 0,$$

которое относительно x_1 имеет степень, меньшую, чем тождество $f = 0$. Продолжая так далее, приходим к тождеству, линейному относительно x_1. На каждом шаге этого процесса вводится новая переменная, а общая степень рассматриваемых тождеств не возрастает. Поэтому степень полученного тождества не превосходит d. Далее переходим к переменной x_2 и так далее. В итоге получим полилинейное тождество, которое выполняется в A и имеет степень не выше d. □

Лемма 5. *Если алгебра A удовлетворяет полилинейному тождеству f, то для любого расширения K поля F алгебра $A \otimes_F K$ также удовлетворяет f.*

Упражнение. Доказать лемму 5.

§5 Теорема Капланского

Лемма 1. *$M_n(F)$ не удовлетворяет никакому тождеству степени $<2n$.*

Доказательство. Можно считать, что тождество полилинейно:

$$f = x_1 \dots x_d + \sum_{\sigma \neq 1} \alpha_\sigma x_{\sigma(1)} \dots x_{\sigma(d)},\ d < 2n.$$

Пусть $x_1 = e_{11}, x_2 = e_{12}, x_3 = e_{22}, x_4 = e_{23}, \dots$. Если $\sigma \neq 1$, то $x_{\sigma(1)} \dots x_{\sigma(d)} = 0$. Следовательно, $f(e_{11}, e_{12}, e_{22}, e_{23}, \dots) = e_{11}e_{12}e_{22}e_{23}\dots \neq 0$. □

Теорема 1. *Если A — примитивная алгебра, удовлетворяющая полиномиальному f тождеству степени d, то A — конечномерная простая алгебра над своим центром Z и $\dim_Z A \leq [d/2]^2$.*

Доказательство. Так как A примитивна, то $A \cong M_n(\Delta) := \Delta_n$ или для любого $m \in \mathbb{N}$ существуют $B \leq A$ и $\phi \in Hom(B, \Delta_m)$ такие, что $\phi(B) = \Delta_m$. Во втором случае f — это тождество на Δ_m для любого $m \in \mathbb{N}$. Следовательно, f — тождество на Z_m, где Z — центр Δ, что в силу леммы 1 невозможно. Значит, $A \cong \Delta_n$.

Пусть K — максимальное подполе в Δ. Тогда кольцо $\Delta \otimes_Z K$ является плотным кольцом линейных преобразований пространства Δ над K. Можно считать, что A удовлетворяет полилинейному тождеству f степени $\leq d$. Тогда f — это тождество и на $\Delta \otimes_Z K$. Как и выше, заключаем, что $\Delta \otimes_Z K \cong M_m(K)$, откуда $A \otimes_Z K \cong \Delta_n \otimes_Z K \cong M_{mn}(K)$. Так как f — тождество на $M_{mn}(K)$, то $d \geq 2mn$ и $mn \leq [d/2]$ Поскольку $\dim_K(A \otimes_Z K) = \dim_Z A = (mn)^2$, то $\dim_Z A \leq [d/2]^2$. □

Как мы видели выше, если A — коммутативная алгебра над полем F, то алгебра $M_n(A)$ удовлетворяет полиному $[x_1, \dots, x_{n^2+1}]$. Можно ли утверждать обратное, т.е. что любое PI-кольцо лежит в B_n для подходящего коммутативного кольца B и $n \in \mathbb{N}$? Это слишком общий подход. К примеру, можно рассмотреть бесконечномерную алгебру Грассмана Γ над полем характеристики ноль с образующими u_i и соотношениями $u_i u_j = -u_j u_i$.

Упражнение. Показать, что $[[x,y],z] = 0$ — тождество на Γ, а $[x_1, \dots, x_k]$ не является тождеством на Γ для любого $k \in \mathbb{N}$.

Теорема 2. *Если A — PI-алгебра без ниль-идеалов, то $A \leq B_m$, где B — коммутативное кольцо (прямая сумма полей).*

Доказательство. По теореме 1 §3 кольцо $A[t]$ полупросто и $A[t] = A\otimes_F F[t]$. Пусть f — тождество на A. Можно считать, что f полилинейно. Тогда f — тождество на $A[t]$. Так как $A \leq A[t]$, то из $A[t] \leq B_m$ следует наше утверждение. Таким образом, считаем, что A полупроста. Тогда A — подпрямая сумма примитивных колец A_α и f — тождество на A_α. Если $\deg f = d$, то $\dim_{Z_\alpha} A_\alpha \leq [d/2]^2$. Используя регулярное представление алгебры A_α, можем вложить её в алгебру $M_k(Z_\alpha)$, где $k = \dim_{Z_\alpha} A_\alpha \leq [d/2]^2$. Тогда существует $m \in \mathbb{N}$ такое, что $A_\alpha \leq M_m(Z_\alpha)$ для любого α. Пусть $B = \oplus_\alpha Z_\alpha$. Тогда $A \leq B_m$. $\square$

Следствие. *Если A — PI-алгебра без ниль-идеалов, то на A выполнено стандартное тождество.*

Алгебру $M_n(F)$ можно отличить от её собственных подалгебр с помощью тождеств. Пусть $r(n)$ — минимальная степень стандартных тождеств выполняющихся в $M_n(F)$.

Лемма 2. $r(n) \geq r(n-1) + 2$.

Доказательство. Имеем вложение $M_{n-1}(F) \hookrightarrow M_n(F)$, $A \mapsto \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$. Пусть $t = r(n-1) - 1$. Тогда существуют $a_1, \ldots, a_t \in M_{n-1}(F)$ такие, что $[a_1, \ldots, a_t] \neq 0$. Следовательно, $[a_1, \ldots, a_t, e_{kn}, e_{nn}] = [a_1, \ldots, a_t]e_{kn} \neq 0$ для некоторого k, откуда $r(n) > t + 2 = r(n-1) + 1$. $\square$

Теорема 3. *Пусть R — простая алгебра, конечномерная над своим центром F, $A \leq R$ такая, что любое полилинейное тождество с коэффициентами из простого подполя $P \subseteq F$, выполняющееся в A, имеет место и в R. Тогда $A = R$.*

Доказательство. Если $\bar{F}$ — алгебраическое замыкание поля F, то условия теоремы верны для $R \otimes_F \bar{F}$. Следовательно, можно считать, что поле F алгебраически замкнуто. Тогда $R = M_n(F)$ по теореме Веддербарна.

Если A полупроста, то $A \cong M_{n_1}(F) \oplus \ldots \oplus M_{n_k}(F)$. Если g выполняется на $M_s(F)$, то g выполняется на A, где $g \in P[\bar{x}]$, $s = max\{n_1, \ldots, n_k\}$, т.е. g выполняется на $M_n(F)$ и по лемме 2 $s = n$ и $A = R$.

Если A не полупроста, то её радикал $N \neq 0$ и $A/N \cong M_{n_1}(F) \oplus \ldots \oplus M_{n_k}(F)$, где все $n_i < n$. Если $s = max\{n_1, \ldots, n_k\}$, то на A/N выполняется стандартное тождество степени $r := r(s)$, т.е. $[a_1, \ldots, a_r] \in N$ для любых $a_1, \ldots, a_r \in A$. Пусть $N^t = 0$. Так как $g = b_1[a_1, \ldots, a_r]b_2[a_{r+1}, \ldots, a_{2r}] \ldots b_t[a_{r(t-1)+1}, \ldots, a_{rt}] \in P[\bar{x}]$, то из выполнимости g на A следует выполнимость g на $M_n(F)$, а потому элементы $[x_1, \dots, x_r]$ ($x_i \in M_n(F)$) порождают нильпотентный идеал в $M_n(F)$. Следовательно, $[x_1, \dots, x_r] = 0, s < n$. Противоречие. $\square$

§6 Проблема Куроша для PI-алгебр

Проблема Куроша для алгебр, аналогичная проблеме Бернсайда для групп, формулируется следующим образом. Пусть A — алгебраическая алгебра над полем; верно ли, что любое конечное множество элементов из A порождает конечномерную подалгебру в A? В такой общности ответ отрицателен, однако если A является PI-алгеброй, то ответ положителен.

Алгебра над полем называется *локально конечной*, если любая её подалгебра, порождённая конечным числом элементов, является конечномерной.

Лемма 1. *Пусть A — алгебра над полем F, $B \trianglelefteq A$, B и A/B локально конечны. Тогда алгебра A локально конечна.*

Доказательство. Пусть $\{a_1, \dots, a_r\} \subseteq A, \bar{a}_1, \dots, \bar{a}_r \in A/B$, $alg\langle \bar{a}_1, \dots, \bar{a}_r\rangle = \langle \bar{a}_1, \dots, \bar{a}_r, \bar{a}_{r+1}, \dots, \bar{a}_m\rangle_F$. Пусть $a_1, \dots, a_m$ — их прообразы. Так как $\bar{a}_i, \bar{a}_j = \sum \alpha_{ijk}\bar{a}_k$, то $a_i a_j = \sum \alpha_{ijk} a_k + b_{ij}$, где $b_{ij} \in B$. Пусть $M = alg\langle b_{ij}, a_k b_{ij}, b_{ij} a_k, a_k b_{ij} a_t\rangle \subseteq B$. Тогда M конечномерна. Положим $W = alg\langle a_1, \dots, a_m\rangle$. Тогда $M \trianglelefteq W$ и $W/M = \langle a_1 + M, \dots, a_m + M\rangle_F$. Следовательно, M и W/M конечномерны. Тогда и W конечномерна , но $\{a_1, \dots, a_r\} \subseteq W$. $\square$

Лемма 2. *Пусть B, C — локально конечные идеалы в A. Тогда $B+C$ также локально конечный идеал в A.*

Доказательство. Имеем $(B + C)/C \cong B/(B \cap C)$ и $B/(B \cap C)$ локально конечна как гомоморфный образ локально конечной алгебры. $\square$

Если $\{B_\alpha\}$ — линейно упорядоченное по включению семейство локально конечных идеалов A, то $\cup B_\alpha$ — локально конечный идеал. Следовательно, существует максимальный локально конечный идеал в A и справедлива

Лемма 3. *В любой алгебре A существует единственный локально конечный идеал $L(A)$, в котором содержатся все локально конечные идеалы алгебры A.*

Идеал $L(A)$ называется *локально конечным радикалом* алгебры A.

Лемма 4. $L(L/L(A)) = 0$.

Доказательство. Если $\bar{C}$ — локально конечный идеал в $\bar{A}$ и C — его прообраз в A, то $C \supseteq L(A)$ и $C/L(A) = \bar{C}$. Следовательно, C локально конечен, $C \subseteq L(A) = \bar{C} = 0$. □

Теорема 1. *Если C — левый локально конечный идеал в A, то $C \subseteq A$.*

Доказательство. Переходя к $A/L(A)$, можно считать, что $L(A) = 0$. Надо доказать, что $C = 0$.

Рассмотрим идеал CA в A. Покажем, что он локально конечен. Пусть $x_1, \ldots, x_m \in CA$. Можно считать, что $x_i = c_i a_i$. Пусть $y_{ij} = a_i c_j$. Тогда $y_{ij} \in C$ и $W = alg\,\langle c_1, y_{ij}\rangle$ конечномерна над F. Имеем

$$x_i x_j = c_i a_i c_j a_j = c_i y_{ij} a_j \in W a_j \subseteq \sum W a_j := T,$$

$$W a_j x_t = W a_j c_t a_t = W y_{jt} a_t \subseteq W a_t \subseteq T.$$

Следовательно, $alg\,\langle x_1, \ldots, x_m\rangle \subseteq T + \langle x_1, \ldots, x_m\rangle_F$ конечномерна, т.е. CA локально конечен, откуда $CA = 0$ и C — локально конечный идеал в A. Значит, $C = 0$. □

Теорема 2. *Пусть A — алгебраическая PI-алгебра над полем F, A конечнопорождена и без ниль-элементов. Тогда $L(A) \neq 0$.*

Доказательство. Упражнение. Показать, что в алгебраической алгебре $J(A)$ — ниль-идеал.

Можем считать, что A полупроста. Пусть a — необратимый ненулевой элемент из A. Тогда $a^n + \alpha_1 a^{n-1} + \ldots + \alpha_k a^{n-k} = 0, \alpha_k \neq 0, n - k \geq 1$, откуда $((a^k + \alpha_1 a^{k-1} + \ldots + \alpha_k)a)^{n-k} = 0$ и $a^{k+1} + \alpha_1 a^k + \ldots + \alpha_k a = 0$. Следовательно, существует $p(x) \in F[x]$ такой, что $a = a^2 p(a)$. Значит $e = ap(a)$ — идемпотент ($e \neq 0, 1$) и $ae = a$.

Далее, для любого имеем

$$(xe - exe)^2 = 0,\ (ex - exe)^2 = 0 \Rightarrow xe = exe = ex \Rightarrow e \in Z(A).$$

Пусть $M \trianglelefteq A$, $a_1, \ldots, a_n \in M$. Покажем по индукции, что существует идемпотент $e \in M, e \in Z(A)$ такой, что $a_i e = a_i$ для всех i. Пусть существует $e_1 \in M$ такой, что $a_1e_1 = a_1, \ldots, a_{n-1}e_1 = a_{n-1}$ и $a_ne_1 - a_n \neq 0$. Тогда существует $e_2 \in M$ такой, что $(a_ne_1 - a_n)e_2 = a_ne_1 - a_n$ или $a_n = a_n(e_1 + e_2 - e_1e_2)$. Заметим, что $e := e_1 + e_2 - e_1e_2$ — идемпотент и

$$a_ne = a_n,\ a_ie = a_i(e_1 + e_2 - e_1e_2) = a_i + a_ie_2 - a_ie_2 = a_i.$$

Пусть P такой идеал в A, что A/P примитивна. Тогда A/P — простая конечномерная над своим центром алгебра. Так как A/P алгебраична над F, то $Z(A/P)$ — алгебраическое расширение поля F. Алгебра A конечнопорождена, поэтому и A/P конечнопорождена над F. Покажем, что $Z(A/P)$ конечнопорождена над F.

Пусть $\bar{e}_1, \ldots, \bar{e}_n$ — базис A/P над $Z(A/P)$, $\bar{a}_1, \ldots, \bar{a}_m$ — образующие в A/P. Тогда $\bar{a}_i = \sum \lambda_{ij}\bar{e}_j,\ \bar{e}_i\bar{e}_j = \sum \gamma_{ijk}\bar{e}_k,\ \lambda_{ij}, \gamma_{ijk} \in Z(A/P)$ и $Z(A/P) = alg\,\langle \lambda_{ij}, \gamma_{ijk}\rangle$. В итоге $\dim_F A/P < \infty$.

Пусть $\bar{y}_1, \ldots, \bar{y}_m$ — базис A/P над F и $\bar{x}_1, \ldots, \bar{x}_n$ — образующие алгебры A. Если y_i — прообраз элемента $\bar{y}_i$, то

$$x_i = \sum_{j=1}^{m} \alpha_{ij}y_j + u_i, y_iy_j = \sum_{j=1}^{m} \rho_{ijk}y_k + u_{ij},$$

где $u_i, u_{ij} \in P$. Пусть $P_0 = id\,\langle u_i, u_{ij}\rangle \trianglelefteq A$. Тогда $P_0 \subseteq P$. Так как $alg\,\langle x_1, \ldots, x_n\rangle = A$, то для любого $a \in A$ имеем $a = \sum \gamma_iy_i + u$, где $\gamma_i \in F, u \in P_0$. В частности, если $a \in P$, то, переходя к фактор-алгебре A/P, получим $\sum \gamma_i\bar{y}_i = 0$. Следовательно, $\gamma_i = 0$ и $a = u \in P_0$, откуда $P = P_0$.

Существует идемпотент $e \in P$ такой, что $u_ie = u_i, u_{ij}e = u_{ij}$ для любых i, j, при этом $e \in Z(A)$. Так как $P = id\,\langle u_i, u_{ij}\rangle$, то $ep = p$ для любого $p \in P$, откуда $P = Ae$. Положим $P_1 = \{x - xe : x \in A\} \trianglelefteq A$. Тогда $A = P \oplus P_1$ и $P_1 \cong A/P$. Так как A/P конечномерна над F, то она локально конечна. Следовательно, P_1 — локально конечный идеал в A, а потому $L(A) \neq 0$. □

Теорема 3. *Пусть A — алгебраическая PI-алгебра над полем F. Тогда A локально конечна.*

Доказательство. Пусть A удовлетворяет полилинейному тождеству степени d. Индукция по d. Если $d = 2$, то либо A коммутативна, либо A антикоммутативна, а потому локально конечна. Переходя к $\bar{A} = A/L(A)$, можно считать, что $L(A) = 0$. Более того, можно считать, что она конечнопорождена (так как нас интересует конечномерность конечнопорождённых подалгебр, то и рассматриваем такую. Если у неё $A = L(A)$, то доказывать нечего, если $A \neq L(A)$, то факторизуем по $L(A)$ и приходим к противоречию).

Если A без нильпотентных элементов, то $L(A) \neq 0$ по теореме 2.

Пусть $a \in A$ такой, что $a^2 = 0$ и T — левый идеал, порожденный элементом a. Тогда $Ta = 0$. Пусть в выполнено $f(x_1, \dots, x_d) = x_1 q(x_2, \dots, x_d) + h(x_1, \dots, x_d) = 0$, где в h слагаемые не начинаются на x_1. Возьмём $x_1 = a$ и $x_2, \dots, x_d \in T$. Тогда $aq(x_2, \dots, x_d) = 0$. Пусть $W = \{x \in T : ax = 0\}$. Тогда $TW = 0$ и $W \trianglelefteq T$. Так как $q(t_2, \dots, t_d) \in W$ для любых $t_2, \dots, t_d \in T$, то в $\bar{T} = T/W$ выполняется $q(x_2, \dots, x_d) = 0$. По индукции $\bar{T}$ локально конечна. Так как $W^2 = 0$, то W локально конечна. Следовательно, T — ненулевой локально конечный левый идеал в A. Теперь $T \subseteq L(A)$ по теореме 1. □

Теорема 4. *Пусть A — алгебраическая алгебра ограниченной степени над полем F. Тогда A локально конечна.* □

§7 Лемма Ширшова

Рассмотрим ассоциативные слова от $R = \{x_1, \dots, x_k\}$, $x_1 < \dots < x_k$. Слово α называется x_k-неразложимым, если оно имеет вид $\alpha = x_k \dots x_k x_{i_1} \dots x_{i_s}, s \geq 1, i_t \neq k$. Представление слова β в виде произведения x_k-неразложимых слов называется x_k-разложением слова β. Для β существует (при том единственное) x_k-разложение $\iff \beta = x_k \dots x_s$, где $s \neq k$.

Пусть $l(\alpha)$ означает длину слова α. На ассоциативных словах от R введём частичный порядок: если $l(\alpha) = l(\beta)$, то положим $\alpha > \beta$ в лексикографическом смысле. Пусть T — множество всех x_k-неразложимых слов. Линейный порядок на T: пусть $\alpha, \beta \in T$, полагаем $\alpha > \beta$, если $\alpha >_{lex} \beta$ или α — начало слова β. Ассоциативное слово γ называется n-разбиваемым, если оно может быть представлено в виде произведения своих подслов так, что при любой нетождественной перестановке этих подслов получаются слова меньшие γ.

Пример. Слово $\gamma = x_3x_1x_2x_2x_1x_1x_2x_1x_1x_1$ является 3-разбиваемым, при этом имеем 3 различных разбиения:

$$(x_3x_1)(x_2x_2x_1x_1)(x_2x_1x_1x_1), (x_3x_1x_2)(x_2x_1x_1)(x_2x_1x_1x_1),$$

$$(x_3)(x_1x_2x_2x_1x_1x_2)(x_1x_1x_1).$$

Слово $x_1x_2x_1x_3x_2x_1x_2x_3x_2$ не является 2-разбиваемым.

Слова, допускающие x_k-разложение, можно рассматривать как слова в алфавите T (T-слова), при этом можно говорить о T-длине и R-длине. На множестве всех ассоциативных T-слов введём частичный порядок $\prec$: для T-слов α и β с одной длиной положим $\alpha \prec \beta$, если $\alpha <_{lex} \beta$. Имеет смысл говорить об n-разбиваемых T-словах. Поэтому в дальнейшем используем термины: n_R-разбиваемость и n_T-разбиваемость.

Лемма 1. *Пусть α — ассоциативное T-слово. Тогда из его n_T-разбиваемости следует n_R-разбиваемость.*

Доказательство. Пусть $\alpha = \alpha_1 \ldots \alpha_n$ — n_T-разбиение. Тогда $\alpha, \alpha_1, \ldots, \alpha_n$ допускают x_k-разложение. Так как $\alpha \prec_T \alpha_{i_1} \ldots \alpha_{i_n}$, то это же верно и для R-слов: $\alpha > \alpha_{i_1} \ldots \alpha_{i_n}$. □

Лемма 2. *$(n-1)_T$-разбиваемость α влечёт n_R-разбиваемость αx_k.*

Доказательство. Из леммы 1 следует существование $(n-1)_R$-разбиения слова α:

$$\alpha = (x_k x_{i_1} \ldots x_{i'_1})(x_k x_{i_2} \ldots x_{i'_2}) \ldots (x_k x_{i_{n-1}} \ldots x_{i'_{n-1}}),$$

где $x_{i'_t} \neq x_k$. Тогда для слова αx_k имеем n_R-разбиение:

$$\alpha x_k = (x_k)(x_{i_1} \ldots x_{i'_1} x_k)(x_{i_2} \ldots x_{i'_2} x_k) \ldots (x_{i_{n-1}} \ldots x_{i'_{n-1}} x_k).$$

Действительно, если есть перестановка, сохраняющая (x_k), то она преобразует αx_k в $\alpha' x_k$, где α' получается перестановкой подслов в $(n-1)_R$-разбиваемом слове α. Следовательно, $\alpha > \alpha'$ и $\alpha x_k > \alpha' x_k$.

Если же x_k смещается, то полученное слово будет начинаться меньшим числом символов x_k по сравнению с αx_k. □

Лемма 3 (*А.И.Ширшов*). *Для любых $k, s, n \in \mathbb{N}$ существует $N(k,s,n) \in \mathbb{N}$ такое, что в любом ассоциативном слове длины $N(k,s,n)$ от k упорядоченных символов либо встретится s равных подслов, либо n-разбиваемое подслово.*

Доказательство. Рассматриваем слова от $R = \{x_1, \ldots, x_k\}$, $x_1 < \ldots < x_k$. Число $N(k,s,1)$ существует для любых $k, s \in \mathbb{N}$. Индукция по n. Предположим, что существует $N(k,s,n-1)$ для любых $k, s \in \mathbb{N}$. Число $N(1,s,n)$ существует. Далее индукция по k. Пусть существует $N(k-1,s,n)$. Докажем, что существует $N(k,s,n)$.

Рассмотрим произвольное ассоциативное слово α длины

$$[s + N(k-1,s,n)][N(k^{s+N(k-1,s,n)}, s, n-1) + 1].$$

Если в начале α стоят символы $x_i, i \neq k$, и их число $\geq N(k-1,s,n)$, то выполняется предположение индукции к этому подслову. Поэтому можно считать, что его длина $< N(k-1,s,n)$. В конце α может быть подслово $x_k \dots x_k$ и можно считать, что его длина $< s$. Отбросив эти подслова (если они существуют), получим слово α_1, длина которого больше числа

$$[s + N(k-1,s,n)][N(k^{s+N(k-1,s,n)}, s, n-1)].$$

Для α_1 существует x_k-разложение $\alpha_1 = \alpha_{11} \dots \alpha_{1m}$. Можно предполагать, что длина каждого x_k-неразложимого слова $\alpha_{1i} < s + N(k-1,s,n)$. Существует $\leq k^{s+N(k-1,s,n)}$ различных x_k-неразложимых слов при указанном ограничении на длину. Рассмотрим α_1 как T-слово. Его T-длина $> N(k^{s+N(k-1,s,n)}, s, n-1)$, т.е. в α_1 или s последовательных равных подслов, или $(n-1)_T$-разбиваемое подслово β. Если второе, то ввиду строгого неравенства для T-длины T-слова α_1 мы можем считать, что за β следует символ x_k. По лемме 2 слово βx_k является n_R-разбиваемым. □

Лемма 4. *Пусть α — ассоциативное слово длины m $(\alpha \neq \beta^t, t > 1)$. Тогда для любого $n \leq m$ слово α^{2n} содержит n-разбиваемое подслово.*

Доказательство. Из α циклической перестановкой порождающих можно получить m слов: $\alpha = \alpha_0, \alpha_1, \dots, \alpha_{m-1}$. Так как $\alpha \neq \beta^t$, то $\alpha_i \neq \alpha_j$. Пусть $\alpha_{i_0} > \alpha_{i_1} > \dots > \alpha_{i_{m-1}}$. Очевидно, что $\alpha_i = u_i v_i$, где $v_i u_i = \alpha$. Рассмотрим слово

$$\alpha^{2n} = v_{i_0} u_{i_0} v_{i_0} u_{i_0} v_{i_1} u_{i_1} v_{i_1} u_{i_1} \dots v_{i_{n-1}} u_{i_{n-1}} v_{i_{n-1}} u_{i_{n-1}}.$$

Пусть $\alpha'_{i_k} = u_{i_k} v_{i_k} u_{i_k} v_{i_{k+1}},\ k = 0, \dots, n-2,\ \alpha'_{i_{n-1}} = u_{i_{n-1}} v_{i_{n-1}} u_{i_{n-1}},\ \gamma = v_{i_0}$. Тогда $\alpha^{2n} = \gamma \alpha'_{i_0} \alpha'_{i_1} \dots \alpha'_{i_{m-1}}$. Так как начало α'_j совпадает со словом α_j, то $\alpha'_{i_0} \alpha'_{i_1} \dots \alpha'_{i_{m-1}}$ является n-разбиваемым. □

§8 Теорема Ширшова о высоте

Пусть F — ассоциативное коммутативное кольцо с 1 и A — ассоциативная алгебра, порождённая $a_1, \dots, a_n$. Обозначим через $F[X]$ свободную ассоциативную алгебру от порождающих $x_1, \dots, x_n$. Для любого $f(x_1, \dots, x_k) \in F[X]$ через $\bar{f}$ обозначим образ f при гомоморфизме $F[X] \mapsto A$ таком, что $x_i \mapsto a_i$.

Будем говорить, что одночлен $u \in F[X]$ имеет *тип* $[n_1, \ldots, n_k]$, если слово u содержит x_i ровно n_i раз, причём $n_k \neq 0$, но $n_j = 0$ для $j > k$. Пусть $u = x_{i_1}^{j_1} \ldots x_{i_h}^{j_h}$, причём $i_r \neq i_{r+1}$ для $r = 1, \ldots, h-1$. Число h назовём *высотой* u.

Пусть $Y = \{f_1, \ldots, f_l\}$ — однородные многочлены из $F[X]$, $\bar{Y} = \{\bar{f}_1, \ldots, \bar{f}_l\}$, v — одночлен из $F[X]$. Предположим, что существуют $q \in \mathbb{N}$ и одночлены $u_i(x_1, \ldots, x_l)$ с максимумом высот q такие, что $\bar{v} = \sum_i u_i(\bar{f}_1, \ldots, \bar{f}_l)$ и каждый элемент $u_i(f_1, \ldots, f_l)$ имеет тот же тип, что и v. Наименьшее число q с этим свойством называется *высотой одночлена* $\bar{v}$ *относительно* $\bar{Y}$. Если высоты всех одночленов алгебры A относительно $\bar{Y}$ ограничены в совокупности некоторым числом h, то A — *алгебра ограниченной высоты* h *относительно* $\bar{Y}$.

Примеры. 1) В $F[x_1, x_2]$ высота одночлена $x_1x_1x_2x_1x_1x_2x_1x_1x_2$ равна 6 относительно $\{x_1, x_2\}$ и равна 1 относительно $\{x_1x_1x_2\}$.

2) Любая коммутативная конечнопорождённая алгебра A — это алгебра ограниченной высоты. Действительно, если v типа $[i_1, \ldots, i_k]$, то $\bar{v} = \alpha a_1^{i_1} \ldots x_k^{i_k}$, т.е. высота $\bar{v}$ относительно множества $\{a_1, \ldots, a_k\}$ не превосходит k.

Теорема 1 (*А.И.Ширшов*). *Пусть A — ассоциативная конечнопорождённая PI-алгебра над F от порождающих $\{a_1, \ldots, a_k\}$ с тождеством степени n. Тогда A — ограниченной высоты относительно множества $\bar{Y}$, где Y — все слова из $F[X]$ длины $< n$.*

Доказательство. Можно считать, что тождество полилинейно. Достаточно доказать, что существует $M = M(n, k)$ такое, что любое ассоциативное слово s от $x_1, \ldots, x_k$ высоты $\geq M$ относительно Y содержит n-разбиваемое подслово. Действительно, в A выполняется $\bar{s} = \sum_i \alpha_i \bar{s}_i$, где s_i — слова от $x_1, \ldots, x_k$ того же состава, что и s, но меньшие s. Если s_i высоты $\geq M$, то продолжаем далее. Ввиду строгой монотонности, получим требуемое.

По лемме Ширшова существует $N = N(k, 2n, n)$ такое, что любое ассоциативное слово длины N от $x_1, \ldots, x_k$, не содержащее n-разбиваемых подслов, содержит подслово v^{2n}. Можно считать, что $v \neq v_1^t, t > 1$. Тогда по лемме 4 §7 $d(v) < n$. Следовательно, любое слово от $x_1, \ldots, x_k$ высоты $\geq N + 2$ относительно Y без n-разбиваемых подслов содержит подслово v_1 вида $v^n v'$, где $n > d(v) > d(v')$ и v' не начало v. Ввиду конечности подслов указанного вида, для большого M любое слово высоты $\geq M$ относительно Y, без n-разбиваемых послов, содержит

n равных подслов вида $v^n v'$. Но тогда существует n-разбиение:

$$(v^n v' u_1 v)(v^{n-1} v' u_2 v^2) \dots (v v' u_n),$$

$$(v' u_1 v^{n-1})(v v' u_2 v^{n-2}) \dots (v^{n-1} v' u_n),$$

в зависимости от того, какое из слов v, v' больше. □

Следствие 1 (*И.Капланский*). *Ассоциативная конечнопорождённая алгебраическая PI-алгебра над полем конечномерна.*

Доказательство. Пусть V — множество всех произведений $< n$ порождающих алгебры A (n — степень тождества), а m — максимум их степеней алгебраичности, h — высота A относительно V. Тогда A порождается как векторное пространство конечным числом ($< (m-1)nh$) элементов. □

Следствие 2 (*Левицкий*). *Ассоциативная конечнопорождённая ниль-PI-алгебра над кольцом нильпотентна. В частности, ассоциативная ниль-алгебра ограниченного индекса локально нильпотентна.*

Будем говорить, что алгебра A имеет *локально ограниченную высоту*, если каждая её конечнопорождённая подалгебра есть алгебра ограниченной высоты.

Следствие 3 (*Левицкий*). *Всякая ассоциативная имеет локально ограниченную высоту.*

Пусть I — некоторый идеал в F. Элемент F-алгебры A называется *алгебраическим* над I, если существуют $i_k \in I$ и $m \in \mathbb{N}$, такие что $a^m = \sum_{k=1}^{m-1} i_k a^k$. Конечнопорождённая алгебра A называется *конечной над* I, если существуют $a_1, \dots, a_k \in A$ и $m \in \mathbb{N}$ такие, что для любого $c \in A^m$ имеем $c = \sum_{k=1}^{m-1} i_k a_k$ для некоторых $i_k \in I$. Алгебра A называется *локально конечной над* I, если каждая её конечнопорождённая подалгебра является конечной над I. В частности, если $I = 0$, алгебраические элементы над I — это просто нильпотентные элементы, а локальная конечность над I превращается в локальную нильпотентность. Если же $I = F$, то алгебраичность и локальная конечность над I превращаются в обычную алгебраичность и локальную конечномерность над F.

Теорема 2. *Если в ассоциативной конечнопорождённой PI-алгебре A над F все произведения $< n$ порождающих алгебраичны над F, то A конечна над F.*

§9 Теорема Оре

Элемент кольца R называется *регулярным*, если он не является ни левым ни правым делителем нуля. Кольцо $Q(R) \supseteq R$ называется *левым кольцом частных* для R, если
1) любой регулярный $r \in R$ обратим в $Q(R)$;
2) любой $x \in Q(R)$ имеет вид $x = a^{-1}b$, где $a, b \in R$, a — регулярный элемент.
При этом кольцо R называется *левым порядком* в $Q(R)$.

Теорема 1. *Кольцо R имеет левое кольцо частных $\iff$ для любых $a, b \in R$ (b регулярен) существуют такие $a_1, b_1 \in R$ (b_1 регулярен), что $a_1 b = b_1 a$ (условия Оре).*

Доказательство. Если существует $Q(R)$, то существует $ab^{-1} \in Q(R)$, а потому $ab^{-1} = b_1^{-1}a_1$.

Обратно, пусть выполнены условия Оре и $\mathcal{M} = \{(a, b) : a, b \in R, b \text{ регулярен}\}$. Определим в $\mathcal{M}$ отношение $\sim$, полагая $(a, b) \sim (c, d) \iff$ существуют такие $b_1, d_1 \in R$, что $d_1 a = b_1 c$, $d_1 b = b_1 d$ и b_1 регулярен. Покажем, что d_1 регулярен. Из $d_1 b = b_1 d$ следует, что d_1 не является правым делителем нуля. Так как d регулярен, то существуют $b_2, d_2 \in R$ такие, что $d_2 b = b_2 d$ и d_2 регулярен. Тогда существуют $e_1, e_2 \in R$ такие, что $e_1 b_1 = e_2 b_2$ и e_2 регулярен. Следовательно,

$$e_1 b_1 d = e_2 b_2 d = e_1 d_1 b = e_2 d_2 b \Rightarrow e_1 d_1 = e_2 d_2.$$

Так как e_2, d_2 регулярны, то d_1 не является левым делителем нуля, а потому d_1 регулярен.

Покажем, что отношение $\sim$ не зависит от выбора регулярных элементов $b_1, d_1 \in R$ таких, что $d_1 b = b_1 d$.

Действительно, пусть $b_2, d_2 \in R$ регулярны и $d_2 b = b_2 d$. Из тех же рассуждений следует, что

$$e_1 b_1 = e_2 b_2,\ e_1 d_1 = e_2 d_2 \Rightarrow e_2 d_2 a = e_1 d_1 a = e_1 b_1 c = e_2 b_2 c \Rightarrow d_2 a = b_2 c.$$

Упражнение. Показать, что $\sim$ является отношением эквивалентности.

Класс, содержащий пару (a, b) обозначим через a/b. Пусть $Q(R)$ — множество всех классов эквивалентности. Определим операции на $Q(R)$:

$$a/b + c/d = (d_1 a + b_1 c)/b_1 d, \text{ где } d_1 b = b_1 d;$$

$$(a/b)(c/d) = (a_1c)/(g_1b), \text{ где } g_1a = a_1d, g_1 \text{ регулярен.}$$

Упражнение. Проверить корректность определения операций и аксиомы кольца на $Q(R)$. □

§10 Теоремы Голди

Пусть S — непустое подмножество в кольце R. Левым аннулятором множества S называется множество $l(S) = \{x \in R : xs = 0 \forall s \in S\}$. Левый идеал I называется левым аннуляторным идеалом, если $I = l(S)$ для некоторого $S \subseteq R$. Аналогично для правых идеалов.

Кольцо R называется *левым кольцом Голди*, если
1) R удовлетворяет условию обрыва возрастающих цепей левых аннуляторов;
2) R не содержит бесконечных прямых сумм левых идеалов.

Пример. Пусть R — нётерово слева кольцо.

Упражнение. Пусть $A = R[x_1, \ldots, x_n, \ldots]$. Показать, что A — кольцо Голди и A не нётерово.

Левый идеал I кольца R называется *существенным* (*большим*), если $I \cap J \neq 0$ для любого ненулевого левого идеала J из R.

Упражнение. Условие обрыва возрастающих цепей левых аннуляторов эквивалентно условию обрыва убывающих цепей аннуляторов.

Лемма 1. *Пусть R — полупервичное кольцо, удовлетворяющее условию обрыва возрастающих цепей левых аннуляторов. Если $A, B \trianglelefteq_l R$, $A \supseteq B$ и $r(A) \neq r(B)$, то существует такой $a \in A$, что $Aa \neq 0$, $Aa \cap B = 0$.*

Доказательство. Так как $A \supset B$, то $r(A) \subset r(B)$ и включения строгие. Пусть U — правый аннулятор минимальный по отношению к свойству $r(A) \subset U \subseteq r(B)$. Тогда $AU \neq 0$ и $AUAU \neq 0$. Пусть ua такой, что $AuaU \neq 0$. Покажем, что $Aua \cap B = 0$. В противном случае существует такой $x \in A$, что $0 \neq xua \in Aua \cap B$. Так как $x \in A$, то $r(x) \supset r(A)$. Рассмотрим $r(x) \cap U$, который является правым аннулятором. Тогда $r(A) \subset r(x) \cap U \subseteq r(B)$. Действительно, $xua \in B$, поэтому $xuaU = 0$ и $uaU \subseteq r(x) \cap U$, но $uaU \not\subseteq r(A)$. Следовательно, $r(x) \cap U = U, U \subseteq r(x)$, и $xu = 0$, что противоречит неравенству $xua \neq 0$. □

Следствие 1. *Пусть R удовлетворяет условию леммы, а Rx, Ry — существенные левые идеалы в R, тогда R — существенный левый идеал в R.*

Доказательство. Пусть A — ненулевой левый идеал в R и $\bar{A} = \{r \in R : ry \in A\}$. Так как Ry — существенный левый идеал, то $\bar{A} \neq 0$ и $\bar{A}y = Ry \cap A \neq 0$. Далее, $\bar{A} \supseteq l(y)$, $\bar{A}y \neq 0$ и $l(y)y = 0$. По лемме 1 существует такой $T \subseteq \bar{A}$, что $T \neq 0$ и $T \cap l(y) = 0$. Пусть $\bar{T} = \{r \in R : rx \in T\}$. Тогда $\bar{T}x = Rx \cap T \neq 0$ и $\bar{T}xy \neq 0$. Поскольку $\bar{T}xy \subseteq Ty \subseteq A$, то $Rxy \cap A \neq 0$. $\square$

Следствие 2. *Пусть R удовлетворяет условию леммы, а Ra — существенный левый идеал в R, тогда a регулярен.*

Доказательство. Кольцо R полупервично, значит $r(R) = 0$. Если $r(A) \neq 0$, то условия леммы выполнены для $A = R, B = Ra$. Так как Ra — существенный левый идеал в R, то $r(a) = 0$. Рассмотрим $l(a)$. Цепь $l(a) \subseteq l(a^2) \subseteq l(a^3) \subseteq \ldots$ обрывается на n-ом шаге: $l(a^n) = l(a^{n+1})$. Если $x \in Ra^n \cap l(a)$, то $x = ya^n$ и $xa = ya^{n+1} = 0$, откуда $y \in l(a^{n+1}) = l(a^n)$. Следовательно $x = 0$ и $Ra^n \cap l(a) = 0$, но Ra^n — существенный левый идеал в R, поэтому $l(a) = 0$. $\square$

Далее в этом параграфе предполагаем, что R — полупервичное левое кольцо Голди.

Лемма 2. *Кольцо R удовлетворяет условию обрыва убывающих цепей левых аннуляторов.*

Доказательство. Пусть $L_1 \supset L_2 \supset \ldots \supset L_n \supset \ldots$ — строго убывающая цепь. Тогда $r(L_i) \neq r(L_{i+1})$. По лемме 1 в каждом L_i существует $C_i \trianglelefteq_l R$ такой, что $C_i \cap L_{i+1} = 0$. Но тогда в R существует бесконечная прямая сумма $\oplus \sum C_i$. $\square$

Лемма 3. *Если $l(c) = 0$, то Rc — существенный левый идеал в R, а потому c регулярен.*

Доказательство. Пусть A — ненулевой левый идеал в R. Тогда $A \cap Rc = 0$, а потому левые идеалы Ac^n $(n \geq 0)$ образуют бесконечную прямую сумму. Действительно, если $a_0 + a_1c + \ldots + a_nc^n = 0$, где n минимально, то $a_0 \in A \cap Rc$, откуда $(a_1 + \ldots + a_nc^{n-1})c = 0$ и $a_1 + \ldots + a_nc^{n-1}$. $\square$

Идеал S кольца R называется аннуляторным, если $S = l(T)$, где $T \trianglelefteq_l R$.

Заметим, что $ST = 0 \Rightarrow (TS)^2 = 0 \Rightarrow TS = 0$.

Лемма 4. *Ненулевой минимальный аннуляторный идеал в R является первичным кольцом Голди. Существует конечная прямая сумма таких идеалов, образующая существенный левый идеал в R.*

Доказательство. Пусть S — ненулевой минимальный аннуляторный идеал в R и T — ненулевой левый идеал в S. Тогда $ST \neq 0$, так как иначе $S \cap r(S)$ — ненулевой нильпотентный идеал. Кроме того, $T \supseteq ST \trianglelefteq_l R$, т.е. S не содержит бесконечных прямых сумм.

Упражнение. Условие максимальности переносится на подкольцо.

В итоге, S — левое кольцо Голди.

Пусть $A, B \trianglelefteq S$ такие, что $AB = 0$. Тогда $ASB = 0$ и $A \subseteq l(SB) \cap S$ — аннуляторный идеал в R. Если $A \neq 0$, то $S \subseteq l(SB)$, откуда $(SB)^2 = 0$. Следовательно, $SB = 0$, т.е. $B = 0$ и S — первичное кольцо Голди.

Пусть $A = S_1 \oplus \ldots \oplus S_n$ — максимальная прямая сумма минимальных аннуляторных идеалов. Пусть — K ненулевой левый идеал в R. Если $A \cap K = 0$, то $AK \subseteq A \cap K = 0$, откуда $K \subseteq r(A) = l(A) \neq 0$. Так как R полупервично, то $A \cap r(A) \neq 0$. Следовательно, существует ненулевой минимальный аннуляторный идеал в $r(A)$, который не пересекается с A, но тогда его можно присоединить к прямой сумме. Значит, $A \cap K \neq 0$. $\square$

Лемма 5. *Если I — существенный левый идеал в R, то I содержит регулярный элемент.*

Доказательство. Пусть R первично и $a \in I$ такой, что $l(a)$ минимален. Если a регулярен, то всё доказано. Иначе существует ненулевой идеал J такой, что $Ra \cap J = 0$. Так как I является существенным, то $I \cap J \neq 0$, а потому можно считать, что $J \subseteq I$. Если $x \in J$ и $b \in l(a + x)$, то $ba = -bx \in Ra \cap J = 0$, откуда $b \in l(a) \cap l(x)$ и из минимальности $l(a)$ следует, что $l(a) \subseteq l(x)$. Значит, $l(a)x = 0$ для любого $x \in J$, а потому $l(a)J = 0$. Но в первичном кольце левый аннулятор ненулевого левого идеала равен нулю, т.е. $l(a) = 0$ и a регулярен.

Пусть теперь R полупервично, $A = S_1 \oplus \ldots \oplus S_n$, S_i — первичное кольцо Голди и $S_i \cap I$ — существенный левый идеал в S_i. Тогда $S_i \cap I$ содержит регулярный элемент r_i. Покажем, что $r = r_1 + \ldots + r_n$ регулярен в R. Если $l(r) \neq 0$, то из существенности идеала A следует, что $l(r) \cap A \neq 0$. Пусть $0 \neq t \in l(r) \cap A$, $t = t_1 + \ldots + t_n$ $(t_i \in S_i)$. Тогда $tr = \sum t_i r_i = 0$, а потому $t_i r_i = 0$. Теперь регулярность r_i в S_i даёт $t_i = 0$. $\square$

Теорема 1. *Пусть R — полупервичное левое кольцо Голди. Тогда существует левое кольцо частных $Q(R)$.*

Доказательство. Пусть $a, b \in R$, a регулярен. По лемме 3 Ra — существенный левый идеал в R, а потому $M = \{r \in R : rb \in Ra\}$ — существенный левый идеал в R (так как если $0 \neq A \trianglelefteq_l R$, то $Ab \trianglelefteq_l R$ и если $Ab = 0$, то $A \subseteq M$; если $Ab \neq 0$, то $Ab \cap Ra \neq 0$, а значит $M \cap A \neq 0$). По лемме 5 существует регулярный элемент $c \in M$ и $cb = da$. □

Упражнение. $I \trianglelefteq_l R \Rightarrow I = Q(I \cap R)$.

Упражнение. Если $A = A_1 \oplus \ldots \oplus A_n$ — прямая сумма левых идеалов в R, то $QA = QA_1 \oplus \ldots \oplus QA_n$ — прямая сумма левых идеалов в $Q(R)$.

Указание: если $x_1, \ldots, x_k \in Q$, то существует регулярный $a \in R$ такой, что $x_i = a^{-1}b_i$, где $b_1, \ldots, b_k \in R$.

Теорема 2. *Кольцо Q полупросто и удовлетворяет условию минимальности для левых идеалов.*

Доказательство. Пусть I — ненулевой левый идеал в Q и $I_1 = I \cap R$. Рассмотрим максимальную прямую сумму $S = I_1 \oplus \ldots \oplus I_n \trianglelefteq_l R$. Тогда S — существенный идеал в R. Пусть $K = I_2 \oplus \ldots \oplus I_n \trianglelefteq_l R$. Следовательно, $S = I_1 \oplus K$, а потому по лемме 5 существует регулярный элемент в S, но тогда $Q(I_1 \oplus K) = I \oplus QK = Q$. Так как $1 \in Q$, то $1 = i + k$, откуда $i^2 = i$, $k^2 = k$, $ik = ki = 0$. Ясно, что $I = Qi$. Таким образом, Q нётерово слева, а потому это левое кольцо Голди. Так как любой идеал порождается идемпотентом, то нет нильпотентных идеалов, т.е. Q полупервично.

Пусть I — ненулевой левый идеал в Q. Тогда $I = Qe$, $e^2 = e$ и $r(Qe) = r(e) = (1-e)Q$; $l((1-e)Q) = l(1-e) = Qe$. Следовательно, любой левый идеал является левым аннулятором, а потому по лемме 2 Q удовлетворяет условию минимальности для левых идеалов. Радикал $J(Q)$ такого кольца нильпотентен, т.е. $J(Q) = 0$. □

Теорема 3. *Пусть S — полупростое артиново кольцо, R — левый порядок в S. Тогда R — полупервичное кольцо Голди. Кроме того, если S просто, то R первично.*

Доказательство. Так как S — полупростое артиново кольцо, то любой левый идеал порождается идемпотентом. Следовательно, S удовлетворяет условию максимальности для левых аннуляторов. Так как это свойство переносится и на подкольца, то R удовлетворяет условию максимальности.

Пусть $A_1, \ldots, A_n$— левые идеалы в R такие, что сумма $A_1 + \ldots + A_n$ является прямой. Тогда и сумма $SA_1 + \ldots + SA_n$ также прямая. Действительно, если $\sum s_i a_i = 0$, то существует регулярный $d \in R$ такой, что $s_i = d^{-1}b_i$, $b_i \in R$. Тогда $\sum b_i a_i = 0 \Rightarrow b_i a_i = 0 \Rightarrow d^{-1}b_i a_i = 0 \Rightarrow s_i a_i = 0$. В итоге, R — кольцо Голди.

Пусть N — нильпотентный идеал в R, $N^m = 0, N^{m-1} \neq 0$. Тогда $0 \neq SNS \trianglelefteq S$ $(1 \in S) \Rightarrow SNS = eS$ $(e \in Z(S))$. Пусть $e = \sum a_i u_i b_i$. Следовательно, существует регулярный $a \in R$ такой, что $a_i = a^{-1}c_i$, где $c_i \in R$. Тогда $e = a^{-1}\sum c_i u_i b_i = a^{-1}\sum w_i b_i$, где $w_i = c_i u_i \in N$ (так как $ae = ea$). Далее,

$$N^{m-1}ea = N^{m-1}ae = N^{m-1}\sum w_i b_i = 0.$$

Так как a регулярен, то $N^{m-1}e = 0$. Но e — единица в SNS. Значит, $Ne = N, N^{m-1} = 0$ — противоречие.

Если S просто и $0 \neq A \trianglelefteq R$, то $0 \neq SAS \trianglelefteq S \Rightarrow SAS = S, 1 = \sum a_i u_i b_i$ $(u_i \in A)$, и существует регулярный $a \in R$ такой, что $a_i = a^{-1}c_i$, где $c_i \in R$. Тогда $1 = a^{-1}\sum c_i u_i b_i$. Если $B \trianglelefteq R$ такой, что $BA = 0$, то

$$Ba = Ba \cdot 1 = B\sum c_i u_i b_i = 0.$$

Так как a регулярен, то $B = 0$. □

Теорема 4 (*E.Posner*). *Пусть R — первичное кольцо, которое удовлетворяет полиномиальному тождеству над своим центроидом. Тогда R — порядок в D_n, где D — алгебра с делением конечномерная над своим центром.*

§11 S-градуированные алгебры и супералгебры

Пусть A — алгебра над полем F, $\langle S; +\rangle$ — абелева полугруппа. Говорят, что алгебра A является *S-градуированной*, если $A = \oplus_{s\in S} A_s$, причём

$$A_{s_1}A_{s_2} \subseteq A_{s_1+s_2}.$$

Подпространства A_s называются *однородными компонентами* A, и элементы из $\cup_{s\in S} A_s$ называются *однородными*.

Примеры. 1) A — алгебра многочленов, $A = F[x]$, $S = \mathbb{N}$, $A_n = \langle x^n\rangle$. Тогда $A = \oplus_n A_n$.

2) $A = F[x_1, \ldots, x_k]$, $S = \mathbb{N}$, $A_n = \langle u : u -$ одночлен $, deg\, u = n\rangle$;

3) $A = F[x_1, \dots, x_k]$, $S = \mathbb{N}^k = \{(n_1, \dots, n_k)\}$ — сложение покомпонентно; $A_{(n_1,\dots,n_k)} = \langle x_1^{n_1} \dots x_k^{n_k} \rangle$.

Если A — градуированная алгебра, $I \subseteq A$, то подпространство I называется *однородным*, если $I = \oplus_{s \in S}(I \cap A_s)$.

Упражнение. $I \subseteq A$ однородно $\iff$ для любого $i \in I$ все однородные компоненты элемента i также лежат в I.

4) Пусть A — свободная ассоциативная алгебра над полем F от порождающих $x_1, \dots, x_k$. Тогда $A = \oplus A_{(n_1,\dots,n_k)}$, где $A_{(n_1,\dots,n_k)} = \langle u : deg_{x_i} u = n_i,\ i = 1, \dots, k \rangle$.

Пусть M — класс алгебр. Алгебра $F_M[X] \in M$ называется *M-свободной* от множества порождающих X, если для любой алгебры $A \in M$ и любого отображения $\phi : X \mapsto A$ существует единственный $\tilde{\phi} \in Hom_F(F_M[X], A)$, продолжающий ϕ.

Многообразие алгебр M называется *однородным*, если

$$F_M[X] = \oplus F_M[X]_{(n_1,\dots,n_k)}.$$

Упражнение. Показать, что многообразие F-алгебр, заданное тождествами

$$(xy)z = x(yz), xy = yx, x^2 = x$$

не является однородным, если $F = \mathbb{Z}_2$.

Упражнение. Над бесконечным полем любое многообразие алгебр однородно.

5) $A = M_n(F)$, $S = \mathbb{Z}_n$ — циклическая группа порядка n, $A_i = \langle e_{rs} : s = r + i \,(\mathrm{mod}\, n) \rangle$, A_0 — диагональные матрицы, $A_i A_j \subseteq A_{i+j (\mathrm{mod}\, n)}$.

6) $A = F[x_1, \dots, x_k]$, $S = \mathbb{Z}_2$, $A_0 = \langle$одночлены чётной степени $\rangle$, $A_1 = \langle$одночлены нечётной степени $\rangle$, $A = A_0 \oplus A_1$.

Супералгебра — это $\mathbb{Z}_2$-градуированная алгебра $A = A_0 \oplus A_1$, A_0 называется *чётной частью* A, а A_1 называется *нечётной частью* A, $A_i A_j \subseteq A_{i+j (\mathrm{mod}\, 2)}$; элементы из A_0 называются *чётными*, а элементы из A_1 — *нечётными*.

Примеры. 1) $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}\imath$;

2) $A = F[u] = F \oplus Fu, u^2 = \alpha \in F$; $A = F[\epsilon] = F \oplus F\epsilon, \epsilon^2 = 0$ — алгебра дуальных чисел.

Если A и B — супералгебры над F, то можно рассмотреть их тензорное произведение $C = A \otimes B = C_0 \oplus C_1$, где

$$C_0 = A_0 \otimes B_0 + A_1 \otimes B_1, C_1 = A_0 \otimes B_1 + A_1 \otimes B_0.$$

Умножение: $(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2)$.

Градуированное (скрученное) тензорное произведение: $C = C_0 \oplus C_1$ как и выше, но умножение такое:

$$(a_1 \tilde{\otimes} b_1)(a_2 \tilde{\otimes} b_2) = (-1)^{p(b_1)p(a_2)}(a_1 a_2 \tilde{\otimes} b_1 b_2),$$

a_i, b_j — однородные, $p(x)$ — *чётность элемента* x, если x однороден, т.е.

$$p(x) = \begin{cases} 0, & \text{если } x \text{ чётный,} \\ 1, & \text{если } x \text{ нечётный.} \end{cases}$$

Если A и B — ассоциативные алгебры, то $A \tilde{\otimes} B$ — ассоциативная алгебра.

Упражнение. $\mathbb{C} \tilde{\otimes} \mathbb{C} \cong \mathbb{H}$ — кватернионы.

3) *Алгебра Грассмана*: $\Gamma_n = (F[\epsilon])^{\tilde{\otimes} n} = F[\epsilon] \tilde{\otimes} \ldots \tilde{\otimes} F[\epsilon]$, $\dim \Gamma_n = 2^n$, базис $\Gamma_n : \{e_1 \tilde{\otimes} \ldots \tilde{\otimes} e_n : e_i \in \{1, \epsilon\}\}$. Пусть $\varepsilon_i = 1 \tilde{\otimes} \ldots \tilde{\otimes} \epsilon \tilde{\otimes} \ldots \tilde{\otimes} 1$, где ϵ стоит на i-ом месте. Тогда $\varepsilon_i^2 = 0$, $\varepsilon_i \varepsilon_j = -\varepsilon_j \varepsilon_i$ $(i \neq j)$. Пусть $\varepsilon_{i_1 \ldots i_k} = 1 \tilde{\otimes} \ldots \tilde{\otimes} \epsilon \tilde{\otimes} \ldots \tilde{\otimes} \epsilon \tilde{\otimes} \ldots \tilde{\otimes} 1$, где ϵ стоит на $i_1, \ldots, i_k$-местах, $i_1 < \ldots < i_k$. Тогда $\varepsilon_{i_1 \ldots i_k} = \varepsilon_{i_1} \ldots \varepsilon_{i_k}$, т.е. $\Gamma_n = alg \langle \varepsilon_1, \ldots, \varepsilon_n \rangle$, Γ_n ассоциативна (играет роль *суперскаляров*) и является супералгеброй. Более того,

$$\langle 1, \varepsilon_{i_1} \ldots \varepsilon_{i_k}, k \in 2\mathbb{N} \rangle - \text{ чётная часть} \Gamma_n,$$

$$\left\langle \varepsilon_{i_1} \ldots \varepsilon_{i_{k+1}}, k \in 2\mathbb{N} \right\rangle - \text{ нечётная часть} \Gamma_n.$$

4) Пусть $F[u_i] = F \oplus F u_i, u_i^2 = \alpha_i \in F$, $i = 1, \ldots, n$. Тогда $F[u_1] \tilde{\otimes} \ldots \tilde{\otimes} F[u_n] := Cl[u_1, \ldots, u_n]$ — *алгебра Клиффорда*. Если $\tilde{u}_i = 1 \tilde{\otimes} \ldots \tilde{\otimes} u_i \tilde{\otimes} \ldots \tilde{\otimes} 1$, где u_i стоит на i-ом месте, то $Cl[u_1, \ldots, u_n] = alg \langle \tilde{u}_1, \ldots, \tilde{u}_n \rangle$, $\tilde{u}_i^2 = \alpha_i$, $\tilde{u}_i \tilde{u}_j = -\tilde{u}_j \tilde{u}_i$, $\dim Cl[u_1, \ldots, u_n] = 2^n$, базис $Cl[u_1, \ldots, u_n]$: $\{1, \tilde{u}_{i_1} \ldots \tilde{u}_{i_k}\}$, где $i_1 < \ldots < i_k$.

Гомоморфизмы супералгебр предполагаются сохраняющими градуировку, поэтому "идеалы" в супералгебрах — это однородные идеалы. Супералгебра называется *простой*, если она не содержит собственных однородных идеалов.

Пусть A — алгебра над F, $B = (A, A), B_0 = B_1 = A$ как векторное пространство. Определим умножение на B:

$$(a,b)(c,d) = (ac + bd, bc + ad).$$

Упражнение. $(A, A) \cong A \otimes F[u] = A \otimes 1 \oplus A \otimes u$, где $A \otimes 1$ — чётная часть, $A \otimes u$ — нечётная часть.

Полученную алгебру обозначают $A[u]$ и называют *удвоением* алгебры A.

Упражнение. Если A — простая алгебра, то $A[u]$ — простая супералгебра.

Упражнение. $F[u]$ проста как супералгебра, но $\langle 1+u \rangle \trianglelefteq F[u]$ как в алгебре ($u^2 = 1$).

Теорема 1. *Пусть A — простая супералгебра. Тогда либо A — простая алгебра, либо $A \cong A_0[u]$, где A_0 — простая алгебра.*

Доказательство. Пусть A не проста как алгебра и I — ненулевой идеал в A. Заметим, что $I \cap A_0 = I \cap A_1 = 0$. Действительно, если, к примеру, $I \cap A_0 \neq 0$, то $id_A \langle I \cap A_0 \rangle$ — ненулевой однородный идеал в A. Рассмотрим отображения $\pi_i : A \mapsto A_i$ $(i = 1, 2)$ такие, что $\pi_i(a) = a_i$, если $a = a_1 + a_2$. Тогда $\operatorname{Ker} \pi \cap I = 0$. Далее, $J = \pi_0(I) + \pi_1(I)$ — ненулевой однородный идеал в A. Действительно, если $c = c_0 + c_1 \in I$, то $I \ni ca_i = c_0a_i + c_1a_i$, где $c_0a_i \in A_i,\ c_1a_i \in A_{i+1}$. Тогда $c_0a_i = \pi_i(ca_i) \in J$. Остальные случаи разбираются аналогично. Следовательно, $J = A$ и $\pi_0(I) = A_0, \pi_1(I) = A_1$.

Если $a \in A$, то существуют $i, j \in I$ такие, что $a = \pi_0(i) + \pi_1(j)$. Рассмотрим отображение $u : A \mapsto A$, определённое правилом: если $a = \pi_0(i) + \pi_1(j)$, то $u(a) = \pi_0(j) + \pi_1(i)$.

Корректность: если $\pi_0(i) = \pi_0(i_1)$, $\pi_1(j) = \pi_1(j_1)$, то $\pi_0(i - i_1) = 0$, $\pi_1(j - j_1) = 0 \Rightarrow i - i_1 \in A_1 \cap I = 0, j - j_1 \in A_0 \cap I = 0 \Rightarrow i = i_1, j = j_1$.

Легко видеть, что линейно. Покажем, что $u \in C(A)$ где $C(A) = \{\phi \in End(A) : \phi(ab) = a\phi(b) = \phi(a)b\ \forall a, b \in A\}$ — центроид A.

Покажем, что $u(ax) = u(a)x = au(x)$. Достаточно это доказать только для однородных a и x. Пусть, например, $a \in A_0,\ x \in A_1$. Тогда $a = \pi_0(i),\ x = \pi_1(j)$ для некоторых $i, j \in I$, т.е. $i = a + i_1,\ j = j_0 + x$, где $j_0 \in A_0, i_1 \in A_1$. Так как $I \ni aj = aj_0 + ax$, то $ax = \pi_1(aj)$, а потому

$$u(ax) = \pi_0(aj) = aj_0 = a\pi_0(j) = au(x).$$

Остальные случаи разбираются аналогично. Так как $u(A_0) = A_1$, то $A = A_0 \oplus u(A_0)$.

Так как $u^2 = id_{|_A}$, то легко видеть, что $A \cong A_0 \otimes F[u] = A_0[u]$.

Покажем, что A_0 проста. Действительно, если $J \trianglelefteq A_0$, то $J[u] := J + u(J)$ — однородный идеал в A. □

Упражнение. Показать, что $I = A_0(1+u) = \{a + u(a) : a \in A_0\}$ и I — единственный идеал в A. Если характеристика поля не 2, то I и A_0 как алгебры изоморфны.

Упражнение. Пусть характеристика основного поля не равна 2. Показать, что алгебра A допускает структуру супералгебры $\iff$ существует автоморфизм $\phi \in Aut\,A$ такой, что $\phi^2 = id$. При этом $\phi(a_0 + a_1) = a_0 - a_1,\ A_0 = \{a \in A : \phi(a) = a\},\ A_1 = \{a \in A : \phi(a) = -a\}$ (назовём такой автоморфизм *стандартным*).

§12 Классификация простых конечномерных ассоциативных супералгебр над алгебраически замкнутыми полями.

Пусть V — векторное пространство над полем F, $V = V_0 \oplus V_1,\ A = End_F(V)$. Тогда $A = A_0 \oplus A_1$, где

$$A_0 = \{\phi \in A : \phi(V_i) \subseteq V_i\},\ A_1 = \{\phi \in A : \phi(V_i) \subseteq V_{i+1}\}.$$

Если V конечномерно, то $A = End_F(V) \cong M_n(F)$ — простая алгебра. Пусть $v_1, \ldots, v_k$ — базис V_0, $v_{k+1}, \ldots, v_n$ — базис V_1. Тогда

$$A_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a \in M_k(F), b \in M_{n-k}(F) \right\},$$

$$A_1 = \left\{ \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} : c \in M_{k,n-k}(F), b \in M_{n-k,k}(F) \right\}.$$

Построенная матричная супералгебра обозначается $M_{k,n-k}(F)$ и называется *супералгеброй Мори́та.*

Теорема 2. *Всякая простая конечномерная ассоциативная супералгебра A над алгебраически замкнутым полем F характеристики не 2 изоморфна либо $M_n(F)[u]$, либо $M_{k,n-k}(F)$.*

Доказательство. По теореме 1 либо $A \cong B[u]$, где B проста, либо A проста. Так как поле алгебраически замкнуто, то либо $A \cong M_n(F)[u]$, либо $A \cong M_n(F)$. Пусть $A \cong M_n(F)$. Определим градуировку в A. Рассмотрим A как $End_F(V)$, где $\dim V = n$. Отображение $\phi : A \mapsto A$ такое, что $\phi(a_0+a_1) = a_0-a_1$, где $a_i \in A_i$, является автоморфизмом в A, $\phi^2 = id$, $A_0 = \{a \in A : \phi(a) = a\}$, $A_1 = \{a \in A : \phi(a) = -a\}$. По теореме Нётер-Сколема существует обратимый $x \in A$ такой, что $\phi(a) = x^{-1}ax$ для любого $a \in A$. Так как $\phi^2 = id$, то $a = \phi(\phi(a)) = x^{-2}ax^2$ для любого $a \in A$, откуда $x^2 \in Z(A) = F \cdot 1$, т.е. $x^2 = \alpha \cdot 1 \in F \cdot 1$. Так как поле алгебраически замкнуто, то вместо x можно рассмотреть элемент $y = x/\sqrt{\alpha}$. Тогда $x^{-1}ax = y^{-1}ay$ и $y^2 = 1$. Таким образом, можно считать, что $x^2 = 1$. Тогда $V = V_0 \oplus V_1$, где $V_0 = \{v \in V : x(v) = v\}$, $V_1 = \{v \in V : x(v) = -v\}$. Действительно, если $v \in V$, то $2v = (v + x(v)) + (v - x(v))$. Более того, так как $A_0 = \{a \in A : xax = a\}$, $A_1 = \{a \in A : xax = -a\}$, то $A_0 = (End\, V)_0$, $A_1 = (End\, V)_1$. Действительно, если, к примеру, $v \in V_0, a \in A_0$, то $a(v) = xax(v) = xa(v)$, т.е. $a(v) \in V_0$. Остальные случаи разбираются аналогично. $\square$

Пусть A — супералгебра, Γ — алгебра Грассмана от счетного числа порождающих. Подалгебра $\Gamma(A) := \Gamma_0 \otimes A_0 + \Gamma_1 \otimes A_1 \leq \Gamma \otimes A$ называется *грассмановой оболочкой* супералгебры A.

Пусть $\mathcal{M}$ — некоторый класс алгебр. Говорят, что супералгебра A является $\mathcal{M}$-*супералгеброй*, если $\Gamma(A) \in \mathcal{M}$.

Пусть X и Y — непересекающиеся множества неизвестных. Назовём элементы из X чётными, а из Y — нечётными. Рассмотрим свободную алгебру $F\{X \cup Y\}$. Элемент $f(x_1, \dots, x_n; y_1, \dots, y_m) \in F\{X \cup Y\}$ называется *градуированным тождеством* супералгебры A, если $f(a_1, \dots, a_n; b_1, \dots, b_m) = 0$ для любых $a_1, \dots, a_n \in A_0$, $b_1, \dots, b_m \in A_1$.

Если мы знаем полилинейные тождества $\{f_i : i \in I\}$, определяющие $\mathcal{M}$, то градуированные тождества $\{\bar{f}_i : i \in I\}$, задающие $\mathcal{M}$-супералгебры, определяются *правилом знаков Капланского*: если элементы x_i и x_j поменялись местами $i < j$, то перед данным слагаемым добавляется знак $(-1)^{p(x_i)p(x_j)}$ (мы предполагаем, что слагаемое $\alpha x_1 \dots x_n$ содержится в рассматриваемом тождестве $f(x_1, \dots, x_n)$).

Совокупность всех градуированных тождеств образует идеал в $F\{X \cup Y\}$, так называемый T_2-*идеал* — идеал, устойчивый относительно эндоморфизмов в $F\{X \cup Y\}$ как супералгебры (считаем элемент $f \in F\{X \cup Y\}$ нечётным, если число нечётных неизвестных y_i в нём нечётно).

§13 PI-супералгебры и полупервичные супералгебры

Пусть A — ассоциативная супералгебра. Тогда A называется PI-супералгеброй, если A — ассоциативная PI-алгебра.

Теорема 3. *Пусть F — поле характеристики не 2. Супералгебра $A = A_0 + A_1$ — PI-супералгебра $\Longleftrightarrow$ A — PI-алгебра.*

Доказательство. Пусть A является PI-супералгеброй. Тогда $\Gamma(A) = \Gamma_0 \otimes A_0 + \Gamma_1 \otimes A_1$ — ассоциативная PI-алгебра. Следовательно, $\Gamma_0 \otimes A_0$ — PI-алгебра. Так как $A_0 \leq \Gamma_0 \otimes A_0$, то A_0 — PI-алгебра. Используем следующую теорему *В.К.Харченко*: *если A — ассоциативная алгебра, на которой действует конечная группа автоморфизмов G, в A нет $|G|$-кручения, $A^G := \{x \in A : x^g = x \, \forall g \in G\}$ — PI-алгебра, то A — PI-алгебра.*

Рассмотрим стандартный автоморфизм ϕ на A. Пусть $G = gr\,\langle\phi\rangle$. Тогда $A^G = A_0$, A_0 — PI-алгебра. Следовательно, A — PI-алгебра.

Обратно, пусть A — PI-алгебра. Так как Γ — это также PI-алгебра (например, с тождеством $[[x, y], z]$), то $\Gamma \otimes A$ — PI-алгебра по теореме *А.Регева*: *если A, B — ассоциативные PI-алгебры, то $A \otimes B$ — ассоциативная PI-алгебра.*

Поскольку $\Gamma(A) \leq \Gamma \otimes A$, то $\Gamma(A)$ — PI-алгебра. □

Супералгебра $A = A_0 + A_1$ называется *полупервичной*, если она не содержит однородных идеалов с нулевым умножением.

Теорема 4. *Пусть F — поле характеристики не 2. Супералгебра $A = A_0 + A_1$ полупервична $\Longleftrightarrow$ A полупервична как алгебра.*

Доказательство. Пусть $I \trianglelefteq A, I^2 = 0$, а ϕ — стандартный автоморфизм на A. Заметим, что

$$(I + I^\phi)^2 \subseteq II^\phi + I^\phi I \subseteq J := I \cap I^\phi.$$

Поскольку $J^\phi \subseteq J$, то J — однородный идеал в A и $J^2 = 0$. Следовательно, $J = 0$, а потому и $I = 0$.

В обратную сторону утверждение очевидно. □

Предметный указатель