МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
"Алтайская государственная педагогическая академия"

Ю.Н. Мальцев, Е.В. Журавлев

Лекции по теории ассоциативных колец

Учебное пособие

Барнаул 2014

ББК 22.1
УДК 512.55
М

Мальцев Ю.Н., док. физ.-мат. наук, профессор (кафедра алгебры и методики обучения математике АлтГПА).

Журавлев Е.В., канд. физ.-мат. наук, доцент (кафедра алгебры и математической логики АлтГУ).

Лекции по теории ассоциативных колец : учебное пособие / Ю.Н. Мальцев, Е.В. Журавлев. – Барнаул : АлтГПА, 2014. – 422с.
ISBN 978-5-88210-735-1

Рецензенты:
Бокуть Л.А., док. физ.-мат. наук, профессор (ИМ СО РАН).
Волков М.В., док. физ.-мат. наук, профессор (УрФУ).
ISBN 978-5-88210-735-1

Учебное пособие написано на основе лекций по теории колец, которые авторы читали в течении многих лет в Алтайском государственном университете и в Алтайской государственной педагогической академии. Изложены основы структурной теории ассоциативных колец, теория колец с тождественными соотношениями, классические кольца частных, а также теоремы коммутативности.

Пособие предназначено для студентов старших курсов, магистрантов и аспирантов математических факультетов университетов и академий, специализирующихся по алгебре, а также для научных работников.

Оглавление

Предисловие

Учебное пособие написано на основе лекций по теории ассоциативных колец, которые авторы читали в течение многих лет в Алтайском государственном университете и в Алтайской государственной педагогической академии.

Большая часть книги опирается на университетский курс высшей алгебры и доступно студентам второго и третьего курсов. Первые две главы пособия посвящены теории радикалов (Джекобсона, Левицкого, Бэра и верхнего ниль радикала) ассоциативных колец, а также строению полупростых (в смысле данного радикала) колец. Особое внимание уделено строению примитивных колец. В книге приведено описание примитивных колец с минимальными односторонними идеалами, а также доказана теорема Литоффа. В качестве приложения даны два доказательства "основной теоремы некоммутативной алгебры". В главе 3 дано подробное доказательство теоремы Оре о существовании правых колец частных, доказана теорема Голди о строении полупервичных колец Голди, а также (впервые на русском языке) изложена известная теорема Смолла о существовании артинового правого кольца частных. Изложение теории PI-колец в главе 4 содержит знаменитую теорему Ширшова о высоте, доказательство конечной базируемости многообразия, порожденного конечным кольцом и нахождение базисов тождеств алгебры верхних треугольных матриц над полем, а также алгебры матриц второго порядка над конечным полем. В главе 5, помимо доказательства классических результатов, ка-

сающихся коммутативности колец, изложены другие подходы к исследованию условий коммутативности колец. В конце каждой главы приведены упражнения и указания к их решению. Некоторые упражнения представляют собой результаты научных статей и дополняют содержание соответствующих глав. В конце книги мы поместили статью из газеты "Алтайская правда"(№ 43-44, 18.02.2011 г.), посвященную 90-летию выдающегося математика А.И. Ширшова, который учился и начинал свою трудовую деятельность на Алтае.

План книги, ее содержание и упражнения, включенные в нее, обсуждались в течение ряда лет на семинаре по теории колец АлтГПА. Авторы приносят участникам семинара благодарность за советы и критику, постановку задач и их интересные решения. Также авторы благодарны сотрудникам редакционно-издательского отдела АлтГПА за ценные советы и замечания, и помощь в подготовке данного пособия к изданию.

Учебное пособие соответствует программе специального курса по теории колец для студентов математических факультетов университетов и может быть использовано также аспирантами и научными работниками.

Учебное пособие написано и проведено в рамках задания № 2014/418 на выполнение государственных работ в сфере научной деятельности (в рамках базовой части государственного задания Минобрнауки России) и при частичной финансовой поддержке РФФИ (код проекта 12.01.00329а).

Список обозначений

В тексте используются следующие обозначения:
$\mathbb{N}$ – множество натуральных чисел,
$\mathbb{Z}$ – группа или кольцо целых чисел,
$\mathbb{Q}$ – группа или поле рациональных чисел,
$\mathbb{R}$ – поле вещественных чисел,
$\mathbb{C}$ – поле комплексных чисел,
$\mathbb{H} = \left(\frac{-1,1}{\mathbb{R}}\right)$ – тело кватернионов,
$\mathbb{Z}_n$ – кольцо классов вычетов по модулю n.
M/N – фактор-модуль,
$A(M)$ – аннулятор модуля M,
$\langle a_1, a_2, \ldots\rangle$ – подкольцо (или подалгебра), порожденное элементами $a_1, a_2, \ldots$,
$(b_1, b_2, \ldots)$ – идеал, порожденный элементами $b_1, b_2, \ldots$,
$\Phi\langle x_1, x_2, \ldots\rangle$ – свободная ассоциативная алгебра над коммутативной алгеброй Φ,
$k(G)$ – групповая алгебра группы G над полем k,
$\Phi_n(x)$ – круговой многочлен степени $\varphi(n)$,
$S[y;\alpha]$ – кольцо косых многочленов,
$\sum\limits_{i\in I}\bigoplus M_i$ – прямая сумма модулей,
$\sum\limits_{i\in I}\bigoplus\limits_{s} R_i$ – подпрямая сумма колец R_i, $i \in I$,
$\deg f(x)$ – степень многочлена $f(x)$,

$\mathrm{tr}(A)$ – след матрицы A,

$|F|$ – мощность множества F,

$[x]$ – целая часть числа x,

$[x, y] = xy - yx$ – коммутатор элементов x, y,

$[x_1, \ldots, x_n] = \big[[x_1, \ldots, x_{n-1}], x_n\big]$, при $n \geq 2$.

Если R – некоторое кольцо, то

$M_n(R)$ – кольцо квадратных матриц порядка n,

$R[x]$ – кольцо многочленов с коэффициентами из R,

R^+ – аддитивная группа кольца,

R^* – группа обратимых элементов кольца,

$R^\#$ – кольцо с присоединенной единицей,

$Z(R)$, $\mathrm{Cent}(R)$ – центр кольца,

$I <_r R$, I – правый идеал R,

$I \lhd R$, I – идеал R,

$\mathrm{End}_R M$ – централизатор кольца R на M (или кольцо всех R – гомоморфизмов модуля M),

$r(R)$ – правый аннулятор R,

$\ell(R)$ – левый аннулятор R,

$\mathrm{Ann}\, T$ – аннулятор подмножества T ($\mathrm{Ann}\, T = r(T) \bigcap \ell(T)$),

$\mathrm{Spec}\, R$ – множество простых идеалов кольца R,

$J(R)$ – радикал Джекобсона,

$\mathrm{un}R$ – верхний ниль-радикал кольца R,

$L(R)$ – локально нильпотентный радикал кольца R,

$\mathrm{ln}(R)$ – нижний ниль-радикал кольца R,

$Q(R)$ – классическое кольцо частных R.

$\diamondsuit \ldots \diamondsuit$ – указание к решению упражнения,

$\square \ldots \square$ – доказательство утверждения,

$N_G(x)$ – централизатор элемента x в группе G,

$[R, R]$ – коммутаторный идеал кольца R.

Глава 1

Радикал Джекобсона. Примитивные кольца

1.1. Модули

Абелева группа $\langle M, + \rangle$ называется *правым модулем* над ассоциативным кольцом R, если определено отображение

$$M \times R \to M,$$

переводящее каждую пару (m, r) из $M \times R$ в элемент $m \cdot r \in M$, такое, что для любых элементов $m, n \in M$ и $a, b \in R$ выполнены следующие условия:

1. $m(a + b) = ma + mb$;
2. $(m + n)a = ma + na$;
3. $m(ab) = (ma)b$.

Если кольцо R содержит единичный элемент 1 и $m \cdot 1 = m$ для любого элемента $m \in M$, то модуль M_R называется *унитарным.*

Пример 1.1. Если R – поле (тело), то произвольное векторное пространство V_R является R-модулем.

Пример 1.2. Произвольная абелева группа является $\mathbb{Z}$-модулем.

Пример 1.3. Если I – правый идеал кольца R ($I <_r R$), то I – правый R-модуль, относительно естественной композиции $(i, r) \to i \cdot r$, где $i \in I$, $r \in R$.

Если $\{M_i |\ i \in I\}$ – множество правых R-модулей, то

$$M = \sum_{i \in I} \oplus M_i = \{(m_1, m_2, \dots, m_n, 0, 0, \dots) |\ m_i \in I_i\}$$

является модулем относительно операций:

$$(m_i) + (m_i') = (m_i + m_i'), \quad (m_i)r = (m_i \cdot r).$$

Этот модуль называется *прямой суммой модулей* M_i, $i \in I$.

Пусть M – правый R-модуль и $N \subseteq M$. Тогда N называется *подмодулем* над кольцом R (в обозначении $N_R \leq M_R$), если для любых элементов $u, v \in N$ и $a \in R$ выполнено

$$(u + v) \in N \quad \text{и} \quad u \cdot a \in N.$$

Если $N_R \leq M_R$, то положим

$$\bar{M} = M/N = \{\bar{m} = m + N | m \in M\}$$

– множество всех смежных классов. Известно, что $\langle \bar{M}, + \rangle$ является абелевой группой относительно операции

$$\bar{m}_1 + \bar{m}_2 = \overline{m_1 + m_2}.$$

Определим на $\bar{M}$ структуру правого R-модуля следующим образом:

$$\bar{m} \cdot a = \overline{ma},$$

где $\bar{m} \in \bar{M}$ и $a \in R$. Модуль $\bar{M} = M/N$ называется *факторомодулем* модуля M по подмодулю N.

Заметим, что операция $\bar{m} \cdot a = \overline{ma}$ определена корректно. А именно, если $\bar{m} = \bar{m}_1$, то $ma - m_1a = (m - m_1)a \in N$, так как $(m - m_1) \in N$ и, следовательно, $\overline{ma} = \overline{m_1a}$, $\bar{m} \cdot a = \bar{m}_1 \cdot a$.

Пусть M_R и N_R – два R-модуля. Отображение $\varphi : M_R \to N_R$ называется *гомоморфизмом*, если для любых $m_1, m_2 \in M$ и $a, b \in R$

$$(m_1a + m_2b)\varphi = (m_1)\varphi a + (m_2)\varphi b.$$

Предложение 1.1. *Если $N_R \leq M_R$, то каждый подмодуль $K_R \leq M/N$ имеет вид P/N, где $N_R \leq P_R \leq M_R$.*

□ Пусть $\pi : M \to M/N$ – естественный гомоморфизм, отображающий произвольный элемент $m \in M$ в $(m)\pi = \bar{m}$ и пусть P – полный прообраз K в M. Тогда $(P)\pi = K$, $N \subseteq P$. Так как $\operatorname{Ker}\pi = N$, то $K = P/N$. □

Предложение 1.2. *Если N_1 и N_2 – подмодули M, то*

$$N_1 + N_2/N_2 \cong N_1/N_1 \cap N_2.$$

□ Рассмотрим естественный гомоморфизм модулей $\pi : N_1 \to N_1 + N_2/N_2$, отображающий произвольный элемент $v \in N_1$ в $(v)\pi = \bar{v} = v + N_2$. Тогда π – сюръективный гомоморфизм с ядром $\operatorname{Ker}\pi = N_1 \cap N_2$. Следовательно, $(N_1)\pi \cong N_1/\operatorname{Ker}\pi = N_1/N_1 \cap N_2$. Так как $(N_1)\pi = N_1 + N_2/N_2$, то $N_1/N_1 \cap N_2 \cong N_1 + N_2/N_2$. □

Пусть M_R – правый R-модуль. Множество

$$A(M) = \{x \in R |\ M \cdot x = 0\}$$

называется *аннулятором* модуля M. Если $A(M) = \{0\}$, то говорят, что M_R – *точный R-модуль.*

Предложение 1.3.

1. $A(M) \lhd R$;
2. M – *точный $R/A(M)$-модуль.*

□ Если $x, y \in A(M)$, $r \in R$ и $m \in M$, то $m(x+y) = mx+my = 0$, $m(rx) = (mr)x = 0$, так как $Mx = 0$. Откуда следует, что $(x+y)$, $rx \in A(M)$. Далее, $m(xr) = (mx)r = 0$. Следовательно, $A(M) \triangleleft R$. Пусть $\bar{a} \in R/A(M)$. Положим, $m \cdot \bar{a} = m \cdot a$. Тогда M – $\bar{R}$-модуль и если $M \cdot \bar{a} = 0$, то $Ma = 0$ и $a \in A(M)$. Откуда следует, что $\bar{a} = 0$. Итак, M – точный $\bar{R}$-модуль. □

Пусть M – R-модуль и

$$\mathrm{End}_R M = \mathrm{Hom}_R(M, M) = \{\varphi |\ \varphi : M \to M\}$$

– множество всех гомоморфизмов модуля M в себя. Это множество называется *централизатором* кольца R на M или кольцом всех гомоморфизмов модуля M в себя.

Заметим, что $\mathrm{End}_R M$ является ассоциативным кольцом с единицей относительно операций:

$$(m)(\varphi + \psi) = m\varphi + m\psi,\ m(\varphi \cdot \psi) = (m\varphi)\psi,$$

где $m \in M$, $\varphi, \psi \in \mathrm{End}_R M$. Проверим, например, что $\varphi + \psi \in \mathrm{End}_R M$. Пусть $m, n \in M$ и $a, b \in R$, тогда $(ma + nb)(\varphi + \psi) = (ma + nb)\varphi + (ma + nv)\psi = (m\varphi)a + (n\varphi)b + (m\psi)a + (n\psi)b = (m(\varphi + \psi))a + (n(\varphi + \psi))b$. Следовательно, $\varphi + \psi \in \mathrm{End}_R M$.

Модуль M_R называется *неприводимым*, если $MR \neq 0$ и M не содержит подмодулей, отличных от (0) и M_R.

Правый идеал $I <_r R$ называется *модулярным*, если существует такой элемент $e \in R$, что для любого элемента $a \in R$ справедливо $(a - ea) \in I$.

Ясно, что в кольце с единицей любой правый идеал является модулярным ($e = 1$).

Предложение 1.4 (лемма Шура).
Если M_R – неприводимый R-модуль, то $D = \mathrm{End}_R M$ – тело.

□ D – ассоциативное кольцо с единицей ε, где ε – тождественное отображение. Пусть $\lambda \in D$, $\lambda \neq 0$. Тогда $M\lambda \leq M$. Так как M_R не содержит ненулевых собственных подмодулей, то

$M\lambda = M$. Рассмотрим $\operatorname{Ker}\lambda \leq M$. Если $\operatorname{Ker}\lambda = M$, то $\lambda = 0$. Противоречие. Следовательно, $\operatorname{Ker}\lambda = 0$ и λ – биективное отображение.

Рассмотрим обратное отображение λ^{-1}. Докажем, что элемент $\lambda^{-1} \in \operatorname{End}_R M$. Пусть $m, n \in M$ и $a, b \in R$. Равенство

$$(ma + nb)\lambda^{-1} = (m\lambda^{-1})a + (n\lambda^{-1})b$$

равносильно равенству

$$((ma + nb)\lambda^{-1})\lambda = ((m\lambda^{-1})a + (n\lambda^{-1})b)\lambda.$$

Которое, в свою очередь, можно переписать в виде

$$ma + nb = ((m\lambda^{-1})\lambda)a + ((n\lambda^{-1})\lambda)b,$$

а значит, λ – обратимый элемент в D. □

Предложение 1.5.

1. *Если M_R – неприводимый R-модуль, то $M \cong R/I$, где I – некоторый максимальный модулярный правый идеал R;*

2. *Пусть I – максимальный модулярный правый идеал R. Тогда $M = R/I$ – неприводимый модуль.*

□ Пусть M_R – неприводимый модуль. Тогда существует элемент $m \in M$ такой, что $mR \neq 0$. Так как $mR \leq M$, то $M = mR$. Рассмотрим отображение $\varphi : R \to M$, полагая $(a)\varphi = ma$, где $a \in R$. Пусть $I = \{x \in R,\ mx = 0\}$. Тогда $I = \operatorname{Ker}\varphi$ – максимальный правый идеал R. Так как $m \in mR$, то существует такой элемент $e \in R$, что $m = me$. Следовательно, $m(a - ea) = ma - ma = 0$ и $(a - ea) \in I$ для любого элемента $a \in R$.

Обратно, пусть I – максимальный модулярный идеал кольца R и $M = R/I$. Если $MR = (0)$, то $R^2 \subseteq I$ и для любого элемента $a \in R$, $a = (a - ea) + ea \in I$. Противоречие. Следовательно, $MR \neq (0)$. Если N – подмодуль M, то $N = L/I$, где L – правый идеал, содержащий I. Следовательно, $L = I$ или $L = R$. Поэтому $N = (0)$, или $N = M$. □

Пример 1.4. Пусть V – 2-мерное векторное пространство над полем действительных чисел $\mathbb{R}$ и

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \operatorname{End}_{\mathbb{R}} V = M_2(\mathbb{R}).$$

Пусть $A = \mathbb{R} \cdot 1 + \mathbb{R} \cdot a$ – подалгебра, порожденная a. Тогда V – точный A-модуль.

Если $W_A \leq V_A$ и $W \neq 0$, $W \neq V$, то $\dim_{\mathbb{R}} W = 1$ и характеристический многочлен $|\lambda \cdot 1 - a| = 0$ имеет действительные корни. Противоречие. Следовательно, V_A – неприводимый A-модуль.

По лемме Шура, $D = \operatorname{End}_A V$ – тело. Так как $1 \in A$, то $\operatorname{End}_A V \subseteq \operatorname{End}_{\mathbb{R}} V$. Поэтому $\operatorname{End}_A V$ состоит из матриц перестановочных с $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Из равенства

$$\begin{pmatrix} a_1 & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & b \\ c & d \end{pmatrix}$$

следует, что $b = -c$, $a_1 = d$.

Таким образом,

$$\operatorname{End}_A V = \left\{ \begin{pmatrix} d & -c \\ c & d \end{pmatrix} \middle| \, d, c \in \mathbb{R} \right\} \cong \mathbb{C},$$

где $\mathbb{C} = \{a_1 + bi |\ a_1, b \in R,\ i^2 = -1\}$ – поле комплексных чисел.

Пример 1.5. Пусть $R = \mathbb{Z}$ и M – неприводимый $\mathbb{Z}$-модуль. Тогда, согласно предложению 1.5, $M \cong \mathbb{Z}/I$, где I – максимальный идеал $\mathbb{Z}$. Так как $I = (a)$, где $a \in \mathbb{Z}$, то a – простое число и $M \cong \mathbb{Z}_a$ – циклическая группа простого порядка.

1.2. Радикал Джекобсона

Пусть R – ассоциативное кольцо. *Радикалом Джекобсона* $J(R)$ кольца R называется множество элементов из R, аннулирующих все неприводимые R-модули, если они существуют, или само кольцо R, если неприводимых R-модулей не существует.

Другими словами, $J(R) = \cap A(M)$, где M пробегает все неприводимые R-модули или $J(R) = R$, если неприводимых R-модулей не существует. Заметим, что не каждое кольцо имеет неприводимые модули. Например, если R – нильпотентное кольцо (то есть, $R^n = 0$, для некоторого натурального числа n) и M – неприводимый R-модуль, то

$$M = MR = (MR)R = \cdots = MR^n = 0.$$

Противоречие доказывает, что нильпотентные кольца не имеют неприводимых модулей и, следовательно, совпадают со своими радикалами Джекобсона.

Из определения следует, что $J(R) \lhd R$.

Пример 1.6. Пусть $R = \mathbb{Z}$. Тогда множество неприводимых $\mathbb{Z}$-модулей совпадает с множеством циклических групп простого порядка. Заметим, что $\mathbb{Z}/(p)$ – $\mathbb{Z}$-модуль и его аннулятор $A(\mathbb{Z}/(p)) = p\mathbb{Z}$. Следовательно,

$$J(\mathbb{Z}) = \bigcap_{p \in \pi} (p) = (0),$$

где $\pi = \{2, 3, 5, \ldots\}$ – множество простых натуральных чисел.

Кольцо R называется *полупростым*, если $J(R) = 0$. В частности, кольцо целых чисел – полупростое кольцо. Если $R = J(R)$, то кольцо R называется *радикальным*. Ранее мы отмечали, что неприводимые R-модули исчерпываются с точностью до изоморфизма фактор-модулями R/I, где I пробегает множество всех модулярных максимальных правых идеалов. Ясно, что $A(R/I) = \{x \in R |\ Rx \subseteq I\}$. Это множество обозначается символом $(I : R)$. По определению $(I : R) \lhd R$. Так как I – модулярный правый идеал, то существует элемент $e \in R$ такой, что для любого элемента $a \in R$ выполнено $(a - ea) \in I$. В частности, если $x \in (I : R)$, то $x = (x - ex) + (ex) \in I$. Это доказывает, что $(I : R)$ – наибольший двусторонний идеал кольца R, содержащийся в I и

$$J(R) = \cap(I : R),$$

где I пробегает множество всех максимальных модулярных правых идеалов (если они существуют, иначе $J(R) = R$).

Предложение 1.6. *Если $T <_r R$ и T – модулярный, то T содержится в максимальном модулярном правом идеале.*

□ Рассмотрим множество

$$\mathcal{M} = \{K <_r R |\ T \subseteq K\}.$$

Это множество состоит из собственных модулярных правых идеалов и является частично упорядоченным по включению. Пусть e – такой элемент, что $(a - ea) \in T$ для любого элемента $a \in R$. Тогда $e \notin T$, $T \in \mathcal{M}$, и если $K_1 \subseteq K_2 \subseteq \ldots$ – цепь элементов $\mathcal{M}$, то $\cup K_i$ – правый модулярный идеал, содержащий T и не содержащий e, то есть $\cup K_i$ – верхняя грань в $\mathcal{M}$ для цепи $K_1 \subseteq K_2 \subseteq \ldots$. По лемме Цорна $\mathcal{M}$ содержит максимальный модулярный правый идеал, содержащий T. □

Предложение 1.7. *$J(R) = \cap I$, где I пробегает непустое множество $\mathcal{N}$ всех максимальных модулярных правых идеалов или $J(R) = R$, если $\mathcal{N}$ пусто.*

□ Так как $(I : R) \subseteq I$, то $J(R) = \cap(I : R) \subseteq \cap I = K$, где I пробегает множество $\mathcal{N}$ (предполагается, что $\mathcal{N}$ – непустое множество). Если $J(R) \neq K$, то существует неприводимый R-модуль M такой, что $MK \neq (0)$. Следовательно, $mK \neq (0)$ для некоторого элемента $m \in M$. Так как mK – подмодуль M, то $M = mK$ и $m = -ma$ для некоторого элемента $a \in K$. Рассмотрим правый идеал $\{x - (-a)x |\ x \in R\} = T$. Он является модулярным (по определению). Если $T \neq R$, то, согласно выше приведенному замечанию, T содержится в собственном максимальном модулярном правом идеале I_0, не содержащим $(-a)$. Так как $a \in K \subseteq I_0$, то получаем противоречие. Следовательно, $T = R$ и для некоторого элемента $b \in R$ справедливо равенство $b - (-a)b = -a$ или $a + b + ab = 0$. Откуда следует, что $m = m(-a) = m(b + ab) = mb + mab = mb - mb = 0$. Противоречие доказывает, что $J(R) = K = \cap I$. □

Следствие 1.1. *Для любого элемента $a \in J(R)$ существует такой элемент $b \in R$, что $a + b + ab = 0$.*

Элемент b называется *правым квазиобратным* для a, а сам элемент a называется *право-квазирегулярным*. Таким образом, $J(R)$ состоит из право-квазирегулярных элементов.

Правый идеал $K <_r R$ называется *правоквазирегулярным*, если каждый его элемент является правоквазирегулярным.

Предложение 1.8.

1. *$J(R)$ – правый право-квазирегулярный идеал, содержащий любой правый правоквазирегулярный идеал;*

2. *$J(R)$ – лево-квазирегулярный идеал.*

□ Пусть $K <_r R$ и каждый элемент из K имеет правый квазиобратный элемент. Если $K \not\subset J(R)$, то для некоторого неприводимого R-модуля M выполнено $MK \neq 0$ и, следовательно, существует элемент $m \in M$ такой, что $M = mK$, откуда следует, что $m = -ma$ для некоторого элемента $a \in K$. Пусть b – правый квазиобратный для a. Тогда $a + b + ab = 0$ и $m = -ma = m(b + ab) = mb - mb = 0$. Противоречие доказывает, что $K \subseteq J(R)$. Итак, $J(R)$ – максимальный правый право-квазирегулярный идеал.

Если $a \in J(R)$ и b – правый квазиобратный для a, то $b = -a - ab \in J(R)$. Пусть c – правый квазиобратный для b. Тогда $b+c+bc = 0$, $a+b+ab = 0$. Откуда следует, что $ab+ac+abc = 0$, $ac + bc + abc = 0$, $ab = bc$ и $a = c$. Таким образом, $ab = ba$ и b является левым квазиобратным элементом для a, то есть $J(R)$ – лево-квазирегулярный идеал R. □

В нашем определении радикала использовались правые R-модули. Аналогично можно определить радикал для левых R-модулей. Так как правый радикал Джекобсона является левоквазирегулярным, то он содержится в максимальном левоквазирегулярном идеале, совпадающим с левым радикалом.

Очевидно, что справедливо и обратное включение. Итак, правый радикал Джекобсона совпадает с левым радикалом и является максимальным квазирегулярным идеалом в кольце.

Предложение 1.9. *Если $I <_r R$ и I – ниль-кольцо, то $I \subseteq J(R)$.*

□ Действительно, пусть $a \in I$ и $a^n = 0,\ n \geq 1$. Тогда элемент

$$b = -a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1}$$

является квазиобратным для a. Следовательно, I – квазирегулярный правый идеал и по предложению 1.8 $I \subseteq J(R)$. □

Если R содержит единицу и b – квазиобратный к a, то

$$(1 + a)(1 + b) = (1 + b)(1 + a) = 1,$$

то есть, $1 + b = (1 + a)^{-1}$.

Если кольцо R является алгеброй над полем F, то есть R – векторное пространство над полем F и для любых элементов $x, y \in R$, $\alpha \in F$, $\alpha(xy) = (\alpha x)y = x(\alpha y)$, то радикал Джекобсона кольца R совпадает с радикалом Джекобсона алгебры R. Для доказательства этого замечания достаточно заметить, что каждый максимальный модулярный правый идеал I кольца R является подпространством. Действительно, если $F \cdot I \not\subset I$, то $R = F \cdot I + I$ и $R^2 \subseteq (F \cdot I + I) \cdot R \subseteq I \cdot R + I \cdot R \subseteq I$. Так как I – модулярный правый идеал, то $R \subseteq I$. Противоречие доказывает, что $F \cdot I = I$ и радикал кольца R совпадает с радикалом алгебры R.

Предложение 1.10. $J(R/J(R)) = 0$.

□ Предположим, что $J(R/J(R)) = K/J(R) \neq 0$. Тогда идеал K кольца R строго содержит $J(R)$. Докажем, что K – квазирегулярный идеал. Пусть $a \in K$. Так как $\bar{a} \in J(R/J(R))$, то существует такой элемент $\bar{b} \in \bar{R} = R/J(R)$, что $\bar{a} + \bar{b} + \bar{a}\bar{b} = \bar{0}$. Следовательно, $a + b + ab = c \in J(R)$. Пусть элемент $x \in R$ является квазиобратным к c. Тогда $(a+b+ab)+x+(a+b+ab)x =$

$a + (b + x + bx) + a(b + x + bx) = 0$. Таким образом, $(b + x + bx)$ – квазиобратный элемент для a. Итак, K – квазирегулярный идеал и $K \subseteq J(R)$. Противоречие доказывает утверждение. □

Другими словами, мы доказали, что $R/J(R)$ – полупростое кольцо.

Предложение 1.11. *Если R – полупростое кольцо и $A \lhd R$, то A – тоже полупростое кольцо.*

□ Пусть $J(A) \neq 0$. Рассмотрим правый идеал $T = J(A)R$. Так как $T^2 = J(A)(RJ(A)R) \subseteq J(A)A \subseteq J(A)$, то T^2 – правый квазирегулярный идеал кольца R. Следовательно, $T^2 \subseteq J(R) = (0)$. Так как нильпотентные односторонние идеалы содержатся в радикале (см. предложение 1.9), то $T = 0$. Рассмотрим левый аннулятор кольца R $l(R) = \{x \in R |\ xR = (0)\}$. Ясно, что $l(R) \lhd R$, $l(R)^2 = 0$ и $J(A) \subseteq l(R)$. Так как $l(R) \subseteq J(R)$ и $J(R) = (0)$, то $J(A) = (0)$. Противоречие. □

Предложение 1.12. *Пусть R – произвольное кольцо и $A \lhd R$. Тогда $J(A) = J(R) \cap A$.*

□ Докажем сначала, что $J(R) \cap A$ – квазирегулярный идеал в A. Действительно, если элемент $x \in J(R) \cap A \subseteq J(R)$, то существует элемент $y \in R$ такой, что $x+y+xy = 0$. Так как $y = -x - xy \in A$, то $J(R) \cap A$ – квазирегулярный идеал кольца A. Поэтому $J(R) \cap A \subseteq J(A)$. Рассмотрим фактор-кольцо $\bar{R} = R/J(R)$. В силу предложения 1.10 оно является полупростым и, следовательно, его идеал $\bar{A} = (A+J(R))/J(R)$ тоже является полупростым (см. предложение 1.11). Так как $\bar{A} \cong A/A \cap J(R)$ и $J(A)/A \cap J(R)$ – квазирегулярный идеал $A/A \cap J(R)$, то, по предложению 1.11, $J(A)/A \cap J(R) = \bar{0}$. Следовательно, $J(A) = A \cap J(R)$. □

Так как в кольце с единицей каждый правый идеал является модулярным, то радикал Джекобсона коммутативного кольца с единицей равен пересечению всех его максимальных идеалов.

Пример 1.7.

$$J(\mathbb{Z}) = \bigcap_p (p) = (0).$$

Если $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ – каноническое разложение числа n на простые множители p_i, то

$$J(\mathbb{Z}_n) = (\bar{p}_1) \cap (\bar{p}_2) \cdots \cap (\bar{p}_s) = (\overline{p_1 p_2 \dots p_s}).$$

Предложение 1.13. *Если R - конечномерная алгебра или конечное кольцо, то $J(R)$ – наибольший нильпотентный идеал.*

□ Пусть R – конечное кольцо (конечномерная алгебра над некоторым полем F). Рассмотрим цепь идеалов

$$J = J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq \dots$$

Ввиду конечности кольца R (конечномерности алгебры R соответственно) существует целое число $n \geq 1$ такое, что

$$T = J(R)^n = J(R)^{n+1} = \dots = J(R)^{2n} = \dots$$

Докажем, что $T = (0)$. Если $T \neq (0)$, то в множестве правых идеалов $\{I |\ I <_r R,\ I \subseteq J(R)^n,\ I \cdot J^n \neq 0\}$ существует правый идеал I_0 минимального порядка (минимальной размерности соответственно). Пусть $a \in I_0$ такой элемент, что $a \cdot J^n \neq 0$. Тогда $(aJ^n)J^n = aJ^{2n} = aJ^n \neq 0$ и $aJ^n \subseteq I_0 \subseteq J(R)^n$. Ввиду минимальности идеала I_0, получаем $a \cdot J^n = I_0$. Следовательно, существует такой элемент $x \in J^n$, что $ax = -a$. Пусть $y \in J$ квазиобратный элемент для x. Тогда

$$ax = a(-y - xy) = -ay + ay = 0$$

и $a = 0$. Противоречие доказывает, что $T = J(R)^n = 0$. □

Пусть, далее, R – произвольное кольцо. Рассмотрим множество

$$R^{\#} = R \times \mathbb{Z} = \{(a, n) |\ a \in R,\ n \in \mathbb{Z}\}$$

и определим на нем следующие операции:

$$(a,n)+(b,m)=(a+b,\ n+m),$$

$$(a,n)\cdot(b,m)=(ab+am+bn,\ n\cdot m).$$

Относительно этих операций $\langle R^{\#},+,\cdot\rangle$ является снова ассоциативным кольцом, содержащим единицу $\mathbf{1}=(0,1)$. Отображение $a\to(a,0)$ является инъективным гомоморфизмом кольца R в $R^{\#}$. Его образом является идеал I (который иногда отождествляют с R) такой, что $R^{\#}/I\cong\mathbb{Z}$.

Предложение 1.14. $J(R^{\#})=J(I)\cong J(R)$.

□ Так как $I=\{(a,0)|\ a\in R\}\lhd R^{\#}$, то по предложению 1.12 $J(I)=I\cap J(R^{\#})$. Так как $\mathbb{Z}\cong R^{\#}/I$ – полупростое кольцо, то образ $J(R^{\#})$ в $R^{\#}/I$ при естественном гомоморфизме равен $(\bar{0})$. Таким образом, $J(R^{\#})\subseteq I$ и $J(I)=J(R^{\#})\cong J(R)$. □

Заметим, что если y – квазиобратный элемент для $x\in R$, то равенство $x+y+xy=0$ в кольце R можно переписать в виде $(1+x)(1+y)=1$ (в кольце $R^{\#}$). Это бывает удобно в различных приложениях. Далее, в силу предложения 1.14, будем полагать, что R – кольцо с единицей.

Наша ближайшая цель - исследование кольца многочленов $R[t]$ над полупростым кольцом R и доказательство известной теоремы Амицура о его полупростоте.

Идеал P кольца R называется *простым*, если для любых идеалов A, B из R таких, что $AB\subseteq P$ следует, что либо $A\subseteq P$, либо $B\subseteq P$. В случае коммутативного кольца R это равносильно тому, что если $ab\in P$ для некоторых элементов $a,b\in R$, то либо $a\in P$, либо $b\in P$.

Лемма 1.1. *Пусть A – коммутативное кольцо и* $\operatorname{Spec}A$ *– множество всех его простых идеалов. Тогда множество N всех его нильпотентных элементов является идеалом и*

$$N=\bigcap_{P\in\operatorname{Spec}A}P.$$

□ Если $a \in N$, то $a^n = 0$ для некоторого целого числа $n \geq 1$. Пусть $P \in \operatorname{Spec} A$. Тогда $a^n \in P$ и, следовательно, $a \in P$, то есть $N \subseteq \bigcap\limits_{P \in \operatorname{Spec} A} P$. Пусть далее $\bigcap\limits_{P \in \operatorname{Spec} A} P \neq N$ и x – ненильпотентный элемент из $\bigcap\limits_{P \in \operatorname{Spec} A} P$. Рассмотрим множество идеалов

$$\mathfrak{M} = \{I \lhd A |\ I \cap \{x, x^2, \ldots\} = \varnothing\}.$$

Это множество содержит идеал (0), является частично упорядоченным по включению и удовлетворяет условию леммы Цорна. По лемме Цорна $\mathfrak{M}$ содержит максимальный идеал $Q \lhd A$. Покажем, что $Q \in \operatorname{Spec} A$. Пусть a, b – элементы кольца A такие, что $a \notin Q$, $b \notin Q$ и $ab \in Q$. Тогда идеалы $Q + (a)$, $Q + (b)$ строго содержат Q. Следовательно, существуют целые числа $i, j \geq 1$ такие, что $x^i \in Q + (a)$, $x^j \in Q + (b)$. Откуда следует, что $x^{i+j} \in (Q + (a))(Q + (b)) \subseteq Q$. Противоречие доказывает, что $Q \in \operatorname{Spec} A$ и $x \in Q$. Противоречие. Следовательно, $\bigcap\limits_{P \in \operatorname{Spec} A} P \subseteq N$. □

Лемма 1.2. *Пусть A – коммутативное кольцо с единицей и*

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in A[t].$$

Тогда $f(t)$ – обратимый элемент в $A[t]$ тогда и только тогда, когда a_0 – обратимый элемент в A и $\{a_1, \ldots, a_n\}$ – нильпотентные элементы в A.

□ Пусть для некоторых $c \in A$ и $k \in \mathbb{N}$ справедливы равенства $a_0 c = 1$ и $a_1^k = \cdots = a_n^k = 0$. Тогда

$$f(t) \cdot c = 1 + (a_1 c)t + \cdots + (a_n c)t^n$$

и подкольцо $T = \langle a_1 c, \ldots, a_n c \rangle$ нильпотентно, причем индекс нильпотентности не превышает nk. Рассмотрим многочлен

$$g(t) = (a_1 c)t + \cdots + (a_n c)t^n.$$

Так как $T^{nk} = 0$, то $g(t)^{nk} = 0$ и

$$(1+g)(1-g+g^2-\cdots+(-1)^{nk-1}g^{nk-1}) = 1.$$

Поэтому многочлен

$$c\cdot(1-g+g^2-\cdots+(-1)^{nk-1}g^{nk-1})$$

является обратным к $f(t)$.

Обратно, если $f(t)$ – обратимый многочлен, то a_0 – обратимый элемент в A и для любого простого идеала $P \lhd A$ многочлен

$$\bar{f}(t) = \bar{a}_0 + \bar{a}_1 t + \cdots + \bar{a}_n t^n$$

– обратимый элемент в области целостности $(R/P)[t]$. Следовательно, $\bar{a}_1 = \bar{a}_2 = \cdots = \bar{a}_n = 0$ и $\{a_1, \ldots, a_n\} \subseteq \bigcap\limits_{P\in \operatorname{Spec} A} P = N$. $\square$

Теорема 1.1 (С. Амицур).
Если кольцо R не содержит ненулевых ниль-идеалов и содержит единицу, то кольцо многочленов $R[t]$ является полупростым кольцом.

$\square$ Пусть R – кольцо без ненулевых ниль-идеалов. Предположим противное, пусть $J(R[t]) \neq (0)$. Выберем в радикале $J(R[t])$ ненулевой многочлен

$$f(t) = a_0 t^{n_0} + a_1 t^{n_1} + \cdots + a_k t^{n_k}$$

с минимальным числом ненулевых слагаемых $(n_0 < \cdots < n_k)$. Так как R содержит единицу, то, умножая $f(t)$ на t, мы можем считать, что $n_0 \geq 1$. Многочлен

$$[a_i, f] = [a_i, a_0]t^{n_0} + \ldots$$
$$\ldots + [a_i, a_{i-1}]t^{n_{i-1}} + [a_i, a_{i+1}]t^{n_{i+1}} + \ldots + [a_i, a_k]t^{n_k},$$

где $i \leq k$, принадлежит радикалу и содержит меньше слагаемых. Следовательно, коэффициенты $\{a_0, a_1, \ldots, a_k\}$ перестановочны между собой. Пусть

$$s(t) = \sum_{i=0}^{p} b_i t^i \in J(R[t])$$

является квазиобратным элементом для f. Тогда

$$s(t) = -f - fs = -f + f^2 + f^2 s = -f + f^2 - f^3 - f^3 s = \ldots$$
$$\cdots = -f + f^2 - \cdots + (-1)^{m+1} f^{m+1} + (-1)^{m+1} f^{m+1} s.$$

Так как нижняя степень f^{m+1} не менее $m+1$, то, выбирая число $m > \deg s(t)$, получим, что коэффициенты $\{b_0, b_1, \ldots, b_p\}$ принадлежат подкольцу $\langle 1, a_0, a_1, \ldots, a_k \rangle$ и $b_0 = 0$. Из равенства $(1+f)(1+s) = 1$ и леммы 1.2 следует, что $\{a_0, a_1, \ldots, a_k\}$ – нильпотентные элементы и

$$K = \{a \in R |\ at^{n_0} + a_1' t^{n_1} + \cdots + a_k' t^{n_k} \in J(R[t])\}$$

– ненулевой ниль-идеал R, содержащий a_0. Противоречие. □

Следующее предложение принадлежит С. Амицуру.

Предложение 1.15. *Пусть R – конечнопорожденная алгебра с единицей над несчетным полем k. Тогда $J(R)$ – ниль-идеал.*

□ Пусть $a \in J(R)$ и $\lambda \in k$. Тогда существует элемент $(1-\lambda a)^{-1}$. Так как R – счетномерное пространство над k, то множество элементов $\{(1-\lambda a)^{-1} |\ \lambda \in k\}$ является линейно зависимым. Тогда существуют ненулевые $\beta_1, \ldots, \beta_n, \lambda_1, \ldots, \lambda_n \in k$, такие, что

$$\beta_1 (1 - \lambda_1 a)^{-1} + \cdots + \beta_n (1 - \lambda_n a)^{-1} = 0.$$

Пусть

$$f(t) = (1 - \lambda_1 t) \cdot \ldots \cdot (1 - \lambda_n t) \in k[t].$$

Многочлен

$$g(t) = \beta_1 \cdot \frac{f(t)}{(1-\lambda_1 t)} + \cdots + \beta_n \cdot \frac{f(t)}{(1-\lambda_n t)} \neq 0,$$

так как при $t = \frac{1}{\lambda_1}$ он принимает ненулевое значение. Это означает, что $g(a) = 0$ и a – алгебраический элемент степени $\leq n-1$. Из равенства

$$a^q + \alpha_1 a^{q+1} + \cdots + \alpha_{n-1} a^{q+(n-1)} = 0,$$

где $\alpha_i \in k$, следует, что

$$a^q(1+b) = 0,$$

где

$$b = (\alpha_1 a + \cdots + \alpha_{n-1} a^{n-1-q}) \in J(R).$$

Умножая это равенство справа на $(1+b)^{-1}$, получим, что $a^q = 0$ (если же $q = 0$, то $1 \in J(A)$, что невозможно). Тем самым доказано, что $J(R)$ – ниль-идеал. $\square$

Пусть k – поле и G – группа. Рассмотрим векторное пространство $k(G)$ над полем k с базисом

$$\{v_g |\ g \in G\}.$$

Определим умножение на базисных элементах v_{g_1}, v_{g_2} по правилу

$$v_{g_1} \cdot v_{g_2} = v_{g_1 g_2}.$$

Множество $\langle k(G), +, \cdot \rangle$ является ассоциативной k-алгеброй, называемой *групповой алгеброй группы G над полем k*. Базисный элемент v_g принято отождествлять с самим элементом $g \in G$, то есть

$$k(G) = \left\{ \sum \alpha_g \cdot g \,\middle|\ g \in G,\ \alpha_g \in k \right\}.$$

Предложение 1.16. *Пусть G – некоторая группа. Тогда*

$$J(\mathbb{C}(G)) = 0.$$

□ Пусть $a = \sum \alpha_g \cdot g \in J(\mathbb{C}(G))$ и $a \neq 0$. Пусть H – подгруппа, порожденная конечным множеством $\operatorname{supp} a = \{g|\ \alpha_g \neq 0\}$ и

$$G = \bigcup_{i \in I} H x_i, \quad x_1 = 1.$$

Тогда

$$\mathbb{C}(G) = \sum_{i \in I} \mathbb{C}(H) x_i$$

– левый свободный $\mathbb{C}(H)$-модуль. $\mathbb{C}(H)$ является конечно порожденной алгеброй над несчетным полем $\mathbb{C}$. По предыдущей теореме $J(\mathbb{C}(H))$ – ниль-идеал.

Докажем, что $\alpha \in J(\mathbb{C}(H))$. Так как $\alpha \in J(\mathbb{C}(G)) \cap \mathbb{C}(H)$, то

$$\alpha + \beta + \alpha\beta = 0,$$

где $\beta = \beta_0 + \beta_1 \in J(\mathbb{C}(G))$ и $\beta_0 \in \mathbb{C}(H)$, $\beta_1 \in \sum\limits_{i \neq 1} \mathbb{C}(H) x_i$. Откуда следует, что

$$(\alpha + \beta_0 + \alpha\beta_0) + (\beta_1 + \alpha\beta_1) = 0,$$

$$\alpha + \beta_0 + \alpha\beta_0 = 0.$$

Значит, $J(\mathbb{C}(G)) \cap \mathbb{C}(H) \subseteq J(\mathbb{C}(H))$.

Рассмотрим отображение

$$* : \mathbb{C}(H) \to \mathbb{C}(H),$$

такое, что

$$\Big(\sum \beta_h \cdot h\Big)^* = \sum \bar{\beta}_h \cdot h^{-1}.$$

Тогда

$$(\beta + \gamma)^* = \beta^* + \gamma^* \quad \text{и} \quad (\beta\gamma)^* = \gamma^* \beta^*$$

для любых $\beta, \gamma \in \mathbb{C}(H)$.

Заметим, что

$$\beta = \alpha \cdot \alpha^* = \Big(\sum |\alpha_g|^2\Big) \cdot 1 + \sum_{h \neq 1} \beta_h \cdot h = \beta^* \in J(\mathbb{C}(H)).$$

Так как $\beta \neq 0$, то $\beta^2 = \beta \cdot \beta^* \neq 0 \in J(\mathbb{C}(H))$. Аналогично, $\beta^4 = \beta^2 \cdot \beta^2 = \beta^2 \cdot (\beta^2)^* \neq 0$ и т.д. Это противоречит тому, что $J(\mathbb{C}(H))$ – ниль-идеал. Следовательно, $J(\mathbb{C}(G)) = (0)$. $\square$

Пример 1.8 (В. Марков). Приведем пример конечнопорожденной алгебры R над счетным полем k, радикал Джекобсона $J(R)$ которой не является ниль-алгеброй (этот пример является ответом на старый вопрос С. Амицура, см. [6]) .

Пусть k – счетное или конечное поле и

$$N = \left\{ \frac{a(t) \cdot t}{b(t)} \in k(t) \middle| \, a(t), b(t) \in k[t], \ b(0) \neq 0 \right\}.$$

Тогда N – радикальная k-алгебра без делителей нуля, имеющая счетную размерность над k. Действительно, множество N имеет счетную мощность и, следовательно, размерность N над полем k является счетной. Если

$$r = \frac{a(t)t}{b(t)} \in N,$$

то

$$1 + r = \frac{b(t) + a(t)t}{b(t)}$$

и $(1 + r)(1 + s) = 1$, где

$$\frac{b(t)}{b(t) + a(t) \cdot t} - 1 = s \in N.$$

Это означает, что N – квазирегулярная алгебра.

Пусть $A = k\langle x, y\rangle$ – свободная ассоциативная алгебра с единицей и образующими x, y. Тогда

$$yA = k\langle y, \ yx, \ yx^2, \dots \rangle$$

– свободная счетнопорожденная алгебра. Существует сюръективный гомоморфизм $\varphi : yA \to N$ с ядром $B = \operatorname{Ker} \varphi \lhd yA$. Пусть

$$K = \sum_{i=0}^{\infty} x^i B^2 A.$$

Тогда $K \lhd A$ и

$$yA \cap K = B^2A = B(BA) \subseteq B(yA) \subseteq B.$$

Итак,

$$B^2 \subseteq yA \cap K \subseteq B.$$

Докажем, что алгебра $R = A/K$ является искомой. Она является 2-порожденной алгеброй с единицей. Рассмотрим ее правый идеал $\bar{y}R$. Так как

$$\bar{y}R = (yA + K)/K \cong yA/yA \cap K = yA/B^2A,$$

$$yA/B \cong N, \quad (B/B^2A)^2 = (\bar{0}),$$

то yA/B^2A – радикальная (в смысле радикала Джекобсона) алгебра, не являющаяся ниль-алгеброй. Следовательно, R – конечнопорожденная, счетномерная алгебра, имеющая ненулевой радикал Джекобсона $J(R)$, содержащий правый идеал $\bar{y}R$, не являющийся ниль-алгеброй.

Предложение 1.17. *Пусть $M_n(R)$ – полное кольцо матриц порядка n над кольцом R. Тогда*

$$J(M_n(R)) = M_n(J(R).$$

□ Докажем сначала включение $J(M_n(R)) \subseteq M_n(J(R))$. Пусть M – неприводимый правый R-модуль. Тогда модуль

$$M^{(n)} = \{(m_1, \ldots, m_n);\ m_i \in M\} = \underbrace{M \oplus \cdots \oplus M}_{n}$$

является неприводимым R_n-модулем и если $A = (a_{ij}) \in J(M_n(R))$, то $M^{(n)} \cdot A = 0$. Откуда следует, что $Ma_{ij} = 0$. Это означает, что $a_{ij} \in J(R)$ и $A \in M_n(J(R))$. Таким образом, $J(M_n(R)) \subseteq M_n(J(R))$.

Докажем обратное включение. Пусть

$$I_i = \left\{ \left(\begin{array}{cccc} 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{array} \right) \middle| \; a_{ij} \in J(R) \right\}.$$

Тогда $I_i <_r R_n$ и

$$M_n(J(R)) = I_1 + I_2 + \dots + I_n.$$

Докажем, что каждый правый идеал I_i, содержится в $J(M_n(R))$. Пусть

$$A = \left(\begin{array}{cccc} 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{array} \right) \in I_i.$$

Так как $a_{ii} \in J(R)$, то существует элемент $b \in J(R)$ такой, что $a_{ii} + b + a_{ii}b = 0$. Рассмотрим матрицу

$$B = \left(\begin{array}{ccccc} 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & b & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{array} \right)$$

из $M_n(J(R))$. Тогда

$$A + B + AB = \left(\begin{array}{ccccc} 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \dots & 0 & \dots & a_{in} \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{array} \right) = \gamma.$$

Так как $\gamma^2 = 0$, то $A + (B - \gamma + B(-\gamma)) + A(B - \gamma + B(-\gamma)) = \gamma - \gamma + B(-\gamma) - A\gamma + AB(-\gamma) = -(A + B + AB)\gamma = 0$. Итак, I_i – правый квазирегулярный идеал R_n. Следовательно, $I_i \subseteq J(M_n(R))$ и $M_n(J(R)) \subseteq J(M_n(R))$. □

Предложение 1.18. *Если R – алгебраическая алгебра над полем k, то есть каждый элемент $a \in R$ порождает конечномерную подалгебру $k[a]$, то $J(R)$ – ниль-алгебра.*

□ Пусть $a \in J(R)$. Из конечномерности алгебры $k[a]$ следует линейная зависимость векторов $\{a, a^2, a^3, \dots\} \subseteq k[a]$. Следовательно, существуют элементы $\lambda_i \in k$ такие, что

$$a^k = \lambda_1 a^{k+1} + \cdots + \lambda_m a^{k+m} = a^k b,$$

где $b \in J(R)$. Пусть c – квазиобратный элемент к $(-b)$. Тогда получаем $(-b) + c + (-b)c = 0$ и $a^k = a^k(c - bc) = a^k c - (a^k b)c = a^k c - a^k c = 0$. Итак, $J(R)$ – ниль-алгебра. □

Предложение 1.19. *Пусть K – коммутативная область целостности и ρ – простой идеал K. Рассмотрим в поле частных кольца K подкольцо*

$$K_\rho = \left\{ \frac{a}{b} \middle| \ b \notin \rho,\ a \in \rho \right\}.$$

Тогда $J(K_\rho) = K_\rho$.

□ Достаточно заметить, что квазиобратным к элементу $\frac{a}{b} \in K_\rho$ является элемент $\frac{(-a)}{a+b} \in K_\rho$. □

В 1964 г. польский математик Е. Сансяда построил пример простого радикального кольца, то есть кольца R с ненулевым умножением ($R^2 \neq 0$), не содержащего нетривиальных идеалов (отличных от нуля и R) и совпадающего с $J(R)$ (см. [71]).

В течение многих лет оставалась открытой проблема существования простого ниль-кольца. В 1969 г. профессор Ю. Рябухин доказал, что если такое кольцо существует, то существует и счетное простое ниль-кольцо (см. [57]). В 2002 г. польский

математик А. Смоктунович построила пример простого ниль кольца (см. [112]). Подробное изложение этого примера представлено в препринте [93].

Приведем в заключение следующие три нерешенные в настоящее время знаменитые проблемы, связанные с радикалом Джекобсона:

1. (С. Амицур). Если R – ниль-кольцо, то всегда ли кольцо многочленов $R[x]$ является радикальным кольцом?

2. (Н. Джекобсон). Если R – ниль-кольцо, то всегда ли кольцо матриц второго порядка над ним является ниль-кольцом?

3. (Д. Кете). Если R содержит правый ненулевой ниль-идеал, то всегда ли R содержит двусторонний ниль-идеал (ненулевой)?

Польский математик Ян Кремпа доказал (см. [89]), что утвердительное решение одной из проблем влечет утвердительное решение остальных двух проблем, то есть эти задачи эквивалентны.

В работе А. Смоктунович [113] построен пример ниль-алгебры R над счетным полем, для которой кольцо многочленов $R[x]$ не является ниль алгеброй.

1.3. Примитивные кольца

Пусть R – произвольное кольцо. Обозначим через R_a и L_b соответственно *операторы правого и левого умножения* кольца, то есть, такие отображения $R \to R$, что $xR_a = xa$ и $xL_b = bx$ для всякого $x \in R$.

Пусть R – алгебра над коммутативным кольцом k с единицей. Обозначим через

$$U(R) = \left\{ R_a + L_b + \sum R_{a_i} L_{b_i} \,\middle|\, a, b, a_i, b_i \in R \right\}$$

подкольцо в $\operatorname{End} R^+$, порожденное всеми операторами правого и левого умножения. $U(R)$ называется *алгеброй умножений* R. Ясно, что R является $U(R)$-модулем. Централизатор $\Gamma = \operatorname{End}_{U(R)} R$ этого модуля называется *центроидом* алгебры R.

Заметим следующие свойства центроида.

Предложение 1.20.

1. *R – левый Γ-модуль и если $\gamma \in \Gamma$, $x, y \in R$, то*

$$(xy)\gamma = (x)\gamma \cdot y = x \cdot (y)\gamma.$$

2. *Если R – точный k-модуль, то $k \subseteq \Gamma$.*

3. *Если $R^2 = R$ или $r(R) = \{x \in R |\ Rx = 0\} = 0$, то Γ – коммутативное кольцо.*

4. *Если R – кольцо с единицей, то центроид совпадает с центром $Z(R)$.*

5. *Если R – простое кольцо, то R является точным правым неприводимым $U(R)$-модулем.*

□ Докажем пункт 3. Пусть $\gamma_1, \gamma_2 \in \Gamma$. Тогда

$$(xy)(\gamma_1\gamma_2) = ((xy)\gamma_1)\gamma_2 = (x \cdot (y)\gamma_1))\gamma_2 = (x)\gamma_2 \cdot (y)\gamma_1$$

$$(xy)(\gamma_2\gamma_1) = ((xy)\gamma_2)\gamma_1 = ((x)\gamma_2 \cdot y)\gamma_1 = (x)\gamma_2 \cdot (y)\gamma_1$$

и

$$(xy)[\gamma_1, \gamma_2] = 0.$$

Если $R^2 = R$, то $[\gamma_1, \gamma_2] = 0$ и Γ – коммутативное кольцо. Если $R^2 \neq R$, то из последнего равенства следует $x\,((y)[\gamma_1, \gamma_2]) = 0$ и $(y)[\gamma_1, \gamma_2] \in r(R)$. Так как $r(R) = 0$, то $[\gamma_1, \gamma_2] = 0$.

Докажем пункт 4. Пусть $\gamma \in \Gamma$ и $c = \gamma(1)$, тогда

$$(x)\gamma = (1 \cdot x)\gamma = cx = (x \cdot 1)\gamma = x \cdot c$$

и $c \in Z(R)$. Отображение $\gamma \to \gamma(1)$ является изоморфизмом между Γ и $Z(R)$.

Докажем пункт 5. Согласно пункту 3, Γ – коммутативное кольцо. Так как подмодули $U(R)$-модуля R являются идеалами R, то R – неприводимый $U(R)$-модуль. В силу леммы Шура $\Gamma = \mathrm{End}_{U(R)} R$ – поле. Тогда кольцо R является точным неприводимым $U(R)$-модулем. $\square$

Кольцо R называется *примитивным* (справа), если оно обладает точным неприводимым правым R-модулем.

Примером примитивного кольца является кольцо умножений $U(S)$ простого кольца S. Другими примерами примитивных колец являются тела и полные матричные кольца конечного порядка над телами, так как они изоморфны кольцам всех линейных преобразований конечномерных векторных пространств над телами. Именно, если V – n-мерное векторное пространство над телом D, то V – точный неприводимый модуль над кольцом $\mathrm{End}_D V$, которое изоморфно $M_n(D)$. Если M – неприводимый правый R-модуль, то M изоморфен R/I, где I – максимальный модулярный правый идеал R. Аннулятором этого модуля является идеал $(I : R)$, являющийся максимальным двусторонним идеалом кольца R, содержащимся в I. Следовательно, M – точный неприводимый $R/(I : R)$-модуль и кольцо $R/(I : R)$ является правым примитивным кольцом.

Приведенная конструкция является самой общей для построения примитивных колец. В частности, кольцо R является примитивным (справа), если существует максимальный модулярный правый идеал $I <_r R$, не содержащий ненулевых двусторонних идеалов кольца R.

Если R – коммутативное кольцо с единицей, то оно является примитивным тогда и только тогда, когда не содержит собственных двусторонних идеалов, то есть является полем. В частности, кольца классов вычетов $\mathbb{Z}_n$, $n = 2, 3, \ldots$ являются примитивными, если n – простое число, а фактор-алгебра $k[x]/(p(x))$ кольца многочленов $k[x]$ над полем k является примитивным, если $p(x)$ – неприводимый многочлен.

Идеал $P \lhd R$ называется *примитивным*, если R/P – примитивное кольцо.

Ясно, что идеалы вида $(I : R)$, где I пробегает множество всех максимальных модулярных идеалов, и только они являются примитивными. Из определения следует, что радикал Джекобсона $J(R) = \cap(I : R)$ является пересечением всех примитивных идеалов. В частности, если R – примитивное (справа) кольцо, то для некоторого максимального модулярного правого идеала I_0 идеал $(I_0 : R) = 0$ и, следовательно, $J(R) = 0$. Это означает, что примитивное кольцо является полупростым. Заметим, что если S – простое кольцо, не являющееся радикальным, то S содержит элемент e, не имеющий квазиобратного. Следовательно, модулярный правый идеал $\{x - ex |\ x \in S\}$ является собственным и, следовательно, содержится в максимальном модулярном правом идеале I (по лемме Цорна). Так как S – простое кольцо, то $(I : S) = 0$ и S – примитивное кольцо. Итак, произвольное простое кольцо либо совпадает с радикалом Джекобсона, либо является примитивным. Заметим также, что в 1963 г. Дж. Бергман (Беркли, США) построил остроумный пример правого примитивного кольца, не являющегося левым примитивным кольцом (см. [67]).

Пусть V – векторное пространство над телом D и R – подкольцо $\mathrm{End}_D V$. R называется *плотным подкольцом линейных преобразований*, если для любого $n \geq 1$, любых линейно независимых векторов $u_1, \ldots, u_n \in V$ и любых векторов $v_1, \ldots, v_n \in V$ существует линейный оператор $a \in R$ такой, что

$$u_1 a = v_1,\ u_2 a = v_2,\ \ldots,\ u_n a = v_n.$$

Плотным подкольцом линейных преобразований является, например, само кольцо $\mathrm{End}_D V$. Заметим также, что если R – плотное подкольцо в $\mathrm{End}_D V$, то V – точный неприводимый R-модуль. Действительно, если $u, v \in V$, $u \neq 0$, то существует элемент $a \in R$ такой, что $ua = v$. Это означает, что $V = u \cdot R$ и V – неприводимый R-модуль. Точность модуля следует из включения $R \subseteq \mathrm{End}_D V$. Таким образом, плотные

подкольца в $\mathrm{End}_D V$ являются примитивными. Заметим далее, что если $\dim_D V = n < \infty$ и R – плотное подкольцо в $\mathrm{End}_D V \cong M_n(D)$, то $R = \mathrm{End}_D V$. Действительно, если $\varphi \in \mathrm{End}_D V$ и $\{e_1, \ldots, e_n\}$ – базис V, то существует элемент $a \in R$ такой, что $e_1\varphi = e_1 a, \ldots, e_n\varphi = e_n a$. Откуда следует, что $V(\varphi - a) = 0$ и $\varphi = a \in R$. Таким образом, в случае конечномерных пространств плотные подкольца в $\mathrm{End}_D V$ совпадают со всем кольцом линейных преобразований.

Теорема 1.2 (Джекобсон-Шевалле).
Пусть R – примитивное (справа) кольцо, M – точный неприводимый R-модуль и $D = \mathrm{End}_R M$. Тогда R – плотное кольцо линейных преобразований в $\mathrm{End}_D M$.

□ Сразу заметим, что по лемме Шура D – тело. Доказательство теоремы опирается на следующий важный факт, который мы и докажем сначала. Именно, если V – конечномерное подпространство M_D и $m \in M$, $m \notin V$, то существует элемент $a \in R$ такой, что $Va = 0$, $ma \neq 0$. Доказательство этого факта проведем методом математической индукции (по $\dim_D V$).

Если $V = (0)$, то утверждение следует из равенства $M = mR$.

Сделаем предположение индукции и рассмотрим равенство

$$V = V_0 + wD,$$

где $\dim_D V_0 = \dim V - 1$, $w \notin V_0$. Пусть

$$I = \{x \in R |\ V_0 x = 0\} <_r R.$$

Из предположения индукции следует, что если $v \in M$, $vI = 0$, то $v \in V_0$. В частности, $wI \neq 0$ и $wI \leq M$. Ввиду неприводимости модуля M, имеем $M = wI$. Допустим противное, то есть существует вектор $m \notin V$ такой, что из равенства $Vr = 0$, $r \in R$, следует $mr = 0$. Рассмотрим отображение

$$\tau : M \to M, \quad x\tau = ma,$$

если $x = wa$, $a \in I$. Оно корректно, так как, если $x = wa_1 = wa_2$, для некоторых $a_1, a_2 \in I$, то $w(a_1 - a_2) = 0$. Откуда следует, что $V(a_1 - a_2) = 0$ и $m(a_1 - a_2) = 0$. Поэтому $x\tau = ma_1 = ma_2$, то есть, τ – корректное отображение. Докажем, что $\tau \in \mathrm{End}_R M$. Действительно, имеем следующие равенства

$$(xr)\tau = ((wa)r)\tau = (w(ar))\tau = m(ar) = (ma)r = (x\tau)r.$$

Далее, для любого элемента $s \in I$

$$(m - w\tau)s = ms - (w\tau)s = ms - (ws)\tau = 0.$$

По предложению индукции получаем, что $m - w\tau \in V_0$ или $m \in V$. Противоречие доказывает наше вспомогательное утверждение.

Пусть $u_1, u_2, \ldots, u_n$ – линейно независимые векторы из M и $v_1, \ldots, v_n$ – произвольные векторы из M. Обозначим через V_i – подпространство, порожденное

$$\{u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n\}.$$

Тогда $u_i \notin V_i$ и существуют такие элементы $a_i \in R$, $i \leq n$, что

$$V_i a_i = 0, \ u_i a_i \neq 0.$$

Ввиду неприводимости модуля M справедливы равенства

$$M = u_i a_i R, \quad i \leq n.$$

Поэтому существуют элементы $b_i \in R$ такие, что

$$u_i a_i b_i = v_i, \quad i \leq n.$$

Тогда элемент

$$a = \sum_{i=1}^{n} a_i b_i \in R$$

является искомым, то есть $u_1 a = v_1, \ldots, u_n a = v_n$. $\square$

Следствие 1.2. *Если R – кольцо линейных преобразований векторного пространства V над телом $\triangle$ и R действует транзитивно на V, то есть для любых элементов $u, v \in V$, $u \neq 0$, существует элемент $a \in R$ такой, что $ua = v$, то R – примитивное кольцо. При этом V является неприводимым точным R-модулем с централизатором $D = \mathrm{End}_R V$, содержащим $\triangle$ в качестве подтела.*

Следствие 1.3. *Пусть R – примитивное кольцо, V – точный неприводимый правый R-модуль. Пусть $D = \mathrm{End}_R V$ и K – подтело, содержащее центр C тела D. Тогда*

$$R_K = \left\{ \sum a_i \alpha_i \,\middle|\, a_i \in R,\ \alpha_i \in K \right\}$$

– подкольцо $\mathrm{Hom}_{\mathbb{Z}}(V, V)$, порожденное R и K, является примитивным с точным неприводимым модулем V.

□ Если $v \in V$, $a_i \in R$, $\alpha_i \in K$, то положим

$$v \left(\sum a_i \alpha_i \right) = \sum (va_i)\, \alpha_i = \sum (v\alpha_i)\, a_i,$$

так как $a_i \alpha_i = \alpha_i a_i$. Учитывая $R \subseteq R_K$, получаем, что R_K – примитивное кольцо.

Пусть $\lambda \in \mathrm{End}_{R_K} V$. Тогда λ перестановочен с любым элементом из R. Следовательно, $\lambda \in D$. Пусть $\alpha \in K$. Тогда для любых элементов $v \in V$, $r \in R$ справедливы равенства

$$v\,([\lambda, \alpha] r) = v\,(\lambda\alpha)\, r - v\,(\alpha\lambda)\, r = (v\alpha r - v\alpha r)\lambda = 0,$$

$$V[\lambda, \alpha] R = 0.$$

Поэтому $[\lambda, \alpha] = 0$ и $\lambda \in K^*$, где

$$K^* = \{\tau \in D |\ \tau\alpha = \alpha\tau,\ \alpha \in K\}$$

– централизатор подтела K в теле D. Итак, $\mathrm{End}_{R_k} V = K^*$. В частности, если K – максимальное подполе в D, то $K^* = K$ и $\mathrm{End}_{R_k} V = K$. □

Следствие 1.4. *Пусть R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$, где D – тело и C – центр тела D. Пусть $a, b \in R$ такие, что*

$$axb = bxa,$$

для любого элемента $x \in R$. Тогда

$$b = \lambda a,$$

для некоторого $\lambda \in C$.

□ Приведем доказательство, принадлежащее Дж. Гонкалвесу и А. Манделе (г. Сан-Пауло, Бразилия). Мы можем считать, что $a \neq 0$. Выберем вектор $v \in V$ такой, что $va \neq 0$. Если векторы vb и va являются линейно независимыми, то по теореме плотности существует элемент $r \in R$ такой, что

$$vbr = v, \quad var = v.$$

Откуда следует, что

$$vbra = va = varb = vb.$$

Противоречие. Следовательно,

$$vb = (va)\lambda,$$

где $\lambda \in D$. Пусть $u \in V$. Тогда существует элемент $y \in R$ такой, что

$$(va)y = u$$

и

$$ub = vayb = vbya = va\lambda ya = (v(aya))\lambda = (ua)\lambda = u(a\lambda).$$

Поэтому $b = a\lambda$.

Докажем, что $\lambda \in C$. Если $\beta \in D$, то

$$va[\lambda, \beta] = va(\lambda\beta - \beta\lambda) = (vb)\beta - (v\beta)(a\lambda) = (vb)\beta - (v\beta)b = 0$$

и

$$[\lambda, \beta] = 0.$$

Таким образом, $\lambda \in C$. □

Следствие 1.5. *Пусть R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$, D – тело с центром C и F – максимальное подполе D. Если $\{\alpha_i\}$ – C-базис F, то каждый элемент примитивного кольца R_F может быть единственным образом выражен в виде $\sum a_i\alpha_i$, где $a_i \in RC$.*

□ Если

$$\sum_{i=1}^{k} a_i\alpha_i = 0$$

и число k является минимальным числом с этим свойством, то из равенства

$$a_k x\left(\sum_{i=1}^{k} a_i\alpha_i\right) - \left(\sum_{i=1}^{k} a_i\alpha_i\right) x a_k = \sum_{i=1}^{k-1} (a_k x a_i - a_i x a_k)\,\alpha_i = 0$$

следует, что

$$a_k x a_i = a_i x a_k$$

для любого элемента $x \in R$, $i \le k-1$. В силу предыдущего следствия $a_i = \lambda_i a_k$, $\lambda_i \in C$ и

$$\sum_{i=1}^{k} a_i\alpha_i = a_k(\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_{k-1}\alpha_{k-1} + \alpha_k) = 0.$$

Следовательно, $a_k = 0$, либо

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_{k-1}\alpha_{k-1} + \alpha_k = 0.$$

Противоречие. □

Следствие 1.6. *Пусть $R = RC$ – плотное кольцо линейных преобразований в $\mathrm{End}_D V$, где D – тело с центром C и максимальным подполем F. Если R_F содержит линейное преобразование конечного ранга в $\mathrm{End}_F V$, то $R = RC$ содержит преобразование конечного ранга в $\mathrm{End}_D V$ и $[D : F] < \infty$.*

□ Пусть $\{\alpha_i\}$ – C-базис поля F и пусть

$$\varphi = \sum_{i=1}^{k} r_i \alpha_i$$

– преобразование конечного ранга в R_F. Тогда $[V\varphi : F] < \infty$. Будем считать, что число k является минимальным. Для любого элемента $x \in R$ линейный оператор

$$r_k x\varphi - \varphi x r_k = \sum_{i=1}^{k-1} (r_k x r_i - r_i x r_k)\alpha_i$$

имеет конечный ранг, так как

$$V(r_k x\varphi - \varphi x r_k) \subseteq V\varphi + (V\varphi)xr_k.$$

Следовательно,

$$r_k x r_i = r_i x r_k,$$

$i \leq k-1$ и $r_i = \lambda_i r_k$, где $\lambda_i \in C$. Поэтому $\varphi = r_k \cdot \alpha$, где $\alpha \in F$. Откуда следует, что $V\varphi = (V\alpha)r_k = Vr_k$ и Vr_k – D-подпространство V. При этом размерность

$$[Vr_k : F] = [Vr_k : D] \cdot [D : F].$$

Следовательно, r_k – преобразование конечного ранга в R и $[D : F] < \infty$. Можно доказать, что условие $[D : F] < \infty$ влечет за собой конечномерность тела D над центром C. □

Теорема 1.3. *Пусть R – примитивное кольцо. Тогда существует тело D такое, что либо R изоморфно полному кольцу матриц $M_n(D)$, либо для любого натурального числа $m \geq 1$ кольцо $M_m(D)$ является гомоморфным образом некоторого подкольца кольца R.*

□ Пусть M – точный неприводимый правый R-модуль и $D = \mathrm{End}_R M$. Тогда D – тело и R – плотное кольцо в $\mathrm{End}_D M$. Если

$\dim_D M = n$ и $\{m_1, \dots, m_n\}$ – базис векторного D-пространства M, то для любого линейного преобразования $\varphi \in \mathrm{End}_D M$ существует элемент $a \in R$ такой, что

$$m_i a = m_i \varphi,$$

$i \leq n$. Следовательно, $m_i(a - \varphi) = 0$, $i \leq n$ и $\varphi = a \in R$. Это означает, что

$$R = \mathrm{End}_D M \cong M_n(D).$$

Пусть M – бесконечномерное D-пространство и $\{e_1, e_2, \dots\}$ – счетномерное линейно независимое подпространство в M. Рассмотрим векторное подпространство

$$V_m = e_1 D + \dots + e_m D$$

и множества

$$S = \{x \in R |\ V_m x \subseteq V_m\}, \quad I = \{x \in S |\ V_m x = 0\}.$$

Тогда $S \leq R$, $T \lhd S$ и, ввиду плотности кольца R, любой линейный оператор $\varphi \in \mathrm{End}_D V_m$ индуцируется некоторым элементом из S. Откуда следует, что

$$S/I \cong \mathrm{End}_D V_m \cong M_m(D).$$

□

Теорема 1.4. *Пусть R – примитивное кольцо. Тогда*

1. *если I – ненулевой идеал R, то I – примитивное кольцо;*
2. *если R не содержит ненулевых нильпотентных элементов, то R – кольцо без делителей нуля.*

□ Пусть M – точный неприводимый правый R-модуль и I – ненулевой идеал R. Тогда $MI \neq 0$ и, следовательно, $MI = M$.

Если K – I-подмодуль MI и $K \neq 0$, то $KI \neq 0$ и KI – R-модуль M. Поэтому $K = M$. Ясно, что $A(M) = 0$. Откуда следует, что M – точный неприводимый I-модуль.

Если R не содержит ненулевых нильпотентных элементов и a, b такие элементы в R, что $ab = 0$, то $(ba)^2 = b(ab)a = 0$. Откуда следует, что $ba = 0$ и $(xb)a = 0$ для любого элемента $x \in R$. Поэтому $axb = 0$ или $aRb = (0)$.

Обозначим через $(c) = \mathbb{Z}c + cR + Rc + RCR$ – идеал, порожденный элементом $c \in R$. Тогда из выше доказанного следует, что $(a)(b) = (0)$. Предполагая, что $a \neq 0$ и $b \neq 0$, получим, что

$$M = M(a) = M(a)(b) = (0).$$

Противоречие доказывает, что либо $a = 0$, либо $b = 0$, то есть R – кольцо без делителей нуля. $\square$

Пример 1.9 (Дж. Бергман).
Приведем ранее упоминавшийся пример правого примитивного кольца, не являющегося левым примитивным кольцом(см. [67]).

Пусть $S = \mathbb{Q}(x)$ – поле рациональных функций. Отображение $\alpha : S \to S$, переводящее произвольную дробь $r(x) \in S$ в $r(x^2)$, является гомоморфизмом поля S. При этом $\alpha(S) \not\ni x$. Рассмотрим кольцо косых многочленов

$$A = S[y;\ \alpha] = \left\{ \sum s_i y^i \,\middle|\, ys = \alpha(s)y,\ s \in S \right\}.$$

Кольцо A является областью (то есть кольцом без делителей нуля, содержащим единицу) главных левых идеалов. Действительно, если $L <_e A$ и $f(x) = s_0 + \cdots + s_n y^n$ – ненулевой многочлен из L минимальной степени, то для любого многочлена $g(x) = t_0 + \cdots + t_m y^m \in L$, $t_m \neq 0$ разность

$$g - t_m \cdot \alpha^{m-n}(s_n)^{-1} \cdot y^{m-n} \cdot f$$

содержится в L и имеет степень меньшую, чем g. Считая, что, по предположению индукции, все многочлены из L степени меньшей, чем m, содержатся в левом идеале Af, получаем, что $L = A \cdot f$.

Пусть n – нечетное число и $\Phi_n(x)$ – круговой многочлен степени $\varphi(n)$ ($\varphi(n)$ – функция Эйлера). Если $a(x) \in \mathbb{Z}[x]$ – многочлен, то $\nu_n(a(x))$ – наибольшая степень степень вхождения $\Phi_n(x)$ в разложение $a(x)$ на неприводимые множители.

Пусть $\frac{p(x)}{q(x)} \in Q(x)$. Положим

$$\nu_n\left(\frac{p(x)}{q(x)}\right) = \nu_n(p) - \nu_n(q).$$

Далее, для всякого элемента $a = \sum\limits_{i \in I} s_i y^i \in A$ положим

$$\nu_n(a) = \min\left\{\nu_n(s_i) |\ i \in I\right\}.$$

Пусть

$$R = \left\{a \in A |\ \nu_{2n-1}(a) \geq 0, n \in N\right\}.$$

Тогда R является правым примитивным кольцом, но не является левым примитивным кольцом.

Для доказательства этого утверждения докажем ряд лемм.

Лемма 1.3. *Пусть B – подкольцо A, содержащее x, y и являющееся $\mathbb{Q}$-алгеброй. Тогда B – правое примитивное кольцо.*

□ Для любого элемента $r(x) \in \mathbb{Q}(x)$ положим

$$r^*(x^2) = \frac{r(x) + r(-x)}{2}.$$

Определим на абелевой группе $\langle \mathbb{Q}(x), + \rangle$ структуру A-модуля следующим образом:

$$r \cdot y = r^*, \quad r \cdot a(x) = ra,$$

где $r(x), a(x) \in \mathbb{Q}(x)$. Для проверки аксиом модуля достаточно показать, что для любых элементов $a, b \in \mathbb{Q}(x)$ справедливо равенство

$$(a \cdot y) \cdot b(x) = a \cdot (y \cdot b(x)).$$

Имеем, что

$$(ay)b = a^*b, \quad a \cdot (y \cdot b) = a \cdot (\alpha(b) \cdot y) = (a\alpha(b)) \cdot y = (a\alpha(b))^*.$$

Итак, наше искомое равенство равносильно равенству

$$a^*b = (a\alpha(b))^*.$$

Имеем, что

$$\begin{aligned}(a^*b)(x^2) = a^*(x^2)b(x^2) = \\ = \tfrac{1}{2}\left[a(x) + a(-x)\right] \cdot b(x^2) = \tfrac{1}{2}\left[a(x)b(x^2) + a(-x)b((-x)^2)\right] = \\ = \tfrac{1}{2}\left[a(x)\alpha(b) + a(-x)\alpha(b(-x))\right] = \left[a\alpha(b)\right]^*(x^2).\end{aligned}$$

Следовательно, $a^*b = (a\alpha(b))^*$ и $\mathbb{Q}(x)$ – правый A-модуль.

Заметим, далее, что

$$x^n \cdot y^m = x^{\frac{n}{2^m}},$$

если $2^m | n$ и

$$x^n \cdot y^m = 0,$$

если $2^m \nmid n$. Пусть $M = xB \leq \mathbb{Q}(x)$. Покажем, что M – точный неприводимый B-модуль. Пусть $\frac{a(x)}{b(x)}$ – ненулевой элемент из M $(a(x), b(x) \in \mathbb{Q}[x])$, $n = \deg a(x)$ и m – такое натуральное число, что $n < 2^m$. Тогда

$$\frac{a(x)}{b(x)} \cdot \left(b(x) \cdot x^{2^m - n} \cdot y^m\right) = a(x) \cdot x^{2^m - n} \cdot y^m = cx,$$

где c – старший коэффициент $a(x)$. Таким образом, B – подмодуль в M, порожденный $\frac{a(x)}{b(x)}$, содержит x и, следовательно, совпадает с M. Это означает, что M – неприводимый B-модуль. Докажем, что M – точный B-модуль. Если

$$b = \sum_{i=0}^{k} q_i(x) y^i$$

– ненулевой элемент из B такой, что $Mb = (0)$, то, выбрав в $Q[x]$ такой многочлен $x \cdot p(x)$, что $s_i(x) = x \cdot p(x)q_i(x) \in \mathbb{Q}[x]$, получим ненулевой элемент

$$xp(x)b = \sum_{i=0}^{k} s_i(x)y^i \in B,$$

аннулирующий M и для каждого $s_i(x) \in \mathbb{Q}[x]$, $i \leq k$. Пусть j – наименьшее целое число такое , что $s_j \neq 0$ и

$$d = \max_i(\deg s_i(x) - \deg s_j(x)).$$

Выберем целое число n так, что $2^n \geq \deg s_j(x)$, $2^{n-j-1} > d$. Пусть $m = \deg s_j(x)$. Рассмотрим элемент

$$x^{2^n-m} \cdot \left(\sum_i s_i y^i\right).$$

В слагаемом $x^{2^n-m} \cdot s_j(x)$ наивысшая степень x равна x^{2^n}. Поэтому $x^{2^{n-j}}$ входит с ненулевым коэффициентом в слагаемое $x^{2^n-m} \cdot s_j(x)y^j$. Пусть $i > j$. Наивысшая степень x, входящая в $x^{2^n-m} \cdot s_i(x)$ не превосходит $2^n - m + \deg s_i(x) \leq 2^n + d$. Следовательно, степени переменной x, входящие в качестве слагаемых в $x^{2^n-m} \cdot s_i(x)y^i$, не превосходят числа

$$\frac{2^n + d}{2^i} \leq 2^{n-i} + d \leq 2^{n-j-1} + d \leq 2^{n-j-1} + 2^{n-j-1} \leq 2^{n-j}.$$

Другими словами,

$$x^{2^n-m}\left(\sum s_i(x)y^i\right) \neq 0$$

и

$$M\left(\sum s_i y^j\right) \neq (0).$$

Противоречие. $\square$.

Лемма 1.4. *Пусть n – нечетное число. Тогда для любого элемента $r(x) \in \mathbb{Q}(x)$*

$$\nu_n(r(x)) = \nu\left(r_n\left(x^2\right)\right).$$

□ Круговой многочлен $\Phi_n(x)$ является неприводимым в $\mathbb{Q}[x]$ и если многочлен $a(x) \in \mathbb{Q}[x]$ имеет общий корень с $\Phi_n[x]$, то $a(x)$ делится на $\Phi_n(x)$. Пусть

$$\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Тогда

$$\Phi_n(x) = \prod_{\substack{(i,n)=1\\1\le i\le n-1}} \left(x - \varepsilon^i\right)$$

и

$$\Phi_n(x^2) = \prod_{\substack{(i,n)=1\\1\le i\le n-1}} \left(x^2 - \varepsilon^{2i}\right) = \prod_{\substack{(i,n)=1\\1\le i\le n-1}} \left(x - \varepsilon^i\right)\left(x + \varepsilon^i\right).$$

Таким образом, $\pm\varepsilon^i$ – корни $\Phi_n(x^2)$ и $\Phi_n(x)$ – делитель $\Phi_n(x^2)$.

Далее,

$$\Phi_n(-x) = \prod_{\substack{(i,n)=1\\1\le i\le n-1}} \left(-x - \varepsilon^i\right) = (-x-\varepsilon) \prod_{\substack{(i,n)=1\\2\le i\le n-1}} \left(-x - \varepsilon^i\right)$$

– неприводимый многочлен, имеющий общий корень $(-\varepsilon)$ с $\Phi_n(x^2)$. Следовательно, $\Phi_n(-x)$ – делитель $\Phi_n(x^2)$ и, сравнивая степени $\Phi_n(x^2)$ и $\Phi_n(x)\Phi_n(-x)$, получаем, что

$$\Phi_n(x^2) = \Phi_n(x)\Phi_n(-x), \quad \nu\left(\Phi_n(x^2)\right) = \nu_n\left(\Phi_n(x)\right) = 1.$$

Далее, если $\left(\Phi_n(x), a(x)\right) = 1$, то $\left(\Phi_n(x), a(x^2)\right) = 1$. Поэтому для любого многочлена $a(x) \in \mathbb{Q}[x]$ имеем

$$\nu(a(x)) = \nu_n(a(x^2)),$$

а, следовательно, если $\frac{a(x)}{b(x)} \in \mathbb{Q}[x]$, то

$$\nu_n\left(\frac{a(x)}{b(x)}\right) = \left(\frac{a(x^2)}{b(x^2)}\right).$$

Что и требовалось доказать. □

Итак, докажем, что кольцо

$$R = \{a \in A|\ \nu_{2n-1}(a) \geq 0, n \in N\}$$

из примера 1.9 является правым примитивным кольцом, но не является левым примитивным кольцом.

□ Из леммы 1.4 следует, что

$$\nu_n(r(x)) = \nu(r(x^2)) = \nu_n(\alpha(r(x)))$$

для любого элемента $r(x) \in \mathbb{Q}[x]$ и нечетного числа $n \geq 1$. $\mathbb{Q}$ – алгебра R содержит x и y. По лемме 1.3 R – правое примитивное кольцо. Докажем, что R не является левым примитивным кольцом. Для этого достаточно показать, что любой максимальный левый идеал содержит ненулевой двусторонний идеал кольца R.

Пусть I – максимальный левый идеал кольца R. Рассмотрим левый идеал AI в кольце A. Если $AI = A$, то

$$1 = a_1 i_1 + \ldots + a_s i_s,$$

где $a_k \in A$, $i_k \in I$, $i \leq k$. Пусть $w \in \mathbb{Q}[x]$ такой ненулевой многочлен, что $\nu_n(wa_i) \geq 0$ для всех индексов $i \leq s$ и произвольного нечетного числа $n \geq 1$. Тогда $wa_i \in R$, $i \leq s$ и

$$w = \sum_{k=1}^{s} (wa_k)\, i_k \in RI \subseteq I.$$

В частности, $Rw \subseteq I$. Так как w – обратимый элемент в A и $\nu_n\left(w^{-1}\upsilon w\right) = \nu(\upsilon)$ для любого элемента $\upsilon \in A$, то $w^{-1}Rw = R$

и $Rw = wR$ – ненулевой двусторонний идеал кольца R, содержащийся в I. Если $AI \neq A$, то AI – левый главный идеал, порожденный, например, элементом

$$g = a_0(x) + a_1(x)y + \ldots + a_m(x)y^m,$$

где $m \geq 1$, $a_m(x) \neq 0$ (если $m = 0$, то I содержит обратимый элемент $a_0(x)$ и $AI = A$). Выберем нечетное число n так, чтобы $\nu_n(g) = \nu_n(a_m) = 0$. Для любого элемента

$$a = \sum_i b_i(x)y^i$$

обозначим через

$$\delta(a) = \max\{i|\ \nu_n(a) = \nu_n(b_i)\}.$$

Тогда для любых элементов $u, v \in A$ имеем

$$\delta(uv) = \delta(u) + \delta(v).$$

Так как $\nu_n(g) = 0$ и $\nu_n(a_m) = 0$, то $\delta(g) = m > 0$. Следовательно, для любого элемента $u \in AI = Ag(y)$ имеем $\delta(u) \geq \delta(g) > 0$. Многочлен $\Phi_n(x)$ является обратимым в A. Поэтому $\Phi_n(x) \in R$, $\Phi_n(x) \notin I$. Левый идеал I является максимальным в R. Следовательно, $R = I + R\Phi_n(x)$ и $1 = i + a \cdot \Phi_n(x)$ для некоторых элементов $i \in I$, $a \in R$. Откуда следует, что

$$\delta(i) = \delta(1 - a\Phi_n(x)) = 0 \geq m > 0.$$

Противоречие доказывает, что I содержит ненулевой двусторонний идеал и R не является левым примитивным кольцом. □

Пример 1.10. Ранее отмечалось, что в работе [71] построен пример простого радикального кольца. А именно, пусть $A = F\langle\langle x, y\rangle\rangle$ – кольцо формальных степенных рядов от некоммутативных переменных x, y и A' – подкольцо, состоящее из рядов с нулевым свободным членом. Пусть U – максимальный идеал, содержащий $(x - yx^2y)$ и не содержащий x. Пусть S – идеал в A'/U, порожденный $\overline{x}$. Тогда S – простое радикальное кольцо.

1.4. Подпрямые суммы колец и полупростые кольца

Пусть $\{R_i|\ i \in I\}$ – некоторое семейство колец и

$$R = \prod_{i\in I} R_i = \{f = (a_i)|\ a_i \in R_i\}$$

– множество всех функций $f : I \to \bigcup\limits_{i\in I} R_i$ таких, что $f(i) \in R_i$. Введем на R операции сложения и умножения, полагая

$$(a_i) + (b_i) = (a_i + b_i), \quad (a_i)(b_i) = (a_i b_i).$$

Множество $\langle R, +, \cdot\rangle$ является кольцом, называемым полной прямой суммой колец R_i (или прямым произведением колец R_i) и обозначается

$$R = \prod_{i\in I} R_i = \sum_c \bigoplus_{i\in I} R_i.$$

Пусть S – подкольцо $R = \prod\limits_{i\in I} R_i$ и для любого индекса $i \in I$ гомоморфизм $\pi : S \to R_i$ такой, что если $a = (a_i) \in S$, то $\pi_i(a) = a_i \in R_i$ является сюръективным. Тогда S называется *подпрямой суммой колец* R_i, $i \in I$ и обозначается

$$S = \sum\nolimits_s \bigoplus_{i\in I} R_i.$$

Пример 1.11. Пусть

$$S = \sum\nolimits_d \bigoplus_{i\in I} R_i = \left\{ (a_i) \in \prod_{i\in I} R_i \,\middle|\, a_i = 0 \right.$$

$$\left. \text{всюду, за исключением конечного числа индексов} \right\}$$

– дискретная прямая сумма колец R_i. Ясно, что S – подпрямая сумма колец R_i, $i \in I$.

Если $A \subseteq \prod\limits_{i\in I} R_i$ – подпрямая сумма колец R_i, $i \in I$ и

$$I_i = \operatorname{Ker} \pi_i \lhd A,$$

то

$$\bigcap_{i\in I} I_i = (0), \quad A/I_i \cong R_i.$$

Обратно, пусть в кольце A содержится семейство идеалов $\{I_k |\ k \in I\}$ такое, что $\bigcap\limits_{k\in I} I_k = (0)$. Тогда существует инъективный гомоморфизм

$$\varphi : A \to \prod_{k\in I} A/I_k$$

такой, что для любого элемента $x \in A$, $\varphi(x) = (x + I_k)$. Подкольцо $\varphi(A)$ является подпрямой суммой колец A/I_k, $k \in I$.

Пример 1.12. Пусть $A = \mathbb{Z}$ и $I = \{2, 3, 5, \ldots\}$ – множество положительных простых чисел. Тогда

$$A = \sum\nolimits_s \bigoplus_{p\in I} \mathbb{Z}/(p) = \sum\nolimits_s \bigoplus_{i\in\mathbb{N}} \mathbb{Z}/\left(q^i\right),$$

где q – фиксированное простое число.

Пусть $A = \sum_s \bigoplus\limits_{i\in I} R_i$ – подпрямая сумма колец R_i, $i \in I$. A называется *плотной подпрямой суммой*, если для любых элементов

$$a_{i_1} \in R_{i_1},\ a_{i_2} \in R_{i_1},\ \ldots,\ a_{i_k} \in R_{i_k},\quad i_s \neq i_t,\ \text{при } s \neq t,$$

существует элемент $a \in A$ такой, что

$$a = (\ldots, a_{i_1}, \ldots, a_{i_2}, \ldots, a_{i_k}, \ldots).$$

Приведем критерий того, что A – плотная подпрямая сумма. Пусть $A_i = \operatorname{Ker} \pi_i$, где $\pi_i : A \to R_i$ – гомоморфизм колец, такой, что если $x = (x_i) \in A$, то $\pi_i(x) = x_i \in R_i$.

Предложение 1.21. *A – плотная подпрямая сумма колец R_i, $i \in I$ тогда и только тогда, когда для любого подмножества $\{i_1, i_2, \dots i_k\} \subseteq I$*

$$A_{i_1} + \bigcap_{t=2}^{k} A_{i_t} = A.$$

□ Пусть A – плотная подпрямая сумма колец R_i, $i \in I$, $a = (a_i)$ – произвольный элемент A и $\{i_1, i_2, \dots, i_k\}$ – произвольное конечное множество I. В силу плотности существует такой элемент $b \in A$, что

$$b = (\dots, \underset{\uparrow\, i_1}{a_{i_1}}, \dots, \underset{\uparrow\, i_2}{0}, \dots, \underset{\uparrow\, i_k}{0}, \dots).$$

Это означает, что $b \in \bigcap_{t=2}^{k} A_{i_t}$ и $(a-b)(i_1) = 0$, то есть $(a - b) \in A_{i_1}$.

Таким образом, $a = (a - b) + b$, где $(a - b) \in A_{i_1}$, $b \in \bigcap_{t=2}^{k} A_{i_t}$, то есть

$$A = A_{i_1} + \bigcap_{t=2}^{k} A_{i_t}.$$

Для доказательства обратного утверждения достаточно доказать, что для любого подмножества $\{i_1, i_2, \dots, i_k\} \subseteq I$ и для любого элемента $a_{i_1} \in R_{i_1}$ существует элемент $a \in A$ такой, что

$$a = (\dots, \underset{\uparrow\, i_1}{a_{i_1}}, \dots, \underset{\uparrow\, i_2}{0}, \dots, \underset{\uparrow\, i_k}{0}, \dots).$$

Так как A – подпрямая сумма колец R_i, то существует элемент $b \in A$ такой, что

$$b = (\dots, \underset{\uparrow\, i_1}{a_{i_1}}, \dots).$$

По условию $A = A_{i_1} + \bigcap\limits_{t=2}^{k} A_{i_t}$. Следовательно, $b = x + y$, где $x \in \bigcap\limits_{t=2}^{k} A_{i_t}$ и $y \in A_{i_1}$. В частности, $(b - x)(i_1) = y(i_1) = 0$ и $x(i_1) = a_{i_1}$, $x(i_2) = 0$, …, $x(i_k) = 0$. □

Следствие 1.7. *Пусть A – подпрямая сумма колец R_i, $i \in I$ и $A_i = \operatorname{Ker} \pi_i$, где $\pi_i : A \to R_i$ – сюръективный гомоморфизм, такой, что если $a = (a_i) \in A$, то $\pi_i(a) = a_i$. Если для любых $i, j \in I$, $i \neq j$*

$$A_i + A_j = A \ и \ (A/A_i)^2 = A/A_i,$$

то A – плотная подпрямая сумма колец R_i, $i \in I$.

□ Для доказательства достаточно проверить равенство

$$A_{i_1} + \bigcap_{t=2}^{k} A_{i_t} = A,$$

где $\{i_1, \ldots, i_k\}$ – произвольное конечное подмножество I. Имеем, что

$$\begin{aligned} A = A^2 + A_{i_1} = (A^2 + A_{i_1})^2 + A_{i_1} = A^4 + A_{i_1} = \ldots \\ = A^k + A_{i_1} = (A_{i_2} + A_{i_1})(A_{i_3} + A_{i_1}) \ldots (A_{i_k} + A_{i_1}) + A_{i_1} = \\ = A_{i_1} + (A_{i_2} A_{i_3} \ldots A_{i_k}) = A_{i_1} + \bigcap_{t=2}^{k} A_{i_t}. \ \square \end{aligned}$$

В частности, если $\{A_i\}$ – множество различных максимальных идеалов и A содержит единицу, то A – плотная подпрямая сумма колец R_i.

Пусть R – произвольное ассоциативное кольцо, не совпадающее со своим радикалом Джекобсона. Тогда $J(R)$ является пересечением примитивных идеалов, то есть $J(R) = \bigcap (I : R)$,

где I пробегает множество максимальных правых модулярных идеалов. Рассмотрим отображение

$$\varphi : R/J(R) \to \prod_I R/(I:R),$$

$$\varphi(\bar{a}) = (\ldots, a + (I:R), \ldots).$$

Это отображение является мономорфизмом колец. Отождествляя кольцо $R/J(R)$ с его образом $\operatorname{Im}\varphi$, получаем, что $R/J(R)$ является подпрямой суммой примитивных колец $R/(I:R)$, где I пробегает множество максимальных модулярных правых идеалов. Таким образом, изучение произвольного полупростого кольца сводится (в известном смысле) к изучению примитивных колец и их подпрямых сумм. Иллюстрацией этого тезиса является следующее предложение.

Предложение 1.22. *Пусть R – ассоциативное кольцо, в котором для любого элемента $a \in R$ выполнено $a = a^3$. Тогда R – коммутативное кольцо.*

□ Пусть $a \in J(R)$. Тогда $a(1-a^2) = 0$ в кольце $R^{\#}$. Элемент $1-a^2$ имеет обратный элемент в $R^{\#}$. Умножая на него левую и правую часть предыдущего равенства, получим, что $a(1-a^2)(1-a^2)^{-1} = a = 0$. Таким образом, R – полупростое кольцо, являющееся подпрямой суммой примитивных колец S_i, $i \in \Omega$, каждое из которых удовлетворяет тождеству $x = x^3$. По теореме 1.3 кольцо S_i ($i \in \Omega$) либо изоморфно $M_n(D)$, либо для любого натурального числа m кольцо S_i содержит подкольцо T, чей гомоморфный образ изоморфен $M_m(D)$, где D – тело.

Если имеет место первый случай, то есть $S_i \cong M_n(D)$, то $n = 1$. Действительно, в противном случае матричная единица $e_{12}^2 = 0$ и $e_{12} = e_{12}^3 = 0$. Противоречие доказывает, что $S_i \cong D$ и для любого элемента $a \in D$ справедливо $a(a-1)(a+1) = 0$. Откуда следует, что S_i изоморфно одному из полей $GF(2)$, $GF(3)$.

Во втором случае, при $m = 2$ кольцо S_i содержит подкольцо T, гомоморфный образ которого изоморфен $M_2(D)$. Так как тождество $x - x^3 = 0$ переносится на гомоморфные образы, то $M_2(D)$ удовлетворяет этому тождеству. Выше мы показали, что это невозможно. Итак, R – подпрямая сумма полей $GF(2)$ и $GF(3)$ и, следовательно, R является коммутативным кольцом. $\square$

Пусть S – подмножество кольца R и

$$\ell(S) = \{x \in R | xS = \{0\}\}, \quad r(S) = \{x \in R | Sx = \{0\}\}.$$

Левый идеал $\ell(S)$ называется *левым аннулятором* подмножества S, а правый идеал $r(S)$ называется *правым аннулятором* подмножества S.

Предложение 1.23. *Пусть R – полупростое кольцо. Тогда*

1. *если $I \leq_r R$, то $J(I) = \ell(I) \cap I$;*
2. *если $I \leq_l R$, то $J(I) = r(I) \cap I$.*

$\square$ Так как $\ell(I) \cap I \lhd I$ и $(\ell(I) \cap I)^2 = (0)$, то $\ell(I) \cap I \subseteq J(I)$. Заметим, что $J(I) \cdot I \leq_r R$ и $J(I) \cdot I \subseteq J(I)$. Следовательно, $J(I) \cdot I$ – правый квазирегулярный идеал и $J(I) \cdot I \subseteq J(R)$. Так как $J(R) = (0)$, то $J(I) \cdot I = (0)$ и $J(I) \subseteq \ell(I) \cap I$.

Аналогично доказывается равенство $J(I) = r(I) \cap I$. $\square$

Пусть R – алгебра над коммутативным кольцом K с единицей, то есть $\langle R, + \rangle$ – унитарный K-модуль и для любых элементов $\alpha \in K$, $a, b \in R$

$$\alpha(ab) = (\alpha a)b = a(\alpha b).$$

Ранее мы заметили, что если R – алгебра над полем, то ее радикал как алгебры совпадает с радикалом кольца R. Ниже следующее предложение обобщает это утверждение для алгебр над коммутативным кольцом.

Предложение 1.24. *Пусть R – K-алгебра. Тогда множество модулярных максимальных правых идеалов в R как алгебре совпадает с множеством модулярных правых идеалов в R как кольце и радикал алгебры R совпадает с радикалом кольца R.*

□ Пусть I – максимальный модулярный правый идеал кольца R и $e \in R$ такой элемент, что $x - ex \in I$ для любого элемента $x \in R$. Пусть $\alpha \in K$. Если правый идеал αI не содержится в I, то, ввиду максимальности I, $I + \alpha I = R$ и $e = i_1 + \alpha i_2$, где $i_1, i_2 \in I$. Отсюда следует, что $e^2 = i_1 e + \alpha i_2 e = i_1 e + i_2(\alpha e) \in I$. Так как $e - e^2 \in I$, то $e \in I$ и $I = R$. Противоречие доказывает, что I – K-подалгебра R, то есть I – максимальный модулярный правый идеал в R как алгебры.

Обратно, пусть I – максимальный модулярный правый идеал R как алгебры. Используя лемму Цорна, получаем, что I содержится в максимальном модулярном правом идеале I' кольца R. Ранее, мы доказали, что I' – K-алгебра. Следовательно, $I' = I$. Так как радикал Джекобсона является пересечением всех максимальных модулярных правых идеалов, то радикал алгебры R совпадает с радикалом кольца R. □

Пусть R – алгебра над коммутативным кольцом K с единицей. Пусть $\mathfrak{M}$ – унитарный левый K-модуль и правый R-модуль такой, что

$$\alpha(ma) = (\alpha m)a = m(\alpha a)$$

для любых элементов $\alpha \in K$, $m \in \mathfrak{M}$, $a \in R$. Тогда $\mathfrak{M}$ называется *алгебра – R-модуль*.

Предложение 1.25. *Пусть R – алгебра над коммутативным кольцом K с единицей. Тогда*

1. *Каждый неприводимый алгебра – R-модуль является неприводимым R-модулем;*

2. *Каждый неприводимый R-модуль можно рассматривать единственным образом как неприводимый алгебра – R-модуль.*

□ Пусть $\mathfrak{M}$ – неприводимый алгебра – R-модуль и $m \neq 0$, $m \in \mathfrak{M}$. Тогда mR – ненулевой алгебра – R-модуль и, следовательно, $\mathfrak{M} = mR$, то есть $\mathfrak{M}$ – неприводимый R-модуль (по условию $\mathfrak{M}R \neq (0)$).

Пусть $\mathfrak{M}$ – неприводимый R-модуль. Тогда $\mathfrak{M} \cong R/I$, где I – максимальный модулярный правый идеал кольца R. В предложении 1.24 мы доказали, что I – K-подалгебра R и, следовательно, R/I – алгебра – R-модуль. Если K/I – его алгебра – R-модуль, то ввиду максимальности I, либо $K = I$, либо $K = R$, то есть R/I – неприводимый алгебра – R-модуль. □

Так как

$$\mathbb{Z} = \sum_s \bigoplus_{n \in \mathbb{Z}} \mathbb{Z}_n = \sum_s \bigoplus_p \mathbb{Z}_p,$$

где p пробегает множество всех простых чисел, то естественно изучить свойства многочленов $\mathbb{Z}[x]$ и их образов в $\mathbb{Z}_n[x]$, $\mathbb{Z}_p[x]$. Следующие примеры показывают, что некоторые свойства многочленов, выполнимые в $\mathbb{Z}_n[x]$ и $\mathbb{Z}_p[x]$ могут быть невыполнимы в $\mathbb{Z}[x]$.

Пример 1.13. Многочлен

$$f(x) = 6x^2 - 5x + 1 = (2x - 1)(3x - 1)$$

не имеет корней в кольце $\mathbb{Z}$. С другой стороны, если

$$n = 2^a(2b + 1),$$

то по китайской теореме об остатках существует целое число c такое, что

$$2c \equiv 1 \ (\mathrm{mod}\, 2^a), \quad 3c \equiv 1 \ (\mathrm{mod}(2b + 1)).$$

Следовательно, $\overline{c}$ – корень уравнения $\overline{f}(x) = \overline{6}x^2 - \overline{5}x + \overline{1}$ в кольце $\mathbb{Z}_n$.

Пример 1.14. Покажем существование многочлена $f(x)$, который является неприводимым в $\mathbb{Z}[x]$, но для любого целого

числа $n \geq 1$ его образ $\overline{f}(x)$ в $\mathbb{Z}_n[x]$ является приводимым многочленом. Для этого возьмем два различных нечетных простых числа p и q, таких, что символы Лежандра

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1, \quad p \equiv 1(\mathrm{mod}8), \quad q \equiv 1(\mathrm{mod}4),$$

например, $p = 49$, $q = 5$. Рассмотрим многочлен

$$\begin{aligned} f(x) &= (x^2 - p - q)^2 - 4pq = (x^2 - p + q)^2 - 4qx^2 = \\ &= (x^2 + p - q)^2 - 4px^2 = x^4 - 2(p+q)x^2 + (p-q)^2 = \\ &= (x - \sqrt{p} - \sqrt{q})(x - \sqrt{p} + \sqrt{q})(x + \sqrt{p} - \sqrt{q})(x + \sqrt{p} + \sqrt{q}) \end{aligned}$$

и докажем, что он искомый.

Ясно, что $f(x)$ – неприводимый многочлен в $\mathbb{Z}[x]$. Пусть

$$n = 2^a p_1^{a_1} \dots p_s^{a_s}$$

– каноническое разложение на простые множители числа n. Тогда

$$\mathbb{Z}_n = \mathbb{Z}_{2^a} \oplus \mathbb{Z}_{p_1^{a_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{a_s}}$$

и

$$\mathbb{Z}_n[x] \cong \mathbb{Z}_{2^a}[x] \oplus \mathbb{Z}_{p_1^{a_1}}[x] \oplus \dots \oplus \mathbb{Z}_{p_s^{a_s}}[x]$$

Следовательно, многочлен

$$\overline{f}(x) = (x^2 - \overline{p} - \overline{q})^2 - 4\overline{pq} \in \mathbb{Z}_n[x]$$

можно представит в виде

$$\overline{f}(x) = (f_0(x), f_1(x), \dots, f_s(x)),$$

где $f_0(x), f_1(x), \dots, f_s(x)$ – многочлены из

$$\mathbb{Z}_{2^a}[x], \ \mathbb{Z}_{p_1^{a_1}}[x], \ \dots, \ \mathbb{Z}_{p_s^{a_s}}[x]$$

соответственно. Для приводимости многочлена $\overline{f}(x)$ достаточно показать, что каждый многочлен $f_i(x)$ является приводимым.

Рассмотрим образ многочлена $f(x)$ в $\mathbb{Z}_{2^a}[x]$ и в $\mathbb{Z}_{p_s^{a_s}}[x]$. Докажем, что одно из чисел p, q или pq является квадратом в кольце коэффициентов (отсюда и будет следовать приводимость $\overline{f}(x)$).

Если $a \leq 2$, то

$$p \equiv q \equiv 1 \pmod{2^a}$$

и

$$\overline{p} = \overline{q} = 1^2$$

в $\mathbb{Z}_{2^a}$. Если $a \geq 3$, то

$$p \equiv \pm 5^{\nu} \pmod{2^a}.$$

Если $p \equiv -5^{\nu} \pmod{2^a}$, то $p \equiv -1 \pmod{4}$. Противоречие. Если $p \equiv 5^{2\beta+1} \pmod{2^a}$, то $p \equiv 5 \pmod{8}$. Противоречие. Следовательно,

$$p \equiv 5^{2\beta} \pmod{2^a}$$

и

$$\overline{p} = \left(\overline{5}^{\beta}\right)^2$$

в $\mathbb{Z}_{2^a}$.

Для дальнейших рассуждений нам понадобится следующая лемма.

Лемма 1.5. *Пусть p – простое число. Сравнение*

$$x^2 = v \pmod{p},$$

где p – простое число и $(v, p) = 1$, разрешимо в $\mathbb{Z}$ тогда и только тогда, когда для любого целого числа $m \geq 1$ сравнение

$$x^2 \equiv v \pmod{p^m}$$

разрешимо в $\mathbb{Z}$.

□ Достаточно показать, что если сравнение

$$x^2 \equiv v \pmod{p^m}$$

разрешимо, то сравнение

$$x^2 \equiv v \pmod{p^{m+1}}$$

также разрешимо. Пусть $x_0 \in \mathbb{Z}$ и $x_0^2 \equiv v \pmod{p^m}$. Положим $x = x_0 + p^m t$ и выберем t так, чтобы $x^2 \equiv v \pmod{p^{m+1}}$. Это можно сделать ввиду разрешимости сравнения

$$2tx_0 \equiv \frac{v - x_0^2}{p^m} \pmod{p},$$

p – нечетное простое число. □

Вернемся к примеру. Рассмотрим образы чисел $\overline{p}$ и $\overline{q}$ в $\mathbb{Z}_{p_i^{a_i}}$, $1 \leq i \leq s$. Если p и q – простые числа не равные p_i, то

$$p = g^u, \quad q = g^v \quad \text{и} \quad pq = g^{u+v},$$

где $\mathbb{Z}_{p_i}^* = \left\{\overline{1}, g, g^2, \ldots, g^{p_i-2}\right\}$. Одно из чисел u, v, $(u+v)$ является четным. Поэтому один из элементов $\overline{p}$, $\overline{q}$, $\overline{pq}$ является квадратом в $\mathbb{Z}_{p_i}$ и, по лемме, квадратом в $\mathbb{Z}_{p_i^{a_i}}$. Поэтому $\overline{f}(x)$ приводим в $\mathbb{Z}_{p_i^{a_i}}[x]$. Если, например, $p = p_i$, то в кольце $\mathbb{Z}_p[x]$

$$\overline{f}(x) = (x^2 - p - q)^2 - 4pq = (x^2 - q)^2.$$

Так как символ Лежандра $\left(\frac{q}{p}\right) = 1$, то $q = s^2$ в $\mathbb{Z}_p$ для некоторого элемента $s \in \mathbb{Z}_p$, $s \neq 0$. Следовательно,

$$\overline{f}(x) = (x^2 - s^2)^2 = (x - s)^2(x + s)^2$$

– произведение взаимно простых многочленов в $\mathbb{Z}_p[x]$. По лемме Гензеля (см. [5]), $\overline{f}(x)$ – приводимый многочлен в $\mathbb{Z}_{p_i^{a_i}}[x]$

1.5. Примитивные кольца с минимальными односторонними идеалами

В настоящем параграфе мы уточним строение примитивных колец, содержащих минимальные односторонние идеалы, а также изучим примитивные фактор-кольца односторонних идеалов примитивных колец.

Предложение 1.26. *Пусть R – правое примитивное кольцо, M – точный неприводимый R-модуль, $D = \mathrm{End}_R M$, $I \leq_r R$ и*

$$(0 : I) = \{m \in M \,|\, mi = 0 \text{ для любого элемента } i \in I\}.$$

Тогда $(0 : I)$ – D-подпространство M и для любых D-независимых по модулю $(0 : I)$ векторов $\{u_1, \ldots, u_n\}$ и для любых векторов $\{v_1, \ldots, v_n\}$ из M существует такой элемент $b \in I$, что $u_i b = v_i$, $i \leq n$.

□ Предположим, что для любого $i \leq n$ существует такой элемент $b_i \in I$, что $u_i b_i \neq 0$ и $u_j b_i = 0$, $j \neq i$. Тогда $u_i b_i R = M$, $i \leq n$ и существуют такие элементы $a_1, \ldots, a_n \in R$, что

$$u_1 b_1 a_1 = v_1, \ \ldots, \ u_n b_n a_n = v_n.$$

Положим

$$b = \sum_{i=1}^{n} b_i a_i \in I.$$

Тогда

$$u_1 b = v_1, \ldots, u_n b = v_n.$$

Докажем методом математической индукции существование таких элементов $b_1, b_2, \ \ldots, \ b_n$ из правого идеала I.

Если $n = 1$, то $u_1 I$ – ненулевой правый R-подмодуль M и, следовательно, $u_1 I = M$, то есть существует такой элемент $x \in I$, что $u_1 x = v_1$.

Сделаем предположение индукции и докажем наше утверждение для n линейно независимых по $\mathrm{mod}(0:I)$ элементов $\{u_1, u_2, \ldots, u_n\}$. Пусть

$$A = \{x \in I |\ u_1 x = u_2 = \ldots = u_{n-2}x = 0\} \leq_r R.$$

По предположению индукции и в силу неприводимости модуля M имеем, что $u_{n-1}A = M$. Пусть

$$B = \{x \in I |\ u_1 x = \ldots = u_{n-2}x = u_{n-1}x = 0\}.$$

Покажем, что $u_n B = M$. Предположим противное, то есть $u_n B \neq M$. Так как $B \leq_r R$, то $u_n B$ – правый R-подмодуль в неприводимом R-модуле M. Следовательно, $u_n B = (0)$.

Рассмотрим R-модульное отображение

$$\lambda : u_{n-1}A \to u_n A$$

(по предположению индукции $u_{n-1}A = u_n A = M$) такое, что

$$\lambda(u_{n-1}a) = u_n a.$$

Это отображение является корректным, так как если $u_{n-1}a = 0$, то $a \in B$ и, следовательно, $u_n a = 0$. Следовательно, $\lambda \in D$ и $(\lambda u_{n-1} - u_n)a = 0$ для любого элемента $a \in A$. По предположению индукции векторы $\{u_1, u_2, \ldots, u_{n-2}, \lambda u_{n-1} - u_n\}$ являются D-линейно независимыми. Противоречие. □

Предложение 1.27. *Пусть R – правое примитивное кольцо, M – точный неприводимый R-модуль, $I \leq_r R$. Тогда $I/J(I)$ – правое примитивное кольцо с точным неприводимым модулем $M/(0:I)$.*

□ В предложении 1.23 было доказано, что $J(I) = \ell(I) \cap I$. Рассмотрим I-модуль $M/(0:I) = M_1$. Если $x \in I$ аннулирует его, то $Mx \subseteq (0:I)$ и $M(xI) = (0)$, то есть $xI = (0)$ и $x \in J(I)$. Итак, M_1 – точный $I/J(I)$-модуль. Из предложения 1.26 следует, что он является неприводимым $I/J(I)$ - модулем. □

Предложение 1.28. *Пусть R – правое примитивное кольцо и $L \leq_l R$. Тогда $L/r_L(L)$ – правое примитивное кольцо, где $r_L(L) = r(L) \cap L$.*

□ Пусть M_R – точный неприводимый правый R-модуль, $D = \mathrm{End}_R M$ – тело. Положим

$$V = ML = \left\{ \sum_{i=1}^{k} m_i l_i \;\middle|\; m_i \in M, l_i \in L \right\}.$$

Тогда V – правый L-модуль и если элемент $a \in L$ удовлетворяет условию $Va = M(La) = (0)$, то $La = 0$ и $a \in r_L(L) = J(L)$ (см. предложение 1.23). Таким образом, V – точный $L/r_L(L)$-модуль. Докажем его неприводимость. Пусть x – произвольный ненулевой элемент из V и $y = \sum\limits_{i=1}^{k} m_i l_i$ – произвольный элемент из V. Тогда существуют элементы $a_i \in R$ такие, что $xa_i = m_i$, $i \leq k$. Следовательно,

$$x \left(\sum_{i=1}^{k} a_i l_i \right) = \sum_{i=1}^{k} (xa_i) l_i = \sum_{i=1}^{k} m_i l_i = y$$

и $\sum\limits_{i=1}^{k} a_i l_i \in L$, то есть V – точный неприводимый $L/r_L(L)$-модуль. □

Предложение 1.29. *Пусть V – левое векторное пространство над телом D. Тогда*

1. *Линейный оператор $e \in \mathrm{End}_D V$ является оператором проектирования (на некоторое подпространство) тогда и только тогда, когда $e = e^2$;*

2. *$\mathrm{End}_D V$ – регулярное кольцо, то есть для любого элемента $a \in \mathrm{End}_D V$ существует элемент $a \in \mathrm{End}_D V$ такой, что $a = aba$.*

□ Докажем 1. Ясно, что оператор проектирования является идемпотентом. Обратно, если $e = e^2 \in \mathrm{End}_D V$, то для любого вектора $u \in V$, $u = ue + u(1-e)$, $V = Ve \dot{+} (\mathrm{Ker}\, e)$ и e – оператор проектирования на подпространство (Ve).

Докажем 2. Пусть $a \in \mathrm{End}_D V$. Рассмотрим образ $\mathrm{Im}\, a = Va = \langle u_1, u_2, \ldots \rangle$ линейного оператора a, где $\{u_1, u_2, \ldots\}$ – базис Va. Тогда существуют $\{v_1, v_2, \ldots\} \subseteq V$ такие, что $v_i a = u_i$. Дополним $\{u_1, u_2, \ldots\}$ до базиса $\{u_1, u_2, \ldots, w_1, w_2, \ldots\}$ всего пространства V и рассмотрим линейное отображение $b : V \to V$ такое, что $u_i b = v_i$ и $w_j b = 0$. Из разложения

$$V = \langle v_1, v_2, \ldots \rangle \dot{+} \mathrm{Ker}\, a$$

следует, что $a = aba$. □

Предложение 1.30. *Пусть R – плотное подкольцо линейных преобразований в $\mathrm{End}_D V$, где V – левое векторное пространство над телом D и $a \in R$ – преобразование конечного ранга. Тогда существует такой элемент $b \in R$, что $a = aba$.*

□ По условию $Va = Du_1 + Du_2 + \ldots + Du_k$, где $\{u_1, \ldots, u_k\}$ – некоторый базис подпространства Va. Существуют векторы $\{v_1, \ldots, v_k\} \subseteq V$ такие, что $v_i a = u_i$, $i \leq k$. Векторы $\{u_1, \ldots, u_k\}$ являются линейно независимыми. Ввиду плотности R в $\mathrm{End}_D V$ существует элемент $b \in R$ такой, что

$$u_1 b = v_1,\ u_2 b = v_2,\ \ldots,\ u_k b = v_k.$$

Так как

$$V = (Dv_1 + \ldots + Dv_k) \oplus \mathrm{Ker}\, a,$$

то для любого вектора $w \in V$

$$w = \sum_{i=1}^{k} \lambda_i v_i + w_1,$$

где $w_1 \in \mathrm{Ker}\, a$ и

$$wa = \sum_{i=1}^{k} \lambda_i (v_i a_i) = \sum_{i=1}^{k} \lambda_i u_i = w(aba),$$

то есть $a = aba$. $\square$

Предложение 1.31. *Пусть R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$, где D – тело. Пусть также $0 \neq c^2 = e \in R$ и $\dim(Ve) = m < \infty$. Если U – произвольное конечномерное подпространство в V, то существует такой идемпотент $a^2 = a \in R$, что $a \in ReR$ и a – проектор V на U, то есть $Va = U$.*

$\square$ Пусть $U = Dv$ – одномерное подпространство в V. Если Ve имеет базис $\{u_1, \ldots, u_m\}$, то, ввиду плотности R, существует такой элемент $b \in R$, что $u_1 b = v$ и $u_2 b = \ldots = u_m b = 0$. Следовательно, $V(eb) = U$ и $eb = e \cdot e \cdot b \in ReR$. Если $\omega(eb) = v$, то, ввиду плотности R, существует такой $c \in R$, что $vc = \omega$. Следовательно, $v(ceb) = v$, где $ceb \in ReR$. Пусть $a = ceb \in R$. Тогда $a \in ReR$, $Va = Dv = U$, $va = v$ и для любого вектора $u \in V$ справедливо $ua = \lambda v = \lambda(va)$, где $\lambda \in D$. Отсюда следует, что $(u - \lambda v) \in \mathrm{Ker}\, a$, $V = Dv \oplus \mathrm{Ker}\, a$ и так как $ua^2 = (ua)a = (\lambda v)a = \lambda v = ua$, то $a = a^2$ – искомый элемент.

Воспользуемся далее методом математической индукции. Пусть

$$U = Dv_1 + \ldots + Dv_k,$$

где $\{v_1, \ldots, v_k\}$ – базис U. По предположению индукции существует идемпотент $f^2 = f \in ReR$ такой, что

$$Vf = Dv_1 + \ldots + Dv_{k-1} = W = Wf,$$

где f – проектор V на W. Так как $v_k f \in Vf = W$, то

$$v_k f = \sum_{i=1}^{k-1} \lambda_i v_i = \sum_{i=1}^{k-1} \lambda_i (v_i f) = \left(\sum_{i=1}^{k-1} \lambda_i v_i \right) f,$$

где $\lambda_i \in D$. Следовательно,

$$\left(v_k - \sum_{i=1}^{k-1} \lambda_i v_i \right) f = 0$$

и

$$U = Dv_1 + \ldots + Dv_{k-1} + Dz,$$

где

$$z = \left(v_k - \sum_{i=1}^{k-1} \lambda_i v_i \right) \in \operatorname{Ker} f.$$

Пусть $e_1^2 = e_1 \in ReR$ – проектор V на Dz, который существует в силу вышесказанного. Рассмотрим $g = e_1 + f - fe_1 \in ReR$. Тогда $ze_1 = z$, $zf = 0$, $zg = z$, $Vg = U$, $e_1 f = 0$ и $g^2 = g$, $g \in ReR$. □

Предложение 1.32. *Пусть R – плотное кольцо линейных преобразований в $\operatorname{End}_D V$ и все элементы из R имеют конечный ранг. Тогда R – простое регулярное кольцо.*

□ Пусть $I \lhd R$ и $I \neq (0)$. Пусть $a \in I$, а $\neq 0$. Тогда из предложения 1.30 следует, что существует $b \in R$ такой, что $a = aba$ Пусть $e = ab \in I$. Тогда $e^2 = (aba)b = ab = e \in I$, $e \neq 0$ и $\dim(Ve) < \infty$. Пусть x – произвольный элемент кольца R. Тогда $Vx = U$ – конечномерное подпространство и согласно предложению 1.31 существует проектор $a^2 = a \in ReR$ пространства V на $U = Vx$, то есть $Va = U = Vx$ и для любого элемента $u = vx \in U$ $ua = u$. Следовательно, $vx = v(xa)$ или $V(x - xa) = 0$. Отсюда $x = xa \in ReR \subseteq I$ и $R = I$. Регулярность кольца R следует из предложения 1.30. □

Предложение 1.33. *Пусть R – плотное кольцо линейных преобразований в $\operatorname{End}_D V$ и R содержит ненулевые преобразования конечного ранга. Обозначим через I множество всех преобразований конечного ранга кольца R. Тогда $I \lhd R$ и I – сердцевина кольца R, то есть I – наименьший ненулевой идеал кольца R. При этом I является простым регулярным кольцом.*

□ Заметим, что $I \lhd R$, $I \neq (0)$. Пусть K – ненулевой идеал R. Тогда $V(KI) = (VK)I = VI = V$ и KI – ненулевой идеал R,

содержащийся в $I \cap K$. В частности, он состоит из преобразований конечного ранга. Применяя предложение 1.32 к кольцу I (оно является примитивным кольцом с тем же неприводимым модулем V), получим, что $I = I \cap K \subseteq K$. Отсюда следует, что I – сердцевина кольца R, являющаяся простым регулярным кольцом. □

Предложение 1.34. *Пусть V – счетномерное векторное пространство над телом D. Тогда $\mathrm{End}_D V$ содержит единственный ненулевой собственный идеал A, состоящий из всех преобразований конечного ранга.*

□ Пусть $R = \mathrm{End}_D V$. Тогда R – плотное кольцо линейных преобразований. Если $I \lhd R$ и $I \neq (0)$, то согласно предложению 1.33 $I \supseteq A$. Если I состоит только из преобразований конечного ранга, то $I = A$. Пусть $a \in I$ и $\dim(Va) = \chi_0$. Так как R – регулярное кольцо, то $a = aba$ для некоторого элемента $b \in R$. Пусть $e = ba$. Тогда $e^2 = e$ и $Ve = Va$. Пусть $\{v_1, v_2, \ldots\}$ – базис Ve, $\{u_1, u_2, \ldots\}$ – базис V. Тогда существуют линейные преобразования $s, t \in \mathrm{End}_D V$ такие, что $u_i s = v_i$, $v_i t = u_i$, $i = 1, 2, \ldots$ и $(\mathrm{Ker}\, e)t = 0$. Следовательно, для любого числа i имеем, что

$$u_i(set) = (u_i s)et = (v_i e)t = v_i t = u_i,$$

то есть $set = 1 \in ReR \subseteq I$ и $I = R$. □

Предложение 1.35. *Пусть R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$ и R содержит преобразования конечного ранга. Тогда R содержит минимальный правый идеал.*

□ Пусть a – такой ненулевой элемент из R, что $\dim(Va) = m$, $m < \infty$. Если $Va = Dv_1 + \ldots + Dv_m$, то, ввиду плотности R, существует $b \in R$ такой, что $v_1 b = v_1$ и $v_2 b = \ldots = v_m b = 0$. Следовательно, $V(ab) = Dv_1$ и $c = ab \in R$. Согласно предложению 1.30 существует элемент $x \in R$ такой, что $c = cxc$. Пусть $e = xc \in R$. Тогда $e^2 = e$ и $Ve = Dv_1$. Докажем, что $I = eR$ –

минимальный правый идеал в R. Пусть $y = ex$ – ненулевой элемент в I. Тогда $Vy = (Ve)x = (Dv_1)x = D(v_1x)$ – одномерное подпространство в V. Ввиду плотности кольца R существует элемент $z \in R$ такой, что $(v_1x)z = v_1$. Следовательно, из равенств $v_1e = v_1$, $V = Ve \oplus V(1-e)$ следует, что $V(1-e)y = (0)$, $v_1(e-yz) = v_1 - v_1(yz) = v_1 - v_1(exz) = v_1 - (v_1x)z = v_1 - v_1 = 0$ и $V(e-yz) = (Ve)(e-yz) = (Dv_1)(e-yz) = 0$ и $e = yz \in yR$, то есть I – минимальный правый идеал. $\square$

Предложение 1.36. *Пусть R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$ и R содержит минимальный правый идеал $I \neq (0)$. Тогда R содержит преобразования конечного ранга.*

$\square$ Так как $I^2 \neq (0)$, то существует такой элемент $a \in I$, что $aI \neq (0)$ и, следовательно, $I = aI$. В частности, $a = ae$, где $e \in I$. Отсюда следует, что $a(e^2 - e) = 0$ и

$$(e^2 - e) \in \{x \in I |\ ax = 0\} \leq_r R.$$

Так как I – минимальный правый идеал, то $\{x \in I |\ ax = 0\} = 0$ и $e^2 = e$ – идемпотент, порождающий I, то есть $I = eR$. Предположим, что $\dim(Ve) = \infty$. Тогда $V = Ve \oplus V(1-e)$ и Ve имеет бесконечный базис $\{v_1, v_2, \ldots\}$, где $v_ie = v_i$, $i = 1, 2, \ldots$. Ввиду плотности кольца R существует элемент $a \in R$ такой, что $v_1a = v_1$ и $v_2a = 0$. Тогда $ea \in I$, $v_1(ea) = (v_1e)a = v_1a = v_1$, $v_2(ea) = v_2a = 0$ и $ea \in \{x \in I |\, v_2x = 0\} \leq_r R$. Так как $ea \neq 0$, то $I = \{x \in I |\, v_2x = 0\}$. В частности, $e \in I = \{x \in I |\, v_2x = 0\}$ и $v_2e = v_2 = 0$. Противоречие доказывает, что Ve – одномерное подпространство в V, если $I = eR$ – минимальный правый идеал и $e^2 = e$. $\square$

Из предложений 1.35, 1.36 следует важная теорема.

Теорема 1.5. *Правое примитивное кольцо R содержит минимальный правый идеал тогда и только тогда, когда R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$ (V – векторное пространство над телом D), содержащее преобразование конечного ранга.*

Кольцо R называется *полупервичным*, если оно не содержит ненулевых нильпотентных идеалов.

Предложение 1.37. *Пусть R – полупервичное кольцо и $e^2 = e$ – ненулевой идемпотент из R. Тогда eR – минимальный правый идеал тогда и только тогда, когда eRe – тело.*

□ Пусть eR – минимальный правый идеал. Заметим, что eRe содержит единицу e. Пусть $eae \neq 0$. Тогда $(eae)R \subseteq eR$ и $(eae)R \leq_r R$. Так как $(eae)R$ содержит $(eae)e = eae \neq 0$, то, ввиду минимальности eR, $(eae)R = eR$ и, следовательно, существует $x \in R$ такой, что $(eae)x = e$ или $(eae)(exe) = e^2 = e$, то есть для любого ненулевого элемента из eRe существует обратный (справа) элемент в eRe. В частности, существует eye такой, что $(exe)(eye) = e$. Откуда следует, что $(eae)(exe) = (exe)(eae) = e$ и eRe – тело.

Обратно, предположим, что eRe – тело и $ea \neq 0 \in eR$. Покажем, что $(ea)R = eR$. Так как R – полупервичное кольцо, то $(ea)R \neq 0$ и, более того, $(eaR)^2 \neq 0$. В частности, найдутся такие элементы $x, y \in R$, что $(eax)(eay) \neq 0$. Элемент $eaxe \neq 0$. Следовательно, существует такой элемент $eve \in eRe$, что $(eaxe)(eve) = e$, то есть $e \in (eaxe)R \subseteq (ea)R$, $eR \subseteq eaR \subseteq eR$ и $(ea)R = eR$. Откуда следует, что eR – минимальный правый идеал. □

Подкольцо S кольца R называется *квази-идеалом* в R, если $SR \cap RS \subseteq S$. Кольцо R называется *строго локально матричным кольцом* над кольцом D, содержащим единицу, если для любого конечного множества элементов $\{a_1, \ldots, a_n\} \subseteq R$ существует квази-идеал $S \subseteq R$ такой, что $\{a_1, \ldots, a_n\} \subseteq S$ и $S \cong M_n(D)$.

Примером квази-идеала может служить подкольцо eRe, где $e^2 = e \in R$. Заметим также, что если квази-идеал S имеет единицу $f = f^2$, то $S = fRf$. Действительно,

$$fRf = fR \cap Rf \subseteq SR \cap RS \subseteq S \subseteq fRf.$$

Это доказывает, что подкольцами вида eRe, где $e^2 = e \in R$ исчерпываются все квази-идеалы, содержащие единицу.

Предложение 1.38. *Пусть R – строго локально матричное кольцо над телом D. Тогда R – простое кольцо с минимальными правыми идеалами.*

□ Заметим, что R – простое кольцо. Действительно, если $I \lhd R$ и $a \neq 0 \in I$, то для любого элемента $0 \neq x \in R$ существует квази-идеал $S \leq R$ такой, что $\{a, x\} \subseteq S$ и $S \cong M_n(D)$. Рассмотрим пересечение $I \cap S$. Оно ненулевое (так как содержит a) и является идеалом в простом кольце S. Следовательно, $I \cap S = S$ и $x \in I$, то есть $I = R$.

Далее, R содержит ненулевые идемпотентные элементы. Поэтому $J(R) = 0$ и R – полупервичное кольцо. Возьмем некоторый квази-идеал $S \leq R$ и пусть e – его единица. Тогда

$$eRe = eR \cap Re \subseteq SR \cap RS \subseteq S \subseteq eRe,$$

то есть $S = eRe \cong M_n(D)$. Пусть s_0 – прообраз матричной единицы e_{11} при этом изоморфизме. Тогда

$$e_{11}M_n(D)e_{11} = D \cong s_0Ss_0 = (s_0e)R(es_0) = s_0Rs_0$$

– тело, так как $s_0^2 = s_0$ и $s_0e = es_0 = s_0$. Согласно предложению 1.37 s_0R – минимальный правый идеал. □

Предложение 1.39. *Пусть R – полупервичное кольцо и $e^2 = e$, $e \in R$, $e \neq 0$. Тогда eR – минимальный правый идеал тогда и только тогда, когда Re – минимальный левый идеал*

□ Доказательство следует из предложения 1.37.□

Следующая теорема принадлежит Литоффу и изложена, например, в книге [6]. Мы приведем более короткое доказательство, следуя статье [107].

Теорема 1.6. *Кольцо R – является простым кольцом с минимальными правыми идеалами тогда и только тогда, когда R – строго локально матричное кольцо над некоторым телом.*

В силу предложения 1.38, достаточно доказать, что каждое простое кольцо с минимальными правыми идеалами является строго локально матричным кольцом над телом. Для доказательства этого утверждения сначала докажем ряд вспомогательных предложений.

Предложение 1.40. *Пусть R – кольцо, содержащее минимальные правые идеалы. Пусть I – минимальный правый идеал и S – сумма всех минимальных правых идеалов, изоморфных I (как R-модули). Тогда $S \lhd R$ и S – прямая сумма минимальных правых идеалов, изоморфных I.*

□ Пусть $a \in R$. Рассмотрим правый идеал $aI \leq_r R$. Если он ненулевой, то отображение $\varphi : I \to aI$, $\varphi(i) = ai$, $i \in I$ является сюръективным R-модульным гомоморфизмом, ядро которого (в силу минимальности I) равно (0), то есть $I_R \cong aI_R$ (если $aI \neq (0)$). Таким образом, $S \lhd R$. По условию $S = \sum\limits_{\alpha \in A} I_\alpha$, где $I_\alpha \leq_r R$, $(I_\alpha)_R \cong I_R$. По лемме Цорна существует максимальное подмножество $B \subseteq A$ такое, что

$$\sum_{\beta \in B} I_\beta = \sum_{\beta \in B} \oplus I_\beta.$$

Покажем, что

$$S = \sum_{\beta \in B} \oplus I_\beta.$$

Иначе существует элемент $\alpha \in A$ такой, что $I_\alpha \nsubseteq \sum\limits_{\beta \in B} \oplus I_\beta$ и, следовательно,

$$I_\alpha \cap \left(\sum_{\beta \in B} \oplus I_\beta \right) = (0).$$

Отсюда $B' = B \cup \{\alpha\} \supsetneqq B$ и сумма $\sum\limits_{\beta \in B'} I_\beta$ – тоже является прямой. Противоречие. □

Предложение 1.41. *Пусть R – простое кольцо, содержащее минимальные правые идеалы. Тогда R – прямая сумма правых (левых) идеалов, изоморфных как R-модули.*

□ Доказательство следует из предложения 1.40 □

Предложение 1.42.

$$\mathrm{Hom}_R\,(eR, fR) \cong fRe$$

(как абелевы группы).

□ Действительно, если $\varphi \in \mathrm{Hom}_R(eR, fR)$ и $\varphi(e) = fa \in fR$, то для любого $x \in R$, $\varphi(ex) = \varphi(e(ex)) = \varphi(e)ex = (fae)x$. Рассмотрим отображение

$$\lambda : \mathrm{Hom}_R\,(eR, fR) \to fRe$$

такое, что $\lambda(\varphi) = fae$. Оно аддитивное и если $fae = 0$, то $\varphi = 0$, то есть является мономорфизмом. Докажем, что оно является сюръективным. Для этого рассмотрим произвольных элемент $fre \in fRe$ и рассмотрим отображение $\psi \in \mathrm{Hom}_R(eR, fR)$ $\psi(ex) = (fre)(ex) = (fre)x$ для любого элемента $x \in R$. Оно является корректным, то есть если $ex_1 = ex_2$, то

$$\psi\,(ex_1) = (fre)\,x_1 = fr\,(ex_2) = (fre)\,x_2 = \psi\,(ex_2)$$

и принадлежит $\mathrm{Hom}_R\,(eR, fR)$. □

Предложение 1.43. *Пусть $e^2 = e$, $f^2 = f$ – идемпотенты кольца R. Правые идеалы eR и fR изоморфны (как R-модули) тогда и только тогда, когда для некоторых элементов $u, v \in R$ $vu = e$, $uv = f$.*

□ Если $eR \cong fR$ (как R-модули), то по предложению 1.42 существует элемент $u = fae$, соответствующий изоморфизму $eR \to fR$ и элемент $v = ebf$, соответствующий обратному изоморфизму $fR \to eR$. Тогда

$$e \to (fae)e = u \to (ebf)u = vu = e$$

и

$$f \to (ebf) = v \to (fae)v = uv = f.$$

Обратно, допустим, что $vu = e$, $uv = f$. Тогда $ue = u(vu) = (uv)u = fu$, $vf = ev$ и отображения

$$ex \to uex = fux, \quad fy \to vfy = evy$$

– взаимно обратные изоморфизмы модулей eR и fR. □

Пусть R – простое кольцо, содержащее ненулевые минимальные правые идеалы.

Предложение 1.44. *Пусть $e^2 = e$, $f^2 = f$ и fR – минимальный правый идеал такой, что $fR \cap eR = (0)$. Тогда существует идемпотент $f' = (f')^2 \in R$ такой, что*

$$eR + fR = eR + f'R = (e + f')R$$

и $ef' = f'e = 0$. При этом $f'R \cong fR$ (как R-модули). В частности, $f'R$ – минимальный правый идеал.

□ Пусть

$$A = eR, \quad B = fR, \quad B_1 = (1 - e)B = (1 - e)fR.$$

Если $B_1 = (0)$, то для любого элемента $a \in R$, $fa - efa = 0$ и $fa = efa \in fR \cap eR = (0)$. Противоречие.

Далее

$$A + B_1 = \{ex + (1 - e)fy| \ x, y \in R\} = \\ = \{ex + fy| \ x, y \in R\} = A + B.$$

Отображение $b \to (1 - e)b$ является изоморфизмом R-модулей $B = fR$ и $B_1 = (1-e)B$. Следовательно, правый идеал B_1 является минимальным. Поэтому $B_1 = f_1R$, где $f_1 = (1 - e)b = f_1^2$, $b \in B$ (см. доказательство предложения 1.36 Заметим, что $ef_1 = 0$. Положим $f' = f_1(1 - e)$. Тогда $ef' = ef_1(1 - e) = 0$,

$f'e = 0$, $f'f_1 = f_1(1-e)f_1 = f_1^2 = f_1$, $(f')^2 = f_1(1-e)f_1(1-e) = f_1(1-e) = f'$ и $f_1 = f'f_1 \in f'R$. Откуда следует, что $f'R \subseteq f_1R \subseteq f'R$ и $B_1 = f'R$, где $f'e = ef' = 0$, $(f')^2 = f'$ и $B_1 = f'R$ – минимальный правый идеал, изоморфный fR такой, что $eR + fR = eR \oplus f'R$. Заметим, что $e + f' = e'$ – идемпотент и $A + B = eR \oplus f'R = (e + f')\,R = e'R$, где $(e')^2 = e'$. □

Предложение 1.45. *Пусть R – простое кольцо, содержащее ненулевые правые минимальные идеалы $e_1R, e_2R, \ldots, e_nR$ такие, что $e_i^2 = e_i$ и*

$$e_iR \cap \left(\sum_{j\neq i} e_jR\right) = (0),$$

$i \leq n$. Тогда существуют попарно ортогональные идемпотенты $f_1, \ldots, f_n \in R$ такие, что

$$f_iR \cong e_iR,$$

$$e_1R \dotplus \ldots \dotplus e_nR = f_1R \dotplus \ldots \dotplus f_nR.$$

□ Доказательство следует из предложения 1.44. □

Доказательство теоремы 1.6. Из предложений 1.41, 1.45 получаем, что для любого конечного множества $\{r_1, \ldots, r_n\} \subseteq R$ существуют попарно ортогональные идемпотенты $\{a_1, \ldots, a_k\}$ такие, что $\{r_1 \ldots, r_n\} \subseteq \bigoplus_{i=1}^{k} a_iR$ и $a_iR \cong eR$ (как R-модули), где $c^2 = e$ – фиксированный идемпотент такой, что eR – минимальный правый идеал R. Пусть $a = a_1 + a_2 + \ldots + a_k$. Тогда $a^2 = a$, $a_1R \oplus \ldots \oplus a_kR = aR$, $\{r_1 \ldots, r_n\} \subseteq aR$, $ar_i = r_i$, $i \leq n$. Аналогично существуют попарно ортогональные идемпотенты $b_1, \ldots, b_m$ такие, что $\{a, r_1, \ldots, r_n\} \subseteq \bigoplus_{i=1}^{m} Rb_i$, $Rb_i \cong Re$ (как R-модули). Пусть $b = b_1 + \ldots + b_m$. Тогда $b^2 = b$, $b_ib = bb_i = b_i$, $i \leq m$. Так как $a^2 = a$, то $Ra \cap R(1-a) = (0)$. Откуда следует, что

$$Rb = Ra \oplus R(b - ba).$$

Действительно, так как $a \in \bigoplus_{i=1}^{n} Rb_i = Rb$, то $ab = a$, $Rb \supseteq Ra$ и для любого $x \in R$, $xb = xba + x(b - ba) \in Ra \oplus Rb(1 - a) \subseteq Rb$, то есть $Ra \subseteq Rb$ и $Rb(1 - a) \subseteq Rb + Ra \subseteq Rb$, а значит, $Rb = Ra \oplus R(b - ba)$.

Пусть $c = b - ba$. Тогда

$$c^2 = b(1-a)b(1-a) = b(b-a)(1-a) = \\ = b\left(b - ba - a + a^2\right) = b - ba = c,$$

$$ca = b(1-a)a = 0, \quad ac = ab(1-a) = a(1-a) = 0.$$

Пусть $f = a + c = a + b - ba$. Тогда

$$f^2 = f, \quad af = a^2 + ab - aba = 2a - a = a, \quad fa = a^2 + ba - baa = a.$$

Далее $Rb = Ra \oplus Rc = Rf$ и, следовательно, $bf = b$, $fb = f$. Обозначим через $e_i = fb_i$, $i \leq m$. Тогда

$$e_1 + \ldots + e_m = f\left(b_1 + \ldots + b_m\right) = fb = f,$$

$$e_i e_j = fb_i fb_j = f(bb_i)fb_j = f(b_i b)fb_j = \\ = fb_i(bf)b_j = fb_i bb_j = fb_i b_j = \begin{cases} 0, & i \neq j; \\ fb_i = e_i, & i = j, \end{cases}$$

где $1 \leq i, j \leq m$. Далее, $b_i = bb_i = bfb_i = be_i$ и $Rb_i = Re_i \cong Re$ (как R-модули) для каждого $i \leq m$. Из предложения 1.43 следует, что существуют такие элементы s_i, t_i $(i = 1, 2, \ldots, m)$, что $e = s_i t_i$, $t_i s_i = e_i$, $s_i = es_i = s_i e_i$, $t_i = e_i t_i = t_i e$ для всех $i \leq m$. Далее, так как $\{a, r_1, \ldots, r_m\} \subseteq Rf$, то $ar_i = r_i$, $i \leq n$, $af = a$, $r_i f = r_i$, $fr_i = far_i = (fa)r_i = ar_i = r_i$ для всех $i \leq n$. Это означает, что $\{r_1, \ldots, r_n\} \subseteq fRf$. Покажем, что

$$fRf \cong M_m(eRe).$$

Так как eRe – тело, то отсюда и будет следовать наша теорема, ибо fRf – квази-идеал R.

Рассмотрим отображение $h : fRf \to M_m(eRe)$ такое, что для любого элемента $x \in R$,

$$fxf = \left(\sum_{i=1}^{m} e_i\right) x \left(\sum_{i=1}^{m} e_i\right) = \sum_{i,j=1}^{m} (e_i x e_j)$$

и $h(fxf) = (s_i x t_j) \in M_m(eRe)$, где $s_i x t_j = e s_i x t_j e \in eRe$, $1 \le i, j \le m$. Если $fxf = fyf$, то

$$s_i x t_j = e s_i x e_j t_j = s_i (e_i x e_j) t_j = s_i (e_i y e_j) t_j = s_i y t_j$$

и отображение h является корректным. Далее, легко видеть, что для любых элементов $x, y \in R$

$$h(fxf + fyf) = h(fxf) + h(fyf),$$

$$h\left((fxf)\cdot(fyf)\right) = h\left(f\,(xfy)\,f\right) = h\left(\sum_{i,j=1}^{m} e_i\,(xfy)\,e_j\right) =$$

$$= \left(s_i\,(xfy)\,t_j\right) = \left(s_i x \left(\sum_{k=1}^{m} e_k\right) y t_j\right) = \left(s_i x \left(\sum_{k=1}^{k} t_k s_k\right) y t_j\right) =$$

$$= \left(\left(\sum_{k=1}^{m} s_i x t_k \cdot s_k y t_j\right)\right) = (s_i x t_j)\cdot(s_i y t_j) = h\left(fxf\right) h\left(fyf\right).$$

Следовательно, h – гомоморфизм кольца fRf в кольце матриц $M_m(eRe)$. Если $h(fxf) = 0$, то матрица $(s_i x t_j) = 0$ и для любых индексов $1 \le i, j \le m$

$$s_i x t_j = 0, \quad t_i s_i x t_j s_j = e_i x e_j = 0, \quad fxf = \sum_{i,j=1}^{m} e_i x e_j = 0.$$

Таким образом, h – мономорфизм. Докажем, что h – сюръективное отображение. Пусть $A = (e x_{ij} e)$ – произвольная матрица из $M_m(eRe)$. Положим

$$x = \sum_{i,j=1}^{m} \left(t_i x_{ij} s_j\right).$$

Тогда $x \in fRf$ и $h(x) = (e x_{ij} e) = A$. $\square$

1.6. Основная теорема некоммутативной алгебры

В 1799 г. К. Гаусс в своей диссертации доказал так называемую "основную теорему (коммутативной) алгебры". Именно, он доказал, что произвольный многочлен $f(x) \in \mathbb{C}[x]$ ненулевой степени имеет комплексный корень, то есть существует число $\alpha \in \mathbb{C}$ такое, что $f(\alpha) = 0$. В то время под алгеброй понималась область математики, в которой изучались алгебраические уравнения, системы таких уравнений и методы их решения. Еще с XVI века были известны алгоритмы решения произвольных уравнений 3-й и 4-й степеней. Они были предложены итальянскими математиками Н. Тарталья, Д. Кардано и Л. Феррари и заключались в представлении корней многочленов степени не выше 4 через коэффициенты этих уравнений с помощью операций $+$, $-$, $\cdot$, $:$, $\sqrt[n]{}$. Выше приведенная теорема Гаусса дала новый толчок для исследования возможности "решения в радикалах" произвольного многочлена с комплексными коэффициентами. В результате в 20-х годах XIX века усилиями норвежского математика Н. Абеля и французского математика Э. Галуа было доказано, что такого алгоритма в общем случае не существует. В процессе этой работы были заложены основы современной алгебры как науки. Алгебра – область современной математики, в которой изучаются алгебраические системы, то есть множества с выделенными на них алгебраическими операциями и предикатами.

Вернемся к теореме Гаусса и переформулируем ее на языке линейных преобразований конечномерных векторных пространств.

Предложение 1.46. *Произвольный многочлен $f(x) \in \mathbb{C}[x]$ имеет комплексный корень тогда и только тогда, когда для любого конечномерного векторного пространства V над полем $\mathbb{C}$ и для любого линейного оператора $\varphi \in \mathrm{End}_{\mathbb{C}} V$ существует одномерное подпространство $W \subseteq V$ инвариантное относительно φ, то есть $\varphi(W) \subseteq W$.*

□ Пусть для любого конечномерного пространства V над полем $\mathbb{C}$ и для любого линейного оператора $\varphi \in \mathrm{End}_{\mathbb{C}} V$ существует собственный вектор $v \neq 0$. Следовательно, существует одномерное подпространство $W \leq V$, порожденное этим вектором, такое, что $\varphi(W) \subseteq W$. Возьмем любой многочлен

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \in \mathbb{C}[x].$$

где $n = \deg f(x) \geq 1$ и покажем существование числа $\alpha \in \mathbb{C}$, такого, что $f(\alpha) = 0$. Действительно, рассмотрим линейный оператор φ, который в некотором базисе имеет матрицу

$$[\varphi]_e = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \dots \\ \vdots & \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix}.$$

Тогда ее характеристический многочлен $|\lambda E - [\varphi]_e| = f(\lambda)$ и так как для φ существует ненулевой собственный вектор $v \in V$ с собственным значением $\alpha \in \mathbb{C}$, то $f(\alpha) = 0$.

Доказательство обратного утверждения аналогично. □

В такой формулировке теорема К. Гаусса имеет следующий некоммутативный аналог, доказанный в начале 1900 годов шотландским математиком У. Бернсайдом (1852–1927) и называемый в литературе "The fundamental theorem of noncommutative algebra".

Теорема 1.7 (У. Бернсайд).
Пусть V – n-мерное векторное пространство над полем комплексных чисел $\mathbb{C}$ и A – собственная подалгебра в $\mathrm{End}_{\mathbb{C}} V$ ($n \geq 2$). Тогда существует ненулевое собственное подпространство $W \subseteq V$ такое, что $AW \subseteq W$, то есть W инвариантно относительно действия любого оператора из A.

Теорема Гаусса следует из теоремы Бернсайда, если в качестве подалгебры $A = \mathbb{C}[\varphi]$ взять подалгебру, порожденную оператором $\varphi \in \mathrm{End}_{\mathbb{C}} V$.

Цель настоящей лекции – доказать теорему Бернсайда и вывести из нее многочисленные следствия, каждое из которых представляет собой "жемчужину"современной алгебры.

□ Предположим противное, то есть пусть в V нет ненулевых собственных подпространств, инвариантных относительно A. Возьмем произвольный ненулевой вектор $u \in V$. Если $Au = 0$, то одномерное пространство $\mathbb{C}u$ не совпадает с V (так как $\dim V \geq 2$) и инвариантно относительно A. Противоречие. Следовательно, $Au \neq (0)$ и $A(Au) = A^2u \subseteq Au$, то есть Au – инвариантное ненулевое подпространство. Следовательно, $V = Au$ (для любого вектора $u \neq 0$). В частности, для любых векторов $u \neq 0$, $v \in V$ существует преобразование $a \in A$ такое, что $au = v$. Таким образом, V – точный неприводимый левый A-модуль. По лемме Шура $\mathrm{End}_A V = D$ – алгебра с делением (тело), содержащее поле $\mathbb{C}$. Действительно, для любых $\alpha \in \mathbb{C}$, $a \in A$ и $v \in V$ имеем, что $\alpha(a(v)) = a(\alpha(v))$. V является левым векторным пространством над телом D и

$$[V : \mathbb{C}] = [V : D][D : \mathbb{C}] = n.$$

Отсюда следует, что D – конечномерное векторное пространство над полем $\mathbb{C}$. Пусть $m = \dim_{\mathbb{C}} D$ и $\alpha \in D$. Тогда векторы $\{1, \alpha, \alpha^2, \ldots, \alpha^m\}$ являются линейно зависимыми над полем $\mathbb{C}$ и, следовательно, существуют числа $a_0, a_1, \ldots, a_m \in \mathbb{C}$ (не все равные нулю) такие, что

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_m \cdot \alpha^m = 0.$$

Многочлен $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in \mathbb{C}[x]$ раскладывается на линейные множители (по теореме Гаусса):

$$f(x) = (x - \mu_1 \cdot 1) \cdot \cdots \cdot (x - \mu_m \cdot 1),$$

где $\mu_i \in \mathbb{C}$, $i \leq m$. Следовательно,

$$f(\alpha) = (\alpha - \mu_1 \cdot 1) \cdot \cdots \cdot (\alpha - \mu_m \cdot 1) = 0.$$

Если, например, $\alpha - \mu_1 \cdot 1 \neq 0$, то, умножая слева на $(\alpha - \mu_1 \cdot 1)^{-1}$, получим, что

$$(\alpha - \mu_2 \cdot 1) \cdot \dots \cdot (\alpha - \mu_m \cdot 1) = 0.$$

Рассуждая аналогично, мы докажем, что $\alpha = \mu_i \cdot 1$ для некоторого $i \leq m$, то есть $D = \mathbb{C}$. По теореме плотности Джекобсона–Шевалле A – плотное кольцо линейных преобразований в кольце $\operatorname{End}_D V = \operatorname{End}_{\mathbb{C}} V \cong M_n(\mathbb{C})$ и, следовательно, $A = \operatorname{End}_{\mathbb{C}} V$. Противоречие. $\square$

Это доказательство использует теорему плотности, поэтому приведем второе "элементарное"доказательство теоремы Бернсайда.

$\square$ Ранее мы заметили, что, рассуждая от противного, мы можем считать, что A действует транзитивно на V, то есть для любых векторов $u \neq 0$, $v \in V$ существует оператор $a_1 \in A$ такой, что $a_1 u = v$. Докажем, что A содержит преобразование ранга один. Действительно, пусть $a \in A$ – такой ненулевой линейный оператор, что $\dim(aV) = \operatorname{rank}(a)$ является наименьшим числом. Предположим, что $\operatorname{rank}(a) \geq 2$. Тогда существуют векторы $u, w \in V$ такие, что $\{au, aw\}$ – линейно независимые векторы. Так как A действует транзитивно на V, то существует элемент $b \in A$ такой, что $b(au) = w$. Отсюда следует, что $(aba)u = aw$ и au – линейно независимые векторы. Подпространство aV является инвариантным относительно ab (так как $(ab)(aV) = a(baV) \subseteq aV$). Следовательно, в aV существует вектор $av_0 \neq 0$, являющийся собственным для (ab), то есть $ab(av_0) = \lambda_0(av_0)$, где $\lambda_0 \in \mathbb{C}$. Отсюда следует, что $\operatorname{Ker}(aba - \lambda_0 a)$ строго содержит $\operatorname{Ker}(a)$, ибо $v_0 \in \operatorname{Ker}(aba - \lambda_0 a)$ и $\operatorname{Ker}(a) \not\ni v_0$. Это означает, что $\dim \operatorname{Ker}(aba - \lambda_0 a) > \dim \operatorname{Ker}(a)$ и $\dim \operatorname{Im}(aba - \lambda_0 a) \lneq \dim(\operatorname{Im}(a))$ и $(aba)u = aw = \lambda_0(au)$, то есть $\{aw, au\}$ – линейно зависимые векторы. Противоречие доказывает, что A содержит линейное преобразование ранга один.

Докажем далее, что все преобразования из $\operatorname{End}_{\mathbb{C}} V$ ранга один принадлежат A. Согласно предыдущему A содержит пре-

образование a ранга один. Тогда $aV = \mathbb{C}\cdot u$ и для любого вектора $x \in V$ $a(x) = \alpha(x)u$, где $\alpha(x) \in \mathbb{C}$. Заметим, что отображение $\alpha : V \to \mathbb{C}$, определенное по правилу $x \to \alpha(x)$ является линейным функционалом, то есть принадлежит линейному пространству V^* всех линейных функционалов. Далее, существует вектор $x_0 \in V$ такой, что $a(x_0) = u = \alpha(x_0)u$, то есть $\alpha(x_0) = 1$. Обозначим через

$$M = \{f \in V^* | \text{ существует } b \in A \text{ такой, что для любого вектора } x \in V,\ b(x) = f(x)u\}.$$

Ясно, что $0, \alpha \in M$ и $M \leq V^*$. Покажем, что $M = V^*$. Предположим, что $M \neq V^*$. Пусть $\{m_1, m_2, \ldots, m_k\}$ – базис M, где $k < n = \dim_{\mathbb{C}} V^*$. Мы знаем, что существуют векторы $\{a_1, \ldots, a_k\} \subseteq V$ такие, что для любого вектора $x \in V$, $m_i(x) = (x, a_i)$, $i \leq k$, где (x, y) – скалярное умножение в унитарном пространстве ${}_{\mathbb{C}}V$ [17, стр. 216]. Пусть c – ненулевой вектор из ортогонального дополнения к подпространству, натянутому на $\{a_1, \ldots, a_k\}$. Тогда $m_i(c) = 0$, $i \leq k$ и, следовательно, $m(c) = 0$ для любого функционала $m \in M$. Ввиду транзитивности, существует элемент $b \in A$ такой, что $bc = x_0$. Следовательно, $(ab)V = a(bV) \leq aV$ и $(ab)c = a(bc) = a(x_0) = u \neq 0$. Это означает, что (ab) – ненулевое преобразование ранга один, образ которого равен $\mathbb{C} \cdot u$. Поэтому найдется линейный функционал $\varphi \in M$ такой, что $(ab)(x) = \varphi(x)u$ для любого вектора $x \in V$. В частности, $\varphi(c) = 1$. Но с другой стороны, по выбору c $\varphi(c) = 0$. Противоречие. Это означает, что для любого функционала $\psi \in V^*$ отображение $x \to \psi(x)u$ принадлежит A.

Возьмем теперь любое преобразование ранга один $r \in \mathrm{End}_{\mathbb{C}} V$. По условию $rV = \mathbb{C} \cdot v$, где $v \in V$. Тогда для любого элемента $x \in V$ имеем, что $rx = f_0(x)v$, и существует такой элемент y, что $f_0(y) = 1$. Ввиду транзитивности существует элемент $s \in A$ такой, что $su = v$ и в силу ранее доказанного можно выбрать такой элемент $s_1 \in A$, что $s_1(x) = f_0(x)u$. Покажем, что $r = ss_1 \in A$. Имеем, что $r(x) = f_0(x)v$ и $ss_1(x) = s(s_1(x)) = s(f_0(x)u) = f_0(x)s(u) = f_0(x)v$. Следовательно, $r = ss_1 \in A$.

Итак, все преобразования ранга один из $\mathrm{End}_{\mathbb{C}} V$ принадлежат подалгебре A.

Покажем, что отсюда следует равенство $A = \mathrm{End}_{\mathbb{C}} V$. Для этого достаточно показать, что любое линейное преобразование в $\mathrm{End}_{\mathbb{C}} V$ раскладывается в сумму преобразований ранга один. Пусть $\varphi \in \mathrm{End}_{\mathbb{C}} V$ и φV имеет базис $\{v_1, \ldots, v_k\}$. Дополним его до базиса $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ всего пространства V и пусть $b_i : V \to V$ – такое линейное преобразование, что $b_i v_i = v_i$, $i \leq k$ и $b_i v_j = 0$ при $j \neq i$. Тогда $(b_i\varphi)V = \mathbb{C}v_i$, $\varphi = b_1\varphi + \cdots + b_k\varphi$ и $\mathrm{rank}(b_i\varphi) = 1$.

Второе доказательство разложения линейного преобразования в сумму преобразований ранга один следует из того, что каждая матрица $A_1 = (a_{ij}) \in \mathbb{C}_{n\times n}$ ранга r является суммой r матриц ранга один. Действительно, применяя элементарные преобразования к строкам и столбцам матрицы A_1, мы получим такие две невырожденные матрицы $U_1, U_2 \in \mathbb{C}_{n\times n}$, что

$$U_1 A_1 U_2 = \mathrm{diag}(\underbrace{1, 1, \ldots, 1}_{r}, \underbrace{0, 0, \ldots, 0}_{n-r}) = e_{11} + \cdots + e_{rr}.$$

Отсюда следует, что

$$A_1 = \left(U_1^{-1} e_{11} U_2^{-1}\right) + \cdots + \left(U_1^{-1} e_{rr} U_2^{-1}\right)$$

– сумма матриц ранга один. $\square$

Приведем некоторые следствия из теоремы Бернсайда. Каждое из них является важной теоремой в современной алгебре.

Следствие 1.8 (И. Шур). *Пусть A – коммутативная подалгебра в $\mathrm{End}_{\mathbb{C}} V$, где V – конечномерное пространство над полем $\mathbb{C}$. Тогда в пространстве V существует базис, в котором все элементы из A имеют верхнетреугольный вид.*

$\square$ По условию A – коммутативная подалгебра в $\mathrm{End}_{\mathbb{C}} V$. Пусть $n = \dim_{\mathbb{C}} V$. Доказательство проведем методом математической индукции по n. Если $n = 1$, то $\mathrm{End}_{\mathbb{C}} V = \mathbb{C}$ и наше утверждение очевидно. Если $n \geq 2$, то, учитывая, что

$\mathrm{End}_{\mathbb{C}} V$ – некоммутативная алгебра, имеем, что $A \neq \mathrm{End}_{\mathbb{C}} V$. Следовательно, по теореме Бернсайда при $n = 2$ существует одномерное подпространство $W \subseteq V$. Дополним базисный вектор w подпространства $W = \mathbb{C} \cdot w$ до до базиса $\{w, u\}$ всего пространства V. Тогда в этом базисе все элементы из A имеют верхнетреугольные матрицы, то есть A вложима в алгебру $\begin{pmatrix} \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{C} \end{pmatrix}$.

Пусть $n \geq 3$. По теореме Бернсайда существует собственное подпространство $W \subseteq V$ такое, что $AW \subseteq W$ и $W \neq (0)$, $W \neq V$. Представим $V = W \oplus W_1$ и пусть $e^2 = e$ – оператор проектирования V на W, то есть $W = eV$, $W_1 = (1-e)V = \mathrm{Ker}\, e$. Идемпотент $e \in \mathrm{End}_{\mathbb{C}} V$, вообще говоря, не принадлежит A. Рассмотрим пирсовское разложение произвольного элемента $a \in A$:

$$a = eae + ea(1-e) + (1-e)ae + (1-e)a(1-e).$$

Так как $aW = a(eV) \subseteq W = eV$, то $eae = ae$ и $(1-e)ae = 0$, то есть

$$a = eae + ea(1-e) + (1-e)a(1-e).$$

Подалгебры eAe, $(1-e)A(1-e)$ в $\mathrm{End}_{\mathbb{C}} V$ тоже являются коммутативными, при этом $W = eV$ инвариантно относительно действия (eAe), а $(1-e)V = W_1$ – инвариантно относительно действия $(1-e)A(1-e)$.

Так как $\dim W < n$, $\dim W_1 < n$, то по предположению индукции в W существует базис $\{f_1, \ldots, f_k\}$, относительно которого все элементы из (eAe) имеют верхнетреугольный вид, и в W_1 существует базис $\{f_{k+1}, \ldots, f_n\}$, относительно которого все элементы из $(1-e)A(1-e)$ тоже имеют верхнетреугольный вид. Нетрудно видеть, что $\{f_1, \ldots, f_k, f_{k+1}, \ldots, f_n\}$ – искомый базис для A, то есть в этом базисе все операторы из A имеют верхнетреугольный вид. $\square$

Следствие 1.9. *Пусть A – конечномерная ассоциативная ал-*

гебра над полем $\mathbb{C}$, удовлетворяющая тождеству

$$[x_1, x_2][x_3, x_4] \dots [x_{2n-1}, x_{2n}] = 0.$$

Тогда A вложима в алгебру верхнетреугольных матриц над полем $\mathbb{C}$ ($[x, y] = xy - yx$ – коммутатор элементов x, y).

□ Аналогично доказательству следствия 1.8. □

Следствие 1.10 (Д. Веддерберн). *Пусть A – конечномерная ассоциативная $\mathbb{C}$-алгебра, имеющая нильь-базис. Тогда A – нильпотентная алгебра.*

□ Пусть $A = \mathbb{C} \cdot a_1 + \dots + \mathbb{C} \cdot a_k$ – конечномерная $\mathbb{C}$-алгебра, имеющая базис $\{a_1, \dots, a_k\}$, где $a_1^{n_1} = \dots = a_k^{n_k} = 0$. Используя правое регулярное представление алгебры A, можно считать, что $A \subseteq M_n(\mathbb{C}) \cong \mathrm{End}_{\mathbb{C}} V$, где $n = \dim_{\mathbb{C}} V$. Для доказательства следствия воспользуемся методом математической индукции относительно числа n.

Если $n = 1$, то $A \subseteq \mathbb{C}$ и $A = (0)$. Сделаем предположение индукции о нильпотентности подалгебр с ниль-базисами, содержащихся в $\mathrm{End}_{\mathbb{C}} W$, если $\dim_{\mathbb{C}} W < n$. Докажем наше утверждение для $A \subseteq \mathrm{End}_{\mathbb{C}} V$, $n = \dim_{\mathbb{C}} V$. Если $A = \mathrm{End}_{\mathbb{C}} V$, то воспользуемся свойствами функции следа матрицы. Именно, если $a = (a_{ij}) \in M_n(\mathbb{C})$, то

$$\mathrm{tr}\,(a) = a_{11} + a_{22} + \dots + a_{nn} \in \mathbb{C}$$

– след матрицы a. Ясно, что

$$\mathrm{tr}\,(\alpha a + \beta b) = \alpha \mathrm{tr}\,(a) + \beta \mathrm{tr}\,(b)$$

для любых матриц a, b и любых чисел $\alpha, \beta \in \mathbb{C}$. При этом

$$\mathrm{tr}\,(ab) = \mathrm{tr}\,(ba)$$

и если b – невырожденная матрица, то

$$\mathrm{tr}\,(b^{-1}ab) = \mathrm{tr}\,(abb^{-1}) = \mathrm{tr}\,(a).$$

Отсюда следует (например, используя форму Жордана), что если a – нильпотентная матрица, то $\mathrm{tr}\,(a) = 0$. Так как A имеет ниль-базис, то $\mathrm{tr}\,(a) = 0$ для любого элемента $a \in A$. С другой стороны, $\mathrm{tr}\,(e_{11}) = 1$ и $e_{11} \in A$. Таким образом, A – собственная подалгебра в $\mathrm{End}_{\mathbb{C}} V$. По теореме Бернсайда существует собственное подпространство $W \subseteq V$ такое, что $AW \subseteq W$ и $W \neq (0)$. Пусть

$$C = \{x \in A |\ xW = (0)\} \lhd A \quad \text{и} \quad D = \{x \in A |\ xV \subseteq W\} \lhd A.$$

Тогда $A/C \subseteq \mathrm{End}_{\mathbb{C}} W$ и $A/D \subseteq \mathrm{End}_{\mathbb{C}} V/W$ и обе эти алгебры имеют ниль-базис. По предположению индукции $(A/D)^s = \overline{0}$ и $(A/C)^t = 0$ для некоторых целых чисел $s \geq 1$, $t \geq 1$. Следовательно, $A^s \subseteq D$ и $A^s V \subseteq W$, $A^t \subseteq C$ и $A^t W = (0)$, то есть $A^{s+t}V = A^t(A^s V) \subseteq A^t W = (0)$ и $A^{s+t} = (0)$. □

По поводу следующего следствия выдающийся математик Эмиль Артин писал: "this extraordinary result has excited the fantasy of every algebraist and still does so in our days".

Следствие 1.11 (Ф. Молин). *Пусть R – простая конечномерная $\mathbb{C}$-алгебра. Тогда $R = M_n(\mathbb{C})$.*

Следствие 1.12. *Пусть $\langle G, \cdot \rangle$ – ниль-полугруппа в $M_n(\mathbb{C})$ Тогда $G^N = 0$.*

□ Если $\langle G, \cdot \rangle$ – ниль-полугруппа в $\langle M_n(\mathbb{C}), \cdot \rangle$, то, рассмотрим ассоциативную подалгебру

$$A = \mathbb{C}\langle G \rangle = \left\{ \sum_{g \in G} \alpha_g \cdot g \,\middle|\, \alpha_g \in \mathbb{C} \right\},$$

порожденную элементами подгруппы G. Тогда A имеет ниль-базис. Далее достаточно воспользоваться следствием 1.10. □

Следствие 1.13 (У. Бернсайд). *Пусть G – группа матриц в $M_n(\mathbb{C})$, удовлетворяющая тождеству $x^N = 1$. Тогда G – конечная группа.*

□ Пусть G – группа матриц в $M_n(\mathbb{C})$, удовлетворяющая тождеству $x^N = E$, где $E = \operatorname{diag}(1, 1, \ldots, 1)$ – единичная матрица. Покажем, что G – конечная группа. Для этого рассмотрим подалгебру $\mathbb{C}(G) = A$, порожденную группой G. Доказательство проведем методом математической индукции относительно числа n.

Если $n = 1$, то $G \subseteq \mathbb{C}$ и

$$G \subseteq \mathbb{C}_N = \left\{ \alpha \in \mathbb{C} \,\middle|\, \alpha^N = 1 \right\} = \\ = \left\langle 1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{N-1} \,\middle|\, \varepsilon = \cos\frac{2\pi}{N} + i \sin\frac{2\pi}{N} \right\rangle$$

– конечная группа. Сделаем предположение индукции и докажем для групп $G \subseteq M_n(\mathbb{C})$. Если $A = M_n(\mathbb{C})$, то рассмотрим билинейную форму $(x, y) = \operatorname{tr}(xy)$ на A. Заметим, что для любых элементов $x, y, z \in A$ $(x, y) = (y, x)$ и $(xy, z) = (x, yz)$. Поэтому $I = \{a_1 \in A |\ (a_1, A) = 0\} \lhd A$. Так как A – простая алгебра, то $I = (0)$ или $I = A$. Если $I = A$, то $(1, A) = \operatorname{tr}(A) = \operatorname{tr}(1) = n \cdot 1 = 0$. Противоречие. Следовательно, $I = (0)$ и (x, y) – невырожденная билинейная форма. Пусть $a \in G$. Тогда $a^N = e$. Следовательно, все собственные значения оператора a являются корнями N-й степени из единицы, а $\operatorname{tr}(a)$ – сумма таких корней. Поэтому множество всех следов $\operatorname{tr}(G)$ является конечным.

Пусть $\{g_1, \ldots, g_{n^2}\} \subseteq G$ – базис алгебры $\mathbb{C}(G)$ и g – произвольный элемент из G. Тогда

$$g = \lambda_1 g_1 + \lambda_2 g_2 + \cdots + \lambda_{n^2} g_{n^2}$$

и

$$(g, g_1) = \lambda_1 (g_1, g_1) + \cdots + \lambda_{n^2} (g_{n^2}, g_1),$$
$$\vdots$$
$$(g, g_{n^2}) = \lambda_1 (g_1, g_{n^2}) + \cdots + \lambda_{n^2} (g_{n^2}, g_{n^2}).$$

Так как $\det((g_i, g_j)) \neq 0$ (ввиду невырожденности (x, y)) и (g_i, g_j), (g, g_i) принимают конечное множество значений, то (следует из правила Крамера) $\lambda_1, \lambda_2, \ldots, \lambda_{n^2}$ принимают конечное число возможных значений, то есть $|G| < \infty$.

Предположим далее, что $A \neq M_n(\mathbb{C})$. Тогда A – собственная подалгебра в $\mathrm{End}_{\mathbb{C}} V$ и, следовательно, по теореме Бернсайда существует собственное ненулевое подпространство $W \subsetneqq V$ такое, что $AW \subseteq W$. Выберем в W некоторый базис $\{f_1, \ldots, f_k\}$ и дополним его до базиса всего пространства $\{f_1, \ldots, f_k, \ldots, f_n\}$. В этом базисе каждый элемент $g \in G$ имеет следующий вид:

$$g = \begin{pmatrix} g_1 & a \\ 0 & g_2 \end{pmatrix},$$

где $g_1 \in M_n(\mathbb{C})$, $g_2 \in M_{n-k}(\mathbb{C})$. Обозначим через

$$G_1 = \{g_1\} \subseteq M_k(\mathbb{C}) \quad \text{и} \quad G_2 = \{g_2\} \subseteq M_{n-k}(\mathbb{C}).$$

Тогда G_1, G_2 – подгруппы в $M_n(\mathbb{C})$ и $M_{n-k}(\mathbb{C})$ соответственно, удовлетворяющие тождеству $x^N = e$. По предположению индукции они обе конечны.

Пусть

$$\begin{pmatrix} g_1 & a \\ 0 & g_2 \end{pmatrix}, \ \begin{pmatrix} g_1 & b \\ 0 & g_2 \end{pmatrix} \in G.$$

Тогда

$$c = \begin{pmatrix} g_1 & a \\ 0 & g_2 \end{pmatrix} \begin{pmatrix} g_1 & b \\ 0 & g_2 \end{pmatrix}^{-1} = \begin{pmatrix} g_1 & a \\ 0 & g_2 \end{pmatrix} \begin{pmatrix} g_1^{-1} & -g_1^{-1} b g_2^{-1} \\ 0 & g_2^{-1} \end{pmatrix} =$$
$$= \begin{pmatrix} E_k & (a-b)g_2^{-1} \\ 0 & E_{n-k} \end{pmatrix} \in G.$$

Так как $c^N = E$, то $(a-b) = 0$, то есть существует единственная матрица

$$\begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix} \in G$$

с фиксированными g_1, g_2. Поэтому G – конечная группа. $\square$

Используя аналогичные рассуждения можно доказать следующее следствие.

Следствие 1.14 (У. Бернсайд). *Пусть G – периодическая конечно порожденная группа матриц в $M_n(\mathbb{C})$. Тогда G – конечная группа.*

Последние два следствия опубликованы У. Бернсайдом в работе [68].

1.7. Строение артиновых колец

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

Аналогично можно ввести понятие кольца *артинова слева*. Заметим, что артиново справа кольцо может не быть артиновым слева. Примером тому служит кольцо матриц вида

$$\left\{ \left(\begin{array}{cc} \alpha & 0 \\ \beta & 0 \end{array} \right) \middle| \text{ где } \alpha, \beta - \text{ рациональные числа} \right\}.$$

Все результаты, доказанные ниже для артиновых справа колец, будут верны и для левоартиновых (для краткости слово "справа" будет опускаться и артиновы справа кольца будем называть артиновыми).

Легко показать (предоставим это читателю), что кольцо является артиновым тогда и только тогда, когда любая убывающая цепь правых идеалов

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots \supseteq I_m \supseteq \ldots$$

кольца R обрывается, то есть когда, начиная с некоторого номера n, все правые идеалы равны:

$$I_n = I_{n+1} = I_{n+2} = \ldots.$$

В этом случае говорят, что кольцо R удовлетворяет условию обрыва убывающих цепей правых идеалов.

Пример 1.15.

1. Любое тело артиново, так как оно не содержит нетривиальных правых идеалов.

2. Если R – артиново, то $M_n(R)$ – артиново.

3. Конечная прямая сумма артиновых колец – артиново кольцо.

4. Гомоморфный образ артинова кольца – артиново кольцо.

Предложение 1.47. *Если R – артиново кольцо, то $J(R)$ – нильпотентный идеал.*

□ Рассмотрим убывающую цепь идеалов

$$J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq \cdots \supseteq J(R)^n \supseteq \dots .$$

Пусть k – такое число, что

$$R' = J(R)^k = J(R)^{k+1} = \dots .$$

Докажем, что $J(R)^k = 0$. Предположим противное, пусть $J(R)^k \neq 0$. Положим

$$S = \left\{ I |\ I <_r R,\ I \subseteq R',\ IR' \neq 0 \right\}.$$

Так как $R' <_r R$, $R' \cdot R' = J^{2k}(R) = R' \neq 0$, то $S \ni R'$, то есть $S \neq \varnothing$. Следовательно, S содержит минимальный элемент I_m. Поскольку $I_m R' \neq 0$, то существует элемент $b \in I_m$ такой, что $bR' \neq 0$. Так как $bR' <_r R$ и $bR' \subseteq I_m$,

$$(bR')R' = b(J(R))^{2k} = bR' \neq 0,$$

значит $bR' \in S$. Откуда следует, ввиду минимальности I_m, что $bR' = I_m$. Поэтому существует элемент $x \in R'$ такой, что $b = -bx$. Если x' – квазиобратный элемент к x, то $0 = b + bx + (b + bx)x' = b + b(x + x' + xx') = b$, а это противоречит тому, что $bR' \neq 0$. Следовательно, $J^k(R) = 0$. □

А так как каждый односторонний ниль-идеал содержится в $J(R)$, то имеет место следствие.

Следствие 1.15. *Всякий односторонний ниль-идеал артинова кольца нильпотентен.*

Предложение 1.48. *Пусть R – такое кольцо, что для любого элемента $a \in R$ выполняется $a \in RaR$. Тогда идеалы матричного кольца $M_n(R)$ имеют вид $M_n(I)$, где I – некоторый идеал в R.*

□ Если $a \in R$, то через A_{pq} обозначим матрицу порядка $n \times n$ с элементом a на (p, q)-м месте и 0 в остальных местах. Пусть S – идеал в $M_n(R)$ и I – множество элементов из R, появляющихся в качестве компонент матриц из S. Очевидно, что $S \subseteq M_n(I)$.

Докажем обратное включение. Пусть $u \in I$, то есть для некоторых p и q элемент u находится на (p, q)-м месте матрицы $V = (u_{ij}) \in S$. Поскольку $u \in RuR$, то u можно представить в виде $u = \sum\limits_k a_k u b_k$. Если A^k_{ip} – матрица, у которой на $(i, p) -$ м месте находится элемент a_k, а на остальных – нули, и B^k_{qj} – матрица, у которой на (q, j)-м месте находится b_k и нули на остальных местах, то

$$A^k_{ip} V B^k_{qj} = a_k u b_k.$$

Следовательно, $S \ni \sum\limits_k A^k_{ip} V B^k_{qj} = U_{ij}$. А так как любую матрицу из $M_n(I)$ можно представить в виде $\sum\limits_{ij} U_{ij}$, где u пробегает все множество I, то $S = I_n$. Ясно, что $I \lhd R$. □

Предложение 1.49. *Если R – простое кольцо, то $M_n(R)$ – тоже простое кольцо.*

□ Пусть $a \in R$. Так как R – простое кольцо, то либо $RaR = 0$, либо $RaR = R$. Покажем, что если $a \neq 0$, то $RaR = R$. Рассмотрим множество

$$N = \{a |\ RaR = 0\}.$$

N является идеалом в R. Следовательно, либо $N = 0$, либо $N = R$. Если $N = 0$, то все доказано. Пусть $N = R$. Тогда $R^3 = 0$. Так как R – простое кольцо, то $R = R^2 = R^3 = \dots$ и $R = 0$. Противоречие. Следовательно, для любого элемента $a \in R$, $a \neq 0$, $R = RaR$ и по предложению 1.48 кольцо $M_n(R)$ – простое. $\square$

Предложение 1.50. *Пусть R – артиново кольцо. Тогда эквивалентны следующие три условия:*

1. *R – примитивное (справа) кольцо;*
2. *R изоморфно полному кольцу линейных преобразований некоторого конечномерного векторного пространства над подходящим телом;*
3. *R – простое кольцо.*

$\square$ Докажем, что $1 \Rightarrow 2$. Пусть M – точный неприводимый правый R-модуль, и пусть $\triangle$ – централизатор M. По лемме Шура, $\triangle$ является телом. Покажем, что M – конечномерное векторное пространство над $\triangle$. В противном случае в M существует бесконечное множество $\{x_i |\ i = 1, 2, \dots\}$ линейно независимых векторов. Пусть

$$\rho_i = \{r \in R |\ X_i r = 0\},$$

где $X_i = \{x_1, x_2, \dots, x_i\}$, $i = 1, 2, \dots$. Тогда $\rho_i <_r R$ и

$$\rho_1 \supseteq \rho_2 \supseteq \dots \supseteq \rho_i \supseteq \dots.$$

В силу теоремы плотности, существуют такие элементы $b_i \in R$, что $b_i \in \rho_i$ и $b_i \notin \rho_{i+1}$. Поэтому

$$\rho_1 \supset \rho_2 \supset \dots \supset \rho_i \supset \dots,$$

что противоречит условию обрыва убывающих цепей. Следовательно, M является конечномерным векторным пространством над $\triangle$.

Докажем, что $2 \Rightarrow 3$. Пусть $R = \mathrm{End}_{\triangle} V$, где $n = \dim_{\triangle} V$, $n < \infty$. По предложению 1.49, $M_n(\triangle)$ является простым кольцом.

Докажем, что $3 \Rightarrow 1$. Пусть R – простое кольцо. Покажем, что R – полупростое кольцо. Так как $J(R) \triangleleft R$, то либо $J(R) = 0$, либо $J(R) = R$. Если $J(R) = R$, то, по предложению 1.47, отсюда следует, что R – нильпотентно, то есть $R^n = 0$, для некоторого целого числа n. Но $R^2 \triangleleft R$, причем $R^2 \neq 0$ по определению простого кольца, значит $R^2 = R$. Поэтому $R^n = R^2 = R \neq 0$. Следовательно, $J(R) = 0$.

Возьмем произвольный минимальный правый идеал кольца R и рассмотрим его как правый R-модуль. Очевидно, что он неприводим. Покажем его точность. Так как аннулятор $\mathrm{Ann}_R I \triangleleft R$, то либо $\mathrm{Ann}\, I_R = 0$, либо $\mathrm{Ann}\, I_R = R$. Если $\mathrm{Ann}\, I = R$, то $IR = 0$, $I^2 = 0$. Поэтому $I \subseteq J(R)$. Противоречие. Итак, I – точный неприводимый правый R-модуль и R – примитивное (справа) кольцо. $\square$

Итак, простое артиново кольцо R является полным матричным кольцом над телом, то есть $R = M_n(D)$, где D – тело. Докажем, далее, что число n определяется однозначно, а тело D с точностью до изоморфизма.

Предложение 1.51. *Пусть D и D_1 – тела. Если $M_n(D) \cong M_m(D_1)$, то $m = n$ и $D \cong D_1$.*

$\square$ Пусть φ – изоморфизм кольца $M_n(D)$ на кольцо $M_m(D_1)$. Обозначим через e_{ij} матрицу порядка $n \times n$, у которой на (i, j) месте стоит 1, а на остальных – нули. Тогда $e_{11} M_n(D)$ – минимальный правый идеал кольца $M_n(D)$ и, следовательно, $\varphi(e_{11}) M_m(D_1)$ – минимальный правый идеал кольца $M_m(D_1)$. Элемент $\varphi(e_{11})$ является идемпотентом в $M_m(D_1)$. Поэтому существует такой автоморфизм кольца $M_m(D_1)$, при котором $\varphi(e_{11})$ переходит в матрицу вида

$$\mathrm{diag}(\underbrace{1, 1, \ldots, 1}_{r}, \underbrace{0, 0, \ldots, 0}_{m-r}).$$

Так как $\varphi(e_{11})M_m(D_1)$ – минимальный правый идеал в $M_m(D_1)$, то $r = 1$. Далее,

$$D \cong e_{11}M_n(D)e_{11} \cong \varphi(e_{11})M_m(D_1)\varphi(e_{11}) \cong D_1.$$

Правый идеал $e_{11}M_n(D)$ является левым векторным пространством над телом $e_{11}M_n(D)e_{11}$ размерности n, а правый идеал $\varphi(e_{11})M_m(D_1)$ является левым векторным пространством над телом $\varphi(e_{11})M_m(D_1)\varphi(e_{11})$ размерности m. Ввиду изоморфизма, получаем, что $m = n$. □

Элемент $e \neq 0$ кольца R называется *идемпотентом*, если $e^2 = e$.

Предложение 1.52. *Пусть R – кольцо, не имеющее ненулевых нильпотентных идеалов, и ρ – минимальный правый идеал в R. Тогда $\rho = eR$ для некоторого идемпотента $e \in R$.*

□ Так как $\rho^2 \neq 0$, то существует $x \in \rho$ такой, что $x\rho \neq 0$, $x\rho <_r R$ и $x\rho \subseteq \rho$. Следовательно, из минимальности правого идеала ρ следует, что $x\rho = \rho$. В частности, $x = xe$ для некоторого $e \in \rho$. Поэтому $xe = xe^2$ и $x(e - e^2) = 0$. Если $\rho_0 = \{a \in \rho |\ xa = 0\}$, то $\rho_0 <_r R$ и $\rho_0 \subseteq \rho$. Кроме того, $\rho_0 \neq \rho$ (иначе, $x\rho = 0$). Следовательно, $\rho_0 = 0$, а так как $e - e^2 \in \rho_0$, то $e = e^2$. Итак, e – идемпотент кольца R. Далее, $eR \subseteq \rho (e \in \rho)$, и так как $0 \neq e = e^2 \in eR$, то $eR = \rho$. □

Предложение 1.53. *Пусть R – произвольное кольцо и для некоторого $a \in R$ элемент $(a^2 - a)$ является нильпотентным. Тогда либо a нильпотентный элемент, либо существует такой многочлен $g(x)$ с целыми коэффициентами, что элемент $e = ag(a)$ является идемпотентом.*

□ Пусть $(a^2 - a)^k = 0$, для некоторого натурального k. Тогда

$$a^k = a^k a p(a),$$

где $p(x)$ – многочлен с целыми коэффициентами. Подставим значение a^k из этого равенства в его правую часть:

$$a^k = a^k \cdot ap(a) = a^{k+1}p(a) \cdot ap(a) = a^k[ap(a)]^2.$$

Продолжая этот процесс, находим:

$$a^k = a^k[ap(a)]^k = a^{2k}p(a)^k.$$

Если $a^k \neq 0$, то $e = a^k p(a)^k \neq 0$ и

$$e^2 = [a^{2k}p(a)^k]p(a)^k = a^k p(a)^k = e.$$

Что и требовалось доказать. □

Предложение 1.54. *Если R – артиново кольцо и ρ – ненулевой ненильпотентный правый идеал в R, то ρ содержит ненулевой идемпотент.*

□ Так как ρ – ненильпотентный идеал, то по предложению 1.47 $\rho \not\subseteq J(R)$. Положим $\bar{R} = R/J(R)$. Кольцо $\bar{R}$ – полупростое. Пусть $\bar{\rho}$ – образ ρ в $\bar{R}$. Так как $\bar{\rho} \neq 0$, то в $\bar{\rho}$ содержится минимальный правый идеал $\bar{\rho}$ кольца $\bar{R}$. По предложению 1.52 $\bar{\rho} = \bar{e}\bar{R}$ для некоторого идемпотента $\bar{e} \in \bar{R}$. Пусть $a \in \rho$ – элемент, образ которого равен $\bar{e}$. Тогда $a^2 - a$ отображается в $\bar{0} \in \bar{R}$. Следовательно, $a^2 - a \in J(R)$ и $a^2 - a$ – нильпотентный элемент. Так как $\bar{a}^k = \bar{e}^k = \bar{e} \neq 0$, то a – ненильпотентный элемент. В силу предложения 1.53, ρ содержит ненулевой идемпотент $e = a^k p(a)^k$ для некоторого k. □

Предложение 1.55. *Пусть R – полупростое артиново кольцо и $0 \neq \rho <_r R$. Тогда $\rho = eR$ для некоторого идемпотента $e \in R$.*

□ Так как R – полупростое кольцо, то ρ – ненильпотентный правый идеал и, по предложению 1.54, ρ содержит ненулевой

идемпотент. Каждому идемпотенту $e \in \rho$ поставим в соответствие множество

$$A(e) = \{x \in \rho |\ ex = 0\}.$$

Ясно, что $A(e) <_r R$. Множество правых идеалов $A(e)$ непустое и, следовательно, имеет минимальный элемент $A(e_0)$.

Если $A(e_0) = 0$. Тогда для любого элемента $x \in \rho$ получаем $e_0(x - e_0x) = 0$ и, следовательно, $x - e_0x = 0$, то есть $x = e_0x$. Поэтому $\rho = e_0R$.

Пусть $A(e_0) \neq 0$. Так как $A(e_0) <_r R$, то существует ненулевой идемпотент $e_1 \in A(e_0)$. По определению $e_1 \in \rho$ и $e_0e_1 = 0$. Рассмотрим элемент

$$e = e_0 + e_1 - e_1e_0 \in \rho.$$

Непосредственные вычисления показывают, что $e = e^2$. Так как

$$ee_1 = e_0e_1 + e_1^2 - e_1e_0e_1 = e_1,$$

то $e \neq 0$. Пусть теперь $ex = 0$ для некоторого $x \in \rho$, тогда $e_0ex = 0$. Но

$$e_0e = e_0e_0 + e_0e_1 - e_0e_1e_0 = e_0.$$

Следовательно, $e_0x = 0$. Отсюда $x \in A(e_0)$ и $A(e) \subseteq A(e_0)$. Так как $e_1 \in A(e_0)$, но $e_1 \notin A(e)$, то $A(e) \subset A(e_0)$. Это противоречит минимальности $A(e_0)$. Таким образом, ситуация $A(e_0) \neq 0$ невозможна. □

Предложение 1.56. *Пусть $A \lhd R$, где R – полупростое артиново кольцо. Тогда существует идемпотент e из центра кольца R такой, что $A = eR = Re$.*

□ Так как $A <_r R$, то $A = eR$, где $e^2 = e$. Покажем, что для любого элемента $x \in A$ $x = xe$. Рассмотрим

$$B = \{x - xe |\ x \in A\} <_l R.$$

Очевидно, что $Be = 0$, $eA = A$ и e – левая единица. Тогда $B^2 \subseteq BA = BeA = 0$. Так как R не содержит односторонних нильпотентных идеалов, то $B = 0$, то есть $x - xe = 0$. Получаем, что $A = Ae \subseteq Re \subseteq A$, то есть $A = Re = eR$. Если $x \in R$, то $ex \in A$ и $ex = exe$. Аналогично $xe = exe$. Поэтому $ex = xe$ и элемент e лежит в центре R. $\square$

Предложение 1.57. *Полупростое артиново кольцо является прямой суммой конечного числа идеалов, каждый из которых является простым артиновым кольцом.*

$\square$ Если R – простое кольцо, то утверждение теоремы доказано. Пусть R – не простое кольцо. Выберем минимальный двусторонний идеал $A \lhd R$, отличный от нуля. Покажем, что A – простое кольцо. В силу предложения 1.47 $A^2 \neq 0$. Если $0 \neq B \lhd A$, то $ABA \lhd R$, $ABA \subseteq B$, и так как $A \ni 1$, то $ABA \neq 0$. Так как $ABA \subseteq B \subseteq A$ и A – минимальный идеал R, то $B = A$, то есть A – простое кольцо.

В силу предложения 1.56 $A = eR$, где $e^2 = e$ – центральный идемпотент. Обозначим через $A_1 = (1 - e)R$. Так как $1 - e$ лежит в центре R, то $A_1 \lhd R$. Покажем, что $A \cap A_1 = 0$. Пусть $a \in A \cap A_1$, $a = eb = (1 - e)c$, $ea = e^2b = ec - e^2c = 0$, то есть $ea = 0$, но, с другой стороны, $ea = e^2b = eb = a$, то есть $a = 0$. Получим $R = A \oplus A_1$. Если A_1 – минимальный идеал, то теорема доказана, если нет, то в A_1 выбираем минимальный двусторонний идеал $J \lhd A_1$, $J = fA_1$, $J \lhd R$, A_1 – полупростое артиново кольцо. В результате получим

$$R = A \oplus J \oplus J_1,$$

где $J_1 = (1 - f)A_1 = (1 - f)(1 - e)R$. Продолжая этот процесс, получим идеалы кольца R

$$A_0 = A,\ A_1 = J,\ A_2, \ldots,$$

которые являются артиновыми кольцами и сумма

$$A_0 + A_1 + \cdots + A_k$$

является прямой для любого k.

Покажем, что эта сумма конечна. Если бы это было не так, то последовательность идеалов кольца R

$$\begin{gathered} R_0 = A_0 \oplus A_1 \oplus \dots, \\ R_1 = A_1 \oplus A_2 \oplus \dots, \\ \dots \\ R_n = A_n \oplus A_{n+1} \oplus \dots \end{gathered}$$

была бы бесконечной строго убывающей, что противоречит артиновости кольца R. $\square$

Единственность разложения полупростого артинова кольца устанавливает следующее предложение.

Предложение 1.58. *Если R – полупростое артиново кольцо и*

$$R = A_1 \oplus \dots \oplus A_k,$$

где A_i - идеалы, являющиеся простыми кольцами, то A_i пробегает множество всех минимальных идеалов кольца R.

$\square$ Пусть $B \neq 0$ – минимальный идеал кольца R. Так как $R \ni 1$, то $RB \neq 0$. Но

$$RB = A_1B \oplus A_2B \oplus \dots \oplus A_kB.$$

Пусть $A_iB \neq 0$. Ясно, что $A_iB \lhd R$ и $A_iB \subseteq A_i$. Тогда, в силу минимальности идеала A_i, имеем, что $A_iB = A_i$. Аналогично $A_iB \subseteq B$ и $A_iB = B$ в силу минимальности B. Тогда $A_i = B$. Таким образом, доказано, что B совпадает с одним из идеалов A_i. $\square$

Теорема 1.8.
Пусть R – правое артиново кольцо. Тогда $J(R)$ – нильпотентный идеал и

$$R/J(R) = M_{n_1}(D_1) \oplus \dots \oplus M_{n_k}(D_k)$$

– прямая сумма матричных колец над телами.

Доказательство следует из вышеприведенных предложений.

Теорема 1.8 для конечномерных алгебр над полем комплексных чисел была доказана Ф. Молиным в 1893 г., над произвольным полем Д. Веддерберном в 1907 г., а для артиновых колец Э. Артином (1927 г.) и К. Гопкинсом (1939 г.)

1.8. Упражнения

Упражнение 1.1. *Пусть* $a = \bar{3} + \bar{2}x + \bar{2}x + \bar{2}x^2 \in \mathbb{Z}_4[x]$. *Найдите элемент* a^{-1}.

Упражнение 1.2. *Докажите, что конечное кольцо* R, *удовлетворяющее тождеству* $x = x^2$, *изоморфно конечной прямой сумме полей* $GF(2)$.

Упражнение 1.3. *Пусть* R – *кольцо без нильпотентных элементов и* $e^2 = e$ *для некоторого* $e \in R$. *Докажите, что для любого элемента* $a \in R$ *справедливо* $ae = ea$.

Упражнение 1.4. *Для каких целых* $n \in \mathbb{Z}^+$ *кольцо* $\mathbb{Z}_n$ *не содержит идемпотентов, отличных от 0, 1 и нильпотентных элементов?*

Упражнение 1.5. *Пусть* $R = \{0, \pm 2, \pm 4, \dots\} = 2 \cdot \mathbb{Z}$. *Докажите, что*

$$I = \begin{pmatrix} 4\mathbb{Z} & R \\ R & R \end{pmatrix} = \begin{pmatrix} 2R & R \\ R & R \end{pmatrix} \lhd M_2(R)$$

и не существует такого идеала $K \lhd R$, *что* $I = M_2(K)$.

Упражнение 1.6. *Пусть* p – *простое число и*

$$A = \left\{ p \cdot \frac{a}{b} \in \mathbb{Q} \,\middle|\, p \text{ не делит } b \right\}.$$

Докажите, что $J(A) = A$.

Упражнение 1.7. *Пусть*

$$A = \left\{ \frac{2m}{n} \in \mathbb{Q} \,\middle|\, 2 \text{ не делит } n \right\}$$

и

$$B = \left\{ \frac{3m}{n} \in \mathbb{Q} \,\middle|\, 3 \text{ не делит } n \right\}.$$

Докажите, что $\mathbb{Q} = A + B$.

$\diamondsuit$ Так как числа вида $\frac{1}{p^n}$, где p – простое число, являются аддитивным порождающим $\mathbb{Q}^+$, то достаточно доказать, что $\frac{1}{p^n} \in A + B$. Если $p \neq 2, 3$, то

$$\frac{1}{p^n} = \frac{-2}{p^n} + \frac{3}{p^n} \in A + B.$$

По лемме о НОД существуют целые числа a, b, c, d такие, что

$$2^{n+1}a + 3b = 1, \quad 3^{n+1}c + 2d = 1,$$

откуда следует, что

$$\frac{1}{2^n} = 2 \cdot \frac{a}{1} + \frac{3b}{2^n} \in A + B$$

и

$$\frac{1}{3^n} = \frac{3 \cdot c}{1} + \frac{2d}{3^n} \in A + B.$$

Так как $J(\mathbb{Q}) = 0$, то из представимости кольца в виде суммы двух радикальных подколец не следует его радикальность. $\diamondsuit$

Упражнение 1.8. *Пусть*

$$A = \mathbb{Z}_2[1, x_1, x_2, \dots]/(x_1^2, x_2^2, \dots), \quad B = \langle \bar{x}_1, \bar{x}_2, \dots \rangle \subseteq A$$

и

$$R = \begin{pmatrix} B & B \\ A & B \end{pmatrix}, \quad R_1 = \begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} B & B \\ 0 & B \end{pmatrix}$$

Докажите, что $R_1^2 = 0$, R_2 – сумма нильпотентных идеалов и $R = R_1 + R_2$. Докажите также, что R не является суммой нильпотентных идеалов. Другими словами, из представимости кольца R в виде суммы двух подколец, каждое из которых является суммой нильпотентных идеалов, не следует, в общем случае, что само кольцо является суммой нильпотентных идеалов.

$\diamondsuit$ Заметим, что идеал кольца R, порожденный элементом

$$e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

содержит подкольцо, изоморфное B, которое, в свою очередь, не является нильпотентным. $\diamondsuit$

Упражнение 1.9. *Пусть $F[x]$ – кольцо многочленов над полем F.*

1. *Докажите, что неприводимые $F[x]$-модули изоморфны $F[x]/(p)$, где p – неприводимый многочлен.*

2. *Докажите, что $J(\mathbb{Z}_n) = 0$ тогда и только тогда, когда n не делится на квадрат простого числа.*

3. *Определите все неприводимые R-модули, если*

   (a) $R = \mathbb{C}[x]$;

   (b) $R = \mathbb{Q}[x]/(x^3 - 5)$;

   (c) $R = \mathbb{Z}[i]$;

   (d) $R = \mathbb{C}[x, y]$;

   (e) $R = C[0, 1]$.

4. *Докажите, что*

$$J(\mathbb{Z}_{p^n}) = (\bar{p}),$$

   если p – простое число.

5. *Пусть*
$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \in \mathbb{Q} \middle| \ (p,n) = 1 \right\}.$$
Докажите, что
$$J\left(\mathbb{Z}_{(p)}\right) = p \cdot \mathbb{Z}_{(p)}.$$

6. *Пусть* $f : R \to S$ *– сюръективный гомоморфизм. Докажите, что* $f(J(R)) \subseteq J(S)$.

Упражнение 1.10. *Вычислите* $J(R)$ *следующих колец:*

1. $R = \mathbb{Z}_8$;
2. $R = \mathbb{Z}_{60}$;
3. $R = \mathbb{Q}[x]/(x^3 - 5x)$;
4. $R = \mathbb{Z}[x]$;
5. $R = C[0,1]$ *– кольцо всех непрерывных функций на [0,1];*
6. $R = \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$.

Упражнение 1.11. *Пусть* $e \in R$ *и* $e^2 = e$. *Докажите, что* $J(eRe) = eJ(R)e$.

Упражнение 1.12 (лемма Накаямы).
Пусть M *– конечнопорожденный* R*-модуль,* R *содержит единицу и* $J(R)M = M$. *Докажите, что* $M = 0$.

$\diamondsuit$ Пусть
$$M = Rx_1 + \cdots + Rx_n.$$
Так как $J(R)M = M$, то
$$x_1 \in J(R)x_1 + \cdots + J(R)x_n.$$

Следовательно,

$$x_1 = a_1x_1 + \cdots + a_nx_n$$

где $a_i \in J(R)$. Поэтому

$$(1 - a_1)x_1 = a_2x_2 + \cdots + a_nx_n.$$

Так как $a_1 \in J(R)$, то существует такой элемент $b \in J(R)$, что

$$(1 - b)(1 - a_1) = 1.$$

Умножая слева предыдущее равенство на $(1 - b)$, имеем, что

$$x_1 = b_2x_2 + \cdots + b_nx_n$$

и M порождается $\{x_2, \ldots, x_n\}$. Считая n минимальным числом, приходим к противоречию. $\diamondsuit$

Упражнение 1.13. *Если N – подмодуль конечнопорожденного R-модуля M и $N + J(R)M = M$. Докажите, что $N = M$.*

Упражнение 1.14. *Пусть R – конечномерная алгебра с единицей над полем F и $a \in R$. Тогда либо a – обратимый элемент в R, либо a – левый и правый делитель нуля.*

Упражнение 1.15. *Пусть R – множество всех бесконечных конечнострочных матриц над некоторым полем F. Докажите, что $\langle R, +, \cdot\rangle$ – ассоциативная алгебра с единицей. Пусть*

$$a = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots \\ 0 & 0 & 1 & 0 & \ldots \\ 0 & 0 & 0 & 1 & \\ \vdots & \vdots & & \ddots & \ddots \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 & 0 & \ldots \\ 1 & 0 & 0 & \ldots \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \ddots \\ \vdots & \vdots & & \ddots \end{pmatrix}$$

– матрицы из R. Докажите, что $ab = 1$ и $ba \neq 1$.

Упражнение 1.16. *Пусть R – кольцо с единицей и $a, b \in R$ такие элементы, что $ab = 1$, $ba \neq 1$. Докажите, что*

1. $e_{ij} = b^i a^j - b^{i+1} a^{j+1} \neq 0$, $e_{ij} e_{st} = \delta_j^s \cdot e_{it}$;

2. $e_{11} R \subset (e_{11} + e_{22}) R \subset (e_{11} + e_{22} + e_{33}) R \subset \ldots$ – *строго возрастающая цепь правых главных идеалов;*

3. $(1 - e_{11}) R \supset (1 - e_{11} - e_{22}) R \supset \ldots$ – *строго убывающая цепь правых главных идеалов.*

Упражнение 1.17. *Пусть R – простое кольцо без делителей нуля, содержащее единицу и не являющееся телом. Пусть I – правый идеал R, отличный от (0) и R. Докажите, что IR – простое кольцо, не содержащее единицу.*

$\diamondsuit$ Если $T \triangleleft IR$, то $IRTIR \subseteq T$ и $I(RTIR) = IR$. Если $e^2 = e$ – единица в IR, то $e(er) = er$ и $er = r$. Откуда следует, что $R = eR \subseteq IR \cdot R \subseteq I$. $\diamondsuit$

Упражнение 1.18. *Докажите, что тело кватернионов $\left(\frac{-1,1}{\mathbb{R}}\right)$ удовлетворяет тождеству*

$$(xi)^2 - (ix)^2 + (xj)^2 - (jx)^2 + (xk)^2 - (kx)^2 = 0.$$

Упражнение 1.19. *Докажите, что алгебра матриц $M_n(F)$ над полем F удовлетворяет тождеству*

$$e_{11} x e_{11} y e_{11} - e_{11} y e_{11} x e_{11} = 0.$$

Упражнение 1.20. *Пусть I – правый идеал алгебры R, удовлетворяющий тождеству $f(x_1, \ldots, x_d) = 0$. Докажите, что R удовлетворяет обобщенному тождеству*

$$f(ay_1, \ldots, ay_d) = 0,$$

где $a \in I$, $a \neq 0$.

Упражнение 1.21. *Докажите, что произвольное тело D вложимо в тело, бесконечномерное над центром.*

$\diamondsuit$ Тело D является подтелом тела

$$T = D\langle\langle t\rangle\rangle = \left\{ \sum_{i=m}^{\infty} \alpha_i t^i \;\middle|\; \alpha_i \in D,\ m \in \mathbb{Z} \right\}.$$

Отображение

$$\sigma : T \to T, \quad \sigma\left(\sum_{i=m}^{\infty} \alpha_i t^i\right) = \sum_{i=m}^{\infty} \alpha_i t^{2i}$$

является гомоморфизмом, образ которого $\sigma(T)$ не содержит t. Пусть

$$A = T[x, \sigma] = \left\{ \sum_{i=0}^{k} a_i x^i \;\middle|\; a_i \in T,\ x\alpha = \sigma(\alpha)x,\ \alpha \in T \right\}$$

– кольцо косых многочленов. Если $L <_e A$ и $f(x)$ – многочлен минимальной степени в L, то $L = A \cdot f$. Это означает, в частности, что для любых элементов $a, b \in A$ цепочка левых идеалов

$$Aa \subseteq Aa + Aab \subseteq Aa + Aab + Aab^2 \subseteq \ldots$$

обрывается. Следовательно, $Aa \cap Ab \neq (0)$. Таким образом, A удовлетворяет левому условию Оре (см. главу 3).

Пусть $\triangle$ – левое (классическое) тело частных A. Ясно, что $D \subseteq \triangle$. Пусть C – центр $\triangle$. Если $n = [\triangle : C] < \infty$, то $\triangle$ удовлетворяет тождеству

$$S_{n+1}(x_1, \ldots, x_{n+1}) = 0.$$

Следовательно, $\triangle$ и A удовлетворяют тождеству

$$S_{n+1}(x, xy, \ldots, xy^n) = 0.$$

Пусть $c, d \in A$, $c \neq 0$, $d \neq 0$. Из последнего тождества следует, что $cA \cap dA \neq (0)$. Это означает, что A – правое кольцо Оре. В частности,

$$xg(x) = txf(x) \in xA \cap (tx)A, \quad xg(x) = txf(x) \neq 0$$

для некоторых $g(x),\ f(x) \in A$. Если

$$g = b_m x^m + \cdots + b_0, \quad f = a_n x^n + \cdots + a_0,$$

то $\sigma(b_m) = t\sigma(a_n)$ и $t \in \sigma(T)$. Противоречие. $\diamondsuit$

Упражнение 1.22. *Пусть k – поле и*

$$G_1 = \langle a_1 |\ a_1^2 = 1 \rangle, \quad G_2 = \langle a_2 |\ a_2^2 = 1 \rangle$$

– циклические группы второго порядка. Обозначим через

$$R_1 = k[G_1], \quad R_2 = k[G_2]$$

групповые алгебры, а через $R = R_1 * R_2$ – свободное произведение алгебр R_1, R_2. Легко видеть, что $R \cong k[G]$, где

$$G = \langle a_1, a_2 |\ a_1^2 = a_2^2 = 1 \rangle.$$

Положим $a = a_1 a_2$. Тогда $\langle a \rangle \lhd G$ и $[G : \langle a \rangle] = 2$. Докажите, что R является подалгеброй $M_2(k[a])$, содержит собственный ненулевой идеал и не является примитивной алгеброй.

Упражнение 1.23. *Пусть R – простое кольцо, удовлетворяющее некоторому тождеству. Пусть Q – простое артиново правое кольцо частных с центром F. Известно, что $[Q : F] < \infty$. Докажите, что $RF = R$ и R содержит единичный элемент.*

$\diamondsuit$ Если $f = ac^{-1} \in F$, $a \in R$, $c \in R$, то

$$X = \{x \in R |\ fx \in R\} <_r R$$

и $c \in X$. Так как f – центральный элемент, то $X \lhd R$ и, следовательно, $X = R$. Это означает, в частности, что $fR = Rf = R$ и R – конечномерное F-пространство. Пусть $[R : F] = m$ и c – регулярный элемент в R. Тогда из линейной зависимости векторов $c, c^2, \ldots, c^{m+1}$ следует равенство

$$c^k = c^{k+1} f_{k+1} + \cdots + c^{m+1} f_{k+1},$$

где $f_i \in F$. Так как c – регулярный элемент в R, то $1 = c \cdot a$, где $a \in R$. Откуда следует, что $1 \in R$. $\diamondsuit$

Упражнение 1.24. *Пусть R – примитивное кольцо. Докажите, что $M_n(R)$ – примитивное кольцо.*

Упражнение 1.25. *Пусть V – векторное пространство над телом D и $\dim_D V = \chi_0$. Пусть R – множество матриц вида*

$$\begin{pmatrix} A & & & \\ & d & 0 & \\ & 0 & d & \\ & & & \ddots \end{pmatrix},$$

где A – квадратная матрица конечного порядка над телом D и $d \in D$. Докажите, что R – примитивное кольцо. Более того, R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$.

Упражнение 1.26. *Пусть R – примитивное кольцо и $e^2 = e$, $e \in R$, $e \neq 0$. Докажите, что eRe – примитивное кольцо.*

Упражнение 1.27. *Пусть $V = \mathbb{R}[x]$ и $d, \varphi \in \mathrm{End}_{\mathbb{R}} V$ такие, что*

$$d(f) = f' \quad \text{и} \quad \varphi(f) = x \cdot f.$$

Докажите, что

1. $d\varphi - \varphi d = 1$;
2. $A = \mathbb{R}\langle \varphi, d \rangle$ – примитивная алгебра;
3. A – простая алгебра с единицей.

Упражнение 1.28. *Пусть $A = \prod\limits_{i \in \mathbb{N}} A_i$ – абелева группа, являющаяся прямым произведением счетного числа абелевых групп A_i, изоморфных группе $\langle \mathbb{Q}, + \rangle$. Пусть $R = \mathrm{End}_{\mathbb{Z}} A$ и a, b, c, d – такие элементы из R, что для любого $x = (a_1, a_2, \ldots) \in A$*

$$a(x) = (a_1, a_3, a_5, \ldots), \quad b(x) = (a_2, a_4, a_6, \ldots),$$

$$c(x) = (a_1, 0, a_2, 0, a_3, \ldots), \quad d(x) = (0, a_1, 0, a_2, \ldots).$$

Проверьте, что $ac = \varepsilon$, $bd = \varepsilon$, $bc = ad = 0$ и $ca + db = \varepsilon$, где ε – тождественное отображение.

Упражнение 1.29. *Пусть E_1, E_2 – поля, содержащие поле K. Докажите, что существует поле L, содержащее E_1 и E_2.*

$\diamondsuit$ $A = E_1 \otimes_K E_2$ содержит поля $E_1 \otimes 1$, $1 \otimes E_2$, изоморфные E_1 и E_2 соответственно. Пусть M – максимальный идеал A. Тогда $L = A/M$ – искомое поле. $\diamondsuit$

Упражнение 1.30. *Пусть A и B – простые алгебры, содержащие единицы. Докажите, что существует простая алгебра, содержащая A и B, тогда и только тогда, когда $charA = charB$.*

$\diamondsuit$ Пусть $charA = charB$ и Z_1, Z_2 – центры алгебр A и B соответственно. Согласно предыдущей задаче существует поле L, содержащее Z_1 и Z_2. Рассмотрим алгебры $A_1 = A \otimes_{Z_1} L$, $B_1 = B \otimes_{Z_2} L$. Они являются простыми L-алгебрами (с единицами) и $A_1 \supseteq A \otimes 1$, $B_1 \supseteq B \otimes 1$. Тогда алгебра $A_1 \otimes B_1$ – центральная простая L-алгебра, содержащая подалгебры, изоморфные A и B.

Другое решение этой задачи следует из теоремы Л. Бокутя о том, что любая ассоциативная алгебра над полем вложима в простую алгебру R, в которой разрешимо уравнение $xay = b$ для любых элементов $a \neq 0$, $b \in R$. $\diamondsuit$

Упражнение 1.31. *Пусть R – кольцо с единицей и множество всех обратимых элементов образует тело D. Докажите, что R – полупростое (в смысле радикала Джекобсона) кольцо. В частности, если F – поле, то коммутативное кольцо многочленов $F[x_1, \ldots, x_n]$ и свободная ассоциативная алгебра $F\langle x_1, \ldots, x_n\rangle$ являются полупростыми кольцами.*

$\diamondsuit$ Если $a \in J(R)$, то $1 + a$ – обратимый элемент в R и $a = (1+a)-1 \in D$. Так $J(R) \cap D$ – идеал в теле D, то $J(R) \cap D = (0)$ и $a = 0$. $\diamondsuit$

Упражнение 1.32. *Пусть R – ассоциативное кольцо, являющееся суммой двух нильпотентных подколец A и B, то есть $R = A + B$, где $A^m = B^n = 0$ для некоторых натуральных чисел m, n. Докажите, что R – нильпотентное кольцо.*

$\diamondsuit$ Воспользуемся методом математической индукции (относительно числа m). Рассмотрим правый идеал

$$P = A + AB = A + AR = A + (P \cap B).$$

Так как $A^{m-1} \subseteq \ell(P) \cap P$, где

$$\ell(P) = \{x \in R |\, xP = (0)\},$$

то $\ell(P) \cap P \lhd P$, $P/(\ell(P) \cap P) = \bar{A} + \bar{B}$. По предположению индукции существует целое число $k \geq 1$ такое, что $P^k \subseteq \ell(P) \cap P$ и $P^{k+1} = (0)$. Пусть $I = P + RP \lhd R$. Тогда $I^{k+1} = (0)$ и $R/I \cong B/(B \cap I)$ – нильпотентное кольцо. Следовательно, R – нильпотентное кольцо. $\diamondsuit$

Этот результат был доказан немецким математиком О. Кегелем [90]. Профессор Л. Бокуть (г. Новосибирск) построил пример простой алгебры, являющейся суммой трех нильпотентных подколец [37], то есть выше приведенный результат не имеет места (в общем случае) для колец, представимых в виде суммы трех нильпотентных подколец.

В работе К. Бейдара и А. Михалева [38], доказано, что если кольцо $R = A + B$, где A, B – подкольца, удовлетворяющие тождеству

$$[x_1, x_2][x_3, x_4] \ldots [x_{2n-1}, x_{2n}] = 0,$$

то R тоже удовлетворяет некоторому тождеству. В этой же работе сформулирован следующий вопрос: будет ли R-PI – кольцом, если R – сумма двух PI-подколец?

Упражнение 1.33. *Пусть D – тело и F – алгебраически замкнутое подполе его центра. Пусть также $\dim_F D < |F|$. Докажите, что $D = F$.*

$\diamondsuit$ Если D не совпадает с F и $\alpha \in D \backslash F$, то множество элементов

$$\left\{ (\alpha - a \cdot 1)^{-1} \middle| \ a \in F \right\}$$

является линейно зависимым, то есть существуют $b_1, \ldots, b_n \in F$ (не все равны нулю) такие, что

$$b_1(\alpha - a \cdot 1)^{-1} + \ldots + b_n(\alpha - a \cdot 1)^{-1} = 0.$$

Откуда следует, что α – алгебраический элемент над полем F. $\diamondsuit$

Упражнение 1.34. *Пусть $R = M_2(F)$, где F – поле характеристики два,*

$$G = \left\{ E, \ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

– группа матриц порядка два и

$$R^G = \left\{ a \in R | \ g^{-1}ag = a, g \in G \right\}$$

– подалгебра неподвижных элементов (относительно группы автоморфизмов G). Докажите, что

$$R^G = \left\{ \begin{pmatrix} u & v \\ 0 & u \end{pmatrix} \middle| \ u, v \in F \right\}$$

В частности, R^G не является полупервичной алгеброй.

Упражнение 1.35. *Пусть F – поле, $F\langle 1, x, y\rangle$ – свободная ассоциативная алгебра с единицей, порожденная элементами x, y и $A = F\langle 1, x, y\rangle/(yx - 1)$, где $(yx - 1)$ – идеал, порожденный элементом $yx - 1$. Докажите, что A – правая примитивная алгебра и для любого ненулевого простого идеала $P \lhd A$ $(xy - 1) \in P$, то есть A/P – гомоморфный образ $F\left[x, x^{-1}\right]$.*

$\diamondsuit$ Правый идеал

$$I = \bar{x}A = \left\{ \sum_{i \geq 1} \alpha_{ij} \bar{x}^i \bar{y}^j \middle| \ \alpha_{ij} \in F \right\}$$

является максимальным в A. Действительно, если

$$b = \varphi_0(\bar{y}) + \bar{x}\varphi_1(\bar{y}) + \ldots + \bar{x}^n\varphi_n(\bar{y}) \notin I,$$

то $\varphi_0(\bar{y}) \neq \bar{0}$. Пусть

$$\varphi_0(\bar{y}) = a_0 + a_1\bar{y} + \ldots + a_m\bar{y}^m,$$

где $a_i \in F$, $a_m \neq 0$. Тогда $bA + I$ содержит

$$\varphi_0(\bar{y})\bar{x}^m a_0^{-1} = 1 + \bar{x}\psi(\bar{x})$$

и, следовательно, $bA+I = A$. Таким образом, I – максимальный правый идеал A. Если Q – ненулевой идеал A, содержащийся в I и

$$b = \bar{x}^k\psi_k(\bar{y}) + \ldots + \bar{x}^{k+t}\psi_{k+t}(\bar{y})$$

– ненулевой элемент из Q, $\psi_k(\bar{y}) \neq 0$, то

$$\bar{y}^k b = \psi_k(\bar{y}) + \bar{x}\psi_{k+1}(\bar{y}) + \ldots + \bar{x}^t\psi_{k+t}(\bar{y}) \in Q \subseteq I.$$

Откуда следует, что $\psi_k(\bar{y}) \in I$. Пусть

$$\psi_k(\bar{y}) = b_0 + b_1\bar{y} + \ldots + b_s\bar{y}^s \in I,$$

где $b_i \in F$ и $b_s \neq 0$. Тогда

$$\psi_k(\bar{y})\bar{x}^s b_s^{-1} = 1 + \bar{x} \cdot f(\bar{x}) \in I$$

и $1 \in I$. Противоречие доказывает, что I – максимальный правый идеал, не содержащий ненулевых двусторонних идеалов кольца A. Следовательно, A – правая примитивная алгебра. Пусть P – ненулевой простой идеал алгебры A. Если $P \cap F[\bar{y}] \neq (\bar{0})$ и

$$h(\bar{y}) = a_0 + a_1\bar{y} + \ldots + a_n\bar{y}^n$$

– ненулевой многочлен в $P \cap F[\bar{y}]$ минимальной степени, $a_i \in F$, то $a_0 \neq 0$. Действительно, если $a_0 = \bar{0}$, то

$$h(\bar{y})x = a_1 + a_2\bar{y} + \ldots + a_n\bar{y}^{n-1} \in P \cap F[\bar{y}]$$

имеет степень $n-1$. Противоречие. Итак, $a_0 \neq \bar{0}$ и

$$h(\bar{y})a_0^{-1} = 1 + \bar{y}\varphi(\bar{y}) = 1 + \varphi(\bar{y})\bar{y} \in P$$

и $\bar{y}$ – обратимый элемент в A/P и $xy - 1 \in P$.

Пусть $P \cap F[\bar{y}] = (0)$ и

$$f = u_0(\bar{y}) + \bar{x}u_1(\bar{y}) + \ldots + \bar{x}^m u_m(\bar{y})$$

– произвольный ненулевой элемент из P, $u_m(\bar{y}) \neq \bar{0}$. Тогда $\bar{y}^m f \in P \cap F[\bar{y}] = (0)$ и $\bar{y}^{m-1} f = q(\bar{y}) + \bar{x}u_m(\bar{y})$. Откуда следует, что $u_m(\bar{y}) = -\bar{y}q(\bar{y})$ и

$$\bar{y}^{m-1} f = q(\bar{y}) - \bar{x}\bar{y}q(\bar{y}) = (1 - \bar{x}\bar{y})q(\bar{y}) \in P,$$

$(1-\bar{x}\bar{y})x^a y^b q(\bar{y}) \in P$, для любых целых неотрицательных чисел a и b. Поэтому $(1 - \bar{x}\bar{y})Aq(\bar{y}) \subseteq P$. Так как P – простой идеал, не содержащий ненулевой элемент $q(\bar{y})$, то $(1 - \bar{x}\bar{y}) \in P$. $\diamondsuit$

Упражнение 1.36. *Пусть R – конечное простое ассоциативное кольцо. Докажите, что R, как кольцо, порождается двумя элементами.*

$\diamondsuit$ Ясно, что R – правое артиново простое кольцо. Следовательно, $R = M_n(D)$, где D – конечное тело. По теореме Веддерберна $D = GF(q)$ – конечное поле Галуа, мультипликативная группа которого $GF(q)^* = GF(q)\backslash\{0\}$ является циклической, то есть $GF(q)^* = \langle \lambda, \lambda^2, \ldots, \lambda^{q-1} = 1 \rangle$. Если $n = 1$, то R порождается элементом λ. Если $n \geq 2$, то $a = \lambda e_{11}$ и $b = e_{12} + e_{23} + \ldots + e_{n-1n} + e_{n1}$ являются порождающими элементами кольца R, так как $b^{n-i+1} \cdot e_{11} = e_{i1}$, $e_{11} \cdot b^{j-1} = e_{1j}$ и $e_{ij} = e_{i1}e_{1j} = b^{n-i+1}e_{11}b^{j-1}$, $b^n = 1$. $\diamondsuit$

Упражнение 1.37 (Китайская теорема об остатках). *Пусть R – коммутативное кольцо с единицей и $\{I_1, \ldots, I_n\}$ – такие идеалы R, что для любых чисел $1 \leq i, j \leq n$, $i \neq j$, $I_i + I_j = R$. Докажите, что*

$$R/\bigcap_{i=1}^{n} I_i \cong R/I_i \oplus \ldots \oplus R/I_n.$$

$\diamondsuit$ Рассмотрим отображение

$$\varphi : R \to \bigoplus_{i=1}^{n} R/I_i$$

такое, что

$$\varphi(a) = (a + I_1, \ldots, a + I_n),$$

где $a \in R$. Проверьте, что φ – гомоморфизм колец с ядром равным $\bigcap\limits_{i=1}^{n} I_i$. Из равенств

$$R = I_1 + I_2 = \ldots = I_1 + I_n$$

следует, что

$$R = R^{n-1} = (I_1 + I_2)\ldots(I_1 + I_n) = \\ = I_1 + (I_2 I_3 \ldots I_n) = I_1 + (I_2 \cap \ldots \cap I_n).$$

Пусть x – произвольный элемент в R. Тогда $x = a + b$, где $a \in I_1$, $b \in \bigcap\limits_{i=1}^{n} I_i$. Следовательно,

$$\varphi(b) = (x + I_1, \bar{0}, \ldots, \bar{0})$$

и образ $\varphi(R)$ включает в себя множество

$$(R/I_1 \oplus (0) \oplus \ldots \oplus (0))$$

и

$$\varphi(R) = \bigoplus_{i=1}^{n} R/I_i.$$

Так как $\varphi(R) = R/\operatorname{Ker}\varphi$, то $R/\bigcap\limits_{i=1}^{n} I_i \cong \bigoplus\limits_{i=1}^{n} R/I_i$. $\diamondsuit$

Упражнение 1.38. *Докажите следующие изоморфизмы для групповых алгебр:*

1. $\mathbb{C}(C_2) \cong \mathbb{C} \oplus \mathbb{C}$;

2. $\mathbb{C}(S_3) \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$;

3. $\mathbb{C}(C_3) \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$;

4. $\mathbb{Q}(C_2) \cong \mathbb{Q} \oplus \mathbb{Q}$;

5. $\mathbb{Q}(C_3) \cong \mathbb{Q} \oplus \mathbb{Q}[x]/\left(x^2 + x + 1\right)$,

где C_n – циклическая группа порядка n и S_n – симметричная группа степени n.

♢ Воспользоваться теоремой Машке, а также китайской теоремой об остатках. ♢

Упражнение 1.39. *Постройте пример конечной группы G, для которой не существует ассоциативного кольца с единицей с группой обратных элементов изоморфной G.*

♢ Примером такой группы является циклическая группа C_5. Действительно, если R – ассоциативное кольцо с единицей и его группа обратимых элементов R^* изоморфна C_5, то из равенства $(-1)^2 = 1 \in R^*$ следует, что $-1 = 1$ и $R - GF(2)$ – алгебра. Следовательно, существует гомоморфизм алгебры $GF(2)[x]/\left(x^5 - 1\right)$ в R, отображающий $\bar{x}$ в образующий элемент группы R^*. Многочлен $x^4+x^3+x^2+x+1$ является неприводимым в $GF(2)[x]$. Из китайской теоремы об остатках следует, что

$$GF(2)[x]/\left(x^5 - 1\right) \cong GF(2) \oplus GF(16)$$

и $\left|\left(GF[x]/\left(x^5 - 1\right)\right)^*\right| = 15$, то есть $|R^*| \geq 15$. Противоречие. ♢

Упражнение 1.40. *Конечная абелева группа является циклической тогда и только тогда, когда среди ее подгрупп нет подгруппы изоморфной $C_p \times C_p$, где C_p – циклическая группа порядка p, где p – простое число.*

♢ Воспользуйтесь тем, что конечная абелева группа является прямым произведением примарных циклических групп. ♢

Упражнение 1.41. *Пусть G – конечная подгруппа мультипликативной группы F^* поля F. Докажите, что G – циклическая группа.*

$\diamondsuit$ Если G – не циклическая группа, то из предыдущего упражнения следует, что G содержит подгруппу $C_p \times C_p$ порядка p^2 (p – простое число), каждый элемент которой является корнем уравнения $x^p - 1 = 0$. Известно, что в поле число различных корней многочлена не превосходит его степени, то есть $p^2 \leq p$. Противоречие. $\diamondsuit$

Упражнение 1.42. *Пусть F – поле и*

$$f(x) = p_1^{k_1}(x) \dots p_s^{k_s}(x) \in F[x]$$

– ненулевой многочлен, где $p_1(x), \dots, p_s(x)$ – различные неприводимые многочлены. Докажите, что

$$F[x]/\left(f(x)\right) \cong F[x]/(p_1^{k_1}) \oplus \dots \oplus F[x]/(p_s^{k_s}).$$

$\diamondsuit$ Воспользуйтесь предыдущим упражнением. Для этого заметьте, что идеалы $(p_i^{k_i}) = p_i^{k_i}F[x]$ и $(p_j^{k_j}) = p_j^{k_j}F[x]$ при $i \neq j$ являются взаимно простыми, то есть их сумма равна $F[x]$. $\diamondsuit$

Упражнение 1.43. *Пусть $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ – кольцо классов вычетов по модулю n, где $n = p_1^{k_1} \dots p_s^{k_s}$ – каноническое разложение n на простые множители. Докажите, что*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}}.$$

$\diamondsuit$ Воспользуйтесь упражнением 1.37. Для этого заметьте, что идеалы $p_i^{k_i}\mathbb{Z}$ и $p_j^{k_j}\mathbb{Z}$ при $i \neq j$ являются взаимно простыми, то есть их сумма равна $\mathbb{Z}$. $\diamondsuit$

Упражнение 1.44. *Пусть $\mathbb{Z}_n^*$ – группа обратимых элементов кольца $\mathbb{Z}_n$. Докажите, что*

1. *$|\ \mathbb{Z}_n^*| = \varphi(n)$, где $\varphi(n)$ – функция Эйлера;*

2. $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \ldots \times \mathbb{Z}_{p_s^{k_s}}^*$, *где* $n = p_1^{k_1} \ldots p_s^{k_s}$ *– каноническое разложение числа* n *на простые множители;*

3. $\mathbb{Z}_n^*$ *является циклической группой тогда и только тогда, когда* $n = 2, 4, 2p^m, p^m$, *где* p *– нечетное простое число.*

$\diamondsuit$ Утверждение 2) следует из упражнения 1.43. Рассмотрим утверждение 3). Так как

$$\left|\mathbb{Z}_{p^k}^*\right| = \varphi\left(p^k\right) = p^{k-1}(p-1),$$

где p – нечетное простое число, то группа $\mathbb{Z}_{p^k}^* = A \times B$, где

$$A = \left\{\bar{x} \in \mathbb{Z}_{p^k}^* \,\middle|\, \bar{x}^{p^{k-1}} = \bar{1}\right\} \quad \text{и} \quad B = \left\{\bar{x} \in \mathbb{Z}_{p^k}^* \,\middle|\, \bar{x}^{p-1} = \bar{1}\right\}.$$

Докажем, что A и B – циклические группы взаимно простых порядков и как следствие получим цикличность группы $\mathbb{Z}_{p^k}^*$. Если $k = 1$, то $\mathbb{Z}_p$ – поле и цикличность группы $\mathbb{Z}_p^*$ доказана в упражнении 1.41. Следовательно, существует целое число a такое, что

$$a + (p),\ a^2 + (p),\ \ldots,\ a^{p-1} + (p)$$

– различные элементы $\mathbb{Z}_p$. Пусть $k \geq 2$ и $b = \bar{a}^{p^{k-1}} \in \mathbb{Z}_{p^k}^*$. Тогда $b^{p-1} = \bar{a}^{\varphi(p^k)} = \bar{1}$ и $b \in B$. Так как $b + (p) = a + (p)$, то

$$b + (p^k),\ b^2 + (p^k),\ \ldots,\ b^{p-1} + (p^k)$$

– попарно различные элементы в $\mathbb{Z}_{p^k}^*$, то есть $|B| \geq p-1$. С другой стороны, $\varphi(p^k) = |A| \cdot |B|$, где A – силовская p – подгруппа $\mathbb{Z}_p^*$ и $|A| = p^{k-1}$. Следовательно, $|B| = p - 1$ и B – циклическая группа. Если A не является циклической группой, то A – прямое произведение s циклических групп ($s \geq 2$) и число элементов в A порядка p равно p^s. С другой стороны, их число не превосходит p, так как если $\bar{x}^p = \bar{1}$, то p делит число $(x-1) = (x - x^p) + (x^p - 1)$.

Пусть

$$x = 1 + yp^f + zp^{f+1},$$

где $1 \leq y < p$. Тогда

$$x^p = 1 + yp^{f+1} + up^{f+2},$$

$f+1 = k$ и такие элементы исчерпываются смежными классами

$$\overline{1},\ \overline{1 + p^{k-1}},\ \overline{1 + 2p^{k-1}},\ \ldots, \overline{1 + (p-1)p^{k-1}}.$$

Таким образом, $p^s \leq p$ и $s \leq 1$. Противоречие доказывает, что A – циклическая группа.

Заметим, далее, что при $k \geq 3$ группа $\mathbb{Z}^*_{2^k}$ является прямым произведением циклической группы порядка 2 и циклической группы порядка 2^{k-2}, порожденной смежным классом $\bar{5}$. Так как $\overline{1}$, $\overline{-1}$, $\overline{1 + 2^{k-1}}$ и $\overline{-1 + 2^{k-1}}$ – элементы порядка два в $Z^*_{2^k}$, то $Z^*_{2^k}$ – прямое произведение по меньшей мере двух циклических групп. Покажем, что $\bar{5}$ – элемент порядка 2^{k-2}. Для этого заметим, что $5^2 = 1 + 2^3 \cdot 3$ и если $5^2 = 1 + 2^{m+2}u$, где 2 не делит u, то

$$5^{2^{m+1}} = 1 + 2^{m+3}u + 2^{2m+4}u^2 = 1 + 2^{m+3}u_1,$$

где 2 не делит u_1. Поэтому $\bar{5}$ – элемент максимального порядка 2^{k-2}. Следовательно, подгруппа $\langle\bar{5}\rangle$ отщепляется прямым множителем, то есть $\mathbb{Z}^*_{2^k} = A \times \langle\bar{5}\rangle$. Сравнивая порядки, имеем, что $|A| = 2$ и $\mathbb{Z}^*_{2^k} = \langle\pm 1\rangle \times \langle\bar{5}\rangle$. Приведенные выше рассуждения доказывают , что при $n = 2, 4, p^m, 2p^m$ (p – нечетное простое число) Z^*_n – циклическая группа.

Пусть $\mathbb{Z}^*_n$ – циклическая группа и $n \neq 2, 4, p^m, 2p^m$, где p – нечетное простое число. Тогда либо $n = p^\alpha \cdot q^\beta \ldots$, где p, q – нечетные простые числа, либо $n = 2^\alpha p^m$, где $\alpha \geq 3$ и p – нечетное простое число, либо, наконец, $n = 4p^e$, где $e \geq 1$ и p – нечетное простое число. В первом случае из изоморфизма

$$\mathbb{Z}^*_n = \mathbb{Z}^*_{p^\alpha} \times \mathbb{Z}^*_{q^\beta} \times \ldots$$

следует, что в циклической группе $\mathbb{Z}^*_n$ есть подгруппа

$$C_2 \times C_2 \subseteq C_{p^{\alpha-1}} \times C_{p-1} \times C_{q^{\beta-1}} \times C_{q-1} \times \ldots,$$

так как $p-1$ и $q-1$ – четные числа. Противоречие. Во втором случае $\mathbb{Z}_n^*$ содержит подгруппу $\mathbb{Z}_{2^\alpha}^*$, не являющуюся циклической (при $\alpha \geq 3$). В третьем случае

$$\mathbb{Z}_n^* = \mathbb{Z}_4^* \times \mathbb{Z}_{p^e}^* = C_2 \times C_{p^e-1} \times C_{p-1}$$

и $\mathbb{Z}_n^*$ содержит подгруппу изоморфную $C_2 \times C_2$, что противоречит цикличности группы $\mathbb{Z}_n^*$. $\diamondsuit$

Упражнение 1.45. *Пусть R – коммутативное кольцо с единицей, K – ниль-идеал R, $f(t)$ – многочлен с целыми коэффициентами, $\bar{u}$ – такой элемент R/K, что $f(\bar{u}) = \bar{0}$ и $f'(\bar{u})$ – обратимый элемент в R/K. Докажите, что существует элемент $a \in R$ такой, что $f(a) = 0$ и $\bar{a} = \bar{u}$.*

$\diamondsuit$ Так как $b = f(u) \in K$, то $b^n = 0$ для некоторого натурального числа n. Пусть $y \in R$. Тогда

$$f(u+y) = f(u) + yf'(u) + y^2 f_2(n) + \ldots + y^m f_m(u),$$

где $m = \deg f(t)$ и $f_2(u), \ldots, f_m(u)$ – элементы подкольца $\langle 1, u\rangle$. Элемент $f'(u)$ обратим в R. Положим $c = -b\,(f'(u))^{-1}$. Тогда $c^n = 0$ и

$$\big(f'(u)\big)^{-1} f(u+y) = -c + y + y^2 g_2(u) + \ldots + y^m g_m(u),$$

где $g_i(u) = f_i(u)\,(f'(u))^{-1}$. Докажем, что существует элемент $y = c + \lambda_2 c^2 + \ldots + \lambda_{n-1} c^{n-1}$ такой, что $f(u+y) = 0$, $\overline{u+y} = \bar{u}$. Для этого рассмотрим правую часть равенства

$$\begin{aligned}(f'(u))^{-1} f(u+y) &= -c + y + y^2 g_2(u) + \ldots + y^m g_m(u) = \\ &= (\lambda_2 c^2 + \ldots + \lambda_{n-1} c^{n-1}) + (c + \lambda_2 c^2 + \ldots + \lambda_{n-1} c^{n-1})^2 g_2(u) + \ldots \\ &\quad \ldots + (c + \lambda_2 c^2 + \ldots + \lambda_{n-1} c^{n-1}) g_m(u) = \\ &= (\lambda_2 + g_2) c^2 + (\lambda_3 + 2\lambda_2 g_2 + g_3) c^3 + \ldots .\end{aligned}$$

Полагая $\lambda_2 = -g_2(u)$, $\lambda_3 = -2\lambda_2 g_2 - g_3$, …, мы найдем искомый элемент $a = u + y$. $\diamondsuit$

Упражнение 1.46. *Пусть R – кольцо, содержащее единицу, K – ниль-идеал R и u – идемпотент в R/K. Докажите, что существует идемпотент $e \in R$ такой, что $\bar{e} = u$.*

$\diamondsuit$ Пусть $u = \bar{x}$ и $y = 1 - x$. Тогда $yx = xy \in K$ и существует натуральное число n такое, что $(xy)^n = 0$. Заметим, что

$$1 = (x+y)^{2n-1} = x^{2n-1} + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} x^{2n-2}y + \ldots$$
$$\ldots + \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} x^n y^{n-1} + \begin{pmatrix} 2n-1 \\ n \end{pmatrix} x^{n-1}y^n + \ldots + y^{2n-1}.$$

Положим

$$e = x^n \left(x^{n-1} + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} x^{n-2}y + \ldots + \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} y^{n-1} \right).$$

Тогда

$$\bar{e} = u^n \left(u^{n-1} + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} u^{n-2}(1-u) + \ldots \right.$$
$$\left. \ldots + \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} (1-u)^{n-1} \right) =$$
$$= u \left(u + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} u(1-u) + \ldots + (1-u)^{n-1} \right) = u,$$

$$e^2 = x^{2n} \left[x^{n-1} + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} x^{n-2}y + \ldots + \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} y^{n-1} \right]^2 =$$
$$= x^n \left[x^{2n-1} + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} x^{2n-2}y + \ldots + \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} x^n y^{n-1} \right] \cdot$$
$$\cdot \left[x^{n-1} + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} x^{n-2}y + \ldots + \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} y^{n-1} \right] =$$
$$= x^n \left[1 - \begin{pmatrix} 2n-1 \\ n \end{pmatrix} x^{n-1}y^n - \ldots - y^{2n-1} \right] \cdot$$
$$\cdot \left[x^{n-1} + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} x^{n-2}y + \ldots + \begin{pmatrix} 2n-1 \\ 1 \end{pmatrix} y^{n-1} \right] = e. \quad \diamondsuit$$

Упражнение 1.47. *Докажите, что каждая матрица в кольце $M_n(\mathbb{C})$, где $\mathbb{C}$ – поле комплексных чисел, представима в виде суммы идемпотентной матрицы и обратимой матрицы.*

$\diamondsuit$ Воспользуйтесь жордановой нормальной формой матриц. $\diamondsuit$

Упражнение 1.48. *Пусть R – правое примитивное кольцо, содержащее конечный правый идеал. Докажите, что R – конечное кольцо.*

$\diamondsuit$ Пусть I – конечный правый идеал минимального порядка. Тогда I – точный неприводимый правый R-модуль. По лемме Шура $D = \mathrm{End}_R I$ – конечное тело (и, следовательно, то теореме Веддерберна $D = GF(q)$ – конечное поле Галуа). Так как $|I| < \infty$, то I – конечномерное $GF(q)$ – пространство и R – плотное кольцо линейных преобразований в $\mathrm{End}_{GF(q)} I = M_n(GF(q))$, где $n = \dim_{GF(q)} I$. Следовательно, $R = M_n(GF(q))$ и $|R| = q^n$. $\diamondsuit$

Упражнение 1.49. *Пусть R – простая алгебра с единицей над полем рациональных чисел, $A = R[x]$ – кольцо многочленов и $d : A \to A$, $d(f(x)) = f'(x)$ – дифференцирование в A. Пусть*

$$B = A[y, d] = \left\{ \sum_{i=0}^{n} a_i y^i \;\middle|\; ya = ay + d(a),\ a_i, a \in A \right\}$$

– кольцо дифференциальных многочленов над кольцом A с дифференцированием d. Докажите, что B – простая алгебра с единицей (в частности, B – примитивная алгебра).

$\diamondsuit$ Заметим, что

$$[x^n, y] = -nx^{n-1},$$
$$[x^n, \underbrace{y, y, \ldots, y}_{n}] = \pm n!.$$

Пусть

$$a = g_0(y) + x \cdot g_1(y) + \ldots + x^n \cdot g_n(y)$$

– ненулевой элемент идеала $I \lhd B$, $g_n(y) \neq 0$. Тогда

$$[a, \underbrace{y, y, \ldots, y}_{n}] = \pm n! g_n(y) \in I$$

и

$$g_n(y) = b_m y^m + b_{m-1} y^{m-1} + \ldots + b_0 \in I,$$

где $b_i \in R$, $b_m \neq 0$, $i \leq m$. Пусть m – минимальное число с этим свойством. Если $m \geq 1$, то

$$[g, x] = m b_m y^{m-1} + \sum_{i=0}^{m-2} c_i y^i,$$

$c_i \in R$ имеет меньшую степень и принадлежит I. Противоречие. Следовательно, $g_n(y) = b_0 \in R \cap I$. Так как R – простая алгебра, то $Rb_0R = R \subseteq I$, $A \subseteq I$, $B \subseteq I$ и B – простая алгебра. $\diamondsuit$

Приведенная выше конструкция позволяет строить новые простые алгебры, исходя из простых алгебр.

Упражнение 1.50. *Приведите пример ассоциативной алгебры с единицей, в которой радикал Джекобсона не является пересечением максимальных двусторонних идеалов.*

$\diamondsuit$ Пусть F – поле характеристики нуль и $\sigma : F \to F$ – автоморфизм бесконечного порядка. Например, $F = \mathbb{Q}(x)$ и

$$\sigma\left(\frac{f(x)}{g(x)}\right) = \frac{f(x+1)}{g(x+1)}.$$

Рассмотрим множество косых многочленов

$$R = F[x, \sigma] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; (ax^n)(bx^m) = a\sigma^n(b)x^{n+m},\ a, b \in F \right\}$$

над полем F. Докажем, что каждый ненулевой идеал $I \lhd R$ имеет вид Rx^n, где $n \geq 0$. Действительно, пусть

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n,$$

$a_n \neq 0$ – ненулевой многочлен минимальной степени в I. Если $n = 0$, то I содержит $1 = a_0^{-1}a_0$ и $I = R$. Пусть $n \geq 1$. Тогда для любого элемента $b \in F$ многочлен $f(x)b - \sigma^n(b)f(x) \in I$ имеет меньшую степень и, следовательно, равен нулю. В частности, $a_i\left(\sigma^i(b) - \sigma^n(b)\right) = 0$ для $i \leq n-1$. Если существует индекс $i_0 < n$ такой, что $a_{i_0} \neq 0$, то $\sigma^{n-i_0}(b) = b$ для любого элемента $b \in F$ и σ – автоморфизм конечного порядка. Противоречие. Поэтому $a_0 = a_1 = \ldots = a_{n-1} = 0$ и $I \supseteq Rx^n$. Если существует многочлен

$$g(x) = c_i x^i + c_{i+1}x^{i+1} + \ldots + c_m x^m \in I,$$

для которого $c_i \neq 0 \in F$ и $i \leq n-1$, то

$$g(x)x^{n-1-i} = c_i x^{n-1} + x^n \cdot \varphi(x) \in I$$

и $x^{n-1} \in I$. Противоречие.

Итак, все идеалы алгебры R исчерпываются идеалами вида $\left\{(0), R, Rx, Rx^2, \ldots\right\}$. Ясно, что среди них Rx – единственный максимальный двусторонний идеал. Покажем, далее, что $J(R) = (0)$. Действительно, иначе $J(R) = Rx^n$ и $(1 + x^n)$ – обратимый элемент алгебры R. Противоречие доказывает, что R – полупростая (в смысле радикала Джекобсона) алгебра, содержащая единственный максимальный двусторонний идеал Rx. Пусть $a \neq 0 \in F$. Тогда правый идеал $(x - a)R$ является максимальным модулярным правым идеалом, не содержащим ненулевые двусторонние идеалы. Таким образом, R – правая примитивная алгебра, идеалы которой образуют цепь $R \supset Rx \supset Rx^2 \ldots$. $\diamondsuit$

Упражнение 1.51. *Пусть M – конечный (как множество) правый R-модуль. Докажите, что $R/A(M)$ – конечное кольцо.*

$\diamondsuit$ Если $M = \{a_1 = 0, a_2, \ldots, a_n\}$, то отображение

$$\varphi : R \to \underbrace{M \oplus \ldots \oplus M}_{n},$$

$$\varphi(x) = (a_1x, a_2x, \ldots, a_nx)$$

является гомоморфизмом R-модулей с ядром $A(M)$. $\diamondsuit$

Упражнение 1.52. *Пусть $\{e_{ij}\}$ – множество матричных единиц алгебры $M_n(F)$, где F – поле. Пусть*

$$h_{pq} = \frac{1}{m_{pq}} \left(\sum_{i=1}^{p} \sum_{j=1}^{q} e_{ij} \right),$$

где $m_{pq} = \min(p, q)$. Докажите, что

$$h_{pq}^2 = h_{pq}, \quad h_{pq}h_{st} = k_{pqst}h_{pt},$$

где

$$k_{pqst} = \frac{m_{qs}m_{pt}}{m_{pq}m_{st}}$$

и $\{h_{pq}\}$ образуют базис $M_n(F)$ (таким образом, полная матричная алгебра $M_n(F)$ имеет базис, состоящий из идемпотентов).

Упражнение 1.53. *Пусть p – простое число и a, b – произвольные элементы кольца R. Докажите, что*

$$(a+b)^p = a^p + b^p + \sum_{i \in I} [a_i, b_i] + pc,$$

где c, a_i, b_j – некоторые элементы R. Например,

$$(a+b)^3 = a^3 + b^3 + [ab, a] + [b, ab] + [b, a^2] + [b^2, a] + 3(a^2b + ab^2).$$

$\diamondsuit$ Имеем

$$(a+b)^p - a^p - b^p = \sum u_1u_2 \ldots u_p,$$

где $u_i = a, b$ и каждое такое слово $(u_1 \ldots u_p)$ содержит оба элемента. С каждым слагаемым можно связать p слов

$$u_pu_1u_2 \ldots u_{p-1}, \ u_{p-1}u_pu_1 \ldots u_{p-2}, \ \ldots, \ u_2u_3 \ldots u_pu_1,$$

полученных циклическим сдвигом. Покажем, что они попарно различные. Если, например,

$$(u_1u_2\dots u_p) = (u_1u_2\dots u_i)(u_{i+1}\dots u_p) = (u_{i+1}\dots u_p)(u_1u_2\dots u_i)$$

и $i \le \frac{p}{2}$, то

$$(u_{i+1}\dots u_p) = (u_1\dots u_i)^e v,$$

где v – либо пустое слово, либо $v = v'u_jv''$, где v' – начало (возможно пустое) слова $(u_1\dots u_i)$, не равное $(u_1\dots u_i)$, $v'u_j$ не являются началом $(u_1\dots u_i)$. Тогда

$$(u_1\dots u_i)^{e+1}\left(v'u_jv''\right) = (u_1\dots u_i)^e\left(v'u_jv''\right)(u_1\dots u_i)$$

и

$$(v'u_jv'')(u_1\dots u_i) = (u_1\dots u_i)\left(v'u_jv''\right).$$

Противоречие. Следовательно, v – пустое слово и $p = i(e+1)$, где $i \ge 2$ (так как $u_1\dots u_p$ не равно a^p, b^p). Так как p – простое число, то все слова

$$\{u_1\dots u_p,\ u_pu_1\dots u_{p-1},\ \dots,\ u_2u_3\dots u_pu_1\}$$

попарно различные. Далее, заметим, что

$$(u_1\dots u_i)(u_{i+1}\dots u_p) - (u_{i+1}\dots u_p)(u_1\dots u_i) = \left[a_i', b_i'\right].$$

Следовательно, сумма таких слов

$$u_1u_2\dots u_p + u_pu_1\dots u_{p-1} + \dots + u_2u_3\dots u_pu_1 = \\ = p(u_1u_2\dots u_p) + \sum_{j=2}^{p}\left[a_j'', b_j''\right].$$

Поэтому

$$(a+b)^p - a^p - b^p = pc + \sum_{i\in I}[a_i, b_i].$$

$\diamondsuit$

Упражнение 1.54. *Пусть $V = \mathbb{C}[x]$ – векторное пространство многочленов с комплексными коэффициентами и φ, ψ – такие линейные операторы V, что*

$$\varphi\left(a_0 + a_1 x + \ldots + a_n x^n\right) = a_1 + a_2 x + \ldots + a_n x^{n-1},$$

$$\psi\left(a_0 + a_1 x + \ldots + a_n x^{n+1}\right) = a_0 x + \ldots + a_n x^{n+1}.$$

Докажите, что $\varphi\psi = \varepsilon$, $\psi\varphi \neq \varepsilon$, где ε – тождественный оператор.

Упражнение 1.55. *Пусть r – такой элемент кольца R, что*

$$r^n = \lambda_1 r^{n+1} + \ldots + \lambda_t r^{n+t},$$

где $\lambda_i \in \mathbb{Z}$. Пусть также

$$a = \lambda_1 + \lambda_2 r + \ldots + \lambda_t r^{t-1} \in R^{\#}$$

и $e = (ar)^n$. Докажите, что $e = e^2$.

$\diamondsuit$ Заметим, что

$$r^n = a \cdot r^{n+1} = a\left(ar^{n+1}\right) r = \ldots = a^m \cdot r^{n+m}$$

для любого целого числа $m \geq 1$. Следовательно,

$$e^2 = a^n r^n a^n r^n = a^{2n} r^{2n} = a^n\left(a^n r^{2n}\right) = a^n r^n = e$$

$\diamondsuit$

Упражнение 1.56. *Пусть L_1 – максимальный модулярный левый идеал и L – модулярный левый идеал кольца R. Докажите, что $L_1 \cap L$ – модулярный левый идеал R. В частности, пересечения конечного числа максимальных левых модулярных идеалов снова является модулярным идеалом.*

$\diamondsuit$ Если $L \subseteq L_1$, то $L \cap L_1 = L$ – модулярный левый идеал. Если $L \nsubseteq L_1$, то $R = L_1 + L$. Пусть e_1, e – такие элементы в R, что $x(1-e) \in L$, $x(1-e_1) \in L_1$ для любого элемента $x \in R$. Тогда $e_1 = a_1 + b_1$, $e = a_2 + b_2$, где $a_1, a_2 \in L_1$, $b_1, b_2 \in L$. Положим $f = a_2 + b_1$. Тогда для любого элемента $x \in R$ имеем

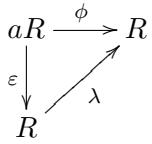
$$x - xf = (x - xe_1) + x(e_1 - f) = (x - xe_1) + x(a_1 - a_2) \in L_1,$$

$$x - xf = (x - xe) + x(e - f) = (x - xe) + x(b_2 - b_1) \in L.$$

Следовательно, $(x - xf) \in L_1 \cap L$ и $L_1 \cap L$ – модулярный левый идеал R. $\diamondsuit$

Упражнение 1.57. *Пусть R – ассоциативное кольцо с единицей. Докажите, что для любого элемента $a \in R$ $Ra = \ell(r(a))$ тогда и только тогда, когда R – модульное отображение каждого главного правого идеала в R продолжается на весь R_R.*

$\diamondsuit$ Пусть для любого правого главного идеала aR и для любого R-модульного отображения $\phi : aR \to R$ существует R-модульный гомоморфизм $\lambda : R \to R$ такой, что диаграмма



является коммутативной (ε – тождественное отображение). Докажем, что для любого элемента $b \in R$ $Rb = \ell(r(b))$. Заметим, что $Rb \subseteq \ell(r(b))$. Докажем обратное включение. Пусть $c \in \ell(r(b))$. Рассмотрим отображение $\phi : bR \to R$ такое, что $\phi(bx) = cx$. Оно является корректным, так как если $bx = 0$, то $x \in r(b)$ и, следовательно, $cx = 0$. Отображение ϕ является R-модульным гомоморфизмом. Оно продолжается до гомоморфизма $R_R \xrightarrow{\lambda} R_R$ В частности, $c = \lambda(b) = \phi(b)$ и $c = \lambda(1)b \in Rb$. Итак, $Rb = \ell(r(b))$.

Докажем обратное утверждение. Пусть для любого элемента $a \in R$ справедливо равенство $Ra = \ell(r(a))$. Рассмотрим произвольный R-модульный гомоморфизм $aR \xrightarrow{\psi} R$. Пусть $b = \psi(a)$. Если $x \in r(a)$, то $bx = \psi(a)x = \psi(ax) = \psi(0) = 0$, то есть $b \in \ell(r(a)) = Ra$. Следовательно, $b = ca$ для некоторого элемента $c \in R$. Рассмотрим отображение $\lambda : R \to R$ такое, что для любого $r \in R$ $\lambda(r) = cr$. Это отображение является R-гомоморфизмом, и если $ax \in aR$, то $\lambda(ax) = cax = (ca)x = bx = \psi(a)x = \psi(ax)$, то есть λ продолжает отображение ψ. $\diamondsuit$

Упражнение 1.58. *Докажите, что кольцо классов вычетов $\mathbb{Z}_n$ не содержит идемпотентов, отличных от $\bar{0}$ и $\bar{1}$ тогда и только тогда, когда $n = p^m$, где p – простое число.*

Упражнение 1.59. *Докажите, что кольцо $\begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & 0 \end{pmatrix}$ содержит бесконечное число левых единиц, но не имеет правых единиц.*

Упражнение 1.60. *Пусть R – кольцо без нильпотентных элементов и $e^2 = e \in R$. Докажите, что e принадлежит центру кольца R и $R = eRe \oplus (1 - e)R(1 - e)$.*

Упражнение 1.61. *Пусть R – кольцо и для любого элемента $0 \neq a \in R$ существует единственный элемент $b \in R$ такой, что $aba = a$. Докажите, что R – тело.*

$\diamondsuit$ Если $a \neq 0$, $b \neq 0$ и $ab = 0$, то пусть $x \in R$ – такой элемент, что $axa = a$. Тогда $a(x + b)a = a$. По условию $x = x + b$, откуда следует, что $b = 0$. Противоречие. Следовательно, R – кольцо без делителей нуля. Пусть $0 \neq a \in R$. Тогда $axa = a$ для некоторого элемента $x \in R$. Следовательно, $axax = ax = e$ – идемпотент. Так как

$$eb(1 - e)e = e(1 - e)be = e(1 - e)b(1 - e) = 0,$$

то $R = eRe$ и e является единицей кольца R. Заметим, что $ax = e$. Аналогично доказывается, что xa – идемпотент. Следовательно, он равен e и R – тело. $\diamondsuit$

Упражнение 1.62. *Пусть F – поле и*

$$A = \{a + bi + cj + dk |\ \ a, b, c, d \in F,\ i^2 = j^2 = k^2 = -1,\\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j\}$$

– алгебра кватернионов над полем F. Докажите, что

1. *если $F = \mathbb{Q}$ или $F = \mathbb{R}$, то A – тело;*
2. *если $F = \mathbb{Z}_2$ или $F = \mathbb{C}$, то A не является телом.*

Упражнение 1.63. *Пусть R – кольцо, содержащее единицу и $I \lhd M_n(R)$. Докажите, что $I = M_n(K)$, где $K \lhd R$.*

Упражнение 1.64. *Пусть $R = M_n(\mathbb{Z}_{p^m})$, где p – простое число. Докажите, что $J(R) = M_n(\overline{p} \cdot \mathbb{Z}_{p^m})$*

Упражнение 1.65. *Докажите, что простые коммутативные кольца являются полями.*

Упражнение 1.66. *Пусть R имеет ненулевой минимальный правый идеал. Докажите, что сумма всех минимальных правых идеалов кольца R является двусторонним идеалом.*

Упражнение 1.67. *Пусть $I \lhd R$. Докажите, что*

1. *$M_n(R/I) \cong M_n(R)/M_n(I)$;*
2. *$(R/I)[x] \cong R[x]/I[x]$.*

Упражнение 1.68. *Докажите, что идеал $R(x-a)+R(y-b)$ является максимальным в алгебре многочленов $R = \mathbb{C}[x, y]$, где $a, b \in \mathbb{C}$ и он не является главным.*

Упражнение 1.69. *Пусть R – кольцо с единицей и $P \lhd R$. Докажите, что $M_n(P)$ простой идеал в $M_n(R)$ тогда и только тогда, когда P – простой идеал в R.*

Упражнение 1.70. *Пусть R – простое кольцо и e – левая единица кольца R. Докажите, что e – единица кольца R.*

$\diamondsuit$ Рассмотрите равенство $(ae-a)x=(ae-a)(ex)=0$. $\diamondsuit$

Упражнение 1.71. *Пусть $A \leq_r M_n(D) = R$, где D – тело. Докажите, что $A = eR$, где $e = e^2$.*

$\diamondsuit$ Разложим $R = A_1 \dotplus A_2 \dotplus \ldots \dotplus A_n$ в прямую сумму минимальных правых идеалов $A_1, A_2, \ldots, A_n$. Для любого числа $i \leq n$ либо $A \cap A_i = (0)$, либо $A \cap A_i = A_i$. Если $A_1 \not\subseteq A$, то рассмотрим $A_1 \dotplus A = B_1$. Если $B_1 \neq R$, то, например, $A_2 \cap B_1 = (0)$ и рассмотрим $B_1 \dotplus A_2 = B_2$. Рассуждая аналогично, мы приходим к равенству $R = A \dotplus C$, где $C \leq_r R$. Если $1 = e + f$, где $e \in A$, $f \in C$, то $A = eR$ и $e = e^2$. $\diamondsuit$

Упражнение 1.72. *Пусть V – n-мерное векторное пространство над телом D и $R = \operatorname{End}_D V \cong M_n(D)$. Пусть $A \leq_r R$,*

$$A^* = \{v \in V |\ vA = (0)\} \leq V$$

и

$$A^{**} = \{a \in R |\ A^*a = (0)\}.$$

Докажите, что $A = A^{**}$ и каждая цепочка правых идеалов в R содержит не более $n+1$ членов.

$\diamondsuit$ Известно, что $A = eR$, где $e^2 = e$ (см. упражнение 1.71). Тогда

$$A^* = (0:e) = \{v \in V |\ vA = (0)\} = \\ = \{v \in V |\ ve = 0\} = v_1D + \ldots + v_kD,$$

где $k = \dim_D A^*$. Докажем, что $A^{**} = \bigcap\limits_{i=1}^{k} (0:v_i) = A$. Пусть r – произвольный элемент A^{**}. Тогда $v_1r = \ldots = v_kr = 0$. Пусть

$$Ve = f_{k+1}D + \ldots + f_nD,$$

где $f_i = v_i e$, $k+1 \le i \le n$ – базис Ve. Тогда

$$V = A^* \dotplus \langle v_{k+1}, \ldots, v_n \rangle$$

и существует линейное преобразование $s \in R$ такое, что

$$(v_{k+1}e)\, s = v_{k+1}r, \ \ldots, \ (v_n e)s = v_n r.$$

Тогда

$$V = v_1 D + \ldots + v_k D + v_{k+1} D + \ldots + v_n D$$

и $v_i(es - r) = 0$ для любого числа $i \le n$, то есть $r = es \in eR = A$. Для доказательства второго утверждения заметим, что если $A \subseteq B$ – два правых идеала в R, то $B^* \subseteq A^*$ – соответствующие подпространства в V и если $A^* = B^*$, то $A = A^{**} = B^{**} = B$. $\diamondsuit$

Упражнение 1.73. *Пусть*

$$A = M_2(\mathbb{Z}), \ B = M_2(2\mathbb{Z}) \ \ и \ \ C = \begin{pmatrix} 4\mathbb{Z} & 4\mathbb{Z} \\ 2\mathbb{Z} & 2\mathbb{Z} \end{pmatrix}.$$

Докажите, что $B \lhd A$, $C \lhd B$, но C не является идеалом в A.

Упражнение 1.74 (лемма В. Андрунакиевича).
Пусть $C \lhd B \lhd A$ и $H = C + AC + CA + ACA \subseteq B$. Докажите, что $H^3 \subseteq C \subseteq H \subseteq B$, то есть C содержит идеал H^3 кольца A. В частности, C – нильпотентное кольцо тогда и только тогда, когда H – нильпотентное кольцо.

$\diamondsuit$ Имеем, что $H^3 \subseteq BHB = B(C + AC + CA + ACA)B \subseteq BCB + (BA)CB + BC(AB) + (BA)C(AB) \subseteq BCB \subseteq B$. $\diamondsuit$

Упражнение 1.75. *Кольцо A называется подпрямо неразложимым, если пересечение M всех его ненулевых идеалов не равно нулю (M называется сердцевиной A). Докажите, что произвольное кольцо является подпрямой суммой подпрямо неразложимых колец.*

$\diamondsuit$ Воспользоваться леммой Цорна. $\diamondsuit$

Упражнение 1.76. *Пусть R – подпрямо неразложимое кольцо с сердцевиной $M \neq (0)$. Докажите, что $M^2 = (0)$, либо M – простое кольцо.*

$\diamondsuit$ Если $S \subseteq R$, то обозначим

$$r(S) = \{x \in R |\ Sx = (0)\} <_r R,\ \ell(S) = \{x \in R |\ xS = (0)\} <_e R.$$

Пусть $M^2 \neq (0)$ и $I \lhd M$, $I \neq (0)$. Рассмотрим идеал $MIM \subseteq I$. Если $MIM \neq (0)$, то $M \subseteq MIM \subseteq I$ и $M = I$. Если $MIM = (0)$, то $IM \subseteq r(M) \cap M = (0)$ и $IM = (0)$. Следовательно, $I \subseteq \ell(M) \cap M = (0)$. Противоречие. $\diamondsuit$

Упражнение 1.77. *Пусть A – коммутативное кольцо с единицей. Пусть $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in R = A[x_1, \ldots, x_n]$ – такие ненулевые многочлены в R, что $fg = 0$. Докажите, что существует ненулевой элемент $b \in A$, принадлежащий идеалу кольца A, порожденному коэффициентами $g(x_1, \ldots, x_n)$, такой, что $f(x_1, \ldots, x_n)b = 0$.*

$\diamondsuit$ Рассмотрим лексикографический порядок на множестве слов от $\{x_1, \ldots, x_n\}$:

$$x_1^{a_1} \ldots x_n^{a_n} > x_1^{b_1} \ldots x_n^{b_n},$$

если существует индекс i такой, что

$$a_i > b_i \ \text{ и } \ a_1 = b_1,\ \ldots,\ a_{i-1} = b_{i-1}.$$

Представим f, g в виде

$$f = \sum_{i=1}^{s} \alpha_i m_i, \quad g = \sum_{j=1}^{t} \beta_j n_j,$$

где $\alpha_i, \beta_i \in A$, $m_1 > \ldots > m_s$, $n_1 > \ldots > n_t$. Для доказательства воспользуемся методом математической индукции относительно чисел s и t. Если $s = 1$ или $t = 1$, то положим $b = \beta_1$. Пусть $t \geq 2$. Тогда $\alpha_s \beta_t = 0$. Рассмотрим $\alpha_s g$. Если $\alpha_s g \neq 0$, то

$f \cdot (\alpha_s g) = 0$, число слагаемых в $(\alpha_s g)$ меньше t и по предположению индукции существует элемент $0 \neq b \in A$, принадлежащий идеалу, порожденному коэффициентами $(\alpha_s g)$, такой, что $f \cdot b = 0$. Если $\alpha_s g = 0$, то

$$f_1 = \sum_{i=1}^{s-1} \alpha_i m_i = f - \alpha_s m_s$$

удовлетворяет равенству $f_1 g = 0$. По предположению индукции существует элемент $b \neq 0$, принадлежит идеалу, порожденному всеми коэффициентами g такой, что $f_1 b = 0$. Так как $\alpha_s b = 0$, то $fb = 0$. $\diamondsuit$

Упражнение 1.78. *Найдите в алгебре матриц $M_2(\mathbb{C})$ такой базис $\{1, u, v, w\}$, что $u^2 = v^2 = w^2 = -1$, $uv = -vu = w$, $wv = -u$, $vw = u$, $wu = v = -uw$.*

$\diamondsuit$ Пусть

$$u = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ v = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ w = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Тогда $\{1, u, v, w\}$ – искомый $\mathbb{C}$ – базис $M_2(\mathbb{C})$. $\diamondsuit$

Упражнение 1.79. *Пусть $V - GF(q)$ – подпространство кольца $M_n(GF(q))$, состоящее из вырожденных матриц. Докажите, что $\dim_{GF(q)} V \leq n^2 - n$.*

$\diamondsuit$ Поле $GF(q^n)$ является n-мерной $GF(q)$-алгеброй. Используя (правое) регулярное представление, мы можем считать, что

$$GF(q^n) \subseteq M_n(GF(q))$$

и матрицы, представляющие элементы, этого поля являются невырожденными. Если $\dim_{GF(q)} V \geq n^2 - n + 1$, то порядок $|V| \geq q^{n^2-n+1}$. Пусть

$$GF(q^n) = \{0 = a_1, a_2, \ldots, a_{q^n}\}.$$

Тогда $(a_i+V)\cap(a_j+V)=\varnothing$ при $i\neq j$ и $\bigcup\limits_{i=1}^{q^n}(a_i+V)$ содержит не менее $q^{n^2-n+1}\cdot q^n=q^{n^2+1}$ различных элементов. Противоречие. $\diamondsuit$

Упражнение 1.80. *Пусть*

$$R_1=\prod_{n=0}^{\infty}GF\left(p^{q^{2n}}\right)\ \ и\ \ R_2=\prod_{n=0}^{\infty}GF\left(p^{q^{2n+1}}\right),$$

где p, q – простые числа. Тогда R_1, R_2 – коммутативные кольца с единицами, не содержащие нильпотентных элементов такие, что они не являются изоморфными кольцами, но вложимыми друг в друга.

$\diamondsuit$ Если $\varphi: R_1\to R_2$ – изоморфизм колец и $e_1=(1,0,0,\ldots)\in R_1$, то $\varphi(e_1)=(\ldots,1,\ldots)$ и $\varphi(e_1R_1)=\varphi(GF(p))=\varphi(e_1)R_2$ – прямое произведение полей, не изоморфных $GF(p)$. $\diamondsuit$

Упражнение 1.81. *Пусть F – некоторое поле и φ – автоморфизм алгебры $M_n(F)$. Тогда существует матрица $s\in M_n(F)$ такая, что $\varphi(x)=s^{-1}xs$ для любой матрицы $x\in M_n(F)$.*

$\diamondsuit$ Пусть $\{e_{ij}|\ 1\leq i,j\leq n\}$ – система из n^2 матричных единиц алгебры $M_n(F)$ и $\{f_{ij}=\varphi(e_{ij})\}$ – ее образ. Тогда $\{f_{ij}\}$ – система матричных единиц, и пусть $f_{11}=\sum d_{st}e_{st}$, где, например, $d_{pq}\neq 0$. Положим $a=d_{pq}^{-1}e_{1p}f_{11}$, $b=f_{11}e_{q1}$. Докажем, что $ab=e_{11}$, $ba=f_{11}$. Действительно,

$$ab=d_{pq}^{-1}e_{1p}f_{11}e_{q1}=d_{pq}^{-1}d_{pq}e_{11}=e_{11},$$

$$ba=(f_{11}e_{q1}e_{1p}f_{11})\,d_{pq}^{-1}=d_{pq}^{-1}\,(f_{11}e_{qp}f_{11})=d_{pq}^{-1}\cdot u_{11}\cdot f_{11},$$

где $e_{qp}=\sum u_{st}f_{st}$, $u_{st}\in F$.

Далее, $(ba)^2=b(ab)a=be_{11}a=ba$ в поле $f_{11}F_nf_{11}\cong F$. Следовательно, $d_{pq}^{-1}u_{11}=1$ и $ba=f_{11}$. Положим

$$h=\sum_{i=1}^{n}e_{i1}af_{1i}\ \ и\ \ g=\sum_{j=1}^{n}f_{j1}be_{1j}.$$

Тогда

$$h \cdot g = \sum_{i,j} e_{i1} a f_{11} f_{1i} f_{j1} b e_{1j} = \sum_i e_{i1} a f_{11} b e_{1i} =$$

$$= \sum_i e_{i1}(ab)e_{1i} = \sum_i e_{ii} = 1$$

и

$$g e_{st} g^{-1} = g e_{st} h = f_{s1} b e_{1s} e_{st} e_{t1} a f_{1t} = f_{s1} (f_{11}) f_{1t} = f_{st} = \varphi(e_{st})$$

Следовательно, $\varphi(x) = gxg^{-1} = h^{-1}xh$ для любого элемента $x \in M_n(F)$. $\diamondsuit$

Упражнение 1.82. *Пусть $\mathbb{C}$ – поле комплексных чисел и G, H – конечные абелевы группы, порядки которых равны. Докажите, что групповые алгебры $\mathbb{C}(G)$ и $\mathbb{C}(H)$ изоморфны.*

Упражнение 1.83. *Пусть $K = GF(2)(t)$ – поле рациональных функций и*

$$A = K[x]/\left(x^4 - t^2\right),$$

где $\left(x^4 - t^2\right)$ – идеал кольца многочленов $K[x]$, порожденный многочленом $x^4 - t^2 = \left(x^2 - t\right)^2$. Найдите $J(A)$ и докажите, что в A нет подалгебры, изоморфной $A/J(A)$. В частности, A не представима в виде $B \dotplus J(A)$, где B – подалгебра, изоморфная $A/J(A)$.

$\diamondsuit$ Заметим, что

$$A = K \cdot \bar{1} + K \cdot \bar{x} + K \cdot \bar{x}^2 + K \cdot \bar{x}^3$$

и $J(A) \supseteq \left(x^2 - t\right)$. Если $\bar{f}(x) \in J(A)$ и

$$f(x) = \left(x^2 - t\right)\varphi(x) + ax + b,$$

где $a, b \in K$, то $a\bar{x} + b \in J(A)$,

$$(a\bar{x} + b)^2 = a^2x^2 + b^2,$$

$$(a\bar{x}+b)^4 = a^4\bar{x}^4 + b^4 = a^4t^2 + b^4 = 0$$

и в поле K

$$t^2 = \frac{a\left(t^4\right)}{b\left(t^4\right)}.$$

Противоречие. Следовательно, $J(A)$ совпадает с идеалом, порожденным многочленом $\left(\bar{x}^2 - t\right)$.

Фактор-алгебра $A/J(A) \cong K[x]/\left(x^2 - t\right)$ – двумерная алгебра, содержащая элемент, квадрат которого равен t. Если бы A содержала подалгебру B, изоморфную $A/J(A)$, то в B существовал бы элемент

$$a_0 1 + a_1\bar{x} + a_2\bar{x}^2 + a_3\bar{x}^3,$$

квадрат которого был бы равен t, то есть

$$\left(a_0 1 + a_1\bar{x} + a_2\bar{x}^2 + a_3\bar{x}^3\right)^2 = t.$$

Откуда следует, что

$$a_0^2 + a_1^2\bar{x}^2 + a_2^2t^2 + a_3^2t^2\bar{x}^2 = t$$

или

$$\left(a_0^2 + a_2^2t^2 + t\right) + \left(a_1^2 + a_3^2t^2\right)\bar{x}^2 = \bar{0}$$

и $t \in GF(2)(t^2)$. Противоречие. $\diamondsuit$

Глава 2

Ниль-радикалы колец

2.1. Теорема Нагаты-Хигмана

Пусть $A = GF(2)[x_1, x_2, \ldots]$ – кольцо коммутативных многочленов над полем $GF(2)$ от счетного множества порождающих элементов $\{x_1, x_2, \ldots\}$ и I – идеал A, порожденный элементами $\{x_1^2, x_2^2, \ldots\}$. Тогда алгебра $R = A/I$ удовлетворяет тождествам $x^2 = 0$, $[x, y] = 0$, но не является нильпотентной.

В работах Д. Дубнова, В. Иванова [72] и М. Нагата [105] было доказано, что ассоциативная алгебра над полем характеристики нуль, удовлетворяющая тождеству $x^n = 0$, является нильпотентной. В работе Г. Хигман [83] доказано, что произвольная ассоциативная алгебра над полем характеристики нуль или конечной характеристики $p > n$, удовлетворяющее тождеству $x^n = 0$, удовлетворяет также тождеству $x_1 x_2 \ldots x_N = 0$, где $N \leq 2^n - 1$. Наименьшее число N с этим свойством обозначим через $f(n)$. В этой работе отмечено также, что $f(2) = 3$, $f(3) = 6$ и доказана оценка снизу $f(n) > \frac{n^2}{e^2}$ для достаточно больших натуральных чисел n. В работе Е. Кузьмина [43] построен пример алгебры A над полем характеристики нуль, удовлетворяющей тождеству $x^n = 0$ и $A^{\frac{n(n+1)}{2}-1} \neq (0)$. Другими словами, $f(n) \geq \frac{n(n+1)}{2}$. Профессор Е. Кузьмин сформулиро-

вал гипотезу о том, что $f(n) = \frac{n(n+1)}{2}$ для любого целого числа $n \geq 1$. В работе Ю. Размыслова [59] доказано, что $f(n) \leq n^2$.

Справедлива следующая теорема.

Теорема 2.1 (Дубнова-Иванова-Нагаты-Хигмана). *Пусть A – ассоциативная алгебра над полем F характеристики нуль или конечной характеристики $p > n$. Если A удовлетворяет тождеству $x^n = 0$, то $A^{2^n-1} = (0)$.*

□ Доказательство теоремы проведем методом математической индукции относительно числа n. Если $n = 2$, то A удовлетворяет тождеству $x^2 = 0$. Подставим вместо x элемент $(a + b)$, где $a, b \in A$ и раскроем скобки. Мы получим равенство $ab + ba = 0$. Следовательно, для любых элементов $a, b, c \in A$ $(ab)c = -c(ab) = acb = -abc$ или $2(abc) = 0$. Так как по предположению 2 – обратимый элемент в поле F, то $abc = 0$ и $A^3 = (0)$. Предположим, что наше утверждение верно для алгебр, удовлетворяющих тождеству $x^{n-1} = 0$. Докажем его для алгебры A. Пусть $\alpha \in F$ и $a, b \in A$. Тогда

$$(a + \alpha b)^n = a^n + \alpha f_1(a, b) + \alpha^2 f_2(a, b) + \ldots + \alpha^n b^n,$$

где

$$f_1(a, b) = a^{n-1}b + a^{n-2}ba + \ldots + ba^{n-1}.$$

По условию поле F содержит $(n - 1)$ различных ненулевых элементов $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$. Систему равенств

$$\alpha_i f_1(a, b) + \alpha_i^2 f_2(a, b) + \ldots + \alpha_i^{n-1} f_{n-1}(a, b) = 0,$$

где $i \leq n - 1$, можно представить в матричном виде

$$\begin{pmatrix} \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_{n-1}^2 & \ldots & \alpha_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_{n-1} \end{pmatrix} = 0$$

Определитель этой матрицы равен

$$(\alpha_1\alpha_2\dots\alpha_{n-1})\cdot\prod_{i>j}(\alpha_i-\alpha_j)\neq 0.$$

Умножая слева левую и правую части матричного равенства на обратную матрицу

$$\begin{pmatrix} \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_{n-1}^2 & \dots & \alpha_{n-1}^2 \end{pmatrix}^{-1}$$

получим, что

$$f_1(a,b)=a^{n-1}b+\ldots+ba^{n-1}=0$$

для любых элементов $a,b\in A$. Пусть, далее, a, b, c – произвольные элементы A. Рассмотрим элемент

$$z=\sum_{i,j=0}^{n-1}a^icb^ja^{n-i-1}b^{n-j-1}.$$

Вычислим его двумя способами. Имеем, что

$$z=\sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1}a^i\left(cb^j\right)a^{n-i-1}\right)b^{n-j-1}=0,$$

так как $f_1(a,cb^j)=0$. С другой стороны,

$$z=\sum_{i=0}^{n-1}a^ic\left(\sum_{j=0}^{n-1}b^ja^{n-i-1}b^{n-j-1}\right)=n\left(a^{n-1}cb^{n-1}\right).$$

Так как $n\cdot 1$ – обратимый элемент в поле F, то $x^{n-1}yz^{n-1}=0$ тождество в алгебре A.

Пусть I-идеал алгебры A, порожденный всеми элементами вида $a^{n-1}, a\in A$. Тогда A/I удовлетворяет тождеству $x^{n-1}=0$

и по предположению индукции $A^{2^{n-1}-1} \subseteq I$. Так как из тождества $x^{n-1}yz^{n-1} = 0$ следует равенство $IAI = (0)$, то $A^{2^n-1} = A^{2^{n-1}-1} \cdot A \cdot A^{2^{n-1}-1} \subseteq IAI = (0)$. $\square$

Сделаем несколько замечаний о кольцах, удовлетворяющих тождеству $x^n = 0$. В выше приведенной работе Г. Хигмана доказано, что если I – векторное пространство свободной ассоциативной алгебры $F\langle x_1, x_2, \ldots\rangle$, порожденное всеми элементами вида a^n, где $a \in F\langle x_1, x_2, \ldots\rangle$, то I – идеал $F\langle x_1, x_2, \ldots\rangle$ (характеристика поля F либо равна нулю, либо простому числу $p > n$).

Я. Левицкий в работе [94] доказал, что кольцо, удовлетворяющее тождеству $x = 0$, совпадает со своим локально нильпотентным радикалом, то есть любое его конечно порожденное подкольцо является нильпотентным. Мы докажем этот результат в разделе 2.7 для произвольных ниль-колец, удовлетворяющих тождеству. Из теоремы Левицкого следует предложение.

Предложение 2.1. *Если кольцо R удовлетворяет тождеству $x^N = 0$, то полное кольцо матриц $M_k(R)$ также удовлетворяет некоторому тождеству вида $x^t = 0$.*

$\square$ Пусть $F = \mathbb{Z}\langle x_1, x_2, \ldots, x_{k^2}\rangle$ – свободное ассоциативное кольцо, порожденное элементами $\{x_1, x_2, \ldots, x_{k^2}\}$ и Q – вполне характеристический идеал (T-идеал) F, порожденный многочленом x_1^N. Тогда кольцо F/Q – k^2-порожденное кольцо, удовлетворяющее тождеству $x^N = 0$. По теореме Левицкого $(F/Q)^t = \bar{0}$ для некоторого числа $t \geq 1$ (см. раздел 2.7). В частности, $F^t \subseteq Q$. Пусть $A = (a_{ij}) \in M_k(R)$ и $S = \langle a_{ij}\rangle$ – подкольцо R, порожденное элементами $\{a_{ij} |\ 1 \leq i, j \leq n\}$. Тогда $S^t = (0)$ и $A^t = 0$, то есть $M_n(R)$ удовлетворяет тождеству $x^t = 0$. $\square$

Заметим также, что в работах А. Клейна [85, 86] доказаны следующие предложения.

Предложение 2.2. *Если кольцо R удовлетворяет тождеству $x^N = 0$, то кольцо многочленов $R[t]$ тоже удовлетворяет*

некоторому тождеству вида $x^m = 0$, *где* m – *натуральное число.*

Предложение 2.3. *Если* I, J – *правые идеалы кольца* R, *удовлетворяющие тождеству* $x^N = 0$, *то* $(I + J)$ *удовлетворяет некоторому тождеству вида* $x^m = 0$, *где* m – *натуральное число.*

2.2. Верхний ниль-радикал

Кольцо R называется *первичным*, если для любых ненулевых идеалов I_1, I_2 их произведение $I_1 \cdot I_2 \neq (0)$.

Предложение 2.4. *Кольцо* R *является первичным тогда и только тогда, когда для любых ненулевых элементов* $a, b \in R$ *существует элемент* $x \in R$ *такой, что* $axb \neq 0$.

□ Если R – первичное кольцо и $aRb = 0$, то $(a)R(b) = 0$. Если $a \neq 0$ и $b \neq 0$, то $(a) \cdot R = 0$. Противоречие.

Пусть R – не первичное кольцо и $I_1 \cdot I_2 = (0)$, где I_1, I_2 – ненулевые идеалы R. Пусть $0 \neq a \in I_1$ и $0 \neq b \in I_2$, тогда $aRb = 0$. Противоречие. □

Кольцо R называется *полупервичным*, если оно не содержит ненулевых нильпотентных идеалов. Идеал $P \lhd R$ называется *простым*, если R/P – первичное кольцо. Множество всех простых идеалов R обозначается как $\operatorname{Spec} R$.

Ясно, что первичное кольцо будет полупервичным. Обратное утверждение неверно. Например, прямая сумма двух полей является полупервичным, но не первичным кольцом. Первичным кольцом является любое кольцо без делителей нуля, а полупервичным – любое кольцо без нильпотентных элементов.

Предложение 2.5. *Сумма двух ниль-идеалов кольца* R *является ниль-идеалом.*

□ Действительно, если $A \lhd R$, $B \lhd R$ и A, B – ниль-кольца, то $(A+B)/B \cong A/A\cap B$ – ниль-кольцо. Так как расширение ниль-кольца с помощью ниль-кольца является снова ниль-кольцом, то $(A+B)$ – ниль-кольцо. □

Обозначим через $\mathrm{un}(R)$ сумму всех ниль-идеалов кольца R. Из предложения 2.5 следует, что $\mathrm{un}(R)$ – наибольший ниль-идеал кольца R. Он называется *верхним ниль-радикалом* кольца R.

Предложение 2.6. $\mathrm{un}\,(R/\mathrm{un}(R)) = \bar{0}$.

□ Если $\mathrm{un}\big(R/\mathrm{un}(R)\big) = A/\mathrm{un}(R)$, где A – идеал R, содержащий $\mathrm{un}(R)$, то A является расширением ниль-кольца $\mathrm{un}(R)$ с помощью ниль-кольца $A/\mathrm{un}(R)$. Следовательно, A – ниль-идеал. Поэтому $A \subseteq \mathrm{un}(R)$ и $\mathrm{un}\big(R/\mathrm{un}(R)\big) = \bar{0}$. □

До сих пор не решена проблема Кете: если кольцо R содержит односторонний ненулевой ниль-идеал, то содержит ли R двусторонний ненулевой ниль-идеал?

Теорема 2.2. *Если R не содержит ненулевых ниль-идеалов, то R – подпрямое произведение первичных колец без ненулевых ниль-идеалов.*

□ Пусть $a \in R$, $a \neq 0$ и s – некоторый ненильпотентный элемент в (a). По лемме Цорна существует максимальный идеал I_a такой, что $I_a \cap \{s, s^2, s^3, \dots\} = \varnothing$. Если $A \lhd R$, $B \lhd R$ и $AB \subseteq I_a$, то, предполагая, что $A \not\subset I_a$, $B \not\subset I_a$, имеем, что идеалы $A + I_a$, $B + I_a$ пересекаются с множеством $\{s^n |\ n \geq 1\}$. Пусть, например, $s^i = a + i_1$, $s^j = b + i_2$, тогда $s^{i+j} \in AB + I_a \subseteq I_a$. Противоречие доказывает, что I_a – простой идеал.

Если $\mathrm{un}\big(R/I_a\big) = C/I_a \neq (\bar{0})$, то идеал C строго содержит I_a и, следовательно, пересекается с $\{s^n |\ n \geq 1\}$. Если $s^n \in C$, то $(\bar{s}^n)^m = \bar{0}$ для некоторого целого $m \geq 1$, то это означает, что $s^{nm} \in I_a$. Противоречие доказывает, что R/I_a не имеет ненулевых ниль-идеалов.

Рассмотрим пересечение $\bigcap\limits_{a\neq 0} I_a$. Если оно содержит элемент $b \neq 0$, то $b \in I_b$. Противоречие. Итак, R – подпрямое произведение первичных колец R/I_a, $a \neq 0$ без ниль-идеалов. □

2.3. Локально нильпотентный радикал

Кольцо R называется *локально нильпотентным*, если любое его конечно порожденное подкольцо является нильпотентным.

Предложение 2.7. *Пусть $A = \langle a_1, \ldots, a_n\rangle$ – конечно порожденное кольцо. Тогда любая его степень A^m тоже является конечно порожденным кольцом.*

□ Заметим, что A^2 порождается конечным множеством

$$\{a_i a_j, a_i a_j a_s\},$$

A^3 порождается конечным множеством

$$\{a_i a_j a_s, a_i a_j a_s a_t, a_i a_j a_s a_t a_e\}$$

и, наконец, A^m порождается всеми словами от образующих $\{a_1, \ldots, a_n\}$, длина которых не превосходит $(2m-1)$. □

Предложение 2.8.

1. *Если R – локально нильпотентное кольцо и $I \lhd R$, то R/I – локально нильпотентное кольцо.*

2. *Если I_1, I_2 – локально нильпотентные идеалы кольца R, то $(I_1 + I_2)$ – локально нильпотентный идеал.*

3. *Если I – правый локально нильпотентный идеал R, то $(I + RI)$ – двусторонний локально нильпотентный идеал R.*

□ Первое утверждение очевидно. Докажем второе. Пусть S – конечно порожденное подкольцо в $I_1 + I_2$. Тогда $(S + I_2)/I_2$ – нильпотентное кольцо в $(I_1 + I_2)/I_2 \cong I_1/I_1 \cap I_2$. Если $S^m \subseteq I_2$, то из конечной порожденности S^m следует нильпотентность $(S^m)^k = S^{mk} = 0$. Таким образом, $(I_1 + I_2)$ – локально нильпотентное кольцо.

Докажем третье утверждение. Пусть S – подкольцо $I + RI$, порожденное

$$a_1 = i_1 + \sum a_{1t} i_{1t},\ \ldots,\ a_m = i_m + \sum a_{mt} i_{mt},$$

где $i_t, i_{st} \in I$ и $a_{it} \in R$. Множество $\{i_t, i_{st}, i_t a_{pq}, i_{st} a_{pq}\}$ является конечным и порождает в I нильпотентное подкольцо T, например, $T^N = 0$. Тогда подкольцо, порожденное элементами $\{a_1, a_2, \ldots, a_m\}$, является нильпотентным индекса N. □

Пусть $L(R)$ – сумма всех локально нильпотентных идеалов R. Этот идеал является наибольшим локально нильпотентным идеалом в R. Он называется *радикалом Левицкого* (в честь израильского математика Я. Левицкого, который ввел в рассмотрение данный радикал).

Предложение 2.9.

1. *$L(R)$ содержит все односторонние локально нильпотентные идеалы.*

2. *Если $B \triangleleft A$ – локально нильпотентный идеал такой, что A/B – локальнонильпотентное кольцо, то A – локально нильпотентное кольцо.*

3. *$L\big(R/L(R)\big) = \bar{0}$.*

□ Доказательство первого утверждения следует из предыдущего предложения. Докажем второе утверждение. Если S – конечно порожденное подкольцо A, то $(S+B)/B$ – конечно порожденное подкольцо A/B и, следовательно, $\big((S+B)/B\big)^m = \bar{0}$. Это влечет за собой включение $S^m \subseteq B$. Так как S^m – конечно

порожденное подкольцо, то $(S^m)^p = S^{mp} = 0$. Это означает, что A – локальнонильпотентное кольцо.

Пусть далее $L\big(R/L(R)\big) = A/L(R)$, где $A \lhd R$, содержащий $L(R)$, тогда A – расширение локально нильпотентного кольца $L(R)$ с помощью локально нильпотентного кольца $A/L(R)$. Согласно второму утверждению, $A \subseteq L(R)$ и, следовательно, $L(R/L(R)) = \bar{0}$. □

Теорема 2.3 (А. Бабич). *Пусть $L(R) = 0$, тогда R – подпрямое произведение первичных колец с нулевым радикалом Левицкого.*

□ Пусть

$$V = \{P \in \operatorname{Spec} R \mid L(R/P) = \bar{0}\}$$

и

$$K = \bigcap_{P \in V} P.$$

Если $K \neq (0)$, то K содержит ненулевой элемент a. Идеал (a) не является локально нильпотентным, поэтому (a) содержит конечно порожденное ненильпотентное подкольцо T. Рассмотрим множество идеалов

$$\mathcal{M} = \{I \lhd R \mid T^n \nsubseteq I \text{ для любого целого числа } n \geq 1\}.$$

Ясно, что $(0) \in \mathcal{M}$ и $\mathcal{M}$ удовлетворяет условию леммы Цорна По лемме Цорна $\mathcal{M}$ содержит максимальный идеал $P \in \mathcal{M}$. Если $P \notin \operatorname{Spec} R$, то для некоторых идеалов $A, B \lhd R$, строго содержащих P, их произведение $A \cdot B$ содержится в P. Так как $A \notin \mathcal{M}$ и $B \notin \mathcal{M}$, то $A \supseteq T^s$, $B \supseteq T^t$ и $P \supseteq T^{s+t}$. Противоречие доказывает, что $P \in \operatorname{Spec} R$.

Если $L(R/P) = C/P \neq (\bar{0})$, где $C \lhd R$, то C содержит некоторую степень T^m подкольца T (ибо $C \notin \mathcal{M}$). Так как T^m – конечно порожденное кольцо, то $(T^m + P)/P$ – нильпотентное кольцо. Поэтому $(T^m)^l \subseteq P$ для некоторого числа $l \geq 1$. Противоречие доказывает, что $P \in V$ и $T \subseteq (a) \subseteq P$. Противоречие. Итак, $K = (0)$ и R – подпрямое произведение первичных колец R/P, где $P \in \operatorname{Spec} R$, имеющих нулевой радикал Левицкого.

2.4. Нижний ниль-радикал

Предложение 2.10.

1. *Если R – нильпотентное кольцо и $I \lhd R$, то R/I – нильпотентное кольцо.*

2. *Если $B \lhd A$ и B, A/B – нильпотентные кольца, то A – нильпотентное кольцо.*

3. *Если $I <_r R$, $I^n = 0$, то двусторонний идеал $I + RI$ является нильпотентным кольцом.*

4. *Если $I_1 \lhd R$, $I_2 \lhd R$, $I_1^n = I_2^n = 0$, то $I_1 + I_2$ – нильпотентный идеал R.*

□ Докажем последовательно все утверждения, начиная с первого.

Если $R^n = 0$, то $(R/I)^n = \bar{0}$.

Пусть $B \lhd A$ и $B^n = 0$, $(A/B)^m = \bar{0}$. Тогда очевидно, что $A^m \subseteq B$ и $A^{mn} = (A^m)^n \subseteq B^n = 0$.

Если $I <_r R$, то индукцией по числу $k \geq 1$ легко доказать, что $(I + RI)^k \subseteq I^k + RI^k$. Откуда следует, что $(I + RI)^n = 0$.

Докажем утверждение 4. Рассмотрим фактор-кольцо

$$(I_1 + I_2)/I_2 \cong I_1/I_1 \cap I_2.$$

Оно является нильпотентным кольцом (как гомоморфный образ I_1). По утверждению 2, $(I_1 + I_2)^{n^2} = 0$. □

Из этого предложения следует, что сумма конечного числа нильпотентных идеалов кольца R является снова нильпотентным идеалом. Поэтому сумма всех нильпотентных идеалов кольца R является локально нильпотентным идеалом, но, в общем случае, ненильпотентным идеалом.

Для каждого порядкового числа α определим идеал $\mathcal{N}(\alpha)$ кольца R следующим образом:

1. $\mathcal{N}(0) = 0$;

2. $N(1)$ – сумма всех нильпотентных идеалов кольца R;

3. Пусть $\mathcal{N}(\beta)$ определен для всех трансфинитных чисел $\beta < \alpha$. Если $\alpha = \gamma + 1$, то $\mathcal{N}(\alpha)$ – идеал кольца R такой, что $\mathcal{N}(\alpha)/\mathcal{N}(\gamma)$ – сумма всех нильпотентных идеалов кольца $R/\mathcal{N}(\gamma)$. Если α – предельное порядковое число, то полагаем
$$\mathcal{N}(\alpha) = \sum_{\beta<\alpha} \mathcal{N}(\beta).$$
Существует такой ординал τ, что $\mathcal{N}(\tau) = \mathcal{N}(\tau+1)$. Идеал
$$\ln(R) = \mathcal{N}(\tau)$$
называется *нижним ниль-радикалом* кольца R (или *радикалом Бэра*).

Предложение 2.11.

1. $L(R) \supseteq lnR$.

2. $\ln(R/\ln R) = \bar{0}$.

3. *Радикал* $\ln R$ *содержит все односторонние нильпотентные идеалы.*

□ Докажем индукцией по α, что $N(\alpha)$ – локально нильпотентный идеал кольца R. Ранее мы отмечали, что $N(1) \subseteq L(R)$. Предположим, что $N(\beta) \subseteq L(R)$ для любого ординала $\beta < \alpha$. Если α – предельное трансфинитное число, то $N(\alpha) \subseteq L(R)$. Если $\alpha = \beta+1$, то $N(\alpha)$ является расширением локально нильпотентного идеала $N(\beta)$ с помощью локально нильпотентного идеала $N(\alpha)/N(\beta)$. Следовательно, $N(\alpha) \subseteq L(R)$ для любого порядкового числа α. Это означает, что $\ln R \subseteq L(R)$.

В силу предложения 2.10 каждый односторонний нильпотентный идеал порождает двусторонний нильпотентный идеал и, следовательно, содержится в $\ln R$.

Докажем второе утверждение. Пусть $\ln(R/\ln R) = A/\ln R$, где A – идеал R, содержащий $\ln R$. Если $A \neq \ln R = N(\tau) =$

$N(\tau+1)$, то существует идеал $C \not\subset \ln R$, $C \lhd R$, некоторая степень которого содержится в $\ln R$. Это означает, что $C \subseteq N(\tau+1)$. Противоречие доказывает, что $\ln(R/\ln R) = \bar{0}$. $\square$

Если $\ln R = 0$, то кольцо R является полупервичным.

Предложение 2.12. *R – полупервичное кольцо тогда и только тогда, когда для любого элемента $a \neq 0 \in R$, $aRa \neq (0)$.*

$\square$ Если $\ln R = 0$ и $aRa = (0)$ для некоторого элемента $a \in R$, то $(a)^3 = (0)$. Это означает, что $(a) = 0$ и $a = 0$. Обратно, если I – нильпотентный идеал кольца R (не равный нулю) и $I^n = 0$, $I^{n-1} \neq 0$, то для любого ненулевого элемента $a \in I^{n-1}$ справедливо равенство $aRa = (0)$. Противоречие доказывает наше предложение. $\square$

Предложение 2.13 (Р. Бэр).

$$\ln R = \bigcap_{P \in \operatorname{Spec} R} P.$$

$\square$ Если $P \in \operatorname{Spec} R$, то R/P – первичное кольцо и, следовательно, $N(1) \subseteq P$. Предположим, что $N(\beta) \subseteq P$ для всех ординалов $\beta < \alpha$. Если α – предельный ординал, то

$$N(\alpha) = \sum_{\beta<\alpha} N(\beta) \subseteq \ln R.$$

Если $\alpha = \gamma + 1$, то $(N(\alpha) + P)/P$ – сумма нильпотентных идеалов в первичном кольце R/P, откуда следует, что $N(\alpha) \subseteq P$ для любого ординала α, в частности, $\ln R = N(\tau) \subseteq P$, поэтому $\ln R \subseteq \bigcap_{P \in \operatorname{Spec} R} P$.

Предположим, что $\ln R \neq \bigcap_{P \in \operatorname{Spec} R} P$ и $a \in \bigcap_{P \in \operatorname{Spec} R} P$, $a \notin \ln R$. Тогда идеал (a) не является нильпотентным по модулю $\ln R$, в частности, $aRa \notin \ln R$ (см. также предложение 2.12). Пусть $a_1 = ab_1a \notin \ln R$. Аналогично существует такой элемент $a_2 =$

$a_1 b_2 a_1 \in (a)$, что $a_2 \notin \ln R$. Таким образом, мы можем построить счетную последовательность $\{a, a_1, a_2, \dots\}$ элементов из идеала (a) таких, что

1. $a_i \notin \ln R$;

2. $a_{n+1} = a_n b_{n+1} a_n$, $n = 1, 2, \dots$.

Пусть

$$\mathcal{M} = \{I \lhd R |\ \ln R \subseteq I,\ I \cap \{a, a_1, a_2, \dots\} = \varnothing\}.$$

Тогда $\ln R \in \mathcal{M}$. По лемме Цорна в $\mathcal{M}$ существует максимальный идеал $Q \lhd R$. Докажем, что $Q \in \operatorname{Spec} R$. Предположим противное. Тогда существуют такие идеалы $T, S \lhd R$, что $T \cdot S \subseteq Q$, $Q \subset T$, $Q \subset S$ ($Q \neq T$, $Q \neq S$). Ввиду максимальности идеала Q, идеалы T и S не принадлежат $\mathcal{M}$, поэтому существуют элементы a_i и a_j, принадлежащие соответственно T и S. Если $i \leq j$, то $a_j \in T$ и $a_j \in S$, поэтому $a_{j+1} = a_j b_{j+1} a_j \in T \cdot S \subseteq Q$. Противоречие доказывает, что Q – простой идеал. Это влечет за собой включение $(a) \subseteq Q$. Противоречие. Таким образом, $\ln R = \bigcap\limits_{P \in \operatorname{Spec} R} P$. $\square$

Из теоремы следует, что полупервичное кольцо является подпрямым произведением первичных колец.

2.5. Пример конечно-порожденной не нильпотентной ниль-алгебры

В работе Е. Голода [41] впервые был построен пример d порожденной алгебры над произвольным полем ($d \geq 2$), которая не является нильпотентной, хотя все ее подалгебры с $(d-1)$ порождающими нильпотентны. В частности, такая алгебра является ниль-алгеброй. В такой алгебре верхний ниль-радикал не совпадает с локально нильпотентным радикалом. Перейдем к построению примера Е. Голода.

Пусть F – произвольное поле и $T = F\langle x_1, x_2, \ldots, x_d\rangle$ – свободная ассоциативная алгебра от некоммутативных переменных $\{x_1, \ldots, x_d\}$. Пусть V_n – F-пространство T, порожденное элементами вида $x_{i_1}x_{i_2}\ldots x_{i_d}$. Ясно, что $\dim_F V_n = d^n$. Элементы V_n – однородные некоммутативные многочлены в T степени n. Заметим, что

$$T = V_0 \dot{+} V_1 \dot{+} V_2 \dot{+} \ldots, \quad V_0 = F.$$

Пусть $\{f_1, f_2, \ldots\}$ – множества однородных элементов T, степени которых удовлетворяют неравенствам $2 \leq n_1 \leq n_2 \leq \ldots$, где $n_i = \deg f_i$, $i = 1, 2, \ldots$. Обозначим через $I = (f_1, f_2, \ldots)$ – двусторонний идеал, порожденный этими многочленами и через r_i число таких элементов f_j, что $n_j = \deg f_j = i$. Фактор-алгебра $A = T/I$ представима в виде

$$A = A_0 \dot{+} A_1 \dot{+} A_2 \dot{+} \ldots, \quad A_i \cong V_i/I \cap V_i,$$

$i = 1, 2, \ldots$. Пусть $b_n = \dim A_n$, $n \geq 0$.

Теорема 2.4 (Е. Голод).
Алгебра A, построенная выше, имеет следующие свойства:

1. *Для любого числа $n \geq 1$*

$$b_n \geq db_{n-1} - \sum_{n_i \leq n} b_{n-n_i}.$$

2. *A – бесконечномерная алгебра, если для любого $i \geq 0$*

$$r_i \leq \left(\frac{d-1}{2}\right)^2.$$

□ Построим линейные отображения φ, ψ так, чтобы последовательность

$$(A_{n-n_1} \dot{+} \ldots \dot{+} A_{n-n_k} \dot{+} \ldots) \xrightarrow{\varphi} \left(\underbrace{A_{n-1} \dot{+} \ldots \dot{+} A_{n-1}}_{d}\right) \xrightarrow{\psi} A_n \to 0$$

была точной, то есть $\operatorname{Im}\varphi = \operatorname{Ker}\psi, \operatorname{Im}\psi = A_n$. Первая сумма берется по всем $n_i \leq n$, а вторая содержит d слагаемых. Из точности последовательности следует первое утверждение теоремы, так как

$$db_{n-1} = b_n + \dim_F(\operatorname{Ker}\psi) \leq b_n + \sum_{n_i \leq n} b_{n-n_i}.$$

Определим сначала линейные отображения Φ и Ψ в алгебре T

$$(V_{n-n_1} \dotplus \ldots \dotplus V_{n-n_k} \dotplus \ldots) \xrightarrow{\Phi} \left(\underbrace{V_{n-1} \dotplus \ldots \dotplus V_{n-1}}_{d} \right) \xrightarrow{\Psi} V_n \to 0$$

следующим образом:

1. Если
$$t_1 \dotplus t_2 \dotplus \ldots \dotplus t_\alpha \in \underbrace{V_{n-1} \dotplus \ldots \dotplus V_{n-1}}_{d},$$
то
$$(t_1 \dotplus \ldots \dotplus t_d)\,\Psi = \sum_{i=1}^{d} t_i x_i \in V_n.$$

2. Если

$$s_{n-n_1} \dotplus s_{n-n_2} \dotplus \ldots \dotplus s_{n-n_k} \dotplus \ldots \in V_{n-n_1} \dotplus \ldots \dotplus V_{n-n_k} \dotplus \ldots,$$

то $\sum\limits_i s_{n-n_i} f_i \in V_n$ и, следовательно, его можно представить в виде

$$\sum s_{n-n_i} f_i = \sum_{i=1}^{d} u_i x_i,$$

где $u_i \in V_{n-1}$. Положим

$$(s_{n-n_1} \dotplus \ldots \dotplus s_{n-n_k} \dotplus \ldots)\Phi = u_1 \dotplus \ldots \dotplus u_d.$$

Легко видеть, что Φ, Ψ – линейные отображения и Ψ – сюръективное отображение. Пусть $I_i = I \cap V_i$, где $i = 0, 1, 2, \ldots$. Если $t_1, \ldots, t_d \in I_{n-1}$, то учитывая $I \lhd T$, получаем $\sum\limits_i t_i x_i \in I_n$. Это позволяет определить корректное сюръективное отображение

$$\varphi : \underbrace{A_{n-1} \dot{+} \ldots \dot{+} A_{n-1}}_{d} \to A_n,$$

которое индуцируется Ψ.

Пусть $s_{n-n_1} \in I_{n-n_1}, s_{n-n_2} \in I_{n-n_2}, \ldots$. Тогда

$$\sum_{n_i \le n} s_{n-n_i} f_i = \sum_{i=1}^{d} u_i x_i \in I_n.$$

Покажем, что $\{u_1, u_2, \ldots, u_d\} \subseteq I_{n-1}$. Пусть

$$f_i = \sum_{j=1}^{d} g_{ij} x_j.$$

Тогда

$$s_{n-n_i} f_i = \sum_{j=1}^{d} (s_{n-n_i} g_{ij}) x_j,$$

$$\sum_{n_i \le n} s_{n-n_i} f_i = \sum_{j=1}^{d} \left(\sum_{n_i \le n} s_{n-n_i} g_{ij} \right) x_j$$

и

$$u_j = \sum_{n_i \le n} s_{n-n_i} g_{ij} \in I_{n-1},$$

так как $s_{n-n_i} \in I$ и u_j – однородный многочлен степени $(n-1)$.

Отображение Φ индуцирует соответствующее корректное отображение

$$\varphi : (A_{n-n_1} \dot{+} A_{n-n_2} \dot{+} \ldots) \to \underbrace{A_{n-1} \dot{+} \ldots \dot{+} A_{n-1}}_{d}.$$

Покажем, что справедливо включение $\operatorname{Im}\varphi \subseteq \operatorname{Ker}\psi$. Пусть $s_{n-n_1} \in V_{n-n_1}, s_{n-n_2} \in V_{n-n_2}, \ldots$. Тогда

$$(s_{n-n_1} \dot{+} s_{n-n_2} \dot{+} \ldots)\Phi\Psi = \sum_{i=1}^{d} u_i x_i = \sum_{n_i \leq n} s_{n-n_i} f_i \in I$$

и образ всего пространства $(V_{n-n_1} \dot{+} V_{n-n_2} \dot{+} \ldots)$ при отображении $\Phi\Psi$ содержится в $I_n \subseteq I$. Поэтому $\varphi \cdot \psi = 0$ и $\operatorname{Im}\varphi \subseteq \operatorname{Ker}\psi$. Покажем, что $\operatorname{Ker}\psi \subseteq \operatorname{Im}\varphi$. Пусть $(t_1 \dot{+} t_2 \dot{+} \ldots \dot{+} t_d)\Psi \in I$. Для доказательства включения $(t_1 \dot{+} \ldots \dot{+} t_d) \in \operatorname{Im}\varphi$ покажем, что существуют элементы $u_1, \ldots, u_d \in V_{n-1}$ такие, что $u_i \equiv t_i (\operatorname{mod} I_{n-1})$, $i \leq d$ и

$$\sum_{i=1}^{d} u_i x_i = \sum_{n_i \leq n} s_{n-n_i} f_i$$

для некоторых элементов $s_{n-n_i} \in V_{n-n_i}$. Так как по условию $\sum\limits_{i=1}^{d} t_i x_i \in I = (f_1, f_2, \ldots)$, то

$$\sum_{i=1}^{d} t_i x_i = \sum_{k,e} a_{ke} f_k b_{ke} + \sum_{k,e} c_{ke} f_k,$$

где a_{ke}, b_{ke}, c_{ke} – однородные многочлены и степень b_{ke} больше или равна единицы. Так как f_n – однородные многочлены, то можно считать, что $(a_{ke} f_k b_{ke})$ и $c_{ke} f_k$ принадлежат V_n. Пусть $b_{ke} = \sum\limits_{m=1}^{d} d_{kem} x_m$. Тогда

$$\sum_{k,e} a_{ke} f_k b_{ke} = \sum_{k,l,m} a_{ke} f_k d_{kem} x_m = \sum_{m=1}^{m} d_m x_m,$$

где $d_m = \sum\limits_{k,e} a_{ke} f_k d_{kem} \in I_{n-1}$. Полагая $u_i = t_i - d_i$, $i = 1, 2, \ldots, d$, получим, что $u_i \equiv t_i \,(\operatorname{mod} I_{n-1})$, $i \leq d$ и

$$\sum_{i=1}^{d} u_i x_i = \sum_{k,e} c_{ke} f_k = \sum_{k} \left(\sum_{e} c_{ke} \right) f_k,$$

где $\sum\limits_{e} c_{ke} \in V_{n-n_k}$. Следовательно, $\operatorname{Im}\varphi = \operatorname{Ker}\psi$ и последовательность

$$(A_{n-n_1} \dot{+} \ldots \dot{+} A_{n-n_k} \dot{+} \ldots) \xrightarrow{\varphi} (A_{n-1} \dot{+} \ldots \dot{+} A_{n-1}) \xrightarrow{\psi} A_n \to 0$$

является точной. Тем самым, первое свойство доказано.

Докажем второе свойство. Для формальных степенных рядов от переменной t с целыми коэффициентами определим бинарное отношение

$$\sum_{i=0}^{\infty} p_i t^i \geq \sum_{i=0}^{\infty} q_i t^i,$$

если $p_i \geq q_i$ для всех индексов i. Тогда согласно первому свойству имеем

$$\sum_{i=1}^{\infty} b_n t^n \geq d\left(\sum_{i=1}^{\infty} b_{n-1} t^n\right) - \sum_{i=1}^{\infty}\left(\sum_{n_i \leq n} b_{n-n_i}\right) t^n.$$

Далее,

$$\sum_{i=1}^{\infty}\left(\sum_{n_i \leq n} b_{n-n_i}\right) t^n = \sum_{n_i, m} b_m t^{n_i+m} =$$

$$= \sum_{i,m} r_i b_m t^{i+m} = \left(\sum_{i=2}^{\infty} r_i t^i\right)\left(\sum_{m=0}^{\infty} b_m t^m\right).$$

Пусть

$$P_A(t) = \sum_{m=0}^{\infty} b_m t^m.$$

Тогда, выше приведенное неравенство имеет вид

$$P_A(t) - 1 \geq dt P_A(t) - \left(\sum_{i=2}^{\infty} r_i t^i\right) P_A(t),$$

$$P_A(t)\left(1 - dt + \sum_{i=2}^{\infty} r_i t^i\right) \geq 1.$$

Так как

$$\left(1-dt+\sum_{i=2}^{\infty}r_it^i\right)^{-1}\geq\left(1-dt+\sum_{i=2}^{\infty}\left(\frac{d-1}{2}\right)^2t^i\right)^{-1}=$$

$$=(1-t)\left(1-\left(\frac{d+1}{2}\right)t\right)^{-2}\geq 1,$$

то все коэффициенты ряда $\left(1-dt+\sum\limits_{i=2}^{\infty}r_it^i\right)^{-1}$ неотрицательны и

$$P_A(t)\geq\left(1-dt+\sum_{i=2}^{\infty}r_it^i\right)^{-1}.$$

Неотрицательный ряд

$$f(t)=\left(1-dt+\sum_{i=2}^{\infty}r_it^i\right)^{-1}$$

не является многочленом, так как иначе ряд

$$f(t)\left(1+\sum_{i=2}^{\infty}r_it^i\right)=1+dtf(t)$$

тоже является многочленом. Если $n=\deg f(t)$, то, сравнивая коэффициенты при t^{n+2} в левой и правой частях, получим, что $r_2=0$. Аналогично $r_i=0$ при $i\geq 2$. Противоречие. Поэтому среди b_n существует бесконечно много положительных чисел и, следовательно, A – бесконечномерная алгебра. $\square$

Вернемся к построению примера. Пусть F – конечное или счетное поле и $T=F\langle x_1,x_2,x_3\rangle$ – свободная ассоциативная алгебра над полем F от трех некоммутативных переменных $\{x_1,x_2,x_3\}$, $d=3$. Тогда $T=T_0\dot{+}T_1\dot{+}T_2\dot{+}\ldots$, где $T_0=F\cdot 1$ и T_n – пространство однородных многочленов степени n. Ясно, что $\dim_F T_n=3^n$. Рассмотрим идеал $B=T_1\dot{+}T_2\dot{+}T_3\dot{+}\ldots$. Это счетное множество $B=\{b_1,b_2,b_3,\ldots\}$. Пусть $m_1\geq 2$. Тогда

$$b_1^{m_1}=b_{12}+b_{13}+\ldots+b_{1k_1},$$

где $b_{1e} \in T_e$. Выберем целое число m_2, так, чтобы $b_2^{m_2} \in T_{k_1+1} \dot{+} T_{k_1+2} \dot{+} \ldots$. Тогда

$$b_2^{m_2} = b_{2k_1+1} \dot{+} \ldots \dot{+} b_{2k_2},$$

где $b_{2e} \in T_e$. Рассуждая аналогично, мы получим последовательности чисел $\{m_1, m_2, \ldots\}$ и $k_1 < k_2 < k_3 < \ldots$ такие, что

$$b_i^{m_i} = b_{ik_{i-1}+1} \dot{+} \ldots \dot{+} b_{ik_i},$$

где $b_{ie} \in T_e$.

Пусть I – идеал, порожденный всеми однородными многочленами b_{ij}. Каждое число $r_i = 0, 1$ и, следовательно, $r_i \leq \left(\frac{3-1}{2}\right)^2$. По теореме 2.4 алгебра $A = T/I$ имеет бесконечную размерность и содержит ниль-подалгебру B/I, порожденную тремя элементами $\bar{x}_1$, $\bar{x}_2$, $\bar{x}_3$. Ясно, что B/I – тоже бесконечномерная алгебра.

Пусть в выше приведенном примере $F = GF(p)$ и $a_1 = x_1 + I$, $a_2 = x_2 + I$, $a_3 = x_3 + I$ – элементы алгебры $A = T/I$. Обозначим через G мультипликативную полугруппу A, порожденную элементами $(1 + a_1)$, $(1 + a_2)$, $(1 + a_3)$. Любой элемент этой полугруппы имеет вид $(1 + b)$, где $b \in B/I$. Так как b – нильпотентный элемент, то $b^{p^n} = 0$ для некоторого целого числа $n \geq 1$ и $(1 + b)^{p^n} = 1 + b^{p^n} = 1$. Это означает, что G – конечно порожденная периодическая группа. Если G – конечная группа, то множество

$$\left\{ \sum_{g \in G} \alpha_g g \middle| \ \alpha_g \in GF(p) \right\}$$

являлось бы конечномерной подалгеброй, содержащей элемент $a_i = (1 + a_i) - 1$, $i \leq 3$. Следовательно, подалгебра B/I являлась бы конечномерной. Противоречие. Итак, G – периодическая 3-порожденная бесконечная группа (этот пример является решением проблемы Бернсайда).

2.6. Пример первичной алгебры с ненулевым радикалом Левицкого

Приведем далее пример первичной алгебры с ненулевым радикалом Левицкого (пример построен Е. Зельмановым).

Пусть $F = k\langle x, y\rangle$ – свободная ассоциативная алгебра с двумя образующими x, y над полем k и $W = \langle x, y\rangle$ – свободная полугруппа. Если $w \in W$, то $d(w)$ – степень w, а $d_x(w)$ – степень w относительно переменной x. Рассмотрим отображение

$$f : W \to Q^+,$$

полагая

$$f(w) = \frac{dw}{(d_x w)^2 + 1},$$

где $w \in W$.

Пусть I – идеал F, порожденный всеми словами w из W, с условием $f(w) < 1/2$. Тогда алгебра $R = F/I$ является первичной и элемент $x + I$ порождает локально нильпотентный идеал в R. Действительно, если $a \neq \bar{0}$ и $b \neq \bar{0}$ из R и

$$a = \sum \alpha_i a_i, \quad b = \sum \beta_i b_i,$$

где $a_i, b_j \in W \setminus I$, то, полагая

$$N = \left[\max_{i,j}(d_x a_i + d_x b_j)\right]^2 + 1,$$

имеем, что $a_i y^N b_j \notin I$. Следовательно, $a y^N b \notin I$. Это доказывает первичность алгебры R.

Рассмотрим конечное множество слов $w_1, \ldots, w_n \in W$ таких, что $d_x w_i \geq 1$, $i \leq n$. Пусть

$$M = 2 \max_{1 \leq i \leq n} (d(w_i)).$$

Тогда

$$f(w_{i_1}w_{i_2}\dots w_{i_M}) = \left(\sum_{i=1}^{M} dw_{i_t}\right) \Big/ \left(\sum_{j=1}^{M} d_x w_{i_t}\right)^2 + 1 \leq$$
$$\leq \frac{M \max d(w_{i_t})}{M^2+1} < \frac{1}{2}$$

и полугруппа, порожденная $w_1, \dots, w_n$, нильпотентна индекса M в алгебре R. Так как $f(x) = \frac{1}{2}$, то $\bar{x}$ порождает в R ненулевой локально нильпотентный идеал.

Построенные примеры показывают, что в общем случае включения

$$J(R) \supseteq \mathrm{un}(R) \supseteq L(R) \supseteq \mathrm{ln}(R)$$

являются строгими.

2.7. Ниль-радикалы колец, удовлетворяющих тождеству

Пусть $F[x_1, x_2, \dots]$ – коммутативное кольцо многочленов над полем F и I – идеал, порожденный элементами

$$\{x_1^2, x_2^3, x_3^4, \dots, x_n^{n+1}, \dots\}.$$

Пусть

$$A = F[x_1, x_2, \dots]/I$$

и B – подалгебра A, порожденная $a_i = x_i + I$, $i = 1, 2, \dots$. Тогда B – коммутативная ненильпотентная ниль-алгебра.

Рассмотрим алгебру

$$R = \begin{pmatrix} \mathrm{B} & \mathrm{A} \\ \mathrm{B} & \mathrm{B} \end{pmatrix} = \left\{ \begin{pmatrix} b_1 & a \\ b_2 & b_3 \end{pmatrix} \in M_2(A) \,\middle|\, b_i \in B,\ i \leq 3,\ a \in A \right\}.$$

Из локальной нильпотентности алгебры B следует, что R – ниль-алгебра.

Так как A – коммутативная алгебра, то $M_2(A)$ удовлетворяет полилинейному тождеству

$$S_4(x_1, x_2, x_3, x_4) = \sum_{\sigma \in S_4} (\operatorname{sgn} \sigma) x_{\sigma(1)} x_{\sigma(2)} x_{\sigma(3)} x_{\sigma(4)},$$

где $\operatorname{sgn} \sigma = 1$, если σ – четная подстановка и $\operatorname{sgn} \sigma = -1$, если σ – нечетная подстановка. Пусть I – идеал алгебры R, порожденный матрицей e_{12}, то есть

$$I = (e_{12}) = F \cdot e_{12} + Re_{12} + e_{12}R + Re_{12}R.$$

Этот идеал содержит подалгебру

$$e_{12} \cdot (Be_{21}) = Be_{11},$$

которая не является нильпотентной. Следовательно, I – конечнопорожденный идеал алгебры R, не являющейся нильпотентным идеалом. Поэтому I не содержится в сумме всех нильпотентных идеалов алгебры R, удовлетворяющей полилинейному тождеству $S_4(x_i) = 0$. Этот пример показывает, что в алгебре, удовлетворяющей тождеству, верхний ниль-радикал (в общем случае) не совпадает с суммой всех нильпотентных идеалов.

Пусть R – алгебра над коммутативным кольцом Φ с единицей. Пусть $\Phi\langle x_1, x_2, \ldots\rangle$ – свободная ассоциативная Φ-алгебра и

$$f(x_1, \ldots, x_d) = x_1 x_2 \ldots x_d + \sum_{(i) \neq (1)} \alpha_i x_{i_1} \ldots x_{i_d}$$

– ненулевой полилинейный многочлен из $\Phi\langle x_1, x_2, \ldots\rangle$, один из коэффициентов которых равен единице. Скажем, что

$$f(x_1, \ldots, x_d) = 0$$

является *тождеством* в алгебре R, если для любых элементов $a_1, \ldots, a_d \in R$ выполнено $f(a_1, \ldots, a_d) = 0$

Теорема 2.5 (Я. Левицкий).
Пусть R – ниль-алгебра, удовлетворяющая полилинейному тождеству $f(x_1, \ldots, x_d) = 0$. Тогда $R = L(R)$.

□ Доказательство проведем методом математической индукции по числу d. Если $d \leq 2$, то R удовлетворяет тождеству $x_1x_2 = \alpha x_1x_2$, где $\alpha \in \Phi$. Пусть A – подалгебра R, порожденная, например, элементами $\{a_1, \ldots, a_m\}$, где $a_i^{k_i} = 0$, $i \leq m$. Тогда $A^N = (0)$, где $N = \sum\limits_{i=1}^{m}(k_i - 1) + 1$. Таким образом, R – локально нильпотентная алгебра.

Предположим, что произвольная ниль-алгебра, удовлетворяющая полилинейному тождеству степени не более $d-1$, является локально нильпотентной. Пусть R – ниль-алгебра, удовлетворяющая тождеству $f(x_1, \ldots, x_d) = 0$. Предположим, что $R \neq L(R)$ и рассмотрим алгебру $\bar{R} = R/L(R) \neq \bar{0}$. Выберем в $\bar{R}$ ненулевой элемент a такой, что $a^2 = \bar{0}$ и запишем тождество $f = 0$ в виде

$$f(x_1, \ldots, x_d) = x_1x_2 \ldots x_d + \sum_{(i)\neq(1)} \alpha_{(i)} x_{i_1} \ldots x_{i_d} = \\ = x_1 f_1(x_2, \ldots, x_d) + f_2(x_1, \ldots, x_d),$$

где f_2 – линейная комбинация одночленов, не начинающаяся с элемента x_1. Положим $x_1 = a$, $x_2 = b_2a$, $\ldots$, $x_d = b_da$, где $b_i \in \bar{R}$, $2 \leq i \leq d$. Тогда $af_1(b_2a, \ldots, b_da) = \bar{0}$. Пусть

$$I = \left\{x \in \bar{R}a \middle| \, (\bar{R}a)x = \bar{0}\right\} \lhd \bar{R}a.$$

Тогда $\bar{R}a/I$ удовлетворяет тождеству $f_1(x_2, \ldots, x_d) = 0$ степени $d-1$ и по предположению индукции

$$L\left(\bar{R}a/I\right) = \bar{R}a/I.$$

Учитывая, что $I^2 = \bar{0}$, получаем равенство

$$L(\bar{R}a) = \bar{R}a \subseteq L(\bar{R}) = (\bar{0}).$$

Следовательно, $\bar{R}a = \bar{0}$ и a принадлежит идеалу

$$r(\bar{R}) = \left\{x \in \bar{R} \middle| \, \bar{R}x = \bar{0}\right\} \lhd R,$$

$r(\bar{R})^2 = \bar{0}$. Отсюда следует, что $r(\bar{R}) \subseteq L(\bar{R})$ и $L(\bar{R}) \neq (\bar{0})$. Противоречие доказывает, что R – локально нильпотентная алгебра. □

Следствие 2.1. *Пусть R – ниль-кольцо ограниченного индекса n. Тогда R – локально нильпотентное кольцо.*

□ По условию кольцо R удовлетворяет тождеству $x^n = 0$. Применяя линеаризацию к многочлену x^n (см. главу 4), получим, что R удовлетворяет тождеству

$$\sum_{\sigma \in S_n} x_{\sigma_{(1)}} \dots x_{\sigma_{(n)}} = 0.$$

По теореме 2.5 $R = L(R)$. □

Теорема 2.6 (С. Амицур, Я. Левицкий).
Пусть R – алгебра над коммутативным кольцом Φ с единицей, удовлетворяющая пилилинейному тождеству степени d. Пусть B – ниль-подалгебра R и $N(1)$ – сумма всех нильпотентных идеалов R. Тогда

$$B^{\left[\frac{d}{2}\right]} \subseteq N(1).$$

□ Пусть

$$\left\{b_1, b_2, \dots, b_{\left[\frac{d}{2}\right]}\right\}$$

– произвольные элементы из B и

$$S = \Phi\left\langle b_1, \dots, b_{\left[\frac{d}{2}\right]}\right\rangle$$

– подалгебра, ими порожденная. По предыдущей теореме S – нильпотентная алгебра. Поэтому существует наименьшее число $n \geq 1$ такое, что RS^nR – нильпотентный идеал.

Рассмотрим множества

$$U_1 = S^{n-1}R,\ U_2 = S^{n-1}RS,\ \dots,\ U_{2i-1} = S^{n-i}RS^{i-1},$$
$$U_{2i} = S^{n-i}RS^i,\ \dots,\ U_{2n-1} = RS^{n-1},\ U_{2n} = RS^n.$$

Заметим, что для любых чисел $m > k$

$$U_m U_k \subseteq RS^n R$$

и для любого числа $t \leq 2n$

$$U_1 U_2 \dots U_t = (S^{n-1}R)^t \cdot S^{\left[\frac{t}{2}\right]}.$$

Пусть $n > \left[\frac{d}{2}\right]$. Тогда $2n > d$ и подставляя в тождество

$$f(x_1, \dots, x_d) = x_1 x_2 \dots x_d + \sum_{(i)\neq 1} \alpha_{(i)} x_{i_1} \dots x_{i_d} = 0$$

$x_i = a_i \in U_i$, $i = 1, 2, \dots, d$ получим, что $a_1, a_2, \dots, a_d \in RS^n R$ или

$$\left(S^{n-1}R\right)^d S^{\left[\frac{d}{2}\right]} \subseteq RS^n R.$$

Следовательно,

$$(RS^{n-1}R)^{d+1} \subseteq RS^n R$$

и $RS^{n-1}R$ – нильпотентный идеал. Противоречие. Следовательно, $RS^{\left[\frac{d}{2}\right]}R$ – нильпотентный идеал. Таким образом, идеал

$$S^{\left[\frac{d}{2}\right]} + RS^{\left[\frac{d}{2}\right]} + S^{\left[\frac{d}{2}\right]}R + RS^{\left[\frac{d}{2}\right]}R$$

является нильпотентным и

$$S^{\left[\frac{d}{2}\right]} \subseteq N(1).$$

В частности,

$$b_1 b_2 \dots b_{\left[\frac{d}{2}\right]} \in N(1).$$

□

Следствие 2.2. *Пусть R – алгебра над коммутативным кольцом с единицей, удовлетворяющая полилинейному тождеству. Тогда*

$$\ln R = L(R) = \mathrm{un}R = N(2).$$

□ Действительно, из теоремы следует, что

$$(\mathrm{un}R)^{\left[\frac{d}{2}\right]} \subseteq N(1)$$

и $\mathrm{un}R \subseteq N(2)$. □

2.8. Ниль-кольца с условиями обрыва некоторых цепей односторонних идеалов

Известно, что конечномерная ниль-алгебра является нильпотентной. К. Гопкинс доказал, что односторонний ниль-идеал кольца, удовлетворяющего условию обрыва убывающих цепей правых идеалов, является нильпотентным. В 1960 г. английский математик А. Голди доказал, что ниль-подкольцо кольца, удовлетворяющего условию обрыва возрастающих цепей правых идеалов, является нильпотентным.

Цель этого параграфа – доказать замечательную теорему, принадлежащую Р. Шоку (R. Shock), и обобщающую известные до него результаты о ниль-кольцах с условиями конечности на односторонние идеалы.

Лемма 2.1. *Пусть R – ассоциативное кольцо и (xy) – нильпотентный элемент при некоторых $x, y \in R$. Тогда либо $xyx = 0$, либо $l(x) \subset l(yx)$.*

□ Пусть $xyx \neq 0$, $(xy)^n = 0$, $(xy)^{n-1} \neq 0$. Если $(xy)^{n-1} \cdot x \neq 0$, то $(xy)^{n-1} \in l(xyx)$ и $(xy)^{n-1} \notin l(x)$. Если же $(xy)^{n-1}x = 0$, то $(xy)^{n-2} \in l(xyx)$ и $(xy)^{n-2} \notin l(x)$. □

Теорема 2.7. *Пусть R – кольцо, удовлетворяющее условию обрыва возрастающих цепей левых аннуляторных идеалов и N – ниль-подкольцо R, которое не является нильпотентным. Тогда существует такая последовательность $\{a_n |\ n \in \mathbb{Z}^+\}$ ненулевых элементов в N, что*

1. $r(\{a_1, a_2, a_3 \dots\}) \subset r(\{a_2, a_3 \dots\}) \subset r(\{a_3, a_4 \dots\}) \subset \dots$.
2. *Если $Ra_n \neq 0$ для любого целого числа $n \geq 1$, то сумма $\sum\limits_{n\geq 1} Ra_n$ является прямой; если $Ra_n = 0$, то существует целое число $k \geq n$ такое, что сумма $\sum\limits_{m\geq k} R^{\#}a_m$ является прямой ($R^{\#}b = Rb + \mathbb{Z}b$, $b \in R$).*

□ Рассмотрим следующую цепь левых аннуляторных идеалов

$$l(N) \subseteq l(N^2) \subseteq l(N^3) \subseteq \dots.$$

По условию теоремы существует целое число $t \geq 1$ такое, что

$$l(N^t) = l(N^{t+1}) = l(N^{t+2}) = \dots.$$

Положим $K = l(N^t)$. Если $N \subseteq K$, то $N^{t+1} = 0$. Противоречие. Поэтому существует такой элемент $x \in N$, что $R^{\#}x \not\subset K$. Среди всех таких элементов выберем элемент $x_1 \in N$, для которого идеал левый $l(x_1)$ является максимальным из возможных, то есть $l(x_1)$ максимальный в множестве

$$\{l(x)|\ x \in N,\ R^{\#}x \not\subset K\}.$$

Если $R^{\#}x_1N \subset K$, то $R^{\#}x_1N^{t+1} = 0$ и $R^{\#}x_1 \subseteq l(N^{t+1}) = K$. Противоречие доказывает, что существует такой элемент $x \in N$, что $R^{\#}x_1x \not\subset K$. Выберем такой элемент $x_2 \in N$, что $l(x_2)$ является максимальным в множестве

$$\{l(x)|\ x \in N,\ R^{\#}x_1x \not\subset K\}.$$

Пусть элементы $\{x_1, x_2, \dots, x_n\} \subseteq N$ выбраны. Тогда

$$R^{\#}x_1x_2 \dots x_nN \not\subset K.$$

Выберем $x_{n+1} \in N$ так, что $l(x_{n+1})$ является максимальным в множестве

$$\{l(x)|\ x \in N,\ R^{\#}x_1x_2 \dots x_nx \not\subset K\}.$$

Пусть $a_n = x_1x_2 \dots x_n$, $n \geq 1$. Заметим, что для любых чисел $j, m \in \mathbb{Z}^+$,

$$Rx_j \cap l(x_{j+1}x_{j+2} \dots x_{j+m}) = 0.$$

Действительно, если $rx_j \in Rx_j \cap l(x_{j+1} \dots x_{j+m})$ и $rx_j \neq 0$, то $rx_j \dots x_{j+m} = 0$. Следовательно, $r \in l(x_jx_{j+1} \dots x_{j+m}) \setminus l(x_j)$. Так как

$$R^{\#}x_1 \dots x_{j-1}(x_jx_{j+1} \dots x_{j+m}) \not\subseteq K,$$

то мы получаем противоречие с выбором x_j. Далее заметим, что $l(a_1) = l(a_n)$, $n \in \mathbb{Z}^+$. Действительно, $l(a_1) \subseteq l(a_n)$ и если $l(a_1) \neq l(a_n)$, то мы получаем противоречие с выбором $a_1 = x_1$ (так как $R^{\#}a_n \not\subset K$). Докажем далее, что

$$a_n x_n = a_{n+1}x_n = a_{n+2}x_n = \cdots = a_{n+j}x_n = 0,$$

где $j \geq 0$, $n \geq 1$.

Допустим, что $a_{n+j}x_n \neq 0$ для некоторых целых чисел $j \geq 0$, $n \geq 1$. Тогда из включения

$$R^{\#}a_{n+j}x_n \subseteq Rx_n$$

и равенства

$$Rx_n \cap l(x_{n+1}x_{n+2}\dots x_{n+m}) = 0,$$

$m \geq 1$, следует, что

$$R^{\#}a_{n+j}x_n(x_{n+1}\dots x_{n+m}) \neq 0.$$

В частности,

$$R^{\#}a_{n+j}x_n \not\subset K,$$

так как

$$0 \neq a_{n+j}x_n = x_1x_2\dots x_{n-1}(x_nx_{n+1}\dots x_{n+j}x_n).$$

По лемме 2.1

$$l(x_n) \subset l(x_nx_{n+1}\dots x_{n+j}x_n)$$

при $j \geq 1$. Следовательно, мы получаем противоречие с выбором x_n. Если $j = 0$, то

$$R^{\#}a_nx_n = R^{\#}a_{n-1}x_n^2 \not\subset K.$$

Так как x_n – нильпотентный элемент, то имеем $l(x_n) \subset l(x_n^2)$ и $l(x_n) \neq l(x_n^2)$. Опять получаем противоречие с максимальностью $l(x_n)$. Итак, $a_{n+j}x_n = 0$, $j \geq 0$, $n \geq 1$. Отсюда следует, что

$$r(\{a_k, a_{k+1}, \dots\}) \subset r(\{a_{k+1}, a_{k+2}, \dots\}),$$

ибо x_{k+1} содержится в $r(\{a_{k+1}, a_{k+2}, \dots\})$ и не содержится в $r(\{a_k, a_{k+1}, \dots\})$. Пусть далее $Ra_n \neq 0$, $n \geq 1$ и

$$r_{s+1}a_{s+1} = r_1a_1 + r_2a_2 + \cdots + r_sa_s$$

для некоторых элементов $r_1, r_2, \dots, r_{s+1} \in R$. Умножая это равенство справа на x_2, имеем, что $r_1a_2 = 0$. Следовательно, $r_1 \in l(a_2) = l(a_1)$, то есть $r_1a_1 = 0$. Аналогично, умножая наше равенство на x_3, получим $r_2a_3 = r_2a_2 = 0$. Данные рассуждения доказывают, что сумма

$$\sum_{n\geq 1} Ra_n$$

является прямой. Если $Ra_n = 0$, то $Ra_j = 0$ для любого $j \geq n$. Если некоторый элемент a_t, $t \geq n$, имеет конечный аддитивный порядок, то, начиная с некоторого номера, порядки всех элементов равны. Таким образом, можно считать, что при $j \geq n$ либо все элементы a_j не имеют конечные аддитивные порядки, либо аддитивные порядки элементов $a_n, a_{n+1}, a_{n+2}, \dots$ равны. Докажем, что сумма

$$\sum_{m\geq n} R^{\#}a_m$$

является прямой. Предполагая противное, имеем равенство

$$m_1a_n + m_2a_{n+1} + \cdots + m_{s+1}a_{n+s} = m_{s+2}a_{n+s+1},$$

где $m_t \in \mathbb{Z}$. Умножая левую и правую части этого равенства на x_{n+1}, получим, что $m_1a_{n+1} = 0$. Следовательно, $m_1a_n = 0$. Рассуждая аналогично, мы докажем, что каждое слагаемое $m_{i+1}a_{n+i}$ в сумме равно нулю, то есть сумма $\sum\limits_{m\geq n} R^{\#}a_m$ является прямой. □

Следствие 2.3 (И. Херстейн, Л. Смолл).
Пусть R – кольцо, удовлетворяющее условию обрыва возрастающих цепей левых и правых аннуляторных идеалов. Тогда каждое ниль-подкольцо кольца R является нильпотентным.

□ Достаточно заметить, что R не содержит возрастающих цепей вида $r(\{a_k, a_{k+1} \dots\}) \subseteq r(\{a_{k+1}, a_{k+2}, \dots\})$. □

Следствие 2.4 (А. Голди).
Пусть R – кольцо с условием максимальности для левых идеалов. Тогда каждое ниль-подкольцо кольца R является нильпотентным.

□ Заметим, что R не содержит бесконечных прямых сумм левых идеалов $\sum\limits_{i\geq 1} \oplus L_i$. Действительно, если R содержит такую сумму, то мы получаем бесконечную возрастающую цепь левых идеалов

$$L_1 \subset L_1 \oplus L_2 \subset L_1 \oplus L_2 \oplus L_3 \subset \dots.$$

Противоречие доказывает следствие. □

Следствие 2.5. *Пусть R – кольцо с условием обрыва убывающих цепей правых и левых идеалов. Тогда каждое нильподкольцо кольца R является нильпотентным.*

Следствие 2.6 (К. Лански).
Пусть R – левое кольцо Голди. Тогда каждое ниль-подкольцо кольца R является нильпотентным.

□ Действительно, если R содержит ниль-подкольцо, не являющееся нильпотентным, то согласно теореме в R существует бесконечная прямая сумма левых идеалов, что противоречит условиям Голди (см. главу 3). □

2.9. Теорема Андрунакиевича-Рябухина

Следующая теорема описывает строение колец без нильпотентных элементов и играет важную роль в доказательствах теорем коммутативности для колец.

Теорема 2.8 (В. Андрунакиевич, Ю. Рябухин [36]). *Кольцо R не содержит ненулевых нильпотентных элементов тогда и только тогда, когда R – подпрямая сумма колец без делителей нуля.*

□ Если

$$R = \sum\nolimits_s \bigoplus_{i \in I} R_i$$

– подпрямая сумма колец R_i, $i \in I$, без делителей нуля и элемент $a = (a_i) \in R$ нильпотентен, то $a^n = (a_i^n) = 0$ для некоторого целого числа $n \geq 1$. Откуда следует, что $a_i^n = 0$ и $a_i = 0$, для всех $i \in I$, то есть $a = 0$.

Докажем обратное утверждение. Пусть R – кольцо без нильпотентных элементов и $a, b \in R$ такие, что $ab = 0$. Тогда

$$(ba)^2 = b(ab)a = 0.$$

Так как R не содержит нулевых нильпотентных элементов, то $ba = 0$.

Обозначим через

$$(x) = \mathbb{Z}x + Rx + xR + RxR$$

– идеал, порожденный x. Пусть $a_1, a_2, \ldots, a_n$ – такие элементы кольца R, что

$$a_1 a_2 \ldots a_n = 0.$$

Докажем, что

$$(a_1)(a_2)\ldots(a_n) = (0).$$

Действительно, из равенства $a_1(a_2 \ldots a_n) = 0$ следует, что

$$(a_2 a_3 \ldots a_n)a_1 = 0,\ (a_1 a_3 \ldots a_n)(a_1 x_1) = 0$$

и, следовательно,

$$(a_1 x_1)(a_2 \ldots a_n) = 0$$

для любого элемента $x_1 \in R$. Аналогично доказывается, что для любых элементов $x_1, \ldots, x_{n-1}$ из R справедливо равенство

$$a_1 x_1 a_2 x_2 a_3 \ldots a_{n-1} x_{n-1} a_n = 0.$$

Это означает, что $(a_1)(a_2)\ldots(a_n) = (0)$.

Докажем далее, что из равенства

$$a_1 a_2 \ldots a_n = 0$$

для некоторых элементов $a_1, \ldots, a_n \in R$ следует равенство

$$a_{i_1} a_{i_2} \ldots a_{i_n} = 0,$$

где $\{i_1, \ldots, i_n\}$ – перестановка чисел $\{1, 2, \ldots, n\}$. Пусть

$$b = a_{i_1} a_{i_2} \ldots a_{i_n}.$$

Тогда

$$b^n = (a_{i_1} \ldots a_1 \ldots a_{i_n})(a_{i_1} \ldots a_2 \ldots a_{i_n}) \ldots (a_{i_1} \ldots a_n \ldots a_{i_n})$$

содержится в $(a_1)(a_2)\ldots(a_n) = (0)$. Так как R – кольцо без нильпотентных элементов, то $b = a_{i_1} \ldots a_{i_n} = 0$.

Возьмем произвольный элемент $a \neq 0$ в R и рассмотрим полугруппу $S = \{a, a^2, a^3, \ldots\}$. Тогда $S \cap (0) = \varnothing$. По лемме Цорна существует подполугруппа M в R, содержащая S и не пересекающаяся с (0). Рассмотрим множество $I_a = R \setminus M$. Докажем, что $I_a \lhd R$. Пусть $x, y \in I_a$. Тогда полугруппы $\langle M, x\rangle$ и $\langle M, y\rangle$ содержат нуль, то есть

$$m_1 x^{i_1} m_2 x^{i_2} \ldots m_n x^{i_n} = 0$$

и

$$v_1 y^{j_1} v_2 y^{j_2} \ldots v_k y^{j_k} = 0,$$

где $m_i, v_i \in M$. Из предыдущего следует, что

$$(m_1 m_2 \ldots m_n) x^{i_1 + i_2 + \ldots + i_n} = 0,$$

$$(v_1 \dots v_k) y^{j_1 + \dots + j_k} = 0.$$

Пусть

$$m = m_1 \dots m_n,\ N = i_1 + \dots + i_n,\ v = v_1 \dots v_k,\ N_1 = j_1 + \dots + j_k.$$

Тогда

$$m^N x^N = 0,\ (mx)^N = 0 \ \text{ и } \ v^{N_1} y^{N_1} = (vy)^{N_1} = 0.$$

Так как R – кольцо без нильпотентных элементов, то $mx = 0$ и $vy = 0$ для некоторых элементов $m, v \in M$. Откуда следует, что

$$vmx = (mv)x = (mv)y = (mv)(x \pm y) = 0$$

и для любого элемента $r \in R$

$$(mx)r = m(xr) = m(rx) = 0.$$

это означает, что $(x \pm y),\ rx, xr \in I_a$, то есть $I_a \lhd R$ и I_a не содержит элемент a.

Покажем, что R/I_α – кольцо без делителей нуля. Пусть $\bar{u}$ и $\bar{v}$ – такие ненулевые элементы R/I, что $\bar{u} \cdot \bar{v} = \bar{0}$. Тогда $u \in M$, $v \in M$ и $u \cdot v \in M$ (так как M – полугруппа). С другой стороны, $\bar{u}\bar{v} = \overline{uv} = \bar{0}$ и $uv \in I_a = R \setminus M$. Противоречие.

Если $\bigcap\limits_{a \neq 0} I_a$ содержит ненулевой элемент $b \in R$, то $b \in I_b$. Противоречие. Следовательно, $\bigcap\limits_{a \neq 0} I_a = (0)$ и R – подпрямая сумма колец без делителей нуля R/I_a, где a пробегает все ненулевые элементы R. $\square$

Применим теорему Андрунакиевича-Рябухина для доказательства следующего критерия коммутативности кольца R.

Предложение 2.14. *Пусть R – кольцо, удовлетворяющее тождеству $[x - x^{2n}, y] = 0$. Тогда R – коммутативное кольцо.*

$\square$ Пусть $a, b \in R$. Тогда

$$[-a, b] = \left[(-a)^{2n}, b\right] = \left[a^{2n}, b\right] = [a, b]$$

и $2[a,b]=0$. Если a – нильпотентный элемент кольца R, то существует целое число $k\geq 1$ также, что $a^k=0$. Из равенств

$$[a,b]=\left[a^{2n},b\right]=\left[a^{4n^2},b\right]=\ldots=\left[a^{2^k\cdot n^k},b\right]=0$$

следует, что a – центральный элемент. Пусть R – некоммутативное кольцо и $\{a,b\}$ – такие его элементы, что $[a,b]\neq 0$. По лемме Цорна существует максимальный идеал $I\lhd R$, не содержащий $[a,b]$. Рассмотрим фактор-кольцо $S=R/I$. Если верхний ниль-радикал $\mathrm{un}S$ ненулевой, то он содержит сердцевину $\left(\left[\bar{a},\bar{b}\right]\right)$. Откуда следует, что $\left[\bar{a},\bar{b}\right]$ – ненулевой нильпотентный элемент в S, лежащий в центре S. В частности,

$$\begin{aligned}\left[\bar{a},\bar{b}\right]&=\left[\bar{a}^{2n},\bar{b}\right]=\bar{a}\left[\bar{a}^{2n-1},b\right]+\left[\bar{a},\bar{b}\right]\bar{a}^{2n-1}=\\&=\bar{a}\left(\bar{a}\left[\bar{a}^{2n-2},\bar{b}\right]+\left[\bar{a},\bar{b}\right]\bar{a}^{2n-2}\right)+\left[\bar{a},\bar{b}\right]\bar{a}^{2n-1}=\\&=\bar{a}^2\left[\bar{a}^{2n-2},\bar{b}\right]+2\left[\bar{a},\bar{b}\right]\bar{a}^{2n-1}=\ldots=2n\left[\bar{a},\bar{b}\right]\bar{a}^{2n-1}=\bar{0},\end{aligned}$$

так как $2\left[\bar{a},\bar{b}\right]=\bar{0}$. Противоречие доказывает, что $\mathrm{un}S=(0)$ и S – кольцо без нильпотентных элементов.

Так как S – подпрямое неразложимое кольцо, то по теореме Андрунакиевича-Рябухина S – кольцо без делителей нуля. Докажем, что $J(S)=(0)$. Если $c\in J(S)$, то $\left(c^{2n}-c\right)=\lambda$ принадлежит центру кольца S. В частности,

$$\left[\lambda\bar{a},\bar{b}\right]=\left[(\lambda\bar{a})^{2n},\bar{b}\right]=\lambda^{2n}\left[\bar{a}^{2n},\bar{b}\right]=\lambda^{2n}\left[\bar{a},\bar{b}\right]$$

и

$$\left(\lambda^{2n}-\lambda\right)\left[\bar{a},\bar{b}\right]=\bar{0}.$$

Так как S – кольцо без делителей нуля и $[\bar{a},\bar{b}]\neq\bar{0}$, то получаем $\lambda^{2n}-\lambda=0$. Пусть $\mu\in J(S)$ квазиобратный элемент для $\left(-\lambda^{2n-1}\right)$. Тогда

$$\left(-\lambda^{2n-1}\right)+\mu+\left(-\lambda^{2n-1}\right)\mu=0$$

и

$$\lambda=\lambda\cdot\lambda^{2n-1}=\lambda\left(\mu-\lambda^{2n-1}\mu\right)=\lambda\mu-\lambda\mu=0.$$

Следовательно, $c = c^{2n} \in J(S)$. Рассуждая аналогично, получим, что $c = 0$. Следовательно, S – полупростое кольцо (в смысле радикала Джекобсона) с ненулевой сердцевиной. Поэтому S – примитивное кольцо. По теореме плотности, S – плотное кольцо линейных преобразований в $\mathrm{End}_D V$, где V – векторное пространство над телом D. Если $\dim_D V \geq 2$ и $\{u, v\}$ – линейно независимые векторы V, то по теореме плотности существуют элементы $a_1, a_2 \in S$ такие, что $ua_1 = v$, $va_1 = 0$, $ub_1 = 0$, $vb_1 = v$. Откуда следует, что

$$u\,[a_1, b_1] = u\,(a_1 b_1 - b_1 a_1) = v = \\ = u\left[a_1^{2n}, b_1\right] = u\left(a_1^{2n} b_1 - b_1 a_1^{2n}\right) = 0.$$

Противоречие доказывает, что $\dim_D V = 1$ и S – тело. Пусть r – произвольный элемент S. Тогда элемент $\left(r^{2n} - r\right) = \lambda$ принадлежит центу S. Из предыдущего следует, что

$$\left(\lambda^{2n} - \lambda\right)[\bar{a}, \bar{b}] = \bar{0}$$

и

$$\lambda^{2n} - \lambda = \left(r^{2n} - r\right)^{2n} - \left(r^{2n} - r\right) = r + r^{2n+1} f(r) = 0,$$

где $f(t) \in Z[t]$ – тождество в теле S. Элемент $\bar{b}$ порождает конечное поле

$$GF(2^k) = \{\lambda_1 = 0, \lambda_2, \ldots, \lambda_{2^k}\}.$$

Рассмотрим отображения

$$T_{\bar{b}} : S \to S,\ L_\lambda : S \to S$$

такие, что для любого элемента $s \in S$

$$sT_{\bar{b}} = [s, \bar{b}],\ sL_\lambda = \lambda s.$$

Тогда

$$\bar{a}\left(T_{\bar{b}}^{2^k} - T_{\bar{b}}\right) = [\bar{a}, \underbrace{\bar{b}, \bar{b}, \ldots, \bar{b}}_{2^k}] - \left[\bar{a}, \bar{b}\right] = \left[\bar{a}, \bar{b}^{2^k} - \bar{b}\right] = \bar{0}.$$

С другой стороны, $T_{\bar{b}} - L_\lambda = L_\lambda T_{\bar{b}}$ и

$$\bar{a}\left(T_{\bar{b}}^{2^k} - T_{\bar{b}}\right) = \bar{a}\left(T_{\bar{b}} - L_{\lambda_1}\right)\left(T_{\bar{b}} - L_{\lambda_2}\right)\ldots\left(T_{\bar{b}} - L_{\lambda_{2^k}}\right) = 0,$$

где

$$\bar{a}\left(T_{\bar{b}} - L_{\lambda_1}\right) = [\bar{a}, \bar{b}] \neq \bar{0}.$$

Пусть i – такой индекс, что

$$\omega = \bar{a}\left(T_{\bar{b}} - L_{\lambda_1}\right)\ldots\left(T_{\bar{b}} - L_{\lambda_1}\right) \neq \bar{0} \quad \text{и} \quad \omega\left(T_{\bar{b}} - L_{\lambda_{i+1}}\right) = \bar{0},$$

$1 \leq i \leq 2^k - 1$. Тогда

$$\omega\bar{b} - \bar{b}\omega = \lambda_{i+1}\omega$$

и подкольцо, порожденное $\{\bar{b}, \omega\}$, является конечным некоммутативным телом. Это противоречит теореме Веддерберна о конечных телах (см. главу 5). $\square$

В главе 5 мы докажем коммутативность произвольного кольца, удовлетворяющего тождеству $[x - x^n, y] = 0$, где $n \geq 2$.

Кольцо R имеет ограниченный индекс (нильпотентности) n, если для любого нильпотентного элемента $a \in R$ $a^n = 0$. Ясно, что кольца без нильпотентных элементов имеют ограниченный индекс 1. Справедлива следующая теорема, доказанная в работе [62].

Теорема 2.9. *Пусть R – полупервичное кольцо ограниченного индекса n. Тогда R – подпрямая сумма первичных колец ограниченного индекса n.*

Перед доказательством теоремы приведем несколько лемм.

Лемма 2.2. *Пусть R – полупервичное кольцо и n – натуральное число. Тогда следующие условия эквивалентны:*

1. *R имеет ограниченный индекс n.*

2. *Для любых подмножеств* $X_1, X_2, \ldots, X_n$ *кольца* R *таких, что*

$$X_i X_j = (0)$$

при $i \geq j$ *следует, что*

$$X_1 X_2 \ldots X_n = (0).$$

3. *Для любого подмножества* $X \subseteq R$

$$r\left(X^n\right) = r\left(X^{n+1}\right).$$

4. *Для любого элемента* $a \in R$

$$r\left(a^n\right) = r\left(a^{n+1}\right).$$

□ Предположим, что выполнено условие 1) и подмножества $X_1, \ldots, X_n \subseteq R$ такие, что $X_i X_j = 0$ для любых индексов $i \geq j$. Пусть $a_1 \in X_1, \ldots, a_n \in X_n$. Тогда

$$(a_1 + a_2 + \ldots + a_n)^{n+1} = 0$$

и, следовательно,

$$(a_1 + \ldots + a_n)^n = a_1 a_2 \ldots a_n = 0,$$

то есть $X_1 X_2 \ldots X_n = (0)$.

Пусть выполнено условие 2) и $X \subseteq R$. Положим

$$X_i = r\left(X^i\right) R X^i,$$

где $i \leq n$. Тогда

$$X_i X_j = r\left(X^i\right) R X^i r\left(X^j\right) R X^j = \\ = r\left(X^i\right) R X^{i-j} \cdot \left(X^j r\left(X^j\right)\right) R X^j = (0)$$

при $i \geq j$ и согласно условию 2)

$$X_1 X_2 \ldots X_n = r(X) R X r\left(X^2\right) R X^2 \ldots r\left(X^n\right) R X^n = (0).$$

Так как при $m \leq n$ множество $X^{n-m}r\left(X^{n+1}\right)$ содержится в $r\left(X^{m+1}\right)$, то

$$RX^n r\left(X^{n+1}\right) \subseteq RX^m \cdot X^{n-m} r\left(X^{n+1}\right) \subseteq RX^m \cdot r\left(X^{m+1}\right)$$

и

$$(0) = Rr(X) \cdot RXr\left(X^2\right) \cdot \ldots \cdot RX^{n-1} r(X^n) \cdot RX^n r\left(X^{n+1}\right) \supseteq \\ \supseteq \left(RX^n r\left(X^{n+1}\right)\right)^{n+1}.$$

Полупервичное кольцо R не содержит односторонних ненулевых нильпотентных идеалов. Поэтому

$$RX^n r\left(X^{n+1}\right) = (0) \quad \text{и} \quad X^n r\left(X^{n+1}\right) = (0).$$

Откуда следует, что

$$r\left(X^n\right) = r\left(X^{n+1}\right).$$

Ясно, далее, что из условия 3) следует условие 4). Пусть выполнено условие 4). Докажем, что R имеет ограниченный индекс n. Для этого возьмем произвольный нильпотентный элемент $a \in R$ и предположим, что $a^{n+k} = 0$, $a^{n+k-1} \neq 0$, где $k \geq 1$. Тогда $a^{k-1} \in r\left(a^{n+1}\right) = r\left(a^n\right)$ и $a^{n+k-1} = 0$. Противоречие. $\square$

Лемма 2.3. *Пусть R – полупервичное кольцо и n – натуральное число. Тогда R имеет ограниченный индекс n в том и только в том случае, если для любого идеала $T \lhd R$ и для любого элемента $a \in R$*

$$r\left(Ta^n\right) = r\left(Ta^{n+1}\right).$$

$\square$ Пусть для любого идеала $T \lhd R$ и для любого элемента $a \in R$ выполнено $r(Ta^n) = r(Ta^{n+1})$. Докажем, что $r\left(a^n\right) = r\left(a^{n+1}\right)$. Пусть $T = R$ и $b \in r\left(a^{n+1}\right)$. Тогда $r\left(Ra^n\right) = r\left(Ra^{n+1}\right) \ni b$. Следовательно, $(Ra^n)b = R(a^n b) = 0$ и, ввиду полупервичности кольца R, $a^n b = 0$, то есть $b \in r(a^n)$. Таким образом,

$r(a^n) = r\left(a^{n+1}\right)$ и, по предыдущей лемме, R имеет ограниченный индекс n.

Докажем обратное утверждение. Пусть R имеет ограниченный индекс n и T – произвольный идеал R и a – произвольный элемент кольца R. Положим

$$X_i = r\left(Ta^i\right) Ta^i,$$

где $i = 1, 2, \ldots, n$. Тогда

$$X_i X_j = r\left(Ta^i\right) Ta^i r\left(Ta^j\right) Ta^j = (0)$$

при $i \geq j$. Согласно лемме 2.2, имеем, что

$$0 = X_1 X_2 \ldots X_n = TX_1 X_2 \ldots X_n =$$
$$= (Tr(Ta))\left(Tar\left(Ta^2\right)\right)\left(Ta^2 r\left(Ta^3\right)\right)\ldots\left(Ta^{n-1} r\left(Ta^n\right)\right) Ta^n.$$

Так как

$$a^{n-i} r\left(Ta^{n+1}\right) \subseteq r\left(Ta^{i+1}\right),$$

то

$$Ta^n r\left(Ta^{n+1}\right) \subseteq Ta^i \cdot a^{n-i} r\left(Ta^{n+1}\right) \subseteq Ta^i r\left(Ta^{i+1}\right)$$

при $i \leq n$. Следовательно,

$$\left(Ta^n \cdot r\left(Ta^{n+1}\right)\right)^{n+1} = (0)$$

и в силу полупервичности кольца R

$$Ta^n r\left(Ta^{n+1}\right) = 0.$$

Откуда следует, что $r\left(Ta^{n+1}\right) \subseteq r\left(Ta^n\right)$. $\square$

Лемма 2.4. *Пусть R – полупервичное кольцо индекса n, $T \lhd R$. Тогда $R/\operatorname{Ann} T$ – полупервичное кольцо индекса n.*

□ Из полупервичности кольца R следует, что

$$r(T) = \ell(T) = \operatorname{Ann}(T) = \{x \in R |\ xT = Tx = (0)\}.$$

Если $\bar{a}$ – такой элемент в $R/\operatorname{Ann} T$, что $\bar{a}(R/\operatorname{Ann} T)\bar{a} = \bar{0}$, то $aRa \subseteq \operatorname{Ann} T$ и $(aRa)T = 0$. Откуда следует, что

$$(aT)\,R\,(aT) = ((aT)\,R)^2 = (0)$$

и в силу полупервичности кольца R получаем $(aT)R = (0)$, $aT = (0)$ и $a \in \operatorname{Ann} T$, то есть $\bar{a} = \bar{0}$ и $R/\operatorname{Ann} T$ – полупервичное кольцо. Докажем, что $R/\operatorname{Ann} T$ имеет ограниченный индекс n. Для этого (согласно лемме 2.2) достаточно проверить равенство $r(\bar{a}^n) = r\left(\bar{a}^{n+1}\right)$ для любого элемента $\bar{a} \in R/\operatorname{Ann} T$. Пусть $\bar{c} \in r\left(\bar{a}^{n+1}\right)$. Тогда $\bar{a}^{n+1} \cdot \bar{c} = \bar{0}$, $a^{n+1}c \in \operatorname{Ann} T$ и $Ta^{n+1}c = (0)$. Так как в силу леммы 2.3 $r\left(Ta^{n+1}\right) = r\left(Ta^n\right)$, то $Ta^nc = (0)$, $a^nc \in \operatorname{Ann} T$, $\bar{a}^n \cdot \bar{c} = (\bar{0})$, $\bar{c} \in r\left(\bar{a}^n\right)$. □

Доказательство теоремы. Пусть a – произвольный ненулевой элемент из R. В силу полупервичности кольца R существуют такие элементы $\{b_1, b_2, \ldots\}$, что

$$a_2 = a_1b_1a_1 \neq 0,\ \ldots,\ a_{i+1} = a_ib_ia_i \neq 0,\ \ldots.$$

Рассмотрим непустое множество идеалов

$$\mathfrak{M} = \{A |\ A \lhd R,\ A \cap \{a_1, a_2, \ldots\} = \varnothing,\ R/A \text{ – кольцо, имеющее ограниченный индекс } n\}.$$

В силу леммы Цорна, $\mathfrak{M}$ имеет максимальный элемент $P \lhd R$. Покажем сначала, что P – полупервичный идеал. Пусть $K \lhd R$, $P \subseteq K$ и $K^2 \subseteq P$. Тогда R/K имеет отрицательный индекс нильпотентности n, так как R/P имеет отрицательный индекс n. Если $P \neq K$, то K содержит некоторый элемент a_i и, следовательно, $a_{i+1} = a_ib_ia_i \in K^2 \subseteq P$. Противоречие. Таким образом, $K \in \mathfrak{M}$ и, ввиду максимальности P, $K = P$ и R/P – полупервичное кольцо. Докажем его первичность. Если A, B – такие

идеалы R, что $P \subset A$, $P \subset B$ и $AB \subseteq P$, то в полупервичном кольце R/P ограниченного индекса n имеем $\bar{A} \cdot \bar{B} = (\bar{0})$. Пусть $\bar{B}_1 = \operatorname{Ann} \bar{A}$ и $\bar{A}_1 = \operatorname{Ann} \bar{B}_1$. Тогда $\bar{A}_1 \cdot \bar{B}_1 = (\bar{0})$ и по лемме 2.4 R/B_1, R/A_1 – полупервичные кольца индекса n. Ввиду максимальности P существуют элементы $a_i \in B_1$ и $a_j \in A_1$. Следовательно, $a_{j+1} = a_j b_j a_j \in A_1 B_1 \subseteq P$, если $j \geq i$. Противоречие доказывает, что P – простой идеал R, не содержащий a и R/P, имеет ограниченный индекс n. Пересечение всех таких простых идеалов равно нулю и R – подпрямая сумма первичных колец ограниченного индекса n. $\square$

В работе [88] приведены многочисленные нетривиальные примеры колец без нильпотентных элементов. Например, доказано, что:

1. Если $\delta : R \to R$ – дифференцирование кольца R (без нильпотентных элементов), то кольцо косых многочленов
$$R[x;\delta] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; xa = ax + \delta(a),\ a \in R \right\}$$
не содержит ненулевых нильпотентных элементов.

2. Если $\sigma : R \to R$ – мономорфизм (R – кольцо без нильпотентых элементов), такой, что для любого элемента $a \in R$, $a \neq 0$, $a\sigma(a) \neq 0$, $\delta : R \to R$ – δ-дифференцирование кольца R (то есть такое аддитивное отображение, что $\delta(ab) = \delta(a)b + \delta(a)\delta(b)$) для любых элементов $a, b \in R$), то кольцо косых многочленов
$$R[x;\sigma,\delta] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; xa = \sigma(a)x + \delta(a),\ a \in R \right\}$$
не содержит ненулевых нильпотентных элементов.

2.10. Упражнения

Сделаем несколько замечаний относительно некоторых известных проблем, касающихся ниль-колец. В работах [112, 93] по-

строен пример простой ниль ассоциативной алгебры над любым счетным или конечным полем. Тем самым, решена известная проблема теории колец. В работе [89] доказана эквивалентность следующих до сих пор нерешенных проблем:

1. (С. Амицур) Пусть R – ниль-кольцо. Будет ли кольцо многочленов $R[x]$ радикальным (в смысле Джекобсона)?

2. (Г. Кете) Пусть кольцо R содержит ненулевой ниль односторонний идеал. Содержит ли R ненулевой ниль двусторонний идеал?

3. (Ян Кремпа) Пусть R – ниль-кольцо. Верно ли, что кольцо матриц $M_2(R)$ тоже является ниль-кольцом?

В этой работе обсуждается также и следующая интересная нерешенная проблема И. Херстейна: Пусть для любых элементов a, b кольца R существует целое число $n = n(a,b) \geq 1$ такое, что $(ab - ba)^n = 0$. Верно ли, что множество всех нильпотентных элементов R образует идеал?

Упражнение 2.1. *Пусть* $A = GF(2)[x_1, x_2, \ldots]$ *– коммутативное кольцо многочленов от счетного множества переменных* $\{x_1, x_2, \ldots\}$ *и* $R = A/\left(x_1^2, x_2^2, \ldots\right)$. *Докажите, что нильрадикал* $\mathrm{un}A$ *порождается как идеал элементами* $\{\bar{x}_1, \bar{x}_2, \ldots\}$, *удовлетворяет тождеству* $x^2 = 0$, *но не является нильпотентным идеалом.*

Упражнение 2.2. *Докажите, что кольцо* R *удовлетворяет тождеству* $x_1 x_2 \ldots x_N = 0$ *тогда и только тогда, когда существует такое целое число* $k > \frac{N}{2}$, *что полное кольцо матриц* $M_k(R)$ *удовлетворяет тождеству* $x^N = 0$.

$\diamondsuit$ Если $M_k(R)$ удовлетворяет тождеству $x^N = 0$ и $k > \frac{N}{2}$, то $M_k(R)$ удовлетворяет полилинейному тождеству

$$\sum_{(i)} x_{i_1} x_{i_2} \ldots, x_{i_N} = 0,$$

полученному линеаризацией из $x_N = 0$. Пусть $a_1, a_2, \ldots, a_N$ – произвольные элементы из R. Полагая в тождестве

$$x_1 = a_1 e_{11},\ x_2 = a_2 e_{12},\ x_3 = a_3 e_{22},\ x_4 = a_4 e_{23},\ \ldots,$$

мы получим, что

$$(a_1 a_2 \ldots a_N) e_{1\left[\frac{N}{2}\right]+1} = 0,$$

где $\left[\frac{N}{2}\right] + 1 \leq k$. Откуда следует, что $R^N = (0)$. $\diamondsuit$

Упражнение 2.3. *Пусть кольцо R удовлетворяет тождеству $x^n = 0$. Докажите, что R удовлетворяет тождеству*

$$x^{n-1} y x^{n-1} = 0.$$

$\diamondsuit$ Представьте в кольце $R^{\#}$ правую часть равенства

$$\left(x^{n-1} y + x\right)^n = 0$$

в виде $x^{n-1} y x^{n-1}\,(1 + v)$, где $v \in R$. $\diamondsuit$

Упражнение 2.4. *Пусть A – коммутативная область целостности с единицей. Элемент $a \in A$ называется простым (неразложимым), если идеал $(a) = aA$ является простым (соответственно, если a – необратимый элемент и из разложения $a = bc$ следует, что либо $b|1$, либо $c|1$)). Докажите, что простой элемент является неразложимым. Верно ли обратное утверждение?*

$\diamondsuit$ Рассмотрите область целостности

$$Z[i\sqrt{5}] = \{a + bi\sqrt{5} |\ a, b \in Z\}$$

и проверьте, что 2 является неразложимым элементом, а идеал (2) содержит $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ и не является простым. $\diamondsuit$

Упражнение 2.5. *Пусть R – кольцо с единицей, I – нильидеал R, a – такой элемент R, что его образ $\bar{a} \in R/I$ является обратимым элементом в R/I. Докажите, что a – обратимый элемент в R.*

Упражнение 2.6. *Пусть $R_1, \ldots, R_n$ – кольца и*

$$R = R_1 \oplus \ldots \oplus R_n$$

– их прямая сумма. Докажите, что идеал $P \lhd R$ является простым тогда и только тогда, когда

$$P = R_1 \oplus \ldots \oplus R_{i-1} \oplus P_i \oplus R_{i+1} \oplus \ldots \oplus R_n$$

для некоторого числа $i \leq n$, где p_i – простой идеал R_i.

$\diamondsuit$ Пусть P – простой идеал R. Тогда, например, $R_1 \nsubseteq P$ (мы отождествляем R_1 с множеством $\{(a_1, 0, \ldots, 0) |\ a_1 \in R_1\}$). Из включений $R_1 \cdot R_2 = (0) \subseteq P, \ldots, R_1 \cdot R_n = (0) \subseteq P$ следует, что $R_2 \oplus \ldots \oplus R_n \subseteq P$ и $P = (P \cap R_1) \oplus R_2 \oplus \ldots \oplus R_n$. Поэтому $R/P \cong R_1/P \cap R_1$ – первичное кольцо и идеал $P_1 = P \cap R_1$ является простым в R_1. $\diamondsuit$

Упражнение 2.7. *Пусть R – первичное кольцо и I – конечный ненулевой правый идеал кольца R. Докажите, что R – конечное кольцо.*

$\diamondsuit$ Пусть $I = \{0, x_1, x_2, \ldots, x_n\}$ и R – бесконечное кольцо. Так как $x_i R \subseteq I$, то индекс

$$\left[R^+ : r(x_i)\right] \leq n + 1,$$

$i \leq n$. Пусть $K = \bigcap\limits_{i=1}^{n} r(x_i)$. Тогда $[R^+ : K] < \infty$ и K – бесконечный правый идеал кольца R такой, что $IK = (0)$. Откуда следует, что $IRK \subseteq (IR)K \subseteq IK = (0)$. Противоречие. $\diamondsuit$

Упражнение 2.8. *Пусть V – n-мерные векторные пространства над телом D и S – ниль-полугруппа в $\mathrm{End}_D V$. Докажите, что $S^n = (0)$.*

$\diamondsuit$ Доказательство проведем методом математической индукции по n. Ясно, что $S = (0)$ при $n = 1$. Сделаем предположение индукции об истинности утверждения для пространств меньшей размерности и докажем наше утверждение для пространства V. Если $VS \neq V$, то $\dim VS \leq n-1$, $(VS)\,S \subseteq VS$ и по предположению индукции $(VS)\,S^m = (0)$, где $m \leq n-1$ и, следовательно, $VS^{m+1} = (0)$, где $m+1 \leq n$. Если же $VS = V$, то $V = Vs_1 + \ldots + Vs_t$ для некоторых элементов $s_1, \ldots, s_t \in S$. Откуда следует, что для любого целого числа $k \geq 1$

$$V = \sum_{(i)} V\left(s_{i_1} \ldots s_{i_k}\right).$$

Пусть $a \in \{s_1, \ldots, s_t\}$. Тогда $Va \neq V$ и $(Va)(Sa) \subseteq Va$. По предположению индукции $(Va)\,(Sa)^N = (0)$ и $V\,(Sa)^{N+1} = (0)$. Таким образом, существуют такие числа $N_1 \geq 1, \ldots, N_t \geq 1$, что

$$(Ss_1)^{N_1} = (0),\ \ldots,\ (Ss_t)^{N_t} = (0).$$

Пусть

$$k = \sum_{i=1}^{t} (2N_i + 2).$$

Тогда каждое слово

$$s_{i_1} \ldots s_{i_k}$$

содержит некоторое подслово вида

$$\underbrace{{*}s_i * s_i * \ldots * s_i{*}}_{N_i},$$

$i \leq t$, и, следовательно, равно нулю. Поэтому $V = (0)$. $\diamondsuit$

Упражнение 2.9. *Пусть R – коммутативная область целостности с единицей, P – простой идеал R и*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in R[X]$$

такой, что $a_0 \notin P$, $\{a_1, \ldots, a_n\} \subseteq P$ и $a_n \notin P^2$. Пусть также

$$a_0R + a_1R + \ldots + a_nR = R.$$

Докажите, что $f(x)$ – неприводимый многочлен в $R[x]$ (например, $x^5y^3 + x^4z^3 + x^3yx^2 + y^2z$ – неприводимый многочлен в $Z[x, y, z]$).

$\diamondsuit$ Если $f(x) = cg(x)$, где $g(x) \in R[x]$, то $a_i \in cR$ и $cR = R$, то есть c – обратимый элемент. Если

$$f(x) = \left(b_0x^k + \ldots\right)\left(c_0x^{n-k} + \ldots\right),$$

то $b_0, c_0 \in P$ и, например, $b_k \in P$. Тогда в $R/P[x]$

$$\bar{f}(x) = \left(\bar{b}_0x^k + \ldots + \bar{b}_k\right)\left(\bar{c}_0x^{n-k} + \ldots\right) = \bar{a}_0x^n$$

и число слагаемых в левой части равенства больше двух. $\diamondsuit$

Упражнение 2.10. *Пусть R – коммутативное кольцо,*

$$\{P_1, \ldots, P_n\}$$

– множество простых идеалов и I – идеал R такой, что

$$I \subseteq \bigcup_{i=1}^{n} P_i.$$

Докажите, что существует простой идеал P_{i_0}, $i_0 \leq n$ такой, что $I \subseteq P_{i_0}$.

$\diamondsuit$ Воспользуемся методом математической индукции по числу n. Тогда можно считать, что существуют элементы

$$\begin{gathered} a_1 \in I \setminus (P_2 \cup \ldots \cup P_n), \\ a_2 \in I \setminus (P_1 \cup P_3 \cup \ldots \cup P_n), \\ \ldots \\ a_n \in I \setminus (P_1 \cup \ldots \cup P_{n-1}). \end{gathered}$$

Пусть

$$a = a_2 a_3 \ldots a_n + a_1 a_3 \ldots a_n + \ldots + a_1 a_2 \ldots a_n \in I.$$

Тогда $a \notin (P_1 \cup \ldots \cup P_n)$. Противоречие. $\diamondsuit$

Упражнение 2.11. *Пусть $R, R^2, \ldots, R_{k-1}, R^k = (0)$ – единственные идеалы конечного кольца R. Докажите, что*

$$R \cong x\mathbb{Z}[x] / \left(x^k, f(x)\right),$$

где

$$f(x) = px - a_2 x^2 - \ldots - a_{k-1} x^{k-1},$$

$0 \leq a_i \leq p$, *p – простое число.*

$\diamondsuit$ Идеалы кольца R образуют цепь (по включению). Если p_1, p_2 – различные простые делители $|R|$, то

$$A = \{a \in R |\ p_1 a = 0\},\ B = \{a \in R |\ p_2 a = 0\}$$

– ненулевые идеалы R такие, что $A \not\subseteq B$ и $B \not\subseteq A$. Следовательно $|R| = p^n$, где p – простое число. Пусть $k \geq 2$ и $a \in R \setminus R^2$. Тогда подкольцо $\langle a \rangle + R^2 = \mathbb{Z}a + R^2$ образует идеал R, строго содержащий R^2. Поэтому

$$\begin{aligned} R = \mathbb{Z}a + \left(\mathbb{Z}a + R^2\right)^2 = \mathbb{Z}a + \mathbb{Z}a^2 + R^3 = \ldots \\ = \mathbb{Z}a + \mathbb{Z}a^2 + \ldots + \mathbb{Z}a^{k-1}, \end{aligned}$$

где $a^k = 0$. Если $pa \notin R^2$, то $R = \mathbb{Z}(pa) + R^2$ и

$$a = mpa + \lambda_2 a^2 + \ldots + \lambda_{k-1} a^{k-1}.$$

Откуда следует, что

$$a^{k-1} = mpa^{k-1} = mp\left(mpa^{k-1}\right) = \ldots = m^n p^n a^{k-1} = 0.$$

Противоречие доказывает, что

$$pa = a_2 a^2 + \ldots + a_{k-1} a^{k-1},$$

где $a_i \in \mathbb{Z}$.

Рассмотрим отображение

$$\varphi : x\mathbb{Z}[x] \to R, \quad \varphi\left(xg(x)\right) = ag(a).$$

Оно является гомоморфизмом и его ядро $\operatorname{Ker}\varphi$ содержит x^k, $f(x) = px - \sum\limits_{i=2}^{k-1} a_i x^i$. Если $\operatorname{Ker}\varphi$ не совпадает с идеалом, порожденным $\left\{x^k, f(x)\right\}$, то он содержит многочлен

$$c_1 x + c_2 x^2 + \ldots + c_{k-1} x^{k-1},$$

где $0 \leq c_i < p$ и некоторый коэффициент $c_{i_0} \neq 0$, $i_0 \leq k-1$. Откуда следует, что $a^{i_0} \in R^{i_0+1}$. Противоречие доказывает, что $\operatorname{Ker}\varphi = \left(x^k, f(x)\right)$ и $R \cong x\mathbb{Z}[x]/\left(x^k, f(x)\right)$. $\diamondsuit$

Упражнение 2.12. *Пусть R – кольцо без нильпотентных элементов и*

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{i=0}^{m} b_i x_i$$

– два многочлена из $R[x]$ таких, что $f(x) \cdot g(x) = 0$. Докажите, что $a_i b_j = 0$, где $0 \leq i \leq n$, $0 \leq j \leq m$.

$\diamondsuit$ По теореме Андрунакиевича-Рябухина существуют идеалы $\{P_\alpha \lhd R | \, \alpha \in \Omega\}$ такие, что $\bigcap\limits_{\alpha\in\Omega} P_\alpha = (0)$ и R/P_α – кольцо без делителей нуля. Если, например, $a_{i_0}b_{j_0} \neq 0$, то существует идеал P_α, $\alpha \in \Omega$, такой, что $a_{i_0}b_{j_0} \notin P_\alpha$. Следовательно, $a_{i_0} \notin P_\alpha$, $b_{j_0} \notin P_\alpha$ и многочлены

$$\bar{f}(x) = \sum_{i=0}^{n} \bar{a}_i x^i, \quad \bar{g}(x) = \sum_{j=0}^{m} \bar{b}_j x^j$$

являются ненулевыми в кольце $R/P_\alpha[x]$. Так как R/P_α – кольцо без делителей нуля, то кольцо многочленов $R/P_\alpha[x]$ тоже не содержит делителей нуля, то есть $\bar{f}(x) \cdot \bar{g}(x) \neq \bar{0}$. С другой стороны, естественный гомоморфизм

$$\pi : R \to R/P_\alpha$$

продолжается до гомоморфизма

$$\pi_1 : R[x] \to R/P_\alpha[x], \quad \pi_1 \left(\sum_{i=0}^{k} c_i x^i \right) = \sum_{i=0}^{k} \bar{c}_i x^i.$$

Следовательно, из равенства $f(x)g(x) = 0$ следует $\bar{f}(x)\bar{g}(x) = \bar{0}$. Противоречие доказывает, что $a_i b_j = 0$ для любых чисел $i \leq n$, $j \leq m$. $\diamondsuit$

Упражнение 2.13. *Пусть R – кольцо без нильпотентных элементов и $X \subseteq R$. Тогда*

$$\ell(X) = \{a \in R | \;\; aX = (0)\} = r(X) = \{a \in R | \;\; Xa = (0)\} \lhd R$$

и $R/\ell\,(X)$ – кольцо без нильпотентных элементов.

$\diamondsuit$ Пусть $x \in X$ и $\bar{a}$ – нильпотентный элемент в $R/l\,(X)$. Тогда существует целое число $n \geq 1$ такое, что $a^n x = 0$. Откуда следует, что $a^n x^n = (ax)^n = 0$ и $ax = 0$, то есть $a \in l\,(X)$ и $\bar{a} = \bar{0}$. $\diamondsuit$

Упражнение 2.14. *Пусть $R = F\langle x_1, x_2, \ldots\rangle$ – свободная ассоциативная алгебра без единицы над полем F от бесконечного числа переменных и I – идеал R, порожденный всеми словами*

$$\{x_{i_1}x_{i_2}\ldots x_{i_k}|\ \max\{i_1,\ldots,i_k\} < k\}.$$

Докажите, что R/I – первичная локально нильпотентная алгебра.

Упражнение 2.15. *Пусть R – конечное коммутативное кольцо с единицей и M – его единственный максимальный идеал. Докажите, что множество делителей нуля $R[t]$ совпадает с $M[t]$.*

$\diamondsuit$ Радикал Джекобсона $J(R) = M$ и ввиду конечности кольца R имеем $M^n = (0)$ для некоторого целого числа $n \geq 1$. Поэтому $M[t]$ состоит из делителей нуля. Пусть $a(t)$ и $b(t)$ – ненулевые многочлены из $R[t]$ такие, что $a(t)b(t) = 0$. Покажем, что они оба принадлежат $M[t]$. Если $a(t)$, $b(t)$ не принадлежат $M[t]$, то их образы $\bar{a}(t) \neq \bar{0}$, $\bar{b}(t) \neq \bar{0}$ в $R/M[t]$. Кольцо R/M – поле и $R/M[t]$ – область целостности, то есть $\bar{a}(t)\bar{b}(t) \neq \bar{0}$. Противоречие.

Если $a(t) \notin M[t]$ и $b(t) \in M[t]$, то можно считать, что

$$a(t) = a_0 + a_1t + \ldots + a_{k-1}t^{k-1} + t^k + t^{k+1}\varphi(t),$$

где $a_i \in M$, $i \leq k-1$,

$$b(t) = b_0 + b_1t + \ldots + b_{s-1}t^{s-1} + b_st^s + t^{s+1}\varphi(t),$$

где $b_i \in M^{m+1}$, $i \leq s-1$ и $b_s \in M^m$, $\{b_{s+1}, \ldots\} \subseteq M^m$, $b_s \neq 0$. Тогда $a(t)b(t)$ имеет ненулевой коэффициент из $M^m \backslash M^{m+1}$ при t^{k+s}. Следовательно, $a(t)b(t) \neq 0$. Противоречие доказывает, что $a(t), b(t) \in M[t]$. $\diamondsuit$

Упражнение 2.16. *Пусть R – ненулевое кольцо и для любого ненулевого элемента $x \in R$ выполнено $xR = R$. Докажите, что R – тело.*

$\diamondsuit$ Заметим, что R – простое кольцо без нильпотентных элементов. Следовательно, R – кольцо без делителей нуля и если $x \neq 0$, $x \in R$, $xe = x$, то для любого элемента $y \in R$ $x(ey - y) = 0$, $ey = y$. Далее $(ye - y)x = y(ex) - yx = 0$, то есть $ye = y$ и e – единица кольца R. $\diamondsuit$

Упражнение 2.17. *Пусть R – кольцо без нильпотентных идеалов, удовлетворяющее тождеству*

$$[x_1, x_2, \ldots, x_n] = 0,$$

где

$$[x_1, \ldots, x_m] = \big[[x_1, \ldots, x_{m-1}], x_m\big],$$

$m \geq 2$. Докажите, что R – коммутативное кольцо.

$\diamondsuit$ Пусть $n \geq 3$ и $\{a_1, \ldots, a_{n-1}\}$ – такие элементы R, что

$$a = [a_1, \ldots, a_{n-1}] = [b, a_{n-1}] \neq 0,$$

где $b = [a_1, \ldots, a_{n-2}]$. Тогда a – центральный элемент R и

$$a^2 = [b, a_{n-1}]\,[b, a_{n-1}] = [b\,[b, a_{n-1}]\,, a_{n-1}] - b\,[[b, a_{n-1}]\,, a_{n-1}] = \\ = [[b, ba_{n-1}]\,, a_{n-1}] - b\,[[b, a_{n-1}]\,, a_{n-1}] = 0.$$

Пусть $I = a\mathbb{Z} + aR = (a)$. Тогда $I^2 = 0$. Противоречие. $\diamondsuit$

Упражнение 2.18. *Пусть δ – дифференцирование $\mathbb{Q}$-алгебры R, то есть такое линейное отображение $\delta : R \to R$, что для любых элементов $a, b \in R$ $\delta(ab) = \delta(a)b + a\delta(b)$. Докажите, что $\delta(\mathrm{un}(R)) \subseteq \mathrm{un}R$.*

$\diamondsuit$ Пусть $a \in \mathrm{un}(R)$. Покажем, что $R^{\#}\delta(a)R^{\#}$ – ниль-идеал. Пусть $b = \sum\limits_i x_i\delta(a)y_i$ – произвольный элемент из $R^{\#}\delta(a)R^{\#}$. Положим

$$c = \sum_i x_i a b_i \in \mathrm{un}(R).$$

Тогда $c^m = 0$ для некоторого целого числа $m \geq 1$. Так как

$$\delta(x_i a y_i) = \delta(x_i)\, a y_i + x_i \delta(a) y_i + x_i a \delta(y) \equiv x_i \delta(a) y_i \,(\mathrm{mod}\, \mathrm{un}(R)),$$

то $\delta(c) \equiv b \,(\mathrm{mod}\, \mathrm{un}(R))$. В силу формулы Лейбница

$$\delta^k(ab) = \sum_i \binom{k}{i} \delta^i(a) \delta^{k-i}(b)$$

имеем, что

$$\delta^2\left(c^2\right) = c \cdot \delta^2(c) + \binom{2}{1} \delta(c)\delta(c) + \delta^2(c)c \equiv \binom{2}{1} b^2 \,(\mathrm{mod}\, \mathrm{un}(R)),$$

$$\delta^3\left(c^3\right) = c\delta^3\left(c^2\right) + 3\delta(c)\delta^2\left(c^2\right) + 3\delta^2(c)\delta\left(c^2\right) + \delta^3(c)c^2 \equiv$$
$$\equiv 6b^3 \,(\mathrm{mod}\, \mathrm{un}(R)),$$

$$\ldots,$$

$$\delta^m\left(c^m\right) = 0 = N \cdot b^m + v,$$

где v – некоторый элемент из $\mathrm{un}(R)$ и N – некоторое натуральное число. Следовательно, b – нильпотентный элемент и $\delta(a) \in \mathrm{un}(R)$. $\diamondsuit$

Глава 3

Классические кольца частных

Конструкция кольца частных и локализация относительно простого идеала являются важными техническими средствами при изучении коммутативных колец. Цель настоящей главы – построить аналогическую конструкцию для некоммутативных колец и применить ее к описанию первичных (полупервичных) колец с некоторыми условиями максимальности для правых идеалов. Тем самым, будет получен аналог теоремы Веддерберна-Артина (см. главу 1) для нетеровых колец.

3.1. Кольца частных коммутативных колец

Пусть R – коммутативное кольцо, содержащее хотя бы один регулярный элемент, то есть такой ненулевой элемент $b \in R$, что если $xb = 0$, $x \in R$, то $x = 0$. Пусть M – множество всех регулярных элементов кольца R. Введем на множестве

$$R \times M = \{(a, c) |\ a \in R,\ c \in M\}$$

следующее бинарное отношение. Мы скажем, что пары (a_1, c_1) и (a_2, c_2) эквивалентны (в обозначении, $(a_1, c_1) \equiv (a_2, c_2)$), если

$a_1c_2 = a_2c_1$. В частности, $(a_1, c) \equiv (ac_1, cc_1)$ для любого регулярного элемента $c_1 \in M$. Легко видеть, что отношение $\equiv$ является рефлексивным и симметричным. Проверим его транзитивность. Пусть $(a_1, c_1) \equiv (a_2, c_2)$ и $(a_2, c_2) \equiv (a_3, c_3)$. Тогда $a_1c_2 = a_2c_1$ и $a_2c_3 = a_3c_2$. Следовательно, $a_1c_2c_3 = a_2c_1c_3 = a_3c_2c_1$ или $(a_1c_3 - a_3c_1)c_2 = 0$. Так как c_2 – регулярный элемент в кольце R, то $a_1c_3 = a_3c_1$ и $(a_1, c_1) \equiv (a_3, c_3)$. Итак $\equiv$ – отношение эквивалентности. Оно индуцирует разбиение множества $R \times M$ на классы эквивалентных элементов. Класс, содержащий пару (a, b), будем обозначать $\overline{(a, b)}$ или ab^{-1}. Обозначим множество всех классов через R_M (иногда оно обозначается в виде $M^{-1}R$). Введем на R_M структуру кольца следующим образом:

$$ab^{-1} + cd^{-1} = (ad + cb)(bd)^{-1}, \quad (ab^{-1})(cd^{-1}) = (ac)(bd)^{-1}.$$

Заметим, что из регулярности элементов b, d следует регулярность элемента bd (то есть M является подполугруппой мультипликативной полугруппы $\langle R, \cdot \rangle$). Проверим корректность выше приведенных операций. Пусть $(a, b) \equiv (a_1, b_1)$ и $(c, d) \equiv (c_1, d_1)$. Тогда $ab_1 = a_1b$ и $cd_1 = c_1d$. Следовательно,

$$\begin{aligned}(ac)(b_1d_1) = (a_1b)(c_1d) = (a_1c_1)(bd),\\ (ad + cb)(b_1d_1) = (ab_1)(dd_1) + (cd_1)(bb_1) =\\ = (a_1b)(dd_1) + (c_1d)(bb_1) = (a_1d_1 + c_1b_1)(bd)\end{aligned}$$

и

$$(ad + cb, bd) \equiv (a_1d_1 + c_1b_1, b_1d_1),$$

$$(ac, bd) \equiv (a_1c_1, b_1d_1).$$

Непосредственно проверяется, что R_M – коммутативное и ассоциативное кольцо. Пусть c – фиксированный элемент из M. Тогда класс $\overline{(c, c)} = c \cdot c^{-1}$ является единицей в R_M и отображение $\varphi(a) = (ac)c^{-1}$ является изоморфизмом кольца R в кольцо R_M. Кольцо R_M называется *полным (классическим) кольцом частных* кольца R.

Предложение 3.1.

1. $a \in M \Leftrightarrow \varphi(a) = (ac)c^{-1}$ *регулярный элемент в* R_M.
2. $\varphi(a)$ – *обратимый элемент в* $R_M \Leftrightarrow a \in M$.
3. *Каждый элемент* ab^{-1} *из* R_M *может быть записан в виде* $\varphi(x)\varphi(y)^{-1}$.

□ Если $a \in M$, то $ac \in M$ и $\overline{(c, ac)}$ – обратный элемент к $\varphi(a) = \overline{(ac, c)} = (ac)c^{-1}$. Легко видеть, что если $\varphi(a)$ – обратимый элемент в R_M, то $a \in M$. Далее, $\overline{(a, b)} = \overline{(ac, c)} \cdot \overline{(c, bc)} = \varphi(a) \cdot \varphi(b)^{-1}$. □

Пусть S – полугруппа регулярных элементов кольца R, то есть S – подполугруппа $\langle M, \cdot \rangle$. Обозначим через R_S (или $S^{-1}R$) множество дробей в R_M вида

$$\{as^{-1} |\ a \in R,\ s \in S\}.$$

Тогда R_S – подкольцо R_M. Оно называется *кольцом частных относительно полугруппы* S.

Предложение 3.2. *Пусть* R *– промежуточное кольцо между кольцом целых чисел* $\mathbb{Z}$ *и полем рациональных чисел* $\mathbb{Q}$. *Тогда* $R = \mathbb{Z}_S$ *для некоторой полугруппы* S.

□ Действительно, пусть

$$S = \left\{ b \in \mathbb{Z} \,\middle|\, \text{существует несократимая дробь } \frac{a}{b} \in R \right\}.$$

Пусть $b \in S$ и $\frac{a}{b} \in R$, где $(a, b) = 1$. По лемме о наибольшем общем делителе существуют целые числа x, y такие, что $ax + by = 1$. Следовательно,

$$\frac{a}{b}x + y = \frac{1}{b} \in R.$$

Откуда следует, что S – полугруппа и $R = \mathbb{Z}_S$. □

Пусть R – коммутативная область целостности и I – простой идеал R. Пусть $S = R \setminus I$. Тогда S – мультипликативно замкнутое множество. Рассмотрим кольцо частных $R_S = S^{-1}R$. В нем элементы вида as^{-1}, где $a \in I$, образуют единственный максимальный идеал (то есть $S^{-1}R$ – локальное кольцо). Переход от кольца R к кольцу $S^{-1}R$, где $S = R \setminus I$, называется *локализацией относительно* I. В частности, если $R = \mathbb{Z}$ и $I = p\mathbb{Z}$ (p – простое число), то локализация относительно простого идеала $p\mathbb{Z}$ приводит к кольцу, состоящему из всех рациональных дробей вида

$$\left\{ \frac{a}{b} \,\middle|\, a \in \mathbb{Z},\ (p, b) = 1 \right\}.$$

Пусть R – произвольное коммутативное кольцо и S – подполугруппа мультипликативной полугруппы R. Определим на множестве

$$R \times S = \{(a, s) |\ a \in R,\ s \in S\}$$

следующее бинарное отношение:

$$(a, s) \sim (b, t) \Leftrightarrow (at - bs)u = 0$$

для некоторого элемента $u \in S$. Это отношение является рефлективным, симметричным и транзитивным, то есть отношением эквивалентности на множестве $R \times S$. Оно индуцирует разбиение $R \times S$ на классы эквивалентных элементов. Обозначим через $\overline{(a, s)}$ или $s^{-1}a$ класс, содержащий пару (a, s), и через $S^{-1}R = \{s^{-1}a\}$ – множество всех классов. На множестве $S^{-1}R$ можно ввести структуру кольца, положив

$$s^{-1}a + t^{-1}b = (st)^{-1}(at + bs), \quad \left(s^{-1}a\right) \cdot \left(t^{-1}b\right) = (st)^{-1}(ab).$$

Не сложно проверить корректность этих операций. Множество $S^{-1}R$ является коммутативным кольцом относительно приведенных операций, а отображение $f(a) = s^{-1}(as)$, где s – фиксированный элемент S, является гомоморфизмом кольца R в кольцо $S^{-1}R$. Кольцо $S^{-1}R$ называется *кольцом частных* R *относительно* S.

3.2. Правые кольца частных

В данном разделе мы приведем конструкцию классического правого кольца частных для ассоциативных колец, обобщающую аналогичную конструкцию для коммутативных колец. Пусть R – ассоциативное кольцо. Элемент кольца R называется *регулярным*, если он не является ни левым, ни правым делителем нуля. Пусть S – непустое множество регулярных элементов кольца R, замкнутое относительно умножения (то есть S – подполугруппа регулярных элементов мультипликативной полугруппы кольца R).

Кольцо Q называется *(классическим) правым кольцом частных* кольца R относительно полугруппы регулярных элементов S, если:

1. Q содержит единицу.
2. Каждый элемент из S обратим в Q.
3. Каждый элемент $x \in Q$ представим в виде as^{-1}, где $a \in R$ и $s \in S$.

Если R содержит хотя бы один регулярный элемент и S – полугруппа всех регулярных элементов кольца R, то классическое правое кольцо частных кольца R относительно S называется *полным кольцом частных* R и обозначается $Q(R)$, а кольцо R называется *правым порядком* в $Q(R)$.

Теорема 3.1 (О. Оре).
Кольцо R обладает полным классическим правым кольцом частных относительно полугруппы всех регулярных элементов S тогда и только тогда, когда R удовлетворяет условию Оре: для любых элементов $a \in R$, $s \in S$ существуют элементы $s_1 \in S$, $a_1 \in R$ такие, что $as_1 = sa_1$.

□ Пусть $Q(R)$ – полное классическое правое кольцо частных кольца R и $a \in R$, $s \in S$. Тогда элемент $s^{-1}a \in Q$ представим в виде $a_1 s_1^{-1}$ и, следовательно, $as_1 = sa_1$, где $s_1 \in S$, $a_1 \in R$.

Докажем обратное утверждение. Пусть R удовлетворяет условию Ope. Заметим сначала, что если $x, y, z \in S$ и $xy = zt$ для некоторого элемента $t \in R$, то t – регулярный элемент. Действительно, если $ta = 0$, то $(xy)a = 0$ и $a = 0$. Если $at = 0$, то, выбирая элементы $c, u \in S$, $d, v \in R$ такие, что $zu = xv$, $vc = yd$, имеем, что $xvc = xyd = zuc = ztd$. Так как z – регулярный элемент, то $uc = td$ и $a(uc) = atd = 0$. Откуда следует, что $a = 0$ и t – регулярный элемент.

Введем на множестве $R \times S = \{(a, s) |\ a \in R,\ s \in S\}$ бинарное отношение $\sim$, положив $(a, s) \sim (b, t)$ тогда и только тогда, когда из того, что $sx = ty$ для некоторых элементов $x, y \in S$ следует равенство $ax = by$. Прежде чем проверять, что $\sim$ является отношением эквивалентности, заметим справедливость следующего утверждения. Пусть (a, s), $(b, t) \in R \times S$ и существуют такие элементы $x, x_1, y, y_1 \in S$, что $sx = ty$, $ax = by$, $sx_1 = ty_1$. Тогда $ax_1 = by_1$. Действительно, выберем элементы $u, v \in S$ такие, что $yu = y_1v$. Тогда $sx_1v = ty_1v = tyu = sxu$ и $xu = x_1v$. Поэтому $ax_1v = axu = byu = by_1v$ и $ax_1 = by_1$. Рефлексивность и симметричность отношения $\sim$ очевидны. Докажем транзитивность. Пусть $(a, s) \sim (b, t)$ и $(b, t) \sim (c, z)$. Если $sx = zy$, где $x, y \in S$, то существуют элементы $x_1,\ q \in S$ такие, что $(sx)x_1 = tq = z(yx_1)$. Поэтому $axx_1 = bq = cyx_1$. Так как x_1 – регулярный элемент, то $ax = cy$. Итак, $\sim$ – отношение эквивалентности.

Обозначим через $Q(R)$ (или через RS^{-1}) множество всех классов эквивалентности $\left\{\overline{(a, s)}\right\}$. Каждый класс $\overline{(a, s)}$ будем обозначать через as^{-1}. Определим на множестве $Q(R)$ операции сложения и умножения следующим образом. Пусть as^{-1}, $bt^{-1} \in Q(R)$ и x, y – такие элементы S, что $sx = ty = m$. Положим

$$as^{-1} + bt^{-1} = (ax + by)m^{-1}.$$

Заметим, что $as^{-1} = (ax)m^{-1}$, $bt^{-1} = (by)m^{-1}$. Докажем корректность операции сложения. Если $sx_1 = ty_1 = m_1$ при некоторых элементах $x_1, y_1 \in S$ и $mu = m_1v$, где $u, v \in S$, то $sxu = sx_1v$ и $xu = x_1v$. Аналогично $mu = sxu = tyu = m_1v =$

ty_1v и $yu = y_1v$. Откуда следует, что $(ax + by)u = (ax_1 + by_1)v$ и $(ax + cy)m^{-1} = (ax_1 + by_1)m_1^{-1}$. Итак, определение операции сложения не зависит от выбора элемента m. Докажем, что определение этой операции не зависит от выбора представителей для as^{-1}. Пусть $as^{-1} = a_1s_1^{-1}$. В силу условия Ope существуют элементы $u_i \in S$, $i \leq 6$ такие, что $su_1 = s_1u_2$, $su_3 = tu_4$, $u_1u_5 = u_3u_6$. Тогда $s(u_1u_5) = su_3u_6 = t(u_4u_6) = s_1(u_2u_5)$. Пусть $x_1 = u_1u_5$, $y_1 = u_4u_6$, $z = u_2u_5 \in S$. Тогда $sx_1 = ty_1 = s_1z = m_1$ и $ax_1 = a_1z$. Так как операция сложения не зависит от выбора элемента m, то $as^{-1} + bt^{-1} = (ax + by)m^{-1} = (ax_1 + by_1)m_1^{-1}$. Пара $(ax_1 + by_1, m_1)$ эквивалентна паре $(a_1z + by_1, m_1)$, так как $ax_1 = a_1z$. Следовательно, $(ax_1 + by_1)m^{-1} = a_1s_1^{-1} + bt^{-1} = as^{-1} + bt^{-1}$. Определим в $Q(R)$ операцию умножения по правилу

$$\left(as^{-1}\right)\left(bt^{-1}\right) = (ax_1)\,(ty_1)^{-1},$$

где $n = sx_1 = by_1$, $y_1 \in S$, $x_1 \in R$. Корректность операции умножения доказывается аналогично предыдущему. Если $sx_2 = by_2$, где $y_2 \in S$, $x_2 \in R$, то для проверки эквивалентности пар $(ax_1, ty_1) \sim (ax_2, ty_2)$ предположим, что $ty_1u = ty_2v$, где $u, v \in S$. Тогда $y_1u = y_2v$, $sx_1 = by_1$, $sx_2 = by_2$, $by_1u = sx_1u = b(y_2v) = sx_2v$ и $x_1u = x_2v$. Откуда следует, что $ax_1u = ax_2v$, то есть $(ax_1)(ty_1)^{-1} = (ax_2)(ty_2)^{-1}$.

Итак, мы доказали независимость операции умножения от выбора элемента $n = sx_1 = by_1$. Докажем теперь независимость этой операции от выбора представителей для as^{-1}, bt^{-1}. Пусть $as^{-1} = a_1s_1^{-1}$ и $u, v \in S$ такие элементы, что $su = s_1v$. Тогда $au = a_1v$. Выберем элементы $x \in R$, $y \in S$ такими, что $n_1 = sux = bvy$. Ранее мы доказали независимость операции умножения от выбора $n = sx_1 = by_1$. Поэтому $l = (as^{-1})(bt^{-1}) = (aux)(tvy)^{-1}$. Так как $au = a_1v$, $su = s_1v$, то $n_1 = (s_1v)x = bvy$ и $l = (a_1vx)(tvy)^{-1} = (a_1s_1^{-1}) \cdot (bt^{-1})$. Итак, операция умножения является корректной. Аналогично выше приведенным рассуждениям можно проверить справедливость всех аксиом ассоциативного кольца на множестве $Q(R)$. Положим $a1^{-1} = (as)s^{-1}$, где $a \in R$, $s \in S$. Тогда отображение

$a \to a1^{-1}$ является гомоморфным вложением кольца R в кольцо $Q(R)$ и если $s \in S$, то $1 = s \cdot s^{-1}$ – единица, а $s \cdot 1^{-1}$ – обратимый элемент кольца $Q(R)$. При этом $(s \cdot 1^{-1})^{-1} = 1 \cdot s^{-1}$. Так как $as^{-1} = (a1^{-1})(s \cdot 1^{-1})^{-1}$, то $Q(R)$ – полное классическое правое кольцо частных кольца R. □

Предложение 3.3. *Если*

$$a_1 s_1^{-1}, \ldots, a_n s_n^{-1}$$

– элементы (полного) классического кольца частных $Q(R)$ кольца R, то существуют элементы $b_1, \ldots, b_n \in R$ и регулярный элемент $s \in R$ такие, что

$$a_i \cdot s_i^{-1} = b_i \cdot s^{-1},$$

$i \leq n$, то есть любое конечное множество элементов можно привести к общему знаменателю.

□ Докажем это утверждение методом математической индукции. Предположим, что

$$a_1 s_1^{-1} = b_1 s^{-1}, \ \ldots, \ a_{n-1} s_{n-1}^{-1} = b_{n-1} s^{-1}.$$

Ввиду условия Ope существуют регулярные элементы x, y такие, что $sx = s_n y = t$. Тогда t – регулярный элемент и

$$a_i s_i^{-1} = (b_i \cdot x)t^{-1}, \quad a_n s_n^{-1} = (a_n y)t^{-1},$$

при $i \leq n-1$. □

Кольцо R без делителей нуля, удовлетворяющее правому условию Ope, называется *правой областью Ope.*

Ясно, что область целостности (то есть кольцо без делителей нуля) R является правой областью Ope тогда и только тогда, когда для любых ненулевых элементов $a, b \in R$ справедливо $aR \cap bR \neq (0)$.

Предложение 3.4. *R является правой областью Оре тогда и только тогда, когда R – правый порядок в теле (то есть в кольце с делением).*

Напомним, что кольцо называется *нетеровым справа*, если оно удовлетворяет условию обрыва возрастающих цепей правых идеалов.

Предложение 3.5. *Пусть R – область целостности, являющаяся нетеровым справа кольцом. Тогда R – правая область Оре.*

□ Допустим противное. Тогда существуют ненулевые элементы $a, b \in R$ такие, что $aR \cap bR = (0)$. Рассмотрим возрастающую цепочку идеалов

$$aR \subseteq aR + baR \subseteq aR + baR + b^2aR \subseteq \dots.$$

По условию она стабилизируется, то есть существует натуральное число n такое, что

$$aR + baR + \dots + b^naR = aR + baR + \dots + b^naR + b^{n+1}aR.$$

Откуда следует, что

$$b^{n+1}a^2 = ax_0 + bax_1 + \dots + b^nax_n$$

для некоторых элементов $x_0, \dots, x_n \in R$. Так как

$$ax_0 = b^{n+1}a^2 - (bax_1 + \dots + b^nax_1) \in aR \cap bR,$$

то $x_0 = 0$ и

$$b^na^2 = ax_1 + bax_2 + \dots + b^{n-1}ax_n.$$

Рассуждая аналогично, мы получим, что $ba^2 = 0$. Противоречие. □

Пример 3.1. Пусть F – поле с дифференцированием d, то есть с отображением $d : F \to F$, удовлетворяющим условиям

$$d(a+b) = d(a) + d(b), \quad d(ab) = ad(b) + d(a)b$$

для любых элементов $a, b \in F$, и пусть

$$R = F[t,d] = \left\{ \sum_{i=0}^{n} t^i a_i \,\middle|\, a_i \in F \right\}$$

– кольцо дифференциальных многочленов, в котором сложение многочленов определяется обычным образом, а умножение определяется равенством $at = ta + d(a)$, где $a \in F$. Тогда R – область целостности, являющаяся нетеровым справа кольцом. Более того, в кольце R справедлив алгоритм деления с остатком (справа и слева) и каждый односторонний идеал является главным. Из предложения 3.5 следует, что R – правая область Оре.

Заметим, что если R – артиново справа кольцо и s – регулярный элемент, то цепочка правых идеалов

$$sR^{\#} \supseteq s^2R^{\#} \supseteq \dots$$

стабилизируется, например, на n-м шаге, то есть

$$s^nR^{\#} = s^{n+1}R^{\#}.$$

Откуда следует, что $s^n = s^{n+1}m + s^{n+1}x$, где $m \in \mathbb{Z}$, $x \in R$. В частности, $s^n = s^ne$, где $e = sm + sx$. Для любого элемента $y \in R$ имеем $s^n(y - ey) = s^ny - s^ney = s^ny - s^ny = 0$ и, ввиду регулярности элемента s^n, $y = ey$. Далее, если R – правый порядок в кольце $Q(R)$, то из равенства $s = es$ следует, что e – единица в кольце $Q(R)$ и $s^n = s^{n+1}a$, где $a \in R$. Умножая слева левую и правую части последнего равенства на $(s^n)^{-1}$, получим, что $e = sa$ и $s^{-1} = a \in R$. Откуда следует, что $Q(R) = R$. Итак, если артиново справа кольцо имеет классическое кольцо частных, то оно совпадает с самим кольцом.

3.3. Строение полупервичных колец с условиями Голди

Пусть S – подмножество кольца R. Напомним, что множества

$$r_R(S) = r(S) = \{x \in R |\ sx = 0 \text{ для всех } s \in S\},$$

$$\ell(S) = \{x \in R |\ xs = 0 \text{ для всех } s \in S\}$$

называются соответственно правым и левым аннулятором S и $r(S) \leq_r R$ и $l(S) \leq_l R$.

Кольцо R называется *правым кольцом Голди*, если

1. R удовлетворяет условию обрыва возрастающих цепей правых аннуляторов.

2. R не содержит бесконечных прямых сумм правых идеалов.

Заметим, что любое нетерово справа кольцо R является правым кольцом Голди, так как если в R существует бесконечная прямая сумма правых идеалов $I_1 \oplus I_2 \oplus \ldots$, то существует строго возрастающая цепочка правых идеалов

$$I_1 \subset I_1 \oplus I_2 \subset I_1 \oplus I_2 \oplus I_3 \subset \ldots.$$

Другим примером правого кольца Голди является любая коммутативная область целостности, которая, вообще говоря, не обязана быть нетеровым кольцом. Таким образом, существуют правые кольца Голди, не являющиеся нетеровыми кольцами.

Правый идеал I кольца R называется *существенным*, если он имеет ненулевое пересечение с любым ненулевым правым идеалом кольца R.

Наша цель – доказать две теоремы Голди (см. [77, 78].

Теорема 3.2. *Кольцо R является правым порядком в простом артиновом кольце тогда и только тогда, когда R – первичное правое кольцо Голди.*

Теорема 3.3. *Кольцо R является правым порядком в полупростом артиновом кольце тогда и только тогда, когда R – полупервичное правое кольцо Голди.*

Доказательства этих теорем будет следовать из ниже следующих лемм.

Лемма 3.1. *Пусть R – правый порядок в полупростом (простом) артиновом кольце. Тогда R – ненулевое полупервичное (соответственно, первичное) правое кольцо Голди.*

□ Если $R = (0)$, то в силу определения R не может иметь правое кольцо частных. Итак, $R \neq (0)$ и пусть $Q(R)$ – классическое правое кольцо частных R, являющееся полупростым артиновым кольцом. Так как $Q(R)$ – нетерово справа кольцо и для любого подмножества $S \subseteq R$ $r_R(S) = R \cap r_{Q(R)}(S)$, то R удовлетворяет условию обрыва возрастающих цепей правых аннуляторных идеалов. Если $I_1 \oplus I_2 \oplus \ldots$ – бесконечная прямая сумма правых идеалов кольца R, то рассмотрим сумму $\sum\limits_{i=1}^{\infty} I_i Q(R)$ правых идеалов в кольце $Q(R)$. Докажем, что она тоже является прямой. Действительно, предположив противное, получаем, что

$$x_1(a_1 s_1^{-1}) + \cdots + x_n(a_n s_n^{-1}) = 0,$$

при некоторых элементах $x_i \in I_i$, s_i, $a_i \in R$, $i \leq n$.

Ранее мы доказали, что существует регулярный элемент $s \in R$ и элементы $b_i \in R$ такие, что $a_i s_i = b_i s^{-1}$, $i \leq n$. Следовательно,

$$\sum_{i=1}^{n} x_i \left(a_i s_i^{-1}\right) = \left(\sum_{i=1}^{n} x_i b_i\right) s^{-1} = 0$$

и $\sum\limits_{i=1}^{n} x_i b_i = 0$, где $x_i b_i \in I_i$, $i \leq n$. Так как сумма правых идеалов $I_1 + \cdots + I_n$ является прямой, то $x_i b_i = 0$ и $x_i a_i s_i^{-1} = 0$, $i \leq n$. Противоречие. Итак, R – ненулевое правое кольцо Голди.

Если N_1 – ненулевой нильпотентный идеал кольца R с условиями $N_1^k = (0)$, $N_1^{k-1} \neq (0)$, $k \geq 2$. Тогда $N = N_1^{k-1}$ – ненулевой идеал кольца R с нулевым умножением. Рассмотрим идеал QNQ кольца $Q = Q(R)$. Так как Q – классически полупростое кольцо, то существует центральный идемпотент $e \in Q$ такой, что $QNQ = eQ$. В частности,

$$e = \sum_{i=1}^{n} q_i u_i (a_i s_i^{-1}),$$

где $q_i \in Q$, $u_i \in N$, $a_i \in R$, $s_i \in R$, $i \leq n$. Из предложения 3.3 следует, что $a_i s_i^{-1} = b_i s^{-1}$, при некоторых элементах $s, b_i \in R$, $i \leq n$. Следовательно,

$$e = \left(\sum_{i=1}^{n} q_i \left(u_i b_i \right) \right) s^{-1}, \quad es = \sum_{i=1}^{n} q_i u_i b_i,$$

где $u_i b_i \in N$, $i \leq n$. Поэтому

$$seN = (es)N = \sum_{i=1}^{n} q_i (u_i b_i) N = 0.$$

Так как s – регулярный элемент, то $eN = (0)$ и

$$(QNQ)^2 = eQ \cdot QNQ = Q(eN)Q = (0).$$

Это противоречит полупростоте кольца Q. Итак, R – полупервичное правое кольцо Голди.

Предположим далее, что Q – простое кольцо и в R существуют ненулевые двухсторонние идеалы A, B такие, что $AB = (0)$. Тогда $QAQ = Q$ и

$$1 = \sum_{i=1}^{n} q_i a_i \left(c_i s_i^{-1} \right),$$

при некоторых элементах $q_i \in Q$, $a_i \in A$, c_i, $s_i \in R$, $i \leq n$. Выберем элементы $s, b_i \in R$ так, чтобы $c_i s_i^{-1} = b_i s^{-1}$. Тогда

$$1 = \sum_{i=1}^{n} q_i a_i \left(b_i s^{-1} \right) \quad \text{и} \quad s = \sum_{i=1}^{n} q_i (a_i b_i),$$

где $a_ib_i \in A$, $i \leq n$. Откуда следует, что

$$sB = \left(\sum_{i=1}^{n} q_i(a_ib_i)\right) B = (0).$$

Так как s – регулярный элемент и $B \neq (0)$, то получим противоречие. Итак, если $Q(R)$ – простое артиново кольцо, то R – первичное правое кольцо Голди. □

Лемма 3.2. *Пусть A, B – подмножества кольца R. Тогда*

1. *Если $A \subseteq B$, то $r(A) \supseteq r(B)$.*
2. *$r(A) = r(l(r(A)))$.*
3. *$l(r(l(A))) = l(A)$.*
4. *$l(A \cup B) = l(A) \cap l(B)$.*

□ Утверждения 1 и 4 очевидны. Докажем утверждение 2. Так как $l(r(A)) \supseteq A$, то $r(l(r(A))) \subseteq r(A)$. Пусть $x \in r(A)$. Тогда $l(r(A))x = 0$ и $x \in r(l(r(A)))$. Следовательно, $r(A) = r(l(r(A)))$. Доказательство утверждения 3 аналогично. □

Лемма 3.3. *Кольцо R удовлетворяет условию максимальности на правые аннуляторные идеалы тогда и только тогда, когда R удовлетворяет условию минимальности на левые аннуляторные идеалы.*

□ Пусть кольцо R удовлетворяет условию максимальности на правые аннуляторные идеалы и

$$l(B_1) \supseteq l(B_2) \supseteq \ldots$$

– убывающая цепочка левых аннуляторных идеалов. Тогда по предыдущей лемме мы можем считать, что $B_i = r(l(A_i)$, где $A_i \subseteq R$, $i = 1, 2, \ldots$. Так как

$$l(B_i) = l(r(l(A_i))) = l(A_i) \supseteq l(B_{i+1}) = l(A_{i+1}),$$

то

$$r(l(B_i)) = r(l(A_i)) = B_i \subseteq r(l(B_{i+1})) = r(l(A_{i+1})) = B_{i+1},$$

$i = 1, 2, \ldots$. Следовательно, мы получаем в R неубывающую цепочку правых аннуляторных идеалов

$$B_1 \subseteq B_2 \subseteq \ldots.$$

Пусть она стабилизируется на n-м шаге

$$B_n = B_{n+1} = \ldots.$$

Тогда

$$l(B_n) = l(B_{n+1}) = \ldots$$

и, следовательно, цепь

$$l(B_1) \supseteq l(B_2) \supseteq \ldots$$

тоже стабилизируется. Аналогично доказывается обратное утверждение. □

Лемма 3.4. *Пусть кольцо R удовлетворяет условию обрыва возрастающих цепей для правых аннуляторных идеалов. Тогда для любого элемента $a \in R$ существует натуральное число n такое, что $r(a^k) \cap a^s R = (0)$, где $s \geq n$ и $k \geq 1$.*

□ Рассмотрим цепь правых аннуляторных идеалов

$$r(a) \subseteq r(a^2) \subseteq \ldots.$$

Пусть она стабилизируется на n-м шаге, то есть

$$r(a^n) = r(a^{n+1}) = \ldots.$$

Докажем, что

$$a^n R \cap r(a^n) = (0).$$

Пусть $x \in a^nR \cap r(a^n)$. Тогда $x = a^ny$ и $a^nx = a^{2n}y = 0$. Следовательно, $y \in r(a^{2n}) = r(a^n)$ и $x = a^ny = 0$, а значит, $a^nR \cap r(a^n) = (0)$.

Так как $a^sR \subseteq a^nR$, $r(a^i) \subseteq r(a^n)$ при $1 \leq s,\ i \leq n$ и $r(a^n) = r(a^{n+t})$, $t = 1, 2, \ldots$, то

$$a^sR \cap r(a^n) = a^sR \cap r\left(a^i\right) = a^sR \cap r\left(a^{n+t}\right) = (0).$$

□

Лемма 3.5. *Пусть R – полупервичное ненулевое кольцо с условием максимальности для правых аннуляторных идеалов и пусть A, B – правые идеалы кольца R такие, что $B \subseteq A$ и $l(A) \subset l(B)$, $l(A) \neq l(B)$. Тогда существует такой элемент $a \in A$, что $B \cap aA = (0)$ и $aA \neq (0)$.*

□ Так как кольцо R удовлетворяет условию минимальности для левых аннуляторных идеалов, то существует минимальный левый аннуляторный идеал I такой, что $I \subseteq l(B)$, $l(A) \subset I$, $l(A) \neq I$. Из полупервичности кольца R следует, что $(IA)^2 = IAIA \neq (0)$ и, следовательно, существуют элементы $a \in A$, $i \in I$ такие, что $IaiA \neq (0)$. Докажем, что $B \cap (ai)A = (0)$. Допустим противное и пусть $x = (ai)y \in B$, где $y \in A$, $x \neq 0$. Тогда $Ix \subseteq IB = (0)$. Рассмотрим левый идеал $l(y) \cap I$. Он является левым аннуляторным идеалом, содержащим в $l(A)$ и содержащимся в $l(B)$. Так как $(Iai) \subseteq l(y) \cap I$ и Iai не содержится в $l(A)$, то, ввиду минимальности $I, l(y) \cap I = I$. Откуда следует, что $I \subseteq l(y)$, $Iy = (0)$ и $x = a(iy) = 0$. Противоречие. Итак, $B \cap (ai)A = (0)$ и $(ai)A \neq 0$. □

Лемма 3.6. *Пусть R – ненулевое полупервичное кольцо с условием максимальности на правые аннуляторные идеалы. Если aR и bR – существенные правые идеалы кольца R, то $(ab)R$ – существенный правый идеал R.*

□ Пусть I – некоторый ненулевой правый идеал. Докажем, что $I \cap (ab)R \neq (0)$. Рассмотрим правый идеал

$$I_1 = \{x \in R |\ ax \in I\}.$$

Тогда $aI_1 = aR \cap I \neq (0)$, $I_1 \supseteq r(a)$ и $l(I_1) \subseteq l(r(a))$. Так как $a \in l(r(a))$ и $a \notin l(I_1)$, то по предыдущей лемме существует ненулевой правый идеал T кольца R такой, что $T \subseteq I_1$ и $T \cap r(a) = (0)$. Положим

$$T_1 = \{x \in R |\ bx \in T\}.$$

Тогда $bT_1 = T \cap bR \neq (0)$ и $abT_1 \subseteq aT \subseteq aI_1 \subseteq I \cap (ab)R$. Покажем, что $abT_1 \neq (0)$. Если $abT_1 = (0)$, то $bT_1 \subseteq r(a) \cap T = (0)$. Следовательно, $bT_1 = (0)$. Получаем противоречие. Таким образом, $I \cap (ab)R \neq (0)$. □

Лемма 3.7. *Пусть R – ненулевое полупервичное кольцо с условием максимальности для правых аннуляторных идеалов и aR – существенный правый идеал. Тогда a – регулярный элемент кольца R.*

□ Если $l(a) \neq (0)$, то, полагая в лемме 3.5 $B = aR$, $A = R$, имеем, что для некоторого элемента $x \in R$ справедливо $aR \cap xR \neq 0$ и $xR \neq (0)$. Противоречие. Итак, $l(a) = 0$. По лемме 3.4 существует целое число $n \geq 1$ такое, что $a^nR \cap r(a) = (0)$. По лемме 3.6 a^nR – существенный правый идеал. Следовательно, $r(a) = l(a) = 0$ и a – регулярный элемент кольца R. □

Лемма 3.8. *Пусть R – полупервичное кольцо Голди. Тогда R удовлетворяет условию минимальности на правые аннуляторные идеалы.*

□ Пусть

$$I_1 \supset I_2 \supset I_3 \supset \dots$$

– строго убывающая цепочка правых аннуляторных идеалов кольца R. Тогда по лемме 3.2 можно считать, что $I_i = r(B_i)$, где $l(I_i) = B_i$, $i = 1, 2, \dots$. Из строгого включения $I_n \supset I_{n+1}$ следует, что $B_n \subset B_{n+1}$ и $B_n \neq B_{n+1}$, $n = 1, 2, \dots$. По лемме 3.5 существуют ненулевые правые идеалы $T_n \subseteq I_n$ такие, что $T_n \cap I_{n+1} = (0)$, $n = 1, 2, \dots$. Следовательно, сумма этих правых

идеалов $T_1 + T_2 + \ldots$ является прямой. Противоречие. Итак, исходная цепь правых аннуляторных идеалов должна стабилизироваться и R удовлетворяет условию минимальности на правые аннуляторные идеалы. $\square$

Лемма 3.9. *Пусть R – полупервичное правое кольцо Голди и $a \in R$ такой элемент, что $r(a) = 0$. Тогда правый идеал aR является существенным и a – регулярный элемент кольца R.*

$\square$ Пусть I – такой ненулевой правый идеал кольца R, что $I \cap aR = (0)$. Тогда сумма правых идеалов

$$aI + a^2I + a^3I + \ldots$$

является прямой. Противоречие. Итак, aR – существенный правый идеал кольца R. По лемме 3.7 a – регулярный элемент в кольце R. $\square$

Лемма 3.10. *Пусть R – полупервичное правое кольцо Голди. Тогда*

1. *Каждый ненулевой минимальный аннуляторный идеал R является первичным правым кольцом Голди.*

2. *В кольце R существует конечная прямая сумма ненулевых минимальных аннуляторных идеалов, являющаяся существенным правым идеалом.*

$\square$ Докажем утверждение 1. Пусть A – ненулевой минимальный аннуляторный идеал кольца R. Тогда A удовлетворяет условию максимальности на правые аннуляторные идеалы (так как R удовлетворяет этому условию). Если

$$I_1 + I_2 + \ldots$$

– бесконечная прямая сумма ненулевых правых идеалов кольца A, то

$$(I_1A) + (I_2A) + \ldots$$

– бесконечная прямая сумма правых идеалов кольца R. Действительно, $I_iA \subseteq A$ и $I_iA <_r R$, так как $A \lhd R$ и $I_i <_r A$, $i = 1, 2, \ldots$. Если $I_iA = (0)$, то $(I_i + I_iR)^2 \subseteq I_iA = (0)$ и $I_i + I_iR = (0)$, ввиду полупервичности кольца R. Противоречие доказывает, что кольцо A удовлетворяет условиям Голди.

Докажем первичность этого кольца. Если B, C – ненулевые идеалы A и $BC = (0)$, то $BA \subseteq B$ и $BAC = 0$. Откуда следует, что $C \subseteq r(BA) \cap A$. Так как A – аннуляторный идеал, то $r(BA) \cap A$ – тоже ненулевой аннуляторный идеал A, содержащийся в A. Ввиду минимальности идеала A имеем, что $A \subseteq r(BA)$ и $BA^2 = (0)$, $(BA)^2 \subseteq BA^2 = (0)$. Так как R – полупервичное кольцо, то $BA = (0)$ и $(BR)^2 \subseteq BR \cdot A = (0)$. Откуда следует, что $BR = (0)$ и $B = (0)$. Противоречие. Итак, A – первичное правое кольцо Голди.

Докажем утверждение 2. Из леммы 3.8 следует, что R содержит минимальные аннуляторные идеалы. Пусть

$$T = A_1 \oplus \cdots \oplus A_n$$

– максимальная прямая сумма ненулевых минимальных аннуляторных идеалов кольца R. Докажем, что T – существенный правый идеал кольца R. Допустим противное и I – такой ненулевой правый идеал R, то $T \cap I = (0)$. Тогда $IT \subseteq T \cap T = (0)$ и $I \subseteq l(T)$. Так как R – полупервичное кольцо, то $T \cap l(T) = (0)$ и, следовательно, $Tl(T) = (0)$. Откуда следует, что $l(T) \subseteq r(T)$ и $T \cap r(T) = (0)$. Ввиду условия минимальности на аннуляторные правые идеалы (см. лемму 3.8) в $r(T)$ существует ненулевой минимальный аннуляторный идеал A_{n+1} такой, что $\cap A_{n+1} = (0)$. Это противоречит тому, что $T = A_1 \oplus \cdots \oplus A_n$ – максимальная прямая сумма таких идеалов. $\square$

Лемма 3.11. *Если I – существенный правый идеал первичного кольца Голди R, то I содержит регулярный элемент кольца R.*

$\square$ По лемме 3.8 в I существует такой элемент a, что $r(a)$ является минимальным в множестве $\{r(x) |\, x \in I\}$. Докажем, что aR

– существенный правый идеал кольца R. Если K – ненулевой правый идеал кольца R такой, что $K \cap aR = (0)$, то $K \cap I \neq (0)$ и $R \cap (K \cap I) = (0)$. Поэтому будем считать, что $K \subseteq I$. Пусть $x \in K$ и $b \in r(a+x)$. Тогда $ab = -xb \in K \cap aR = (0)$. Следовательно, $r(a+x) = r(a) \cap r(x) \subseteq r(a)$. Ввиду минимальности правого идеала $r(a)$ имеем, что $r(a) \subseteq r(x)$ и $Kr(a) = (0)$. Так как $K <_r R$ и R – первичное кольцо, то $r(a) = (0)$. По лемме 3.9 aR – существенный правый идеал и a – регулярный элемент. □

Лемма 3.12. *Если R – полупервичное правое кольцо Голди и I – существенный правый идеал, то I содержит регулярный элемент.*

□ По лемме 3.10 в кольце R существует конечная прямая сумма ненулевых минимальных аннуляторных идеалов

$$T = A_1 \oplus \cdots \oplus A_n,$$

являющаяся существенным правым идеалом в R. Докажем, что для любого числа $i \leq n$ ненулевой правый идеал $I \cap A_i$ является существенным в первичном кольце A_i. Действительно, если в кольце A_i существует ненулевой правый идеал L такой, что $(I \cap A_i) \cap L = (0)$, то $I \cap (LA_i) = (0)$. Так как $LA_i <_r R$, то $LA_i = (0)$ и $L^2 = (0)$. A_i – первичное кольцо. Поэтому $L = (0)$. Противоречие. Итак, $I \cap A_i$ – существенный правый идеал и по предыдущей лемме он содержит элемент a_i, являющийся регулярным в кольце A_i. Докажем, что $a = a_1 + a_2 + \cdots + a_n$ – регулярный элемент в R. Пусть $r(a) \neq (0)$. Так как T – существенный правый идеал кольца R, то существует ненулевой элемент $x = x_1 + \cdots + x_n \in T \cap r(a)$, где $x_i \in A_i$, $i \leq n$. Откуда следует, что $ax = 0 = ax_1 + \cdots + ax_n = a_1x_1 + \cdots + a_nx_n$ и $a_ix_i = 0$, $i \leq n$. Так как a_i – регулярный элемент в A_i, $i \leq n$, то $x_i = 0$ и $x = 0$. Итак, $r(a) = (0)$. В силу леммы 3.9, a – регулярный элемент в R. □

Наконец, приведем доказательство выше сформулированной теоремы Голди.

□ Из последней леммы следует, что ненулевое полупервичное правое кольцо Голди R содержит регулярный элемент a. Пусть b – произвольный элемент R. Рассмотрим правый идеал

$$I = \{x \in R |\ bx \in aR\}.$$

Если K – ненулевой правый идеал кольца R, то либо $bK = (0)$ и $K \subseteq I$, либо $bK \neq (0)$ и тогда $bK \cap aR \neq (0)$ (ибо по лемме 3.9 aR – существенный правый идеал кольца R). В последнем случае $K \cap I \neq (0)$. Итак, I – существенный правый идеал R. По лемме 3.12 I содержит регулярный элемент c такой, что $bc = ax$ для некоторого элемента $x \in R$. Тем самым, мы доказали, что R удовлетворяет правому условию Ope, и, следовательно, по теореме Ope R имеет полное правое классическое кольцо частных Q.

Если I – правый идеал Q, то $I = (I \cap R)Q$. Заметим, что если $I_1 \oplus \cdots \oplus I_n$ – прямая сумма правых идеалов кольца R, то

$$I_1Q \oplus \cdots \oplus I_nQ$$

– прямая сумма правых идеалов кольца Q. Действительно, если имеет место равенство

$$i_1a_1b_1^{-1} + \cdots + i_na_nb_n^{-1} = 0,$$

где $i_kc_k \in I_k$, $a_k, b_k \in R$, $k \leq n$, то $a_kb_k^{-1} = c_kc^{-1}$, $k \leq n$ для некоторых элементов $c_k \in R$ и регулярного элемента $c \in R$. Следовательно, $i_1c_1 + i_2c_2 + \cdots + i_nc_n = 0$, где $i_kc_k \in I_k$, $k \leq n$. Так как сумма правых идеалов $I_1 \oplus \cdots \oplus I_n$ является прямой, то $i_kc_k = i_ka_kb_k^{-1} = 0$, $k \leq n$ и $I_1Q + \cdots + I_nQ$ – тоже прямая сумма.

Пусть I – ненулевой правый идеал кольца Q и $I_1 = I \cap R$. Тогда (ввиду условия Голди) существует конечное множество (возможно, пустое) правых идеалов $I_2, \ldots, I_n$ кольца R такое, что сумма

$$A = I_1 \oplus \cdots \oplus I_n$$

является прямой и A – существенный правый идеал кольца R. Пусть

$$B = I_2 \oplus \ldots \oplus I_n.$$

Тогда $A = I_1 \oplus B$ содержит регулярный элемент и

$$AQ = I \oplus BQ = Q.$$

Если e – единица Q, то $e = i + j$, где $j \in BQ$, $i \in I$. Из свойств прямой суммы следует, что $i^2 = i$, $j^2 = j$, $ij = ji = 0$ и $I = iQ$. Итак, каждый правый идеал кольца Q порождается идемпотентом. Откуда следует, что Q – полупервичное кольцо, удовлетворяющее условию максимальности на правые идеалы (в частности, являющиеся правым кольцом Голди), и его радикал Джекобсона $J(Q)$ равен нулю (ибо он не содержит ненулевых идемпотентов). Докажем, что Q – артиново справа кольцо. Из предыдущего мы знаем, что Q удовлетворяет условию минимальности для правых аннуляторных идеалов. Поэтому для доказательства артиновости кольца Q достаточно доказать, что произвольный ненулевой правый идеал $I <_r Q$ является правым аннулятором. Так как $I = fQ$, $f^2 = f$, то $l(I) = Q(1 - f)$ и $r(l(I)) = r(Q(1 - f)) = fQ = I$. Итак, Q – полупростое артиново кольцо. Если R – первичное кольцо и Q не является простым кольцом, то из теоремы Веддерберна-Артина следует существование ненулевых идеалов S, T кольца Q таких, что $ST = (0)$. Откуда следует, что $(S \cap R)(T \cap S) = (0)$ и $S \cap R \neq (0)$, $T \cap R \neq (0)$. Противоречие доказывает, что Q – простое артиново кольцо.$\square$

Пусть R – первичное правое кольцо Голди и $Q(R) = M_n(D)$ – правое кольцо частных R, где D – тело. В работе [76] доказано, что в кольце $Q(R)$ существует полная система матричных единиц $\{e_{ij}\}$, а в кольце R подкольцо $\triangle$ такие, что

$$M_n(\triangle) = \sum e_{ij}\triangle \subseteq R \subset Q(R) = \sum e_{ij}D' = M_n(D')$$

и D' – правое тело частных $\triangle$.

В работе [79] доказано, что если R – первичное кольцо главных правых идеалов, то $R = M_n(\triangle)$, где $\triangle$ – кольцо без делителей нуля, имеющее правое тело частных.

3.4. Теорема Смолла о существовании артиновых колец частных

Пусть A – правое кольцо Голди и $P(A) = \ln A$ – его нижний ниль-радикал. Кольцо A удовлетворяет условию *регулярности*, если из того, что элемент $c+P(A)$ является регулярным в $A/P(A)$ следует, что c – регулярный элемент в A. Если же $c+P(A)$ регулярен в $A/P(A)$ тогда и только тогда, когда c регулярен в A, то говорят, что A *удовлетворяет полному условию регулярности.*

Пусть A – правое кольцо Голди и

$$T_k = P(A) \cap \ell_R \left(P(A)^k \right),$$

где $k \geq 1$. Тогда A называется *правым T-кольцом Голди*, если для любого целого числа $k \geq 1$ A/T_k – правое кольцо Голди.

Справедлива следующая теорема, доказанная Л. Смоллом в работах [114, 115].

Теорема 3.4. *Следующие условия на кольце R эквивалентны:*

1. *R – правый порядок в право артиновом кольце.*
2. *R – ненильпотентное правое T-кольцо Голди, удовлетворяющее условию регулярности.*
3. *R – ненильпотентное правое T-кольцо Голди, удовлетворяющее полному условию регулярности.*

Введем сначала некоторые обозначения, удобные в дальнейшем и докажем ряд предварительных утверждений. Пусть R – ненильпотентное правое кольцо Голди, удовлетворяющее

условию регулярности. Пусть также $R/P(A)$ – правое кольцо Голди и

$$M = \{c \in R |\ c + P(R) \text{ – регулярный элемент в } R/P(R)\}.$$

По теореме Голди $R/P(R)$ содержит регулярные элементы. Поэтому M – полугруппа, состоящая из регулярных элементов R. Пусть

$$T_k = P(R) \cap \ell_R\left(P(R)^k\right) \quad \text{и} \quad R_k = R/T_k,$$

где $k \geq 1$. Будем обозначать элемент $x + T_k$ через x_k $(x \in R)$.

Лемма 3.13. *Для любых натуральных чисел n, k справедливо равенство*

$$T_{k+n}/T_n = P(R_k) \cap \ell_{R_k}\left(P(R_k)^n\right).$$

□ В силу определения идеала T_k имеем, что $T_k \subseteq P(R)$ и $P(R_k) = P(R)/T_k$. Пусть

$$x_k \in P(R_k) \cap \ell_{R_k}\left(P(R_k)^n\right).$$

Тогда $x \in P(R)$ и $x_k P(R_k)^n = \bar{0}$. Это означает, что

$$xP(R)^n \subseteq T_k \subseteq \ell_R\left(P(R)^k\right), \quad xP(R)^{n+k} = 0$$

и $x \in T_{k+n}$, $x_k \in T_{k+n}/T_k$.

Если $y_k \in T_{n+k}/T_k$, то, учитывая включение $T_k \subseteq T_{k+n}$, имеем, что $y \in T_{n+k}$. Поэтому $y \in P(R)$ и $yP(R)^{n+k} = 0$. Откуда следует, что

$$yP(R)^n \subseteq P(R) \cap \ell_R\left(P(R)^k\right) = T_k.$$

Таким образом,

$$y_k \in \ell_{R_k}\left(P(R_k)^n\right) \cap P(R_k).$$

□

Лемма 3.14. *Пусть $a \in M$. Тогда для любого натурального числа k справедливо равенство $r_{R_k}(a_k) = \bar{0}$.*

□ Пусть $x_k \in r_{R_k}(a_k)$. Тогда $a_k x_k = \bar{0}$ и $ax \in T_k$. Это означает, что $ax \in P(R)$ и $(ax)P(R)^k = 0$. Так как $a + P(R)$ – регулярный элемент в $R/P(R)$, то $x \in P(R)$. Далее ввиду условия регулярности a – регулярный элемент в R. Поэтому $xP(R)^k = 0$, $x \in P(R) \cap \ell_R\left(P(R)^k\right) = T_k$ и $x_k = \bar{0}$. □

Лемма 3.15. *Предположим, что R удовлетворяет правому условию Оре относительно полугруппы регулярных элементов M, и пусть Q – правое кольцо частных (относительно полугруппы M). Тогда*

1. *$P(Q)$ – нильпотентный идеал Q и $P(Q) \cap R = P(R)$.*
2. *$P(Q)^n = (P(R)^n)\,Q = (P(Q) \cap R)^n\,Q$, где $n \geq 1$.*
3. *$T_k Q \cap R = T_k$, где $k \geq 1$.*
4. *$T_k Q \lhd Q$ и $Q/T_k Q$ – правое кольцо частных R_k относительно полугруппы $M_k = \{c + T_k |\ c \in M\}$.*

□ Докажем, что правый идеал $P(R)Q$ является нильпотентным. Из предложения 3.3 следует, что каждый элемент $P(R)Q$ имеет вид ra^{-1}, где $r \in P(R)$ и $a \in M$. Для любых элементов $b \in M$ и $y \in P(R)$ произведение $b^{-1}y = zc^{-1}$, где $z \in R$ и $c \in M$. Откуда следует, что $bz = yc \in P(R)$. Так как $b + P(R)$ – регулярный элемент в $R/P(R)$, то $z \in P(R)$. По теореме Шока (см. главу 2) $P(R)$ – нильпотентный идеал кольца R, то есть $P(S)^m = (0)$ для некоторого целого числа $m \geq 1$. Покажем, что $(P(R)Q)^m = (0)$. Для этого достаточно проверить, что

$$r_1 a_1^{-1} r_2 a_2^{-1} \dots r_m a_m^{-1} = 0,$$

где $r_i \in P(R)$ и $a_i \in M$, $i \leq m$. Выше мы заметили, что произведение $a_1^{-1} r_2$ представимо в виде $z_1 c_2^{-1}$, где $z_1 \in P(R)$, $c_2 \in M$. Аналогично произведение $c_2^{-1} a_2^{-1} r_3 = (a_2 c_2)^{-1} r_3$ в виде $z_2 c_3^{-1}$,

где $z_2 \in P(R)$ и $c_3 \in M$ и так далее. Таким образом, существуют такие элементы $z_1, z_2, \ldots, z_{m-1}$ из $P(R)$, что

$$r_1 a_1^{-1} r_2 a_2^{-1} \ldots r_m a_m^{-1} = (r_1 z_1 z_2 \ldots z_{m-1})\, c^{-1} = 0,$$

где $c \in M$. Итак, $P(R)Q$ – нильпотентный правый идеал кольца Q.

$P(Q) \cap R$ – ниль-идеал кольца R. По теореме Шока (см. главу 2) $P(Q) \cap R$ – нильпотентный идеал, содержащийся в $P(R)$. Таким образом, справедливы включения

$$(P(Q) \cap R)\, Q \subseteq P(R)Q \subseteq P(Q).$$

Если $ac^{-1} \in P(Q)$, то $a \in P(Q) \cap R$ и $P(Q) \subseteq (P(Q) \cap R)\, Q$, то есть

$$P(Q) = P(R)Q = (P(Q) \cap R)\, Q$$

– нильпотентный индекса m идеал Q. Так как

$$P(Q) = P(R)Q = QP(R)Q = Q\,(P(Q) \cap R)\, Q,$$

то

$$P(Q)^2 = P(R)QP(R)Q = P(R)(P(R)Q) = P^2(R)Q.$$

Аналогично доказывается, что

$$P(Q)^n = (P(R)^n)\, Q = (P(Q) \cap R)^n\, Q$$

для любого числа $n \geq 1$.

Докажем утверждение 3 нашей леммы. Пусть $x \in T_k Q \cap R$ и $x = rc^{-1}$, где $c \in M$ и $r \in T_k$. Так как $T_k \subseteq P(R)$, то

$$T_k Q \cap R \subseteq P(R)Q \cap R \subseteq P(Q) \cap R \subseteq P(R)$$

и $x \in P(R)$. Далее, $xc = r \in T_k \subseteq \ell_R\left(P(R)^k\right)$. Поэтому

$$x \cdot P(Q)^k = rc^{-1} QP(R)^k Q = rQP(R)^k Q = rP(R)^k Q = (0)$$

(см. утверждение 2 данной леммы). Так как $P(R) \subseteq P(Q)$, то $x \cdot P(R)^k = (0)$, $x \in T_k$ и $T_kQ \cap R \subseteq T_k$.

Докажем утверждение 4. Пусть $r_1a^{-1} \in T_kQ$ и $r_2b^{-1} \in Q$, где $a, b \in M$, $r_1 \in T_k$ и $r_2 \in R$. Докажем, что

$$\left(r_2b^{-1}\right)\left(r_1a^{-1}\right) \in T_kQ.$$

Так как R удовлетворяет правому условию Оре относительно M, то $r_1u = bv$ для некоторых элементов $u \in M$ и $v \in R$. Откуда следует, что

$$(bv)P\left(R\right)^k = r_1uP(R)^k \subseteq r_1P(R)^k = (0).$$

Так как b – регулярный элемент в R, то $vP\left(R\right)^k = (0)$ и

$$v \in \ell_R\left(P\left(R\right)^k\right).$$

Далее $bv = r_1u \in T_k \subseteq P(R)$ и

$$v \in (QP(R)Q) \cap R = P(R)Q \cap R \subseteq P(R).$$

Следовательно, $v \in T_k$ и

$$r_2b^{-1}r_1a^{-1} = r_2\left(vu^{-1}\right)a^{-1} = \left(r_2v\right)\left(au\right)^{-1},$$

где $(r_2v) \in T_k$. Это доказывает, что T_kQ – идеал в Q. Покажем, что кольцо $R_k = R/T_k$ удовлетворяет правому условию Оре относительно

$$M_k = \left\{c + T_k \middle|\ c \in M\right\}.$$

По определению M_k – полугруппа. Пусть $a_k \in M_k$, $r_k \in R_k$ такие элементы, что $r_ka_k = \bar{0}$. Тогда $ra \in T_k = T_kQ \cap R$ и $r \in T_k$. Поэтому $r_k = \bar{0}$. По лемме 3.9 a_k – регулярный элемент в R_k. Таким образом, M_k – полугруппа регулярных элементов в R_k. Пусть $s_k \in R_k$ и $c_k \in M_k$. Так как R удовлетворяет правому условию Оре относительно M, то $sc' = cs'$ для некоторых элементов $c' \in M$, $s' \in R$. Следовательно, $c'_ks_k = c_ks'_k$ и R_k удовлетворяет правому условию Оре относительно M_k. По теореме Оре R_k имеет правое кольцо частных. Отображение

$$\left(ra^{-1} + T_kQ\right) \to (r + T_k)(a + T_k)^{-1},$$

где $a \in M$, $r \in R$ является изоморфизмом кольца Q/T_kQ и правого кольца частных кольца R_k относительно полугруппы регулярных элементов M_k. $\square$

Импликация $1 \to 3$ теоремы Смолла справедлива в силу ниже следующей леммы.

Лемма 3.16. *Пусть R – правый порядок в правом артиновом кольце Q. Тогда R – ненильпотентное правое T-кольцо Голди, удовлетворяющее полному условию регулярности. Кроме этого,*

$$P(R) = P(Q) \cap R, \quad P(Q) = P(R)Q$$

и $Q/P(Q)$ – полное правое кольцо частных $R/P(R)$.

$\square$ Кольцо R не является нильпотентным кольцом, так как по условию содержит регулярные элементы. Пусть

$$I_1 \oplus I_2 \oplus \dots$$

– бесконечная прямая сумма ненулевых правых идеалов кольца R. Тогда из предложения 3.3 следует, что

$$(I_1Q) \oplus (I_2Q) \oplus \dots$$

– бесконечная прямая сумма правых идеалов в правом артиновом кольце Q. Противоречие. Правое артиново кольцо Q содержит единицу и, следовательно, является правым нетеровым кольцом (см. [14]).

Так как Q удовлетворяет условию максимальности для правых аннуляторных идеалов, то его подкольцо R тоже удовлетворяет условию обрыва убывающих цепей правых аннуляторных идеалов. Это доказывает, что R – правое кольцо Голди.

Докажем, что $P(R) = P(Q) \cap R$. По теореме Шока (см. главу 2) идеалы $P(R)$ и $P(Q)$ являются нильпотентными. Поэтому $P(Q) \cap R \subseteq P(R)$. Рассмотрим полупростое артиново кольцо $\bar{Q} = Q/P(Q)$. Пусть

$$R' = \{r + P(Q) |\ r \in R\}$$

и $\bar{x}$ – произвольный элемент из $\bar{Q}$. Тогда $\bar{x} = r' \cdot (c')^{-1}$, где $r', c' \in R'$. Это означает, что $\bar{Q}$ – полное правое кольцо частных кольца R'. По теореме Голди R' – полупервичное кольцо, изоморфное $R/R \cap P(Q)$. Следовательно, $P(R) \subseteq R \cap P(Q)$, $R/P(R) \cong R'$ и $Q/P(Q)$ – правое кольцо частных $R/P(R)$.

По теореме Голди $R/P(R)$ – полупервичное правое кольцо Голди. Докажем, что R удовлетворяет полному условию регулярности. Если a – регулярный элемент в R, то a – обратимый элемент в Q и $a + P(Q)$ – обратимый элемент в $Q/P(Q)$. Откуда следует, что $\bar{a}$ – регулярный элемент в R', а значит и в $R/P(R)$. Пусть $b+P(R)$ – регулярный элемент в $R/P(R)$. Тогда $b + P(R)$ – регулярный элемент в R'. Следовательно, $b + P(Q)$ – обратимый элемент в $Q/P(Q)$ и так как $P(Q)$ – нильпотентный идеал, то b – обратимый элемент в Q. В частности, b – регулярный элемент в R. Полугруппа

$$M = \{a \in R |\ a + P(R) \text{ – регулярный элемент в } R/P(R)\}$$

совпадает с множеством всех регулярных элементов R. Так как Q – полное правое кольцо частных R, то Q удовлетворяет правому условию Ope относительно M и Q – полное правое кольцо частных относительно M. Далее, по лемме 3.15 Q/T_kQ – правое кольцо частных кольца R_k относительно полугруппы M_k, $k \geq 1$. Кольцо Q/T_kQ является правым артиновым кольцом. Как отмечалось выше, в этом случае R_k – правое кольцо Голди ($k \geq 1$). Из леммы 3.15 следует, что $P(Q) = P(R)Q$. $\square$

Импликация $3 \to 2$ теоремы Смолла очевидна. Докажем импликацию $2 \to 1$.

Будем предполагать в трех нижеследующих леммах, что R – ненильпотентное правое T-кольцо Голди, удовлетворяющее условию регулярности,

$$M = \{c \in R |\ c + P(R) \text{ – регулярный элемент в } R/P(R)\}\,,$$

$$T_k = P(R) \cap \ell_R\left(P(R)^k\right)$$

и

$$R_k = R/T_k,$$

где $k \geq 1$.

Лемма 3.17. *Пусть $a \in M$ и $x \in T_k$, $k \geq 1$. Тогда существуют элементы $y \in R$ и $b \in M$ такие, что $xb = ay$.*

□ Доказательство проведем методом математической индукции по числу $k \geq 1$. Так как $r_R(a) = 0$, то aR – существенный правый идеал в R. Действительно, если I – ненулевой правый идеал R, то $\sum\limits_{n\geq 1} a^n I$ не является прямой. Поэтому существует такое число $n \geq 1$, что

$$a^n i_1 + a^{n+1} i_2 + \ldots + a^{n+k} i_{k+1} = 0,$$

где $i_1, i_2, \ldots, i_{k+1} \in I$ и $i_1 \neq 0$. Так как $r_R(a) = 0$, то

$$i_1 = -ai_2 - \ldots - a^k i_{k+1} \in I \cap aR.$$

Докажем утверждение леммы при $k = 1$. Пусть

$$J = \{r \in R |\ xr \in aR\} \leq_r R.$$

Пусть I – произвольный ненулевой правый идеал кольца R. Если $xI = (0)$, то $I \subseteq J$. Если же $xI \neq (0)$, то $xI \cap aR \neq (0)$ (так как aR – существенный правый идеал R) и существуют элементы $i \in I$, $r \in R$ такие, что $xi = ar \neq 0$. В частности, $i \in J$ и $J \cap I \neq (0)$. Если при этом $i \in P(R)$, то, учитывая включение $x \in T_1 = P(R) \cap \ell_R(P(R))$, получим $xi = 0$. Противоречие. Таким образом, $J \cap I \not\subseteq P(R)$ и $P(R) \subseteq J$. Откуда следует, что J – правый идеал, строго содержащий $P(R)$ и имеющий ненулевое пересечение с каждым ненильпотентным правым идеалом. Это означает, что $J/P(R)$ – существенный правый идеал $R/P(R)$. По лемме 3.12 $J/P(R)$ содержит регулярный элемент $c + P(R)$. Так как $P(R) \subset J$ и R удовлетворяет условию регулярности, то $c \in M \cap J$. Таким образом, существует элемент $y \in R$ такой, что $xc = ay$. Итак, лемма доказана при $k = 1$.

Предположим, что утверждение леммы справедливо при $k = n$. Докажем его при $k = n + 1$. Пусть $x \in T_{n+1}$ и $a \in M$. Тогда по лемме 3.14 $r_{R_n}(a_n) = \bar{0}$. Рассмотрим множество

$$K = \{r_n \in R_n |\ x_n r_n \in a_n R_n\}$$

и заметим, что

$$T_{n+1}/T_n = P(R_n) \cap \ell_{R_n}\left(P\left(R_n\right)\right).$$

Учитывая, что $P(R_n) = P(R)/T_n$ и $R_n/P(R_n) \cong R/P(R)$, а также, повторяя рассуждения при $k = 1$, получим, что $a_n y_n = x_n b_n$ для некоторых элементов $b \in M$, $b_k \in K$. Откуда следует, что $xb - ay \in T_n$. По предположению индукции существуют элементы $c \in M$ и $z \in R$ такие, что $az = (xb - ay)c$ или $a(z + yc) = x(bc)$, где $bc \in M$. $\square$

Лемма 3.18. *Кольцо R удовлетворяет правому условию Оре относительно M.*

$\square$ Пусть $x \in R$ и $a \in M$. Докажем, что существуют элементы $u \in R$, $v \in M$ такие, что $au = xv$. Если $x \in P(R)$ и $P(R)^n = (0)$, то при $n = 1$ $x = 0$ и $a \cdot 0 = 0 \cdot a$. Если $n \geq 2$, то x принадлежит $T_{n-1} = P(R) \cap \ell_R\left(P(R)^{n-1}\right)$ и по лемме 3.17 существуют элементы $u \in R$, $v \in M$ такие, что $au = xv$. Если $x \notin P(R)$, то в полупервичном правом кольце Голди $R/P(R)$ существуют элементы $\bar{b}$, $\bar{y}$ такие, что $\bar{x}\bar{b} = \bar{a}\bar{y}$, где $b \in M$, $y \in R$. Откуда следует, что $xb - ay \in P(R)$. Согласно выше приведенному рассуждению, существуют элементы $u \in R$, $v \in M$ такие, что $(xb - ay)v = au$ или $a(u + yv) = x(bv)$, где $(bv) \in M$. $\square$

Из леммы 3.18 и теоремы Оре следует, что существует правое кольцо частных кольца R относительно полугруппы регулярных элементов M. Обозначим его через Q.

Лемма 3.19. *Q – полное правое кольцо частных кольца R, являющееся правым артиновым кольцом.*

□ Пусть n – индекс нильпотентности $P(R)$, то есть $P(R)^n = (0)$ и $P(R)^{n-1} \neq (0)$. Тогда $T_{n-1} = P(R)$. В силу леммы 3.15 имеем $Q/P(Q) \cong Q_{n-1}$ – кольцо частных R_{n-1} относительно полугруппы M_{n-1}, совпадающей с полугруппой всех регулярных элементов полупервичного правого кольца Голди R_{n-1}. По теореме Голди Q_{n-1} – полупростое артиново кольцо. Итак, $Q/P(Q)$ – полупростое артиново кольцо. Так как $Q/T_kQ \cong Q_k$, то Q/T_kQ не имеет бесконечных прямых сумм ненулевых правых идеалов. Откуда следует, что правый Q-модуль $T_{k+1}Q/T_kQ$ не имеет бесконечных прямых сумм Q-подмодулей. По лемме 3.15, учитывая включение $T_{k+1}P(R) \subseteq T_k$, имеем, что

$$T_{k+1}P(R)Q \subseteq T_{k+1}P(Q) \subseteq T_kQ.$$

Откуда следует, что $T_{k+1}Q/T_kQ$ – правый $Q/P(Q)$-модуль, не имеющий бесконечных прямых сумм подмодулей. Так как этот $Q/P(Q)$-модуль является вполне приводимым, то он имеет конечный композиционный ряд из правых Q-модулей. Этот композиционный ряд индуцирует конечный композиционный ряд из правых идеалов кольца Q. По теореме Жордана-Гельдера Q – правое артиново кольцо. Докажем, наконец, что Q – полное правое кольцо частных R. Для этого, учитывая лемму 3.18, достаточно показать, что каждый регулярный элемент $c \in R$ является обратимым в Q. Каждый элемент $c_1 \in Q$ можно представить в виде $c_1 = ra^{-1}$, где $a \in M$, $r \in R$. Если $cc_1 = 0$, то $cra^{-1} = 0$, $cr = 0$ и $r = 0$. Поэтому $r_Q(c) = 0$. Покажем, что $\ell_Q(c) = 0$. Для этого рассмотрим убывающую цепь правых идеалов

$$cQ \supseteq c^2Q \supseteq c^3Q \supseteq \dots.$$

Так как Q – правое артиново кольцо, то существует целое число $n \geq 1$ такое, что $c^nQ = c^{n+1}Q$. Поэтому $c^n = c^{n+1}q$ для некоторого элемента $q \in Q$. Откуда следует, что $cq = 1$ и $c(qc-1) = 0$. Так как $r_Q(c) = 0$, то $qc = 1$ и c – обратимый элемент в Q. □

3.5. Тождества колец частных

Пусть R – алгебра над коммутативным кольцом Φ с единицей и $\langle S, \cdot \rangle$ – подполугруппа центра кольца R (относительно операции умножения). Рассмотрим множество $S \times R$ и определим на нем бинарное отношение:

$$(s_1, x_1) \sim (s_2, x_2),$$

если существует элемент $s \in S$ такой, что

$$s(s_2 x_1 - s_1 x_2) = 0.$$

Проверим, что это бинарное отношение является отношением эквивалентности. Для этого достаточно проверить транзитивность. Пусть

$$(s_1 x_1) \sim (s_2 x_2) \text{ и } (s_2 x_2) \sim (s_3 x_3).$$

Тогда существуют такие элементы $s, s' \in S$, что

$$s(s_2 x_1 - s_1 x_2) = 0 \text{ и } s'(s_2 x_3 - s_3 x_2) = 0.$$

Следовательно,

$$(s' s s_2)(s_3 x_1) = s' s_3 (s s_2 x_1) = s' s_3 (s s_1 x_2) = \\ = s s_1 (s' s_3 x_2) = s s_1 (s' s_2 x_3) = (s' s s_2)(s_1 x_3)$$

и $(s' s s_2)(s_3 x_1 - s_1 x_3) = 0$, где $s' s s_2 \in S$. Таким образом,

$$(s_1, x_1) \sim (s_3, x_3).$$

Класс эквивалентных пар, содержащий (s, x), обозначим через

$$\overline{(s, x)} = s^{-1} x,$$

а множество всех классов через

$$R_s = S^{-1} R.$$

Определим на этом множестве $S^{-1}R$ операции сложения и умножения по правилам

$$s_1^{-1}x_1 + s_2^{-1}x_2 = (s_1s_2)^{-1}(s_2x_1 + s_1x_2),$$

$$(s_1^{-1}x_1)(s_2^{-1}x_2) = (s_1s_2)^{-1}(x_1x_2).$$

Легко проверить корректность этих операций. Множество

$$\langle S^{-1}R, +, \cdot \rangle$$

является ассоциативным кольцом, и если S состоит из регулярных элементов, то отображение $a \to s^{-1}(sa)$ кольца R в $S^{-1}R$ является вложением колец. Кольцо $S^{-1}R$ называется *кольцом частных кольца R относительно полугруппы S.*

Пусть $\Phi\langle x_1, x_2, \ldots\rangle$ – свободная ассоциативная Φ-алгебра и $f(x_1, \ldots, x_d)$ – ненулевой многочлен из $\Phi\langle x_1, \ldots, x_n, \ldots\rangle$. Многочлен $f(x_1, \ldots, x_d)$ называется *тождеством Φ-алгебры R*, если для любых элементов $a_1, \ldots, a_d \in R$ $f(a_1, \ldots, a_d) = 0$.

Теорема 3.5 (Л. Роуэн).
Пусть R – алгебра над коммутативным кольцом Φ с единицей, удовлетворяющая тождеству $f(x_1, \ldots, x_d) = 0$. Пусть $\langle S, \cdot\rangle$ – подполугруппа центра кольца R. Тогда $S^{-1}R$ удовлетворяет тождеству $f(x_1, \ldots, x_d) = 0$.

□ Пусть $s_1^{-1}b_1, \ldots, s_d^{-1}b_d$ – произвольные элементы из $S^{-1}R$. Их можно представить в виде

$$s_1^{-1}b_1 = s^{-1}a_1,\ s_2^{-1}b_2 = s^{-1}a_2,\ \ldots,\ s_d^{-1}b_d = s^{-1}a_d.$$

Докажем, что

$$f(s^{-1}a_1, \ldots, s^{-1}a_d) = 0.$$

Многочлен $f(x_1, \ldots, x_d)$ является суммой однородных слагаемых, то есть

$$f = \sum_{j=1}^{m} f_j,$$

где f_j – сумма одночленов степени j. Пусть $u_i = f_i(a_1, \ldots, a_d)$. Тогда из равенств

$$f(a_1, \ldots, a_d) = \sum_{i=1}^{m} u_i = 0,$$

$$f(sa_1, \ldots, sa_d) = \sum_{i=1}^{m} s^i u_i = 0,$$

$$f(s^2 a_1, \ldots, s^2 a_d) = \sum_{i=1}^{m} s^{2i} u_i = 0,$$

$$\ldots$$

$$f(s^{m-1} a_1, \ldots, s^{m-1} a_d) = \sum_{i=1}^{m} s^{(m-1)i} u_i = 0$$

следует матричное равенство

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ s & s^2 & \ldots & s^m \\ s^2 & s^4 & \ldots & s^{2m} \\ \vdots & \vdots & \ddots & \vdots \\ s^{m-1} & s^{2(m-1)} & \ldots & s^{(m-1)m} \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} = 0$$

Определитель выше приведенной матрицы равен $s^k - s^{k+1}h(s)$, где $h(t) \in \mathbb{Z}[t]$. Умножая (слева) левую и правую части матричного равенства на присоединенную матрицу, получим, что

$$(s^k - s^{k+1}h(s))u_i = 0,$$

где $1 \leq i \leq m$. Откуда следует, что

$$s^{-1}u_j = h(s)u_j \quad \text{и} \quad s^{-j}u_j = h^j(s)u_j.$$

Следовательно,

$$f\left(s^{-1}a_1, s^{-1}a_2, \ldots, s^{-1}a_d\right) = \sum_{j=1}^{m} s^{-j}u_j =$$

$$= \sum_{j=1}^{m} f_j(h(s)a_1, \ldots, h(s)a_d) = f(h(s)a_1, \ldots, h(s)a_d) = 0. \quad \square$$

Обозначим через $T(R)$ множество всех тождеств алгебры R. Из теоремы следует, что $T(R) \subseteq T(S^{-1}R)$ и если S состоит из регулярных элементов кольца R, то $T(R) = T(S^{-1}R)$.

3.6. Упражнения

Упражнение 3.1. *Пусть A – коммутативное кольцо с единицей и M – нетеровый A-модуль. Докажите, что $A/\operatorname{Ann} M$ – нетерово кольцо.*

$\diamondsuit$ Пусть $\bar{A} = A/\operatorname{Ann} M$. Тогда M – точный конечнопорожденный $\bar{A}$-модуль. Пусть

$$M = \bar{A}m_1 + \ldots + \bar{A}m_n.$$

Отображение $\bar{A}$-модулей

$$\varphi : \bar{A} \to \underbrace{M \oplus \ldots \oplus M}_{n}$$

такое, что

$$\varphi(\bar{a}) = (\bar{a}m_1, \ldots, \bar{a}m_n)$$

является вложением $\bar{A}$-модулей. Следовательно, $\bar{A}$ – нетеровый $\bar{A}$-модуль. $\diamondsuit$

Упражнение 3.2. *Пусть A – коммутативное кольцо с единицей и $I_1, \ldots, I_n$ – такие идеалы A, что $\bigcap\limits_{i=1}^{n} I_i = (0)$ и A/I_i – нетерово кольцо, $i \leq n$. Докажите, что A – нетерово кольцо.*

$\diamondsuit$ Отображение $\varphi(a) = (a + I_1, \ldots, a + I_n)$ является вложением A-модуля A в нетеровый A-модуль $A/I_1 \oplus \ldots \oplus A/I_n$. $\diamondsuit$

Упражнение 3.3. *Пусть A – коммутативное локальное кольцо с единицей, максимальный идеал M которого – однопорожденный идеал, то есть $M = (a) = aA$. Докажите, что если $\bigcap\limits_{n=1}^{\infty} M^n = (0)$, то A – нетерово кольцо и если $I \lhd A$, $I \neq (0)$, то $I = M^n$ для некоторого числа $n \geq 1$.*

$\diamondsuit$ Пусть I – ненулевой идеал A. Тогда существует целое число $n \geq 1$ такое, что $I \subseteq M^n$ и $I \not\subset M^{n+1}$. Следовательно, найдется такой элемент $x \in I$, что $x = a^n y$, где $y \notin M$. Так как A/M – поле, то существует элемент $z \in A$ такой, что $\bar{y}\bar{z} = \bar{1}$ или $yz = 1 + m$, где $m \in M$. Идеал M совпадает с радикалом Джекобсона $J(A)$. Поэтому существует $(1+m)^{-1}$ в A. Следовательно, y – обратимый элемент в A и $a^n = xy^{-1} \in I$, то есть $I = M^n = (a^n)A$ – однопорожденный идеал A. $\diamondsuit$

Упражнение 3.4. *Пусть R – коммутативное кольцо с единицей, в котором каждый простой идеал является конечнопорожденным. Докажите, что R – нетерово кольцо.*

$\diamondsuit$ Предположим противное. Тогда множество двухсторонних идеалов

$$\mathfrak{M} = \{I \lhd R |\ I\text{– не является конечнопорожденным идеалом } R\}$$

является непустым. По лемме Цорна $\mathfrak{M}$ содержит максимальный двусторонний идеал $I_\circ \in \mathfrak{M}$. Так как $I_\circ$ – не конечнопорожден (как идеал), то он не является простым и найдутся элементы $x, y \notin I_\circ$ такие, что $xy \in I_\circ$. Рассмотрим идеал $I_\circ + Ry$. Так как $I_\circ + Ry \supsetneqq I_\circ$, то $I_\circ + Ry \notin \mathfrak{M}$ и

$$I_\circ + Ry = Ru_1 + \ldots + Ru_n + Ry,$$

где $u_i \in I_\circ$, $i \leq n$. Пусть

$$(I_\circ : y) = \{a \in R |\ ay \in I_\circ\} \lhd R.$$

Тогда $(I_\circ : y)$ содержит x, $I_\circ$ и, следовательно, $(I_\circ : y) \notin \mathfrak{M}$. Поэтому

$$(I_\circ : y) = R \cdot v_1 + \ldots + Rv_m$$

для некоторых элементов $v_i \in R$, $i \leq m$. Легко видеть, что

$$I_\circ = Ru_1 + \ldots + Ru_n + R(v_1 y) + \ldots + R(v_m y)$$

– конечнопорожденный идеал. Противоречие. $\diamondsuit$

Упражнение 3.5. *Пусть R – коммутативная область целостности, являющаяся кольцом главных идеалов и $\langle S, \cdot\rangle$ – подполугруппа $\langle R, \cdot\rangle$, не содержащая нуль. Докажите, что кольцо частных $S^{-1}R$ – область главных идеалов.*

Упражнение 3.6. *Пусть R – коммутативное нетерова область целостности с единицей и M – ненулевой максимальный идеал R. Докажите, что $M \neq M^2$.*

$\diamondsuit$ Так как

$$M = a_1R + \ldots + a_nR,$$

то, предположив, что $M = M^2$, получим, что

$$M = a_1M + \ldots + a_nM$$

и $a_i = \sum\limits_{j=1}^{n} m_{ij}a_j$, где $m_{ij} \in M$, $i \leq n$. Следовательно,

$$((m_{ij}) - E)\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = 0$$

Обозначим через $((m_{ij}) - E)^*$ – присоединенную матрицу к матрице $((m_{ij}) - E)$ и $d = 1 + m = |((m_{ij}) - E)|$ – определитель $|(m_{ij}) - E|$, где $m \in M$. Тогда

$$((m_{ij}) - E)^*((m_{ij}) - E)\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & d \end{pmatrix}\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0$$

и $da_1 = \ldots = da_n = 0$. Так как R – область целостности и $M \neq (0)$, $M \neq R$, то получаем противоречие. $\diamondsuit$

Упражнение 3.7. *Пусть F – поле, содержащее подполе K и*

$$R = \begin{pmatrix} F & F \\ 0 & K \end{pmatrix}.$$

Докажите, что:

1. *Если V – K-подпространство F, то*

$$\begin{pmatrix} 0 & V \\ 0 & 0 \end{pmatrix} \leq_r R.$$

В частности, если $[F : K] = \infty$, то R не является ни правым артиновым кольцом, ни правым нетеровым кольцом.

2. *Единственными левыми идеалами в R являются:*

$$R, \quad (0), \quad \begin{pmatrix} F & F \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & F \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & F \\ 0 & K \end{pmatrix},$$

$$\left\{ \begin{pmatrix} \alpha & \alpha\beta \\ 0 & 0 \end{pmatrix} \middle| \, \alpha, \beta \in F, \ \beta \text{ – фиксированный элемент} \right\}.$$

В частности, R – левое артиново кольцо и левое нетерово кольцо.

Упражнение 3.8. *Пусть R – кольцо с единицей, удовлетворяющее условию обрыва убывающих цепей вида*

$$Rx \supseteq Rx^2 \supseteq Rx^3 \supseteq \dots.$$

Пусть $a \in R$ такой, что

$$l_R(a) = \{x \in R | \ xa = 0\} = (0).$$

Докажите, что a – обратимый элемент в R.

Упражнение 3.9. *Пусть R – полупервичное кольцо и $I <_r R$. Докажите, что*

1. *Если* $l_I(I) = \{x \in I | \, xI = (0)\} = (0)$, *то* I– *тоже полупервичное кольцо.*

2. $Z(I) = Z(R) \cap I$, *где* $Z(A)$ – *центр кольца* A.

Упражнение 3.10. *Пусть* D – *тело и* a, b – *такие элементы* D, *что* $a \neq 0$, $b \neq 0$, $ab \neq 1$ *и* $a^{-1} + \left(b^{-1} - a\right)^{-1} \neq 0$. *Докажите равенство*

$$\left(a^{-1} + \left(b^{-1} - a\right)^{-1}\right)^{-1} = a - aba$$

Упражнение 3.11. *Докажите, что*

1. $\mathbb{Z}$ – *нетерово кольцо, не являющееся артиновым.*

2. *Пусть* R – *кольцо с нулевым умножением, аддитивная группа которого – квазициклическая группа типа* p^∞. *Докажите, что* R – *артиново кольцо, не являющееся нетеровым.*

3. $\begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$ – *правое нетерово кольцо, не являющееся левым нетеровым кольцом.*

4. $\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$ – *правое артиново кольцо, не являющееся левым артиновым кольцом.*

Упражнение 3.12. *Пусть* A – *коммутативное кольцо с единицей и* I – *конечнопорожденный идеал* A *такой, что* $I = I^2$. *Докажите, что* I *порождается (как идеал) идемпотентом.*

$\diamondsuit$ По условию

$$I = a_1 A + \ldots + a_n A = I^2 = a_n I + \ldots + a_n I.$$

Следовательно, существуют такие элементы $x_{ij} \in I$, $1 \leq i, j \leq n$, что $a_i = \sum\limits_{j=1}^{n} a_j x_{ij}$. Пусть $X = (x_{ij}) \in M_n(A)$, E – единичная

матрица. Тогда

$$(X-E)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0.$$

Умножая слева на присоединенную матрицу $(X-E)^*$, получим, что $da_i = 0$, $i \leq n$, где $d = |X-E| = 1+u$ – определитель матрицы $(X-E)$, $u \in I$. Следовательно, $a_i = -ua_i$, $i \leq n$ и $I = uA$ – однопорожденный идеал A. Так как $I = uA = I^2 = u^2A$, то $u = u^2v$ для некоторого элемента $v \in A$. Пусть $e = uv \in I$. Тогда $I = eA$, $u = ue = ue^2$, $u(e-e^2) = 0$, $I(e-e^2) = (0)$. В частности, $e(e-e^2) = 0$ и $f = e^2 = f^2 \in I$. Из включений $fA \subseteq I \subseteq eA = uA = (ue^2)A \subseteq fA$ следует, что $I = fA$, где f – идемпотент. $\diamondsuit$

Упражнение 3.13. *Пусть G – группа, имеющая конечное число подгрупп. Тогда G – конечная группа.*

$\diamondsuit$ Пусть $\{H_1, \ldots, H_n\}$ – множество всех собственных подгрупп группы G. Доказательство приведем методом математической индукции по n. Заметим, что G – периодическая группа и если $n = 1$, то G – циклическая группа простого порядка. Сделаем предположение индукции о конечности любой группы с меньшим числом подгрупп и докажем конечность группы G. Можно считать, что G – не циклическая группа и, следовательно, $G = \bigcup\limits_{i=1}^{n} H_i$.

Докажем далее, что если

$$G = \bigcup_{i=1}^{n}\bigcup_{j=1}^{m_i} H_i a_{ij},$$

то существует подгруппа H_k, $k \leq n$ конечного индекса. Действительно, если в объединении $\bigcup\limits_{i=1}^{n}\bigcup\limits_{j=1}^{m_i} H_i a_{ij}$ встречаются все смежные классы $H_1 x$ подгруппы H_1, то $[G_i : H_1] < \infty$. Иначе

существует смежный класс, например, H_1a, который не встречается в объединении. Тогда

$$Ha \subseteq \bigcup_{i=2}^{n}\bigcup_{j=1}^{m_i} H_i a_{ij}, \quad H_1 \subseteq \bigcup_{i=2}^{n}\bigcup_{j=1}^{m_i} H_i(a_{ij}a^{-1})$$

и

$$G = \bigcup_{i=2}^{n}\left(\bigcup_{j=1}^{m_i} H_i a_{ij}\right) \bigcup \left(\bigcup_{i=2}^{n}\bigcup_{j=1}^{m_i} H_i\left(a_{ij}a^{-1}a_{1j}\right)\right),$$

то есть G является объединением смежных классов подгрупп $\{H_2, H_3, \ldots, H_n\}$. Рассуждая аналогично, мы докажем существование подгруппы H_i, $i \leq n$, конечного индекса. $\diamondsuit$

Таким образом существует собственная подгруппа H_i, $i \leq n$, группы G такая, что $[G : H_i] < \infty$. H_i содержит меньшее число подгрупп. Следовательно, по предположению индукции, $|H_i| < \infty$ и $|G| < \infty$.

Упражнение 3.14. *Пусть R – кольцо, содержащее конечное число подколец. Докажите, что R – конечное кольцо.*

$\diamondsuit$ R – правое артиново кольцо. Если $R = J(R)$, то $R^n = (0)$ для некоторого числа $n \geq 1$. Если $n = 2$, то абелева группа $\langle R, + \rangle$ содержит конечное число подгрупп и по предыдущей задаче $|R| < \infty$. Если $n \geq 3$, то применяя метод математической индукции относительно n, можно считать, что $\left|R/R^{n-1}\right| < \infty$ и $\left|R^{n-1}\right| < \infty$ (так как $\left(R^{n-1}\right)^2 = (0)$). Следовательно, $|R| < \infty$.

Пусть $R \neq J(R)$. Тогда $|J(R)| < \infty$ и

$$R/J(R) = M_{m_1}(D_1) \oplus \ldots \oplus M_{m_k}(D_k),$$

где $M_{m_i}(D_i)$ – полное кольцо матриц над полем D_i, $i \leq k$. Докажем, что каждое тело D_i является конечным. Если D_i содержит кольцо целых чисел $\mathbb{Z}$, то множество подколец в D_i является бесконечным. Поэтому D_i содержит поле $GF(p)$. Пусть

α – произвольный элемент из D_i и $GF(p)[\alpha]$ – подкольцо, порожденное элементами $\{1, \alpha\}$. Если $GF(p)[\alpha]$ изоморфно кольцу многочленов $GF(p)[x]$, то множество подколец в D_i являются бесконечными. В противном случае α – алгебраический элемент над полем $GF(p)$ и, следовательно, $\alpha^{p^s} = \alpha$ для некоторого числа $s \geq 1$. По теореме Джекобсона (см. главу 5) D_i – поле, являющееся конечнопорожденным алгебраическим расширением поля $GF(p)$, то есть $|D_i| < \infty$, $i \leq k$. Откуда следует, что $|R/J(R)| < \infty$, $|J(R)| < \infty$. Поэтому R – конечное кольцо. $\diamondsuit$

Упражнение 3.15. *Пусть $A = F[x]$ – кольцо многочленов над полем F от переменной x. Докажите, что A удовлетворяет условию максимальности для подалгебр.*

$\diamondsuit$ Условие обрыва возрастающих цепей подалгебр A равносильно тому, что каждая подалгебра A является конечнопорожденной. Пусть B – подалгебра A, не совпадающая с полем F и $b \in B \backslash F$. Тогда

$$b = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n,$$

где $\lambda_i \in F$, $n \geq 1$ и $\lambda_n \neq 0$. Следовательно,

$$x^n = \lambda_n^{-1} \left(b - \lambda_0 - \lambda_1 x - \ldots - \lambda_{n-1} x^{n-1} \right)$$

и A – конечнопорожденный $B_\circ$-модуль, где $B_\circ$ – подалгебра, порожденная $\{1, b\}$. Так как $B_\circ$ – нетерова алгебра, то A – нетеровый $B_\circ$-модуль, в котором B – $B_\circ$-подмодуль. В частности,

$$B = m_1 B_\circ + \ldots + m_k B_\circ$$

– конечнопорожденный $B_\circ$-модуль и $B = F[m_1, \ldots, m_k, b]$ – конечнопорожденная F-алгебра. $\diamondsuit$

Упражнение 3.16. *Пусть $A = F[x, y]$ – коммутативное кольцо многочленов над полем F от переменных x и y. Приведите пример подалгебры в A, которая не является конечнопорожденной F-алгеброй.*

$\diamondsuit$ Рассмотреть подалгебру $F\langle xy, xy^2, xy^3, \ldots\rangle$. $\diamondsuit$

Упражнение 3.17. *Пусть R – коммутативная область целостности с единицей и кольцо многочленов $R[x]$ является областью главных идеалов. Докажите, что R – поле.*

$\diamondsuit$ Пусть $a \in R$, $a \neq 0$. Рассмотрите идеал, порожденный элементами a и x. $\diamondsuit$

Упражнение 3.18. *Пусть $\langle G, +\rangle$ – полная абелева группа, то есть для любого целого числа $n \geq 1$ $nG = G$. Докажите, что G не содержит максимальных подгрупп.*

$\diamondsuit$ Если M – максимальная подгруппа G, то G/M – циклическая группа простого порядка p и $pG = G \subseteq M$. $\diamondsuit$

Упражнение 3.19. *Пусть $\langle G, +\rangle$ – полная абелева группа. Определим на G тривиальное умножение: для любых элементов $a, b \in G$ положим, что $a \cdot b = 0$. Докажите, что кольцо $\langle G, +, \cdot\rangle$ не содержит максимальных подколец и максимальных идеалов.*

Упражнение 3.20. *Пусть $\mathbb{Q}[[x]] = \left\{ \sum\limits_{i=0}^{\infty} a_i x_i \,\middle|\, a_i \in \mathbb{Q} \right\}$ – алгебра формальных степенных рядов от переменной x над полем рациональных чисел и $R = x\mathbb{Q}[[x]]$. Докажите, что R не содержит максимальных идеалов.*

$\diamondsuit$ Если M – максимальный идеал R, то M содержит R^2 и M/R^2 – максимальная подгруппа в полной группе R/R^2. $\diamondsuit$

Упражнение 3.21 (И. Исаев).
Пусть $R = \langle a_1, a_2, \ldots, a_n\rangle$ – конечно порожденное коммутативное кольцо без ненулевых нильпотентных элементов. Докажите, что R содержит регулярный элемент.

$\diamondsuit$ Пусть $\mathbb{Z}[x_1, \ldots, x_n]$ – кольцо многочленов от переменных $\{x_1, \ldots, x_n\}$. По теореме Гильберта о базисе $\mathbb{Z}[x_1, \ldots, x_n]$ является нетеровым кольцом. Каждый идеал подкольца $\langle x_1, \ldots, x_n \rangle$ является идеалом $\mathbb{Z}[x_1, \ldots, x_n]$ и, следовательно, $\langle x_1, \ldots, x_n \rangle$ – нетерово кольцо. Кольцо $R = \langle a_1, \ldots, a_n \rangle$ является гомоморфным образом $\langle x_1, \ldots, x_n \rangle$ и, следовательно, R – нетерово кольцо.

Если

$$(0) = Q_1 \cap Q_2 \cap \ldots \cap Q_s$$

– несократимое примарное разложение нулевого идеала R и

$$\rho_1 = \sqrt{Q_1}, \ \ldots, \ \rho_s = \sqrt{Q_s}$$

– радикалы идеалов $Q_1, \ldots, Q_s$ соответственно, то $\bigcup\limits_{i=1}^{n} \rho_i$ – множество всех делителей нуля R и $R \neq \bigcup\limits_{i=1}^{n} \rho_i$. $\diamondsuit$

Упражнение 3.22. *Пусть R – коммутативное кольцо и D – множество всех делителей нуля кольца R. Докажите, что*

1. *Если R содержит регулярные элементы, то D содержит простой идеал кольца R.*

2. *Если R – подпрямо неразложимое кольцо, то $D \lhd R$.*

$\diamondsuit$ Пусть $A = R \backslash D$ и

$$\mathfrak{M} = \{I \lhd R | \ I \cap A = \varnothing\}.$$

Тогда $\mathfrak{M}$ содержит идеал (0) и по лемме Цорна в $\mathfrak{M}$ существует максимальный идеал P. Если существуют элементы $a \notin P$, $b \notin P$ такие, что $ab \in P$, то существуют элементы

$$x_1 \in ((a) + p) \cap A, \quad x_2 \in ((b) + p) \cap A.$$

Откуда следует, что $x_1 x_2 \in P \cap A$. Противоречие доказывает, что P – простой идеал и $P \subseteq D$.

Пусть $a, b \in D$. Тогда $\mathrm{Ann}(a) \cap \mathrm{Ann}(b)$ содержит ненулевой элемент. Откуда следует, что $a + b$, $ab \in D$ и если $r \in R$, то $ar \in D$. $\diamondsuit$

Упражнение 3.23. *Найти все делители нуля, обратимые в нильпотентные элементы в кольце многочленов $\mathbb{Z}_n[x]$, где $\mathbb{Z}_n$ – кольцо классов вычетов по модулю n, $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ – каноническое разложение числа n на простые множители.*

Упражнение 3.24 (И. Исаев).
Пусть F – поле,

$$A = \begin{pmatrix} F & F \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} F & 0 \\ F & 0 \end{pmatrix}.$$

Докажите, что A и B – неизоморфные F-алгебры, хотя алгебры с присоединенной единицей $A^{\#}$ и $B^{\#}$ являются изоморфными.

Упражнение 3.25. *Пусть F – поле,*

$$A = F\langle e, a \mid e^2 = e, ea = ae = a, a^2 = 0\rangle,$$

$$B = F\langle f, b \mid f^2 = f, fb = bf = 0, b^2 = 0\rangle.$$

Докажите, что A и B – коммутативные неизоморфные F-алгебры, а алгебры с присоединенной единицей $A^{\#}$ и $B^{\#}$ являются изоморфными.

Упражнение 3.26. *Пусть A и B – алгебры над полем F и $A = J(A)$ – радикальная (в смысле радикала Джекобсона) алгебра. Докажите, что если $A^{\#} \cong B^{\#}$, то $A \cong B$.*

$\diamondsuit$ Если $\varphi : A^{\#} \to B^{\#}$ – изоморфизм F-алгебр, то $\varphi(A) \subseteq B$. $\diamondsuit$

Упражнение 3.27. *Привести примеры бесконечных колец R таких, что для любого ненулевого идеала $I \lhd R$ фактор-кольцо R/I является конечным.*

$\diamondsuit$ Например, $\mathbb{Z}$, $\mathbb{Z}[i]$, кольцо всех целых алгебраических чисел конечного алгебраического расширения поля рациональных чисел. Такие кольца удовлетворяют условию максимальности для идеалов. $\diamondsuit$

Упражнение 3.28. *Пусть R – алгебраическая алгебра над полем F, содержащая единицу. Докажите, что если R имеет классическое правое кольцо частных $Q(R)$, то $Q(R)$ совпадает с R.*

Упражнение 3.29. *Пусть R – правое артиново кольцо с единицей. Докажите, что регулярные элементы обратимы в R и, следовательно, R совпадает со своим кольцом частных.*

Упражнение 3.30. *Пусть R – коммутативное кольцо с единицей и $R[x]$ – кольцо многочленов с коэффициентами из R от переменной x. Докажите, что $f(x) \in R[x]$ является делителем нуля в $R[x]$ тогда и только тогда, когда существует элемент $a \in R$, $a \neq 0$ такой, что $af(x) = 0$.*

Упражнение 3.31. *Пусть $R = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \ldots\}$ – кольцо, состоящее из всех четных целых чисел. Докажите, что кольцо многочленов $R[x]$ не является нетеровым.*

Глава 4

Строение колец с тождественными соотношениями

4.1. Основные определения и теорема Амицура-Левицкого

Пусть R – алгебра над коммутативным кольцом Φ с единицей и $\Phi\langle X\rangle = \Phi\langle x_1, x_2, \ldots\rangle$ – свободная ассоциативная Φ-алгебра от счетного множества образующих $\{x_1, x_2, \ldots\}$. Многочлен

$$f(x_1, \ldots, x_d) \in \Phi\langle X\rangle$$

называется *тождеством алгебры* R, если для любых элементов $a_1, a_2, \ldots, a_d \in R$

$$f(a_1, a_2, \ldots, a_d) = 0.$$

Множество $T(R)$ всех многочленов из $\Phi\langle X\rangle$, являющихся тождеством алгебры R, является вполне характеристическим идеалом (или T-идеалом) в $\Phi\langle X\rangle$, то есть, если

$$f(x_1, \ldots, x_d) \in T(R)$$

и

$$\varphi_1(x_i), \ldots, \varphi_d(x_i)$$

– произвольные многочлены из $\Phi\langle X\rangle$, то

$$f(\varphi_1(x_i), \ldots, \varphi_d(x_i)) \in T(R).$$

Алгебра R, удовлетворяющая тождеству $f = 0$, где f – ненулевой многочлен из $\Phi\langle X\rangle$, называется *алгеброй с тождественным соотношением* (или PI*-алгеброй*). Приведем примеры таких алгебр:

Пример 4.1. Произвольная коммутативная алгебра удовлетворяет тождеству $[x, y] = xy - yx = 0$;

Пример 4.2. Произвольная нильпотентная индекса n алгебра удовлетворяет тождеству $x_1x_2 \ldots x_n = 0$;

Пример 4.3. Пусть R – n-мерная алгебра над полем F. Тогда для любого элемента $a \in R$ существуют элементы $\alpha_1, \ldots, \alpha_2 \in F$ такие, что

$$a^{n+1} + \alpha_1 a^n + \alpha_2 a^{n-1} + \ldots + \alpha_n a = 0.$$

Следовательно, для любого $b \in R$ справедливы равенства

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

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

$$\Big[\big[[a^{n+1}, b], [a, b]\big], \big[[a^2, b], [a, b]\big]\Big] + \\ + \alpha_1\Big[\big[[a^n, b], [a, b]\big], \big[[a^2, b], [a, b]\big]\Big] + \ldots \\ \ldots + \alpha_{n-2}\Big[\big[[a^3, b], [a, b]\big], \big[[a^2, b], [a, b]\big]\Big] = 0.$$

Продолжая аналогичные рассуждения, мы получим нетривиальное тождество для алгебры R.

Пример 4.4. Пусть A, B – произвольные матрицы из $M_2(F)$ и $C = [A, B]$. По теореме Гамильтона-Кэли

$$C^2 - \operatorname{tr}(C) \cdot C + |C| \cdot E = 0.$$

Так как $\operatorname{tr} C = 0$, то $C^2 = -|C|E$ принадлежит центру алгебры $M_2(F)$ и, следовательно,

$$\big[C^2, D\big] = \big[[A, B]^2, D\big] = 0$$

для любой матрицы $D \in M_2(F)$. Таким образом, алгебра $M_2(F)$ удовлетворяет тождеству

$$\big[[x, y]^2, z\big] = 0.$$

Пример 4.5. Пусть

$$G^1 = \Phi\left\langle 1, e_1, e_2, \dots \mid e_i^2 = 0,\ e_i e_j + e_j e_i = 0,\ i \neq j \right\rangle$$

– алгебра Грассмана. Ее центр порождается (как Ф-модуль) одночленами вида

$$e_{i_1} e_{i_2} \dots e_{i_{2k}},$$

где $i_1 < i_2 < \dots < i_{2k}$ и для любых двух одночленов

$$a = e_{j_1} \dots e_{j_s}, \quad b = e_{k_1} \dots e_{k_t}$$

коммутатор

$$[a, b] = [e_{j_1} \dots e_{j_s}, e_{k_1} e_{k_2} \dots e_{k_t}]$$

либо равен нулю (если одно из чисел s или t является четным), либо является линейной комбинацией одночленов четной длины. Другими словами, значения коммутатора $[x, y]$ принадлежат центру алгебры G^1 и, следовательно алгебра G^1 удовлетворяет тождеству

$$\big[[x, y], z\big] = 0.$$

В 1956 г. И. Капланский сформулировал проблему: *Пусть R – алгебра над полем F. Является ли R подалгеброй некоторой алгебры $M_n(K)$, где K – коммутативная F-алгебра?*

В. Латышев (МГУ, Москва) и П. Кон (Бэдфорд колледж, Лондон) дали на нее отрицательный ответ. А именно алгебра Грассмана G^1 над полем F является PI-алгеброй и не является подалгеброй $M_n(K)$, где K – коммутативная F-алгебра. Действительно, рассмотрим многочлен

$$S_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) x_{\sigma(1)} \ldots x_{\sigma(n)},$$

где $\operatorname{sgn} \sigma = 1$, если σ – четная подстановка, $\operatorname{sgn}(\sigma) = -1$, если σ – нечетная подстановка. Такой многочлен называется *стандартным многочленом степени n*. Легко видеть, что

$$S_{2n}(e_1, e_2, \ldots, e_{2n}) = (2n)! e_1 e_2 \ldots e_{2n} \neq 0$$

в алгебре Грассмана G^1.

Далее докажем теорему, из которой следует, что алгебра $M_n(K)$, где K – коммутативная F-алгебра, удовлетворяет тождеству $S_{2n}(x_1, \ldots, x_{2n}) = 0$, а значит G^1 не вложима в алгебру $M_n(K)$.

Теорема 4.1 (С. Амицур, Я. Левицкий).
Пусть K – коммутативная Φ-алгебра. Тогда $M_n(K)$ удовлетворяет тождеству $S_{2n}(x_1, x_2, \ldots, x_{2n}) = 0$.

Докажем сначала две леммы.

Лемма 4.1. *Пусть Φ-алгебра R удовлетворяет полилинейному тождеству*

$$f(x_1, \ldots, x_d) = \sum_{(i)} \alpha_{(i)} x_{i_2} \ldots x_{i_d} = 0,$$

где $\alpha_{(i)} \in \Phi$ и K – произвольная коммутативная Φ-алгебра. Тогда тензорное произведение $R \otimes_\Phi K$ тоже удовлетворяет тождеству $f(x_1, \ldots, x_d) = 0$.

□ Так как $f(x_1, \ldots, x_d)$ – полилинейный многочлен, то достаточно доказать, что при подстановке

$$x_1 = a_1 \otimes k_1, \ \ldots, \ x_d = a_d \otimes k_d,$$

где $a_i \otimes k_i \in R \otimes K$, справедливо $f(a_1 \otimes k_1, \ldots, a_d \otimes k_d) = 0$. Действительно,

$$\begin{aligned} f(a_1 \otimes k_1, \ldots, a_d \otimes k_d) &= \sum_{(i)} \alpha_{(i)} (a_{i_1} \otimes k_{i_1}) \ldots (a_{i_d} \otimes k_{i_d}) = \\ &= \sum_{(i)} \alpha_{(i)} (a_{i_1} a_{i_2} \ldots a_{i_d}) \otimes (k_{i_1} \ldots k_{i_d}) = \\ &= \sum_{(i)} \alpha_{(i)} (a_{i_1} \ldots a_{i_d}) \otimes (k_1 k_2 \ldots k_d) = \\ &= f(a_1, \ldots, a_d) \otimes (k_1 k_2 \ldots k_d) = 0. \ \square \end{aligned}$$

Так как $M_n(K) = M_n(\mathbb{Z}) \otimes_{\mathbb{Z}} K$ и $M_n(\mathbb{Z}) \subseteq M_n(\mathbb{Q})$, то из леммы 4.1 следует, что для доказательства теоремы достаточно проверить, что $S_{2n}(x_1, \ldots, x_{2n}) = 0$ – тождество алгебры $M_n(\mathbb{Q})$, где $\mathbb{Q}$ – поле рациональных чисел.

Лемма 4.2. *Пусть C – коммутативная $\mathbb{Q}$-алгебра с единицей и $A \in M_n(C)$ такая, что*

$$\operatorname{tr} A = \operatorname{tr} A^2 = \ldots = \operatorname{tr} A^n = 0.$$

Тогда $A^n = 0$.

□ Рассмотрим общую матрицу $X = (x_{ij}) \in M_n(\mathbb{Q}[x_{ij}])$, где $Q[x_{ij}]$ – кольцо коммутативных многочленов от переменных x_{ij}, где $1 \leq i, j \leq n$. По теореме Гамильтона-Кэли существуют многочлены $\alpha_1, \alpha_2, \ldots, \alpha_n$ с рациональными коэффициентами от $\operatorname{tr} X^i$, $i \leq n$, такие, что

$$X^n + \alpha_1 X^{n-1} + \ldots + \alpha_n \cdot E = 0.$$

Пусть $A = (a_{ij}) \in M_n(C)$. Существует гомоморфизм $\mathbb{Q}[x_{ij}] \to C$ такой, что $x_{ij} \to a_{ij}$. Эта специализация приводит к равенству $A^n = 0$. $\square$

Докажем теорему Амицура-Левицкого.

$\square$ Рассмотрим подалгебру

$$G_{2n}^1 = \left\langle 1, e_1, e_2, \ldots, e_{2n} |\ e_i^2 = 0,\ e_i e_j + e_j e_i = 0,\ i \neq j \right\rangle$$

алгебры Грассмана G^1 (над полем $\mathbb{Q}$). Тогда

$$C = \left\{ \sum_{(i)} \alpha_{(i)} e_{i_1} \ldots e_{i_{2k}} \right\}$$

– центр G_{2n}^1. Пусть $A_1, \ldots, A_{2n}$ – произвольные элементы из $M_n(\mathbb{Q})$ и пусть

$$B = A_1 \otimes e_1 + \ldots + A_{2n} \otimes e_{2n} \in M_n\left(G_{2n}^1\right) = M_n(\mathbb{Q}) \otimes_{\mathbb{Q}} G_{2n}^1.$$

Тогда

$$B^{2n} = S_{2n}(A_1, \ldots, A_{2n}) \otimes (e_1 e_2 \ldots e_{2n})$$

и

$$B^2 = D = \sum [A_i, A_j] \otimes e_i e_j \in M_n(C),$$

где C – коммутативная Q-алгебра. Далее

$$D^i = B^{2i} = \sum S_{2i}(A_{j_1}, \ldots, A_{j_{2k}}) \otimes e_{j_1} \ldots e_{j_{2k}} \in M_n(C),$$

$i \leq n$. Так как

$$\begin{aligned} S_{2n}(x_1, \ldots, x_{2n}) = \\ = x_1 S_{2n-1}(x_2, \ldots, x_{2n}) - x_2 S_{2n-1}(x_1, x_3, \ldots, x_{2n}) + \ldots \\ \ldots + (-1)^{2n-1} x_{2n} S_{2n-1}(x_1, \ldots, x_{2n-1}) = \\ = -S_{2n-1}(x_2, \ldots, x_{2n}) x_1 + S_{2n-1}(x_1, x_3 \ldots, x_{2n}) x_2 + \ldots \\ \ldots + S_{2n-1}(x_1, \ldots, x_{2n-1}) x_{2n}, \end{aligned}$$

то

$$S_{2n}(x_1,\dots,x_{2n}) = \frac{1}{2}\sum_{i=1}^{2n}\left[x_i, S_{2n-1}(x_1,\dots,\hat{x}_i,\dots,x_{2n})\right].$$

Учитывая, что след коммутатора двух матриц равен нулю, мы получаем, что $\operatorname{tr} D = \operatorname{tr} D^2 = \ldots = \operatorname{tr} D^n = 0$. По лемме 4.2 $D^n = B^{2n} = 0$ и $S_{2n}(A_1, A_2, \dots, A_{2n}) = 0$. $\square$

С. Амицур заметил, что многочлен

$$S_n\left([x^n, y], [x^{n-1}, y], \dots, [x, y]\right)$$

является тождеством алгебры $M_n(F)$, где F – бесконечное поле, не принадлежащим T-идеалу $\{S_{2n}\}^T$, порожденному многочленом $S_{2n}(x_1,\dots,x_{2n})$ и поставил вопрос о нахождении образующих T-идеала тождеств алгебры $M_n(F)$. Ю. Размыслов (МГУ, г. Москва) в 1973 г. доказал, что если F – поле характеристики нуль, то идеал тождеств алгебры $M_2(F)$ порождается девятью тождествами степени 4, 5 и 6.

В. Дренски (институт математики, г. София) доказал в 1981 г., что все тождества $M_2(F)$ при $\operatorname{char} F = 0$ следуют из S_4 и $\left[[x,y]^2, z\right]$.

Если $\operatorname{char} F = 0$, то проблема конечно порожденности произвольного T-идеала известно в литературе как "Проблема Шпехта". В 1987 г. А. Кемер (УлГУ, г. Ульяновск) положительно решил эту проблему, доказав, что для произвольного T-идеала $Q \subseteq F\langle X\rangle$ существуют такие элементы $f_1,\dots,f_n \in Q$, что

$$Q = \{f_1,\dots,f_n\}^T = \left\{ \sum_i \varphi_i(\bar{x}) f_i(g_{ij}(\bar{x}))\psi(\bar{x}) \,\middle|\, \varphi_i, \psi_j, g_{ig} \in F\langle X\rangle \right\}.$$

В частности из теоремы Кемера следует, что идеал тождеств алгебры $M_n(F)$, $\operatorname{char} F = 0$, является конечнопорожденным (как T-идеал).

Если $\operatorname{char} F > 0$, то вопрос о конечной порожденности произвольного T-идеала решается отрицательно. В работе [80] до-

казано, что если $\operatorname{char} F = 2$, то T-идеал, порожденный множеством многочленов

$$\left[x, y^2\right] x_1^2 x_2^2 \dots x_n^2 \left[x, y^2\right]^3,$$

$n = 0, 1, 2, \dots$ не является конечнопорожденным.

Израильский математик С. Амицур (26.08.1921-5.09.1994) внес выдающийся вклад в развитие теории PI-колец. Он является учеником известного математика Я. Левицкого. С. Амицуру принадлежит основополагающие результаты по структурной теории PI-колец, по строению приведенно свободных PI-алгебр. Им впервые построен пример конечномерной центральной алгебры с делением, не являющейся скрещенным произведением (K, G, f) (см. [104]).

Вернемся к проблеме Капланского о вложении PI-алгебр в $M_n(K)$, где K – коммутативная алгебра. Если алгебра A является подалгеброй $M_n(K)$, то идеал тождеств $T(A)$ содержит идеал тождеств $T(M_n(K))$ для некоторого целого числа $n \geq 1$. В частности, $T(A) \ni S_{2n}(x_1, \dots, x_{2n})$. Эта идея была основной для построения контрпримера к проблеме Капланского. Поэтому естественно уточнить проблему Капланского следующим образом: *Пусть алгебра A удовлетворяет всем тождествам некоторой полной матричной алгебры над коммутативной алгеброй. Будет ли A подалгеброй некоторой алгебры $M_n(K)$, где K – коммутативная алгебра?*

Приведем пример Л. Смолла конечно порожденной алгебры R над полем F, удовлетворяющей всем тождествам алгебры $M_4(F(t))$, где $F(t)$ – поле рациональных функций над полем F, имеющей нильпотентный радикал Джекобсона и не вложимой в алгебру матриц над коммутативной F-алгеброй (см. [116]). Этот пример показывает, что класс PI-алгебр (даже при довольно сильных ограничениях на алгебры) не исчерпывается подалгебрами полных матричных алгебр над коммутативными кольцами. Перед построением примера сделаем несколько замечаний:

Замечание 4.1. Пусть R – алгебра, $I = r(S) \leq_r R$, где $S \subseteq R$. Тогда

$$r(\ell(I)) = I$$

и если

$$I_1 = r(S_1) \subseteq I_2 = r(S_2),$$

то

$$\ell(I_1) \supseteq \ell(I_2).$$

В частности, если R удовлетворяет условию обрыва возрастающих цепей левых аннуляторных идеалов, то R удовлетворяет условию обрыва убывающих цепей правых аннуляторных идеалов.

Замечание 4.2. Пусть алгебра R удовлетворяет условию обрыва возрастающих (убывающих) цепей правых аннуляторных идеалов и A – ее подалгебра. Тогда A удовлетворяет условию обрыва возрастающих (соответственно, убывающих) цепей правых аннуляторных идеалов. Это следует из того, что, если $S \subseteq A$, то $r_A(S) = r_R(S) \cap A$.

Замечание 4.3. Пусть R – конечнопорожденная подалгебра $M_n(K)$, где K – коммутативная алгебра. Тогда $R \subseteq M_n(K')$, где K' – коммутативная нетерова алгебра и R удовлетворяет условиям максимальности и минимальности на правые аннуляторные идеалы.

Действительно, по условию $R = F\langle a_1, \ldots, a_m\rangle$, где F – поле. Пусть K' – F-подалгебра K, порожденная всеми вхождениями из K в матрицы $a_1, \ldots, a_m \in M_n(K)$. Тогда K' конечнопорожденная F-алгебра и по теореме Гильберта о базисе является нетеровой F-алгеброй. Конечно порожденный K'-модуль $M_n(K')$ является нетеровым K'-модулем и, следовательно, удовлетворяет условиям максимальности на правые и левые аннуляторные кольца. По замечанию 4.2 подалгебра $R \subseteq M_n(K')$ тоже удовлетворяет условиям максимальности на правые и левые аннуляторные идеалы, а, следовательно, по замечанию 1

и условиям минимальности на правые и левые аннуляторные идеалы.

Вернемся к примеру Л. Смолла. Пусть

$$A = \begin{pmatrix} F\left[t, t^{-1}\right] & F\left[t, t^{-1}\right] \\ 0 & F[t] \end{pmatrix}.$$

Тогда A – конечнопорожденная F-алгебра и $A \subseteq M_2(F(t))$. Пусть

$$I = \begin{pmatrix} 0 & F[t] \\ 0 & 0 \end{pmatrix} = e_{12}A <_r A,$$

$$D_i = \begin{pmatrix} F\left[t, t^{-1}\right] & F\left[t, t^{-1}\right] \\ 0 & t^i F[t] \end{pmatrix} = \{a \in A |\ y_i a \in I\} <_r A,$$

где

$$y_i = \begin{pmatrix} 0 & t^{-i} \\ 0 & 0 \end{pmatrix} \in A, \quad i = 1, 2, \ldots.$$

Рассмотрим конечно порожденную алгебру

$$B = \begin{pmatrix} F & A \\ 0 & A \end{pmatrix} \subseteq M_4(F(t))$$

и ее гомоморфный образ

$$R = \begin{pmatrix} F & A/I \\ 0 & A \end{pmatrix},$$

где A/I – (F, A)-бимодуль. Алгебра R является конечнопорожденной F-алгеброй и удовлетворяет всем тождествам алгебры $M_4(F(t))$. Ее радикал Джекобсона

$$J(R) = \begin{pmatrix} 0 & A/J \\ 0 & J(A) \end{pmatrix}$$

является нильпотентным, $J(R)^4 = (0)$. Далее

$$r\left(\begin{pmatrix} 0 & y_i + I \\ 0 & 0 \end{pmatrix}\right) = \begin{pmatrix} F & A/I \\ 0 & D_i \end{pmatrix},$$

где $i = 1, 2, \ldots$. Так как $D_1 \supseteq D_2 \supseteq D_3 \supseteq \ldots$ – строго убывающая цепь идеалов в $F[t]$, то R не удовлетворяет условию минимальности для правых аннуляторных идеалов, а, следовательно, по замечанию 4.1 условие максимальности для левых аннуляторных идеалов. Согласно замечанию 4.3 R не вложима в алгебру матриц над коммутативной алгеброй. Пример построен.

Предположим, что $\Phi = F$ – поле. Напомним, что идеал $I \lhd F\langle X\rangle$ называется T-*идеалом* (или *вполне характеристическим идеалом*) алгебры $F\langle X\rangle$, если для произвольного многочлена $f(x_1, \ldots, x_d) \in F\langle X\rangle$ и любых элементов $\varphi_1, \ldots, \varphi_d \in F\langle X\rangle$ имеем $f(\varphi_1, \ldots, \varphi_d) \in I$.

Многочлен $f(x_1, \ldots, x_d) \in F\langle X\rangle$ *существенно зависит* от $x_1, \ldots, x_d$, если f – линейная комбинация одночленов, содержащих все переменные $x_1, \ldots, x_d$. Ясно, что любой многочлен является суммой конечного числа многочленов, существенно зависящих от своих переменных и каждый T-идеал порождается многочленами, существенно зависящими от своих переменных.

Пусть $f(x_1, \ldots, x_d)$ существенно зависит от переменной x_1 и степень (по x_1) каждого одночлена $m(x_1, \ldots, x_d)$, входящего в запись $f(x_1, \ldots, x_d)$, равна единице, то есть $\deg_{x_1} m = 1$. Тогда говорят, что f – линейный многочлен относительно переменной x_1 и в этом случае

$$f(\alpha u_1 + \beta y_2, x_2, \ldots, x_d) = \alpha f(y_1, x_2, \ldots, x_d) + \beta f(y_2, x_2, \ldots, x_d),$$

где $\alpha, \beta \in F$. Если $f(x_1, \ldots, x_d)$ существенно зависит от $x_1, \ldots, x_d$ и является линейным по всем переменным $x_1, \ldots, x_d$, то его называют *полилинейным многочленом*.

Предложение 4.1. *I – T-идеал алгебры $F\langle X\rangle$ тогда и только тогда, когда $I = T(R)$ – идеал тождеств некоторой F-алгебры R.*

□ Пусть I – T-идеал $F\langle X\rangle$. Тогда I – идеал тождеств алгебры $F\langle X\rangle / T$.

Обратно. Если $I = T(R)$, где R – F-алгебра и многочлен $f(x_1, \ldots, x_d) \in I$, то для любых элементов $\varphi_1(x_i), \ldots, \varphi_d(x_i)$

$$f(\varphi_1, \ldots, \varphi_d) = 0$$

– тождество алгебры R и $f(\varphi_1, \ldots, \varphi_d) \in I$. $\square$

Предложение 4.2. *Каждый ненулевой T-идеал $F\langle X\rangle$ содержит ненулевой полилинейный многочлен.*

$\square$ Пусть $f(x_1, \ldots, x_d)$ – ненулевой многочлен из I, существенно зависящий от $x_1, \ldots, x_d$. Пусть f не является линейным многочленом, например, относительно переменной x_1. Тогда максимальная степень d_1 вхождения x_1 в одночлены f больше 1. Рассмотрим

$$\begin{aligned} g = g(y_1, y_2, x_2, \ldots, x_d) = \\ = f(y_1 + y_2, x_2, \ldots, x_d) - f(y_1, x_2, \ldots, x_d) - f(y_2, x_2, \ldots, x_d). \end{aligned}$$

Тогда $g \in I$,

$$\deg_{y_1} g \leq d_1 - 1, \ \deg_{y_2} g \leq d_1 - 1$$

и

$$\deg_{x_i} g \leq \deg_{x_i} f,$$

где $2 \leq i \leq d$. Если

$$a_0 x_1^{k_1} a_1 x_1^{k_2} \ldots a_{r-1} x^{k_r} a_r$$

– одночлен f степени d_1, $k_1 + k_2 + \ldots + k_r = d_1$, то g содержит (с ненулевым коэффициентом из F) одночлен

$$a_0 y_1^{k_1 - 1} y_2 a_1 y_1^{k_2} \ldots a_{r-1} y_1^{k_r} a_r.$$

Таким образом, $g \neq 0$ и его степени относительно переменных y_1 и y_2 строго меньше d_1. Продолжая этот линеаризационный процесс, мы получим ненулевой полилинейный многочлен в I. $\square$

Пример 4.6. Пусть алгебра R удовлетворяет тождеству

$$f(x,y) = xy^2 - yxy = 0.$$

Тогда R удовлетворяет полилинейному тождеству

$$f(x,y_1+y_2)-f(x,y_1)-f(x,y_2) = xy_1y_2+xy_2y_1-y_1xy_2-y_2xy_1 = 0.$$

Заметим, что если максимальная степень одночленов, входящих в запись f, равна d (то есть $\deg f = d$), то степень полилинейного многочлена, полученного линеаризацией f, не превосходит d.

Многочлен $f(x_1,\ldots,x_d)$ называется *однородным относительно* x_1, если степени по x_1 всех одночленов, входящих в запись f, равны. Если $f(x_1,\ldots,x_d)$ – однородный многочлен по всем переменным $x_1,\ldots,x_d$, то f называется *однородным.*

Предложение 4.3. *Пусть F – бесконечное поле и I – T-идеал $F\langle X\rangle$. Тогда I порождается однородными многочленами.*

□ Пусть $f(x_1,\ldots,x_d) \in I$ и f существенно зависит от переменных $x_1,\ldots,x_d$. Тогда

$$f = f_1 + f_2 + \ldots + f_n,$$

где f_i – сумма всех одночленов f, имеющих степени i относительно переменной x_1. Пусть $\lambda_1,\lambda_2,\ldots,\lambda_n$ – различные ненулевые элементы поля F. Тогда

$$f(\lambda_i x_1, x_2, \ldots, x_d) = \lambda_i f_1 + \lambda_i^2 f_2 + \ldots + \lambda_i^n f_n = 0,$$

$i \le n$, в алгебре $F\langle X\rangle/I$ и

$$\begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \ldots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \ldots & \lambda_2^{n-1} \\ \vdots & & & & \\ 1 & \lambda_n & \lambda_n^2 & \ldots & \lambda_n^{n-1} \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ \ldots \\ f_n \end{pmatrix} = \bar{0}.$$

Определитель выше приведенной матрицы равен

$$\prod_{i>j}(\lambda_i - \lambda_j) \neq 0.$$

Умножая слева на обратную матрицу, получим, что $f_1 = f_2 = \ldots = f_n = 0$ в алгебре $F\langle X\rangle / I$. Таким образом, $f_i \in I$, $i \leq n$ и I порождается своими однородными многочленами. □

Предложение 4.4. *Пусть F – поле характеристики нуль и I – T-идеал $F\langle X\rangle$. Тогда I порождается полилинейными многочленами.*

□ Пусть $f(x_1, \ldots, x_d)$ – однородный многочлен из I, существенно зависящий от $x_1, \ldots, x_d$. Пусть $\deg_{x_1} f = k > 1$. Применяя к f процесс линеаризации, мы получим многочлен

$$g(y_1, y_2, x_2, \ldots, x_d) = \\ = f(y_1 + y_2, x_2, \ldots, x_d) - f(y_1, x_2, \ldots, x_d) - f(y_2, x_2, \ldots, x_d) \in I,$$

степень которого по y_1 и y_2 меньше k. Пользуясь методом математической индукции, можно считать, что g является следствием полилинейных многочленов из I. Так как

$$g(x_1, x_1, x_2, \ldots, x_d) = \\ = 2^k f(x_1, x_2, \ldots, x_d) - 2f(x_1, x_2, \ldots, x_d) = \\ = (2^k - 2) f(x_1, x_2, \ldots, x_d),$$

то f принадлежит T-идеалу, порожденному всеми полилинейными многочленами из I. □

Пусть $F\langle X\rangle^1$ – свободная ассоциативная алгебра с единицей над полем F. Полилинейный многочлен $f(x_1, x_2, \ldots, x_d) \in F\langle X\rangle^1$, существенно зависящий от $x_1, \ldots, x_d$, называется *собственным*, если

$$f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_d) = 0,$$

где $1 \leq i \leq d$. Например,

$$[x_1, x_2, \ldots, x_d] = [[x_1, \ldots, x_{d-1}], x_d]$$

– собственный многочлен.

Предложение 4.5. *Пусть F – поле характеристики нуль и I – T-идеал $F\langle X\rangle$[1]. Тогда I порождается собственными многочленами.*

□ Пусть $f(x_1, \ldots, x_d)$ – полилинейный многочлен из I, существенно зависящий от $x_1, \ldots, x_d$. Предположим, что

$$f(1, x_2, \ldots, x_d) = f(x_1, 1, x_3, \ldots, x_d) = \ldots$$
$$\ldots = f(x_1, \ldots, x_{s-1}, 1, x_{s+1}, \ldots, x_d) = 0.$$

Положим

$$g = f - f(x_1, \ldots, x_s, 1, x_{s+2}, \ldots, x_d)x_{s+1}.$$

Тогда $g \in I$ и

$$g(x_1, \ldots, x_d)|_{x_j=1} = 0$$

при $1 \leq i \leq s+1$. Пользуясь методом математической индукции, можно считать, что $f(x_1, \ldots, x_s, 1, x_{s+2}, \ldots, x_d)$ и g являются следствиями собственных многочленов из I. Следовательно, $f = g + f(x_1, \ldots, x_s, 1, x_{s+2}, \ldots, x_d)x_{s+1}$ тоже является следствием собственных многочленов из I. Согласно предложению 4.4 I порождается своими полилинейными многочленами, а, следовательно, и собственными полилинейными многочленами. □

Предложение 4.6. *Пусть F – поле характеристики нуль и $f(x_1, \ldots, x_d)$ – собственный многочлен. Тогда f – линейная комбинация многочленов вида*

$$\left[x_{i_1}, \ldots, x_{i_{k_1}}\right]\left[x_{j_1}, \ldots, x_{j_{k_2}}\right] \ldots \left[x_{e_1}, \ldots, x_{e_{k_s}}\right].$$

□ Так как

$$x_1x_2\dots x_n - x_2x_3\dots x_nx_1 =$$
$$= [x_1,x_2]x_3\dots x_n + x_2[x_1,x_3]\dots x_n + \dots + x_2x_3\dots x_{n-1}[x_1,x_n],$$

то

$$f = g + h(x_2,x_3,\dots,x_n)x_1,$$

где x_1 входит в запись g как элемент коммутатора. Так как

$$f(1,x_2,\dots,x_n) = 0 = h(x_2,x_3,\dots,x_n),$$

то $f = g$. Продолжая аналогичное рассуждение, мы получим требуемое. □

Таким образом, произвольный T-идеал Q алгебры $F\langle X\rangle^1$ (F – поле характеристики нуль) порождается (как T-идеал) полилинейными многочленами вида

$$\sum_{(i)} \alpha_{(i)} \left[x_{i_1},\dots,x_{i_{k_1}}\right]\left[x_{i_{k_1+1}},\dots,x_{i_{k_2}}\right]\dots\left[x_{i_{k_{s-1}+1}},\dots,x_{i_{k_s}}\right],$$

где $\alpha_{(i)} \in F$. Такая система порождающих T-идеала Q получена в работе [117]. Важность такой системы порождающих T-идеалов следует из следующей теоремы Латышева.

Теорема 4.2. *Пусть*

$$G^1 = F\left\langle 1, e_1, e_2, \dots \mid e_i^2 = 0,\ e_ie_j + e_je_i = 0,\ i \neq j\right\rangle$$

– бесконечно порожденная алгебра Грассмана (с единицей) над полем характеристики нуль. Тогда

$$T(G^1) = \{[x,y,z]\}^T.$$

□ Ранее мы проверили, что

$$\{[x,y,z]\}^T \subseteq T(G^1).$$

Пусть

$$Q = \{[x, y, z]\}^T .$$

Согласно предложениям 4.5, 4.6 $T(G^1)$ порождается полилинейными многочленами

$$f(x_1, \ldots, x_n) = \sum_{(i)} \alpha_{(i)} [x_{i_1}, \ldots, x_{i_k}] \ldots \left[x_{i_{k_{s-1}+1}}, \ldots, x_{i_{k_s}}\right].$$

Так как $[x, y, z] \in Q$, то

$$f \equiv \sum_{(i)} \beta_{(i)} [x_{i_1}, x_{i_2}] \ldots \left[x_{i_{2k-1}}, x_{i_{2k}}\right] (\mathrm{mod}\, Q).$$

Заметим, что

$$\begin{aligned}[x, y][z, t]+[z, y][x, t] = \left[x[z, t], y\right]-x[z, t, y]+\left[z[x, t], y\right]-z[x, t, y] = \\ = [xz, t, y] - \left[[x, t]z, y\right] - x[z, t, y] + \left[z[x, t], y\right] - z[x, t, y] = \\ = [xz, t, y] + \left[z, [x, t], y\right] - x[z, t, y] - z[x, t, y] \equiv 0(\mathrm{mod}\, Q).\end{aligned}$$

Поэтому либо $f \in Q$, либо $n = 2k$ – четное число и

$$f(x_1, \ldots, x_n) \equiv \alpha[x_1, x_2] \ldots [x_{2k-1}, x_{2k}](\mathrm{mod}\, Q).$$

Полагая $x_i = e_i$, $i \leq n$, получим, что $\alpha 2^k e_1 e_2 \ldots e_{2k} = 0$ и $\alpha = 0$, то есть $f \in Q$. Таким образом, $T(G^1) = Q = \{[x, y, z]\}^T$. $\square$

Следующая теорема доказана Ю. Мальцевым в работе [49].

Теорема 4.3. *Пусть F – поле характеристики нуль и*

$$A_n = \left\{ \sum_{i \leq j} \alpha_{ij} e_{ij} \,\middle|\, \alpha_{ij} \in F \right\}$$

– подалгебра верхних треугольных матриц в $M_n(F)$. Тогда

$$T(A_n) = \{[x_1, x_2] \ldots [x_{2n-1}, x_{2n}]\}^T .$$

Перед доказательством теоремы рассмотрим следующие леммы.

Лемма 4.3. *Пусть $f(x_1, \ldots, x_d)$ – полилинейный многочлен из $T(A_n)$, существенно зависящий от $x_1, \ldots, x_d$. Тогда $d \geq 2n$;*

□ Предположим, что $d \leq 2n-1$ и

$$f = x_1 x_2 \ldots x_d + \sum_{(i)\neq(1)} \alpha_{(i)} x_{i_1} \ldots x_{i_d}.$$

Положим $x_1 = e_{11}$, $x_2 = e_{12}$, $x_3 = e_{22}$, $x_4 = e_{23}$, ... Тогда $f(e_{11}, e_{12}, \ldots) \neq 0$. Противоречие. □

Лемма 4.4.

$$[x_1, x_2] \ldots [x_{2n-1}, x_{2n}] \in T(A_n).$$

□ Так как радикал

$$J(A_n) = \{(a_{ij}) \in A_n |\ a_{11} = a_{22} = \ldots = a_{nn} = 0\},$$

$J(A_n)^n = (0)$ и $A_n/J(A_n)$ – коммутативная F-алгебра, то коммутаторный идеал $[A_n, A_n]$ алгебры A_n является нильпотентным индекса n и A_n удовлетворяет тождеству

$$[x_1, x_2] \ldots [x_{2n-1}, x_{2n}] = 0.$$

□

Лемма 4.5. *Пусть $f(x_1, \ldots, x_{2n})$ – полилинейный многочлен степени $2n$, лежащий в $T(A_n)$. Тогда*

$$f(x) = \sum_{\tau=(i_1,\ldots,i_{2n})} \alpha_\tau [x_{i_1}, x_{i_2}] \ldots [x_{i_{2n-1}}, x_{i_{2n}}],$$

где $\alpha_\tau \in F$, $\tau = (i_1, \ldots, i_{2n})$ – перестановки чисел $1, 2, \ldots, 2n$.

□ Пусть

$$f(x) = \sum_{\tau=(i_1,\dots,i_{2n})} \gamma_\tau x_{i_1} x_{i_2} \dots x_{i_{2n}}.$$

Рассмотрим следующие два одночлена, входящих в эту сумму с коэффициентами α и β:

$$\alpha x_{j_1} x_{j_2} \dots x_{j_{2i-1}} x_{j_{2i}} \dots x_{j_{2n}}, \quad \beta x_{j_1} x_{j_2} \dots x_{j_{2i}} x_{j_{2i-1}} \dots x_{j_{2n}}.$$

Положим

$$x_{j_{2i-1}} = x_{j_{2i}} = e_{ii},\ x_{j_{2k-1}} = e_{kk},\ x_{j_{2k}} = e_{kk+1},$$

если $k < i$, и

$$x_{j_{2k-1}} = e_{kk+1}, \quad x_{j_{2k}} = e_{kk},$$

если $k > i$. Подставляя эти значения в многочлен $f(x)$, получим $\alpha + \beta = 0$. Таким образом, в исходной записи многочлена $f(x)$ можно выделить в качестве слагаемого многочлен

$$\alpha \left[x_{j_1}, x_{j_2}\right] \dots \left[x_{j_{2n-1}}, x_{j_{2n}}\right].$$

Применяя эти рассуждения к оставшимся одночленам, получим искомое разложение многочлена $f(x)$. □

Пусть $V_n = T(A)$ и $u_n = [x_1, x_2] \dots [x_{2n-1}, x_{2n}]$, $n \geq 1$.

Лемма 4.6. *Пусть $f(x_1, \dots, x_k)$ – тождество минимальной степени алгебры A_n, $k \leq 2n$. Тогда $f(x)$ принадлежит идеалу $\{u_n\}^T$.*

□ Если $f(x)$ – полилинейный многочлен, то $k = 2n$ и $f(x) \in T(A_n)$ по лемме 4.5. Если многочлен $f(x)$ не линеен, например, по x_1, то его можно записать в виде

$$f(x) = \sum_{i=0}^{m} f_i(x),$$

где $f_i(x)$ – однородные слагаемые степени i относительно переменного x_1. Нам достаточно показать, что $f_i(x) \in \{u_n\}^T$ для

любого $i \leq m$. Применяя к $f(x)$ линеаризационный процесс и воспользуясь индукцией по длине этого процесса, мы можем предполагать, что многочлен полилинеен относительно переменных $x_2, x_3, \ldots, x_k$. Имеем

$$f_i(x+y, x_2, \ldots, x_k) - f_i(x, x_2, \ldots, x_k) - f_i(y, x_2, \ldots, x_k) = \\ = g(x, y, x_2, \ldots, x_k).$$

По предположению индукции $g(x, y, \ldots, x_k) \in \{u_n\}^T$. Положим $x = y = x_1$. Тогда

$$f_i(2x_1, x_2, \ldots, x_k) - 2f(x_1, x_2, \ldots, x_k) = \\ = (2^i - 2) f_i(x_1, \ldots, x_k) \in \{u_n\}^T,$$

где $i > 1$. □

Предложение 4.7. *Пусть $f(x_1, \ldots, x_k)$ тождество минимальной степени алгебры A_n. Тогда $f(x) \in \{u_n\}^T$.*

□ По лемме 4.3, степень многочлена $f(x)$ равна $2n$. Выберем в $f(x)$ слагаемое с фиксированным набором переменных. Тогда, полагая остальные переменные равными нулю, получим, что это слагаемое удовлетворяет условию леммы 4.6. Предложение доказано.

Предложение 4.8.

$$V_2 = \{u_2\}^T.$$

□ Пусть $V_2 \supsetneqq \{u_2\}^T$. Согласно предложению 4.6 в T-идеале V_2 найдется ненулевой собственный многочлен $f(x_1, \ldots, x_n)$ следующего вида

$$f(x_1, \ldots, x_m) = \sum_{(i)} \alpha_{(i)} [x_{i_1}, \ldots, x_{i_m}],$$

где $\alpha_{(i)} \in F$ и $m \geq 2n$. Согласно тождеству Якоби

$$[a, b, x, y] - [a, b, y, x] + \big[x, y, [a, b]\big] = 0.$$

Следовательно,

$$[a,b,x,y] \equiv [a,b,y,x] \left(\mathrm{mod}\{u_2\}^T\right)$$

и

$$f = \sum_{t=2}^{m} \beta_t [x_1, x_t, x_2, \ldots, \hat{x}_t, \ldots, x_m].$$

Если $\beta_{t_0} \neq 0$, то, сделав подстановку $x_{t_0} = e_{12}$, $x_j = e_{11}$, $j \neq t_0$, придем к противоречию. Итак, $V_2 = \{u_2\}^T$. $\square$

Лемма 4.7. *Пусть $f(x_1, \ldots, x_d) \in V_n$ и $f(x)$ является полилинейным многочленом. Запишем $f(x)$ в виде*

$$f(x) = f_1(x_1, \ldots, x_{d-t}) x_{d-t+1} \ldots x_d + f_2(x),$$

где t – четное число, $d - t \geq 1$ и $f_2(x)$ – сумма одночленов, не оканчивающихся на $x_{d-t+1} \ldots x_d$. Тогда

$$f_1(x) \in V_{n-\frac{t}{2}}.$$

$\square$ Пусть $t = 2k$. Для произвольной подстановки вместо переменных $x_1, \ldots, x_{d-t}$ элементов из A_{n-k} имеем

$$f_1(x_1, \ldots, x_{d-t}) = \sum_{i \leq j \leq n-k} \alpha_{ij} e_{ij}.$$

Докажем, что все $\alpha_{ij} = 0$. Действительно, полагая

$$x_{d-t+1} = e_{jn-k+1},\ x_{d-t+2} = e_{n-k+1\,n-k+1},\ \ldots,\ x_d = e_{nn},$$

придем к равенству

$$\left(\sum_{i \leq j \leq n-k} \alpha_{ij} e_{ij} \right) e_{jn} = 0.$$

Откуда следует, что $\alpha_{ij} = 0$ для любых $i, j \leq n - k$. $\square$

Докажем теорему.

□ Доказательство будем вести индукцией по n, а для данного n индукцией по степени тождества. Основания для индукции следуют из предложений 4.8, 4.7. Пусть теорема доказана для всех натуральных чисел $k < n$, и при данном $n \geq 3$, для всех тождеств степени меньшей d. Пусть также $f(x_1, \ldots, x_d)$ – произвольное тождество степени d, причем без ограничения общности, можно считать его полилинейным. По лемме 4.7 ($t = 2$) тождество $f(x)$ можно записать в виде

$$f(x_1, \ldots, x_d) = \sum_{i \neq j} f_{ij}(x) x_i x_j,$$

где $f_{ij}(x) \in V_{n-1}$. По предложению индукции

$$f_{ij}(x) \in \{u_{n-1}\}^T.$$

Преобразуем $f(x)$ следующим образом:

$$f(x) = \sum_{i>j} f_{ij}(x) x_i x_j + \sum_{i<j} f_{ij}(x) x_i x_j = \\ = \sum_{i>j} g_{ij}(x) x_i x_j + \sum_{i<j} f_{ij}(x)[x_i, x_j],$$

где $g_{ij}(x)$ и $f_{ij}(x) \in \{u_{n-1}\}^T$. Очевидно, что

$$\sum_{i<j} f_{ij}(x)[x_i, x_j]$$

принадлежит $\{u_n\}^T$. Нам осталось показать, что

$$g(x_1, \ldots, x_d) = \sum_{i>j} g_{ij}(x) x_i x_j \equiv 0 \left(\mathrm{mod}\{u_n\}^T\right).$$

Введем лексикографическую упорядоченность на множестве пар

$$\{(i,j) |\ i > j,\ 1 \leq i, j \leq d\}.$$

Доказательство будем вести индукцией по максимальной паре (t, s), соответствующей многочлену $g_{ts}(x) \notin \{u_n\}^T$. Основание

для индукции есть, так как если $g_{21}(x)x_2x_1 \in V_n$, то, подставляя $x_2 = x_1 = 1$, получим, что $g_{21}(x) \in V_n$. По предложению индукции относительно степени получим $g_{21}(x) \in \{u_n\}^T$ и, значит, $g_{21}(x)x_2x_1 \in T(u_n)$. Итак, пусть (t, s) – максимальная пара с указанным выше условием. Тогда

$$\frac{\partial g}{\partial x_s} = g(x)\Big|_{x_s=1} \not\equiv 0,$$

так как иначе $g_{ts} = 0$. Заметим, что

$$\frac{\partial g}{\partial x_s} \in \{u_n\}^T$$

и

$$\frac{\partial g}{\partial x_s}x_s - \sum_{i>s,\, i\neq t} g_{is}(x)x_ix_s - \sum_{i<s} g_{si}(x)x_ix_s - \sum_{k>e,\, t\neq k,\, s\neq e} \frac{\partial g_{ke}}{\partial x_s}x_kx_ex_s = \\ = g_{ts}(x)x_tx_s.$$

Это равенство переписывается, очевидно, следующим образом

$$P[x] + \sum_{(t,s)>(k,e)} P_{ke}(x)x_kx_e = g_{ts}(x)x_tx_s,$$

где $P[x] \in \{u_n\}^T$ и $P_{ke}(x) \in \{u_{n-1}\}^T$. Подставим $g_{ts}(x)x_tx_s$ в исходное выражение $g(x)$. Тогда

$$g(x_1, \ldots, x_d) \equiv \sum_{(t,s)>(k,e)} g'_{ke}(x)x_kx_e \left(\mathrm{mod}\{u_n\}^T\right),$$

где $g'_{ke}(x) \in \{u_{n-1}\}^T$. По предположению индукции

$$g(x) \equiv \sum_{(t,s)>(k,e)} g'_{ke}(x)x_kx_e \equiv 0 \left(\mathrm{mod}\{u_n\}^T\right).$$

□

Следствие 4.1. *Пусть F – поле характеристики нуль. Тогда*

$$T(M_n(F)) \subseteq \left(\{[x,y]\}^T\right)^n.$$

□ Доказательство следует из включения $A_n \subseteq M_n(F)$ и равенства

$$T(A_n) = \{[x_1,x_2]\dots[x_{2n-1},x_{2n}]\}^T = \left(\{[x,y]\}^T\right)^n.$$

□

4.2. Строение полупростых алгебр, удовлетворяющих тождественному соотношению

В настоящем параграфе мы дадим описание примитивных, полупростых и полупервичных алгебр над полем F, удовлетворяющих тождественному соотношению.

F-алгебра R называется *центральной*, если ее центр $Z(R)$ совпадает с F.

Предложение 4.9. *Пусть R – простая центральная F-алгебра и S – простая F-алгебра с единицей. Тогда $R \otimes_F S$ – простая алгебра.*

□ Пусть I – ненулевой идеал алгебры $R \otimes_F S$ и

$$i = \sum_{j=1}^{n} a_j \otimes b_j \in I$$

такой элемент, что $\{b_1,\dots,b_n\}$ – линейно независимые элементы алгебры S над полем F и n – минимальное число (для всех ненулевых элементов из I). Для любых элементов $x \otimes 1$, $y \otimes 1 \in R \otimes_F S$

$$(x \otimes 1)i(y \otimes 1) = \sum_{j=1}^{n} xa_jy \otimes b_j \in I.$$

Так как R – простая алгебра, то $Ra_1R = R$ и существуют элементы $x_1, \ldots, x_m, y_1, \ldots, y_m \in R$ такие, что

$$\sum_{j=1}^{m} x_j a_1 y_i = 1.$$

Следовательно,

$$c = \sum_{j=1}^{m} (x_j \otimes 1) i (y_j \otimes 1) = 1 \otimes b_1 + a_2' \otimes b_2 + \ldots + a_n' \otimes b_n \in I.$$

Пусть $x \in R$. Тогда

$$[x \otimes 1, c] = [x, a_2'] \otimes b_2 + \ldots + [x, a_n'] \otimes b_n \in I.$$

Так как целое число n являлось минимальным из возможных, то

$$[x, a_2'] = 0, \ \ldots, \ [x, a_n'] = 0$$

и a_i' – центральные элементы алгебры R, $i \leq n$. Так как R – центральная алгебра, то $a_i' \in F$, $2 \leq i \leq n$ и

$$c = 1 \otimes b_1 + 1 \otimes a_2' b_2 + \ldots + 1 \otimes a_n' b_n = \\ = 1 \otimes (b_1 + a_2' b_2 + \ldots + a_n' b_n) = 1 \otimes b \in I,$$

где $0 \neq b \in S$. Алгебра S является простой F-алгеброй. Поэтому I содержит

$$(1 \otimes S) c (1 \otimes S) = 1 \otimes (ScS) = 1 \otimes S,$$

а, следовательно,

$$R \otimes_F S = (R \otimes 1)(1 \otimes S) \subseteq I.$$

□

Пусть $\triangle$ – тело с центром Z ($\triangle \neq Z$). Подполе $K \subseteq \triangle$ называется *максимальным*, если любое подполе $E \subseteq \triangle$, содержащее K совпадает с K.

Заметим, что по лемме Цорна максимальное подполе существует и подполе K тела $\triangle$ ($\triangle \neq Z$) является максимальным тогда и только тогда, когда оно совпадает со своим централизатором

$$C_{\triangle}(K) = \{x \in \triangle |\ x\alpha = \alpha x,\ \alpha \in K\}.$$

В частности, максимальное подполе содержит центр Z тела $\triangle$. Пусть A – F-алгебра. Обозначим через A° – F-алгебру, антиизоморфную A.

Имеет место следующее предложение.

Предложение 4.10. *Пусть $\triangle$ – тело с центром $Z (Z \neq \triangle)$ и K – максимальное подполе $\triangle$. Тогда $\triangle \otimes_Z K$ – плотная алгебра линейных преобразований в $\mathrm{End}_K \triangle$.*

□ Рассмотрим кольца

$$E = \mathrm{End}_Z \triangle,$$

$$\triangle_r = \{R_a \in E |\, a \in \triangle \text{ и для любого элемента } x \in E\ xR_a = xa\},$$

$$K_e = \{L_b \in E |\, b \in K \text{ и для любого элемента } x \in E\ xL_b = bx\}.$$

Очевидно, что

$$\triangle_r \cong \triangle \quad \text{и} \quad K_e \cong K^{\circ} \cong K.$$

Заметим, что $R_a \cdot L_b = L_b \cdot R_a$ и

$$\triangle_r \cdot K_e = \left\{ \sum_{i=1}^{n} R_{a_i} L_{b_i} \,\middle|\, a_i \in \triangle, b_i \in K \right\}$$

– подкольцо E. Отображение

$$\varphi : \triangle \otimes_Z K \to \triangle_r \cdot K_e,$$

определенное по правилу

$$\varphi \left(\sum_{i=1}^{n} a_i \otimes b_i \right) = \sum_{i=1}^{n} R_{a_i} L_{b_i}$$

является сюръективным гомоморфизмом алгебр.

Так как $\triangle \otimes_Z K$ – простая Z-алгебра (см. предложение 4.9), то ядро этого отображения равно нулю и

$$\triangle \otimes_Z K \cong \triangle_r K_e.$$

Покажем, что $\triangle_r K_e$ – плотная алгебра линейных преобразований в $\triangle_K$. Так как $\triangle$ – тело, то для любого ненулевого элемента $d \in \triangle$ имеем, что $\triangle = d\triangle = d\triangle_r$ и $\triangle$ – точный неприводимый правый $\triangle_r K_e$-модуль. По лемме Шура (см. главу 1) $P = \mathrm{End}_{\triangle_r K_e} \triangle$ – тело. Пусть $\lambda \in P$. Тогда для любых элементов $u, a \in \triangle$, $b \in K$ имеем, что

$$(uR_aL_b)\,\lambda = (u\lambda)R_aL_b$$

или

$$(bua)\lambda = b(u\lambda)a.$$

В частности, $a\lambda = (1 \cdot a)\lambda = (1)\lambda a$, $\lambda = L_{(1)\lambda} \in \triangle_e$ и $P \subseteq \triangle_e$. Покажем, что $L_{(1)\lambda} \in C_{\triangle_e}(K_e)$. Пусть $b \in K$ и $x \in \triangle$. Тогда

$$x(L_{1\lambda}L_b - L_bL_{1\lambda}) = b\,((1)\lambda)\,x - (1)\lambda bx = (bx - bx)\lambda = 0$$

и $P = C_{\triangle_e}(K_e) = K_e$. $\square$

Предложение 4.11. *Алгебра $M_n(F)$ не удовлетворяет полилинейному тождеству степени меньшей $2n$.*

$\square$ Предположим противное. Пусть полилинейный многочлен

$$f(x_1, \ldots, x_d) = x_1x_2 \ldots x_d + \sum_{(i)\neq(1)} \alpha_{(i)}x_{i_1} \ldots x_{i_d}$$

является тождеством в $M_n(F)$ и $d < 2n$. Положим

$$x_1 = e_{11},\ x_2 = e_{12},\ x_3 = e_{23},\ x_4 = e_{33},\ \ldots.$$

Тогда $f(e_{11}, e_{12}, \ldots) = e_{1k} \neq 0$, где $k = \frac{d+1}{2}, \frac{d+2}{2}$. Противоречие. $\square$

Теорема 4.4 (И. Капланский).
Пусть R – примитивная F-алгебра, удовлетворяющая тождеству степени d. Тогда R – простая алгебра, конечномерная над своим центром Z и

$$\dim_Z R \leq [d/2]^2.$$

□ Из предложения 4.2 следует, что R удовлетворяет полилинейному тождеству $f(x_1, \ldots, x_d) = 0$. По следствию из теоремы плотности (см. главу 1) получаем, что либо $R = M_n(D)$, где D – F-алгебра с делением, либо для любого целого числа $m \geq 1$ существует подкольцо $S \subseteq R$, гомоморфно отображающееся на $M_m(D)$. Предположим, что имеет место второй случай. Пусть $m > \left[\frac{d}{2}\right] + 1$. Тогда существует такое подкольцо $S' \subseteq R$, что некоторый его гомоморфный образ $S'/I \cong M_m(D)$ удовлетворяет тождеству $f(x_1, \ldots, x_d) = 0$, где $d < 2m$. Это противоречит предложению 4.11. Следовательно, $R = M_n(D)$, где $n \leq \frac{d}{2}$.

Пусть K – максимальное подполе D и Z – его центр. Согласно предложению 4.10 алгебра $D \otimes_Z K$ является примитивной. Точнее $D \otimes_Z K$ – плотное кольцо линейных преобразований в векторном пространстве D над полем K. Из выше приведенных рассуждений следует, что $D \otimes_Z K$ удовлетворяет тождеству $f(x_1, \ldots, x_d) = 0$ (см. лемму 4.1), $\dim_{K_e} D = t$ и

$$D \otimes_Z K \cong M_t(K),$$

где $t \leq \frac{d}{2}$, $\dim_Z D = t^2$. Таким образом,

$$R \otimes_Z K = (M_n(Z) \otimes_Z D) \otimes_Z K \cong M_n(Z) \otimes_Z (D \otimes_Z K) \cong$$
$$\cong M_n(Z) \otimes_Z M_t(K) \cong M_{nt}(k),$$

где $nt \leq d/2$ и $\dim_Z R = (nt)^2 \leq [d/2]^2$. □

Пусть $g(x_1, \ldots, x_d) \in F\langle X \rangle$. Максимальная степень одночленов, входящих в g с ненулевым коэффициентом, называется *степенью* $g(x_1, \ldots, x_d)$. Пусть R – PI-алгебра и d – минимальная степень многочленов из $T(R)$. Будем говорить, что R – *PI-алгебра степени d.*

Следствие 4.2. *Пусть R – примитивная PI-алгебра степени d и Z – ее центр. Если $|Z| < \infty$, то $R = M_n(Z)$, где $n \leq d/2$.*

□ Из теоремы 4.4 следует, что $R = M_n(D)$, где тело D является конечномерным над полем Z. Так как $|Z| < \infty$, то $|D| < \infty$. По теореме Веддерберна тело D совпадает с Z (см. главу 5). Следовательно, $R = M_n(Z)$ и согласно предложению 4.11, $n \leq d/2$. В частности, R – конечное кольцо. □

В работе [95] доказано, что если полупервичное кольцо R удовлетворяет тождеству и его центр $Z(R)$ является конечным подкольцом, то R – конечное кольцо.

Теорема 4.5. *Пусть R – полупростая PI-алгебра степени d. Тогда $d = 2m$ и R – подпрямая сумма таких простых алгебр, конечномерных над своими центрами, что эти размерности ограниченны $[d/2]^2$.*

□ Так как радикал Джекобсона $J(R) = (0)$, то R – подпрямая сумма примитивных алгебр $R_i = R/P_i$, $i \in I$, удовлетворяющих полилинейному тождеству $f = 0$ степени d. По теореме 4.4

$$R_i \otimes_{Z_i} K_i = M_{n_i}(K_i),$$

$i \in I$, где Z_i – центр R_i и K_i – максимальное подполе тела D_i, являющегося централизатором неприводимого R_i-модуля. Так как тождество $f = 0$ переносится на $M_{n_i}(K_i)$ (см. лемму 4.1), то по предложению 4.11 числа $n_i \leq \left[\frac{d}{2}\right]$, $i \in I$ и, следовательно,

$$\dim_{Z_i} R_i = n_i^2 \leq \left[\frac{d}{2}\right]^2.$$

Если бы для любого индекса $i \in I$ $n_i < \frac{d}{2}$, то по теореме Амицура-Левицкого алгебры $M_{n_i}(K_i)$ удовлетворяли бы стандартному тождеству степени строго меньшей d. Следовательно, алгебра R удовлетворяла бы тождеству степени меньшей d,

что противоречит условию теоремы. Итак, существует индекс $i_\circ \in I$ такой, что $d = 2n_{i_\circ}$ и

$$R = \sum_{i\in I} \bigoplus_s R_i \subseteq \prod_{i\in I} M_{n_i}(K_i) \subseteq M_{\frac{d}{2}}\left(\prod_{i\in I} K_i\right).$$

□

В частности, мы доказали, что полупростая PI-алгебра степени d вложима в алгебру матриц порядка $\frac{d}{2}$ над алгеброй без нильпотентных элементов.

Следствие 4.3. *Пусть R – PI-алгебра нечетной степени d. Тогда R содержит ненулевой нильпотентный идеал, то есть не является полупервичной алгеброй.*

□ Пусть $f(x_1, \ldots, x_d) = 0$ – полилинейное тождество алгебры R и d – нечетное число. Рассмотрим кольцо многочленов $R[t]$. По лемме 4.1 оно удовлетворяет тождеству $f = 0$. Если R – полупервичная алгебра, то она не содержит ниль-идеалов (см. главу 2) и следовательно, по теореме Амицура (глава 1) $R[t]$ – полупростая PI-алгебра степени d. По теореме 4.5 d – четное число. Противоречие. □

Следствие 4.4. *Пусть R – полупервичная PI-алгебра степени d. Тогда d – четное число и R – подалгебра алгебры $M_{\frac{d}{2}}(K)$, где K – коммутативная F-алгебра без нильпотентных элементов.*

□ Из главы 2 следует, что ниль-радикалы $\mathrm{un}R$, $\ln R$ и $L(R)$ совпадают и равны нулю. По теореме Амицура $R[t]$ – полупростая PI-алгебра степени d. По теореме 4.5 d – четное число и $R[t] \subseteq M_{\frac{d}{2}}(K)$, где K – коммутативная F-алгебра без нильпотентных элементов. Откуда следует, что $R \subseteq M_{d/2}(K)$. □

Из следствия 4.4 получаем, что полупервичная PI-алгебра R степени d удовлетворяет тождеству $S_d(x_1, \ldots, x_d) = 0$. Это важное замечание приводит к следующему следствию.

Следствие 4.5. *Всякая PI-алгебра R удовлетворяет тождеству вида $S_{2n}^m(x_1, \ldots, x_{2n}) = 0$.*

□ Пусть $f(x_1, \ldots, x_d) = 0$ – полилинейное тождество степени d алгебры R, $n = \left[\frac{d}{2}\right]$ и

$$\wedge = R^{2n} = \underbrace{R \cdot \ldots \cdot R}_{2n} = \{(r_1, r_2, \ldots, r_{2n}) |\ r_i \in R\}.$$

Рассмотрим алгебру

$$S = \prod_{\alpha \in \wedge} R_\alpha,$$

где $R_\alpha = R$ (полное прямое произведение копий R_α алгебры R). Тогда алгебра S удовлетворяет тождеству $f(x_1, \ldots, x_d) = 0$ и из замечания к следствию 4.4 следует, что полупервичная алгебра $S/\ln S$ удовлетворяет тождеству $S_{2n}(s_1, s_2, \ldots, s_{2n}) = \overline{0}$. Другими словами, для любых $s_1, s_2, \ldots, s_{2n} \in S$

$$S_{2n}(s_1, s_2, \ldots, s_{2n}) \in \ln S.$$

Выберем элементы $s_1, \ldots, s_{2n} \in S$. Пусть

$$\alpha = (r_1, r_2, \ldots, r_{2n}) \in \wedge.$$

Положим

$$s_1(\alpha) = r_1,\ s_2(\alpha) = r_2,\ \ldots,\ s_{2n}(\alpha) = r_{2n}.$$

Тогда $S_{2n}(s_1, \ldots, s_{2n}) \in \ln S$ и является нильпотентным элементом, то есть

$$S_{2n}^m(s_1, \ldots, s_{2n}) = 0.$$

С другой стороны,

$$0 = S_{2n}^m(s_1(\alpha), \ldots, s_{2n}(\alpha)) = S_{2n}^m(r_1, \ldots, r_{2n})$$

для любого $\alpha \in \wedge$. Это означает, что $S_{2n}^m = 0$ – тождество алгебры R. □

Пусть

$$N_r = \{a \in R |\ aR \text{ – ниль-алгебра ограниченного индекса}\},$$

$$R^R = \prod_{i \in R} R_i = \{(r_i) |\ r_i \in R_i\},$$

где $R_i = R$, $i \in R$.

Предложение 4.12. *Пусть R – PI-алгебра степени d. Тогда N_r – двусторонний идеал R такой, что $\ln R^R \cap R = N_r$ и R/N_r – подалгебра $M_m(K)$, где K – коммутативная F-алгебра без нильпотентных элементов и $M_m(K)$ удовлетворяет всем полилинейным тождествам алгебры R.*

□ Пусть $x \in R \cap \ln(R^R)$ и $f \in R^R$ такая функция, что $f(a) = a$ для любого элемента $a \in R$. Тогда $xf \in \ln R^R$ и $(xf)^n = 0$ для некоторого целого числа $n \geq 1$. Следовательно, $(xa)^n = 0$ для любого элемента $a \in R$ и xR – правый идеал ниль индекса n, то есть $R \cap \ln(R^R) \subseteq N_r$.

Пусть $y \in N_r$. Тогда правый идеал yR удовлетворяет тождеству $x^n = 0$ для некоторого целого числа $n \geq 1$. Поэтому для любого элемента $h \in R^R$ и $a \in R$ имеем, что

$$(yh)^n(a) = (yh(a))^n = 0, \quad \ln\left(yR^R\right) = yR^R$$

и $y \in \ln(R^R) \cap R$. Таким образом,

$$N_r = R \cap \ln R^R.$$

Естественный гомоморфизм

$$\pi : R^R \to R^R/\ln R^R$$

индуцирует гомоморфизм

$$R \to R^R/\ln R^R$$

с ядром $N_r = R \cap \ln R^R$. Следовательно, R/N_r – подалгебра полупервичной PI-алгебры $R^R/\ln R^R$, удовлетворяющей тождеству степени d. Согласно следствию 4.4 $R^R/\ln R^R$ – подалгебра некоторой алгебры вида $M_m(K)$, где $m \leq \frac{d}{2}$ и K – F-алгебра без нильпотентных элементов. Полилинейные тождества алгебры R переносятся на R^R, $R^R/\ln R^R[t]$ и, следовательно, на алгебру $M_m(K)$ (см. доказательство теоремы 4.5). $\square$

Из предложения 4.12 следует, что если R удовлетворяет тождеству

$$[x_1, \ldots, x_k] = 0,$$

то коммутаторный идеал $[R, R] \subseteq N_r$. В частности, если R – конечнопорожденная алгебра над полем F характеристики нуль, то по теореме Нагата-Хигмана-Дубнова-Иванова (см. главу 2) N_r – сумма нильпотентных идеалов и $[R, R]$ – конечнопорожденный (R, R)-бимодуль в N_r. Откуда следует, что $[R, R]^m = (0)$ и R удовлетворяет тождеству

$$[x_1, x_2] \ldots [x_{2m-1}, x_{2m}] = 0.$$

4.3. Центральный многочлен Капланского, строение первичных PI-алгебр и приведенно свободных алгебр

Пусть R – алгебра над полем F и $f(x_1, \ldots, x_d)$ – однородный ненулевой многочлен из $F\langle X\rangle$, ненулевой степени и не являющийся тождеством алгебры R. Многочлен f называется *центральным* (*многочленом Капланского*) для алгебры R, если

$$[f(x_1, \ldots, x_d), y] = 0$$

– тождество в алгебре R.

Например, $[x, y]$ – центральный многочлен для алгебры Грассмана и $[x, y]^2$ – центральный многочлен для алгебры $M_2(F)$.

В 1956 г. И. Капланский сформулировал проблему: *Существует ли центральный многочлен для алгебры $M_n(F)$?*

Эта проблема была решена положительно в 1972 г. Ю. Размысловым (МГУ, г. Москва) и Э. Форманеком (см. [59, 75]). Причем их примеры центральных многочленов различны. Пример Ю. Размыслова является полилинейным многочленом степени $3n^2 - 1$, а пример Э. Форманека – однородный не полилинейный многочлен степени n^2. Мы приведем пример Э. Форманека.

Далее будем предполагать, что F – поле характеристики нуль (в этом случае, T-идеалы порождаются полилинейными многочленами).

Теорема 4.6 (Э. Форманек).
Для алгебры $M_n(F)$ существует центральный многочлен степени n^2.

□ Пусть $x_1, x_2, \ldots, x_{n+1}$ и $X, Y_1, \ldots, Y_n$ – соответственно множества коммутативных и некоммутативных переменных. Отображение

$$\sum \alpha_a x_1^{a_1} \ldots x_{n+1}^{a_{n+1}} \to \sum \alpha_a X^{a_1} Y_1 X^{a_2} Y_2 \ldots X^{a_n} Y_n X^{a_{n+1}}$$

связывает с каждым многочленом из коммутативного кольца $F[x_1, \ldots, x_{n+1}]$ некоторый многочлен из свободной ассоциативной алгебры $F\langle X, Y_1, Y_2, \ldots, Y_n\rangle$. Пусть $G(X, Y_1, \ldots, Y_n)$ – образ (при таком отображении) многочлена

$$g(x_1, \ldots, x_{n+1}) = \prod_{2 \le i \le n} (x_1 - x_i)(x_{n+1} - x_i) \cdot \prod_{2 \le j < k \le n} (x_j - x_k)^2.$$

Тогда многочлен

$$\begin{aligned} F(X, Y_1, Y_2, \ldots, Y_n) = \\ = G(X, Y_1, \ldots, Y_n) + G(X, Y_2, \ldots, Y_n, Y_1) + \ldots \\ \ldots + G(X, Y_n, Y_1, Y_2, \ldots, Y_{n-1}) \end{aligned}$$

является искомым центральным многочленом для $M_n(F)$. Докажем это.

Так как $F(X, Y_1, \ldots, Y_n)$ линеен относительно переменных $\{Y_1, \ldots, Y_n\}$, то можно предполагать, что $Y_1, \ldots, Y_n$ – матричные единицы в $M_n(F)$. Пусть

$$X = x_1 e_{11} + x_2 e_{22} + \ldots + x_n e_{nn} = \operatorname{diag}(x_1, x_2, \ldots, x_n)$$

и

$$Y_1 = e_{i_1 j_1}, \ \ldots, \ Y_n = e_{i_n j_n}.$$

Тогда

$$X^{a_1} e_{i_1 j_1} X^{a_2} e_{i_2 j_2} \ldots X^{a_n} e_{i_n j_n} X^{a_{n+1}} = x_{i_1}^{a_1} \ldots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}} e_{i_1 j_1} \ldots e_{i_n j_n}$$

и

$$G(X, e_{i_1 j_1}, \ldots, e_{i_n j_n}) = g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) e_{i_1 j_1} \ldots e_{i_n j_n}.$$

При этом $g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) = 0$, если $(i_1, \ldots, i_n)$ не является перестановкой $(1, 2, \ldots, n)$ и $i_1 \neq j_n$. Если же $(i_1, \ldots, i_n)$ – перестановка $(1, 2, \ldots, n)$ и $i_1 = j_n$, то

$$g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = D.$$

Далее $e_{i_1 j_1} \ldots e_{i_n j_n} = 0$, если не выполняется хотя бы одно из равенств $j_1 = i_2, \ldots, j_{n-1} = i_n$. Если же эти равенства выполняются, то

$$G(X, e_{i_1 j_1}, \ldots, e_{i_n j_n}) = D e_{i_1 i_1}.$$

Иначе,

$$G(X, e_{i_1 j_1}, \ldots, e_{i_n j_n}) = 0.$$

Следовательно,

$$F(X, Y_1, \ldots, Y_n) = DE,$$

где E – единичная матрица, если $j_1 = i_2$, $j_2 = i_3$, …, $j_{n-1} = i_n$ и $j_n = i_1$. В противном случае

$$F(X, Y_1, \ldots, Y_n) = 0.$$

Таким образом, многочлен $F(X, Y_1, \ldots, Y_n)$ принимает центральные значения, если $Y_1, \ldots, Y_n$ – произвольные матрицы, а X – диагональная матрица. При этом эти значения ненулевые, так как F – бесконечное поле, и мы можем выбрать попарно различные элементы на диагонали.

Пусть $F(x_{ij})$ – поле рациональных функций от n^2 переставочных между собой переменных и $X = (x_{ij})$ – общая матрица в $M_n(F(x_{ij}))$. Пусть также L – алгебраическое замыкание поля $F(x_{ij})$. Тогда существует такая невырожденная матрица $T \in M_n(L)$, что

$$T^{-1}XT = \operatorname{diag}(\lambda_1, \ldots, \lambda_n) = X_1,$$

где $\lambda_i \in L$. Откуда следует, что матрица

$$F(X, Y_1, \ldots, Y_n) = TF(T^{-1}XT, T^{-1}Y_1T, \ldots, T^{-1}Y_nT)T^{-1} = \\ = TF(X_1, T^{-1}Y_1T, \ldots, T^{-1}Y_nT)T^{-1}$$

принимает центральные значения в $M_n(L)$. Так как $X = (x_{ij})$ – общая матрица, то $F(X, Y_1, \ldots, Y_n)$ принимает значения из центра в $M_n(F)$ и не является тождеством в $M_n(F)$. $\square$

Заметим, что из доказательства предложения 4.4 следует, что алгебра $M_n(F)$ имеет полилинейный центральный многочлен степени n^2, который получается линеаризацией многочлена $F(X, Y_1, \ldots, Y_n)$.

Пусть R – первичная F-алгебра. Из предложения 4.12 следует, что R – подалгебра некоторой алгебры вида

$$M_m(K) = K \otimes_F M_m(F),$$

где K – коммутативная алгебра. При этом полилинейные тождества алгебр R и $M_m(K)$ совпадают, а значит, совпадают идеалы тождеств (в алгебре $F\langle X\rangle$). Согласно теореме 4.6 $T(M_m(K))$ содержит полилинейный многочлен вида $[f(x_1, \ldots, x_k), y]$, где $f \notin T(M_m(K))$. Следовательно, $f(x_1, \ldots, x_k)$ –центральный многочлен на алгебре R (не являющейся тождеством). Поэтому

центр $Z(R) \neq (0)$. Так как R – первичная алгебра, то ненулевые элементы $Z(R)$ являются регулярными элементами в R. Рассмотрим кольцо частных (см. главу 3)

$$RZ^{-1} = \left\{az^{-1} |\ a \in R,\ z \in Z(R),\ z \neq 0\right\}.$$

R является подалгеброй $RZ^{-1} = Q$ и $T(Q) = T(R)$. Заметим, что центр $Z(Q) = ZZ^{-1}$ – поле, где $Z = Z(R)$.

Лемма 4.8.

1. *RZ^{-1} – первичная алгебра.*

2. *Если*

   $I \lhd R$ и $I \neq 0$, то I – первичная алгебра и $Z(I) = Z(R) \cap I$.

□ Пусть A, B – ненулевые идеалы RZ^{-1} такие, что $AB = (0)$. Тогда

$$(A \cap R) \cdot (B \cap R) = (0).$$

Так как R – первичная алгебра, то, например, $A \cap R = (0)$. Пусть as^{-1} – ненулевой элемент из A. Тогда $a = (as^{-1})s \in A \cap R$ и $a = 0$. Противоречие доказывает, что RZ^{-1} – первичная алгебра.

Докажем, что I – первичная алгебра. Если $i, j \in I$ такие, что $i \cdot I \cdot j = (0)$, то $(iI)R \cdot j = 0$. Так как R – первичная алгебра, то либо $j = 0$, либо $iI = (0)$. Если $iI = (0)$, то $i(RI) = iRI = (0)$. Так как R – первичная алгебра, то либо $i = 0$, либо $I = (0)$. Итак, I – первичная алгебра. Включение $Z(R) \cap I \subseteq Z(I)$ очевидно. Пусть $a \in Z(I)$, $x \in R$ и $i \in I$. Тогда

$$[a, x]i = [a, xi] - x[a, i] = 0$$

и $[a, x]I = (0)$. Откуда следует, что $[a, x]RI = (0)$ и, ввиду первичности алгебры R, $[a, x] = 0$, то есть $a \in Z(R)$. □

Теорема 4.7 (Э. Познер, Л. Роуэн).
Пусть R – первичная PI-алгебра. Тогда центр $Z = Z(R) \neq (0)$ и R-подалгебра центрального кольца частных RZ^{-1}, которая является простой алгеброй, n^2-мерной над своим центром ZZ^{-1}. При этом идеалы тождеств алгебр R и RZ^{-1} совпадают и равны M_n – идеалу тождеств алгебры $M_n(F)$.

□ Пусть I – ненулевой идеал первичной алгебры RZ^{-1}. Тогда $I \cap R \neq (0)$ и согласно лемме 4.8 $(I \cap R)$ – первичная PI-алгебра, то есть $Z(I \cap R) \neq (0)$ и $Z(I \cap R) \subseteq Z(R)$. Поэтому I содержит обратимый элемент из поля $Z \cdot Z^{-1} \subseteq R \cdot Z^{-1}$ и, следовательно, $I = RZ^{-1}$. Это доказывает, что RZ^{-1} – простая F-алгебра с центром $Z \cdot Z^{-1}$, являющимся полем. Поэтому RZ^{-1} – примитивная PI-алгебра. По теореме 4.4

$$RZ^{-1} = M_k(D),$$

где D – тело и

$$\dim_{Z \cdot Z^{-1}} RZ^{-1} = n^2.$$

При этом, если K – максимальное подполе тела D, то

$$R \otimes_{Z \cdot Z^{-1}} K = M_n(K).$$

Обозначив через $M_n = T(M_n(F))$ – идеал тождеств алгебры $M_n(F)$. Тогда, учитывая, что все T-идеалы порождаются полилинейными многочленами, имеем, что $T(R) = M_n$. □

Следствие 4.6. *Пусть R – PI-алгебра без делителей нуля. Тогда ее центр $Z = Z(R) \neq (0)$ и R-подалгебра центрального кольца частных RZ^{-1}, которое является телом n^2-мерным над своим центром $Z \cdot Z^{-1}$ и идеалы тождеств R и тела RZ^{-1} совпадают и равны M_n.*

□ Из теоремы 4.7 следует, что $RZ^{-1} = M_k(D)$, где D – тело. Если $k \geq 2$, то $e_{12} = az^{-1}$, где $a \in R$, $z \in Z$. Тогда $a^2 = 0$ и $a = 0$. Противоречие. Следовательно, $k = 1$ и $RZ^{-1} = D$ – тело

n^2-мерное над своим центром $Z \cdot Z^{-1}$. Из теоремы 4.7 следует, что $T(R) = T(D) = T(M_n(F))$. $\square$

Пусть Q – T-идеал $F\langle X\rangle$. Алгебра $F\langle X\rangle/Q$ называется *приведенно свободной.*

Предложение 4.13. *Пусть R – счетно порожденная PI-алгебра, Q – T-идеал свободной алгебры $F\langle X\rangle$ и $Q \subseteq T(R)$. Тогда R – гомоморфный образ приведенно свободной алгебры $F\langle X\rangle/Q$.*

$\square$ Пусть алгебра R порождается элементами $\{a_1, a_2, \ldots\}$. Тогда отображение

$$\varphi : F\langle X\rangle \to R$$

такое, что

$$\varphi\left(f(x_1, \ldots, x_d)\right) = f(a_1, \ldots, a_d)$$

является сюръективным гомоморфизмом алгебры $F\langle X\rangle$ на алгебру R. Его ядро $\operatorname{Ker}\varphi$ содержит идеал тождеств $T(R)$. Так как $Q \subseteq T(R) \subseteq \operatorname{Ker}\varphi$, то φ индуцирует сюръективный гомоморфизм $\bar{\varphi} : F\langle X\rangle/Q \to R$. $\square$

Предложение 4.14. *Пусть Q – T-идеал свободной алгебры $F\langle X\rangle$. Тогда радикал Джекобсона $J(F\langle X\rangle/Q)$ является нильидеалом в $F\langle X\rangle/Q$.*

$\square$ Пусть $\overline{f(x_1, \ldots, x_d)}$ – произвольный элемент из $J(F\langle X\rangle/Q)$. Тогда $\overline{f(x_1, \ldots, x_d) \cdot x_{d+1}} \in J(F\langle X\rangle/Q)$. Пусть $\bar{q}$ – правый квазиобратный элемент к $\overline{f(x_1, \ldots, x_d) \cdot x_{d+1} \cdot q}$. Тогда

$$\overline{f(x_1, \ldots, x_d)x_{d+1} + q + f(x_1, \ldots, x_d) \cdot x_{d+1}} = \bar{0}.$$

Пусть

$$q = \sum_{i=0}^{m} q_i \in F\langle X\rangle,$$

где q_i – сумма одночленов в q степени i относительно переменной x_{d+1} и $p = f(x_1, \ldots, x_d)x_{d+1}$. Тогда

$$q \equiv -p - pq \equiv -p + p^2 + p^2 q \equiv \ldots$$
$$\ldots \equiv -p + p^2 - p^3 + \ldots \pm p^{m+1} \pm p^{m+1} q (\operatorname{mod} Q).$$

Согласно предложению 4.3 Q содержит однородные компоненты, то есть $p^{m+1} \in Q$ и $\bar{p}^{m+1} = \bar{0}$ в алгебре $F\langle X\rangle/Q$. □

Предложение 4.15. *Пусть Q – идеал тождеств полупервичной PI-алгебры R. Тогда приведенно свободная алгебра $F\langle X\rangle/Q$ является полупростой.*

□ Пусть $\overline{f(x_1,\ldots,x_d)} \in J(F\langle X\rangle/Q)$. Из предложения 4.14 следует, что существует целое число $m \geq 1$ такое, что

$$(f(x_1,\ldots,x_d)x_{d+1})^m = 0$$

– тождество в алгебре R. Пусть $a_1,\ldots,a_d$ – произвольные элементы алгебры R. Тогда правый идеал $f(a_1,\ldots,a_d)R$ является локально нильпотентным (см. главу 2) и, следовательно,

$$f(a_1,\ldots,a_d)R \subseteq \ln R.$$

Так как R – полупервичная алгебра, то $f(a_1,\ldots,a_d) = 0$ и $f(x_1,\ldots,x_d) \in Q$, то есть $J(F\langle X\rangle/Q) = (\bar{0})$. □

Предложение 4.16. *Пусть Q – T-идеал $F\langle X\rangle/Q$ и*

$$J(F\langle X\rangle/Q) = P/Q,$$

где $P \lhd F\langle X\rangle$ и $Q \subseteq P$. Тогда P – T-идеал алгебры $F\langle X\rangle$.

□ Обозначим через T_1 идеал тождеств в $F\langle X\rangle$ алгебры $F\langle X\rangle/P$. Алгебра $F\langle X\rangle/P$ является полупервичной. По предложению 4.15 $F\langle X\rangle/T_1$ – полупростая алгебра. Так как $Q \subseteq T_1 \subseteq P$ и $P/T_1 \subseteq J(F\langle X\rangle/T_1)$, то $P \subseteq T_1$ и $P = T_1$ – T-идеал алгебры $F\langle X\rangle$. □

Пусть $M_n = T(M_n(F))$, где $n \geq 0$. Тогда

$$F\langle X\rangle = M_\circ \supset M_1 \supset M_2 \supset M_3 \supset \ldots$$

и согласно предложению 4.15 $F\langle X\rangle/M_n$ – полупростая алгебра, $n \geq 1$.

Предложение 4.17. *Пусть Q – T-идеал $F\langle X\rangle$. Приведенно свободная алгебра $F\langle X\rangle/Q$ является полупростой тогда и только тогда, когда $Q = M_n$ для некоторого числа $n \geq 1$.*

□ Для доказательства предложения достаточно проверить, что если $F\langle X\rangle/Q$ – полупростая алгебра, то $Q = M_n$ для некоторого числа $n \geq 1$. Алгебра $F\langle X\rangle/Q$ является подпрямой суммой примитивных PI-алгебр R_α, $\alpha \in 1$. Каждая алгебра R_α, $\alpha \in 1$, является простой алгеброй, размерность которой над своим центром Z_α не превосходит $[d/2]^2$, где d – степень некоторого многочлена из Q. Ранее мы отмечали, что $T(R_\alpha) = M_{n_\alpha}$, где $n_\alpha \leq [d/2]$. Пусть $n = \max\{n_\alpha | \alpha \in \wedge\}$. Тогда $T(F\langle X\rangle/Q) = M_n = Q$. □

Из предложений 4.14, 4.16, 4.17 следует, что если Q – произвольный T – идеал $F\langle X\rangle$, то

$$J(F\langle X\rangle/Q) = M_n/Q = \ln(F\langle X\rangle/Q)$$

(если $n = 0$, то $M_0 = F\langle X\rangle$).

Так как $S_{2n} \in M_n$, то Q содержит некоторую степень стандартного тождества S_{2n}. Таким образом, мы получим второе доказательство следствия 4.5.

Предложение 4.18.

1. $\bigcap\limits_{n=1}^{\infty} M_n = (0)$.
2. *$F\langle X\rangle$ – подпрямая сумма алгебр изоморфных $M_n(F)$, где $n = 1, 2, \ldots$.*

□ Пусть $f(x_1, \ldots, x_d)$ – ненулевой многочлен степени m из $\bigcap\limits_{n=1}^{\infty} M_n$. Тогда согласно предложению 4.2 T-идеал $\bigcap\limits_{n=1}^{\infty} M_n$ содержит ненулевой полилинейный многочлен g степени m. В частности, M_m содержит g. Из предложения 4.11 и теоремы 4.1 следует, что минимальная степень полилинейного тождества в кольце $M_m(F)$ равна $2m$. Противоречие.

Пусть $\wedge_n$ – множество всех гомоморфизмов алгебры $F\langle X\rangle$ на $M_n(F)$. Тогда

$$M_n = \bigcap_{\lambda\in\wedge_n} \operatorname{Ker}\lambda$$

и

$$F\langle X\rangle / M_n = \sum_{\lambda\in\wedge_n} \bigoplus_s A_\lambda,$$

где $A_\lambda \cong M_n(F)$. Так как $\bigcap\limits_{n=1}^{\infty} M_n = (0)$, то $F\langle X\rangle$ – подпрямая сумма алгебр изоморфных $M_n(F)$, где $n = 1, 2, 3, \ldots$. $\square$

Предложение 4.19. *Пусть n – натуральное число. Тогда существует тело D, являющееся F-алгеброй и такое, что размерность D над центром Z равна n^2.*

$\square$ Пусть $K = F(\xi_1, \ldots, \xi_n, y)$ – чисто трансцендентное расширение поля F с базисом трансцендентности $\{\xi_1, \ldots, \xi_n, y\}$. Рассмотрим автоморфизм $\varphi : K \to K$ такой, что $\varphi(\xi_i) = \xi_{i+1}$, $i \le n-1$, $\varphi(\xi_n) = \xi_1$, $\varphi(y) = y$ и $\varphi(a) = a$, если $a \in F$. Тогда $\varphi^n = \epsilon$ – тождественный автоморфизм K. Пусть

$$R = K[t;\varphi] = \left\{ \sum_{i=0}^{m} t^i a_i \;\middle|\; a_i \in K,\ at = t\varphi(a) \right\}$$

– алгебра косых многочленов от переменной t. Так как $\varphi^n = \varepsilon$, то многочлен $t^n - y$ принадлежит центру алгебры R. Покажем, что он является неприводимым в R. Предположим противное. Тогда имеет место равенство

$$(t^n - y)\, g = (p_0 + tp_1 + \ldots + t^r p_r)(q_0 + tq_1 + \ldots + t^s q_s),$$

где $g, p_i, q_i \in F[\xi_1, \ldots, \xi_n, y]$ и y не является делителем всех p_i и q_i. Пусть y делит p_k, q_h и не делит $p_0, \ldots, p_{k-1}$, $q_0, \ldots, q_{h-1}$. Тогда $\varphi^m(p_j)$ делится на y при $j < k$ и не делится на y при $j = k$. Следовательно, коэффициент правой части равенства при t^u, $u < k+h$, делится на y, а коэффициент при t^{k+h} не делится

на y. Поэтому $k+h=n$, y не делит g, $k=r$ и $h=s$. С другой стороны, $yg=p_0q_0$ делится на y^2. Противоречие доказывает, что либо $r=0$, либо $s=0$ и t^n-y – неприводимый многочлен.

Пусть (t^n-y) – идеал в алгебре R, порожденный многочленом t^n-y. Рассмотрим алгебру $D=R/(t^n-y)$. Так как t^n-y – неприводимый многочлен, то D – кольцо без делителей нуля. Обозначим через

$$Z=\{h\in K|\ \varphi(h)=h\}$$

– подполе K, состоящее из элементов неподвижных относительно автоморфизма φ. По теореме Артина (см. [15], с. 22) размерность поля $\dim_Z K=n$. Поле Z содержится в центре алгебры D и $\dim_Z D=n^2$. Так как D – конечномерная Z-алгебра без делителей нуля, то D – алгебра с делением.

Докажем, наконец, что $Z(D)=Z$. Пусть

$$p(t)=\bar{a}_0+t\bar{a}_1+\ldots+t^{n-1}\bar{a}_{n-1}\in Z(D).$$

Тогда

$$\bar{0}=[p(t),t]=t\left(\overline{\varphi(a_0)}-\overline{a}_0\right)+\ldots$$
$$\ldots+t^{n-1}\left(\overline{\varphi(a_{n-2})}-\overline{a_{n-2}}\right)+y\left(\overline{\varphi(a_{n-1})}-\overline{a_{n-1}}\right).$$

Откуда следует, что $\varphi(a_i)=a_i$, $i\le n-1$ и, следовательно, $a_i\in Z$. Далее,

$$\bar{0}=[p(t),\xi_1]=t\bar{a}_1(\bar{\xi}_1-\bar{\xi}_2)+\ldots+t^{n-1}\bar{a}_{n-1}(\bar{\xi}_1-\bar{\xi}_{n-1}).$$

Откуда следует, что $\bar{a}_1=\bar{a_2}=\ldots=\bar{a}_{k-1}=\bar{0}$, то есть $Z(D)=Z$. Таким образом, D – алгебра с делением, размерность которой над центром Z, содержащим поле F равна n^2. $\square$

Заметим, что если A – произвольная PI-алгебра над полем F характеристики нуль и K – поле, содержащее F, то идеалы тождеств (в $F\langle X\rangle$) алгебр A и $A\otimes_F K$ совпадают, так как они порождаются полилинейными многочленами.

Теорема 4.8 (С. Амицур).
Приведенно свободная алгебра $F\langle X\rangle/M_n$ не содержит делителей нуля.

□ Пусть $f(x_1,\ldots,x_d)$ и $g(x_1,\ldots,x_d)$ многочлены из $F\langle X\rangle$ такие, что

$$f(x_1,\ldots,x_d)g(x_1,\ldots,x_d)\in M_n.$$

Тогда $f\cdot g=0$ – тождество в алгебре $D\otimes_Z L\cong M_n(L)$, где D – тело, размерность которого над центром Z равна n^2 и L – его максимальное подполе (см. предложение 4.19). Пусть $a_1,\ldots,a_d$ – произвольные элементы из D. Тогда

$$f(a_1,\ldots,a_d)g(a_1,\ldots,a_n)=0.$$

Следовательно, либо $f(a_1,\ldots,a_d)=0$, либо $g(a_1,\ldots,a_n)=0$. Пусть $b\in D$. Тогда $f(a_1,\ldots,a_d)bg(a_1,\ldots,a_d)=0$ и

$$f(x_1,\ldots,x_d)x_{d+1}f(x_1,\ldots,x_d)=0$$

– тождество в алгебре D, а, следовательно, в алгебре $M_n(F)$.

Рассмотрим поле рациональных функций

$$E=F\left(t_{ij}^k\right),$$

где $1\le k\le d+1$, $1\le i,j\le n$. Алгебра

$$M_n(E)=M_n(F)\otimes_F E$$

удовлетворяет тождеству

$$f(x_i)x_{d+1}g(x_i)=0.$$

Положим $x_k=t_k=\left(t_{ij}^k\right)$, $k\le d$. Тогда

$$f(t_1,\ldots,t_d)M_n(E)g(t_1,\ldots,t_d)=0.$$

Так как $M_n(E)$ – первичная алгебра, то, например,

$$f(t_1,\ldots,t_d)=\left(f_{ij}\left(t_{\alpha\beta}\right)^k\right)=0 \text{ и } f_{ij}\left(t_{\alpha\beta}^k\right)=0.$$

Следовательно, $f_{ij}\left(a^k_{\alpha\beta}\right) = 0$ при любой специализации $t^k_{\alpha\beta} = a^k_{\alpha\beta} \in F$. Следовательно, $f(x_1, \ldots, x_d) = 0$ – тождество алгебры $M_n(F)$ и $f \in M_n$. $\square$

Следствие 4.7. *Пусть PI-алгебра R удовлетворяет тождеству*

$$f(x_1, \ldots, x_d)g(x_1, \ldots, x_d) = 0.$$

Тогда R удовлетворяет одному из тождеств $f^m(x_i) = 0$ или $g^m(x_i) = 0$ для некоторого целого числа $m \geq 1$.

$\square$ Пусть $T(R)$ – идеал тождеств алгебры R в свободной алгебре $F\langle X\rangle$. Тогда радикал Джекобсона приведенно свободной алгебры $F\langle X\rangle/T(R)$ равен $M_n/T(R)$ и является ниль-идеалом. Так как $f(x_i) \cdot g(x_i) \in T(R)$, то $f \cdot g \in M_n$. По теореме 4.8 либо $f \in M_n$, либо $g \in M_n$. Если, например, $f \in M_n$, то $f + T(R)$ – нильпотентный элемент в $F\langle X\rangle/T(R)$. Следовательно, существует целое число $m \geq 1$ такое, что $f^m \in T(R)$. $\square$

4.4. Теорема Ширшова о высоте и проблема Куроша

Теорема 4.9. *Пусть R – PI-алгебра над полем F и S – нильподполугруппа $\langle R, \cdot\rangle$ такая, что $R = F[S]$. Тогда R – локально нильпотентная алгебра.*

$\square$ Пусть $L(R)$ – локально нильпотентный радикал алгебры R. Рассмотрим алгебру $\bar{R} = R/L(R)$. Данная алгебра удовлетворяет полилинейному тождеству степени d

$$f(x_1, \ldots, x_d) = x_1x_2 \ldots x_d + \sum_{(i)\neq(1)} \alpha_{(i)}x_{i_1} \ldots x_{i_d} = 0.$$

Методом математической индукции относительно числа d докажем, что $\bar{R} = \bar{0}$. Если $d \leq 2$, то $\bar{R}$ удовлетворяет тождеству $x_1x_2 = \alpha x_2x_1$. Пусть A – конечнопорожденная подалгебра в

$\bar{R}$. Тогда можно считать, что $A = F[s_1, \ldots, s_n]$, где $s_i \in \bar{S}$, $i \leq n$. Если $s_1^m = s_2^m = \cdots = s_n^m = \bar{0}$, то, используя тождество $x_1x_2 = \alpha x_2x_1$, легко видеть, что $A^{nm} = \bar{0}$. Это означает, что $L(\bar{R}) = \bar{R}$. С другой стороны, $L\big(R/L(R)\big) = \bar{0}$. Таким образом, $\bar{R} = \bar{0}$ и $R = L(R)$.

Сделаем предположение индукции об истинности нашего утверждения для алгебр, удовлетворяющих тождеству степени не более $d-1$. Если $\bar{R} \neq (\bar{0})$, то среди элементов полугруппы $\bar{S} = S + L(R)/L(R)$ найдется элемент a такой, что $a \neq \bar{0}$, $a^2 = \bar{0}$. Рассмотрим правый идеал $I = a\bar{R}$ и перепишем наше тождество в виде

$$f = x_1 f_1(x_2, \ldots, x_d) + f_2(x_1, \ldots, x_d),$$

где f_2 – сумма одночленов, не начинающихся с x_1. Для любых элементов $b_1, \ldots, b_d \in \bar{R}$ имеем равенство

$$f(b_1, ab_2, \ldots, ab_d) = b_1 f_1(ab_2, \ldots ab_d) + a \cdot c = \bar{0},$$

где $c \in \bar{R}$. Умножая это равенство слева на a, получим, что

$$ab_1 f_1(ab_2, \ldots, ab_d) = 0,$$

откуда следует, что алгебра $a\bar{R}/a\bar{R} \cap r(a\bar{R})$ порождается нильподполугруппой $a\bar{S}$ и удовлетворяет полилинейному тождеству $f_1(x_2, \ldots, x_d) = 0$ степени $d-1$, один из коэффициентов которого равен 1. По предложению индукции,

$$L\big(a\bar{R}/a\bar{R} \cap r(a\bar{R})\big) = a\bar{R}/a\bar{R} \cap r(a\bar{R}).$$

Так как

$$(a\bar{R} \cap r(a\bar{R}))^2 = \bar{0},$$

то $a\bar{R}$ является расширением локально нильпотентной алгебры с помощью локально нильпотентной алгебры, то есть сама является локально нильпотентной. Это означает, что $a\bar{R} = L(a\bar{R}) \subseteq L(\bar{R}) = \bar{0}$, откуда следует, что $l(\bar{R}) = \{x \in \bar{R} |\ x\bar{R} = \bar{0}\}$ – ненулевой двусторонний идеал с нулевым умножением, поэтому $l(\bar{R}) \subseteq L(\bar{R})$ и $L(\bar{R}) \neq (\bar{0})$. Противоречие. $\square$

Следствие 4.8. *Пусть R – нильалгебра над полем F, удовлетворяющая тождеству. Тогда R – локально нильпотентная алгебра.*

Доказательство следует из теоремы 4.9 при $S = R$.

Следствие 4.9. *Пусть алгебра R удовлетворяет тождеству $x^n = 0$. Тогда R – локально нильпотентная алгебра.*

Пусть R – алгебра над полем F. Элемент $a \in F$ называется *алгебраическим над полем F*, если существует ненулевой многочлен $f(t) \in F[t]$ такой, что $f(a) = 0$. R называется *алгебраической алгеброй*, если каждый ее элемент является алгебраическим. R называется *локально конечной алгеброй*, если каждая ее конечно порожденная подалгебра является конечномерной.

В 1941 г. А. Курош сформулировал следующую проблему (см. [45]): будет ли всякая алгебраическая алгебра локально конечной? В главе 2 указан пример Е. Голода, отрицательно решающий проблему А. Куроша даже в классе нильалгебр. В настоящем параграфе мы дадим положительное решение проблемы А. Куроша в классе алгебраических PI-алгебр, принадлежащее И. Капланскому (США).

Теорема 4.10. *Пусть R – ассоциативная алгебра над полем F, удовлетворяющая полилинейному тождеству степени d*

$$f = x_1 x_2 \dots x_d + \sum_{(i)\neq(1)} \alpha_{(i)} x_{i_1} x_{i_2} \dots x_{i_d} = 0.$$

Пусть $R = F[S]$ порождается полугруппой $\langle S, \cdot \rangle$, каждый элемент которой является алгебраическим над F. Тогда R – локально конечная алгебра, то есть каждая ее конечнопорожденная подалгебра является конечномерной.

□ Пусть A – конечнопорожденная подалгебра R. Тогда можно считать, что $A = F[a_1, \dots, a_m]$, где $\{a_1, \dots, a_m\} \subseteq S$. Рассмотрим свободную ассоциативную алгебру $F\langle x_1, \dots, x_m \rangle$ и в

ней идеал T, порожденный элементами $f(w_1, w_2, \ldots, w_d)$, где w_i – слова от $x_1, \ldots, x_m$. Для каждого слова $w = x_{i_1} \ldots x_{i_k}$ элемент $w(a) = a_{i_1} \ldots a_{i_k} \in S$ является алгебраическим. Пусть $n(w) = \deg f_{w(a)}$, где $f_{w(a)}(t) \in F[t]$, $f_{w(a)}(w(a)) = 0$, и пусть I – идеал алгебры $F\langle x_1, \ldots, x_m\rangle$, порожденный словами $w^{n(w)}$. Идеалы T и I являются однородными. Следовательно, сумма $T + I = J$ тоже является однородным идеалом в $F\langle x_1, \ldots, x_m\rangle$.

Рассмотрим фактор-алгебру $F\langle x_1, \ldots, x_m\rangle/J$. Она удовлетворяет всем условиям теоремы 4.9. Поэтому эта фактор-алгебра является нильпотентной, например, индекса t, откуда следует, что $F\langle x_1, \ldots, x_m\rangle^t \subseteq J$. Из последнего включения следует, что векторное пространство A натянуто на слова $a_{i_1} a_{i_2} \ldots a_{i_k}$, где $k \leq (t-1)$. Действительно, любое слово t от образующих $a_{i_1} a_{i_2} \ldots a_{i_t}$ можно представить в виде

$$\sum u(a_i) f(w_1, \ldots, w_d) v(a_i) + \sum (a_i) w^{n(w)} q(a_i),$$

где каждое слагаемое имеет степень t относительно $\{a_1, \ldots, a_m\}$ (в силу однородности идеала J). Так как $f(w_1, \ldots, w_d) = 0$ в A и $w^{n(w)} = \sum\limits_{j<n} \alpha_j w^j$, то $a_{i_1} \ldots a_{i_t}$ является линейной комбинацией слов меньшей длины. $\square$

Следствие 4.10. *Если R – алгебраическая алгебра над полем, удовлетворяющим полилинейному тождеству вида*

$$x_1 x_2 \ldots x_d + \sum_{(i)\neq(1)} \alpha_{(i)} x_{i_1} x_{i_2} \ldots x_{i_d} = 0,$$

то R – локально конечная алгебра.

Доказательство следует из теоремы 4.10, при $S = R$.

Следствие 4.11. *Пусть R – ассоциативная алгебра над полем F, удовлетворяющая тождеству и содержащая единицу. Если G – периодическая группа, вложимая в $\langle R, \cdot\rangle$, то G – локально конечная группа.*

□ Пусть $H = \langle g_1, \ldots, g_n \rangle$ – конечнопорожденная подгруппа G и $A = F[H]$ – конечнопорожденная подалгебра R. Так как H – периодическая группа, то каждый элемент $h \in H$ является алгебраическим ($f_h(x) = x^m - 1$ для некоторого целого числа $m \geq 1$). По теореме 4.10, A – конечномерная алгебра. Используя регулярное представление, можно считать, что A – подалгебра алгебры матриц $M_N(F)$. Следовательно, H – конечнопорожденная периодическая подгруппа $M_N(F)$. По теореме Бернсайда (см. [22]), H – конечная группа. □

Пусть w и v – элементы свободной полугруппы $\langle x_1, \ldots, x_k \rangle$. Скажем, что w и v имеют *одинаковый состав*, если каждая переменная x_i входит в w и v одинаковое число раз.

Перейдем к так называемой "теореме о высоте".

Теорема 4.11 (А. Ширшов).
Пусть R – ассоциативная алгебра над полем F, удовлетворяющая полилинейному тождеству степени n, и $a_1, \ldots, a_k \in R$. Тогда существует натуральное число $h = h(n, k)$ такое, что произвольное слово w от $\{a_1, \ldots, a_k\}$ представимо в виде линейной комбинации

$$w = \sum \alpha v_1^{k_1} v_2^{k_2} \ldots v_h^{k_h},$$

где $\alpha \in F, v_i$ – слова от $\{a_1, \ldots a_k\}$ длины $\leq n$ (включая пустое слово) и каждое слагаемое правой части имеет одинаковый состав с w.

Следствие 4.12. *Пусть $R = F\langle a_1, \ldots, a_k \rangle$ – k-порожденная алгебра над полем F, удовлетворяющая тождеству степени n. Если существует натуральное число m такое, что каждое слово v от $\{a_i\}$ длины $\leq n$ нильпотентно индекса m, то есть $v^m = 0$, то R – нильпотентная алгебра индекса не более*

$$n(m-1)h(n,k) + 1.$$

□ Действительно, пусть w – слово длины $n(m-1)h(n,k)+1$ от образующих $\{a_1, \ldots, a_k\}$. По теореме о высоте, w является

линейной комбинацией слов вида $v_1^{k_1} \dots v_h^{k_h}$, имеющих тот же состав, что и w. Если $k_i \geq m$, то по условию $v_i^{k_i} = 0$. Следовательно, если $w \neq 0$, то в одном из слагаемых указанного вида

$$k_1 \leq (m-1),\ \dots,\ k_h \leq (m-1),$$

откуда следует, что его длина $\leq n(m-1)h$. Противоречие. $\square$

Следствие 4.13. *Пусть $R = F\langle a_1, \dots, a_k\rangle$ – k-порожденная алгебра, удовлетворяющая тождеству степени n. Если каждое слово w от $\{a_i\}$ длины $\leq n$ является алгебраическим элементом над F, то R – конечномерная F-алгебра.*

$\square$ Множество слов от $\{a_i\}$ длины $\leq n$ является конечным. Каждое такое слово v является алгебраическим, то есть $dim_F F[v] = m_v < \infty$. Пусть

$$m = \max\{m_v |\ v \text{ – слово длины } \leq n \text{ от } \{a_1, \dots, a_k\}\}.$$

По теореме Ширшова, векторное пространство R порождается элементами вида $v_1^{k_1} \dots v_h^{k_h}$, где v_i – слова от $\{a_1, \dots, a_k\}$ длины $\leq n$. Так как векторы $v_i, v_i^2, \dots, v_i^{m+1}$ являются линейно зависимыми, то можно считать, что $k_1 \leq m, \dots, k_h \leq m$. Таким образом, R – конечнопорожденное векторное пространство и $dim_F R < \infty$. $\square$

Следующее изложение доказательства теоремы Ширшова принадлежит Е. Зельманову и А. Белову (см. [119]). В процессе доказательства будет найдена оценка $h(n,k)$.

Рассмотрим конечный упорядоченный алфавит

$$X = \{x_1, x_2, \dots, x_k\},\quad x_k > x_{k_1} > \dots > x_2 > x_1.$$

Определим (частичный) лексикографический порядок на множестве всех непустых слов в алфавите X следующим образом. Пусть $v = x_{i_1} \dots x_{i_s}$ и $w = x_{j_1} \dots x_{j_t}$. Положим, $v < w$, если $i_1 < j_1$, либо существует такой индекс $q \leq s$, что

$$i_1 = j_1,\ i_2 = j_2,\ \dots,\ i_{q-1} = j_{q-1},\ i_q < j_q.$$

Данное определение позволяет сравнивать любые два слова, не являющиеся началом друг друга. В частности, любые два слова одинаковой длины (и тем более одинакового состава) являются сравнимыми.

Если $R = F\langle a_1, \ldots, a_k\rangle$ – k-порожденная алгебра и $w = x_{i_1} \ldots x_{i_s}$, то $w(a) = a_{i_1} \ldots a_{i_s}$ – *значение слова* w в R. Скажем, что слово w является *неприводимым*, если $w(a)$ не представимо в виде

$$w(a) = \sum \alpha_i w_i(a),\ \alpha_i \in F,$$

где w_i – слова одинакового состава с w и лексикографически строго меньшие w. Ясно, что каждое слово $w(a)$ является линейной комбинацией неприводимых слов, имеющих тот же состав.

Слово w назовем *n-разбиваемым*, если

$$w = uw_1w_2 \ldots w_nv,$$

где $w_1, \ldots, w_n$ – непустые слова такие, что

$$w_1w_2 \ldots w_n > w_{\sigma(1)} \ldots w_{\sigma(n)}$$

для любой нетождественной перестановки σ.

Заметим, что если алгебра удовлетворяет полилинейному тождеству степени n, то она не содержит n-разбиваемых неприводимых слов, ибо каждое такое слово $w = uw_1 \ldots w_nv$ можно представить в виде линейной комбинации меньших слов, пользуясь тождеством

$$x_1x_2 \ldots x_n = \sum_{\sigma \neq 1} \alpha_\sigma x_{\sigma(1)} \ldots x_{\sigma(n)},$$

$$w(a) = \sum \alpha_\sigma uw_{\sigma(1)} \ldots w_{\sigma(n)}v.$$

Скажем, что слово v является *началом (концом) слова* w, если $w = v \cdot u$ (соответственно, $w = u \cdot v$).

Лемма 4.9. *Пусть слово v является началом и концом слова w, то есть $w = v \cdot u' = u \cdot v$. Тогда для любого целого числа $m \geq 1$*

$$w(u')^{m-1} = u^m v.$$

В частности, w – начало некоторой степени слова u.

□ Доказательство проведем методом математической индукции. Если $m = 1$, то $w = u \cdot v$. Предположим, что

$$w(u')^{m-1} = u^m \cdot v.$$

Рассмотрим $w(u')^m = w(u')^{m-1} \cdot u' = (u^m \cdot v)u' = u^m(vu') = u^m(u \cdot v) = u^{m+1}v$. □

Пусть $w = x_{i_1} \dots x_{i_m}$ – слово длины m и $m \geq n$. Слово w назовем *совместным*, если слова

$$w_1 = w,\ w_2 = x_{i_2} \dots x_{i_m},\ \dots,\ w_n = x_{i_n} x_{i_{n+1}} \dots x_{i_m}$$

сравнимы между собой, то есть ни одно из них не является началом другого.

Лемма 4.10. *Пусть w – неприводимое слово. Тогда оно не представимо в виде*

$$w = v_1 u v_2 u \dots v_n u v_{n+1},$$

где u – совместное слово.

□ Предположим противное, то есть $w = v_1 u v_2 u \dots u v_{n+1}$, где u – совместное слово. Обозначим через $u_1, u_2, \dots, u_n$ n концов слова u, сравнимых между собой, например, следующим образом:

$$u_{i_1} > u_{i_2} > \dots > u_{i_n}.$$

Перепишем w в виде

$$w = v_1' u_{i_1} v_2' u_{i_2} v_3' \dots u_{i_n} v_{n+1}'.$$

Тогда

$$u_{i_1} v_2' > u_{i_2} v_3' > \dots > u_{i_n} v_{n+1}'$$

и w – n-разбиваемое слово. □

Лемма 4.11. *Пусть w – несовместное слово. Тогда w можно представить в виде*

$$w = v'u^s v'',$$

где $(v'u)$ – слово длины меньшей n, а v'' – собственное начало слова u (в частности, длина слова u меньше n).

□ Так как w – несовместное слово, то существуют два его конца $w_r = x_{i_r} \dots x_{i_m}$ и $w_t = x_{i_t} \dots x_{i_m}$, $r < t \leq n$, которые несравнимы. Это означает, что w_t – начало w_r, то есть $w_r = w_t u'$. С другой стороны, $w_r = u \cdot w_t$, где $u = x_{i_r} \dots x_{i_{t-1}}$. По лемме 4.9 w_r – начало некоторой степени слова u. Следовательно, $w_r = u^s \cdot v''$, где v'' – собственное начало u, откуда следует, что $w = v'u^s v''$, где $v' = x_{i_1} \dots x_{i_{r-1}}$ и длина слова $v'u = x_{i_1} \dots x_{i_{t-1}}$ строго меньше n. □

Лемма 4.12. *Если все слова от образующих $\{a_1, \dots, a_k\}$ длины меньшей n являются нильпотентными индекса $\leq d$, то каждое слово w длины большей или равной $(n-1)d$ является либо совместным, либо его значение $w(a) = 0$.*

□ Если w – несовместное слово, то, по лемме 4.11, $w = v'u^s v''$, где либо $w(a) = 0$, либо $s \leq (d-1)$. Длина $v'u$ не превосходит $(n-1)$, а длина u^{s-1} не превосходит $(n-1)(d-2)$. Так как v'' – слово, длина которого не превосходит $(n-2)$, то длина w не должна превосходить $d(n-1)-1$. Противоречие доказывает следствие. □

Слово $w = x_{i_1} \dots x_{i_m}$, $m \geq n$, называется *вполне совместным*, если w – совместное слово и либо $m = n$, либо $m > n$ и слово $x_{i_1} x_{i_2} \dots x_{i_{m-1}}$ не является совместным.

Лемма 4.13.

1. *Каждое совместное слово имеет вполне совместное начало.*

2. *Каждое вполне совместное слово w может быть представлено в виде $w = v'u^s v'' x_i$, где $v'u$ – слово длины меньшей n, а v'' – собственное начало слова u.*

□ Пусть $w = x_{i_1} \dots x_{i_m}$ – совместное слово. Если $x_{i_1} x_{i_2} \dots x_{i_n}$ – совместное слово, то оно является вполне совместным началом w. Если же оно несовместное, то существует такое число s, что $n < s \leq m$, $v = x_{i_1} \dots x_{i_s}$ – совместное слово, а слово $v_{i_1} \dots v_{i_{s-1}}$ не является совместным. Слово v является искомым вполне совместным началом слова w. Второе утверждение леммы следует теперь из леммы 4.11. □

Лемма 4.14. *Пусть все слова от $\{a_1, \dots, a_k\}$, имеющие длину меньшую, чем n, являются нильпотентными индекса $\leq d$. Тогда число всех различных неприводимых вполне совместных слов меньше числа dn^2k^{n+1}.*

□ Пусть $w = v'u^s v'' x_i$ – вполне совместное неприводимое слово (см. лемму 4.13). Тогда $s \leq d-1$. Так как длина $(v'u)$ меньше n, то число всех таких слов меньше числа k^n. Каждое такое слово можно разделить на два подслова v' и u не более n способами. Число собственных подслов v'' не превосходит числа $n-1$, а число возможных букв x_i не превосходит k. Следовательно, число выборов вполне совместных слов w не превосходит числа $dk^n n(n-1)k$. □

Теорема 4.12 (А. Белов).
Пусть $R = F\langle a_1, \dots, a_k\rangle$ – k-порожденная алгебра над полем F, удовлетворяющая полилинейному тождеству степени n. Если каждое слово от образующих $\{a_1, \dots, a_k\}$, имеющее длину $< n$, является нильпотентным индекса $\leq d$, то алгебра R является нильпотентной индекса $\leq d^2 n^4 k^{n+1}$.

□ Докажем, что R – нильпотентная алгебра индекса не более

$$N = (n-1)d(n^2 dk^{n+1}(n-1) + 1).$$

Рассмотрим произвольное слово w длины N. Докажем, что $w(a) = 0$. Для этого достаточно предполагать, что w является неприводимым. В этом случае каждое подслово w тоже является неприводимым. Разобьем слово $w = w_1 w_2 \dots w_m$ на $m = n^2 dk^{n+1}(n-1)+1$ подслов $w_1, \dots, w_m$, каждое из которых имеет длину $(n-1)d$. По лемме 4.12, либо $w(a) = 0$, либо каждое слово w_i, $i \le m$, является совместным. По лемме 4.13, в каждом таком подслове w_i, $i \le m$, можно выбрать вполне совместное начало u_i. Пусть $w_i = u_i v_i$. По лемме 4.14, существует не более $dn^2 k^{n+1}$ различных вполне совместных слов. Так как $m > n^2 dk^{n+1}(n-1)$, то некоторое такое вполне совместное слово встречается в w не менее n раз, что противоречит лемме 4.10. $\square$

Скажем, что слово $w = x_{i_1} \dots x_{i_m}$ является *периодическим с периодом* t, $t < m$, если для любого числа $j \le m - t$ справедливы равенства

$$i_1 = i_{1+t},\ i_2 = i_{2+t},\ \dots,\ t_j = t_{j+t},\ \dots,\ i_{m-t} = i_m.$$

Под *бесконечным словом* мы понимаем бесконечную последовательность букв $w = x_{i_1} x_{i_2} \dots$. Бесконечное слово называется *периодическим с периодом* t, если для любого числа $j \ge 1$ справедливо $i_j = i_{j+t}$.

Лемма 4.15. *Пусть s и t – два периода бесконечного слова w. Тогда наибольший общий делитель (s,t) чисел s и t тоже является периодом слова w.*

$\square$ Пусть $t > s$. Докажем, что число $t - s$ тоже является периодом w. Действительно, для любого числа $j \ge 1$ имеем, что $i_j = i_{j+t} = i_{j+(t-s)}$. Применяя алгоритм Евклида, получим, что (s,t) – период слова w. $\square$

Заметим, что предыдущая лемма является неверной для слов конечной длины: как показывает пример слова $x_1 x_2 x_1$, числа 2 и 3 являются периодами его, но 1=(2,3) не является его периодом.

Обозначим через $l(w)$ длину слова w.

Лемма 4.16.

1. *Пусть u – слово, не представимое в виде $u = v^s$, $s > 1$ и не начинающееся с буквы x_i, тогда слово $u^n x_i$ является совместным.*

2. *Пусть слово u не представимо в виде $u = v^s$, $s > 1$ и не оканчивается на букву x_i, тогда слово $x_i u^n$ является совместным.*

3. *Пусть слово w содержит подслово вида v^n, где $l(v) < n$ и не содержит совместные слова $x_i u^n$, $u^n x_i$ из первых двух пунктов, где $l(u) < n$, тогда $w = u^s \cdot v'$, где $l(u) < n$, $n \leq s$ и v' – собственное начало слова u.*

□ Если $l(u) = 1$, то утверждение очевидно. Пусть $l(u) \geq 2$ и $w = u^n x_i = x_{i_1} x_{i_2} \dots x_{i_m}$. Если w не является совместным словом, то по лемме 4.11 существуют концы этого слова $w_s = x_{i_s} \dots x_{i_m}$ и $w_t = x_{i_t} \dots x_{i_m}$, $s < t \leq n$ такие, что w_s является началом некоторой степени слова $v = x_{i_s} \dots x_{i_{t-1}}$, откуда следует, что $l(v) = t - s$ – период слова w_s. Покажем далее, что $t - s$ является также периодом бесконечного слова $u^\infty = uuu \dots$. Возьмем две буквы в слове u^∞, расстояние между которыми равно $t - s$. Тогда они являются началом и концом подслова $\tilde{v}$ длины $t - s + 1$. Пусть v' – подслово u^∞ длины $s - 1$, которое лежит слева от $\tilde{v}$. Так как $t - s$ – период w_s, то достаточно доказать, что $\tilde{v}$ подслово w_s. Это будет следовать из того, что $v' \cdot \tilde{v}$ – подслово u^n. Подслово $v'\tilde{v}$ слова u^∞ представимо в виде $v'\tilde{v} = u_1 u^r u_2$, где u_1 – собственный конец, а u_2 – собственное начало слова u. Ясно, что $u_1 u^r u_2$ – подслово u^{r+2}. Если $r \geq n-1$, то

$$t \geq l(v'\tilde{v}) \geq (n-1)l(u) \geq 2(n-1) > n,$$

так как $n \geq 3$ (при $n = 2$ теорема Ширшова является очевидной). Противоречие доказывает, что $r \leq n - 2$ и $v'\tilde{v}$ – подслово u^n. Итак, $t - s$ – период u^∞. По лемме 4.15, наибольший

общий делитель чисел $t-s$ и $l(u)$ тоже является периодом бесконечного слова u^∞. Если собственный делитель $l(u)$ является периодом u, то $u = v^s$, где $s > 1$. Противоречие. Следовательно, $l(u)$ – делитель $t-s$ и $l(u)$ – период слова w_s, откуда следует, что $x_i = x_{i_m}$ – первая буква в слове u. Противоречие доказывает первое утверждение.

Второе утверждение доказывается аналогично.

Докажем третье утверждение. Согласно условию леммы, w содержит подслово вида v^s, где $l(v) < n$, $s \geq n$. Мы можем считать, что v не является степенью никакого собственного подслова. Запишем v в виде $v = v' \cdot x_i$. Тогда либо v^s является началом слова w, либо первая буква слева от v^s в w совпадает с x_i, либо, наконец, w содержит подслово типа 2. Рассмотрим второй случай. По условию

$$w = \dots x_i v^s \cdots = \dots (x_i v')^s x_i \dots .$$

Так как w не содержит подслов типа 2, то, рассуждая аналогично, мы через конечное число шагов представим слово w в виде $w = v^s \cdot w'$. Будем считать, что s – максимальное число с этим свойством, то есть v^{s+1} не является началом w. Пусть v' – максимальное начало слова w', которое является также началом слова v ($v = v' \cdot v''$). Если $v' \neq w'$ и x_i – первая буква w', расположенная справа от v', то

$$w = v^s \cdot (v' x_i \dots) = v' v'' v' v'' \dots v' v'' (v' x_i \dots) = v' (v'' v')^s x_i \dots .$$

Следовательно, w содержит подслово $(v''v')^n \cdot x_i$ типа 1. Противоречие доказывает, что $w = v^s \cdot v'$. $\square$

Слово w имеет *высоту* $h = h(w)$ относительно множества слов длины $< n$, если

$$w = v_1^{s_1} \dots v_h^{s_h},$$

где $l(v_i) < n$, $i \leq h$ и h – минимальное число с этим свойством. Если $w = w_1 w_2$, то

$$h(w) \leq h(w_1) + h(w_2).$$

Перейдем к доказательству теоремы о высоте.

□ Пусть w – неприводимое слово. Рассмотрим его представление в виде

$$w = v_0 u_1 v_1 u_2 \dots u_t v_t,$$

где каждое слово u_j принадлежит множеству слов $A = B \cup C$, где

$$B = \{u^n x_i |\ l(u) < n,\ x_i \text{ не является первой буквой } u\},$$

$$C = \{x_i u^n |\ l(u) < n,\ x_i \text{ не является последней буквой } u\}.$$

Так как мощность множества

$$|A| \leq 2k\frac{(k^n - 1)}{(k-1)}$$

и каждое слово из A является совместным (см. лемму 4.16), то каждое слово из A встречается не более $n-1$ раз, следовательно,

$$t \leq 2(n-1)(k^{n+1} - k).$$

Рассмотрим подслова v_j. Никакое из них не содержит подслов из множества A. Если длина некоторого слова v_j удовлетворяет неравенству

$$l(v_j) \geq N = n^2 \cdot n^4 \cdot k^{n+1},$$

то, в силу теоремы 4.12, v_j содержит подслово вида v^n, где $l(v) \leq n-1$. По лемме 4.16, высота $h(v_j) \leq 2$. Если $l(v_j) < N$, то $h(v_j) \leq N/_{(n-1)}$. Так как $h(u_j) \leq 2$, то

$$\begin{aligned} h(w) &\leq (t+1)\frac{N}{n-1} + 2t \leq \\ &\leq [2(n-1)(k^{n+1} - k) + 1]\frac{N}{n-1} + 2 \cdot 2(n-1)(k^{n+1} - k) < \\ &< 2(k^{n+1} - k)n^6 k^{n+1} + 4(n-1)(k^{n+1} - k) < 2k^{2(n+1)}n^6. \ \square \end{aligned}$$

В. Уфнаровский и Г. Чекану (1988 г., Институт математики, Кишинев) доказали, что если ассоциативная конечнопорожденная алгебра удовлетворяет тождеству степени n и все слова от образующих элементов длины $\leq [n/2]$ являются нильпотентными, то алгебра тоже является нильпотентной.

4.5. Радикал Джекобсона конечно порожденных PI-алгебр

В 1984 г. в работе А. Брауна [69] был доказан следующий выдающийся результат:

Пусть $R = \Phi\langle a_1, \ldots, a_n\rangle$ – конечно порожденная PI-алгебра над коммутативным нетеровым кольцом Φ с единицей. Тогда ниль-радикал алгебры R является нильпотентным идеалом.

В случае, когда Φ – поле характеристики нуль этот результат был доказан ранее Ю. Размысловым (МГУ, г. Москва) и А. Кемером (Ульяновский ГУ). Упрощенный вариант доказательства теоремы Размыслова-Кемера-Брауна содержится в препринте Львова И. (см. [46]).

В настоящем параграфе мы докажем теорему С. Амицура о совпадении радикалов $J(R) = \ln(R)$ для произвольной конечно порожденной PI-алгебры R над полем (см. [63, 64]).

Предложение 4.20. *Пусть $C = F\langle a_1, \ldots, a_n\rangle$ – конечно порожденная алгебра над полем F и*

$$C = Zb_1 + \ldots + Zb_m$$

– конечно порожденный модуль над F-подалгеброй Z из центра алгебры C. Тогда Z – конечно порожденная F-алгебра.

□ По условию

$$a_i = \sum_{j=1}^{m} z_{ij} b_j + \sum_{j=1}^{m} t_{ij} b_j,$$

где $z_{ij} \in Z$, $t_{ij} \in \mathbb{Z}$, $i \leq n$ и

$$b_i b_j = \sum_{s=1}^{m} \gamma_{ij}^s b_s + \sum_{s=1}^{m} p_{ij}^s b_s,$$

$1 \leq i, j \leq m$, где $\gamma_{ij}^s \in Z$, $p_{ij}^s \in \mathbb{Z}$. Пусть

$$Z_0 = F\left\langle z_{ij}, \gamma_{ij}^s \right\rangle$$

– конечно порожденная подалгебра Z. По теореме Гильберта о базисе Z_0 – нетерова F-алгебра и

$$C = Z_0 b_1 + \ldots Z_0 b_m$$

– конечно порожденный Z_0-модуль. Следовательно, C – нетеровый Z_0-модуль и Z – Z_0-подмодуль C. Поэтому

$$Z = Z_0 u_1 + \ldots + Z_0 u_k = F\left\langle z_{ij}, \gamma ij^s, u_i \right\rangle$$

– конечно порожденная F-алгебра. □

Следствие 4.14. *Пусть $E = F\langle a_1, \ldots, a_n\rangle$ – поле, являющееся конечно порожденной алгеброй над полем F. Тогда $\dim_F E < \infty$ (см. [15], с. 289).*

□ Если E – алгебраическое расширение поля F, то очевидно $\dim_F E < \infty$. Иначе, по теореме Штейница, существует подполе $P \subseteq E$, являющееся чисто трансцендентным расширением поля F и E – алгебраическое расширение поля P. Следовательно, $\dim_P E < \infty$. По предложению 4.20 $P = F\langle b_1, \ldots, b_s\rangle$ – конечно порожденная F-алгебра, являющаяся трансцендентным расширением, то есть

$$P = F(x_1, \ldots, x_m) = F\left\langle \frac{f_1(x_i)}{g_1(x_i)}, \ldots, \frac{f_s(x_i)}{g_s(x_i)} \right\rangle.$$

В кольце многочленов $F[x_1, \ldots, x_m]$ существует бесконечно много неприводимых многочленов (при $m \geq 1$). Пусть $q(x_1, \ldots, x_m)$ – неприводимый многочлен, не делящий $g_1(x_i)g_2(x_i)\ldots g_s(x_i)$. Тогда $\frac{1}{q}$ не принадлежит полю P. Противоречие доказывает, что $\dim_F E < \infty$. □

Теорема 4.13 (С. Амицур).
Пусть R – конечно порожденная алгебра над полем F характеристики нуль, удовлетворяющая тождеству. Тогда радикал Джекобсона $J(R)$ – сумма нильпотентных идеалов R.

□ Докажем сначала, что $J(R)$ совпадает с нижним ниль-радикалом $\mathrm{un}R$. Допустим противное. Тогда $R_1 = R/\mathrm{un}R$ – полупервичная алгебра, содержащая ненулевой квазирегулярный идеал $J_1 = J(R)/\mathrm{un}R$. Идеал J_1 является полупервичной алгеброй, так как если $aJ_1a = 0$ для некоторого элемента $a \in J_1$, то $(aJ_1)R_1(aJ_1) = 0$ и $aJ_1 = 0$ и $a \in l(J_1) \cap J_1$. Так как

$$(l(J_1) \cap J_1)^2 = (0)$$

и R_1 – полупервичная алгебра, то $l(J_1) \cap J_1 = (0)$ и $a = 0$. Итак, J_1 – полупервичная алгебра, удовлетворяющая тождеству. Следовательно, по теореме 4.7 J_1 удовлетворяет некоторому тождеству вида

$$[f(x_1, \ldots, x_n), y] = 0,$$

где $f(x_1, \ldots, x_n)$ – многочлен свободной ассоциативной алгебры, не являющейся тождеством в J_1. В частности, центр $Z(J_1)$ алгебры J_1 ненулевой. Заметим, что

$$Z(J_1) = J_1 \cap Z(R_1),$$

где $Z(R_1)$ – центр алгебры R_1. Действительно, для любых элементов $a \in J_1$, $b \in Z(J_1)$, $c \in R_1$ имеем, что

$$a[b, c] = [b, ac] - [b, a]c = 0,\ J_1[b, c] = 0,\ [b, c]J_1[b, c] = 0$$

и ввиду полупервичности алгебры J_1 получаем $[b, c] = 0$, то есть $b \in Z(R_1)$.

Пусть c – ненулевой элемент центра $Z(J_1)$. По лемме Цорна существует максимальный идеал $P \lhd R_1$ такой, что

$$P \cap \{c, c^2, c^3, \ldots\} = \varnothing.$$

Рассмотрим алгебру $R_2 = R_1/P$. Тогда R_2 – первичная F-алгебра, в которой каждый ненулевой идеал содержит некоторую степень элемента c. Пусть

$$Q = R_2\left[\frac{1}{c}\right] = \left\{\frac{a}{c^k}\;\middle|\; a \in R_1, k \geq 0\right\}$$

– алгебра частных. Тогда Q – конечно порожденная простая F-алгебра с единицей, удовлетворяющая тождеству. Она является примитивной алгеброй и по теореме 4.4 конечномерной над своим центром $Z = Z(Q)$. Из предложения 4.20 следует, что поле $Z = Z(Q)$ – конечно порожденная F-алгебра. Из следствия 4.14 получаем, что Z – конечномерное расширение поля F. Следовательно, Q – простая конечномерная F-алгебра, содержащая первичную конечномерную F-подалгебру R_2. В частности, R_2 – простая F-алгебра. С другой стороны, идеал $(\bar{c})$, порожденный элементов $\bar{c}$, является квазирегулярным (так как $0 \neq c \in J_1$). Противоречие. Итак, $J(R) = \mathrm{un}R$.

Докажем, что $J(R)$ – сумма всех нильпотентных идеалов R. Пусть a – произвольный элемент $J(R)$ и $I = (a)$. По условию $R = F\langle a_1, \ldots, a_{m-1}\rangle$ – конечно порожденная алгебра. Положим, что $a_m = a$. Тогда для любого целого числа $q \geq 1$ идеал I^q состоит из линейных комбинаций слов в алфавите $\{a_1, \ldots, a_m\}$, в которых a_m встречается не менее q раз. По теореме Ширшова о высоте эти слова могут быть записаны в виде

$$v_1^{p_1} v_2^{p_2} \ldots v_k^{p_k},$$

где v_i – слова от $\{a_1, \ldots, a_m\}$ степени не выше степени d полилинейного тождества алгебры R и $k \leq h(m, d)$ (высоты Ширшова). Пусть V – множество всех слов от $\{a_1, \ldots, a_m\}$, содержащих a_m и имеющих длину не выше d. Это множество содержится в нижнем ниль-радикале и является конечным. Поэтому существует такое целое число $s \geq 1$, что $v^s = 0$ для любого слова $v \in V$. Пусть $q > dsh(m, d)$. Тогда $I^q = 0$, так как каждое слово $v_1^{p_1} \ldots, v_k^{p_k}$, $k \leq h(m, d)$ равно нулю, ибо обязательно содержит подслово v_i, содержащее $a_m = a$, для которого $p_i \geq s$.

Таким образом, a содержится в нильпотентном идеале и $J(R)$ – сумма нильпотентных идеалов алгебры R. □

Из доказательства выше приведенной теоремы, нетеровости конечно порожденной коммутативной F-алгебры и нильпотентности ниль-подалгебр нетеровых F-алгебр получаем следствие.

Следствие 4.15. *Пусть $R = F\langle a_1, \ldots, a_n\rangle$ – конечно порожденная коммутативная алгебра над (произвольным) полем F. Тогда радикал Джекобсона R является нильпотентным идеалом.*

Следствие 4.16 (В. Латышев). *Пусть $R = F\langle a_1, \ldots, a_n\rangle$ – конечно порожденная алгебра над полем F характеристики нуль, удовлетворяющее тождеству*

$$xy^n + \sum_{i=1}^{n} \alpha_i y^i x y^{n-i} = 0, \tag{1}$$

где $\alpha_i \in F$. Тогда R – лево нетерова алгебра.

□ Докажем сначала, что $S = R/\mathrm{un}R$ – коммутативная алгебра. Для этого заметим, что S – полупервичная алгебра, являющаяся подпрямой суммой первичных алгебр $S_i = S/P_i$, где P_i – простой идеал S, $i \in I$. Пусть Z_i – ненулевой центр алгебры S_i (см. теорему 4.7). Тогда кольцо частных

$$Z_i^{-1}S_i = \left\{az^{-1} |\ a \in S_i,\ z \in Z_i\right\}$$

– простая алгебра, удовлетворяющая тождеству условия теоремы. Она является полной матричной алгеброй $M_{k_i}(D_i)$ над телом D_i конечномерным над центром $Z_i^{-1}Z_i$, $i \in I$. Если $k_i \geq 2$, то, подставляя в тождество $x = e_{12}$, $y = e_{22}$, получим, что $e_{12} = 0$. Противоречие. Следовательно, $Z_i^{-1}S_i = D_i$ – алгебра

с делением, удовлетворяющая тождеству, полученному линеаризацией исходного тождества (1),

$$x\left(\sum_{(i)} y_{i_1}y_{i_2}\dots y_{i_n}\right)+\sum_{(j_1,\dots,j_k)}\beta_{(j)}y_{j_1}\dots y_{j_k}xy_{j_{k+1}}\dots y_{j_n}=0, \tag{2}$$

где $\beta_{(j)}\in F$.

Пусть K_i – максимальное подполе тела D. Тогда

$$D_i\otimes_{Z_i^{-1}Z_i}K_i$$

– примитивная алгебра, удовлетворяющая тождеству (2). Следовательно,

$$D_i\otimes_{Z_i^{-1}Z_i}K_i\cong M_{m_i}(K_i).$$

Если $m_i\geq 2$, то, полагая $x=e_{12}$, $y_1=y_2=\ldots=y_n=e_{22}$, получим, что $n!e_{12}=0$. Противоречие. Следовательно, каждое D_i является полем, $i\in I$ и S – коммутативная алгебра. Это означает, что идеал $[R,R]$ алгебры R, порожденной всеми коммутаторами $\{[a,b]\mid a,b\in R\}$, содержится в $\mathrm{un}(R)$. Так как

$$[R,R]=\sum_{i=1}^{n}\sum_{j=1}^{n}R^{\#}[a_i,a_j]R^{\#}$$

– конечно порожденный идеал R, содержащийся в $\mathrm{un}(R)$, то, учитывая (по теореме 4.13), что $\mathrm{un}(R)$ – сумма нильпотентных идеалов, получаем, что $[R,R]^N=(0)$ для некоторого целого числа $N\geq 1$. Рассмотрим конечную цепь левых R-модулей:

$$R\supset[R,R]\supset\ldots\supset[R,R]^{N-1}\supset(0).$$

Для любого целого числа $k\leq N-1$

$$[R,R]^k/[R,R]^{k+1}$$

порождается (как левый $R/[R,R]$-модуль, где $R/[R,R]$ – коммутативная нетерова алгебра) конечным множеством элементов

$$[a_{i_1},a_{i_2}]a_{2_1}^{\alpha_1}\dots a_{2_n}^{\alpha_n}[a_{i_3},a_{i_4}]a_1^{\beta_1}\dots a_n^{\beta_n}\dots[a_{i_{2k-1}},a_{i_{2k}}]a_1^{\gamma_1}\dots a_n^{\gamma_n},$$

где $0 \leq \alpha_i, \beta_i, \gamma_t \leq n-1$ (ввиду тождества (1)). Следовательно,

$$R/[R,R],\ [R,R]/[R,R]^2,\ \ldots,\ [R,R]^{N-1}$$

– нетеровы $R/[R,R]$-модули. Следовательно, они являются нетеровыми левыми R-модулями и R-лево нетерова алгебра. $\square$

4.6. Тождества конечных колец

В настоящем параграфе мы будем рассматривать ассоциативные кольца, то есть $\mathbb{Z}$-алгебры. Пусть

$$\mathbb{Z}\langle X\rangle = \mathbb{Z}\langle x_1, x_2, \ldots\rangle$$

– свободное ассоциативное кольцо от переменных $\{x_1, x_2, \ldots\}$ и $f_i \in \mathbb{Z}\langle X\rangle$, где $i \in I$.

Абстрактный класс колец $\mathfrak{M}$, состоящий из всех ассоциативных колец, удовлетворяющих всем тождествам $f_i = 0$, $i \in I$, называется *многообразием колец* и обозначается

$$\mathfrak{M} = \mathrm{var}\langle f_i = 0|\ i \in I\rangle.$$

Вполне характеристический идеал (T-идеал) $Q \lhd \mathbb{Z}\langle X\rangle$, порожденный этими многочленами f_i, $i \in I$, обозначается

$$Q = T(\mathfrak{M}) = \{f_i|\ i \in I\}^T$$

и называется *идеалом тождеств многообразия* $\mathfrak{M}$. Кольцо

$$\mathbb{Z}\langle X\rangle / T(\mathfrak{M})$$

называется *приведенно свободным кольцом многообразия* $\mathfrak{M}$. Если $A \in \mathfrak{M}$ и $\{a_1, a_2, \ldots\} \subseteq A$, то отображение

$$x_i \to a_i,$$

$i \in N$, индуцирует естественный гомоморфизм

$$\varphi : \mathbb{Z}\langle X\rangle / T(\mathfrak{M}) \to A$$

такой, что если

$$\overline{f(x_1,\ldots,x_d)} \in \mathbb{Z}\langle X\rangle / T(\mathfrak{M}),$$

то

$$\varphi(\overline{f(x_1,\ldots,x_d)}) = f(a_1,a_2,\ldots,a_d).$$

Теорема 4.14 (Г. Биркгоф).
Абстрактный класс колец $\mathfrak{M}$ является многообразием колец тогда и только тогда, когда

1) *если $R \in \mathfrak{M}$ и A – подкольцо R, то $A \in \mathfrak{M}$ ($s\mathfrak{M} \subseteq \mathfrak{M}$);*

2) *если $R \in \mathfrak{M}$ и $I \lhd R$, то $R/I \in \mathfrak{M}$ ($q\mathfrak{M} \subseteq \mathfrak{M}$);*

3) *если $R_i \in \mathfrak{M}$, $i \in \wedge$, то $\prod\limits_{i\in\wedge} R_i \in \mathfrak{M}$ ($\mathfrak{M} \subseteq \mathfrak{M}$).*

Другими словами, класс $\mathfrak{M}$ является многообразием колец тогда и только тогда, когда он замкнут относительно взятия подколец ($s\mathfrak{M} \subseteq \mathfrak{M}$), гомоморфных образов ($q\mathfrak{M} \subseteq \mathfrak{M}$) и прямых произведений ($c\mathfrak{M} \subseteq \mathfrak{M}$).

□ Если $\mathfrak{M}$ – многообразие колец, то очевидно, что $s\mathfrak{M} \subseteq \mathfrak{M}$, $q\mathfrak{M} \subseteq \mathfrak{M}$ и $c\mathfrak{M} \subseteq \mathfrak{M}$.

Докажем обратное утверждение. Пусть в классе $\mathfrak{M}$ выполняются условия 1), 2) и 3) и пусть Q – множество всех многочленов из $\mathbb{Z}\langle X\rangle$, являющихся тождествами на всех кольцах из $\mathfrak{M}$. Обозначим через

$$\mathfrak{N} = \mathrm{var}\langle q = 0 |\ q \in Q\rangle.$$

Тогда $\mathfrak{M} \subseteq \mathfrak{N}$ и $T(\mathfrak{N}) = Q$. Докажем, что $\mathfrak{M} = \mathfrak{N}$. Для каждого многочлена $f \notin Q$ существует кольцо $A_f \in \mathfrak{M}$, не удовлетворяющее тождеству $f = 0$. Пусть

$$A = \prod_{f\notin Q} A_f \in \mathfrak{M} \quad (c\mathfrak{M} \subseteq \mathfrak{M})$$

и

$$\Im = \{\varphi |\ \varphi : \mathbb{Z}\langle X\rangle \to A\}$$

– множество всех гомоморфизмов свободного кольца $\mathbb{Z}\langle X\rangle$ в A. Заметим, что

$$\bigcap_{\varphi\in\Im} \operatorname{Ker}\varphi = Q.$$

Рассмотрим отображение

$$\lambda : \mathbb{Z}\langle X\rangle \to \prod_{\varphi\in\Im} A_\varphi,$$

где $A_\varphi = A$, такое, что для любого многочлена $f \in \mathbb{Z}\langle X\rangle$

$$\lambda(f)(\varphi) = \varphi(f) \in A_\varphi.$$

Так как

$$\operatorname{Ker}\lambda = \bigcap_{\varphi\in\Im} \operatorname{Ker}\varphi = Q = T(\mathfrak{N}),$$

то это отображение индуцирует вложение приведенно свободного кольца $Z\langle X\rangle / T(\mathfrak{N})$ многообразия $\mathfrak{N}$ в прямое произведение $\prod\limits_{\varphi\in\Im} A_\varphi \in \mathfrak{M}$. Произвольное счетно порожденное кольцо из $\mathfrak{N}$ является гомоморфным образом кольца $\mathbb{Z}\langle X\rangle / T(\mathfrak{N})$. Так как $s\mathfrak{M} \subseteq \mathfrak{M}$, $q\mathfrak{M} \subseteq \mathfrak{M}$, то все счетно порожденные кольца из $\mathfrak{N}$ содержатся в $\mathfrak{M}$. Рассуждая аналогично, можно показать, что произвольное кольцо (с множеством порождающих элементов произвольной мощности) из $\mathfrak{N}$ содержится в $\mathfrak{M}$. $\square$

T – идеал $Q \lhd Z\langle X\rangle$ называется *конечно порожденным T-идеалом*, если существует конечное множество многочленов $\{f_1, \ldots, f_n\}$ из Q такое, что произвольный многочлен $g \in Q$ имеет вид

$$g = \sum_{i=1}^{n} a_i(x_i) f_i\left(\varphi_{i_1}(x_j), \ldots, \varphi_{i_d}(x_j)\right) b_i(x_i),$$

где $a_i, \varphi_k, b_j \in \mathbb{Z}\langle X\rangle$. В обозначении его $Q = \{f_1, \ldots, f_n\}^T$.

Цель настоящего параграфа – доказать следующий интересный результат.

Теорема 4.15 (И. Львов, Р. Крузе).
Идеал тождеств произвольного конечного ассоциативного кольца является конечно порожденным.

Для доказательства этой теоремы введем некоторые определения и обозначения, а также докажем вспомогательные утверждения, имеющие независимый интерес.

Пусть R_i – кольца, $i \in I$. Наименьшее многообразие колец, содержащее все R_i, $i \in I$ называется *многообразием, порожденным* R_i, $i \in I$ и обозначается $\mathrm{var}\{R_i |\ i \in I\}$. Многообразие колец называется *локально конечным*, если все его конечно порожденные кольца являются конечными. *Фактором кольца* R назовем гомоморфный образ S/T, где S – подкольцо R и $T \lhd S$. Фактор S/T называется *собственным*, если либо $S \neq R$, либо $T \neq (0)$. Кольцо называется *критическим*, если оно не принадлежит многообразию колец, порожденному всеми его собственными факторами. Пусть $A_1, \ldots, A_e$ – подмножества кольца R. Обозначим через $\langle A_1, \ldots, A_e \rangle$ подгруппу $\langle R, + \rangle$, порожденную всеми произведениями $a_{\pi(1)} \ldots a_{\pi(e)}$, где $a_i \in A_i$ и π – подстановка на множестве $\{1, 2, \ldots, e\}$.

Лемма 4.17. *Пусть $L, M_1, \ldots, M_n$ – подкольца конечного кольца R такие, что:*

1. *R порождается как кольцо элементами множества*

$$L \cup M_1 \cup \ldots \cup M_n;$$

2. *для любого числа $i \leq n$ R не порождается (как кольцо) множеством*

$$L \cup M_1 \cup \ldots \cup M_{i-1} \cup \ldots \cup M_n;$$

3. *для любого числа $k \geq 0$*

$$\langle M_1, \ldots, M_n, R, \ldots, R \rangle = (0).$$

Тогда R не является критическим кольцом.

□ Пусть B_j – подкольцо кольца R, порожденное множеством

$$(L \cup M_1 \cup \ldots \cup M_{j-1} \cup M_{j+1} \cup \ldots \cup M_n),$$

где $1 \leq j \leq n$. Докажем, что R принадлежит

$$\mathrm{var}\,(B_1 \oplus \ldots \oplus B_n).$$

Предположим противное. Тогда существует некоторый многочлен $f(x_1, \ldots, x_d)$, существенно зависящий от $x_1, \ldots, x_d$, являющийся тождеством в $B_1 \oplus \ldots \oplus B_n$ и не являющийся тождеством в R. Пусть $a_1, \ldots, a_d$ – элементы из R такие, что

$$f(a_1, \ldots, a_d) \neq 0.$$

Если $f(x_1, \ldots, x_d)$ – полилинейный многочлен, то можно полагать, что $a_1, \ldots, a_d$ – слова от порождающего множества $L \cup M_1 \cup \ldots \cup M_n$. При этом для любого числа $i \leq n$ существует элемент a_j, содержащий элемент из M_i (иначе, $f(a_1, \ldots, a_d) = 0$). Поэтому

$$a_{i_1} \ldots a_{i_d} \in \langle M_1, \ldots, M_n, R, \ldots, R \rangle = (0)$$

и $f(a_1, \ldots, a_d) = 0$. Противоречие. Если $f(x_1, \ldots, x_d)$ не является полилинейным многочленом, то, применяя к $f(x_1, \ldots, x_d)$ процесс линеаризации, мы можем считать, что для любого числа $i \leq d$

$$g = f(x_1, \ldots, x_{i-1}, y_1 + y_2, \ldots, x_d) - \\ - f(x_1, \ldots, x_{i-1}, y_1, \ldots, x_d) - f(x_1, \ldots, x_{i-1}, y_2, \ldots, x_d)$$

– тождество в R, а $f(x_1, \ldots, x_d) = 0$ не является тождеством в R. Это означает, что существуют слова $a_1, \ldots, a_d$ от порождающего множества $L \cup M_1 \cup \ldots \cup M_n$ такие, что $f(a_1, \ldots, a_d) \neq 0$. С другой стороны, $f(x_1, \ldots, x_n) = 0$ – тождество в каждом кольце B_i, $i \leq n$. Поэтому для любого числа $i \leq n$ существует

слово a_j, содержащее некоторый элемент из M_i. Это означает, что

$$f(a_1, \ldots, a_d) \in \langle L, M_1, \ldots, M_n \rangle = (0).$$

Противоречие доказывает, что $R \in \operatorname{var} \langle B_1 \oplus \ldots \oplus B_n \rangle$ и R не является критическим кольцом. □

Лемма 4.18 (Я. Левин).
Пусть R – конечно порожденное кольцо и S – подкольцо R такое, что аддитивная подгруппа $\langle S, + \rangle$ имеет конечный индекс в группе $\langle R, + \rangle$. Тогда S – конечно порожденное кольцо.

□ Пусть

$$m = \left[R^+ : S^+ \right].$$

Докажем, что S содержит идеал $I \lhd R$ такой, что

$$[R^+ : I^+] \leq k \cdot m,$$

где

$$k = (m+1)^{(m+1)^2}.$$

Пусть J – наибольший идеал кольца R, содержащийся в S. Тогда S/J не содержит ненулевых идеалов кольца R/J. Покажем, что $\overline{S} = S/J$ содержит ненулевой идеал кольца $\overline{R} = R/J$, если $\left|\overline{S}\right| > k$. Пусть

$$\left\{ u_1 + \bar{S}^+, \ldots, u_m + \bar{S}^+ \right\} = \bar{R}^+ / \bar{S}^+,$$

u_0 – формальная единица и $M = \{0, 1, 2, \ldots, m\}$. Каждый элемент s из $\overline{S}$ индуцирует отображение

$$f_s : M \times M \to M,$$

определенное по правилу

$$u_i s u_j = u_{f(i,j)} + s_1,$$

где $s_1 \in \overline{S}$. Так как число всех таких отображений равно k, то, предположив, что $\left|\overline{S}\right| > k$, мы получим существование двух

различных элементов s_1 и s_2 из $\overline{S}$ таких, что $f_{s_1} = f_{s_2}$. Это означает, что при любых элементах $i, j \in M$ $u_i(s_1 - s_2)u_j \in \overline{S}$. Так как каждый элемент кольца $\overline{R}$ может быть записан в виде $u_i + s$, где $s \in \overline{S}$, то $\overline{S}$ содержит ненулевой идеал кольца $\overline{R}$, порожденный $(s_1 - s_2)$. Противоречие доказывает, что индекс $m_1 = [R^+ : I^+] \leq km$.

По условию $R = \langle a_1, \ldots, a_n \rangle$ – конечно порожденное кольцо. Пусть $F = \mathbb{Z}\langle x_1, \ldots, x_n \rangle$ – свободное ассоциативное кольцо с множеством образующих элементов $\{x_1, \ldots, x_n\}$. Тогда $R \cong F/P$, где $P \lhd F$ и $I = I_1/P$ для некоторого идеала $I_1 \lhd F$. Тогда $|F/I_1| = m_1$. Пусть

$$F/I_1 = \{u_1 + I_1, u_2 + I_1, \ldots, u_{m_1} + I_1\},$$

u_0 – формальная единица в F и A – аддитивная подгруппа $\langle F, + \rangle$, порожденная $\{u_1, u_2, \ldots, u_{m_1}\}$. Тогда

$$x_i = u_{j(i)} + r_i,$$

$1 \leq i \leq n$,

$$u_i u_j = u_{k_1} + s_{ij},$$

$1 \leq i, j \leq m_1$, где $r_i, s_{ij} \in I_1$. Пусть J – подкольцо F, порожденное множеством $\{u_i r_j u_e, u_i s_{jt} u_e\}$. Это подкольцо является идеалом в F. Каждый многочлен $f \in F$ представим в виде

$$f = \sum_{i=1}^{m_1} \alpha_i u_i + r,$$

где $\alpha \in \mathbb{Z}$, $r \in J$. В частности, если $f \in I_1$, то $\sum\limits_{i=1}^{m_1} \alpha_i u_i \in I_1$ и $I_1 = (A \cap I_1) + J$. Подгруппа $(A \cap I_1)^+$ является конечно порожденной абелевой группой. Поэтому I_1 – конечно порожденное кольцо, а, следовательно, S – конечно порожденное кольцо. $\square$

Лемма 4.19.

1. *Пусть R – конечное кольцо. Тогда R удовлетворяет тождествам вида $nx = 0$, $x^k = x^e$ для некоторых натуральных чисел n, k, e $(k < e)$.*

2. $\operatorname{var}\langle nx = 0,\ x^k - x^e = 0,\ \text{где } k < e\rangle$ *– локально конечное многообразие колец.*

□ Пусть $|R| = n$. Тогда для любого элемента a абелевой группы $\langle R, +\rangle$ $na = 0$, то есть

$$nx = 0$$

– тождество в R. Рассмотрим отображения

$$f_i : R \to R$$

такое, что

$$f_i(a) = a^i,$$

где $a \in R$, $i = 1, 2, \ldots$. Так как R – конечное множество, то существуют числа i, j $(i \neq j)$ такое, что $f_i = f_j$. Это означает, что $x^i - x^j = 0$ – тождество в кольце R. Первое утверждение доказано.

Докажем, что многообразие колец

$$\mathfrak{N} = \operatorname{var}\left\langle nx = 0,\ x^k - x^e = 0,\ k < e\right\rangle$$

является локально конечным. Пусть A – конечно порожденное кольцо из $\mathfrak{N}$ и $n = p_1^{s_1} \ldots p_t^{s_t}$ – каноническое разложение на простые числа. Тогда $A = A_1 \oplus \ldots \oplus A_t$, где $A_i \lhd A$, $p_i^{s_i} A_i = (0)$, A_i – конечно порожденное кольцо, $i \leq t$. Докажем, что каждое кольцо A_i является конечным, $i \leq t$. Если $s_i = 1$, то A_i – алгебраическая алгебра над полем $GF(p_i)$. Из теоремы 4.10 следует, что A_i – конечномерная $GF(p_i)$ – алгебра и, следовательно, $|A_i| < \infty$.

Воспользуемся методом математической индукции по числу s_i. Предположим, что любое конечно порожденное кольцо

$T \in \mathfrak{N}$, удовлетворяющее условию $p_i^{s_i-1}T = (0)$, является конечным. Рассмотрим $GF(p_i)$ – алгебру $R_1 = A_i/p_iA_i$. Она является конечной. По лемме 4.18 подкольцо $T = p_iA_i$ является конечно порожденным и удовлетворяет условию $p_i^{s_1-1}T = p_i^{s_i}A_i = (0)$. По предположению индукции T – конечное кольцо, а, следовательно, A_i – конечное кольцо, $i \leq n$. Откуда следует, что $|A| < \infty$ и $\mathfrak{N}$ – локально конечное многообразие колец. $\square$

Из леммы 4.19 следует, что многообразие колец, порожденное конечным кольцом, является локально конечным.

Лемма 4.20. *Пусть R – конечное кольцо и c – наибольший индекс нильпотентности нильпотентных подколец кольца R. Тогда R удовлетворяет тождеству вида*

$$x_1x_2\dots x_c = f(x_1,\dots,x_c),$$

где f – сумма одночленов степени $\geq (c+1)$. В частности, если A – нильпотентное кольцо из $\operatorname{var} R$, *то $A^c = (0)$.*

$\square$ Пусть F_c – приведенно свободное кольцо в $\operatorname{var} R$, порожденное $x_1,\dots,x_c$. Рассмотрим множество

$$\mathfrak{T} = \{\varphi|\ \varphi : F_c \to R\}$$

всех гомоморфизмов кольца F_c в R. По лемме 4.19 $|F_c| < \infty$. Следовательно, $|\mathfrak{T}| < \infty$. Рассмотрим отображение

$$\Theta : F_c \to \prod_{\varphi\in\mathfrak{T}} R_\varphi,$$

где $R_\varphi = R$, такие, что

$$\Theta(f) = (\dots,\varphi(f),\dots),$$

для $f \in F_c$. Ясно, что Θ – гомоморфизм и $\operatorname{Ker}\Theta = (0)$. Таким образом, F_c вложима в $\prod\limits_{\varphi\in\mathfrak{T}} R_\varphi$. Откуда следует, что $J(F_c)^c = (0)$. Рассмотрим кольцо

$$A = F_c/\left(F_c^{c+1} + J(F_c)\right).$$

Оно является нильпотентным ($A^{c+1} = (0)$) и гомоморфным образом полупростого конечного кольца $F_c/J(F_c)$. Следовательно, $A = (\bar{0})$ и $F_c = F_c^{c+1} + J(F_c)$. Так как $J(F_c)^c = (0)$, то $F_c^c = F_c^{c+1}$, $x_1x_2 \dots x_c \in F_c^{c+1}$ и идеал тождеств кольца R содержит многочлен вида $x_1 \dots x_c + f(x_1, \dots, x_c)$, где f – сумма одночленов степени не менее $c+1$. $\square$

Лемма 4.21. *Пусть R – конечное критическое кольцо и*

$$J(R)^c = (0).$$

Тогда кольцо R порождается $5c-3$ элементами.

$\square$ Пусть $R \neq J(R)$ и

$$R/J(R) = \overline{S}_1 \oplus \dots \oplus \overline{S}_n,$$

где $\overline{S}_i$ – простое кольцо, $i \leq n$. Пусть S_i – такое подкольцо R, что $S_i/J(R) = \overline{S}_i$, $i \leq n$. По лемме 4.17 существует подстановка π такая, что $S_{\pi(1)} \dots S_{\pi(n)} \neq (0)$. Так как $S_iS_j \subseteq J(R)$ при $i \neq j$, то $J(R)^{[n/2]} \neq (0)$ и $\frac{n}{2} < c$, то есть $n \leq 2c-1$. Докажем, что $R/J(R)$ может быть порождено $2n$ элементами. Действительно, простое кольцо $M_m(GF(q))$ порождается двумя элементами

$$\lambda e_{12},\ e_{12} + e_{23} + \dots + e_{m-1m} + e_{m1},$$

где $(GF(q)\backslash\{0\}, \cdot) = (\lambda)$. Следовательно, $R/J(R)$ имеет $4c-2$ образующих элементов $\{\bar{a}_1, \dots, \bar{a}_{4c-2}\}$. Пусть $\{b_1, \dots, b_t\}$ – минимальное множество элементов из $J(R)$ такие, что

$$\{a_1, \dots, a_{4c-2}, b_1, \dots, b_t\}$$

порождает кольцо R. Если $t \geq c$, то, полагая

$$L = \langle a_1,\ \dots,\ a_{4c-2} \rangle,\ M_1 = \langle b_1 \rangle, \dots,\ M_t = \langle b_t \rangle,$$

приходим (согласно лемме 4.17) к противоречию с тем, что R – критическое кольцо. Следовательно, $t \leq c-1$ и кольцо R

порождается $5c-3$ элементами. Если $R = J(R)$, то выше приведенные рассуждения показывают, что R порождается $(c-1)$ элементами. $\square$

Перейдем к доказательству теоремы.

$\square$ Пусть R – конечное кольцо. Тогда R удовлетворяет некоторым тождествам вида:

$$f_1 = nx = 0,\ f_2 = x^k - x^e = 0,$$

где $k < e$ и

$$f_3 = x_1 x_2 \dots x_c - f(x_1, \dots, x_i) = 0,$$

где f – сумма одночленов от $x_1, \dots, x_c$ степени $\geq c+1$. Рассмотрим многообразие колец

$$\mathfrak{M} = \operatorname{var} \langle f_1 = 0, f_2 = 0, f_3 = 0 \rangle .$$

Ясно, что $\operatorname{var} R \subseteq \mathfrak{M}$. Согласно лемме 4.19 $\mathfrak{M}$ - локально конечное многообразие колец и $T(\mathfrak{M}) = \{f_1, f_2, f_3\}^T$. Пусть S – критическое кольцо из $\mathfrak{M}$. Оно удовлетворяет тождеству $f_3 = 0$. Поэтому $J(S)^c \subseteq J(S)^{c+1}$. Так как $J(S)$ – нильпотентный идеал в S, то $J(S)^c = (0)$. По лемме 4.21 S порождается $5c-3$ элементами и, следовательно, является гомоморфным образом приведенно свободного кольца $F_{5c-3} \in \mathfrak{M}$, которое, в свою очередь, является конечным. Таким образом, $\mathfrak{M}$ содержит конечное число критических колец.

Каждое подмногообразие $\mathfrak{N} \subseteq \mathfrak{M}$ порождается своими конечно порожденными кольцами, которые в силу леммы 4.19, являются конечными. Пусть $\mathfrak{N}_1$ – подмногообразие $\mathfrak{N}$, порожденное всеми конечными критическими кольцами из $\mathfrak{N}$. Если $\mathfrak{N}_1 \neq \mathfrak{N}$, то найдется конечное кольцо $A \in \mathfrak{N}$ такое, что $A \notin \mathfrak{N}_1$, а все собственные факторы A принадлежат $\mathfrak{N}_1$. Кольцо A является критическим и по определению $A \in \mathfrak{N}_1$. Противоречие доказывает, что каждое подмногообразие $\mathfrak{N} \subseteq \mathfrak{M}$ порождается своими критическими кольцами (число которых в $\mathfrak{M}$ конечно). Таким образом, в $\mathfrak{M}$ конечное число подмногообразий.

Пусть $T = T(R)$. Тогда $T(\mathfrak{M}) = \{f_1, f_2, f_3\}^T \subseteq T$. Если T не является конечно порожденным T-идеалом, то существует счетное множество многочленов $\{g_1, g_2, \ldots\} \subseteq T$ такое, что цепочка T-идеалов

$$T(\mathfrak{M}) \subset T(\mathfrak{M}) + \{g_1\}^T \subset T(\mathfrak{M}) + \{g_1, g_2\}^T \subset \\ \subset T(\mathfrak{M}) + \{g_1, g_2, g_3\}^T \subset \ldots$$

является строго возрастающей. Пусть

$$\mathfrak{M}_i = \operatorname{var} \langle f_1 = 0, f_2 = 0, f_3 = 0, g_k = 0 |\ k \leq i \rangle .$$

Тогда

$$\mathfrak{M} \supset \mathfrak{M}_1 \supset \mathfrak{M}_2 \supset \ldots$$

– строго убывающая цепочка подмногообразий колец. Противоречие. $\square$

Следствие 4.17. *Многообразие колец $\mathfrak{M}$ порождается конечным кольцом тогда и только тогда, когда $T(\mathfrak{M})$ содержит многочлены*

$$nx,\ x^k - x^e,\ x_1 \ldots x_c - f(x_1, \ldots, x_c),$$

где $n, k, e \in N$, $k \leq e - 1$, f – сумма одночленов от $x_1, \ldots, x_c$ степени $\geq c + 1$.

Применим вышеприведенную технику для нахождения базиса тождеств поля $GF(q)$ и кольца $M_2(GF(q))$.

Пусть p – простое число, $q = p^n$, $n \geq 1$. Тогда поле $GF(q)$ удовлетворяет тождествам $px = 0$, $x - x^q = 0$. Докажем, что

$$T(GF(q)) = \{px, x - x^q\}^T.$$

Рассмотрим многообразие колец

$$\mathfrak{M} = \operatorname{var} \langle px = 0, x - x^q = 0 \rangle .$$

Ясно, что $\operatorname{var} GF(q) \subseteq \mathfrak{M}$. По лемме 4.19 $\mathfrak{M}$ – локально конечное многообразие колец. Оно порождается всеми своими конечными критическими кольцами. Пусть $S \in \mathfrak{M}$ и S – конечное критическое кольцо. Тогда для любого элемента $a \in J(S)$, $a = a^q = (a^q)^q = \ldots = 0$, то есть $J(S) = (0)$ и S – полупростое конечное кольцо. Так как S – критическое кольцо, то оно является подпрямо неразложимым кольцом. Следовательно, $S = M_k(GF(q_1))$. Если $k \geq 2$, то $e_{12} = e_{12}^q = 0$. Противоречие доказывает, что $k = 1$ и $S = GF(q_1)$ – подполе $GF(q)$. Откуда следует, что $S \in \operatorname{var} GF(q)$, $\mathfrak{M} = \operatorname{var} GF(q)$ и все тождества поля $GF(q)$ следуют из тождеств $px = 0$, $x - x^q = 0$ (в частности, $[x, y] \in \{px, x - x^q\}^T$).

Следующая теорема (см. [44]) была доказана Е. Кузьминым и Ю. Мальцевым.

Теорема 4.16. *Идеал тождеств кольца матриц $M_2(GF(q))$, где $q = p^n$ и p – простое число, $n \geq 1$ порождается многочленами*

$$px,$$

$$f_1(x, y) = (x - x^q)\left(y - y^{q^2}\right)\left(1 - [x, y]^{q-1}\right),$$

$$f_2(x, y) = (x - x^q) \circ (y - y^q) - ((x - x^q) \circ (y - y^q))^q,$$

где $[x, y] = xy - yx$, $x \circ y = xy + yx$.

Предварительно докажем несколько лемм. Пусть

$$A = M_2(GF(q))$$

и

$$\mathfrak{M} = \operatorname{var} \langle px = 0, f_1 = 0, f_2 = 0 \rangle .$$

Лемма 4.22. $A \in \mathfrak{M}$.

□ Пусть $x \in A$ и $\operatorname{tr} x$, $|x|$ – соответственно след и определитель матрицы x. Легко видеть, что если x и y – матрицы с нулевым следом, то $x \circ y$ – скалярная матрица и

$$(x \circ y) - (x \circ y)^q = 0.$$

Заметим, что для любой матрицы $x \in A$ след матрицы $(x - x^q)$ равен нулю. Действительно, матрица x подобна матрице вида

$$\begin{pmatrix} \lambda_1 & \beta \\ 0 & \lambda_2 \end{pmatrix},$$

где $\lambda_1, \lambda_2 \in GF(q^2)$, $\beta = 0, 1$. Поэтому $\operatorname{tr} x = (\lambda_1 + \lambda_2)$ и

$$\operatorname{tr}(x - x^q) = (\lambda_1 + \lambda_2) - (\lambda_1 + \lambda_2)^q = 0,$$

так как $(\lambda_1 + \lambda_2) \in GF(q)$. Следовательно, $f_2(x, y) = 0$ – тождество в кольце A.

Пусть $x, y \in A$. Рассмотрим значения $f_1(x, y)$. Если характеристические корни матрицы y различны, то y подобна матрице вида

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix},$$

где $\lambda_1, \lambda_2 \in GF(q^2)$, $(y - y^{q^2}) = 0$ и $f_1(x, y) = 0$. Если же характеристические корни матрицы y совпадают, то y подобна матрице вида

$$\begin{pmatrix} \lambda & \varepsilon \\ 0 & \lambda \end{pmatrix},$$

где $\varepsilon = 0, 1$, $\lambda \in GF(q^2)$. Если $\varepsilon = 0$, то $y - y^{q^2} = 0$ и $f_1(x, y) = 0$. Пусть $\varepsilon = 1$. Тогда $2\lambda \in GF(q)$ и $\lambda^2 = |y| \in GF(q)$. Откуда следует, что $\lambda \in GF(q)$. Положим $y' = y - \lambda$. Тогда $y' - (y')^{q^2} = y - y^{q^2}$ и мы можем предполагать, что

$$y = e_{12},\ x = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

где $\alpha, \beta, \gamma, \delta \in GF(q)$. Тогда

$$[x, y] = \begin{pmatrix} -\gamma & \alpha - \delta \\ 0 & \gamma \end{pmatrix}.$$

Если $\gamma = 0$, то $(x - x^q)y = 0$ и $f_1(x, y) = 0$. Если же $\gamma \neq 0$, то

$$\left(y - y^{q^2}\right)\left(1 - [x, y]^{q-1}\right) = 0$$

и $f_1(x,y) = 0$. Таким образом, A удовлетворяет тождествам $px = 0$, $f_1 = 0$, $f_2 = 0$ и A принадлежит многообразию колец $\mathfrak{M}$. $\square$

Аналогичными рассуждениями можно доказать, что $M_2(GF(q))$ удовлетворяет тождеству

$$\left(x - x^{q^2}\right)\left(1 - [x,y]^{q-1}\right)(y - y^q) = 0.$$

Лемма 4.23. $\mathfrak{M} \subseteq \operatorname{var} A$.

$\square$ По теореме 4.15 многообразие колец $\mathfrak{M}$ порождается своими конечными критическими точками. Покажем, что каждое такое критическое кольцо принадлежит $\operatorname{var} A$. Пусть R – конечное критическое кольцо из $\mathfrak{M}$. Покажем, что R – подкольцо A. Если $R = J(R)$, то R – нильпотентное кольцо. Так как R удовлетворяет тождеству $f_1 = 0$, то $R^2 = R^3 = \ldots = (0)$. Учитывая, что R – подпрямо неразложимое кольцо, получаем, что R – одномерная $GF(p)$-алгебра, изоморфная подалгебре $GF(p) \cdot e_{12}$ алгебры A.

Если R – простая алгебра, то $R = M_k(GF(q_1))$. Если $k \geq 3$, то, полагая $x = y = e_{12} + e_{23}$, получим, что

$$f_1(x,y) = xy = e_{13}.$$

Противоречие. Пусть $k = 2$. Полагая $x = \alpha e_{11}$, $y = e_{12}$, получим, что

$$f_1(x,y) = (\alpha - \alpha^q)e_{12} = 0.$$

Откуда следует, что $\alpha - \alpha^q = 0$ и $GF(q_1) \subseteq GF(q)$, то есть, R – подкольцо A. Если же $k = 1$, то

$$f_1(x,x) = (x - x^q)\left(x - x^{q^2}\right) = 0$$

– тождество в поле $GF(q_1)$. Поэтому $GF(q_1)$ – подполе $GF(q^2)$. Используя регулярное представление $GF(q^2)$ как двумерной алгебры над $GF(q)$, снова получаем, что R – подкольцо A.

Пусть теперь

$$R = B \dotplus N,$$

где B – полупростая $GF(p)$-алгебра и $N = J(R)$. Согласно предыдущему имеем, что

$$B = B_1 \oplus \ldots \oplus B_s,$$

где

$$B_i = M_{k_i}\left(GF(p^{t_i})\right),$$

$i \leq s$, $k_i \leq 2$ и $N^2 = (0)$. При этом $N \neq (0)$ и $R \neq N$. Если, например, $B_1 = M_2\left(GF(p^{t_1})\right)$, то, полагая $x = e_{12} \in B_1$ и $y = u \in N$, получим, что $f_1(x, y) = e_{12} \cdot u = 0$. Аналогично $ue_{12} = e_{21}u = ue_{12} = 0$. Откуда следует, что $e_{11}u = ue_{11} = e_{22}u = ue_{22} = 0$ и $B_1 \lhd R$. Это противоречит подпрямой неразложимости кольца R. Следовательно, $k_1 = \ldots = k_s = 1$. Пусть e_i – единица подкольца B_i, $i \leq s$. Так как ни одно из подколец $B_1, \ldots, B_s$ не является идеалом в R, то либо $RN \neq (0)$, либо $NR \neq (0)$. Пусть,например, $RN \neq (0)$. Так как e_iN, $i = 1, \ldots, s$, являются попарно пересекающимися идеалами в R, то отличен от нуля лишь один из них, скажем e_1N. Так как

$$N = e_1N \oplus (1 - e_1)N,$$

то $(1 - e_1)N = (0)$ и $N = e_1N$. Аналогично, Ne_i, $i = 1, \ldots, s$, являются попарно пересекающимися идеалами в R, следовательно, отличным от нуля может быть лишь одни из них. Здесь возможны три случая.

Случай 1. $NR = (0)$.
Тогда $B = B_1 = GF(p^t)$ и N – одномерное (левое) векторное пространство над полем $GF(p^t)$. Элементы кольца R представляются матрицами вида

$$\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix},$$

где $\alpha, \beta \in GF(p^t)$. Так как

$$f_2(\alpha e_{11}, e_{12}) = (\alpha - \alpha^q)e_{12} = 0,$$

то $\alpha - \alpha^q = 0$ и $GF(p^t)$ – подполе $GF(q)$, то есть, R – подкольцо A.

Случай 2. $Ne_1 \neq (0)$ и $N = e_1 N e_1$.
Тогда $B = B_1 = GF(p^t)$ и N – неприводимый $(GF(p^t), GF(p^t))$-бимодуль. Рассматривая $f_1(\alpha e_1, u)$, где $u \in N$ и $\alpha \in GF(p^t)$, получаем, что $GF(p^t) \subseteq GF(q)$ и R изоморфно кольцу матриц

$$\left\{ \begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix} \middle| \; a, b \in GF(p^t),\ \sigma \in \mathrm{Aut}GF(p^t) \right\}.$$

(см. [33]). В частности, $R \subseteq A$.

Случай 3. $Ne_2 \neq (0)$ и $N = e_1 N e_2$.
В этом случае

$$B = B_1 \oplus B_2 = GF(p^{t_1}) \oplus GF(p^{t_2}),\ NB_1 = B_2 N = (0).$$

Если $u \in N$, $\alpha \in GF(p^{t_1})$ и $\beta \in GF(p^{t_2})$, то

$$f_2(\alpha e_1, u) = (\alpha - \alpha^q)u = 0,\ f_2(u, \beta e_2) = u(\beta - \beta^q) = 0$$

и

$$(\alpha - \alpha^q) = (\beta - \beta^q) = 0.$$

Откуда следует, что B_1, B_2 – подполя поля $GF(q)$. Ввиду подпрямой неразложимости R, радикал N является однопорожденным (B_1, B_2) – модулем. Следовательно, элементы кольца R представляются матрицами вида

$$\begin{pmatrix} \alpha & \gamma \\ 0 & \beta \end{pmatrix},$$

где $\alpha \in GF(p^{t_1})$, $\beta \in GF(p^{t_2})$ и γ принадлежит композиту полей $GF(p^{t_1})$ и $GF(p^{t_2})$, содержащемуся в поле $GF(q)$. Снова получаем, что R – подкольцо A. $\square$

Из лемм 4.22, 4.23 следует, что

$$\mathrm{var}\, M_2(GF(q)) = \mathrm{var}\, \langle px = 0, f_1 = 0, f_2 = 0 \rangle .$$

Теорема доказана.

В работах Г. Генова и П. Сидорова [39, 40] найдены конкретные порождающие идеалов тождеств колец $M_3(GF(q))$ и $M_4(GF(q))$. В работе А. Олексенко [56] найдены семь многочленов, порождающих идеал тождеств кольца $M_2(\mathbb{Z}_{p^2})$. В работе Р. Гилмера [81] доказано, что если R – конечное коммутативное кольцо с единицей, то идеал тождеств кольца R в $R[t]$ является главным тогда и только тогда, когда R – прямая сумма конечного числа полей. В работе Е. Зельманова [42] доказано, что алгебра R удовлетворяет стандартному тождеству $S_d = 0$, если

1) R не содержит ненулевых ниль-идеалов;

2) R содержит подалгебру A, удовлетворяющую тождеству степени d;

3) для любого элемента $a \in R$ существует целое число $n(a)$ такое, что $a^{n(a)} \in A$.

Заметим также, что следующая нерешенная проблема является интересной и важной: *для кольца $M_n(GF(q))$ найти тождество вида $x_1x_2\dots x_n = f(x_1,\dots,x_n)$, где f – сумма одночленов степени $\geq n+1$.*

4.7. Упражнения

Упражнение 4.1. *Пусть R – полупервичное кольцо, удовлетворяющее полугрупповому тождеству*

$$u(x_1,\dots,x_k) = v(x_1,\dots,x_k),$$

где u, v – различные одночлены от $x_1,\dots,x_k$ свободного ассоциативного кольца. Докажите, что идеал тождеств кольца R в $\mathbb{Z}\langle x_1, x_2, \dots\rangle$ совпадает с идеалом тождеств некоторого кольца вида $A \oplus B$, где A – конечное кольцо, а B – коммутативное кольцо (см. [55]).

$\diamondsuit$ Полупервичное кольцо R раскладывается в подпрямую сумму первичных колец:

$$R = \sum_{i \in I} \bigoplus_{s} R_i,$$

где $R_i = R/P_i$ – первичные кольца, удовлетворяющие тождеству $u - v = 0$, $i \in I$. Каждое первичное кольцо R_i является либо коммутативным кольцом, либо его центр $Z_i \neq (0)$ и кольцо частных $Z_i^{-1}R_i = M_{n_i}(D_i)$, где D_i – тело конечномерное над своим центром $Z_i^{-1}Z_i$. При этом $n_i \leq \left[\frac{m}{2}\right]$, где $m = \deg u \geq \deg v$ и $Z_i^{-1}R_i$ удовлетворяет тождеству $u - v = 0$. Если $n_i \geq 2$ и $u = wx_iu'$, $v = wx_jv'$, то, полагая $x_i = E + \lambda e_{11}$, $x_t = E + \lambda(e_{11} + e_{21})$, $\lambda \in Z_i^{-1}Z_i$ и, учитывая равенства $e_{11}^2 = e_{11}(e_{11} + e_{21}) = e_{11}$, $(e_{11} + e_{21})e_{11} = (e_{11} + e_{21}) = (e_{11} + e_{21})^2$, получим, что

$$0 = \lambda g_1 + \lambda^2 g_2 + \ldots + \lambda^{m-e} g_{m-e},$$

где e – длина слова w, g_i – элементы подкольца $\langle e_{11}, e_{11} + e_{21}\rangle$ и g_{m-e} равен либо e_{11}, если $\deg v < \deg u$, либо $(e_{11} - (e_{11} + e_{21}))$, если $\deg u = \deg v$. Откуда следует, что $\left|Z_i^{-1}Z_i\right| \leq m + 1$ и $|R_i| \leq f(m)$, $i \in I$. $\diamondsuit$

Упражнение 4.2. *Пусть $\mathbb{Z}_n$ – кольцо классов вычетов по модулю n. Докажите эквивалентность следующих утверждений:*

1. *$\mathbb{Z}_n$ удовлетворяет некоторому тождеству вида*

$$x = x^m,$$

где $m \geq 2$;

2. *$\mathbb{Z}_n$ удовлетворяет некоторому тождеству вида*

$$x = x^2 f(x),$$

где $f(t) \in \mathbb{Z}[t]$;

3. $n = p_1 p_1 \dots p_s$, *где* p_i – *простое число,* $i \leq s$ *и* $p_i \neq p_j$ *или* $i \neq j$.

Упражнение 4.3. *Пусть* $\mathbb{Z}_n$ – *кольцо классов вычетов по модулю* n. *Докажите, что следующие утверждения эквивалентны:*

1. $\mathbb{Z}_n$ *удовлетворяет некоторому тождеству вида*

$$x^2 = x^3 f(x),$$

где $f(t) \in \mathbb{Z}[t]$;

2. $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, *где* p_i – *простое число и* $\alpha_i \leq 2$, $i \leq s$, $p_i \neq p_j$ *при* $i \neq j$.

Упражнение 4.4. *Пусть* R – F-*алгебра с единицей* (F – *поле*), *удовлетворяющая полилинейному тождеству*

$$f(x_1, \dots, x_d) = x_1 x_2 \dots x_d + \sum_{(i) \neq (1)} \alpha_{(i)} x_{i_1} \dots x_{i_d} = 0,$$

$\alpha_i \in F$ *и* $a, b \in R$ *такие, что* $ab = 1$. *Докажите, что* $ba = 1$.

$\diamondsuit$ Пусть $ba \neq 1$ и $e_{ij} = b^i(1 - ba)a^j$. Тогда $e_{ij} \cdot e_{st} = 0$, если $j \neq s$ и $e_{ij}e_{jt} = e_{it}$. Положим

$$x_1 = e_{12},\ x_2 = e_{23},\ x_3 = e_{34},\ \dots,\ x_d = e_{d(d+1)}.$$

Тогда

$$f\left(e_{12}, e_{23}, \dots, e_{d(d+1)}\right) = e_{1(d+1)}.$$

$\diamondsuit$

Упражнение 4.5. *Докажите, что* $M_2(GF(q))$ *удовлетворяет тождеству*

$$(x - x^q)\left(x - x^{q^2}\right) = 0.$$

$\diamondsuit$ Пусть $a \in M_2(GF(q))$. Тогда a подобна матрице вида

$$\begin{pmatrix} \lambda_1 & \beta \\ 0 & \lambda_2 \end{pmatrix},$$

где $\beta = 0, 1$ и $\lambda_1, \lambda_2 \in GF(q^2)$. $\diamondsuit$

В работе [120] доказано, что $M_n(GF(q))$ удовлетворяет тождеству

$$(x - x^q)\left(x - x^{q^2}\right)\ldots\left(x - x^{q^n}\right) = 0.$$

Упражнение 4.6. *Пусть R – простое кольцо, удовлетворяющее тождеству*

$$x = x^3.$$

Докажите, что R изоморфно либо $GF(2)$, либо $GF(3)$.

Упражнение 4.7. *Докажите, что каждая нильь-подалгебра A алгебры $M_n(F)$, где F – поле, является нильпотентной индекса не превосходящего числа n.*

$\diamondsuit$ Воспользоваться тем, что $S_{2n}(x_1, \ldots, x_{2n}) = 0$ – тождество в простой алгебре $M_n(F)$ и теоремой Амицура-Левицкого из главы 2 о том, что $A^{\left[\frac{2n}{2}\right]}$ содержится в сумме нильпотентных идеалов алгебры $M_n(F)$. $\diamondsuit$

Упражнение 4.8. *Пусть R – алгебра с единицей. Докажите, что*

1. *если $M_n(R)$ удовлетворяет тождеству*

$$S_{2n}(x_1, \ldots, x_n) = 0,$$

то R – коммутативная алгебра (см. [96]);

2. *если $M_n(R)$ удовлетворяет тождеству*

$$S_{n+1}\left(xy^n, xy^{n-1}, \ldots, xy, x\right) = 0,$$

то R – коммутативная алгебра.

$\diamondsuit$ Пусть

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

– тождество, полученное линеаризацией

$$S_{n+1}(xy^n, xy^{n-1}, \ldots, xy, x).$$

Положим

$$y = \sum_{i=1}^{n-1} e_{ii+1} + be_{n1} \in M_n(R),$$

$$x_1 = e_{11},\ x_2 = e_{22},\ \ldots,\ x_n = e_{n1},\ x_{n+1} = ae_{1n},$$

где a, b – произвольные элементы из R. Тогда

$$f = \sum_{i,j=1}^{n} \gamma_{ij} e_{ij} = 0,$$

где $\gamma_{1n} = [a, b]$. $\diamondsuit$

Упражнение 4.9. *Пусть F – поле характеристики нуль. Докажите, что*

$$T\left(M_{n+1}(F)\right) \subseteq T(M_n(F)) \cdot T(M_1(F)),$$

где $n = 1, 2, \ldots$.

$\diamondsuit$ Воспользоваться техникой доказательства теоремы 4.3. $\diamondsuit$

Упражнение 4.10. *Пусть R – PI-алгебра. Докажите, что R удовлетворяет тождеству от двух переменных.*

$\diamondsuit$ Если $f(x_1, \ldots, x_d) = 0$ – тождество алгебры R, то

$$f(xy, xy^2, xy^3, \ldots, xy^d) = 0$$

– тождество от двух переменных алгебры R. $\diamondsuit$

Упражнение 4.11. *Пусть R – нильпотентная алгебра над полем F и $\dim_F R = n$. Докажите, что R удовлетворяет тождествам:*

$$\left[x_1, x_2, \ldots, x_{\left[\frac{n+1}{2}\right]+1}\right] = 0$$

и

$$x_1 x_2 \ldots x_{n-2} = x_{\sigma(1)} \ldots x_{\sigma(n-2)},$$

где σ – произвольная подстановка из S_{n-2}. (см. [48]).

Упражнение 4.12. *Пусть R – регулярная алгебра над полем F. Докажите, что*

1) *для любого элемента $a \in R$ существует элемент $b \in R$ такой, что $aba = a$ и $bab = b$;*

2) *если R удовлетворяет полилинейному тождеству степени три*

$$f(x_1, x_2, x_3) = x_1 x_2 x_3 + \sum_{(i)\neq(1)} \alpha_{(1)} x_{i_1} x_{i_2} x_{i_3} = 0,$$

то R – коммутативная алгебра.

$\diamondsuit$ Пусть $a \in R$ и x – элемент кольца R такой, что $axa = a$. Положим $b = xax$. Тогда $aba = axaxa = axa = a$ и $bab = xaxaxax = xaxax = xax = b$.

Если существует ненулевой элемент $a \in R$ такой, что $a^2 = 0$, то согласно задаче существует элемент $b \in R$ такой, что $aba = a$, $bab = b$. Положим

$$f_{11} = ab(1 - ba),\ f_{12} = a,\ f_{21} = b(1 - ba),\ f_{22} = ba.$$

Тогда

$$\{f_{ij} |\ 1 \leq i, j \leq 2\}$$

– система матричных единиц и

$$R \supseteq F\langle f_{11}, f_{12}, f_{21}, f_{22}\rangle = M_2(F).$$

Подставляя в тождество вместо $x_1 = f_{11}$, $x_2 = f_{12}$, $x_3 = f_{22}$, получим, что $f(f_{11}, f_{12}, f_{22}) = f_{12} = 0$. Противоречие доказывает, что R – алгебра без нильпотентных элементов. По теореме Андрунакиевича-Рябухина (см. главу 2)

$$R = \sum_{i \in I} \bigoplus_{s} R_i$$

– подпрямая сумма алгебр R_i, $i \in I$, без делителей нуля. Каждая алгебра R_i имеет тело частных $Z_i^{-1}R_i = D_i$, где Z_i – центр R_i, которое удовлетворяет тождеству $f(x_1, x_2, x_3) = 0$. Если тело D_i не совпадает со своим центром $Z_i^{-1}Z_i$ и K_i – максимальное подполе D_i, то

$$D_i \bigotimes_{Z_i^{-1}Z_i} K_i \cong M_m(K_i),$$

где $m \geq 2$. Алгебра матриц $M_m(K)$ удовлетворяет тождеству $f(x_1, x_2, x_3) = 0$. Противоречие доказывает, что каждое тело D_i является полем ($i \in I$) и R – коммутативная алгебра. $\diamondsuit$

Упражнение 4.13. *Докажите, что первичное регулярное кольцо без нильпотентных элементов является телом.*

Упражнение 4.14. *Докажите, что регулярное кольцо без нильпотентных элементов является подпрямой суммой тел.*

Упражнение 4.15. *Пусть H – тело кватернионов над полем действительных чисел R. Докажите, что*

$$H \bigotimes_{R} H \cong M_4(R).$$

Упражнение 4.16. *Докажите, что R – регулярное кольцо тогда и только тогда, когда для любого элемента $a \in R$ существует идемпотент $e \in R$ такой, что $aR = eR$.*

Упражнение 4.17. *Пусть R – регулярное кольцо и a, b – произвольные элементы R. Докажите, что*

$$aR + bR = e_1R,$$

где $e_1^2 = e_1$.

$\diamondsuit$ Из упражнения 4.16 следует, что $aR = eR$, где $e^2 = e$ и $bR = fR$, где $f^2 = f$, а также $(1-e)fR = gR$, где $g^2 = g$. Заметим, что $eg = 0$, $(1-e)f = g(1-e)f$. Докажем, что $aR + bR = eR + fR = (e+g)R$. Ясно, что $(e+g)R \subseteq eR + fR$. Обратное включение следует из равенств $(e+g) - (e+g)g = e$ и $ef + (e+g)(f - ef) = [(e+g) - (e+g)g]\, f + (e+g)(f - ef) = f$. $\diamondsuit$

Упражнение 4.18. *Пусть R – регулярное кольцо и a, b – произвольные элементы R. Докажите, что существует элемент $c \in R$ такой, что $aR \cap bR = cR$.*

$\diamondsuit$ Из упражнения 4.16 следует, что $aR = eR$, где $e^2 = e$ и $bR = fR$, где $f^2 = f$, а также $R(f - ef) = Rh$, где $h^2 = h$. Тогда $hf = h$ и $(f - ef)h = f - ef$. Докажем, что $eR \cap fR = (f - fh)R$. Для этого заметим, что $f - fh = ef(1-h) \in eR \cap fR$ и если $x = eu = fv \in eR \cap fR$, то $x = ex = fx$. Откуда следует, что $(f - ef)x = 0$. Пусть $h = w(f - ef)$. Тогда $x = fx = fx - fw((f - ef)x) = fx - fhx = (f - fh)x \in (f - fh)R$. $\diamondsuit$

Упражнение 4.19. *Докажите, что конечное кольцо R является регулярным тогда и только тогда, когда*

$$R = \bigoplus_{i=1}^{k} M_{n_i}(GF(q_i)).$$

Упражнение 4.20. *Пусть F – поле характеристики нуль и M_n – идеал тождеств (в свободной ассоциативной алгебре $F\langle x_1, x_2, \ldots\rangle$) алгебры $M_n(F)$. Докажите, что при $n \geq 2$ M_n не порождается (как T-идеал) многочленом $S_{2n}(x_1, \ldots, x_{2n})$.*

$\diamondsuit$ Докажем, что

$$S_n\left([x^n, y], [x^{n-1}, y], \ldots, [x, y]\right) \in M_n$$

и не принадлежит T-идеалу, порожденному $S_{2n}(x_1, \ldots, x_{2n})$. Пусть $a, b \in M_n(F)$. По теореме Гамильтона-Кэли a – корень своего характеристического многочлена, то есть

$$a^n + \alpha_1 a^{n-1} + \ldots + \alpha_{n-1} a + \alpha_n \cdot E = 0$$

для некоторых элементов $\alpha_i \in F$, $1 \leq i \leq n$. Откуда следует, что

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

Так как

$$S_n(\ldots, x, \ldots, x, \ldots) = 0,$$

то

$$S_n\left([a^n, b], [a^{n-1}, b], \ldots, [a, b]\right) = 0.$$

Предположим противное, то есть

$$S_n\left([x^n, y], [x^{n-1}, y], \ldots, [x, y]\right) \in \{S_{2n}\}^T.$$

Тогда существуют одночлены a_i, b_j, h_k такие, что

$$S_n\left([x^n, y], [x^{n-1}, y], \ldots, [x, y]\right) = \sum a_i S_{2n}(h_1, h_2, \ldots, h_{2n}) b_j.$$

Левая часть этого равенства является однородным многочленом степени $\frac{n(n+1)}{2}$ по x и степени n по y. Следовательно, правая часть является однородным многочленом степени $\frac{n(n+1)}{2}$ по x и степени n по y. Переменная y содержится в не более n одночленах $h_1, h_2, \ldots, h_{2n}$. Следовательно, существуют n одночленов $h_{i_1}, h_{i_2}, \ldots, h_{i_n}$, которые являются степенями переменной x. Так как $S_{2n}(\ldots, 1, \ldots) = 0$, то, можно считать, что $h_1 = x$, $h_2 = x^2$, …, $h_n = x^n$, $h_{n+1} = y$, $h_{n+2} = y$, …, $h_{2n} = y$. Откуда следует, что

$$S_n\left([x^n, y], \ldots, [x, y]\right) = \sum a_i S_{2n}(\ldots, y, \ldots, y, \ldots) = 0.$$

Противоречие. $\diamondsuit$

Упражнение 4.21 (А. Клейн).
Пусть $R = A+B$, где A, B – подкольца кольца R, удовлетворяющие тождеству $x^2 = 0$. Докажите, что R удовлетворяет тождеству $x^8 = 0$.

$\diamondsuit$ Пусть $a + b$ – произвольный элемент R, где $a \in A$, $b \in B$. Тогда

$$(a + b)^8 = (ab + ba)^4 = (ab)^4 + (ba)^4.$$

Пусть $ab = a_1 + b_1$, где $a_1 \in A$, $b_1 \in B$. Тогда

$$0 = a(ab) = aa_1 + ab_1,\ ab_1 = -aa_1 = a_1a.$$

Следовательно,

$$a_1(ab_1) = a_1(a_1a) = 0 \text{ и } (ab_1)a_1 = (-aa_1)a_1 = 0.$$

Пусть, далее, $ba_1 = a_2 + b_2$, где $a_2 \in A$, $b_2 \in B$. Тогда

$$b_2a_1 = (ba_1 - a_2)a_1 = -a_2a_1 = a_1a_2,$$

$$\begin{aligned} a_1b_1a_1b_1 = a_1(a_1 + b_1)a_1b_1 = a_1(ab)a_1b_1 = \\ = a_1a(ba_1)b_1 = a_1a(a_2 + b_2)b_1 = -a_2(a_1a)b_1 + a_1ab_2b_1 = \\ = a_1ab_2b_1 = -a_1ab_1b_2 = 0, \end{aligned}$$

$$\begin{aligned} b_1a_1b_1a_1 = (ab)a_1b_1a_1 = a(ba_1)b_1a_1 = a(a_2 + b_2)b_1a_1 = \\ = aa_2b_1a_1 + ab_2b_1a_1 = -a_2(ab_1a_1) - ab_1b_2a_1 = \\ = 0 - ab_1(a_1a_2) = -(ab_1a_1)a_2 = 0. \end{aligned}$$

Откуда следует, что

$$(ab)^4 = (a_1 + b_1)^4 = (a_1b_1)^2 + (b_1a_1)^2 = 0.$$

Аналогично доказывается, что $(ba)^4 = 0$. Следовательно, $x^8 = 0$ – тождество в кольце R. $\diamondsuit$

Упражнение 4.22 (А. Клейн).
Пусть $R = L_1 + L_2$, где L_1, L_2 – левые идеалы кольца R, удовлетворяющие тождеству $x^n = 0$. Докажите, что R удовлетворяет тождеству $x^N = 0$ для некоторого числа $N \geq 1$.

$\diamondsuit$ Пусть $a + b$ – произвольный элемент в R, где $a \in L_1$, $b \in L_2$. Пусть $S = \langle a, b\rangle$ – подкольцо, порожденное $\{a, b\}$ и $A = S^{\#}a$, $B = S^{\#}b$. Тогда

$$S = A + B,$$

$$A = \left\langle a, ba, b^2a, \ldots, b^{n-1}a \right\rangle \subseteq L_1,$$

$$B = \left\langle b, ab, a^2b, \ldots, a^{n-1}b \right\rangle \subseteq L_2.$$

Из теоремы Ширшова о высоте следует, что существует целое число $M = M(n)$ такое, что $A^M = B^M = (0)$. По теореме Кегеля (см. главу 2) существует целое число $f(M, n)$ такое, что $S^{f(M,n)} = (0)$. В частности, $(a + b)^{f(M,n)} = 0$ и R удовлетворяет тождеству $x^{f(M,n)} = 0$. $\diamondsuit$

Упражнение 4.23 (А. Клейн). *Пусть $R = A + B$, где A, B – подкольца кольца R, $A^m = (0)$ и B удовлетворяет тождеству $x^n = 0$. Докажите, что R удовлетворяет некоторому тождеству вида $x^N = 0$, где N – натуральное число.*

$\diamondsuit$ Рассмотрим левый идеал

$$L = A + RA = A + BA = A + (L \cap B)$$

кольца R и пусть

$$I = r_R(L) \cap L \lhd L.$$

Тогда $I^2 = (0)$, $A^{m-1} \subseteq I$ и

$$L/I = (A + I)/I + ((L \cap B) + I)/I,$$

где $(A+I/I)^{m-1} = (\bar{0})$ и $((L\cap B)+I)/I$ удовлетворяет тождеству $x^n = 0$. Пользуясь методом математической индукции по m,

можно считать, что L/I удовлетворяет тождеству $x^t = 0$, $t \geq 1$, а, следовательно, L удовлетворяет тождеству $x^{t+1} = 0$.

Пусть $a + b$ – произвольный элемент R, где $a \in A$, $b \in B$ и $b^n = 0$. Тогда

$$(a+b)^n = (a+b)^{n-1}a + (a+b)^{n-1}b = \\ = (a+b)^{n-1}a + (a+b)^{n-2}ab + \ldots + (a+b)ab^{n-2} + ab^{n-1},$$

$$(a+b)^n \in L + Lb + \ldots + Lb^{n-1}.$$

Так как L удовлетворяет тождеству $x^{t+1} = 0$, то левые идеалы Lb, Lb^2, …, Lb^{n-1} удовлетворяют тождеству $x^{t+2} = 0$ и согласно предыдущей задаче $L + Lb + \ldots + Lb^{n-1}$ удовлетворяет тождеству $x^M = 0$, где M – некоторое натуральное число. Следовательно, $x^{nM} = 0$ – тождество кольца R. $\diamondsuit$

Упражнение 4.24. *Пусть $R = A + B$, где A, B – подкольца R такие, что $A^2 = (0)$, $B^m = (0)$. Докажите, что*

$$R^{m(m+1)} = (0).$$

$\diamondsuit$ Рассмотрим правый идеал

$$P = A + AR = A + AB = A + (P \cap B)$$

кольца R. Тогда $AP = (0)$ и $P/\ell(P) \cap P$ – нильпотентное кольцо индекса m, то есть $P^m \subseteq \ell(P) \cap P$ и $P^{m+1} = (0)$. Рассмотрим двусторонний идеал $I = P + RP \lhd R$. Тогда $I^{m+1} = (0)$ и $(R/I) \cong B/B \cap I$ – нильпотентное кольцо индекса m. Откуда следует, что $R^{m(m+1)} = (0)$. $\diamondsuit$

Упражнение 4.25. *Докажите, что*

$$x^2 = x^8 \ \textit{и} \ \left[(x + x^2)^3, y\right] = 0$$

– тождества в кольце $M_2(GF(2))$.

$\diamondsuit$ Воспользоваться теоремой Гамильтона-Кэли. $\diamondsuit$

Упражнение 4.26. *Докажите, что*

1. $x^2 = x^{26}$ – *тождество в* $M_2(GF(3))$;
2. $x^3 = x^{87}$ – *тождество в* $M_3(GF(2))$;
3. $x^3 = x^{315}$ – *тождество в* $M_3(GF(3))$.

В работе [87] доказано, что $M_n(GF(p^k))$ удовлетворяет тождеству $x^n = x^{n+E}$, где

$$E = p^t \Phi_1(p^k)\Phi_2(p^k)\dots\Phi_n(p^k),$$

t – наименьшее целое число такое, что $p^t \geq n$, $\Phi_m(x)$ – m-й круговой многочлен из $\mathbb{Z}[x]$. Более того, $x^r = x^{r+s}$ – тождество в $M_n(GF(p^k))$ тогда и только тогда, когда $r \geq n$ и E делит s.

Тождества от одной переменной кольца $M_n(GF(q))$ изучались также в работах [106, 120]

Упражнение 4.27. *Пусть R – кольцо с единицей, удовлетворяющее тождеству $(xy)^2 = x^2y^2$. Докажите, что R – коммутативное кольцо.*

$\diamondsuit$ Пусть a, b – произвольные элементы из R. Тогда $((a+1)b)^2 = (a+1)^2b^2$ и $(bab) = ab^2$. Откуда следует, что $xay + yax = a(xy+yx)$ для любых элементов $x, y \in R$. Полагая в последнем равенстве $x = 1$, получаем, что $ya = ay$. $\diamondsuit$

Упражнение 4.28. *Пусть*

$$R = \left\{ \left(\begin{array}{ccc} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{array} \right) \middle| \; a, b, c, d \in GF(2) \right\}.$$

Докажите, что R удовлетворяет тождествам

$$[x^4 - x^8, y] = 0, \; [x^5 - x^9, y] = 0.$$

Упражнение 4.29. *Пусть*

$$R = \left\{ \left(\begin{array}{ccc} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{array} \right) \middle| \ a, b, c, d \in GF(3) \right\}.$$

Докажите, что R удовлетворяет тождествам

$$[x^3 - x^6, y] = 0, \ [x^4 - x^{10}, y] = 0.$$

Упражнение 4.30. *Пусть I – левый идеал кольца R, удовлетворяющий тождеству $x^2 = 0$. Докажите, что двусторонний идеал*

$$IR = \sum_{k=1}^{n} i_k a_k,$$

$i_k \in I$, $a_k \in R$ удовлетворяет тождеству $x^3 = 0$.

$\diamondsuit$ Пусть $u, u_1 \in I$ и $v, v_1 \in R$. Тогда

$$uu_1 + u_1 u = (u + u_1)^2 - u^2 - u_1^2 = 0,$$

$$uvu = -(vu)u = 0, \ uvu_1 = -(vu_1)u = v(uu_1) = -u_1 vu,$$

$$vuv_1 u_1 = -(v_1 u_1)(vu) = v_1(vu)u_1 = -v(v_1 u_1)u = vv_1(uu_1).$$

Пусть $a = \sum\limits_{k=1}^{n} i_k a_k$ – произвольный элемент из IR, $i_k \in I$, $a_k \in R$, $k \leq n$. Тогда

$$\begin{aligned} a^3 = \left(\sum_{m=1}^{n} i_m a_m \right) \left(\sum_{s=1}^{n} i_s a_s \right) \left(\sum_{t=1}^{n} i_t a_t \right) = \\ = \sum_{m,s,t} i_m a_m i_s a_s i_t a_t = \sum_{m,s,t} i_m (a_m a_s i_s i_t) a_t = \\ = -\sum_{m,s,t} (a_m a_s i_s i_t i_m) a_t = \sum_{m,s,t} a_m a_s i_m i_s i_t a_t = \\ = \sum_{m<s,t} a_m a_s (i_m i_s + i_s i_m) i_t a_t = 0. \end{aligned}$$

$\diamondsuit$

Упражнение 4.31. *Пусть $R = F\langle a_1, \ldots, a_k\rangle$ – конечно порожденная алгебра над полем F, удовлетворяющая полилинейному тождеству степени три. Докажите, что каждый элемент алгебры R является линейной комбинацией элементов вида $a_{i_1}^{t_1} a_{i_2}^{t_2} \ldots a_{i_h}^{t_h}$, где $h \leq 2k$.*

$\diamondsuit$ Пусть $a = a_{j_1}^{e_1} \ldots a_{j_s}^{e_1}$ – слово от порождающих элементов $\{a_1, \ldots, a_k\}$ и $s \geq 2k+1$. Тогда существует индекс $i \leq k$ такой, что

$$a = u\,(a_i^e v a_i^p w a_i^m)\,b.$$

Так как R удовлетворяет тождеству

$$x_1x_2x_3 = \lambda_1 x_2x_1x_3 + \lambda_2 x_1x_3x_2 + \lambda_3 x_3x_1x_2 + \lambda_4 x_3x_2x_1 + \lambda_5 x_2x_3x_1,$$

то, подставляя в него вместо $x_1 = a_i^e v$, $x_2 = a_i^p$, $x_3 = w a_i^m$, получим, что

$$\begin{aligned}(a_i^e v a_i^p w a_i^m) = \lambda_1 (a_i^{p+e} v w a_i^m) + \lambda_2 (a_i^e v w a_i^{m+p}) + \\ + \lambda_3 (w a_i^{m+e} v a_i^p) + \lambda_4 (w a_i^{m+p+e} v) + \lambda_5 (a_i^p w a_i^{m+e} v).\end{aligned}$$

Таким образом, слово a является линейной комбинацией слов меньшей высоты (в смысле А. Ширшова). $\diamondsuit$

Упражнение 4.32. *Пусть $R = F\langle a, b\rangle$ – 2-порожденная алгебра над полем F, удовлетворяющая полилинейному тождеству степени три. Докажите, что если $a^n = b^n = 0$, то $R^{4n-3} = (0)$.*

$\diamondsuit$ Согласно предыдущей задаче произвольный элемент R^{4n-3} является линейной комбинацией слов

$$a^{t_1} b^{t_2} a^{t_3} b^{t_4},$$

где $t_1 + t_2 + t_3 + t_4 \geq 4n - 3$. Следовательно, некоторое число $t_i \geq n$ и слово $a^{t_1} b^{t_2} a^{t_3} b^{t_4} = 0$, то есть $R^{4n-3} = (0)$. $\diamondsuit$

В силу теоремы А. Ширшова о высоте (см. [61]) каждый элемент конечнопорожденной алгебры $R = F\langle a_1, \ldots, a_k\rangle$, удовлетворяющей полилинейному тождеству степени n, представим в виде линейной комбинации слов $v_1^{e_1} \ldots v_h^{e_h}$, где v_i – слова длины $\leq (n-1)$ от $\{a_1, \ldots, a_k\}$ и $h(n,k)$ – некоторое фиксированное число (называемое высотой алгебры R). В работе [119] приведена оценка

$$h(n,k) \leq 2n^6 k^{2n+2}.$$

В работе [60] доказано, что

$$h(3,k) \leq 2k, \quad h(4,k) \leq 7k^2 - 2k$$

и сформулирована гипотеза о том, что

$$h(n,k) \leq O\left(k^{[n/2]}\right).$$

Упражнение 4.33. *Пусть алгебра R удовлетворяет полилинейному тождеству степени три и*

$$N_r(R) = \{a \in R \mid aR \text{ – ниль-идеал ограниченного индекса }\}.$$

Докажите, что $N_r(R) \lhd R$ и $R/N_r(R)$ – коммутативная алгебра.

$\diamondsuit$ Пусть $S = \prod_R R$ и $\varphi : R \to S$ – вложение алгебры R в S такое, что для любого элемента $a \in R$, $\varphi(a) = (a, a, a, \ldots)$. Пусть N – нижний ниль-радикал S, $(a, a, a, \ldots) \in N \cap R$ и g – такой элемент из S, что $g(r) = r$ для любого $r \in R$. $g = (\ldots, rr, \ldots) \in S$, то есть $g(r) = r$ для любого $r \in R$. Тогда $(a, a, \ldots)g = (\ldots, ar, \ldots)$ – нильпотентный элемент в S и, следовательно, aR – ниль правый идеал ограниченного индекса, то есть $a \in N_r(R)$. Это доказывает, что идеал $N \cap R = N_r(R)$. Полупервичная алгебра S/N является коммутативной и содержит подалгебру $(R+N)/N \cong R/N_r(R)$. $\diamondsuit$

Упражнение 4.34. *Пусть R – регулярное кольцо. Докажите, что кольцо матриц $M_n(R)$ является регулярным.*

$\diamondsuit$ Справедлива следующая лемма (Н. Маккоя).
Пусть a, x – элементы кольца S такие, что существует элемент $y \in S$, удовлетворяющий условию

$$(axa - a)y(axa - a) = (axa - a).$$

Тогда существует элемент $t \in S$ такой, что $ata = a$.

Действительно, достаточно положить

$$t = (x - y + xay + yax - xayax).$$

Пусть

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$$

и $crc = c$. Тогда

$$A \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} A - A = \begin{pmatrix} arc - a & ard - b \\ 0 & crd - d \end{pmatrix}.$$

Таким образом, согласно лемме, решение задачи достаточно провести для матриц вида

$$B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(R).$$

Пусть $x, y \in R$ такие, что $axa = a$ и $cyc = c$. Тогда

$$B \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} B - B = \begin{pmatrix} 0 & axb - b \\ 0 & 0 \end{pmatrix}.$$

опять согласно лемме решение задачи достаточно осуществить для матриц вида

$$C = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}.$$

Если $czc = c$, то

$$C \begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix} C = C.$$

Итак, $M_2(R)$ – регулярное кольцо, откуда следует, что кольцо $M_{2^n}(R)$ является регулярным. Кольцо $M_n(R)$ изоморфно подкольцу матриц вида

$$\left\{ \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \middle| \text{ где } A \in R_n \right\} \subseteq M_{2^n}(R)$$

и, следовательно, тоже является регулярным. $\diamondsuit$

Упражнение 4.35. *Пусть R – кольцо, удовлетворяющее тождеству $x = x^{14}$. Докажите, что R удовлетворяет тождеству $x = x^2$.*

Упражнение 4.36. *Докажите, что кольцо R удовлетворяет тождеству $x = x^{20}$ тогда и только тогда, когда R удовлетворяет тождеству $x = x^2$.*

Упражнение 4.37. *Пусть $A = F\langle a_1, \ldots, a_n \rangle$ – конечнопорожденная алгебра над полем F и I – идеал A конечной размерности, то есть $\dim_F A/I < \infty$. Докажите, что I – конечнопорожденная F-алгебра.*

$\diamondsuit$ Пусть $\{\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}, \ldots, \bar{a}_m\}$ – система порождающих элементов F-пространства A/I и $\{a_1, \ldots, a_n, \ldots, a_m\}$ – их прообразы в A. Пусть также

$$a_i a_j = \sum_k \alpha_{ijk} a_k + b_{ij},$$

где $b_{ij} \in I$. Обозначим через K – подалгебру, порожденную $\{b_{ij}, a_k b_{ij}, b_{ij} a_k, a_s b_{ij} a_t\} \subseteq I$. Тогда $K \lhd A$ и $\dim_F A/K < \infty$. $\diamondsuit$

Упражнение 4.38. *Пусть R – бесконечномерная алгебра над полем F. R называется почти бесконечномерной, если для любого ненулевого идеала $I \lhd R$, $\dim_F R/I < \infty$.*

1. *Докажите, что алгебра многочленов $F[x]$ является примером почти бесконечномерной алгебры.*

2. *Приведите пример конечнопорожденной почти бесконечномерной алгебры, не удовлетворяющей тождеству.*

$\diamondsuit$ Пусть $R = F\langle a_1, a_2, a_3\rangle$ – конечнопорожденная ниль-алгебра, не являющаяся нильпотентной (пример Голода Е., см. главу 2) и

$$\Phi = \{I \lhd R \mid R/I \text{ – бесконечномерная алгебра}\}.$$

Из упражнения 4.37 и леммы Цорна следует, что $\mathfrak{M}$ содержит максимальный идеал I_0. Если бы алгебра R/I_0 удовлетворяла бы тождеству, то по теореме Левицкого она была бы нильпотентной, то есть $\dim R/I_0 < \infty$. Противоречие. $\diamondsuit$

Упражнение 4.39. *Пусть A – кольцо, содержащее единицу. Докажите, что в $M_n(A)$ существуют такие элементы a, f, что $f^n = 0$ и $1 = af^{n-1} + faf^{n-2} + f^2af^{n-3} + \ldots + f^{n-1}a$.*

$\diamondsuit$ Проверить, что $a = e_{12}$, $f = e_{21} + e_{32} + \ldots + e_{n\ n-1}$ удовлетворяют выше приведенным равенствам. $\diamondsuit$

Замечание. В работе [110] доказано обратное утверждение. Точнее, если в R существуют такие элементы $a_1, a_2, \ldots, a_n, f$, что $f^n = 0$ и $1 = a_1f^{n-1} + fa_2f^{n-2} + f^2a_3f^{n-3} + \ldots + f^{n-1}a_n$, то $R = M_n(A)$, для некоторого кольца A.

Упражнение 4.40. *Пусть*

$$A = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot i + \mathbb{Z}\cdot j + \mathbb{Z}\cdot k$$

– подкольцо в теле кватернионов

$$\mathbb{H} = \mathbb{R}\cdot 1 + \mathbb{R}\cdot i + \mathbb{R}\cdot j + \mathbb{R}\cdot k,$$

порожденное $\{1, i, j, k\}$. Пусть I – ненулевой правый идеал R. Докажите, что $\langle A/I, +\rangle$ – конечная абелева группа.

$\diamondsuit$ Если $a = a_0 + a_1 i + a_2 j + a_3 k$ – ненулевой элемент I, то $N(a) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \in I$ и A/I – конечно порожденный $\mathbb{Z}/(N)$-модуль. $\diamondsuit$

Упражнение 4.41. *Пусть V – некоторое пространство над бесконечным полем F и $W_1, \ldots, W_n$ – его собственные подпространства. Докажите, что $V \neq \bigcup\limits_{i=1}^{n} W_i$.*

$\diamondsuit$ Воспользуемся методом математической индукции по числу n. Можно предполагать, что существуют векторы $v_i \notin \bigcup\limits_{j \neq i} W_j$, $v_i \in W_i$, $1 \leq i \leq n$. Рассмотрим бесконечное множество векторов

$$\left\{ v_1 + \alpha v_2 + \alpha^2 v_3 + \ldots + \alpha^{n-1} v_n \;\middle|\; \alpha \in F \right\}.$$

Найдется подпространство W_{i_0} и различные элементы поля F $\{\alpha_1, \ldots, \alpha_n\}$ такие, что

$$\sum_{k=0}^{n-1} \alpha_i^k v_{k+1} \in W_{i_0}.$$

Откуда следует, что $v_i \in W_{i_0}$, $1 \leq j \leq n$. Противоречие. $\diamondsuit$

Заметим, что в случае конечного поля F конечномерное пространство V является объединением всех своих одномерных подпространств (их конечное число).

Упражнение 4.42. *Докажите, что $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$.*

$\diamondsuit$ Пусть $A = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$,

$$e = \frac{1 + (i \otimes i)}{2}, \quad j = \frac{(1 \otimes i) - (i \otimes 1)}{2}.$$

Тогда $e^2 = e$, $j^2 = -e$, $Ae = Re + Rj \cong \mathbb{C}$ и $A = Ae \oplus A(1-e)$. $\diamondsuit$

Упражнение 4.43. *Пусть*

$$H = \mathbb{R} \cdot 1 + \mathbb{R} \cdot i + \mathbb{R} \cdot j + \mathbb{R} \cdot k$$

– тело кватернионов,

$$A = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot i + \mathbb{Z} \cdot j + \mathbb{Z} \cdot k$$

– его подкольцо. Пусть p – простое число. Докажите, что

$$A/pA \cong M_2(GF(p)),$$

если p – нечетное число и $S = A/2A$ – коммутативная $GF(2)$-алгебра такая, что $S/J(S) \cong GF(2)$ и радикал $J(S)$ имеет базис $\{1+i, 1+j, 1+k\}$.

Упражнение 4.44. *Докажите, что нильпотентное кольцо R удовлетворяет условию максимальности для двусторонних идеалов тогда и только тогда, когда $\langle R, + \rangle$ – конечнопорожденная абелева группа.*

Упражнение 4.45. *Докажите, что произвольное подкольцо конечнопорожденного нильпотентного кольца является конечнопорожденным кольцом.*

Упражнение 4.46. *Докажите, что нильпотентное кольцо R удовлетворяет условию минимальности для двусторонних идеалов тогда и только тогда, когда абелева группа $\langle R, + \rangle$ удовлетворяет условию минимальности для подгрупп.*

Упражнение 4.47. *Докажите, что абелева группа G удовлетворяет условию минимальности для подгрупп тогда и только тогда, когда G – конечная прямая сумма циклических и квазициклических групп вида $C_{p_i^{n_i}}$, где $1 \leq n_i \leq \infty$, p_i – простое число.*

Упражнение 4.48. *Пусть R – кольцо и Φ_R – пересечение всех максимальных правых идеалов кольца R, если они есть. Если же R не содержит максимальных правых идеалов, то положим $\Phi_R = R$. Правый идеал Φ_R называется подкольцом Фраттини. Докажите, что*

1) $\Phi_R = \{a \in R \mid$ *если* $[S,a]_r = R$, *то* $[S]_r = R\}$, *где* $[T]_r$ – *правый идеал кольца* R, *порожденный подмножеством* $T \subseteq R$;

2) $RJ(R) \subseteq \Phi_R \subseteq J(R)$;

3) если R – *нильпотентное* p – *кольцо, то* $\Phi_R = R^2 + pR$ *(*R *называется* p*-кольцом, где* p – *простое число, если для любого элемента* $a \in R$ *существует целое число* $n \geq 1$ *такое, что* $p^n a = 0$*).*

Упражнение 4.49 (Р. Рагхавендран).
Пусть $F = GF(q)$ *и* V – (F,F)*-бимодуль и* V – *конечномерное левое* F *- пространство. Докажите, что существует такой базис*

$$F \cdot x_1 + F \cdot x_2 + \ldots + F \cdot x_n = V$$

и такие автоморфизмы

$$\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}F,$$

что для любого элемента $\alpha \in F$

$$x_i a = \sigma_i(a) x_i, \quad i \leq n.$$

$\diamondsuit$ Если $\dim_F V = 1$, то есть $Fv = V$, то для любого элемента $a \in F$, $va = a_1 v$. Следовательно, отображение $a \to a_1 = \sigma(a)$ удовлетворяет свойствам $v(ab) = a_1 vb = a_1 b_1 v$ и $(ab)_1 = a_1 b_1$, $v(a+b) = (a_1 + b_1)v$. Отсюда $(a+b)_1 = a_1 + b_1$, то есть v – искомый базис и $\sigma \in \mathrm{Aut}F$.

Пусть $\{y_1, \ldots, y_n\}$ – левый F-базис V, то есть

$$V = F \cdot y_1 + \ldots + F \cdot y_n$$

и g – циклический образующий $F^* = F \backslash \{0\}$. Тогда

$$y_1 \cdot g = \sum_{k=1}^{n} a_{1k} y_k, \ \ldots, \ y_n \cdot g = \sum_{k=1}^{n} a_{nk} y_k,$$

то есть

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} g = G \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

где

$$G = \begin{pmatrix} a_{12} & a_{12} & \dots & a_{1n} \\ \vdots & & & \\ a_{n1} & \dots & & a_{nn} \end{pmatrix} \in M_n(F).$$

При этом $Y \cdot g^k = G^k \cdot Y$ для любого $k \geq 1$.

Далее, если $A, B \in M_n(F)$ и $A \cdot Y = B \cdot Y$, то $(A-B)Y = (0)$ и так как $\{y_1, \dots, y_n\}$ – базис V, то $A - B = 0$ и $A = B$. Так как $g^{q-1} = 1$, то $E \cdot Y = G^{q-1} \cdot Y$, следовательно, $G^{q-1} = E$. Рассмотрим отображение

$$0 \to 0$$

$$g \to G$$

$$g^2 \to G^2$$

$$\vdots$$

$$g^{q-1} \to G^{q-1},$$

то есть, $\varphi(g^k) = G^k$, $k \leq q-1$. Тогда

$$Y(g^s + g^t) = Y \cdot g^e = G^e \cdot Y = Y \cdot g^s + Y \cdot g^t = (G^s + G^t)Y$$

и $G^e = G^s + G^t$, то есть,

$$\varphi(g^s + g^t) = \varphi(g^e) = G^e = \varphi(g^s) + \varphi(g^t).$$

Это означает, что

$$\varphi : F \to M_n(F)$$

– аддитивное отображение и $Y \cdot g^s \cdot g^t = G^{s+t}Y$. Следовательно, φ – изоморфизм, то есть множество $\{0, G, G^2, \dots, G^{q-1}\}$ – поле, изоморфное $GF(q) = F$.

Пусть $p(x)$ – минимальный многочлен для G. Тогда

$$p(\lambda)|(\lambda^q - \lambda) = (\lambda - 0)(\lambda - g)\dots(\lambda - g^{q-1}).$$

То есть $p(\lambda)$ без кратных корней. Это означает, что G подобна в $M_n(F)$ диагональной матрице, то есть существует невырожденная $Q \in M_n(F)$ такая, что

$$QGQ^{-1} = \mathrm{diag}(g_1, \dots, g_n) = D.$$

Пусть $g_1^s = g_1^t$. Тогда $Q(G^s - G^t)Q^{-1} = Q(D^s - D^t)Q^{-1}$ – вырожденная матрица, а значит $G^s - G^t$ – вырожденная матрица из поля $\{0, G, \dots, G^{q-1}\}$, то есть, $G^s = G^t$. Рассмотрим отображение : $F \to F$

$$g^k \to g_1^k.$$

Это мультипликативный гомоморфизм (если $g^s = g^t$, то $(s-t)$: $q-1$ и $g_1^s = g_1^t$) и $g^s + g^t = g^e$ влечет за собой $G^s + G^t = G^e$. Откуда следует, что $g_1^s + g_1^t = g_1^e$, то есть это аддитивный гомоморфизм и если $g_1^s = g_1^t$, то $G^s = G^t$ и $g^s = g^t$, то есть это автоморфизм поля F, а значит $\sigma_1(g) = g_1$. Пусть

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = QY$$

– новый левый базис V. Тогда

$$Xg = QYg = QGY = (QGQ^{-1})X = DX = \begin{pmatrix} g_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & g_n \end{pmatrix} X$$

и $x_i g = \sigma_i(g) x_i$. То есть, $\{x_1, \dots, x_n\}$ – искомый базис V. $\diamondsuit$

Глава 5

Условия коммутативности колец

В 1905 году американский математик Д. Веддерберн доказал, что произвольное конечное тело является полем. В конечном теле D произвольный элемент $a \in D$ равен некоторой своей степени $a = a^{n(a)}$, где $n(a) \geq 2$. Естественно возникнет вопрос о коммутативности произвольного тела D, в котором каждый элемент $a \in D$ равен некоторой своей степени $a = a^{n(a)}$, где $n(a) \geq 2$. Оказывается, ответ на этот вопрос положительный (см. теорему 5.2) не только для тел, но и для произвольного ассоциативного кольца. Этот выдающийся результат был доказан американским математиком Н. Джекобсоном в 40-х годах прошлого столетия. Его доказательство - хорошая иллюстрация того, как работает на практике теория радикала Джекобсона и теорема плотности. В дальнейшем теорема Джекобсона обобщалась различными авторами (И. Капланский, И. Херстейн, К. Фейс и др.) и в настоящее время область современной теории ассоциативных колец, в которой рассматриваются те или иные условия, влекущие коммутативность исходного кольца, называется "теоремы коммутативности" или "условия коммутативности для колец"(история развития этого направления подробно изложена в статье [108]).

5.1. Некоммутативные евклидовы кольца, конечные тела и корни многочленов с коэффициентами из тела

Пусть

$$\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right) = \mathbb{R}\cdot 1 + \mathbb{R}\cdot i + \mathbb{R}\cdot j + \mathbb{R}\cdot k$$

– *тело кватернионов*, то есть четырехмерная алгебра над полем действительных чисел $\mathbb{R}$ с базисом $\{1, i, j, k\}$ и следующей таблицей умножения:

$$i^2 = j^2 = k^2 = -1,$$

$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j,$$

$$1^2 = 1,\ i\cdot 1 = 1\cdot i = i,\ j\cdot 1 = 1\cdot j = j,\ k\cdot 1 = 1\cdot k = k.$$

Из таблицы умножения следует, что $\mathbb{H}$ – ассоциативная алгебра с единицей 1. Ее элементы называются кватернионами. Пусть

$$x = a_0 1 + a_1 i + a_2 j + a_3 k \in \mathbb{H}.$$

Положим

$$x^* = a_0 1 - a_1 i - a_2 j - a_3 k$$

и

$$N(x) = xx^*.$$

Элемент x^* называется *сопряженным элементом к* x, а $N(x)$ называется *нормой элемента* x.

Непосредственной проверкой подтверждается справедливость равенств

$$N(x) = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

$$(x+y)^* = x^* + y^*,$$

$$(\alpha x)^* = \alpha x^*,\ \alpha \in \mathbb{R},$$

$$(xy)^* = y^* x^*,$$

где x, y – произвольные кватернионы.

Действительно, первые три свойства очевидны. Из них следует, что четвертое равенство достаточно проверить для базисных элементов. Например,

$$(ij)^* = k^* = -k = ji = j^* i^*.$$

Рассмотрим

$$N(xy) = (xy)(xy)^* = (xy)(y^* x^*) = x(yy^*)x^* = N(x) \cdot N(y).$$

Следовательно, если

$$x = a_0 \cdot 1 + a_1 i + a_2 j + a_3 k,$$

$$y = b_0 \cdot 1 + b_1 i + b_2 j + b_3 k,$$

то

$$\begin{aligned} N(xy) = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3)^2 + \\ + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)^2 + (a_2 b_0 + a_0 b_2 + a_3 b_1 - a_1 b_3)^2 + \\ + (a_0 b_3 + a_3 b_0 + a_1 b_2 - a_2 b_1)^2 = N(x)N(y) = \\ = (a_0^2 + a_1^2 + a_2^2 + a_3^2)(b_0^2 + b_1^2 + b_2^2 + b_3^2). \end{aligned}$$

Таким образом, мы доказали знаменитое тождество Лагранжа.

Заметим далее, что $\mathbb{H}$ является алгеброй с делением (телом). Действительно, для любого ненулевого кватерниона x справедливо равенство

$$x \cdot \frac{x^*}{N(x)} = 1 = \frac{x^*}{N(x)} \cdot x,$$

то есть

$$x^{-1} = \frac{x^*}{N(x)}.$$

Кватернионы были впервые введены в работе У. Гамильтона "On quaternions, or on a new system of imaginaries in algebra"

(1843 г.). А. Пуанкаре сравнивал открытие таких систем в алгебре с открытием неевклидовой геометрии.

Пусть

$$\xi = \frac{1}{2}(1 + i + j + k) \in \mathbb{H}.$$

Рассмотрим абелеву группу

$$\Gamma = \mathbb{Z} \cdot \xi + \mathbb{Z} \cdot i + \mathbb{Z} \cdot j + \mathbb{Z} \cdot k,$$

порожденную ξ, i, j, k. Докажем, что Γ – подкольцо $\mathbb{H}$. Для этого достаточно заметить, что

$$2\xi - i - j - k = 1 \in \Gamma,$$

$$\xi^2 = \xi - 1 \in \Gamma,$$

$$\xi \cdot i = \xi - 1 - k \in \Gamma.$$

Итак, $\Gamma \leq \mathbb{H}$. Кольцо Γ называется *кольцом Гурвица.*

Лемма 5.1. *Если $x \in \Gamma$, то $x^* \in \Gamma$ и $N(x) \in \mathbb{N}$.*

□ Пусть

$$x = m_0\xi + m_1 i + m_2 j + m_3 k \in \Gamma,$$

где $m_i \in \mathbb{Z}$, $i \leq 3$. Тогда

$$x^* = m_0\xi^* - m_1 i - m_2 j - m_3 k = m_0(1-\xi) - m_1 i - m_2 j - m_3 k \in \Gamma$$

и

$$N(x) = m_0^2 + m_1^2 + m_2^2 + m_3^2 + m_0 m_1 + m_0 m_2 + m_0 m_3 \in \mathbb{N}.$$

□

Лемма 5.2. Γ *– евклидово кольцо, то есть для любых элементов $a, b \in \Gamma$, $b \neq 0$ существуют такие элементы $c, d \in \Gamma$, что $a = cb + d$, где $N(d) < N(b)$.*

□ Пусть $b = n$ – натуральное число и

$$a = a_0\xi + a_1 i + a_2 j + a_3 k.$$

Будем искать элемент c в виде

$$c = x_0\xi + x_1 i + x_2 j + x_3 k,$$

где целые числа x_0, x_1, x_2, x_3 выберем подходящим образом. Рассмотрим разность

$$a - cn = \left(\frac{a_0 - x_0 n}{2}\right)\cdot 1 + \left(\frac{a_0 + 2a_1 - (x_0 + 2x_1)n}{2}\right)\cdot i +$$
$$+ \left(\frac{a_0 + 2a_2 - (x_0 + 2x_2)n}{2}\right)\cdot j + \left(\frac{a_0 + 2a_3 - (x_0 + 2x_3)n}{2}\right)\cdot k.$$

Выберем целое число x_0 так, чтобы $|a_0 - x_0 n| \le n/2$. По лемме о делении с остатком (в $\mathbb{Z}$)

$$a_0 + 2a_1 = (x_0 + y_1)n + r,$$

где $0 \le r < n$. Если y_1 – четное число, то положим $x_1 = y_1/2$. Если y_1 – нечетное число, то из равенства

$$a_0 + 2a_1 = (x_0 + y_1 + 1)n + (r - n)$$

следует, что $|r - n| < n$, $(y_1 + 1)$ – четное число. Положим в этом случае $x_1 = (y_1 + 1)/2$. Аналогично найдем целые числа x_2, x_3. Тогда

$$N(a - cn) \le \frac{n2}{16} + \frac{n2}{4} + \frac{n2}{4} + \frac{n2}{4} < n2.$$

Таким образом, лемма доказана в том частном случае, когда $b = n \in \mathbb{N}$.

Пусть b – произвольный ненулевой элемент Γ. Положим $n = N(b) = b\cdot b^*$. В силу доказанного, имеем $ab^* = c\cdot n + r$, где $r, c \in \Gamma$ и $N(r) < n^2$. Откуда следует, что

$$N(r) = N(ab^* - cbb^*) = N(a - cb)N(b^*) = N(a - cb)\cdot n < n^2.$$

Следовательно, $N(a - cb) < N(b)$. □

Лемма 5.3. Γ – *кольцо главных левых идеалов.*

□ Пусть I – ненулевой левый идеал Γ и a – элемент и I с минимальной ненулевой нормой. Покажем, что $I = ra$. Пусть $i \in I$. По лемме 5.2 существуют элементы $c, r \in \Gamma$ такие, что $i = ca + r$, где $N(r) < N(a)$. Так как $r = i - ca \in I$ и $N(r) < N(a)$, то $r = 0$ и $i \in \Gamma A$. Таким образом, $I = \Gamma a$. □

Лемма 5.4. *Пусть R – кольцо с единицей. Если R не содержит собственных ненулевых левых идеалов, то R – тело.*

□ Пусть $a \neq 0 \in R$. Рассмотрим ненулевой левый идеал Ra. По условию $R = Ra$. Следовательно, существует элемент $b \in R$ такой, что $1 = ba$. Из равенства $(1 - ab)a = 0$ следует, что $1 - ab = 0$, либо левый идеал $\ell(a) = \{x \in R |\ xa = 0\} \neq 0$. В последнем случае $1 \in R = \ell(a)$. Противоречие. То есть R – кольцо с делением. □

Теорема 5.1 (Д. Веддерберн).
Конечное тело является полем.

□ Пусть D – конечное тело и e – единица в D. Среди элементов $\{e, 2e, 3e, \ldots\}$ найдутся два равных: $ae = be$, где $a < b$. Следовательно, $(b - a)e = 0$. Пусть

$$p = \min\{n \in N |\ n \cdot e = 0\}.$$

Тогда p – простое число. Действительно, если $p = st$, $1 < t < p$, $1 < s < p$, то из равенства $pe = (se)(te) = 0$ следует, что тело D содержит делители нуля. Противоречие. Итак, p – простое число (называемое характеристикой тела D) и

$$\mathbb{Z}_p = \{0, e, 2e, \ldots, (p-1)e\}$$

содержится в центре Z тела D. Тело D можно рассматривать как векторное пространство на полем $\mathbb{Z}_p$ (или над Z). Если $\dim_{\mathbb{Z}_p} D = a$, $\dim_Z D = n$, $\dim_{\mathbb{Z}_p} Z = b$, то $q = |Z| = p^b$, $|D| = p^a$, $D = q^n$ и $a = b \cdot n$.

Предположим, что $D \neq Z$. Тогда $n > 1$. Из разбиения группы $G = \langle D\backslash\{0\}, \cdot\rangle$ на классы сопряженных элементов следует известное равенство

$$|G| = |D\backslash\{0\}| = q^n - 1 = |Z\backslash\{0\}| + \sum_{x \notin Z} |G : N_G(x)|.$$

Для любого элемента $x \notin Z$ его централизатор $N_{G(x)}$ в G, объединенный с 0, является подтелом, содержащим Z. Следовательно, $|N_G(x)| = q^d - 1$, где d – собственный делитель n. Таким образом, из предположения, что $n > 1$, следует равенство

$$q^n - 1 = (q-1) + \sum_{\substack{d|n \\ 1 \leq d < n}} \frac{(q^n - 1)}{(q^d - 1)},$$

где суммирование во втором слагаемом берется по некоторым делителям числа n.

Покажем, что полученное равенство невозможно. Рассмотрим n -й круговой многочлен

$$\Phi_n(x) = \prod_{\substack{1 \leq i < n \\ (i,n)=1}} (x - \varepsilon^i) \in \mathbb{C}[x],$$

где

$$\varepsilon = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}.$$

Так как

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1 \in \mathbb{Z}[x],$$

то мы можем сделать предположение индукции о том, что

$$\Phi_k(x) \in \mathbb{Z}[x],$$

при $k \leq n - 1$. Так как

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{\substack{n > d \\ d|n}} \Phi_d(x),$$

то $\Phi_n(x) \in \mathbb{Z}[x]$. В частности, $\Phi_n(q)$ – делитель чисел

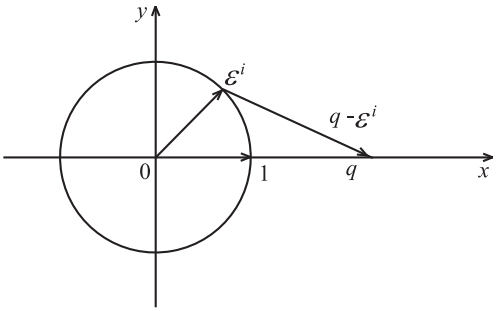
$$(q^n - 1), \quad \frac{q^n - 1}{q^d - 1},$$

где $d < n,\ d|n$. Следовательно,

$$\Phi_n(q)|(q-1).$$

Далее,

$$|\Phi_n(q)| = \left| \prod_{\substack{1 \le d < n \\ (i,n)=1}} (q - \varepsilon^i) \right| > (q-1).$$



Противоречие доказывает теорему. □

Приведем второе доказательство теоремы Веддерберна, основываясь на теореме Нетер-Сколема о том, что если тело D является конечномерным над своим центром Z и K_1, K_2 – максимальные подполя D, изоморфные как Z – алгебры, то

$$K_2 = x^{-1} K_1 x$$

для некоторого элемента $x \in D$ (см. [22]).

Пусть D – конечное тело, Z – его центр. Предположим, что $D \neq Z$. Тогда $[D : Z] = n^2$, каждый элемент содержится в максимальном подполе и если K – максимальное подполе, то

$[K : Z] = n$ и $|K| = q^n$, где $q = |Z|$. Поэтому $D = \bigcup\limits_{x \neq 0} \left(x^{-1} K x\right)$ и мультипликативная группа ненулевых элементов

$$D^* = D \setminus \{0\} = \bigcup_{x \neq 0} \left(x^{-1} K^* x\right),$$

где $K^* = K \setminus \{0\}$. Это равенство невозможно, так как справедлива следующая лемма.

Лемма 5.5. *Пусть H – собственная подгруппа конечной группы G ($G \neq \langle e \rangle$). Тогда*

$$G \neq \bigcup_g g^{-1} H g.$$

□ Действительно, пусть

$$N(H) = \{a|\ a^{-1} H a = H\}.$$

Тогда $H \leq N(H) \leq G$ и индекс $[G : N(H)]$ – число различных подгрупп, сопряженных с H. Если $G = \bigcup\limits_{g \neq 1} g^{-1} H g$, то $H \neq \langle e \rangle$ и число элементов в G, не равных единице равно

$$|G| - 1 \leq [G : N](|H| - 1) \leq$$
$$\leq [G : H](|H| - 1) = |G| - [G : H] \leq |G| - 2.$$

Противоречие. □

Теорема Веддерберна имеет следующее неожиданное применение.

Теорема 5.2 (Ж. Лагранж).
Произвольное натуральное число является суммой четырех квадратов целых чисел.

□ Так как $2 = 1^2 + 1^2 + 0^2 + 0^2$, то ввиду тождества Лагранжа нам достаточно доказать теорему для любого нечетного простого числа p. Рассмотрим гомоморфизм $\varphi : \Gamma \to \Gamma / p\Gamma$, полагая $\varphi(a) = \bar{a} = a + p\Gamma$. Заметим, что $\bar{2}$ – обратимый элемент в

$$\Gamma / p\Gamma = \mathbb{Z}_p \cdot 1 + \mathbb{Z}_p \cdot \bar{i} + \mathbb{Z}_p \cdot \bar{j} + \mathbb{Z}_p \cdot \bar{k}$$

и $\overline{i}\overline{j} \neq \overline{j}\overline{i}$. По теореме Веддерберна о конечных телах наше конечное кольцо $\Gamma/p\Gamma$ не является телом (ибо оно некоммутативное) и следовательно, оно содержит собственный левый идеал $\bar{L} \neq \bar{0}$ (см. лемму 5.4). Используя лемму 5.3 и переходя к прообразам, имеем, что

$$p\Gamma \subset \Gamma u \subset \Gamma,$$

где $\bar{L} = (\Gamma/p\Gamma)\bar{u}$, u – необратимый элемент. Откуда следует, что $p = cu$ и $p^2 = N(p) = N(c)N(u)$. Так как c, u – необратимые элементы в Γ, то $N(u) = p$. То есть, если

$$u = m_0 \cdot \xi + m_1 \cdot i + m_2 \cdot j + m_3 \cdot k,$$

то $2u$ – кватернион с целыми координатами v_0, v_1, v_2, v_3 и

$$N(2u) = 4 \cdot p = v_0^2 + v_1^2 + v_2^2 + v_3^2.$$

Окончание доказательства следует из следующего трюка Эйлера: если

$$2a = x_0^2 + x_1^2 + x_2^2 + x_3^2,$$

то

$$a = \left(\frac{x_0 + x_1}{2}\right)^2 + \left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2.$$

□

Пусть D – тело с центром Z. Рассмотрим множество всех многочленов

$$D[x] = \{f(x) = a_0x^n + \ldots + a_n |\ \ a_i \in D\}.$$

Докажем, что $D[x]$ – евклидово кольцо. Действительно, пусть $f(x)$ и $g(x)$ – некоторые многочлены степени n и m соответственно, $g(x) \neq 0$. Докажем, что существуют многочлены $q_1(x)$, $r_1(x)$, $q_2(x)$, $r_2(x)$ такие, что

$$f = g(x)q_1 + r_1 = q_2g(x) + r_2,$$

где либо $r_1 = 0$, либо $\deg r_1 \leq m-1$ и либо $r_2 = 0$, либо $\deg r_2 \leq m-1$. Доказательство проведем индукцией по числу n. Если $n < m$, то $f = g(x) \cdot 0 + f = 0 \cdot g(x) + f$ и искомые равенства доказаны. Сделаем предположение индукции об истинности нашего утверждения для многочленов степени меньшей n. Пусть a_0 – старший коэффициент $f(x)$ и b_0 – старший коэффициент для $g(x)$. Тогда

$$f_1(x) = f(x) - g(x)\left(b_0^{-1}a_0x^{n-m}\right)$$

и

$$f_2(x) = f(x) - \left(a_0b_0^{-1}\right)x^{n-m} \cdot g(x)$$

– многочлены степени меньшей n. По предположению индукции существуют многочлены q_1, r_1, q_2, r_2 такие, что $\deg r_i < m$, $i = 1, 2$ и

$$f_1 = gq_1 + r_1,\ f_2 = q_2g + r_2.$$

Следовательно,

$$f = g\left(q_1 + b_0^{-1}a_0x^{n-m}\right) + r_1 = \left(q_2 + a_0b_0^{-1}x^{n-m}\right)g + r_2.$$

Лемма 5.6. *$D[x]$ – кольцо главных правых и левых идеалов.*

□ Пусть I – ненулевой правый идеал $D[x]$ и $f(x)$ – ненулевой многочлен минимальной степени из I. Тогда $I \supseteq f(x)D[x]$. Если $q(x) \in I$, то существует многочлены q_1, r_1 такие, что

$$q = fq_1 + r_1,$$

где либо $r_1 = 0$, либо $\deg r_1 < \deg f$. Так как $r_1 = q - fq_1 \in I$, то, ввиду минимальности $\deg f$, остаток $r_1 = 0$, то есть $I = f(x)D[x]$.

Аналогично доказывается, что каждый левый идеал $D[x]$ является главным. □

Лемма 5.7. *Многочлен $f(x)$ принадлежит центру $D[x]$ тогда и только тогда, когда $f(x) \in Z[x]$*

Доказательство очевидно.

Лемма 5.8. *Пусть $h(x)$ и $g(x)$ такие многочлены из $D[x]$, что*

1. $\deg h(x) \geq 1$;
2. *$h(x)$ – левый делитель каждого многочлена вида $a^{-1}g(x)a$, где $a \in D\backslash\{0\}$.*

Тогда $g(x)$ делится на центральный многочлен, то есть, на многочлен из $Z[x]$.

□ Пусть

$$I_h = \{g_1(x) \in D[x] \mid \text{для любого } a \in D, a \neq 0, \\ h(x) \text{ – левый делитель } a^{-1}g_1(x)a\}.$$

Ясно, что многочлен $g \in I_h$ и I_h – правый идеал $D[x]$. По лемме 5.6 $I_h = f(x)D[x]$, где $f(x)$ – многочлен со старшим коэффициентом 1. Если $f(x) \notin Z[x]$, то при некотором $c \neq 0 \in D$ многочлен $f - c^{-1}fc \neq 0$ принадлежит I_h и имеет меньшую степень чем f. Противоречие доказывает, что $f(x) \in Z[x]$ и $f(x)$ – делитель $g(x)$. □

Лемма 5.9. *Элемент $c \in D$ является нулем для*

$$f(x) = a_0x^n + \ldots + a_n \in D[x]$$

тогда и только тогда, когда

$$f(x) = g(x)(x - c)$$

для некоторого многочлена $g(x) \in D[x]$.

□ Если

$$f = (b_0x^{n-1} + \ldots + b_{n-1})(x - c),$$

то

$$a_0 = b_0,\ a_1 = b_1 - b_0c,\ \ldots,\ a_{n-1} = b_{n-1} - b_{n-2}c,\ a_n = -b_{n-1}c.$$

Умножая справа эти равенства соответственно на

$$c^n,\ c^{n-1},\ \ldots,\ c,\ 1$$

и складывая, мы получим, что

$$f(c) = a_0c^n + a_1c^{n-1} + \ldots + a_0 = 0.$$

Обратно, если $f(c) = 0$, то, полагая (при $n \geq 2$)

$$g(x) = a_0x^{n-1} + (a_1 + a_0c)x^{n-2} + \ldots + (a_{n-1} + a_{n-2}c + \ldots + a_0c^{n-1}),$$

имеем, что $f(x) = g(x)(x-c)$. При $n = 1$ из равенства $a_0c + a_1 = 0$ следует равенство $f(x) = a_0(x - c)$. $\square$

Лемма 5.10. *Пусть многочлен $x - a \in D[x]$ является правым делителем $f(x)g(x)$ и $x - a$ не является правым делителем $g(x)$. Тогда существует такой элемент $b \in D$, $b \neq 0$, что $(x - a)$ – правый делитель $b^{-1}f(x)b$.*

$\square$ Разделим $g(x)$ с остатком на $(x - a)$:

$$g(x) = \varphi(x)(x - a) + b,$$

где $b \in D$, $b \neq 0$. Тогда $(x - a)$ – правый делитель

$$f(x)b = fg - f\varphi(x - a)$$

и, следовательно, $(x - a)$ – правый делитель $b^{-1}f(x)b$. $\square$

Лемма 5.11. *Пусть $f(x)$ – неприводимый многочлен в $Z[x]$ и $a, b \in D$ являются его корнями, то есть, $f(a) = f(b) = 0$. Тогда существует такой ненулевой элемент $c \in D$, что $a = c^{-1}bc$.*

□ По лемме 5.9 $x - a$ является и левым, и правым делителем $f(x)$ (так как $f(x)$ – центральный многочлен). В частности, существует такой многочлен $g(x) \in D[x]$, что

$$f(x) = g(x)(x - a).$$

Аналогично многочлен $x - b$ является правым и левым делителем $f(x)$. Так как $f(x)$ – центральный многочлен, то для любого $t \in D$, $t \neq 0$,

$$f(x) = t^{-1}f(x)t = \left(t^{-1}gt\right)\left(x - t^{-1}at\right)$$

делится справа и слева на $x - b$. Откуда следует, что либо для любого $t \in D$, $t \neq 0$ многочлен $x - b$ является левым делителем $t^{-1}gt$, либо существует такой элемент $t_0 \in D$, $t_0 \neq 0$, что $x - b$ не является левым делителем $t_0^{-1}gt_0$. В первом случае (по лемме 5.8) многочлен $g(x)$ делится на центральный многочлен, что противоречит неприводимости $f(x)$ в $\mathbb{Z}[x]$.

Во втором случае (по левому аналогу леммы 5.10) существует такой элемент $s \neq 0 \in D$, что $x - b$ – левый делитель $s^{-1}\left(t^{-1}(x - a)t_0\right)s$, то есть $b = (t_0s)^{-1}a(t_0s)$. □

Доказанный выше результат может быть обобщен следующим образом (см. [22]).

Теорема 5.3 (Нетер-Сколема).
Пусть R – простое артиново кольцо с центром F и A, B – простые подалгебры R, содержащие F и имеющие конечную размерность над F. Если φ – изоморфизм A на B, оставляющий элементы из F неподвижными, то существует обратимый элемент $x \in R$ такой, что $\varphi(a) = x^{-1}ax$ для любого элемента $a \in A$.

Эта теорема не переносится на полупростые подалгебры A и B как показывает следующий пример.

Пример 5.1. Пусть $R = M_3(Q)$,

$$A = \{\alpha + \beta a \mid \alpha, \beta \in Q \text{ и } a = \operatorname{diag}(1, 2, 2)\},$$

$$B = \{\alpha + \beta b \mid \alpha, \beta \in Q \text{ и } b = \mathrm{diag}(1, 1, 2)\}.$$

Отображение

$$\varphi : A \to B$$

такое, что

$$\varphi(\alpha + \beta a) = \alpha + \beta b,$$

является изоморфизмом полупростых алгебр A, B, изоморфных $Q[x]/((x-1)(x-2))$. Если бы этот изоморфизм индуцировался сопряжением с помощью невырожденной матрицы $x \in R$, то $\varphi(a) = b = x^{-1}ax$ и $xb = ax$. Легко видеть, что матрицы x, удовлетворяющие равенству $xb = ax$ имеют вид

$$\begin{pmatrix} \alpha & \beta & 0 \\ 0 & 0 & \gamma \\ 0 & 0 & \delta \end{pmatrix}$$

и являются вырожденными. Интересно также отметить, что при

$$c = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

справедливо $c^{-1}(3-a)c = b$ и $c^{-1}Ac = B$.

Лемма 5.12. *Пусть D – тело характеристики $p > 0$ и a – такой элемент D, что $a \notin Z$, $a^{p^n} = a$. Тогда существует элемент $x \in D$ такой, что $x^{-1}ax = a^i \neq a$.*

□ Рассмотрим поле $F = GF(p)[a]$. Оно является конечным и, следовательно, его мультипликативная группа является циклической с образующим, например, b. То есть

$$F = \left\langle 0, b, b^2, \ldots, b^{p^s-1} \right\rangle,$$

где $|F| = p^s$. Пусть $f(x) \in Z[x]$ – многочлен минимальной степени, корнем которого является b. Так как $b \notin Z$, то $\deg f > 1$. Далее $f(x)$ является делителем

$$x^{p^s} - x = \prod_{\alpha \in F} (x - \alpha).$$

Следовательно, найдется элемент $b^i \neq b$ такой, что $f(b^i) = 0$. По лемме 5.11 эти элементы сопряжены, то есть $b = c^{-1}b^i c$ для некоторого элемента $c \in D$. Элемент a является некоторой степенью b, например, $a = b^j$. Тогда

$$a = \left(c^{-1}b^i c\right)^j = c^{-1}\left(b^j\right)^i c = c^{-1}a^i c.$$

Если $a = a^i$, то $a = cac^{-1}$ и c – элемент, перестановочный с a. Так как $b = \sum \lambda_t a^t \in F = GF(p)[a]$, то $bc = cb$ и $b = b^i$. Противоречие доказывает, что a и a^i – различные сопряженные элементы D. □

Теорема 5.4 (Н. Джекобсон).
Пусть D – тело, в котором для любого элемента $a \in D$ существует натуральное число $n = n(a) > 1$ такое, что $a = a^n$. Тогда D – поле.

□ Пусть e – единица D. Тогда $(e + e)^n = e + e$ для некоторого $n > 1$. Следовательно, характеристика p поля D отлична от нуля. Если $D \neq Z$, то существует элемент $a \in D\backslash Z$. По условию теоремы поле $GF(p)[a]$ является конечным. По лемме 5.12, существует элемент $x \in D$ такой, что $ax = xa^i$, $a^i \neq a$. Подкольцо $GF(p)[x, a]$ является конечным, так как ввиду равенства $ax = xa^i$, любой его элемент представим в виде $\sum \lambda_{ij}x^i a^j$, где $\lambda_{ij} \in GF(p)$, $i \leq n(x)$, $j \leq n(a)$. По теореме Веддерберна $GF(p)[x, a]$ – конечное поле. В частности, $xa = ax$ и $a = a^i$. Противоречие доказывает, что $D = Z$. □

Теорема 5.5. *Пусть $f(x) \in D[x]$ и $\deg f = n$. Тогда множество всех корней $f(x)$ в D содержится в не более чем n классах сопряженных элементов группы $D^* = \langle D\backslash\{0\}, \cdot\rangle$.*

□ Доказательство проведем индукцией по числу n. Если $n = 1$, то $f(x) = ax + b = 0$, $a \neq 0$, имеет единственный корень $-a^{-1}b$. Сделаем предположение индукции об истинности теоремы для многочленов степени, меньшей n. Пусть $c_0, c_1, \ldots, c_n$ – корни

$$f(x) = a_0x^n + \ldots + a_n,$$

$a_0 \neq 0$. Тогда по лемме 5.9

$$f(x) = g_i(x)(x - c_i),$$

$i = 0, 1, \ldots, n$. Пусть $t_i = c_i - c_0$, $i > 0$. Тогда $x - c_0 = (x - c_i) + t_i$ и

$$g_i(x - c_i) = (x - c_i) + g_0 t_i.$$

Следовательно,

$$g_0 = (g_i - g_0)(x - c_i)t_i^{-1} = (g_i - g_0)t_i^{-1}\left(x - t_i c_i t_i^{-1}\right).$$

Таким образом,

$$t_1 c_1 t_1^{-1},\ \ldots,\ t_n c_n t_n^{-1}$$

– корни $g_0(x)$ (см. лемму 5.9). По предположению индукции некоторые два из них сопряжены, например,

$$s^{-1}\left(t_i c_i t_i^{-1}\right) s = t_j c_j t_j^{-1},$$

где $i \neq j$. Откуда следует, что c_i и c_j – сопряженные элементы. $\square$

Теорема 5.6. *Если D – некоммутативное тело и $c \in D$, то*

$$C_D(c) = \{x \in D |\ xc = cx\}$$

– бесконечное подтело D.

$\square$ Допустим противное, то есть существует такой элемент $c \in D$, что его централизатор $C_D(c)$ является конечным телом. Тогда $Z = GF(q) \subseteq C_D(c) = GF\left(q^f\right)$, где $f > 1$ (ибо если $f = 1$, то $c \in C_D(c) = Z$ и $C_D(c) = D$). Так как $c \notin Z$ и $c = c^{q^f}$, то по лемме 5.12, $x^{-1}cx = c^i \neq c$ для некоторого элемента $x \in D$.

Рассмотрим конечное поле $Z[c]$ и его автоморфизм

$$y \to x^{-1}yx.$$

Данный автоморфизм оставляет инвариантными элементы из Z и, следовательно, является степенью автоморфизма $y \to y^q$,

то есть, существует $j \leq f$ такой, что $x^{-1}yx = y^{q^j}$ для всех элементов $y \in Z[c]$. В частности, $x^{-1}cx = c^{q^j}$. Так как

$$x^{-2}cx^2 = \left(x^{-1}cx\right)^{q^j} = c^{q^{2j}},$$

то

$$x^{-f}cx^f = c^{q^{fj}} = \left(c^{q^f}\right)^{q^{f(j-1)}} = \left(c^{q^f}\right)^{q^{f(j-2)}} = \ldots = c^{q^f} = c.$$

Таким образом, $x^f \in C_D(c) = GF\left(q^f\right)$ и, следовательно, подкольцо $Z[c, x]$ является конечным телом. По теореме Веддерберна $cx = xc$. Противоречие. □

Теорема 5.7. *Если $f(x) \in D[x]$ имеет два различных корня в одном классе сопряженных элементов, то в этом классе содержится бесконечно много корней.*

□ Пусть c и ycy^{-1} – два различных корня

$$f(x) = a_0x^n + \ldots + a_n.$$

Тогда

$$f\left(ycy^{-1}\right) = a_0yc^ny^{-1} + \ldots + a_{n-1}ycy^{-1} + a_n = 0,$$

$$a_0yc^n + \ldots + a_{n-1}yc + a_ny = 0, \quad a_0c^n + \ldots + a_{n-1}c + a_n = 0.$$

Пусть $z \in C_D(c)$. Тогда $(y + z)c(y + z)^{-1}$ снова корень $f(x)$. Если при некоторых $z_1, z_2 \in C_D(c)$,

$$(y + z_1)c(y + z_1)^{-1} = (y + z_2)c(y + z_2)^{-1},$$

то

$$(y + z_2)^{-1}(y + z_1) = z_3 \in C_D(c).$$

Следовательно, $y + z_1 = yz_3 + z_2z_3$. Так как $y \notin C_D(c)$, то $z_3 = 1$ и $z_1 = z_2$. Согласно теореме 5.7, $C_D(c)$ – бесконечное тело. Это означает, что множество корней

$$\{(y + z^{-1})c(y + z) |\ z \in C_D(c)\}$$

многочлена $f(x)$ является бесконечным. □

Следствие 5.1. *Пусть $f(x) \in D[x]$. Тогда число корней $f(x)$ в D либо не превосходит* $\deg f$*, либо бесконечно.*

Последние три теоремы были доказаны в работе [82].

5.2. Теорема Джекобсона

Цель этого параграфа – предложить два доказательства следующего замечательного результата.

Теорема 5.8. *Пусть R – кольцо, в котором для любого элемента $a \in R$ существует целое число $n(a) \geq 2$ такое, что $a = a^{n(a)}$. Тогда R – коммутативное кольцо.*

□ Предложим следующую схему для доказательства этой теоремы:

1) R – тело;

2) R – примитивное кольцо;

3) R – полупростое кольцо;

4) R – произвольное кольцо.

Если R – тело, то по теореме 5.4 R – поле.

Если R – коммутативное кольцо, то по теореме плотности R – плотное кольцо линейных преобразований в $\mathrm{End}_D V$, где V – векторное пространство над телом D. Если $\dim_D V \geq 2$ и $\{u, v\}$ – два линейно независимых вектора, то в силу плотности существует такой элемент $a \in R$, что $ua = v$, $va = 0$. Тогда $ua = v = ua^n = (ua)a^{n-1} = va^{n-1} = 0$. Противоречие доказывает, что $\dim_D V = 1$ и R – тело. Согласно предыдущему случаю R – поле.

Если R – полупростое кольцо, то $R = \sum\limits_{i \in I} \bigoplus\limits_{s} R_i$ – подпрямая сумма примитивных колец $R_i = R/P_i$, где P_i – примитивный

идеал R, $i \in I$. Так как условие теоремы $a = a^{n(a)}$ переносится на гомоморфные образы, то каждое примитивное кольцо R_i, $i \in I$ является полем. Следовательно, R – коммутативное кольцо.

Пусть, наконец, R – произвольное кольцо с условием Джекобсона: для любого элемента $a \in R$ существует целое число $n(a) \geq 2$ такое, что $a = a^{n(a)}$. Докажем, что $J(R) = (0)$. Пусть $a \in J(R)$. Тогда $a = a^{n(a)}$ для некоторого числа $n(a) \geq 2$. Так как $-a^{n-1} \in J(R)$, то существует такой элемент $b \in R$, что

$$-a^{n-1} + b + \left(-a^{n-1}\right) b = 0.$$

Следовательно,

$$a = aa^{n-1} = a\left(b - a^{n-1}b\right) = ab - ab = 0.$$

Откуда следует, что $J(R) = (0)$ и R – полупростое кольцо. В силу предыдущего R – коммутативное кольцо. □

Следствие 5.2. *Пусть R – алгебраическая алгебра над конечным полем $GF(q)$, не содержащая ненулевых нильпотентных элементов. Тогда R – коммутативная алгебра.*

□ Пусть a – произвольный элемент алгебры R. Согласно условию существуют элементы $\alpha_1, \ldots, \alpha_k \in GF(q)$ такие, что

$$a^n + \alpha_1 a^{n-1} + \ldots + \alpha_k a^{n-k} = 0.$$

Следовательно, подалгебра $S = GF(q)[a]$ является конечномерной, коммутативной алгеброй без нильпотентных ненулевых элементов. Поэтому S – конечное кольцо, радикал которого равен нулю. Из главы 1 следует, что

$$S = GF(q_1) \oplus \ldots \oplus GF(q_t),$$

где $GF(q_i)$ – поле, содержащее $GF(q)$, $i \leq t$. Легко видеть, что каждый элемент $s \in S$ удовлетворяет равенству

$$s = s^{(q_1-1)\ldots(q_t-1)+1}.$$

В частности,

$$a = a^{(q_1-1)\dots(q_t-1)+1}.$$

По теореме Джекобсона R – коммутативная алгебра. □

Приведем другое доказательство теоремы Джекобсона, приведенное в работе [121]. Предварительно рассмотрим следующие леммы.

Лемма 5.13. *Пусть R – кольцо, удовлетворяющее условию $a = a^{n(a)}$. Тогда R – кольцо без нильпотентных элементов.*

□ Если $a \in R$, $a^k = 0$ и $a^{n(a)} = a$ для некоторых целых чисел $k \geq 1$ и $n(a) \geq 2$, то

$$a = a^{n(a)} = a^{n^2} = a^{n^3} = \dots = a^{n^k} = 0.$$

□

Лемма 5.14. *Пусть R – некоммутативное кольцо, удовлетворяющее условию $a = a^{n(a)}$. Тогда R содержит некоммутативное подкольцо простой характеристики.*

□ Пусть a, b – такие элементы кольца R, что $ab \neq ba$. Ввиду условия $a = a^{n(a)}$ существует целые числа $n, m, k, l \geq 2$ такие, что $a = a^n$, $2a = (2a)^m$, $b = b^k$, $2b = 2b^l$. Откуда следует, что при $s = (n-1)(m-1)+1$ и $t = (k-1)(l-1)+1$ справедливы равенства $a = a^s$, $2a = (2a)^s$, $b = b^t$, $2b = (2b)^t$ и, следовательно,

$$(2^s - 2)a = (2^t - 2)b = 0.$$

Пусть

$$2^s - 2 = p_1^{\alpha_1} \dots p_u^{\alpha_u}$$

– каноническое разложение на простые числа ($p_i \neq p_j$ при $i \neq j$). Тогда

$$((p_1 \dots p_u)a)^N = 0,$$

где $N = \sum_{i=1}^{u} \alpha_i$ и, следовательно, по лемме 5.13

$$(p_1 p_2 \dots p_u)a = 0.$$

Аналогично существуют различные простые числа $q_1, \dots, q_v$ такие, что $(q_1 \dots q_v)b = 0$. Поэтому

$$a = \sum_{i=1}^{u} a_i, \quad p_i a_i = 0, \quad i \le u,$$

$$b = \sum_{j=1}^{v} b_j, \quad q_j b_j = 0, \quad j \le v.$$

Так как $ab \neq ba$, то существуют индексы $i \le u, j \le v$ такие, что $a_i b_j \neq b_j a_i$. Если $p_i \neq q_j$, то

$$p_i[a_i, b_j] = q_j[a_i, b_j] = 0, \quad 1 = p_i x + q_j y$$

для некоторых целых чисел x, y и, следовательно,

$$[a_i, b_j] = [a_i, b_j](p_i x + q_j y) = 0.$$

Противоречие доказывает, что $p_i = q_j$ и некоммутативное подкольцо $\langle a_i, b_j \rangle$ имеет простую характеристику. □

Лемма 5.15. *Пусть R – некоммутативное подкольцо простой характеристики, удовлетворяющее $a = a^{n(a)}$. Тогда R – содержит конечное некоммутативное подкольцо.*

□ Каждый элемент кольца R порождает коммутативное конечное кольцо без нильпотентных элементов, являющееся прямой суммой конечных полей $GF(p^{m_i})$, где $pR = (0)$. Так как R – некоммутативное кольцо, то существует конечное подполе

$$GF(p^n) = \left\langle 0, a, a^2, \dots, a^{p-1} \right\rangle,$$

не содержащееся в центре кольца R. Пусть $e = a^{n(a)-1}$. Тогда

$$e = e^2, \quad (ex - exe)^2 = (exe - xe)^2 = 0,$$

для $x \in R$. Из леммы 5.13 следует, что $ex = exe = xe$, то есть, e – центральный идемпотент. Следовательно,

$$R = a^{n(a)-1}Ra^{n(a)-1} \oplus \left(1 - a^{n(a)-1}\right) R \left(1 - a^{n(a)-1}\right),$$

$$a \in a^{n(a)-1}Ra^{n(a)-1},$$

e – единица в кольце $a^{n(a)-1}Ra^{n(a)-1}$ и a – не центральный элемент в $a^{n(a)-1}Ra^{n(a)-1}$. Таким образом, можно считать, что единица e поля $GF(p^n)$ является единицей всего кольца R. Рассмотрим отображения

$$T_a : R \to R, \quad L_\lambda : R \to R,$$

$\lambda \in GF(p^n)$ такие, что для любого элемента $r \in R$

$$xT_a = [r, a], \quad rL_\lambda = \lambda r.$$

Пусть

$$GF(p^n) = \langle \lambda_1 = 0,\, \lambda_2,\, \ldots,\, \lambda_{p^n} \rangle$$

и b – такой элемент R, что $[b, a] \neq 0$. Ввиду равенств

$$[x, \underbrace{y, \ldots, y}_{n}] = \sum_{i=0}^{n} (-1)^n \binom{n}{i} y^i x y^{n-i},$$

$a^{p^n} = a$ имеем, что

$$b\left(T_a^{p^n} - T_a\right) = [b, \underbrace{a, \ldots, a}_{p^n}] - [b, a] = [b, a^{p^n} - a] = 0.$$

С другой стороны,

$$b\left(T_a^{p^n} - T_a\right) = b(T_a - L_{\lambda_1})(T_a - L_{\lambda_2}) \ldots (T_a - L_{\lambda_{p^n}}) = 0,$$

где

$$b(T_a - L_{\lambda_1}) = [b, a] \neq 0.$$

Пусть i – такой индекс, что

$$c = b(T_a - L_{\lambda_1}) \dots (T_a - L_{\lambda_i}) \neq 0,$$

$$c(T_a - L_{\lambda_{i+1}}) = 0,$$

$1 \leq i \leq p^n - 1$. Тогда $ca - ac = \lambda_{i+1} c$ и подкольцо $\langle a, c \rangle$ является конечным. □

Лемма 5.16. *Пусть R – конечное некоммутативное кольцо простой характеристики, удовлетворяющей условию $a = a^{n(a)}$. Тогда R содержит некоммутативное тело.*

□ Пусть S – минимальное некоммутативное подкольцо R. Если a, b – такие ненулевые элементы S, что $ab = 0$, то из разложения

$$S = a^{n(a)-1} S a^{n(a)-1} \oplus \left(1 - a^{n(a)-1}\right) S \left(1 - a^{n(a)-1}\right)$$

следует, что

$$b \in \left(1 - a^{n(a)-1}\right) S \left(1 - a^{n(a)-1}\right).$$

В частности, оба слагаемых являются ненулевыми и (в силу минимальности порядка $|S|$) коммутативными кольцами. Откуда следует, что S – коммутативное кольцо. Противоречие доказывает, что S – кольцо без делителей нуля, то есть S – тело. □

Их теоремы Веддерберна о конечных телах и лемм следует, что любое кольцо, удовлетворяющее условиям теоремы Джекобсона, является коммутативным.

5.3. Теорема Херстейна

Кольцо R называется *подпрямо неразложимым*, если пересечение всех его ненулевых идеалов S есть ненулевой идеал. S

называется *сердцевиной кольца* R. Если R не является подпрямо неразложимым кольцом и a – произвольный ненулевой элемент его, то по лемме Цорна существует максимальный идеал I_a, не содержащий a. Ясно, что $\bigcap\limits_{a\neq 0} I_a = (0)$ и R является подпрямой суммой подпрямо неразложимых колец R/I_a, где $a \neq 0$. Таким образом, произвольное кольцо является подпрямой суммой подпрямо неразложимых колец, являющихся гомоморфными образами исходного кольца.

Кольцо R называется H – *расширением своего подкольца* A, если для любого $r \in R$ существует целое число $n(r) \geq 2$ такое, что

$$r^{n(r)} - r \in A$$

(в обозначении $R|_H A$)

Справедлива следующая теорема, доказанная И. Херстейном в работе [84].

Теорема 5.9. *Пусть R – H-расширение центра $Z(R)$. Тогда $R = Z(R)$.*

Мы докажем эту важную теорему в предположении, что числа $n(r)$ фиксированы, то есть в кольцо R выполнено тождество

$$[x^n - x, y] = 0,$$

где $n \geq 2$. Доказательство опирается на следующие леммы.

Лемма 5.17. *Коммутаторный идеал $[R, R]$ кольца R содержится в радикале Джекобсона $J(R)$.*

□ Рассмотрим фактор-кольцо $B = R/J(R)$. Пусть C – примитивный гомоморфный образ B. Тогда C удовлетворяет тождеству $[x^n - x, y] = 0$ и является плотным кольцом линейных преобразований в $\mathrm{End}_D V$, где V – векторное пространство над телом D. Если $\dim_D V \geq 2$ и $\{u, v\}$ – линейно независимые векторы в V, то по теореме плотности существует такие элементы $a, b \in C$, что $ua = v$, $va = 0$, $ub = 0$, $vb = u$. Следовательно,

$$u[a^n - a, b] = u(a^n - a)b - ub(a^n - a) = -u(ab) = -vb = -u = 0.$$

Противоречие доказывает, что $\dim_D V = 1$ и C – тело, удовлетворяющее тождеству $[x^n - x, y] = 0$.

Пусть Z_1 – центр тела C и $\lambda \in Z_1$. Тогда для любых элементов $a, b \in C$

$$[(\lambda a)^n, b] = \lambda^n [a^n, b] = \lambda^n [a, b] = [\lambda a, b] = \lambda [a, b]$$

и

$$(\lambda^n - \lambda)[a, b] = 0.$$

Предположим, что тело C не является полем и a, b – такие элементы C, что $[a, b] \neq 0$. Тогда $\lambda^n = \lambda$ для любого элемента поля Z_1. Следовательно, $q = |Z_1| < \infty$ и в кольце C выполнено тождество

$$(x^n - x)^q - (x^n - x) = 0.$$

По следствию 5.2 $C = Z_1$. Итак, каждый примитивный гомоморфный образ факторкольца $B = R/J(R)$ является полем. Полупростое кольцо B является подпрямой суммой своих примитивных гомоморфных образов. Следовательно, B является коммутативным кольцом, а коммутаторный идеал

$$[R, R] = \left\{ \sum_i u_i [a_i, b_i] v_i \mid u_i, v_i \in R^{\#},\ a_i, b_i \in R \right\}$$

содержится в $J(R)$. $\square$

Лемма 5.18. *Радикал Джекобсона $J(R)$ содержится в центре Z кольца R, а кольцо R удовлетворяет тождествам:*

$$\big[[x, y], z\big] = 0, \quad [x, y] = n x^{n-1} [x, y], \quad [x, y]^2 = 0.$$

$\square$ Пусть $a \in J(R)$ и $\lambda = (a^n - a) \in J(R) \cap Z$. Пусть также b, c – произвольные элементы кольца R. Тогда

$$[(\lambda b)^n, c] = \lambda^n [b^n, c] = \lambda^n [b, c] = [\lambda b, c] = \lambda [b, c]$$

и

$$\left(1 - \lambda^{n-1}\right) \lambda [b, c] = 0.$$

Элемент $(1-\lambda^{n-1})$ является обратимым в кольце с присоединенной единицей $R^{\#}$. Умножая предыдущее равенство слева на $\left(1-\lambda^{n-1}\right)^{-1}$, получим, что $\lambda[b,c]=0$ или

$$\left(a^{n-1}-1\right)a[b,c]=0.$$

Так как $a\in J(R)$, то существует элемент $\left(a^{n-1}-1\right)^{-1}$ в $R^{\#}$ и, следовательно, $a[b,c]=0$. Аналогично доказывается равенство $[b,c]a=0$. Это означает, что

$$J(R)[R,R]=[R,R]J(R)=(0).$$

Для любых элементов $a\in J(R)$ и $b\in R$

$$[a,b]=[a^n,b]=a[a^{n-1},b]+[a,b]a^{n-1}=0,$$

то есть, $a\in Z$ и $J(R)\subseteq Z$. Так как $[R,R]\subseteq J(R)$ (см. лемму 5.17), то $\big[[x,y],z\big]=0$, $[x,y]^2=0$ – тождества в кольце R. Из тождества $\big[[x,y],z\big]=0$ легко видеть выполнимость тождества $[x,y]=nx^{n-1}[x,y]$. $\square$

Лемма 5.19. *Пусть R – подпрямо неразложимое кольцо с сердцевиной S, удовлетворяющее тождеству*

$$[x^n-x,y]=0,$$

где $n\geq 2$. Тогда существует простое число p такое, что

$$p[x,y]=0,\quad [x^p,y]=0$$

– тождества в R и $A=\operatorname{Ann}S$ содержится в центре Z кольца R.

$\square$ Согласно леммам 5.17, 5.18 мы можем считать, что R – некоммутативное кольцо, $J(R)\neq 0$ и $S\subseteq J(R)\subseteq Z$. Пусть a, b – произвольные элементы из R. Тогда

$$[(2a)^n,b]=2^n[a^n,b]=2^n[a,b]=[2a,b]=2[a,b]$$

и

$$(2^n - 2)[a, b] = 0.$$

Таким образом, в абелевой группе $\langle R, + \rangle$ существует ненулевые элементы конечного аддитивного порядка. Следовательно, существует простое число p такое, что идеал

$$R_p = \{x \in R \mid px = 0\} \lhd R$$

не равен нулю. Так как S – сердцевина R, то $R \subseteq R_p$ и $pS = (0)$. Это означает, что порядки периодических элементов $\langle R, + \rangle$ являются степенями простого числа p. Так как

$$[pa, b] = [(pa)^n, b] = p^n[a^n, b] = p^n[a, b],$$

то

$$\left(p^{n-1} - 1\right) p[a, b] = 0.$$

Числа p и $\left(p^{n-1} - 1\right)$ являются взаимно простыми. Поэтому $p[a, b] = 0$. Учитывая тождество $\big[[x, y], z\big] = 0$, имеем, что

$$[a^p, b] = pa^{p-1}[a, b] = a^{p-1}(p[a, b]) = 0,$$

то есть, $p[x, y] = 0$, $[x^p, y] = 0$ – тождества в кольце R.

Так как

$$S \subseteq [R, R] \subseteq J(R) \subseteq Z$$

и

$$[R, R]^2 \subseteq J(R)[R, R] = (0),$$

то $S^2 = (0)$ и $A = \operatorname{Ann} S$ – ненулевой двусторонний идеал кольца R, содержащий S. Покажем, что $A \subseteq Z$. Пусть $x \in A$ и y, z – произвольные элементы кольца R. Тогда

$$[x^p y, z] = [x^{pn} y^n, z] = x^{pn}[y^n, z] = x^{pn}[y, z] = x^p[y, z].$$

Пусть $u = x^p[y, z]$. Тогда

$$x^{p(n-1)}u = u, \quad x^{p(n-1)} = \left(x^{n-1}\right)^p \in Z.$$

Пусть

$$M = \{v \in R \mid \ x^{(n-1)p}v = v\Big\}$$

Тогда $u \in M$ и $M \lhd R$. Если $M \neq (0)$, то $M \supseteq S$ и $xS \subseteq AS = (0)$. Пусть $s \in S$. Тогда $x^{(n-1)p}s = s = 0$. Следовательно, $S = (0)$. Противоречие доказывает, что $M = (0)$. В частности,

$$x^p[y, z] = 0$$

для любых элементов $x \in A$, $y, z \in R$. Откуда следует, что

$$[x^p y, z] = x^p[y, z] + [x^p, z]y = 0.$$

Полагая y равным $x, x^2, x^3, \ldots$ получим, что

$$\Big\{x^{p+k} \mid k = 1, 2, \ldots\Big\} \subseteq Z.$$

Выберем число $t \geq 1$ таким, чтобы $n^t \geq p$. Тогда из включений

$$x^n - x \in Z,\ x^{n^2} - x^n \in Z,\ x^{n^3} - x^{n^2} \in Z,\ \ldots,\ x^{n^t} - x^{n^{t-1}} \in Z$$

следует, что $x \in Z$. Следовательно, $A \subseteq Z$. $\square$

Лемма 5.20. *Пусть R – подпрямо неразложимое некоммутативное кольцо с сердцевиной S, удовлетворяющее тождеству $[x^n - x, y] = 0$. Тогда множество всех делителей нуля кольца R совпадает с идеалом $A = \operatorname{Ann} S$ и R/A – конечное поле.*

$\square$ Пусть a – делитель нуля и $ax = 0$, где $x \neq 0 \in R$. Покажем, что a аннулирует некоторый ненулевой элемент из центра. Действительно, если $x^p \neq 0$, то $x^p \in Z$ (см. лемму 5.19) и

$$a(x^p) = (ax)x^{p-1} = 0.$$

Если $x^p = 0$, то из включений

$$x^n - x \in Z,\ x^{n^2} - x^n \in Z,\ \ldots,\ x^{n^p} - x^{n^{p-1}} \in Z$$

следует, что $x^{n^p} = 0$ и $x \in Z$. Таким образом, можно предполагать, что $ax = 0$, где x – некоторый ненулевой элемент из Z. Если идеал $Rx \neq (0)$, то $S \subseteq Rx$ и $aS \subseteq aRx = (0)$, то есть $a \in A$. Если $Rx = (0)$, то $r(R)$ – ненулевой идеал, содержащий S. Поэтому $aS \subseteq ar(R) = (0)$ и $a \in A$. Аналогично рассматривается случай, если $xa = 0$.

Докажем, что R/A – конечное поле. Пусть s – ненулевой элемент из S. Если $Rs = (0)$, то $r(R)$ – ненулевой идеал R, содержащий S и $R \subseteq A \subseteq Z$, то есть R – коммутативное кольцо. Противоречие. Следовательно, $Rs \lhd R$, $Rs \neq 0$ и значит, $S = Rs$. Пусть $a \in R \setminus A$. Тогда a – регулярный элемент в R и $R(as) = S = Rs$. Откуда следует, что для любого элемента $v \in R$ существует элемент $u \in R$ такой, что $vs = u(as)$ или $(v - ua)s = 0$, $(v - ua)SR = (v - ua)S = (0)$ и $\bar{v} = \bar{u}\bar{a}$ в R/A. Это означает, что R/A – тело. Так как

$$[R, R]J(R) = [R, R]S = (0),$$

то $[R, R] \subseteq A$ и R/A – поле. Ранее мы отмечали справедливость тождества

$$(x^{np} - x^p)\,[y, z] = 0$$

в кольце R. Так как R – некоммутативное кольцо, то для любого элемента $w \in R$,

$$w^{np} - w^p \in A$$

и поле R/A удовлетворяет тождеству $x^{np} - x^p = 0$. Поэтому $|R/A| \leq np$. $\square$

Перейдем к доказательству теоремы.

$\square$ Пусть R – произвольное кольцо, удовлетворяющее тождеству $[x^n - x, y] = 0$. Тогда R – подпрямая сумма подпрямо неразложимых колец, удовлетворяющих тождеству $[x^n - x, y] = 0$. Мы можем считать, что R – подпрямо неразложимое кольцо. Если R – некоммутативное кольцо, то согласно лемме 5.20

$R/A = GF(q)$ – конечное поле, где $A = \operatorname{Ann} S \subseteq Z$. Существует такой элемент $a \in R$, что

$$R/A = \left\{\bar{0}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{q-1}\right\}.$$

Пусть $b, c \in R$. Тогда $b = a^i + z_1$, $c = a^j + z_2$, где $z_1, z_2 \in A$ и $1 \leq i, j \leq q-1$, либо один из элементов b, c содержится в A. Так как $A \subseteq Z$, то $[b, c] = 0$, то есть R – коммутативное кольцо. □

Сделаем несколько замечаний к доказанной выше теореме. В работе [97] построен пример некоммутативного кольца, являющегося H – расширением своего коммутативного подкольца, а в работе [50] доказаны следующие результаты:

1. Пусть $R|_H A$, где A – коммутативное подкольцо R. Тогда R удовлетворяет тождеству

$$\big[[x_1, x_2], [x_3, x_4]\big] = 0;$$

2. Пусть $R|_H A$, где A – правый идеал R, удовлетворяющий тождеству. Тогда R удовлетворяет некоторому тождеству.

Рассмотрим следующий удивительный результат, доказанный Т. Лаффи в работе [103] .

Теорема 5.10. *Пусть R – бесконечное кольцо. Тогда R содержит бесконечное коммутативное подкольцо.*

□ Предположим противное, то есть R – бесконечное кольцо, в котором коммутативные подкольца являются конечными. Тогда для любого элемента $a \in R$ подкольцо $\langle a \rangle$, им порожденные, является конечным. В частности, существуют натуральные числа n, m, k такие, что $na = 0$, $a^m = a^{m+k}$.

Докажем, что если $a \in R$ и правый аннулятор $r(a)$ является бесконечным подкольцом, то двусторонний аннулятор $\operatorname{Ann}(a) = r(a) \cap \ell(a)$ – также бесконечное подкольцо. Действительно, пусть $H = r(a)$ – бесконечное подкольцо. Тогда $(Ha)^2 =$

$HaHa = (0)$ и Ha – коммутативное подкольцо. Следовательно, $|Ha| < \infty$. Рассмотрим отображение $\varphi : H \to Ha$, $\varphi(h) = ha$. Оно является сюръективным гомоморфизмом абелевых групп $\langle H, + \rangle$ и $\langle Ha, + \rangle$. Так как H – бесконечная абелева группа, а образ $\varphi(H) = Ha$ – конечная абелева группа, то

$$\operatorname{Ker} \varphi = \{h \in H |\ ha = 0\}$$

является бесконечной подгруппой H, содержащейся в аннуляторе $\operatorname{Ann}(a) = r(a) \cap \ell(a)$. Откуда следует, что $\operatorname{Ann}(a)$ – бесконечное подкольцо.

Аналогично можно доказать, что если левый аннулятор $\ell(a)$ элемента $a \in R$ является бесконечным подкольцом, то и двусторонний аннулятор $\operatorname{Ann}(a)$ – бесконечное подкольцо в R.

Докажем, что если a – нильпотентный элемент кольца R, то $\operatorname{Ann}(a)$ – бесконечное подкольцо. Пусть $a^n = 0$, где n – натуральное число. Так как $a(a^{n-1}R) = 0$, то либо $a^{n-1}R$ – бесконечный правый идеал, либо $|a^{n-1}R| < \infty$. В первом случае $r(a)$ – бесконечное подкольцо и, следовательно, согласно выше доказанному, $\operatorname{Ann}(a)$ – бесконечное подкольцо. Предположим $|a^{n-1}R| < \infty$. Рассмотрим гомоморфизм абелевых групп

$$\psi : R \to a^{n-1}R, \quad \varphi(x) = a^{n-1}x.$$

Его ядро $\operatorname{Ker} \psi = r\left(a^{n-1}\right)$ – бесконечное подкольцо. Тогда аннулятор $\operatorname{Ann}\left(a^{n-1}\right)$ – тоже бесконечное подкольцо. Рассмотрим множество $a \operatorname{Ann}\left(a^{n-1}\right)$. Если оно является конечным, то по аналогии с предыдущим рассуждением $r(a) \cap \operatorname{Ann}\left(a^{n-1}\right)$ – бесконечное подкольцо и, следовательно, $\operatorname{Ann}(a)$ – бесконечное множество. Если же $a \operatorname{Ann}\left(a^{n-1}\right)$ – бесконечное множество, то из равенства

$$a^{n-2}\left(a \operatorname{Ann}\left(a^{n-1}\right)\right) = a^{n-1} \operatorname{Ann}\left(a^{n-1}\right) = 0$$

следует, что $r(a^{n-2})$ – бесконечное подкольцо и следовательно, $\operatorname{Ann}(a^{n-2})$ – бесконечное подкольцо. Рассмотрим множество

$a\,\mathrm{Ann}\left(a^{n-2}\right)$. Если оно конечное, то $r(a) \cap \mathrm{Ann}\left(a^{n-2}\right)$ – бесконечное множество.Тогда $\mathrm{Ann}(a)$ – бесконечное подкольцо. Если же $a\,\mathrm{Ann}(a^{n-2})$ – бесконечное подмножество, то из равенства

$$a^{n-3}\left(a\,\mathrm{Ann}\left(a^{n-2}\right)\right) = a^{n-2}\,\mathrm{Ann}\left(a^{n-2}\right) = 0$$

следует, что $r(a^{n-3})$ и $\mathrm{Ann}\left(a^{n-3}\right)$ – бесконечные подкольца. Продолжая аналогичные рассуждения, мы докажем, что $\mathrm{Ann}(a)$ – бесконечное подкольцо.

Докажем, что если a, b – такие элементы в R, что $ab = 0$, то либо $\mathrm{Ann}(a)$ – бесконечное подкольцо, либо $\mathrm{Ann}(b)$ – бесконечное подкольцо. Действительно, так как $ab = 0$, то $a(bR) = 0$. Если bR – бесконечное подмножество, то $r(a)$ – бесконечное подмножество и аннулятор $\mathrm{Ann}(a)$ – бесконечное подкольцо. Если же $|bR| < \infty$, то $r(b)$ – бесконечное подкольцо и $\mathrm{Ann}(b)$ – бесконечное подкольцо.

Обозначим через

$$X(R) = \{a \in R \mid \ \mathrm{Ann}(a) - \text{бесконечное подкольцо}\}.$$

Тогда $X(R)$ содержит все нильпотентные элементы кольца R и некоторые делители нуля.

Докажем, что $X(R) \neq (0)$. Предположим противное, пусть $X(R) = (0)$ и a – некоторый ненулевой элемент кольца R. Тогда $a^n = a^{n+m}$ для некоторых целых чисел $m, n \geq 1$. Следовательно,

$$\left(a - a^{m+1}\right)^{n+1} = \left(a - a^{m+1}\right) a^{n-1} f(a) = \left(a^n - a^{n+m}\right) f(a) = 0,$$

где $f(t) \in t\mathbb{Z}[t]$. Так как R не содержит ненулевых нильпотентных элементов (ввиду предположения $X(R) = (0)$), то $a - a^{m+1} = 0$. По теореме 5.8 R – бесконечное коммутативное кольцо. Противоречие.

Итак, $X(R) \neq (0)$. Пусть $a_1 \in X(R)$, $a_1 \neq 0$. Тогда $R_1 = \mathrm{Ann}(a_1)$ является бесконечным кольцом, не содержащим бесконечные коммутативные подкольца. Предположим существо-

вание таких элементов $a_1, a_2, \ldots, a_n \in R$ $(n \geq 1)$, что

$$a_{i+1} \in R_i = \bigcap_{j=1}^{i} \mathrm{Ann}(a_j),$$

$i \leq n-1$ и

$$R_n = \mathrm{Ann}(a_1) \cap \mathrm{Ann}(a_2) \cap \ldots \cap \mathrm{Ann}(a_n)$$

– бесконечное подкольцо. Рассмотрим множество

$$X(R_n) = \{x \in R_n | \ \mathrm{Ann}(x) \text{ – бесконечное множество}\}.$$

Мы знаем, что $X(R_n) \neq (0)$. Покажем, что $X(R_n)$ не содержится в множестве $\{0, a_1, a_2, \ldots, a_n\}$. Предположим противное, то есть $X(R_n) \subseteq \{0, a_1, a_2, \ldots, a_n\}$. Тогда элементы из

$$X(R_n) \subseteq R_n = \mathrm{Ann}(a_1) \cap \ldots \cap \mathrm{Ann}(a_n)$$

состоят из нильпотентных элементов, а элементы из дополнения $R_n \backslash X(R_n)$ не являются нильпотентными. При этом $X(R_n)$ содержится в центре кольца R_n. Пусть $b \notin X(R_n)$. Тогда b – ненильпотентный элемент и $b^k = b^{k+m}$ для некоторых целых чисел $m, k \geq 1$. Следовательно, $b^{k-1}(b - b^{m+1}) = 0$. Если $b^{k-1} \in X(R_n)$, то b – нильпотентный элемент. Противоречие. Согласно выше доказанному $b - b^{m+1} \in X(R_n)$ и $X(R_n)$ содержится в центре R_n. Итак, для любого элемента $c \in R_n$ существует целое число $s \geq 2$ такое, что $c - c^s$ содержится в центре R_n. По теореме 5.9 R_n – коммутативное (бесконечное) кольцо. Противоречие. Следовательно, $X(R_n)$ не содержится в $\{0, a_1, \ldots, a_n\}$ и существует элемент $a_{n+1} \in X(R_n)$, не равный ни одному из элементов множества $\{0, a_1, a_2, \ldots, a_n\}$, такой, что $\mathrm{Ann}(a_{n+1}) \cap R_n = R_{n+1}$ – бесконечное кольцо. Пусть S – подкольцо R порожденное бесконечным множеством элементов $\{0, a_1, a_2, \ldots, a_n, \ldots\}$. Тогда $S^2 = (0)$ и S – бесконечное коммутативное кольцо. Противоречие. $\square$

В работах [98, 99] предложены следующее обобщение и аналог выше доказанной теоремы.

Теорема 5.11. *Пусть R – бесконечное периодическое кольцо (то есть для любого элемента $a \in R$ существует целые числа $m, n \geq 1$ такие, что $a^n = a^{n+m}$). Тогда либо R содержит бесконечное подкольцо с нулевым умножением, либо R содержит бесконечное подкольцо, порожденное счетным множеством попарно ортогональных идемпотентов, либо R содержит бесконечный коммутативный идеал конечного индекса.*

Теорема 5.12. *Каждая бесконечномерная алгебра над полем содержит коммутативную бесконечномерную подалгебру.*

Из этой теоремы следует, что алгебраическая алгебра с условием максимальности для подалгебр является конечномерной. (вопрос К.А. Жевлакова).

5.4. Теорема Стреба и ее применения

Цель настоящего параграфа – изложить ниже следующую теорему В. Стреба, доказанную им в работе [118], а также применить ее для доказательства ряда критериев коммутативности колец.

Теорема 5.13 (В. Стреб).
Пусть R – некоммутативное кольцо. Тогда существует подкольцо $B \leq R$, такое, что некоторый гомоморфный образ изоморфен одному из следующих 5 типов колец:

а) $A_1 = \begin{pmatrix} GF(p) & GF(p) \\ 0 & 0 \end{pmatrix}$, $A_1^0 = \begin{pmatrix} GF(p) & 0 \\ GF(p) & 0 \end{pmatrix}$;

б) $\left\{ \begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix} \middle| \; a, b \in GF(q), \right\}$, *где σ – не тождественный автоморфизм поля $GF(q)$;*

в) некоммутативное тело;

г) простое радикальное кольцо;

д) конечное нильпотентное кольцо S такое, что $[S,S]$ – сердцевина S и $S[S,S]=[S,S]S=(0)$.

Для доказательства теоремы докажем сначала несколько лемм.

Лемма 5.21. *Пусть $A=\langle a,b\rangle$ – некоммутативное подпрямо неразложимое кольцо, порожденное двумя элементами a, b. Пусть также A удовлетворяет тождествам*

$$x[y,z]=[x,y]z=0,\quad p^kx=0,$$

где p – простое число. Тогда A – конечное кольцо.

□ Пусть $\mathbb{Z}[X,Y]$ – кольцо многочленов от X и Y. Пусть $\langle X,Y\rangle$ – подкольцо $\mathbb{Z}[X,Y]$, порожденное X и Y. Тогда каждый идеал $\langle X,Y\rangle$ является идеалом в $\mathbb{Z}[X,Y]$. Так как $\mathbb{Z}[X,Y]$ – нетерово кольцо (по теореме Гильберта), то $\langle X,Y\rangle$ – тоже нетерово(коммутативное) кольцо. Кольцо $A/[A,A]=\langle\bar a,\bar b\rangle$ является гомоморфным образом кольца $\langle X,Y\rangle$ и, следовательно, $A/[A,A]$ – нетеровый правый A-модуль. Коммутаторный идеал $[A,A]=\mathbb{Z}_{pk}\cdot[a,b]$ – конечное кольцо. Следовательно, A – правое нетерово кольцо. Пусть $s\in A$. Тогда

$$r(s)\le r(s^2)\le r(s^3)\le\dots$$

Так как A удовлетворяет условию максимальности для правых идеалов, то существует целое число $n\ge 1$ такое, что

$$r(s^n)=r(s^{n+1})=\dots$$

Докажем, что $r(s)\lhd A$. Пусть $u\in r(s)$ и $b\in A$. Тогда

$$s(bu)=[s,b]u+(bs)u=0,$$

так как $[x,y]z=0$ – тождество в A. Таким образом, $r(s)\lhd A$. Докажем, далее, что $As^nA=(0)$. Так как $s^n[a,b]=0$, то $r(s^n)$ содержит $[a,b]$ и идеал $r(s^n)$ не равен нулю. Если $As^nA\neq$

(0), то ввиду подпрямой неразложимости кольца A, существует ненулевой элемент

$$c = \sum_i x_i s^n y_i \in r(s^n) \cap As^nA.$$

Тогда

$$s^n c = s^n \sum_i x_i s^n y_i = s^{2n} \sum_i x_i y_i = 0.$$

Следовательно,

$$\sum_i x_i y_i \in r\left(s^{2n}\right) = r\left(s^n\right).$$

Поэтому

$$s^n \sum_i x_i y_i = \sum_i \left(x_i s^n\right) y_i = c = 0.$$

Противоречие доказывает, что $As^nA = (0)$. В частности, $s^{n+2} = ss^ns = 0$ и A – конечно порожденное ниль-кольцо, удовлетворяющее тождеству. По теореме Левицкого A – нильпотентное кольцо. Так как $p^kA = (0)$, то A – конечное кольцо. □

Лемма 5.22. *Пусть R – некоммутативное кольцо.*

1) *если R – полупростое кольцо (то есть $J(R) = (0)$), то существует подкольцо в R, некоторый гомоморфный образ которого изоморфен кольцу типа а) или b);*

2) *если коммутаторный идеал $[R, R]$ кольца R содержится в центре кольца R, то существует подкольцо в R, некоторый гомоморфный образ которого имеет тип д);*

3) *если существуют такие элементы $x, y \in R$, что $yx = 0$, $xy \neq 0$, то существует подкольцо в R, некоторый гомоморфный образ которого имеет тип а) или д);*

4) *если существует нецентральный элемент $y \in R$ такой, что $(R^{\#}yR^{\#})^2 = (0)$, то существует подкольцо кольца R, чей гомоморфный образ имеет тип а), б) или д).*

□ Докажем утверждение 1). Так как R – некоммутативное подкольцо и $J(R) = (0)$, то существует некоммутативный примитивный гомоморфный образ R/P. Кольцо R/P является плотным кольцом линейных преобразований в $\mathrm{End}_D V$, где V – векторное пространство над телом D. По теореме плотности R/P либо изоморфно телу D^0, либо в R/P есть подкольцо, чей гомоморфный образ изоморфен $M_2(D^0)$. В первом случае R/P имеет тип в). Во втором случае, $M_2(D^0)$ содержит подкольцо, гомоморфно отображающееся на

$$A_1 = \begin{pmatrix} GF(p) & GF(p) \\ 0 & 0 \end{pmatrix}.$$

Перед доказательством утверждений 2)-4) отметим, что:

1) каждое конечно порожденное кольцо, являющееся полем, конечно (см. [5], с. 420);

2) если A – некоммутативное кольцо и $x, y \in A$ такие элементы в A, что $[x, y] \neq 0$, то по лемме Цорна существует максимальный идеал $M \lhd \langle x, y\rangle$, не содержащий $[x, y]$. Фактор-кольцо $S = \langle x, y\rangle/M$ является конечно порожденным некоммутативным кольцом с ненулевой сердцевиной $[S, S]$. Коммутативное 2-порожденное кольцо $S/[S, S]$ является гомоморфным образом $\langle X, Y\rangle$ и, следовательно, является нетеровым кольцом.

Докажем утверждение 2). Пусть R – некоммутативное кольцо и a, b – так же элементы из R, что $[a, b] \neq 0$. Так как $[R, R]$ содержится в центре R, то в R выполнены тождества

$$\big[[x, y], z\big] = 0, \quad [x, y][u, v] = \big[[x, y]u, v\big] - [x, y, z]u = 0.$$

Следовательно, кольцо $S = \langle a, b\rangle/M$ из выше приведенного замечания 2 имеет сердцевину

$$[S, S] = S[\bar{a}, \bar{b}],$$

содержащуюся в центре кольца S. При этом $[S,S]^2=(0)$. Пусть $A=\ell([S,S])$. Если A – коммутативное кольцо, то $A\neq S$ и S/A – левое примитивное кольцо с точным неприводимым модулем $[S,S]=S[\bar{a},\bar{b}]$. По теореме Капланского $S/A=M_n(D)$, где D – тело. Если $n\geq 2$, то, полагая в тождестве

$$[x,y,z]=0$$

$x=e_{12}$, $y=z=e_{11}$, получим, что $e_{12}=0$. Противоречие. Следовательно, $S/A=D$ – тело, удовлетворяющее тождеству $[x,y][u,v]=0$. Поэтому S/A – поле, являющееся Z – порожденным кольцом. По замечанию 1 S/A – конечное поле, то есть $S/A\cong GF(q)$. Пусть $u,v\in S$. Тогда $(u-u^q),(v-v^q)\in A$ и

$$[u-u^q,v-v^q]=$$
$$=[u,v]-qu^{q-1}[u,v]-qv^{q-1}[u,v]+q^2u^{q-1}v^{q-1}[u,v]=[u,v]=0,$$

так как $qu,qv\in A=\ell([S,S])$. Противоречие доказывает, что A – некоммутативное кольцо. Согласно замечанию 2 в A существует 2-порожденное некоммутативное подкольцо, чей гомоморфный образ S_1 имеет сердцевину $[S_1,S_1]$, такую, что

$$S_1[S_1,S_1]=[S_1,S_1]S_1=0.$$

При этом $S_1/[S_1,S_1]$ – нетерово кольцо и

$$\langle[S,S],+\rangle\cong\langle Z_p,+\rangle.$$

Так как S_1 – подпрямо неразложимое кольцо и $p[S_1,S_1]=0$, то множество T всех элементов S_1 конечного аддитивного порядка удовлетворяет условию $p^kT=0$ для некоторого числа $k\geq 1$ (так как S – правое нетерово кольцо) Если $p^kS_1\neq(0)$, то

$$[S_1,S_1]\leq p^kS_1\cap T=p^kT=(0).$$

Противоречие доказывает, что $p^kS_1=(0)$. По лемме 5.21 кольцо S_1 имеет тип д).

Докажем утверждение 3). Пусть x, y – такие элементы кольца R, что $yx = 0$ и $xy \neq 0$. Если $x^2y = 0$ и $xy^2 = 0$, то в кольце $S' = \langle x, y\rangle$ коммутаторный идеал $[S', S']$ содержится в центре S' и согласно утверждению 2) в R есть подкольцо, гомоморфный образ которого имеет тип д). Пусть $x^2y \neq 0$. Тогда $x(xy) \neq 0$ и $(xy)x = (xy)^2 = 0$ и можно считать, что $xy \neq 0$, $yx = 0$, $y^2 = 0$ (заменив y на xy). Построим кольцо

$$S = \langle x, y\rangle / M$$

согласно замечанию 2. Если $\bar{x}^2\bar{y} = \bar{0}$, то из утверждения 2) следует, что в R есть подкольцо, чей гомоморфный образ имеет тип д). Пусть $\bar{x}^2\bar{y} \neq \bar{0}$. Тогда сердцевина $[S, S]$ порождается (как идеал) элементом

$$[\bar{x}, \bar{x}\bar{y}] = \bar{x}^2\bar{y}.$$

Откуда следует, что

$$[S, S] = \mathbb{Z}\bar{x}^2\bar{y} + \langle\bar{x}\rangle\bar{x}^2\bar{y} = [S_1, S_1],$$

где $S_1 = \langle\bar{x}, \bar{x}\,\bar{y}\rangle \leq S$. В частности,

$$\bar{x}\bar{y} = [\bar{x}, \bar{y}] \in [S_1, S_1].$$

Опять исходя из замечания 2, построим кольцо

$$S_2 = \langle\bar{x}, \bar{x}\bar{y}\rangle / M_1 = S_1/M_1,$$

где M_1 – максимальный идеал S_1, не содержащий $[\bar{x}, \bar{x}\bar{y}]$. Пусть $a = \bar{x} + M_1$, $b = \bar{x}\bar{y} + M_1$. Тогда $[S_2, S_2] = (b)$, $bS_2 = (\bar{0})$ и (b) – неприводимый левый $\langle a\rangle$-модуль. Так как $\ell_{\langle a\rangle}((b))$ идеал в S_2, то предположение $\ell_{\langle a\rangle}((b)) \neq (\bar{0})$ влечет за собой

$$(b) \subseteq \ell_{\langle a\rangle}((b)) \subseteq \langle a\rangle,$$

а, следовательно, коммутативность кольца S_2. Поэтому $\ell_{\langle a\rangle}((b)) = \bar{0}$ и $\langle a\rangle$ – поле. По замечанию 1, $\langle a\rangle \cong GF(q)$ для некоторого числа q. Откуда следует, что

$$S_2 = \langle a\rangle \dot{+} \langle a\rangle b \cong \begin{pmatrix} GF(q) & GF(q) \\ 0 & 0 \end{pmatrix}$$

и в кольце R существует подкольцо, чей гомоморфный образ имеет тип а). Если $\bar{x}\bar{y}^2 \neq \bar{0}$, то, рассуждая аналогично, получим, что в R существует подкольцо, чей гомоморфный образ имеет тип а) или е).

Докажем утверждение 4). Пусть R содержит нецентральный элемент y такой, что $\left(R^{\#}yR^{\#}\right)^2 = (0)$. Из замечания 2 следует, что мы можем полагать $R = \langle x, y\rangle$ и $[R, R]$ – сердцевина R. Из утверждения 2) следует также что мы можем полагать $\big[x, [x, y]\big] \neq 0$. Рассмотрим кольцо $S = S_1/M$, где $S_1 = \langle x, [x, y]\rangle$ и M – максимальный идеал S_1, не содержащий $\big[x, [x, y]\big]$. Пусть $a = x + M$, $b = [x, y] + M$. Так как

$$[R, R] = R^{\#}\big[x, [x, y]\big]R^{\#} = (\big[x, [x, y]\big]),$$

то $[R, R] = [S_1, S_1]$ и $[S, S] = \left(S^{\#}bS^{\#}\right) = (b)$. Из утверждения 3) следует, что мы можем предполагать, что для любых двух элементов $u, v \in S$ из равенства $u \cdot v = 0$ следует, что $v \cdot u = 0$.

Докажем, что $\ell_{\langle a\rangle}((b)) \lhd S$. Пусть $z \in \ell_{\langle a\rangle}((b))$ и

$$w = f(a) + \sum_i u_i(a)bv_i(a)$$

– произвольный элемент из S. Тогда

$$zw = zf(a) + \sum_i u_i(a)(zb)v_i(a) = f(a)z \in \ell_{\langle a\rangle}((b)),$$

так как $zb = 0$. Если $\ell_{\langle a\rangle}((b)) \neq (0)$, то $b \in (b) \subseteq \ell_{\langle a\rangle}((b))$ и S – коммутативное кольцо. Противоречие доказывает, что $\ell_{\langle a\rangle}((b)) = (0)$. Пусть a_L и a_R – соответственно операторы левого и правого умножения на элемент a, действующие на (b). Тогда левый $\langle a_L, a_R\rangle$-модуль (b) является неприводимым. Откуда следует, что $\langle a_L, a_R\rangle$ – конечное поле (см. замечание 1). Подполя $\langle a_L\rangle$ и $\langle a_R\rangle$ имеют одинаковый порядок и $S = \langle a\rangle \dot{+} \langle a\rangle b$ имеет тип б), так как согласно работе [111] конечный $(\langle a\rangle, \langle a\rangle)$-бимодуль (b) имеет отмеченный базис, то есть такой элемент $b_1 \in (b)$, что для некоторого нетождественного автоморфизма

σ поля $\langle a\rangle$ и любого элемента $c \in \langle a\rangle$ справедливо равенство $b_1 c = \sigma(c) b_1$. $\square$

Перейдем к доказательству теоремы.

$\square$ Пусть R – произвольное некоммутативное кольцо и x, y – такие его элементы, что $[x, y] \neq 0$. Согласно замечанию 2, мы можем считать, что $R = \langle x, y\rangle$ и $[R, R]$ – сердцевина R . Если $[R, R]^2 = (0)$, то из леммы 5.22 (см. случай 2) и 4)) следует, что гомоморфный образ некоторого подкольца из R имеет тип а), б) или д). Если $[R, R]^2 \neq (0)$, то $[R, R]$ – простое кольцо. Если $J(R) = (0)$, то из леммы 5.22 (случай 1) следует, что гомоморфный образ некоторого подкольца имеет тип а) или в). Если же $J(R) \neq (0)$, то $[R, R]$ – простое радикальное кольцо типа г). $\square$

При доказательстве мы использовали следующий хорошо известный факт: если в подпрямо неразложимом кольце A сердцевина M удовлетворяет условию $M^2 \neq (0)$, то M – простое кольцо. Действительно, пусть I – ненулевой идеал M и $I_1 = I + RI + IR + RIR$. Тогда $I_1 \lhd R$, $I_1 \subseteq M$ и $I_1^3 \subseteq I$. Откуда следует, что $I_1 = M$ и $M = M^2 = M^3 \subseteq I$, то есть M – простое кольцо.

Следствие 5.3 (Х. Коматсу).
Пусть кольцо R содержит единицу и удовлетворяет тождеству

$$x^n[x, y] = [x, y^m],$$

где $(m, n) \neq (1, 0)$. Тогда R– коммутативное кольцо.

$\square$ Так как

$$(x + 1)^n[x + 1, y] = [x + 1, y^m],$$

то

$$\left(\begin{pmatrix} n \\ 1 \end{pmatrix} x^{n-1} + \begin{pmatrix} n \\ 2 \end{pmatrix} x^{n-2} + \ldots \right.$$
$$\left. \ldots + \begin{pmatrix} n \\ n-1 \end{pmatrix} x + 1\right)[x, y] = 0 \qquad (*)$$

для любых элементов $x, y \in R$. Предположим, что R – некоммутативное кольцо. По теореме 5.13 существует подкольцо $B \leqslant R$ такое, что некоторый гомоморфный образ B/I изоморфен одному из колец типов а)-д). Если $B/I = A_1$, то, полагая в $(*)$ $x = e_{12}$, $y = e_{11}$, получим, что

$$\left(\begin{pmatrix} n \\ 1 \end{pmatrix} e_{12}^{n-1} + \ldots + \begin{pmatrix} n \\ n-1 \end{pmatrix} e_{12} + 1 \right) [e_{12}, e_{11}] = -e_{12} = 0.$$

Противоречие. Случай, когда $B/I = A_1^0$, рассматривается аналогично.

Если

$$B/I = \left\{ \left. \begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix} \right| \ a, b \in GF(q), \right\},$$

то, полагая в равенстве $(*)$

$$x = e_{12}, \quad y = \begin{pmatrix} a & 0 \\ 0 & \sigma(a) \end{pmatrix},$$

где $a \neq \sigma(a)$, получим противоречие.

Если B/I – некоммутативное тело, то по теореме Капланского (см. главу 4) тело B/I является конечномерным над своим центром Z. Если Z – конечное тело, то $|B/I| < \infty$ и по теореме Веддерберна $B/I = Z$. Противоречие. Если Z – бесконечное поле, то каждая однородная компонента тождества $(*)$ является тождеством в B/I (см. главу 4). В частности, B/I удовлетворяет тождеству $[x, y] = 0$. Противоречие.

Если B/I – простое радикальное кольцо, то оно удовлетворяет полилинейному тождеству, получаемому линеаризацией тождества $x^n[x, y] - [x, y^m] = 0$. Так как оно является первичным кольцом, то его центр $Z(B/I) \neq (0)$ (см. главу 4) и так как B/I – простое кольцо, то $Z(B/I)$ – поле. Радикальное кольцо не содержит ненулевые идемпотентные элементы. Таким образом, этот случай невозможен.

Рассмотрим, наконец, последний случай. Именно, пусть B/I – конечное нильпотентное кольцо, удовлетворяющее тождеству

$x[y,z]=0$. Тогда учитывая тождество $(*)$ в B/I, получим, что B/I – коммутативное кольцо. Противоречие. □

Следствие 5.4 (Т. Кезлан).
Пусть кольцо R удовлетворяет тождеству

$$[x,y]+\sum_i u_i(x,y)[x,y]v_i(x,y)=0,$$

где $\deg_x u_i+\deg_x v_i\geq 1$. *Тогда R – коммутативное кольцо.*

□ Предположим, что R – некоммутативное кольцо. По теореме 5.13 в R существует подкольцо $B\leq R$ такое, что некоторый его гомоморфный образ B/I изоморфен кольцу одного из типов а) - д).

Если B/I имеет тип а), то подстановка в тождество $x=e_{12}$, $y=e_{11}$ приводит к противоречию. Если B/I имеет тип б), то подстановка в тождество

$$x=e_{12},\quad y=\begin{pmatrix} a & 0\\ 0 & \sigma(a)\end{pmatrix},$$

где $a\neq\sigma(a)$ тоже приводит к противоречию. Если B/I имеет тип в) или г), то $\mathrm{char}B/I=p$ – простое число и B/I удовлетворяет полилинейной линеаризации исходного тождества. Рассуждая, далее, аналогично доказательству следствия 5.3, приходим к противоречию. Если B/I имеет тип д), то B/I удовлетворяет тождеству $x[y,z]=[x,y]z=0$. Так как $\deg_x u_i+\deg_x v_i\geq 1$, то B/I – коммутативное кольцо. Противоречие. □

Другие многочисленные приложения теоремы 5.13 к доказательству "теорем коммутативности"можно найти в работах [91, 92]. При доказательстве "теорем коммутативности"можно использовать язык многообразий колец. А именно из леммы Цорна следует, что произвольное некоммутативное многообразие колец содержит минимальное некоммутативное подмногообразие колец. В работе [51] доказано, что каждое минимальное некоммутативное многообразие колец, порождается одним

из следующих колец:

$$A_1 = \begin{pmatrix} GF(p) & GF(p) \\ 0 & 0 \end{pmatrix}, \quad A_1^0 = \begin{pmatrix} GF(p) & 0 \\ GF(p) & 0 \end{pmatrix}, \quad B,$$

$$\left\{ \begin{pmatrix} a & b \\ 0 & a^{p^t} \end{pmatrix} \middle| \ a, b \in GF(p^{q^l}),\ t = nq^{l-1},\ p, q \text{ – простые числа} \right\},$$

где B – конечное нильпотентное кольцо порядка p^k (p – простое число), удовлетворяющее тождествам

$$x[y, z] = [x, y]z = 0, \quad [x, y] + f(x, y) = 0,$$

где $f(x, y)$ – сумма одночленов (от x, y) степени $n-1$, $B^n = (0)$. В частности, если в многообразии колец все конечные кольца коммутативны, то оно состоит только из коммутативных колец. В работе [52] приведены примеры использования минимальных некоммутативных многообразий колец для доказательства "теорем коммутативности."

5.5. Коммутативность колец, удовлетворяющих тождествам

Кольцо

$$A = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} \middle| \ a, b, c, d \in GF(2) \right\}$$

содержит единицу, удовлетворяет тождеству

$$[(xy)^2, x] = 0,$$

но не является коммутативным.

В работе [109] доказана следующая интересная теорема.

Теорема 5.14. *Пусть R – кольцо с единицей, удовлетворяющее тождествам*

$$[(xy)^n, x] = 0, \quad [(xy)^{n+1}, x] = 0.$$

Тогда R – коммутативное кольцо.

□ Заметим, что если a – такой элемент R, что для любого элемента $x \in R$

$$x^k[x,a] = 0$$

(k– фиксированное натуральное число), то a – центральный элемент. Действительно, из равенств

$$x^k[x,a] = 0, \quad (x+1)^k[x,a] = 0$$

следует, что $x^{k-1}[x,a] = 0$ для любого элемента $x \in R$. Рассуждая аналогично, получим, что $a \in \mathrm{Cent}R$. Пусть u – обратимый элемент в R. Тогда из равенств

$$[(u(u^{-1}x))^n, u] = [x^n, u] = 0,$$

$$[(u(u^{-1}x))^{n+1}, u] = [x^{n+1}, u] = x^n[x,u] + [x^n,u]x = 0$$

следует, что

$$x^n[x,u] = 0.$$

В силу предыдущего замечания получаем, $[x,u] = 0$ для любого элемента $x \in R$, то есть $u \in \mathrm{Cent}R$. В частности, если $a \in J(R)$, то $1+a$ – обратимый элемент и $1+a, a \in \mathrm{Cent}R$, то есть $J(R) \subseteq \mathrm{Cent}R$.

Пусть P – примитивный идеал кольца R. По теореме плотности либо $R/P = M_m(D)$, либо для любого целого числа $k \geq 1$ существует подкольцо $S \leq R/P$ такое, что некоторый его гомоморфный образ $S/I \cong M_k(D)$, где D – тело. Если имеет место второй случай, то, взяв $k = 2$ и положив в тождестве $x = e_{21}$, $y = e_{12} + e_{21}$, получим, что

$$[(xy)^n, x] = [e_{22}, e_{21}] \neq 0.$$

Следовательно, имеет место первый случай, то есть $R/P = M_m(D)$, где D – тело. Если $m \geq 2$, то, рассуждая аналогично предыдущему случаю, получим противоречие. Следовательно, $R/P = D$ – поле. Так как $J(R)$ – пересечение всех примитивных идеалов кольца R, то $R/J(R)$ – коммутативное кольцо. В частности, $(xy)^n - x^n y^n \in J(R) \subseteq \mathrm{Cent}R$ для любых элементов

$x, y \in R$. Поэтому $[x^n y^n, x] = [(xy)^n, x] = 0$ и $x^n[y^n, x] = 0$. Используя выше приведенное замечание, получаем, что $[y^n, x] = 0$ – тождество в кольце R. Аналогично можно доказать, что тождеством в R является $[y^{n+1}, x] = 0$. Следовательно,

$$y^n[y, x] = [y^{n+1}, x] - [y^n, x]y = 0$$

и согласно замечанию $[y, x] = 0$, то есть R – коммутативное кольцо. □

Следующая теорема доказана Т. Лаффи и Д. Макале в работе [100].

Теорема 5.15. *Пусть $f(t) = a_1 t + a_2 t^2 + \ldots + a_n t^n$ – ненулевой многочлен с целым коэффициентом, и $\mathfrak{M}$ – класс всех колец, удовлетворяющих тождеству $f(x) = 0$. Тогда $\mathfrak{M}$ состоит из коммутативных колец тогда и только тогда, когда выполняется одно из условий:*

1) $a_1 = \pm 1$;

2) $a_1 = \pm 2$, a_2 – нечетное число и $u(a_2 + a_3 + \ldots + a_n)$ – нечетное число.

□ Пусть кольцо R удовлетворяет тождеству

$$f(x) = \pm x + a_2 x^2 + \ldots + a_n x^n = 0.$$

Докажем, что радикал Джекобсона $J(R) = (0)$. Пусть $a \in J(R)$. Тогда

$$\pm a = -a_2 a^2 - \ldots - a_n a^n = ag(a)$$

и $a = ab$, где $b \in J(R)$. Ввиду квазирегулярности идеала $J(R)$ существует такой элемент $c \in J(R)$, что $(-b) + c + (-b)c = 0$. Следовательно, $a = ab = a(c - bc) = ac - (ab)c = ac - ac = 0$ и $J(R) = (0)$.

Пусть P – примитивный идеал кольца R. Тогда по теореме плотности R/P – плотное кольцо линейных произведений некоторого векторного пространства V над телом D. Если $\dim_D V \geq 2$ и $\{v_1, v_2\}$ – линейно независимые векторы, то

ввиду плотности R/P существует такой элемент $s \in R/P$, что $v_1 s = v_2$, $v_2 s = 0$. Следовательно,

$$v_1 f(s) = v_1 0 = v_1(\pm s) + v_1\left(a_2 s^2\right) + \ldots + v_1\left(a_n s^n\right) = \pm v_2 + 0 = \pm v_2.$$

Противоречие доказывает, что $\dim_D V = 1$ и $R/P = D$ – тело, удовлетворяющее тождеству

$$\pm x + a_2 x^2 + \ldots + a_n x^n = 0.$$

Если $2D \neq 0$, то

$$\begin{aligned}(\pm 2 + a_2 \cdot 2^2 + \ldots + a_n \cdot 2^n) \cdot 1 = \\ = 2(\pm 1 + a_2 \cdot 2 + \ldots + a_n \cdot 2^{n-1}) \cdot 1 = \\ = (\pm 1 + a_2 \cdot 2 + \ldots + a_n \cdot 2^{n-1}) \cdot 1 = 0\end{aligned}$$

и тело D содержит подполе $GF(p)$ для некоторого простого числа p. Пусть α – произвольный элемент тела D. Тогда

$$\pm\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$$

и подалгебра $GF(p)[\alpha]$ является конечной, то есть конечным полем. Это означает, в частности, что $\alpha = \alpha^{p^k}$ для некоторого числа $k \geq 1$. По теореме Джекобсона 5.4 D – поле. Так как полупростое кольцо R является подпрямым произведением примитивных колец вида R/P, где P – примитивный идеал R и каждое такое кольцо является полем, то R – коммутативное кольцо.

Предположим, что R удовлетворяет тождеству

$$f(x) = \pm 2x + a_2 x^2 + \ldots + a_n x^n = 0,$$

где a_2 и $a_2 + a_3 + \ldots + a_n$ – нечетные целые числа. Докажем, что R – коммутативное кольцо. Для этого заметим, что без ограничения общности, можно считать, что многочлен $f(x)$ имеет вид

$$f(x) = 2x + a_2 x^2 + \ldots + a_n x^n.$$

Тогда

$$g(x) = 2^n f(x) - f(2x) =$$
$$= \left(2^{n+1} - 2^2\right) x + \left(2^n - 2^2\right) a_2 x^2 + \ldots + \left(2^n - 2^{n-1}\right) a_n x^{n-1} = 0$$

является тождеством в кольце R. Продолжая эти рассуждения, мы получим, что

$$\left(2^{n+1} - 2^2\right)\left(2^{n-1} - 2\right) \ldots \left(2^2 - 2\right) x = 0$$

– тождество в кольце R. Пусть

$$\left(2^{n+1} - 2^2\right)\left(2^{n-1} - 2\right) \ldots \left(2^2 - 2\right) = p_1^{k_1} \ldots p_s^{k_s}$$

– каноническое разложение на простые множители. Тогда

$$R = R_1 \oplus \ldots \oplus R_s,$$

где

$$R_i = \{a \in R |\ p_i^{k_i} a = 0\} \lhd R,$$

$i \leq s$. Докажем, что каждое кольцо R_i является коммутативным, $i \leq s$. Если $p_i \neq 2$, то существует целое число q такое, что $2q \equiv 1 (\mathrm{mod}\, p_i^{k_i})$ и R_i удовлетворяет тождеству

$$qf(x) = x + (a_2 q)x^2 + \ldots + (a_n q)x^n = 0.$$

Ранее мы доказали коммутативность таких колец. Пусть $p_i = 2$. Тогда $2^{k_i} R_i = (0)$. Пусть m – наибольший индекс такой, что a_m – нечетное число. Тогда существует целое число l такое, что $l a_m \equiv 1 (\mathrm{mod}\, 2^{k_i})$ и, следовательно,

$$lf(x) = \left(x^m + \sum_{i \leq m-1} \lambda_i x^i\right) + 2\varphi(x) = 0$$

– тождество в кольце R_i. Откуда следует, что

$$\left(x^m + \sum_{i=1}^{m-1} \lambda_i x^i\right)^{k_i} = 0,$$

$\lambda_i \in \mathbb{Z}$. Пусть $a \in R_i$. Тогда

$$a^{mk_i} \in \sum_{t=1}^{mk_i-1} \mathbb{Z}a^t$$

и подкольцо $\langle a \rangle$, порожденное a, является конечным. Покажем, что $\langle a \rangle$ – нильпотентное подкольцо. Для этого достаточно показать, что в нем нет ненулевых идемпотентов. Если $e^2 = e \in \langle a \rangle$, то

$$f(e) = (2 + a_2 + \ldots + a_n)e = 0.$$

Так как $2+a_2+\ldots+a_n$ – нечетное число и $2^{k_i}e = 0$, то $e = 0$. Таким образом, R_i – ниль-кольцо удовлетворяющее тождествам:

$$f(x) = 2x + a_2x^2 + \ldots + a_nx^n = 0,$$

$$f(2x) - 2f(x) = 2a_2x^2 + a_3(2^3 - 2)x^3 + \ldots + a_n(2^n - 2)x^n = 0.$$

Так как a_2 – нечетное число, то существует целое число c такое, что $a_2c \equiv 1 (\mathrm{mod}\, 2^{k_i})$. Следовательно,

$$c(f(2x) - 2f(x)) = 2x^2(1 + x\psi(x)) = 0$$

– тождество в кольце R_i, где $\psi(t) \in \mathbb{Z}[t]$. Пусть $a \in R_i$. Тогда элемент $b = a\psi(a)$ является нильпотентным, а элемент $1 - b$ обратимым в кольце $\langle a \rangle^{\#}$ с присоединенной единицей. Следовательно, $2a^2 = 0$ для любого элемента $a \in R_i$. Поэтому

$$2f(x) = 4x + a_2 \cdot 2x^2 + \ldots + a_n \cdot 2x^n = 4x = 0,$$

$$xf(x) = 2x^2 + a_2x^3 + a_3x^4 + \ldots + a_nx^{n+1} = \\ = a_2x^3 + a_3x^4 + \ldots + a_nx^{n+1} = 0$$

и

$$(cx)f(x) = x^3(1 + x\psi_1(x)) = 0$$

– тождества в кольце R_i. Аналогично предыдущим рассуждениям из последнего тождества следует, что $x^3 = 0$ в кольце R_i. Следовательно, R_i удовлетворяет тождеству

$$f(x) = 2x + x^2 = 0.$$

Пусть $a, b \in R_i$. Тогда

$$2(a+b) + (a+b)^2 - (2a + a^2) - (2b + b^2) = ab + ba = 0$$

и

$$2(ab) + (ab)^2 = 2ab + abab = 2ab - a^2b^2 = \\ = 2ab - (-2a)b^2 = 2ab + a(2b^2) = 2ab = 0$$

и $ab = -ab$, то есть $ab = -ba = -(-ba) = ba$ и R_i – коммутативное кольцо.

Докажем теорему в обратную сторону. Пусть любое кольцо, удовлетворяющее тождеству

$$f(x) = a_1x + a_2x^2 + \ldots + a_nx^n = 0,$$

является коммутативным. Если $a_1 \neq \pm 1, \pm 2$, то кольцо

$$A = \langle u, v |\ u^2 = v^2 = uv + vu = 0, a_1u = a_1v = 0 \rangle$$

является некоммутативным и удовлетворяет тождествам

$$f(x) = 0, \quad x^2 = 0, \quad xyz = 0.$$

Если $a_1 = \pm 1$, то теорема доказана. Пусть $a_1 = \pm 2$. Если a_2 – четное число, то кольцо

$$B = \begin{pmatrix} 0 & GF(2) & GF(2) \\ 0 & 0 & GF(2) \\ 0 & 0 & 0 \end{pmatrix}$$

удовлетворяет тождествам

$$2x = 0, \quad x^3 = 0, \quad f(x) = 0,$$

но не является коммутативным. Итак, a_2 – нечетное число. Если $a_2 + a_3 + \ldots + a_n$ – четное число, то кольцо

$$C = \begin{pmatrix} GF(2) & GF(2) \\ 0 & 0 \end{pmatrix}$$

удовлетворяет тождеству $f(x) = 0$ и не является коммутативным. Противоречие. □

Пусть $\mathbb{Z}\langle x, y, z\rangle$ – свободное ассоциативное кольцо с единицей от трех образующих $\{x, y, z\}$ и $f(x, y, z) \in \mathbb{Z}\langle x, y, z\rangle$. Положим

$$\sigma(f(x, y, z)) = f(x + 1, y, z)$$

и

$$\Delta(f) = f(x + 1, y, z) - f(x, y, z).$$

Легко видеть, что любых многочленов $f, g \in Z\langle x, y, z\rangle$ справедливы равенства:

$$\Delta(f + g) = \Delta(f) + \Delta(g),$$

$$\Delta(f \cdot g) = \Delta(f)\sigma(g) + f(\Delta(g)),$$

$$\Delta^n(f \cdot g) = \sum_{i=0}^{n} \binom{n}{i} \Delta^i(f)\sigma^i\left(\Delta^{n-i}(g)\right)$$

(формула Лейбница).

Лемма 5.23. *Пусть многочлен $f(x, y, z)$ является однородным степени n относительно переменной x. Тогда*

$$\Delta^n(f) = n! f(1, y, z) \quad и \quad \Delta^m(f) = 0,$$

если $m \geq n + 1$.

□ Доказательство леммы достаточно привести для одночленов, в виду равенства

$$\Delta(f + g) = \Delta(f) + \Delta(g).$$

Пусть $f = axb$ – одночлен, содержащий переменную x n-раз, в котором слово a не содержит x, а $\deg_x b = n-1$. Воспользуемся методом математической индукции. Если $n = 1$, то

$$\Delta(f) = \Delta((ax)\cdot b) = \Delta(ax)\cdot\sigma(b) + (ax)\Delta(b) = a\cdot b = 1!f(1,y,z).$$

Сделаем предположение индукции о справедливости утверждения для однородных многочленов степени меньше n и докажем наше утверждение для одночлена $f = axb$. По формуле Лейбница имеем, что

$$\begin{aligned}\Delta^n((ax)b) &= ax\Delta^n(b)+\\ &+ n\Delta(ax)\sigma\left(\Delta^{n-1}(b)\right) + \binom{n}{2}\Delta^2(ax)\sigma^2\left(\Delta^{n-2}(b)\right) + \dots\\ &= (ax)\Delta^n(b) + na\sigma(\Delta^{n-1}(b)) = na((n-1)!b(1,y,z)) =\\ &= n!ab(1,y,z) = n!f(1,y,z). \ \square\end{aligned}$$

В работе [65] доказан следующий полезный результат.

Теорема 5.16. *Пусть R – кольцо с единицей, удовлетворяющее тождеству*

$$f(x,y,[x,y]) = 0,$$

где $f(x,y,z)$ – однородный многочлен степеней n и m относительно переменных x и y соответственно. Тогда R удовлетворяет тождеству

$$n!m!f(1,1,[x,y]) = 0.$$

$\square$ Так как

$$f(x+1,y,[x+1,y]) = f(x+1,y,[x,y]) = 0,$$

то $\sigma(f)$, $\Delta(f)$, $\Delta^n(f)$ – многочлены $\mathbb{Z}\langle x,y,z\rangle$, являющиеся тождествами в кольце R. По лемме 5.23 кольцо R удовлетворяет тождеству

$$n!f(1,y,[x,y]) = 0.$$

Применяя лемму 5.23 к переменной y, получим, что R удовлетворяет тождеству

$$m!n!f(1,1,[x,y])=0.$$

□

Следствие 5.5. *Пусть R – кольцо с единицей, удовлетворяющее тождеству $(xy)^n=x^ny^n$, где $n\geq 2$. Тогда R удовлетворяет тождеству*

$$(n-1)^2\cdot\frac{n(n-1)}{2}\cdot[x,y]=0.$$

□ Так как

$$x^ny^n-(xy)^n=\sum_{k=1}^{n-1}x^k\left(\sum_{i=0}^{k-1}y^i[x,y]y^{n-i}\right)(xy)^{n-k-1},$$

то рассмотрим многочлен

$$f(x,y,z)=\sum_{k=1}^{n-1}x^k\left(\sum_{i=1}^{k-1}y^izy^{n-i}\right)(xy)^{n-k-1}$$

из $\mathbb{Z}\langle x,y,z\rangle$. Он является однородным степени $n-1$ относительно переменных x и y.

Далее, $f(x,y,[x,y])=0$ – тождество в кольце R. Согласно теореме 5.16 кольцо R удовлетворяет тождеству

$$(n-1)!(n-1)!f(1,1,[x,y])=((n-1)!)^2\cdot\frac{n(n-1)}{2}\cdot[x,y]=0.$$

□

Пусть R – кольцо и $X_1,X_2,\ldots,X_n$ – его непустые подмножества. Обозначим через

$$X_1X_2\ldots X_n=\{a_1a_2\ldots a_n|\ a_i\in X_i,i=1,\ldots,n\}.$$

В работе [70] доказано, что если для любых бесконечных подмножеств X, Y бесконечного кольца R выполнено равенство $XY = YX$, то R – коммутативное кольцо. В работе [66] получено усиление этого результата. Доказано, что если в бесконечном кольце R для любых бесконечных подмножеств $X, Y \subseteq R$ пересечение $XY \cap YX$ не является пустым множеством, то R – коммутативное кольцо. В работе [53] доказано, что если в бесконечном кольце R для любых бесконечных множеств $X, Y, Z \subseteq R$ выполнено равенство $XYZ = YXZ$, то R удовлетворяет тождеству $[x, y]z = 0$. В работе [54] доказана следующая теорема, обобщающая выше приведенные результаты.

Теорема 5.17. *Пусть R – бесконечное кольцо, в котором для любых бесконечных подмножеств $X_1, X_2, \ldots, X_n \subseteq R$ справедливо равенство*

$$X_1 X_2 \ldots X_n = X_{i_1} X_{i_2} \ldots X_{i_n},$$

где $(i_1, \ldots, i_n)$ – фиксированная перестановка чисел $\{1, 2, \ldots, n\}$ и $i_1 \neq 1$. Тогда R удовлетворяет тождеству

$$x_1 \ldots x_n = x_{i_1} \ldots x_{i_n}.$$

Выше приведенная теорема 5.15 (Т. Лаффи и Д. Макале) обобщена в работе [47] следующим образом.

Теорема 5.18. *Пусть Φ – конечно порожденное коммутативное кольцо с единицей, являющееся областью главных идеалов и*

$$f(x) = a_1 x + a_2 x^2 + \ldots + a_n x^n \in \Phi[x].$$

Произвольная Φ-алгебра R, удовлетворяющая тождеству $f(x) = 0$ является коммутативной тогда и только тогда, когда либо a_1 – обратимый элемент в Φ, либо a_1 – необратимый элемент, и если

$$a_1 = \pi_1^{k_1} \pi_2^{k_2} \ldots \pi_s^{k_s} \cdot \lambda$$

– его разложение на неприводимые множители ($\lambda | 1$, $\pi_i \neq \pi_j$ при $i \neq j$), то

1) a_1 *делит 2;*

2) $(a_1, a_2) = 1$*;*

3) $a_2x^2+\ldots+a_nx^n = 0$ *не является тождеством ни в одном из полей* $\Phi_i = \Phi/(\pi_i)$, $i \leq S$.

5.6. Упражнения

Упражнение 5.1. *Докажите, что* $\alpha = a_0+a_1i+a_2j+a_3k \in \mathbb{H}$ *является корнем уравнения* $t^2 + 1 = 0$ *тогда и только тогда, когда* $a_0 = 0$, $a_1^2 + a_2^2 + a_3^2 = 1$.

Упражнение 5.2. *Пусть* $\alpha, \beta \in \mathbb{H}$ *являются корнями уравнения* $t^2 + 1 = 0$. *Докажите, что они сопряжены, то есть* $\alpha = \gamma^{-1}\beta\gamma$, *где* $\gamma \in \mathbb{H}$.

Назовем R *кольцом со свойством конечного числа нулей* (или FZP-кольцо, где FZP-сокращенное "finite zero property"), если каждый ненулевой многочлен из $R[x]$ имеет в R конечное число корней (множество корней может быть пустым). Примерами FZP-колец являются конечные кольца и бесконечные коммутативные области целостности.

Упражнение 5.3. *Привести пример FZP-кольца, гомоморфный образ которого не является FZP-кольцом.*

$\diamondsuit$ Пусть $R = \mathbb{Z}[x]$. Тогда $R/6R$ не является FZP-кольцом. Действительно, уравнение $2x = 0$ имеет бесконечно много решений $\{3x^i |\ i = 1, 2, \ldots\}$ $\diamondsuit$

Упражнение 5.4. *Пусть* R *- бесконечное FZP-кольцо. Докажите, что* R *- кольцо без делителей нуля.*

$\diamondsuit$ Если $a, b \in R$ такие ненулевые элементы, что $ab = 0$, то $a(bR) = 0$. Откуда следует, что одно из уравнений $ax = 0$ или $bx = 0$ имеет бесконечное множество решений в R. $\diamondsuit$

Упражнение 5.5. *Пусть*

$$R * \mathbb{Z}[x] = \left\{ \sum a_1 x a_2 x \dots a_n x a_{n+1} \right\}$$

– множество "обобщенных" многочленов над R. Пусть множество корней в R произвольного ненулевого многочлена из множества $R * \mathbb{Z}[x]$ является пустым или конечным. Докажите, что R – конечное кольцо.

$\diamondsuit$ Предположим, что R – бесконечное кольцо. Из предыдущей задачи следует, что R – кольцо без делителей нуля. Пусть a – ненулевой элемент в R. Рассмотрим многочлен $[x, a] \in R * \mathbb{Z}[x]$. Его корнями являются элементы $a, a^2, a^3, \dots$. Так как множество корней конечно, то $a^i = a^j$ для некоторых чисел $i < j$. Откуда следует, что $a^{i-1}(a - a^{j-i+1}) = 0$ и $a = a^{j-i+1}$. По теореме Джекобсона R – коммутативное кольцо, все элементы которого – корни многочлена $[x, a]$. Противоречие. $\diamondsuit$

Упражнение 5.6. *Пусть D – бесконечное тело, являющееся FZP-кольцом. Докажите, что D – поле.*

$\diamondsuit$ Пусть D не совпадает со своим центром. Тогда существуют два элемента a и d такие, что $a \neq dad^{-1}$. Положим

$$c = \left(a - dad^{-1}\right) a \left(a - dad^{-1}\right)^{-1}, \quad b = c - \left(a - dad^{-1}\right).$$

Тогда

$$f(x) = (x - b)(x - a) = (x - c)\left(x - dad^{-1}\right)$$

и a, dad^{-1} – различные сопряженные элементы, являющиеся корнями многочлена $f(x)$. По теореме 5.7 многочлен $f(x)$ имеет бесконечно много корней в D. Противоречие. $\diamondsuit$

Упражнение 5.7. *Пусть*

$$\mathbb{H} = \mathbb{R}1 + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

– тело кватернионов,

$$A = \mathbb{Q}1 + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

и

$$B = \mathbb{Z}1 + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k.$$

Докажите, что B – FZP-кольцо, а A не является FZP-кольцом (A – кольцо частных B).

Упражнение 5.8. *Докажите, что кольцо R удовлетворяет тождеству $x = x^2$ тогда и только тогда, когда R не содержит ненулевых нильпотентных элементов и удовлетворяет тождеству $(x + y)xy = 0$.*

$\diamondsuit$ Если R не содержит ненулевых нильпотентных элементов и удовлетворяет тождеству $(x + y)xy = 0$, то R удовлетворяет тождествам:

$$(x + x)xx = 2x^3 = (2x)^3 = 0, \quad 2x = 0,$$

$$(uv+vu)y = (u+v)^2y+y(u+v)y-(u^2y+yuy)-(v^2y+yvy) = 0,$$

$$[u, v]y = 0, \quad [u, v]^2 = 0, \quad [u, v] = 0.$$

Далее,

$$x^2(x + x^2) + x(x + x^2)^2 = 0, \quad x^4 + x^5 = 0,$$

$$(x + x^2)^4 = 0, \quad x + x^2 = 0.$$

Таким образом, R удовлетворяет тождествам $x = -x^2 = x^2$. $\diamondsuit$

Упражнение 5.9. *Пусть R – кольцо с единицей, удовлетворяющей тождеству $x^n = x^m$, где m, n – натуральные числа такие, что $m-n$ – нечетное число. Докажите, что R – коммутативное кольцо.*

$\diamondsuit$ Так как $(-1)^m = (-1)^n$ и $(m-n)$ – нечетное число, то $2R = 0$. Если $a \in R$ такой элемент, что $a^2 = 0$, то $(1+a)^m = (1+a)^n$ и $(m-n)a = 2a = 0$. Откуда следует, что $a = 0$ и R – кольцо без нильпотентных элементов. Пусть $m < n$. Тогда

$$\left(x^{m-n+1} - x\right)^{n+1} = \\ = \left(x^{m-(n-1)} - x\right) x^{n-1} \left(x^{m-n} - 1\right)^{n-1} \left(x^{m-n+1} - x\right) = 0$$

– тождество в кольце R. Следовательно, R удовлетворяет тождеству $x^{m-n+1} = x$ и по теореме 5.8 является коммутативным кольцом. $\diamondsuit$

Упражнение 5.10. *Пусть R – кольцо с единицей и $I \lhd R$. Докажите, что R/I удовлетворяет тождеству $x = x^q$, где q – натуральное число ($q \geq 2$) тогда и только тогда, когда I – пересечение таких идеалов $P \lhd R$, что R/P – конечное поле и $|R/P| - 1$ делит число $q - 1$.*

$\diamondsuit$ Пусть

$$I = \bigcap_{\alpha \in \Lambda} P_\alpha,$$

где $P_\alpha \lhd R$, R/P_α – конечное поле и $(|R/P_\alpha| - 1) | (q-1)$. Тогда R/I – подпрямое произведение колец R/P_α, каждое из которых удовлетворяет тождеству $x = x^q$.

Докажем обратное утверждение. Пусть кольцо R/I удовлетворяет тождеству $x = x^q$. Тогда R/I – полупростое кольцо и существуют примитивные идеалы $P_\alpha \lhd R$, $\alpha \in \Lambda$, такие, что $P_\alpha \geq I$ и $\bigcap\limits_{\alpha \in \Lambda} P_\alpha = I$. Примитивные кольца R/P_α, $\alpha \in \Lambda$, удовлетворяют тождеству и, следовательно, являются полями с циклическими мультипликативными группами $(R/P_\alpha)^*$ порядка $|R/P_\alpha| - 1$. Так как $x^{q-1} = 1$ – тождество в группе $(R/P_\alpha)^*$, то $|R/P_\alpha| - 1$ делит $q - 1$.

В частности, кольцо $\mathbb{Z}_m$ классов вычетов по модулю $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ удовлетворяет тождеству $x = x^q$ тогда и только тогда, когда $\alpha_1 = \alpha_2 = \dots = \alpha_s$ и для любого числа $i \leq s$, $p_i - 1$ делит $q - 1$. $\diamondsuit$

Упражнение 5.11. *Пусть кольцо R содержит единицу и удовлетворяет тождеству $(xy)^2 = x^2y^2$. Докажите, что R – коммутативное кольцо.*

$\diamondsuit$ Так как

$$((a+1)b)^2 - (a+1)^2b^2 = bab - ab^2 = 0$$

и

$$(a(b+1))^2 - a^2(b+1)^2 = aba - a^2b = 0,$$

то

$$ab^2 = b^2a = bab.$$

Далее,

$$((a+1)(b+1))^2 - (a+1)^2(b+1)^2 =$$
$$= aba+ab^2+3ab+a^2b+bab+ba-(2a^2b+2ab^2+4ab) = ba-ab = 0,$$

то есть R – коммутативное кольцо. $\diamondsuit$

Упражнение 5.12. *Пусть R – кольцо с единицей и для любых элементов $a, b \in R$ существуют целые взаимно простые числа α, β такие, что $\alpha ab = \beta ba$. Докажите, что R – коммутативное кольцо (см. [101]).*

Упражнение 5.13. *Пусть R – кольцо, удовлетворяющее тождествам $px = 0$, $x = x^p$, где p – простое число. Проверьте, что R – подпрямая сумма полей, изоморфных $GF(p)$, пользуясь следующей схемой рассуждения:*

1) *R не содержит нильпотентных элементов;*

2) *если $e^2 = e \in R$ и $x \in R$, то $(ex - exe)^2 = (xe - exe)^2 = 0$ (выведите отсюда, что идемпотентные элементы принадлежат центру);*

3) *если $a = a^p$, то $e = a^{p-1} = e^2$;*

4) $R = \sum\limits_{i\in I} \bigoplus\limits_{S} R_i$, *где* R_i *– подпрямо неразложимое кольцо, удовлетворяющее тождествам* $px = 0$, $x = x^p$, $i \in I$;

5) Если $e^2 = e \in R$, *то* $R = Re \oplus R(1-e)$, *где* $Re \lhd R$, $R(1-e) \lhd R$;

6) если R *– подпрямо неразложимое кольцо, то* R *– тело;*

7) если R *– тело и* $a \in R \setminus (GF(p) \cdot 1)$, *то* $|(GF(p)[a]| \leq p$.

Упражнение 5.14. *Пусть* $F = \mathbb{C}(x)$ *– поле рациональных функций над полем комплексных чисел* $\mathbb{C}$ *и*

$$\varphi : F \to F$$

– автоморфизм поля такой, что

$$\varphi\left(\frac{a(x)}{b(x)}\right) = \frac{a(x+1)}{b(x+1)}.$$

Пусть

$$D = F\langle\langle t\rangle\rangle = \left\{ \sum_{i=n}^{\infty} a_i t^i |\ t(a) = \varphi(a)t,\ a, a_i \in F,\ n \in Z \right\}$$

– кольцо формальных (косых) степенных рядов. Докажите, что D *– некоммутативное тело.*

Упражнение 5.15. *Пусть* R *– кольцо, удовлетворяющее условиям максимальности и минимальности для подколец. Докажите, что* R *– конечное кольцо.*

$\diamondsuit$ R является правым артиновым кольцом, в котором каждое подкольцо конечно порождено. Если R – тело, то R не содержит кольцо целых чисел $\mathbb{Z}$ (так как $\mathbb{Z} \supset 2\mathbb{Z} \supset 2^2\mathbb{Z} \supset \ldots$) и, следовательно, $R \supseteq GF(p)$. Пусть $a \in R$. Рассмотрим убывающую цепочку подколец

$$GF(p)[a] \supseteq GF(p)[a^2] \supseteq \ldots$$

По условию эта цепочка стабилизируется и, следовательно, существует целое число $n \geq 1$ такое, что

$$a^n = \sum_{j=1}^{m} \alpha_j a^{n+j}$$

при некоторых элементах $\alpha_j \in GF(p)$. Это доказывает, что $GF(p)[a]$ – конечное поле и $a = a^{p^k}$ для некоторого целого числа $k \geq 1$. По теореме 5.8 R – поле, являющееся конечнопорожденным алгебраическим расширением поля $GF(p)$. Следовательно, R – конечное поле. Если $R = J(R)$, то $R^n = 0$ для некоторого целого числа $n \geq 1$. Если $n = 2$, то R – конечнопорожденная абелева группа, не содержащая бесконечных циклических подгрупп, то есть $|R| < \infty$. Далее, рассуждая методом математической индукции по n, мы видим, что $|R/R^{n-1}| < \infty$, $(R^{n-1})^2 = (0)$ и $|R^{n-1}| < \infty$. Поэтому $|R| < \infty$.

Рассмотрим общий случай. Так как R – правое артиново кольцо, то при $R \neq J(R)$

$$R/J(R) = M_{n_1}\left(GF\left(p_1^{m_1}\right)\right) \oplus \ldots \oplus M_{n_k}\left(GF\left(p_k^{m_k}\right)\right)$$

и $J(R)$ – нильпотентное кольцо с условием максимальности и минимальности для подколец. Ранее нами было замечено, что $|J(R)| < \infty$. Следовательно, $|R| < \infty$. $\diamondsuit$

В заметке [102] доказано, что бесконечное кольцо, собственные кольца которого конечны либо является квазициклической группой типа p^∞, либо совпадает с $\bigcup\limits_{n=0}^{\infty} GF(p^{q^n})$ для некоторых простых чисел p и q.

Упражнение 5.16. *Пусть R – кольцо, в котором для любого элемента $a \in R$ существует многочлен $p(t) \in \mathbb{Z}[t]$ и целое число $m \geq 1$ такие, что $a^m = a^{m+1}p(a)$. Докажите, что R – периодическое кольцо, то есть для любого элемента $a \in R$ существуют целые числа $m, n \geq 1$ такие, что $a^m = a^{m+n}$.*

$\diamondsuit$ Пусть $a \in R$. Докажем, что некоторая степень a порождает конечное подкольцо. Для этого рассмотрим кольцо $S = \langle a \rangle$.

Пусть N – ниль-радикал S. По условию существует целое число $m \geq 1$ и многочлен $p(t) \in \mathbb{Z}[t]$ такое, что

$$a^m - a^{m+1}p(a) = a^{m-1}(a - a^2p(a)) = 0.$$

Откуда следует, что $\big(a - a^2p(a)\big)^{m+1} = 0$ и $a - a^2p(a) \in N$. В кольце $a = S/N$ элемент $\bar{e} = \bar{a}p(\bar{a})$ является единицей. Это кольцо является гомоморфным образом кольца $\mathbb{Z}[t]$ и, следовательно, A – нетерово кольцо. Пусть $b \in A$. Тогда $b = b^2g(b)$ для некоторого многочлена $g(t) \in \mathbb{Z}[t]$. Элемент $f = bg(b)$ является идемпотентом в A и $A = fA \oplus (1-f)A$. Так как A – нетерово кольцо, $A = A_1 \oplus \ldots \oplus A_k$ – конечная прямая сумма идеалов A_i, $i \leq k$. Каждое кольцо A_i является неразложимым в прямую сумму, $i \leq k$. Поэтому A_i – поля, $i \leq k$.

Пусть e_i – единица A_i и a_i – образ элемента $\bar{a}$ при гомоморфизме

$$\pi_i : A \longrightarrow A_i, \quad \pi_i((x_1, \ldots, x_n)) = x_i.$$

Тогда $2e_i = (2e_i)^2q(2e_i)$, где $q(t)$ – некоторый многочлен из $\mathbb{Z}[t]$ и A_i – поле конечной характеристики p_i, $i \leq k$. A_i является одно порожденным алгебраическим расширением поля $GF(p_i)$ и, следовательно, $A_i \cong GF(p_i^{m_i})$. В частности, $a_i = a_i^{p_i^{m_i}}$. Пусть

$$l = (p_1^{m_1} - 1)(p_2^{m_2} - 1)\ldots(p_n^{m_n} - 1) + 1.$$

Тогда $a_i - a_i^l = 0$ и $a - a^l \in N$ и $(p_1p_2\ldots p_n)a \in N$. Откуда следует, что существуют числа $u \geq 1$ и $v \geq 1$ такие, что $(a - a^l)^u = 0$ и $(p_1\ldots p_n)^v a^v = 0$.

Пусть $c = a^v$. Проводя аналогичные рассуждения относительно элемента c, получим, что $(p_1\ldots p_n)^v c = 0$ и $(c - c^{l_1})^{u_1} = 0$ для некоторых чисел $l_1 \geq 2$ и $u_1 \geq 1$. Откуда следует, что подкольцо $\langle c \rangle$, порожденное c, является конечным. Поэтому найдутся числа $k_1 \geq 1$ и $k_2 \geq 1$ такие, что $c^{k_1} = c^{k_1+k_2}$ или $a^{vk_1} = a^{vk_1+vk_2}$. $\diamondsuit$

Упражнение 5.17. *Пусть $f(t)$, $g(t)$ – многочлены с коэффициентами из поля F. Докажите, что многочлен $f(t)$ принадлежит подалгебре $F\langle 1, g(t)\rangle$ тогда и только тогда, когда в*

кольце многочленов $F[x,y]$ многочлен $f(x)-f(y)$ делится на $g(x)-g(y)$ (см. [73]).

$\diamondsuit$ Предположим, что $f(x)-f(y)$ делится на $g(x)-g(y)$ в $F[x,y]$. Положим $\widetilde{f}(t)=f(t)-f(0)$. Тогда $\widetilde{f}(x)-\widetilde{f}(y)$ делится на разность $\widetilde{g}(x)-\widetilde{g}(y)$. Если мы докажем, что $\widetilde{f}(t)\in F\langle 1,\widetilde{g}(t)\rangle$, то

$$\begin{aligned}\widetilde{f}(t)=f(t)-f(0)=\\ =a_0+a_1\widetilde{g}(t)+\ldots+a_n\widetilde{g}(t)^n=\\ =a_0+a_1(g(t)-g(0))+\ldots+a_n(g(t)-g(0))^n=\\ =c_0+c_1g(t)+\ldots+c_ng(t)^n\end{aligned}$$

и $f(t)\in F\langle 1,g(t)\rangle$.

Итак, можно считать, что $f(t)$ и $g(t)$ – такие многочлены, что $f(0)=g(0)=0$ и $g(x)-g(y)$ делит $f(x)-f(y)$ в $F[x,y]$. Тогда

$$f(x)-f(y)=(g(x)-g(y))h(x,y),$$

где $h(x,y)\in F[x,y]$. Полагая $y=0$, получим, что $f(t)=g(t)f_1(t)$, где $f_1(t)=h(t,0)$. Следовательно,

$$\begin{aligned}g(x)f_1(x)-g(y)f_1(y)=\\ =f_1(y)(g(x)-g(y))+g(x)(f_1(x)-f_1(y))=(g(x)-g(y))h(x,y)\end{aligned}$$

и $g(x)-g(y)$ делит $g(x)(f_1(x)-f_1(y))$. Так как $F[x,y]$ – область с однозначным разложением на множители, $g(x)$ и $g(x)-g(y)$ – взаимно простые многочлены, то $g(x)-g(y)$ делит $f_1(x)-f_1(y)$. Далее можно воспользоваться методом математической индукции по степени многочлена $f(t)$. $\diamondsuit$

Упражнение 5.18. *Пусть R – конечное кольцо, нильпотентные элементы которого лежат в центре. Докажите, что R – коммутативное кольцо.*

$\diamondsuit$ Допустим противное и R – контрпример минимального порядка. Тогда R – ненильпотентное кольцо. Следовательно, R

содержит идемпотент $e^2 = e \neq 0$ Так как $ex - exe$ и $xe - exe$ – нильпотентные элементы, то $e(ex - exe) = (ex - exe)e = 0$ и $e(xe - exe) = (xe - exe)e = 0$. Откуда следует, что $ex = xe$ и

$$R = eR \oplus (1 - e)R = eRe \oplus (1 - e)R(1 - e).$$

Ввиду минимальности $|R|$ получаем $(1 - e)R(1 - e) = (0)$ и e – единица R. Если I – ненулевой идеал R, то I не содержит идемпотентов и, следовательно, $I \subseteq J(R)$ и $R/J(R) = M_n(GF(q))$. Если $n \geq 2$, то прообраз e_{12} в кольце R является нецентральным нильпотентным элементом. Следовательно,

$$R/J(R) = GF(q) = \left\langle \bar{0}, \bar{\lambda}, \bar{\lambda}^2, \ldots, \bar{\lambda}^{q-1} \right\rangle.$$

и R порождается λ и $J(R)$. Так как $J(R)$ содержит в центре R, то R – коммутативное кольцо. $\diamondsuit$

Упражнение 5.19. *Пусть произвольный элемент a кольца R либо принадлежит центру, либо для него существует целое число $n(a) \geq 2$ такое, что $a = a^{n(a)}$. Докажите, что R – коммутативное кольцо.*

$\diamondsuit$ Примените теорему 5.9. $\diamondsuit$

Литература

[1] Андрунакиевич В.А., Рябухин Ю.М. Радикалы и структурная теория.–М.: Наука, 1979.

[2] Бокуть Л.А. Ассоциативные кольца.–Новосибирск: Изд-во НГУ, 1977.–Ч.1.

[3] Бокуть Л.А. Ассоциативные кольца.–Новосибирск: Изд-во НГУ, 1977.–Ч.2.

[4] Бурбаки Н. Алгебра: модули, кольца, формы.–М.: Наука, 1966.

[5] Бурбаки Н. Коммутативная алгебра.–М.: Мир, 1971.–С. 420.

[6] Джекобсон Н. Строение колец.–М.: ИЛ, 1961.

[7] Джекобсон Н. Теория колец.–М.: ИЛ, 1947.

[8] Дрозд Ю.А., Кириченко В.В. Конечномерные алгебры.–Киев: Вища школа, 1980.

[9] Жевлаков К.А., Слинько А.М., Шестаков И.П., Ширшов А.И. Кольца, близкие к ассоциативным.–М.: Наука, 1978.

[10] Каш Ф. Модули и кольца.–М.: Мир, 1979.

[11] Криволапова В.К., Мальцев Ю.Н., Петрова Л.Н. Анатолий Илларионович Ширшов – из когорты великих

ученых. Сборник воспоминаний.–Барнаул: ГИПП "Алтай 2003.

[12] Лагутина Л.А., Мальцев Ю.Н., Петров Е.П. Избранные лекции по алгебре.–Барнаул: Изд-во НЭПП-Банк, 1997.

[13] Львов И.В. Лекции по теории колец.–Барнаул: Изд-во АлтГУ, 2003.

[14] Ламбек И. Кольца и модули.–М.: Мир, 1971.

[15] Ленг С. Алгебра.–М.: Мир, 1968.

[16] Мальцев Ю.Н., Петров Е.П. Лекции по теории колец и модулей.–Барнаул: Изд-во АлтГУ, 2000.

[17] Мальцев А.И. Основы линейной алгебры.–М.: Наука, 1975.

[18] Пирс Р. Ассоциативные алгебры.–М.: Мир, 1986.

[19] Скорняков Л.А. Элементы общей алгебры.–М.: Наука, 1983.

[20] Фейс К. Алгебра: кольца, модули, категории.–М.: Мир, 1977.–Т. 1, 2.

[21] Харченко В.К. Некоммутативная теория Галуа.–Новосибирск: Научная книга, 1996.

[22] Херстейн И. Некоммутативные кольца.–М.: Мир, 1972.

[23] Ширшов А.И. Кольца и алгебры. Избранные труды.–М.: Наука, 1984.

[24] Albert A.A. Structure of algebras.–Providence: Amer. Math. Soc., 1961.

[25] Benson Farb, Keith Dennis R. Noncommutative algebra.–Berlin: Springer-Verlag, 1993.

[26] Drensky V., Formanek E. Polinomial identity rings.–Basel. Boston. Berlin: Birkhauser Verlag, 2004.

[27] Herstein I.N. Topics in Ring theory.–Chicago: Univ. Chicago press, 1969.

[28] Jacobson N. Finite-dimensional division algebras over fields.–Berlin: Springer-Verlag, 1996.

[29] Jategaonkar A.V. Left principal ideal rings.–Berlin: Springer-Verlag, 1970.

[30] Jacobson N. PI-algebras.–Berlin: Springer-Verlag, 1975.

[31] Kanel-Belov A., Rowen L.H. Computation aspects of polynomial identities. Research Notes in Mathem.–V. 9.–Wellesley. Massachusetts, 2005.

[32] Mal'cev Y.N. The structure of associative algebras satisfying the polynomial identities and varieties of algebras.–Barnaul: AltSU publ., 1994.

[33] McDonald B. Finite rings with identity.–New-York: Denker, 1974.

[34] Rowen L.H. Ring theory.–Academic Press, 1991.

[35] Rowen L.H. Polynomial identities in ring theory.–Academic Press, 1980.

Научные статьи

[36] Андрунакиевич В.А., Рябухин Ю.М. Кольца без нильпотентных элементов и вполне простые идеалы // Доклады АН СССР.–1968.–Т. 180, № 1.–С. 9-11.

[37] Бокуть Л.А. Вложение в простые ассоциативные алгебры // Алгебра и логика.–1978.–Т. 15, № 2.–С. 117-142.

[38] Бейдар К.И., Михалёв А.В. Обобщённые полиномиальные тождества и кольца, являющиеся суммами двух подколец // Алгебра и логика.–1995.–Т. 34, №1.–1995.–С. 3-11.

[39] Генов Г.К. Базис тождеств алгебры матриц третьего порядка над конечным полем // Алгебра и логика.–1981.–Т. 20, № 4.–С. 365-388.

[40] Генов Г.К., Сидоров П.Н. Базис тождеств алгебры матриц четвертого порядка над конечным полем // Сердика Българского матем. описание.–1982.–Т. 8.–С. 313-323.

[41] Голод Е.С. О ниль-алгебрах и финитно-аппроксимируемых p-группах // Изв. АН СССР, сер. матем.–1964.–№ 28.–С. 261-272.

[42] Зельманов Е.И. Радикальные расширения PI-алгебр // Сиб. матем. ж.–1978.–Т. 19.–С. 1392-1394.

[43] Кузьмин Е.И. О теореме Нагата-Хигмана // Математические структуры. Вычисл. матем. Математ. моделирование: труды, посвящённые акад. Л. Илиеву.–София, 1975.–С. 101-107.

[44] Кузьмин Е.Н., Мальцев Ю.Н. Базис тождеств алгебры матриц второго порядка под конечным полем // Алгебра и логика.–1978.–Т. 17, № 1.–С. 28-32.

[45] Курош А.Г. Проблемы теории колец, связанные с проблемой Бернсайда о периодических группах // Изв. АН СССР, сер. матем.–1941.–№ 5.–С. 233-240.

[46] Львов И.В. Теорема Брауна о радикале конечно порождённой PI-алгебры. Препринт № 63, СОАН СССР, Институт Матем.–Новосибирск, 1984.–52 с.

[47] Мальцев Ю.Н., Чибриков Е.С. Коммутативность Ф-операторных алгебр, удовлетворяющих тождеству или одной переменной // Известия АлтГУ.–1999.–Т. 1.–С. 7-8.

[48] Мальцев Ю.Н. О тождествах нильпотентных алгебр // Известия вузов. Математика.–1986.–Т. 9.–С. 68-72.

[49] Мальцев Ю.Н. Базис тождеств алгебры верхних треугольных матриц // Алгебра и логика.–1971.–Т. 10, № 4.–С. 393-401.

[50] Мальцев Ю.Н. H – расширение колец с тождественными соотношениями // Алгебра и логика.–1971.–Т. 10, № 5.–С. 495-502.

[51] Мальцев Ю.Н. Почти коммутативное многообразие колец.// Сиб. матем. журнал.–1976.–Т. 17, № 5.–С. 1086-1096.

[52] Мальцев Ю.Н. Об одном методе доказательства теорем коммутативности для колец // Изв. вузов. Математика.–1985.–Т. 11.–С. 26-28.

[53] Мальцев Ю.Н. О тождествах ассоциативных колец с некоторыми комбинаторными условиями на бесконечные множества // Известия АлтГУ.–2006.–Т. 1.–С. 36-38.

[54] Мальцев Ю.Н. О полугрупповых тождествах ассоциативных колец с некоторыми комбинаторными условиями на бесконечном подмножестве // Вестник АлтГПА.–2010.–Т. 2.–С. 46-49.

[55] Михалев А.В., Голубчик Н.З. A note on varieties of semiprime rings with semigroup identities // J. of Algebra.–1978.–V. 54.–P. 42-45.

[56] Олексенко А.Н. Базис тождеств алгебры матриц второго порядка над $\mathbb{Z}_{p^2}$ // Фундам. и приклад. матем.–2000.–Т. 6, № 2.–С. 1-31.

[57] Рябухин Ю.М. О проблеме существования простого нилькольца // Сибирский математический журнал.–1969.–Т. 10.–С. 950-956.

[58] Размыслов Ю.Л. Тождества со следом полной матричной алгебры над полем характеристики нуль // Известие Акад. наук СССР.–1974.–Т. 38.–С. 723-756.

[59] Размыслов Ю.П. О проблеме Капланского // Изв. АН СССР.–1937.–Т. 37.

[60] Чибриков Е.С. О высоте Ширшова конечнопорожденной ассоциативной алгебры, удовлетворяющей тождеству степени четыре // Известия АлтГУ.–2001.–№ 1.–С. 52-56.

[61] Ширшов А.И. О кольцах с тождественными соотношениями // Матем. сборник.–1957.–Т. 43, № 2.–С. 277-283.

[62] Armendariz E. On semiprime rings of bounded index // Proc. Amer. Math. Soc.–1982.–V. 85, № 2.–P. 146-148.

[63] Amitsur S.A. A generalization of Hilbert's Nullstellenstz // Proc. Amer. Math. foc.–1957.–V. 8.–P. 649-656.

[64] Amitsur S.A., Procesi C. Jacobson-rings and Hilbert algebras with polynomial identities // Annali di Mathematica Pura et Applicata.–1966.–V. 71.–P. 61-72.

[65] Ashraf M., Quadri M., Zelinsky D. Some polynomial identities that imply commutativity for rings // American Nathem Monthly.–1988.–V. 95.–P. 336-339.

[66] Abdollahi A., Bell H., Klein A. On commutativity and centrlity in infinite rings// Communications in algebra.–2007.–V. 35.–P. 1323-1332.

[67] Bergman G. A ring primitive on the right but not on the left // Proc. Amer. Math. Soc.–1964.–V. 15.–P. 473-475.

[68] Burnside W. On criteria for the finiteness of the order of linear substitutions // Proc. London Math. Soc.–1905.–V. 3.–P. 435–440.

[69] Braun A. The nilpotency of the radical in a finitely generated PI-ring // Journal of Algebra.–1987.–V. 89.–P. 375-396.

[70] Bell H., Klein A. A commutativity and finitness condition for rings // Archiv der Mathem.–2003.–V. 80.–P. 354-357.

[71] Cohn P.M., Sasiada E. An example of a simple radical ring // Journal of Algebra.–1967.–V. 5.–P. 373-377.

[72] Dubnov J., Ivanov V. Swz l'abaissement du degre des polynomes en affineurs // C.R. (Doklady) Acad. Sci. URSS.–1943.–V. 41.–P. 95-98.

[73] Evyatar A., Scott D. On polynomial in a polynomial // Bull. London Math. Sog.–1972.–V. 4.–P. 176-178.

[74] Formanek E. The polinomial identities and invariants of $n \times n$ matrices // Amer. Math. Soc.–1991.–№ 78.

[75] Formanek E. Central polynomials for matrix rings // J. Algebra.–1972.–V6. 23.

[76] Faith C., Utumi Y. On noetherian prime rings // Trans. Amer. Math. Soc.–1965.–V. 114.–P. 53-60.

[77] Goldie A.W. The structure of prime rings under ascending chain condition // Proc. London Math. Soc.–1958.–V. 8.–P. 589-608.

[78] Goldie A.W. Semi-prime rings with maximum condition // Proc. London Math. Soc.–1960.–V. 10.–P. 201-220.

[79] Goldie A.W. Non-commutative principal ideals rings // Archiv. Math.–1962.–V. 13.–P. 213-221.

[80] Gupta C.K., Krasilnikov A.N. A simple example of a non-finitely based system of polynomial identities // Comm. Algebra.–2002.–V. 30.–P. 4851-4866.

[81] Gilmer R. The ideal of polynomials vanishing on a commutative ring // Proc. Amer. Math. foc.–1999.–V. 127, № 5.–P. 1265-1267.

[82] Gordon B., Motskin T.S. On the zero of polynomials over division ring // Transactions Amer. Math. Soc.–1965.–V. 116, № 4.

[83] Higman G. On a conjecture of Nagata // Proc. Cambridge Philosophical Society.–1956.–V. 52.–P. 1-4.

[84] Herstein I. The structure of a certain class of rings // Amer.J. of Mathem.–1953.–V. 75.–P. 864-871.

[85] Klein A. Rings of bounded index // Comm. Alg.–1984.–V. 12.–P. 9-21.

[86] Klein A. The sum of nil one-sided ideals of bounded index of a ring // Israel Journal of Math.–1994.–V. 88.–P. 25-30.

[87] Klein A. On Fermats theorem for matrices and periodic identities of $M_n(GF(q))$ // Arch. Math.–1990.–V. 34.–P. 399-402.

[88] Krempa J. Fore examples of reduced rings // Algebra Collog.–1996.–3:4.–P. 289-30.

[89] Krempa J. Logical connections between some open problems concerning nil rings // Fundamenta Mathematical.–1972.–V. 76.–P. 121-130.

[90] Kegel O.H. Zur Nilpotenz gewisser assoziativer Ringe // Math. Ann.–1962/63.–V. 193.–P. 258-260.

[91] Komatsu H., Nishinaka T., Tominaga H. On commutativeity of rings // Radovi Matematicki.–1990.–V. 6.–P. 303-311.

[92] Komatsu H., Tominaga H. Commutativity theorems for algebras and rings // Math. J. Okayama Univ.–1991.–V. 33.–P. 71-93.

[93] L'vov I.V. The existence of a simple nil ring. Препринт.–Новосибирск: Институт математики СО РАН, 2003.–№180.

[94] Levitsky Y. On a problem of A. Kurosch // Bull. Amer. Math. Soc.–1946.–V. 52.–P. 1033-1035.

[95] Lanski Ch. The cardinality of the center of ring // Canad. Math. Bull.–1998.–V. 41.–P. 81-85.

[96] Leron Y., Vapne A. Polynomial identities of related rings // Israel J. Math.–1970.–V. 8, № 2.–P. 127-136.

[97] Lin B. H – extension of rings // Journal of Australian Math. Soc.–1969.–V. 10, №1.–P. 236-241.

[98] Laffey T. Commutative subrings of periodic rings // Mathem. Scand.–1976.–V. 39.–P. 161-166.

[99] Laffey T. Commutative subalgebras of infinite dimensional algebras // Bull. London Math. Soc.–1973.–V. 5.–P. 312-314.

[100] Laffey T., Machale D. Polynomials that force a ring to be commutative // Proc. R. Ir. Acad.–1992.–V. 92A.–P. 277-280.

[101] Luh J., Putcha M. // Pacific J. Math.–1977.–V. 68.

[102] Laffey T. Infinite rings with all proper subrings Finite // Amer. Math. Monthly.–1974.–V. 81.–P. 370-373.

[103] Laffey T.J. On commutative subrings of infinite rings // Bull. London Math. Soc.–1972.–V. 4.–P. 3-5.

[104] Mann A. Shimshon Abraham Amitsur (1923-1994) // Israel J. Mathem.–1996.–V. 96.–P. 9-22.

[105] Nagata M. On the nilpotency of nil-algebras // J. Math. Soc. Japan.–1953.–V. 4.–P. 296-301.

[106] Niven I. Fermat‘s theorem for matrices // Duke Math. J.–1948.–V. 15.–P. 823-826.

[107] Pham Ngoc Ahn. On Litoff‘s theorem // Studio Scientlarum Mathenaticorum Hungarica.–1980.–V. 16.–P. 255-259.

[108] Pinter-Lucke J. Commutativity conditions for rings: 1950-2005 // Expositions Mathem.–2007.–V. 25.–P. 165-174.

[109] Quandri M., Ashraf M., Ali A. On a commutativity theorem of Herstein // Radori Matem.–1989.–V. 5.–P. 207-2011.

[110] Robson J. Recognition of matrix rings // Communications in algebra.–1991.–V. 19.–P. 2113-2124.

[111] Ragharendran R. Finite associative rings // Compos. Math.–1969.–V. 21, №2.–P. 195-220.

[112] Smoktunovich A. A simple nil ring exists // Comm. Algebra.–2002.–V. 30.–P. 27-59.

[113] Smoktunovich A. Polinomial rings over nil rings need not be nil // J. Algebra.–2000.–V. 233(2).–P. 427-436.

[114] Small L. Orders in Artinian rings // J. of Algebra.–1966.–V. 4.–P. 13-41.

[115] Small L. Orders in Artinian rings. Corrections and addendum // J. of Algebra.–1996.–V. 4.–P. 505-507.

[116] Small L. An example in PI-rings // Journal of Algebra.–1971.–V. 17.–P. 434-436.

[117] Specht W. Gesetze in Ringen // I. Math. Z.–1950.–V. 52.–P. 219-228.

[118] Streb W. Zur Structur nicht kommutativer ringe // Math. J. Okayama Vniv.–1989.–№ 31.–P. 135-140.

[119] Zelmanov E.I. Nil rings and periodic groups // Korean Mathem. Society.–1992.–P. 72.

[120] Walker G. Fermat's theorem for algebras // Pacific J. Math.–1954.–V. 4.–P. 317-320.

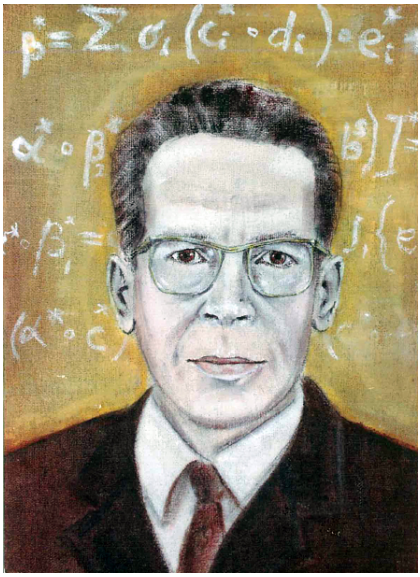
[121] Wamsley J. On a condition commutativity of rings // Journal of London Math. Soc.–1971.–V. 2, № 4.–P. 331-332.

Создатель бриллиантовой леммы

Алтайский край заслуженно гордится своими знаменитыми земляками – космонавтом Германом Титовым, писателем Василием Шукшиным, артистом Валерием Золотухиным, изобретателем Михаилом Калашниковым. Уверены, в плеяде этих замечательных людей место и математику с мировым именем Анатолию Ширшову, научными достижениями которого может гордиться отечественная наука.

Анатолий Илларионович Ширшов родился 8 августа 1921 года в селе Колывань Новосибирской области. Перед войной он начал заочно учиться в Томском университете, одновременно работая в алейской школе учителем. Сначала он преподавал математику, а потом и физику, химию, черчение, физкультуру. В 1942 году, будучи близоруким, он все же ушел на фронт добровольцем.

После демобилизации в 1946-м продолжил обучение в Ворошиловградском пединституте. В 1950 году Анатолий Ширшов поступил в аспирантуру механико-математического факультета МГУ. После успешной защиты в 1953 году кандидатской диссертации на тему "Некоторые вопросы теории неассоциативных колец и алгебр"работал на кафедре высшей алгебры МГУ. Именно на эти годы приходится расцвет его научного творчества, он закладывает основы теории колец, близких к ассоциативным – нового направления в современной алгебре.



А уже в 1958 году математик защищает докторскую диссертацию на тему "О некоторых классах колец, близких к ассоциативным". Спустя три года ему присвоено научное звание профессора, а в 1964 году Анатолий Ширшов избран членом- корреспондентом Академии наук СССР.

С 1960 года его жизнь снова связана с Сибирью: по приглашению академиков С.Соболева, И.Векуа и А.Мальцева Анатолий Ширшов становится одним из создателей сибирской школы алгебры и логики и принимает активное участие в организации Сибирского отделения АН СССР. До 1973 года он являлся заместителем директора Института математики СО АН СССР, а с 1967 года и до последних дней жизни заведовал отделом теории колец Института математики СО АН СССР. Будучи профессором кафедры алгебры и математической логики Новосибирского государственного университета, вел педагогическую работу. Он становится членом бюро Отделения математики Академии наук, членом национального комитета советских математиков, председателем комиссии по алгебре Академии наук, входит в состав ряда ученых советов и редакционных коллегий "Сибирский математический журнал", "Алгебра и логика", "Квант").

Если говорить о научных интересах Анатолия Ширшова, их круг довольно широк: алгебра, математическая логика, теория чисел, проективная геометрия. К тому времени, как он начал работать в области алгебры (это 1953 год), как таковой теории колец, близких к ассоциативным, попросту не существовало. Теперь же это развитая область алгебры, включающая в ка-

честве составных частей теорию бесконечномерных алгебр Ли, теорию альтернативных алгебр, теорию йордановых алгебр, а также теорию более широких классов алгебр – алгебр Мальцева, бинарно-лиевых алгебр, право-альтернативных алгебр и так далее.

Теория колец, близких к ассоциативным, своим современным развитием во многом обязана работам Анатолия Илларионовича и его воспитанников. В 1978 году в Москве в издательстве "Наука" он совместно с учениками Константином Жевлаковым, Аркадием Слинько и Иваном Шестаковым опубликовал монографию "Кольца, близкие к ассоциативным", которая стала популярным руководством по теории.

Его имя связано с такими знаменитыми результатами и понятиями в современной алгебре, как базисы Гребнера-Ширшова, лемма Ширшова о композиции (так называемая бриллиантовая лемма, имеющая множество следствий; ее истинное значение было понято лишь спустя 40 лет), теорема Ширшова-Витта для свободных алгебр Ли, ассоциативные и лиевы слова Линдона-Ширшова, теорема Ширшова-Кона о специальных йордановых алгебрах, теорема Ширшова о высоте.

Теорема Ширшова о высоте использовалась Ефимом Зельмановым при решении знаменитой проблемы Бернсайда, за что он был в 1994 году удостоен медали имени Филдса Международного математического союза (аналог Нобелевской премии для математиков).

Много внимания и заботы Анатолий Илларионович отдавал воспитанию научной смены - он считал это долгом каждого ученого. Созданная им школа в алгебре была предметом его гордости.

Родина высоко оценила заслуги ученого: он награжден тремя орденами Трудового Красного Знамени и пятью медалями.

28 февраля 1981 г. Анатолий Илларионович Ширшов ушел из жизни. Но остались глубокие идеи, заложенные в его работах. В течение последних 30 лет российские математики и общественность Алейска сделали немало для увековечения памя-

ти о великом ученом. Так, по ходатайству участников Второй всесоюзной школы по многообразиям алгебраических систем (она состоялась в Барнауле в 1981 году) одна из улиц Алейска названа именем А.И.Ширшова. А десять лет спустя, в августе 1991 года, в Барнауле прошла международная конференция по алгебре, посвященная 70-летию Анатолия Илларионовича, в работе которой приняли участие более 500 математиков из 38 стран. В 1995 году в Алейском краеведческом музее открылась экспозиция, посвященная Ширшову. Об ученом издано несколько книг.

Прошедшие 30 лет показали, что идеи и научные результаты русского математика не только по-прежнему актуальны, но еще долго будут использоваться учеными всего мира в научной работе.

Мы, ученики Анатолия Илларионовича Ширшова, благодарны ему за годы увлекательной совместной работы и уверены, что его имя навсегда останется в истории мировой алгебры. Наверняка и сегодня на Алтае немало талантливых школьников и студентов, серьезно интересующихся математикой. Вот бы учредить ежегодный краевой грант имени Анатолия Ширшова для молодых ученых-математиков и стипендии для одаренных студентов-математиков. Это лучший способ увековечить память о выдающемся земляке и одновременно помочь перспективным ученым проявить себя в большой науке.

Леонид Бокуть,
доктор физико-математических наук, профессор Института математики СО РАН;

Ефим Зельманов,
доктор физико-математических наук, профессор Университета Сан-Диего (США),
лауреат медали им. Филдса;

Виктор Латышев,
доктор физико-математических наук, профессор, заведующий кафедрой алгебры МГУ;

Юрий Мальцев,
доктор физико-математических наук, профессор АлтГПА;
Иван Шестаков,
доктор физико-математических наук, профессор университета Сан-Паулу (Бразилия)

По материалам газеты "Алтайская правда", № 43-44, 18 февраля 2011 года.