Том 1, Выпуск 4
Стр. 3–34 (2023)

УДК 15A27, 12F10, 16S50
MSC 512.64, 512.623, 512.55

Теоремы плотности и их приложения

А.Н. Абызов

Аннотация. Данная статья является во многом обзорной, и также она носит методический характер. В статье рассматриваются обобщения теоремы плотности Джекобсона–Шевалле, на основе которых излагается ряд результатов из линейной алгебры, связанных с централизаторами локально алгебраических линейных операторов. Также на основе подхода Джекобсона к построению теории Галуа, основанным на теореме плотности, приводится доказательство теоремы Гильберта 90 и некоторые ее известные обобщения.

Ключевые слова: конечная топология, централизатор, локально алгебраический оператор, расширения Галуа.

Введение

Теорема плотности Джекобсона–Шевалле согласно [1, с. 64] была открыта Клодом Шевалле в 1938 году и впервые была опубликована в работе Натана Джекобсона [2] в 1945 году. Эта теорема и ее различные обобщения играют важное значение во многих разделах алгебры. В своей монографии “Строение колец” [3] Н. Джекобсон на основе теоремы плотности развивает структурную теорию колец и теорию Галуа для тел. Изложение классической теории Галуа на основе теоремы плотности Н. Джекобсон приводит во втором томе своего учебника “Основы алгебры” [4]. В книге Н. Бурбаки “Очерки по истории математики” [5, с. 83] было отмечено, что “... работы Е. Артина [6] сделали очевидным линейный характер теории Галуа...”. Подход Н. Джекобсона к построению теории Галуа на основе теории модулей, благодаря которому переходы от классической теории Галуа к ее различным обобщениям и аналогам выглядят вполне естественными, подтверждает эту мысль о линейном характере теории Галуа.

Работа состоит из четырех частей. В разделе 1 приводятся обобщения теоремы плотности Джекобсона–Шевалле из работ [7, 8] и некоторые следствия из них. На основе этих результатов в разделе 2 доказывается теорема Капланского о центре колец эндоморфизмов периодических модулей над полными кольцами дискретного нормирования. Также доказывается вариант теоремы плотности для периодических модулей над коммутативной областью главных идеалов. Различные приложения этой теоремы к централизаторам

Благодарности. Работа поддержана грантом Российского научного фонда (проект № 22-21-00267) и выполнена в рамках реализации программы развития Научно-образовательного математического центра Приволжского федерального округа (соглашение № 075-02-2023-944).

Поступила: 07.10.2023. Принята: 28.11.2023. Опубликована: 26.12.2023.

локально алгебраических линейных операторов рассмотрены в разделе 3. В заключительном разделе на основе подхода Н. Джекобсона излагаются некоторые результаты из теории полей. В частности, рассмотрен метод доказательства теоремы Гильберта 90 и его обобщений, основанный на классическом результате из линейной алгебры, согласно которому все автоморфизмы и все дифференцирования алгебры матриц над полем являются внутренними.

Пусть M, N – правые R-модули. Через $\mathrm{Hom}_R(M, N)$ обозначается множество всех гомоморфизмов из модуля M в модуль N. Кольцо эндоморфизмов модуля M обозначается $\mathrm{End}_R(M)$. Через $\mathrm{End}(M)$ (соответственно $\mathrm{End}(R)$) будем обозначать кольцо эндоморфизмов аддитивной группы модуля M (соответственно кольца R).

В статье мы используем базовые понятия и стандартные обозначения теории колец и модулей (см., например, [9]).

1. Теоремы плотности

Пусть M – левый R-модуль. Для любого конечного подмножества X модуля M через U_X обозначим множество $\{f \in \mathrm{End}_R(M) \mid f(X) = 0\}$. Тогда конечная топология на $\mathrm{End}_R(M)$ определяется как топология, база которой состоит из всех множеств вида $f + U_X$, где $f \in \mathrm{End}_R(M)$ и X – конечное подмножество M. Конечная топология на $\mathrm{End}_R(M) \subseteq M^M$ совпадает с топологией поточечной сходимости, индуцированной из M^M, где M снабжено дискретной топологией. Если $A \subseteq \mathrm{End}_R(M)$, то замыкание A в конечной топологии будем обозначать $\overline{A}$.

Эндоморфизм α аддитивной группы модуля M назовем скалярным, если существует такой элемент $r \in R$, что $\alpha(m) = rm$ для любого $m \in M$. Множество всех скалярных эндоморфизмов модуля M обозначим $\widetilde{R}$. Ясно, что $\widetilde{R}$ – подкольцо кольца эндоморфизмов аддитивной группы модуля M.

Если S – подкольцо кольца R, то множество $\{r \in R \mid \forall s \in S: \ rs = sr\}$ является подкольцом кольца R и обозначается $C_R(S)$. Кольцо $C_{\mathrm{End}(M)}(\mathrm{End}_R(M)) = \mathrm{End}_{\mathrm{End}_R(M)}(M)$ называется кольцом биэндоморфизмов модуля M и обозначается $\mathrm{Biend}(M)$. Несложно заметить, что $\mathrm{Biend}(M)$ замкнуто в конечной топологии, заданной на $\mathrm{End}(M)$. Для любого непустого подмножества I из матричного представления кольца эндоморфизмов модуля $M^{(I)}$ несложно следует, что гомоморфизм колец $\alpha : \mathrm{Biend}(M) \to \mathrm{Biend}(M^{(I)})$, действующий по правилу $f \mapsto ((x_i)_{i\in I} \mapsto (f(x_i))_{i\in I})$, является изоморфизмом.

Пусть M и N – левые R-модули. Говорят, что модуль M порождает модуль N, если $N = \mathrm{Hom}_R(M, N)M$, т. е. N изоморфен фактор-модулю некоторой прямой суммы изоморфных копий модуля M. Если $\bigcap\limits_{f\in \mathrm{Hom}_R(N,M)} \mathrm{Ker}(f) = 0$, то говорят, что модуль M копорождает модуль N. Ясно, что модуль M копорождает модуль N в точности тогда, когда N изоморфен подмодулю некоторого прямого произведения изоморфных копий модуля M.

Теорема 1. *Пусть M – левый R-модуль. Имеют место следующие утверждения*:

1) *если для каждого $n \in \mathbb{N}$ модуль M порождает всякий подмодуль модуля M^n, то* $\overline{\overline{R}} = \mathrm{Biend}_R(M)$;
2) *если для каждого $n \in \mathbb{N}$ левый R-модуль M копорождает всякий фактор-модуль модуля M^n, то* $\overline{\overline{R}} = \mathrm{Biend}_R(M)$.

Доказательство. Так как $\overline{\mathrm{Biend}_R(M)} = \mathrm{Biend}_R(M)$, то для доказательства п. 1) и 2) достаточно показать, что для каждого $f \in \mathrm{Biend}_R(M)$ и всякого набора элементов $m_1, \ldots, m_k$ из M существует такой элемент $r \in R$, что $r \in f + U_{m_1,\ldots,m_k}$.

Пусть $m_1, \ldots, m_k \in M$, $N = R(m_1, \ldots, m_k)$ – циклический подмодуль R-модуля M^k и $R' = \mathrm{Biend}_R(M)$. Так как M является левым R'-модулем, то M^k имеет естественную структуру левого R'-модуля.

1) Поскольку согласно условию теоремы $\mathrm{Hom}_R(M^k, N)M^k = N$, то

$$\begin{aligned} R'(m_1, \ldots, m_k) &= R'N = R'(\mathrm{Hom}_R(M^k, N)M^k) = \mathrm{Hom}_R(M^k, N)(R'M^k) \\ &= \mathrm{Hom}_R(M^k, N)(M^k) = N = R(m_1, \ldots, m_k). \end{aligned}$$

Таким образом, для произвольного $f \in R'$ существует такой элемент $r \in R$, что $f(m_1, \ldots, m_k) = r(m_1, \ldots, m_k)$. Последнее равносильно выполнимости условия $r \in f + U_{m_1,\ldots,m_k}$.

2) Предположим, что $\alpha(m_1, \ldots, m_k) \notin N$ для некоторого $\alpha \in R'$. Положим $b = \alpha(m_1, \ldots, m_k)$ и $\bar{b} = \alpha(m_1, \ldots, m_k) + N$. Согласно условию теоремы $f(\bar{b}) \neq 0$ для некоторого гомоморфизма $f \in \mathrm{Hom}_R(M^k/N, M)$. Обозначим через $p : M^k \to M^k/N$ канонический гомоморфизм. Тогда

$$f(\bar{b}) = fp(b) = fp(\alpha(m_1, \ldots, m_k)) = \alpha(fp((m_1, \ldots, m_k))) = 0.$$

Получили противоречие с выбором гомоморфизма f. Таким образом, $R'(m_1, \ldots, m_k) = R(m_1, \ldots, m_k)$. □

Замечание 2. Утверждения п. 1) и 2) теоремы 1 приведены соответственно в работах [7] и [8].

Левый R-модуль M называется строго порождающим, если для некоторого левого R-модуля N имеет место изоморфизм $M \cong_R R \oplus N$.

Теорема 3 ([10, теорема 7.1])**.** *Если левый R-модуль M является порождающим, то $\widetilde{R} = \mathrm{Biend}_R(M)$. В частности, кольцо $\widetilde{R}$ является замкнутым в конечной топологии.*

Доказательство. Предположим, что модуль M является строго порождающим. Тогда для некоторого подмодуля M_0 модуля M имеет место разложение $M = eR \oplus M_0$, где $\mathrm{Ann}(e) = 0$. Пусть $\pi : eR \oplus M_0 \to eR$ – естественная проекция. Рассмотрим произвольный биэндоморфизм f модуля M. Тогда $f\pi = \pi f$ и, следовательно, $f(e) = re$ для некоторого $r \in R$. Покажем, что $f \in \widetilde{R}$. Для произвольного элемента m из M существует гомоморфизм $g \in \mathrm{End}_R(M)$, для которого выполнено равенство $g(e) = m$. Тогда $f(m) = fg(e) = gf(e) = g(re) = rg(e) = rm$.

Пусть M – порождающий модуль. Тогда для некоторого $n \in \mathbb{N}$ модуль M^n является строго порождающим. Рассмотрим произвольный биэндоморфизм f модуля M. Через $\overline{f}$ обозначим эндоморфизм аддитивной группы модуля M^n, действующий согласно правилу $(m_1, \ldots, m_n) \to (f(m_1), \ldots, f(m_n))$. Из матричного представления кольца эндоморфизмов модуля M^n непосредственно следует $\overline{f} \in \mathrm{Biend}_R(M^n)$. Тогда согласно изложенному выше для некоторого $r \in R$ равенство $(rm_1, \ldots, rm_n) = (f(m_1), \ldots, f(m_n))$ имеет место для любого набора $m_1, \ldots, m_n$ элементов из M. Таким образом, $f \in \widetilde{R}$. $\square$

Следующие утверждения непосредственно вытекают из предыдущих теорем.

Следствие 4 (теорема плотности Джекобсона–Шевалле)**.** *Если M – полупростой левый R-модуль, то $\widetilde{\widetilde{R}} = \mathrm{Biend}_R(M)$.*

Следствие 5. *Если R – классически полупростое кольцо и M – левый R-модуль, то $\widetilde{R} = \mathrm{Biend}_R(M)$. В частности, кольцо $\widetilde{R}$ является замкнутым в конечной топологии.*

Пусть A – кольцо и $\mathrm{End}(A)$ – кольцо эндоморфизмов аддитивной группы кольца A. Для каждого $a \in A$ через $r(a)$ обозначим эндоморфизм из $\mathrm{End}(A)$, действующий согласно правилу $x \mapsto xa$ для каждого $x \in A$. Положим $A_r = \{r(a) \mid a \in A\}$. Ясно, что A_r – подкольцо кольца $\mathrm{End}(A)$, антиизоморфное кольцу A.

Замкнутое в конечной топологии подкольцо A_0 кольца $\mathrm{End}(A)$ назовем неприводимым, если

a) $A_r \subseteq A_0$;

b) модуль ${}_{A_0}A$ является простым.

Через $\mathcal{R}(A)$ обозначим множество всех неприводимых подколец кольца $\mathrm{End}(A)$. Множество всех подтел кольца A обозначим $\mathcal{F}(A)$.

В дальнейшем мы будем отождествлять элементы из кольца A с эндоморфизмами из $\mathrm{End}(A)$ с помощью вложения $\iota : A \to \mathrm{End}(A)$, действующего по правилу $a \mapsto (x \mapsto ax)$. Таким образом, можно считать, что $A = \mathrm{End}_A(A_A) \subseteq \mathrm{End}(A)$.

Если $F \in \mathcal{F}(A)$, то, очевидно, что $A_r \subseteq C_{\mathrm{End}(A)}(F)$ и согласно [11, лемма 2.2] $C_{\mathrm{End}(A)}(F)$ – замкнутое подкольцо кольца $\mathrm{End}(A)$. Так как каждое векторное пространство как модуль над своим кольцом эндоморфизмов является простым модулем, то ${}_{C_{\mathrm{End}(A)}(F)}A$ – простой модуль и, следовательно, $C_{\mathrm{End}(A)}(F) \in \mathcal{R}(A)$.

Если $A_0 \in \mathcal{R}(A)$, то $A_r \subseteq A_0$, и отсюда $C_{\mathrm{End}(A)}(A_0) \subseteq A = \mathrm{End}_A(A_A)$. Поскольку модуль ${}_{A_0}A$ прост, из леммы Шура имеем $C_{\mathrm{End}(A)}(A_0) = \mathrm{End}_{A_0}({}_{A_0}A)$ – тело. Значит, $C_{\mathrm{End}(A)}(A_0) \in \mathcal{F}(A)$.

Таким образом, имеют место отображения $\Psi : \mathcal{F}(A) \to \mathcal{R}(A)$ и $\Phi : \mathcal{R}(A) \to \mathcal{F}(A)$, действующие соответственно согласно правилам $F \mapsto C_{\mathrm{End}(A)}(F)$ и $A_0 \mapsto C_{\mathrm{End}(A)}(A_0)$ для любых $F \in \mathcal{F}(A)$ и $A_0 \in \mathcal{R}(A)$.

Следствие 6 (соотвествие Джекобсона–Бурбаки для колец)**.** *Пусть A – кольцо. Тогда отображения Ψ и Φ являются взаимно обратными антиизоморфизмами между частично упорядоченными множествами $(\mathcal{R}(A), \subseteq)$ и $(\mathcal{F}(A), \subseteq)$.*

Доказательство. Пусть $F \in \mathcal{F}(A)$. Так как каждый F-модуль является порождающим, то согласно теореме 3 $\Phi\Psi(F) = C_{\mathrm{End}(A)}(C_{\mathrm{End}(A)}(F)) = F$. Если $A_0 \in \mathcal{R}(A)$, то поскольку модуль ${}_{A_0}A$ является простым, из теоремы Джекобсона–Шевалле следует равенство $\Psi\Phi(A_0) = C_{\mathrm{End}(A)}(C_{\mathrm{End}(A)}(A_0)) = \overline{A_0} = A_0$. $\square$

Если A – тело, то, очевидно, $\mathcal{R}(A)$ совпадает с множеством всех таких замкнутых подколец A_0 кольца $\mathrm{End}(A)$, что $A_r \subseteq A_0$. Множество всех подтел T тела A, для которых векторное пространство ${}_TA$ конечномерно, обозначим через $\mathcal{F}_f(A)$. Через $\mathcal{R}_f(A)$ обозначим множество всех таких подколец A_0 кольца $\mathrm{End}(A)$, что $A_r \subseteq A_0$ и векторное пространство ${}_{A_r}A_0$ конечномерно. Ясно, что A_0 – артиново кольцо. Поскольку левый модуль ${}_{A_0}A$ является точным и простым, A_0 – простое артиново кольцо и из следствия 5 вытекает, что A_0 – замкнутое подкольцо кольца $\mathrm{End}(A)$. Таким образом, $\mathcal{R}_f(A) \subseteq \mathcal{R}(A)$.

Следствие 7 (соотвествие Джекобсона–Бурбаки для тел)**.** *Пусть A – тело. Тогда отображения Ψ и Φ являются взаимно обратными антиизоморфизмами между частично упорядоченными множествами $(\mathcal{R}(A), \subseteq)$ и $(\mathcal{F}(A), \subseteq)$. Причем $\Psi(\mathcal{F}_f(A)) = \mathcal{R}_f(A)$ и отображение Ψ индуцирует антиизоморфизм между частично упорядоченными множествами $(\mathcal{F}_f(A), \subseteq)$ и $(\mathcal{R}_f(A), \subseteq)$. При этом если $T \in \mathcal{F}_f(A)$ и $\dim({}_TA) = n$, то $\dim({}_{A_r}\Psi(T)) = n$.*

Доказательство. Пусть $T \in \mathcal{F}(A)$ и $e_1, \dots, e_n$ – независимая система элементов из векторного пространства ${}_TA$ и $\varphi_1, \dots, \varphi_n$ – семейство эндоморфизмов из $\mathrm{End}_T({}_TA)$, удовлетворяющие для каждых $1 \le i, j \le n$ условиям $\varphi_i(e_i) = 1$ и $\varphi_i(e_j) = 0$, если $i \ne j$. Покажем, что $\varphi_1, \dots, \varphi_n$ – независимое семейство векторного пространства ${}_{A_r}\Psi(T)$. Действительно, если

$$\sum_{k=1}^{n} r(a_k)\varphi_k = 0, \text{ где } a_1, \dots, a_n \in A,$$

то для каждого $1 \le i \le n$ имеем

$$0 = \left(\sum_{k=1}^{n} r(a_k)\varphi_k\right)(e_i) = r(a_i)\varphi_i(e_i) = a_i.$$

Таким образом, если $\Psi(T) \in \mathcal{R}_f(A)$, то $T \in \mathcal{F}_f(A)$. Если $T \in \mathcal{F}_f(A)$ и $e_1, \dots, e_n$ – базис векторного пространства ${}_TA$, то для любого эндоморфизма $\varphi \in \mathrm{End}_T({}_TA)$ и для каждого $1 \le i \le n$ имеет место равенство

$$\left(\sum_{k=1}^{n} r(\varphi(e_k))\varphi_k\right)(e_i) = \varphi(e_i).$$

Следовательно, $\varphi_1, \dots, \varphi_n$ – базис векторного пространства ${}_{A_r}\Psi(T)$. Таким образом, $\Psi(\mathcal{F}_f(A)) = \mathcal{R}_f(A)$ и $\dim({}_TA) = \dim({}_{A_r}\Psi(T))$. $\square$

Замечание 8. Предыдущее утверждение впервые встречается в статье Н. Джекобсона [12], опубликованной в 1947 году, и согласно работе [13] Эли Картана, вышедшей в том же году, приведено в §5, гл. 2 книги Н. Бурбаки "Алгебра", на тот момент еще неопубликованной.

2. Теорема Капланского

Пусть R – коммутативная область главных идеалов. Через $P(R)$ будем обозначать множество всех попарно неассоциированных простых элементов кольца R. Пусть P – непустое подмножество $P(R)$. P-адической топологией на R будем называть линейную топологию, у которой базу окрестностей нуля образуют идеалы вида aR, где a – элемент из R, являющийся произведением неотрицательных степеней простых элементов из P. Если $P = P(R)$, то P-адическая топология на R называется полиадической. Согласно [14, теорема 8.1] кольцо R, снабженное P-адической топологией, вкладывается как плотное подкольцо в полное хаусдорфово кольцо, которое определено однозначно с точностью до топологического изоморфизма. Это кольцо будем обозначать через $\widehat{R}_P$. Если $p \in P(R)$, то через $\widehat{R}_p$ будем обозначать пополнение кольца R относительно p-адического нормирования.

Хорошо известно, что всякий p-примарный R-модуль M имеет естественную структуру $\widehat{R}_p$-модуля. Умножение произвольного элемента $m \in M$, для которого выполнено равенство $mp^n = 0$, на элемент $\widehat{r} \in \widehat{R}_p$ определяется согласно правилу: $m\widehat{r} = mr$, где r – элемент из R, удовлетворяющий условию $r \equiv \widehat{r} \bmod (p^n)$.

Лемма 9. *Пусть R – коммутативная область главных идеалов, M – ненулевой периодический R-модуль. Тогда следующие условия эквивалентны*:

1) *конечная топология на $Z(\mathrm{End}_R(M))$ является дискретной*;

2) *M – ограниченный модуль.*

Доказательство. 1) $\Rightarrow$ 2). Из условия п. 1) следует, что для некоторого конечного семейства элементов $m_1, \ldots, m_k \in M$ выполнено равенство $\{f \in Z(\mathrm{End}_R(M)) \mid f(m_1) = \ldots = f(m_k) = 0\} = 0$. Пусть $\mathrm{Ann}(m_i) = r_iR$ для каждого $i = 1, \ldots, k$ и q – наименьшее общее кратное элементов $r_1, \ldots, r_k$. Рассмотрим гомоморфизм $\tilde{q} \in \tilde{R} \subseteq Z(\mathrm{End}_R(M))$, действующий согласно правилу: $m \mapsto qm$. Так как $\tilde{q} \in \{f \in Z(\mathrm{End}_R(M)) \mid f(m_1) = \ldots = f(m_k) = 0\} = 0$, то $qM = 0$.

2) $\Rightarrow$ 1). Существует элемент $q \in R$ такой, что $qM = 0$ и $q'M \neq 0$ для каждого делителя q' элемента q, неассоциированного с q. Так как каждая примарная компонента модуля M является прямой суммой циклических модулей и модуль M является конечной прямой суммой своих ненулевых примарных компонент, то существует такой элемент $m \in M$, что $\mathrm{Ann}(m) = qR$ и mR – прямое слагаемое модуля M. Несложно заметить, что для каждого $n \in M$ существует гомоморфизм $g \in \mathrm{End}(M)$, для которого выполнено равенство $g(m) = n$.

Пусть $f \in Z(\mathrm{End}_R(M))$, для которого выполнено равенство $f(m) = 0$, и n – произвольный элемент из модуля M. Для некоторого гомоморфизма $g \in \mathrm{End}(M)$ имеем

$g(m) = n$. Тогда $f(n) = f(g(m)) = g(f(m)) = 0$. Таким образом, открытое множество $\{f \in Z(\mathrm{End}_R(M)) \mid f(m) = 0\}$ содержит только нулевой гомоморфизм. $\square$

Используя рассуждения из предыдущей леммы, аналогично можно показать, что если M – периодический модуль над кольцом дискретного нормирования R, то конечная топология на $\mathrm{End}_R(M)$ является дискретной в точности тогда, когда M – конечно порожденный модуль.

Теорема 10. *Пусть R – область дискретного нормирования, M – примарный R-модуль. Тогда $\overline{\widetilde{R}} = Z(\mathrm{End}_R(M))$, т. е. для любого $f \in Z(\mathrm{End}_R(M))$ и любого конечного множества $x_1, \ldots, x_k \in M$ существует элемент $r \in R$ такой, что $rx_i = f(x_i)$ для $i = 1, \ldots, k$.*

Доказательство. Пусть M – периодический модуль над кольцом дискретного нормирования R. Если M является редуцированным модулем, то из [9, следствие 2.3.1] и [9, следствие 2.5.3] вытекает, что каждый циклический подмодуль модуля M^n ($n \in \mathbb{N}$) изоморфен фактор-модулю некоторого циклического прямого слагаемого модуля M. Таким образом, M порождает каждый подмодуль модуля M^n. Если M не является редуцированным модулем, то M обладает прямым слагаемым, изоморфным квазициклическому модулю $R(p^\infty)$. Хорошо известно, что модуль $R(p^\infty)$ является копорждающим объектом в категории R-модулей. Таким образом, из теорем 1 и 3 следует, что для всякого примарного модуля M над кольцом дискретного нормирования R замыкание кольца $\tilde{R}$ в конечной топологии, заданной на $\mathrm{End}_R(M)$, совпадает с $\mathrm{Biend}_R(M) = Z(\mathrm{End}_R(M))$. $\square$

Если R – область дискретного нормирования и M – примарный R-модуль, который не является ограниченным, то не сложно заметить, что ограничение конечной топологии на R совпадает с p-адической топологией на R, где p – простой элемент R. Тогда из леммы 9 и предыдущей теоремы получаем следующее утверждение.

Теорема 11 (И. Капланский, [15])**.** *Пусть M – примарный модуль над полной областью дискретного нормирования R и p – простой элемент R. Тогда $\widetilde{R} = Z(\mathrm{End}_R(M))$, т. е. $Z(\mathrm{End}_R(M)) = R_{p^k}$, если M – ограниченный модуль и p^k – точная верхняя грань порядков его элементов, и $Z(\mathrm{End}_R(M)) = R$ в противном случае.*

Теорема 12. *Пусть R – коммутативная область главных идеалов, M – периодический R-модуль. Тогда $\overline{\widetilde{R}} = Z(\mathrm{End}_R(M))$, т. е. для любого $f \in Z(\mathrm{End}_R(M))$ и любого конечного множества $x_1, \ldots, x_k \in M$ существует $r \in R$ такой, что $rx_i = f(x_i)$ для $i = 1, \ldots, k$.*

Доказательство. Пусть $M = \bigoplus\limits_{p \in P_M} M_p$ – разложение модуля M в прямую сумму его ненулевых примарных компонент, где $P_M \subseteq P(R)$.

Рассмотрим произвольное конечное семейство элементов $x_1, \ldots, x_k$ из модуля M и произвольный элемент f из центра кольца $\mathrm{End}_R(M)$. Так как любой конечный набор элементов из модуля M содержится в прямой сумме конечного числа его примарных компонент, то существует такое конечное семейство $p_1, \dots, p_t$ попарно неассоциированных простых элементов из кольца R, что для каждого $1 \le i \le k$ имеет место равенство

$$x_i = \sum_{j=1}^{t} x_{ij}, \text{ где } x_{ij} \in M_{p_j} \text{ для } 1 \le j \le t.$$

Для каждого $p_0 \in P_M$ через $\varepsilon_{p_0} : M_{p_0} \to M$ и $\pi_{p_0} : \bigoplus_{p \in P_M} M_p \to M_{p_0}$ обозначим естественное вложение и естественную проекцию соответственно. Так как кольцо эндоморфизмов модуля M естественно изоморфно прямому произведению колец эндоморфизмов его примарных компонент и центр прямого произведения колец равен прямому произведению центров, то

$$f(x_i) = f\left(\sum_{j=1}^{t} x_{ij}\right) = \sum_{j=1}^{t} \pi_{p_j} f \varepsilon_{p_j}(x_{ij}), \text{ где } \pi_{p_j} f \varepsilon_{p_j} \in Z(\mathrm{End}_R(M_{p_j})) \text{ для } 1 \le j \le t.$$

Каждую примарную компоненту M_{p_j} можно естественно рассматривать как $\widehat{R}_{p_j}$-модуль. Тогда по теореме 11 для каждого $1 \le j \le t$ существует такой $\widehat{r}_j \in \widehat{R}_{p_j}$, что для любого $x \in M_{p_j}$ выполняется $\pi_{p_j} f \varepsilon_{p_j}(x) = \widehat{r}_j x$.

Для каждого $1 \le j \le t$ выберем натуральное число n_j такое, что равенство $p_j^{n_j} x_{ij} = 0$ выполнено для любого $1 \le i \le k$. Для всякого $1 \le j \le t$ выберем элемент $r_j \in R$, для которого выполнено сравнение $r_j \equiv \widehat{r}_j \mod (p_j^{n_j})$. Тогда для каждого $1 \le j \le k$ имеем $r_j x_{ij} = \widehat{r}_j x_{ij} = f_j(x_{ij})$.

Согласно китайской теореме об остатках существует такой элемент $r_0 \in R$, что $r_0 \equiv r_j \mod (p_j^{n_j})$ для каждого $1 \le j \le t$. Поскольку для каждых $1 \le i \le k$ и $1 \le j \le t$ выполнено равенство $p_j^{n_j} x_{ij} = 0$, то также выполнено и равенство $r_j x_{ij} = r_0 x_{ij}$. Таким образом, для каждого $1 \le i \le k$ имеем

$$f(x_i) = \sum_{j=1}^{t} \pi_{p_j} f \varepsilon_{p_j}(x_{ij}) = \sum_{j=1}^{t} r_j x_{ij} = \sum_{j=1}^{t} r_0 x_{ij} = r_0 x_i. \qquad \square$$

Для произвольной коммутативной области главных идеалов R рассмотрим связи между конечными топологиями на кольцах эндоморфизмов периодических R-модулей и P-адическими топологиями на R. Пусть M – ненулевой периодический R-модуль, у которого каждая ненулевая примарная компонента является неограниченной, и $M = \bigoplus_{p \in P_M} M_p$ – разложение M в прямую сумму ненулевых примарных компонент, где $P_M \subseteq P(R)$.

Так как модуль M является неограниченным, то гомоморфизм $\iota : R \to \widetilde{R}$, $r \mapsto (m \mapsto rm)$ является изоморфизмом. Далее будем отождествлять каждый элемент r из кольца R с соответствующим ему скалярным эндоморфизмом $\iota(r)$ модуля M.

Рассмотрим произвольный конечный набор элементов $m_1, \dots, m_k$ из модуля M. Для произвольного R-модуля конечной длины N через $lg(N)$ будем обозначать длину этого модуля, т. е. длину максимальной цепочки подмодулей модуля N. Пусть $p \in P(R)$ и $m \in M$. Для каждого $p \in P_M$ положим $\alpha_p = \max(lg(\pi_p(m_1)R), \ldots, lg(\pi_p(m_k)R))$, где $\pi_p : \bigoplus_{p \in P_M} M_p \to M_p$ – естественная проекция для каждого $p \in P_M$. Ясно, что условие $\alpha_p > 0$ выполнено для конечного множества элементов из P_M. Пусть $\{p_1, \ldots, p_k\}$ – множество всех попарно различных элементов p из P_M, для которых выполнено неравенство $\alpha_p > 0$. Тогда $U_{m_1,\ldots,m_k} \cap \widetilde{R} = p_1^{\alpha_{p_1}} \ldots p_k^{\alpha_{p_k}} \widetilde{R}$. Так как для каждого $p \in P_M$ модуль M_p является неограниченным, то несложно показать, что для каждого $n \in \tilde{R} \setminus \{0\}$ идеал $n\tilde{R}$ имеет вид $U_{m_1,\ldots,m_k} \cap \tilde{R}$. Таким образом, P_M-адическая топология на $\tilde{R}$ является ограничением конечной топологии на $\tilde{R}$.

Согласно теореме 12 кольцо $Z(\mathrm{End}(M))$ является пополнением кольца относительно P_M-адической топологии, которое согласно [14, теорема 8.1] определено однозначно с точностью до топологического изоморфизма колец. Из приведенных выше рассуждений следует, что $Z(\mathrm{End}(M_p))$ является замыканием кольца $\widetilde{R} \subseteq \mathrm{End}(M_p)$ в конечной топологии для каждого $p \in P_M$. В частности, $Z(\mathrm{End}(M_p))$ является полным кольцом дискретного нормирования изоморфным $\widehat{R}_p$. Так как M_p для каждого $p \in P_M$ является вполне инвариантным подмодулем модуля M, то из определения конечной топологии непосредственно вытекает топологический изоморфизм колец

$$\mathrm{End}_R(M) \cong \prod_{p \in P_M} \mathrm{End}_R(M_p),$$

где топология на прямом произведении $\prod_{p \in P_M} \mathrm{End}_R(M_p)$ является тихоновской. Таким образом, если $P \subseteq P(R)$, то имеет место хорошо известный топологический изоморфизм колец

$$\widehat{R}_P \cong \prod_{p \in P} \widehat{R}_p.$$

В заключение приведем элементарный пример применения P-адических топологий. В [16] с помощью полиадической топологии на кольце целых чисел $\mathbb{Z}$ было получено новое доказательство теоремы Евклида о бесконечности простых чисел. Используя аналогичные рассуждения, можно показать, что если R — коммутативная область главных идеалов, которая не является полем и $|U(R)| < |R|$, то множество $P(R)$ бесконечно. Действительно, рассмотрим на R полиадическую топологию. Так как R является областью целостности, то мощность любого ненулевого идеала R совпадает с $|R|$. Следовательно, мощность любого непустого открытого множества R совпадает с $|R|$. Предположим, что $P(R)$ – конечное множество. Тогда $\bigcup_{p \in P(R)} (p)$ – замкнутое множество. Значит, $R \setminus \bigcup_{p \in P(R)} (p) = U(R)$ является открытым множеством. Получаем противоречие. Полиадические числа, т. е. пополнение кольца $\mathbb{Z}$ относительно полиадической топологии на $\mathbb{Z}$, играют важное значение как в теории абелевых групп, так и в теории чисел (см., например, [17]).

3. Приложения в линейной алгебре

Пусть V – векторное пространство над полем F и $A : V \to V$ – некоторый линейный оператор. Тогда векторное пространство V имеет естественную структуру $F[X]$-модуля, в котором умножение вектора на многочлен определяется согласно правилу:

$$\left(\sum_{i=0}^{n} \alpha_i X^i\right) v := \sum_{i=0}^{n} \alpha_i A^i(v), \quad \text{где } v \in V \ \text{ и } \ \sum_{i=0}^{n} \alpha_i X^i \in F[X]. \tag{1}$$

Линейный оператор $A : V \to V$ называется локально алгебраическим, если для каждого вектора $v \in V$ существует такой ненулевой многочлен $p(x) \in F[x]$, что $p(A)(v) = 0$. Примерами локально алгебраических линейных операторов являются алгебраические линейные операторы, а также триангулизируемые линейные операторы, изученные в работе [18].

В случае, когда A – локально нильпотентный оператор, модуль ${}_{F[X]}V$ является примарным, и его можно рассматривать как модуль над кольцом формальных степенных рядов $F[[X]]$, т. е. над X-адическим пополнением $F[X]$, при этом модульное умножение определяется следующим образом:

$$\left(\sum_{i=0}^{\infty} \alpha_i X^i\right) v := \sum_{i=0}^{\infty} \alpha_i A^i(v), \quad \text{где } v \in V \ \text{ и } \ \sum_{i=0}^{\infty} \alpha_i X^i \in F[[X]].$$

Если линейный оператор $A : V \to V$ является локально алгебраическим, то модуль ${}_{F[X]}V$ является периодическим, и имеет место примарное разложение

$${}_{F[X]}V = \bigoplus_{g \in P(F[X])} V_g, \quad \text{где } V_g = \{v \in V |\ g^n v = 0 \text{ для некоторого } n \in \mathbb{N}\}.$$

Если g – неразложимый многочлен, то g-адическое пополнение $F[[X]]_g$ кольца $F[X]$ состоит из всех рядов вида $\sum\limits_{i=0}^{\infty} f_i g^i$, где $f_i \in F[X]$ и $\deg(f_i) < \deg(g)$ для каждого неотрицательного целого числа i, которые, очевидно, сходятся в g-адической топологии. Каждую g-компоненту V_g можно рассматривать как примарный $F[[X]]_g$-модуль.

Если A – линейный оператор, действующий на векторном пространстве V, то его централизатор $\{X \in \mathrm{End}(V) \mid XA = AX\}$ обозначается $C(A)$. Двойной централизатор $\{X \in \mathrm{End}(V) \mid \ \forall\, Y \in C(A) : XY = YX\}$ линейного оператора A обозначается $CC(A)$.

Лемма 13. *Пусть V – векторное пространство над полем F и $A : V \to V$ – линейный оператор. Тогда*

1) $C(\overline{F[A]}) = C(A)$;
2) $\overline{F[A]}$ *– коммутативная подалгебра алгебры* $\mathrm{End}(V)$, *и* $\overline{F[A]} \subseteq CC(A)$.

Доказательство. 1) Достаточно показать, что имеет место включение $C(A) \subseteq C(\overline{F[A]})$. Пусть $A' \in C(A)$ и $B \in \overline{F[A]}$. Рассмотрим произвольный вектор $v \in V$. Тогда существует такой линейный оператор $A_0 \in F[A]$, что $A_0(v) = B(v), A_0(A'(v)) = B(A'(v))$. Отсюда $(A'B - BA')(v) = A'A_0(v) - A_0A'(v) = 0$. Таким образом, $A' \in C(\overline{F[A]})$.

2) Так как согласно [18, лемма 26] подалгебра $CC(A)$ замкнута в конечной топологии, и $F[A] \subseteq CC(A)$, то $\overline{F[A]} \subseteq CC(A)$. Коммутативность подалгебры $\overline{F[A]}$ следует из того, что $CC(A) = Z(\mathrm{End}_{F[X]}(V))$. $\square$

Непосредственным следствием теоремы 12 является

Теорема 14. *Пусть V – векторное пространство над полем F и $A : V \to V$ – локально алгебраический линейный оператор. Тогда $\overline{F[A]} = CC(A)$, т. е. для любого линейного оператора $B \in CC(A)$ и любого конечного множества векторов $v_1, \dots, v_k \in V$ существует линейный оператор $A' \in F[A]$ такой, что $A'(v_i) = B(v_i)$ для $i = 1, \dots, k$.*

Замечание 15. Утверждение теоремы 14 приведено в книге И. Капланского [15, с. 72] в качестве упражнения, также оно приведено в качестве открытой проблемы в [18, вопрос 32].

Теорема 16. *Пусть V – векторное пространство над полем F. Локально алгебраический линейный оператор $A : V \to V$ является алгебраическим в точности тогда, когда $CC(A) = F[A]$.*

Доказательство. Если A – алгебраический линейный оператор, то из леммы 9 и теоремы 12 вытекает равенство $CC(A) = F[A]$.

Предположим, что имеет место равенство $CC(A) = F[A]$. Согласно (1) векторное пространство V имеет естественную структуру $F[X]$-модуля. Пусть $V = \bigoplus_{g \in P_0} V_g$, где $P_0 \subseteq P(F[X])$ и V_g – ненулевая g-примарная компонента $F[X]$-модуля V для каждого $g \in P_0$. Тогда

$$F[A] = CC(A) = Z(\mathrm{End}_{F[X]}(V)) = \prod_{g \in P_0} Z(\mathrm{End}_{F[X]}(V_g)),$$

и согласно теореме 12 для каждого $g \in P_0$ кольцо $Z(\mathrm{End}_{F[X]}(V_g))$ изоморфно либо $F[[X]]_g$, либо $F[X]/(g^{n_g})$ $(n_g \in \mathbb{N})$. Предположим, что $F[A] \cong F[X]$. Случай $|P_0| > 1$ невозможен, так как кольцо $F[X]$ неразложимо. Случай $|P_0| = 1$, очевидно, также невозможен. Таким образом, $F[A] \ncong F[X]$ и, следовательно, для некоторого многочлена $f \in F[X]$, степень которого ≥ 1, имеет место изоморфизм $F[A] \cong F[X]/(f)$. $\square$

Следствие 17. *Пусть V – векторное пространство над полем F и $A, B \in \mathrm{End}(V)$ – локально алгебраические линейные операторы. Тогда*

1) *включение $\overline{F[B]} \subseteq \overline{F[A]}$ имеет место в точности тогда, когда $C(A) \subseteq C(B)$;*
2) *равенство $\overline{F[A]} = \overline{F[B]}$ имеет место в точности тогда, когда $C(A) = C(B)$.*

Доказательство. Если $\overline{F[B]} \subseteq \overline{F[A]}$, то согласно теореме 14 имеем $CC(B) \subseteq CC(A)$ и, значит, $C(A) = CCC(A) \subseteq CCC(B) = C(B)$.

Обратно, если $C(A) \subseteq C(B)$, то $CC(B) \subseteq CC(A)$. Таким образом, по теореме 14 имеем $\overline{F[B]} \subseteq \overline{F[A]}$. $\square$

Следствие 18. *Пусть V – векторное пространство над полем F и $A, B \in \operatorname{End}(V)$ – алгебраические линейные операторы. Тогда*

1) *включение $F[B] \subseteq F[A]$ имеет место в точности тогда, когда $C(A) \subseteq C(B)$;*
2) *равенство $F[A] = F[B]$ имеет место в точности тогда, когда $C(A) = C(B)$.*

Пусть $\mathbb{L}$ – множество всех локально алгебраических линейных операторов, действующих на векторном пространстве V, $\mathbb{A} = \{\overline{F[A]} \mid A \in \mathbb{L}\}$ и $\mathbb{B} = \{C(A) \mid A \in \mathbb{L}\}$. Через $\mathbb{L}_f$ обозначим множество всех алгебраических линейных операторов, действующих на векторном пространстве V. Также положим $\mathbb{A}_f = \{F[A] \mid A \in \mathbb{L}_f\}$ и $\mathbb{B}_f = \{C(A) \mid A \in \mathbb{L}_f\}$. Учитывая введенные выше обозначения, имеет место

Теорема 19.

1) *Отображение $\Psi : \mathbb{A} \to \mathbb{B}$, действующее согласно правилу $\overline{F[A]} \mapsto C(A)$, является антиизоморфизмом частично упорядоченных множеств $(\mathbb{A}, \subseteq)$ и $(\mathbb{B}, \subseteq)$.*
2) *Отображение $\Psi' : \mathbb{A}_f \to \mathbb{B}_f$, действующее согласно правилу $F[A] \mapsto C(A)$, является антиизоморфизмом частично упорядоченных множеств $(\mathbb{A}_f, \subseteq)$ и $(\mathbb{B}_f, \subseteq)$.*

Доказательство. Утверждение непосредственно вытекает из леммы 13, теоремы 14, следствий 17 и 18. □

Выясним, при каких условиях для локально алгебраического линейного оператора $A \in \operatorname{End}_F(V)$ выполнено равенство $\overline{F[A]} = C(A)$. Для этого нам потребуются следующие утверждения.

Лемма 20. *Пусть R – коммутативная область главных идеалов, M – p-примарный модуль, который не является неразложимым. Тогда M содержит прямое слагаемое вида $A_1 \oplus A_2$, где A_i – либо ненулевой циклический, либо квазициклический модуль для $i = 1, 2$.*

Доказательство. Всякий неразложимый периодический модуль над кольцом R является либо циклическим, либо квазициклическим ([9, следствие 2.3.4]). Если M содержит квазициклический подмодуль, то он выделяется прямым слагаемым. Всякий ненулевой редуцированный примарный модуль содержит ненулевое циклическое прямое слагаемое ([9, следствие 2.3.4]). Из указанных фактов вытекает утверждение леммы. □

Лемма 21. *Пусть R – коммутативная область главных идеалов и M – p-примарный R-модуль. Тогда равносильны следующие условия*:

1) *кольцо $\operatorname{End}_R(M)$ коммутативно*;
2) *модуль M является либо циклическим, либо квазициклическим*;
3) *M является модулем Безу.*

Доказательство. 1) $\Rightarrow$ 2). Пусть кольцо $\operatorname{End}_R(M)$ коммутативно. Согласно лемме 20 произвольный разложимый примарный R-модуль N содержит прямое слагаемое вида $A \oplus B$, где каждый из модулей A и B является либо ненулевым циклическим, либо квазициклическим. Так как либо $\mathrm{Hom}(A, B) \neq 0$, либо $\mathrm{Hom}(B, A) \neq 0$, то кольцо $\mathrm{End}(N)$ некоммутативно. Таким образом, M – неразложимый модуль и, значит, согласно [9, следствие 2.3.4] модуль M является циклическим либо квазициклическим.

2) $\Rightarrow$ 1) следует из хорошо известных изоморфизмов $\mathrm{End}_R(R_{p^n}) \cong R_{p^n}$ $(n \in \mathbb{N})$ и $\mathrm{End}_R(R_{p^\infty}) \cong \widehat{R}_p$.

2) $\Rightarrow$ 3). Всякий циклический R-модуль, очевидно, является модулем Безу. Квазициклический R-модуль является цепным модулем и, значит, модулем Безу.

3) $\Rightarrow$ 2). Пусть M – модуль Безу. Если M – разложимый модуль, то согласно лемме 20 модуль M содержит прямое слагаемое вида $A \oplus B$, где каждый из модулей A и B является либо ненулевым циклическим, либо квазициклическим, что невозможно. Таким образом, согласно [9, следствие 2.3.4] модуль M является либо циклическим, либо квазициклическим. □

Лемма 22. *Пусть R – коммутативная область главных идеалов, M – периодический R-модуль. Тогда эквивалентны следующие условия:*

1) *кольцо эндоморфизмов модуля M коммутативно;*
2) *$M = \bigoplus\limits_{p \in P_M} M_p$, где $P_M \subseteq P(R)$ и M_p – p-примарная компонента M для каждого $p \in P_M$, которая является либо циклической, либо квазициклической;*
3) *M является модулем Безу.*

Доказательство. Импликация 1) $\Rightarrow$ 2) следует из леммы 21. Импликация 3) $\Rightarrow$ 2) следует из леммы 21 и из того очевидного факта, что подмодуль модуля Безу является модулем Безу.

Импликация 2) $\Rightarrow$ 1) следует из изоморфизма

$$\mathrm{End}_R(M) \cong \prod_{p \in P_M} \mathrm{End}_R(M_p), \text{ где } \mathrm{End}_R(M_p) \cong \begin{cases} \widehat{R}_p, & \text{если } M_p \cong R_{p^\infty}; \\ R_{p^n}, & \text{если } M_p \cong R_{p^n}. \end{cases}$$

2) $\Rightarrow$ 3). Для каждого $p_0 \in P_M$ через $\pi_{p_0} : \bigoplus\limits_{p \in P_M} M_p \to M_{p_0}$ обозначим естественную проекцию. Пусть N – конечно порожденный подмодуль модуля M. Так как M_p является вполне инвариантным подмодулем модуля M для каждого p, то имеет место равенство $N = \bigoplus\limits_{p \in P'} \pi_p(N)$, где P' – конечное подмножество P. Так как согласно условию п. 2) для каждого $p \in P'$ модуль $\pi_p(N)$ является циклическим, то, очевидно, модуль N также является циклическим. □

Пусть V – векторное пространство над полем F, $A : V \to V$ – локально алгебраический линейный оператор. Пространство V называется A-квазициклическим, если для некоторого неприводимого многочлена $g \in F[X]$ пространство V как $F[X]$-модуль является g-примарным квазициклическим модулем. Аналогично определяется A-циклическое векторное пространство.

Теорема 23 ([20]). *Пусть V – векторное пространство над полем F, $A : V \to V$ – локально алгебраический линейный оператор. Тогда равносильны следующие утверждения:*

1) *для каждого конечного семейства векторов $v_1, \dots, v_k \in V$ существует натуральное число n и вектор $v \in V$ такие, что $v_1, \dots, v_k \in \langle v, A(v), \dots, A^{n-1}(v)\rangle$;*
2) $CC(A) = C(A)$;
3) $\overline{F[A]} = C(A)$;
4) $\overline{F[A]}$ *– максимальная коммутативная подалгебра алгебры* $\mathrm{End}_F(V)$;
5) $V = \bigoplus\limits_{g \in P_0} V_g$, *где $P_0 \subseteq P(F[X])$, и каждое подпространство V_g является либо A-циклическим, либо A-квазициклическим.*

Доказательство. Согласно (1) векторное пространство V можно рассматривать как $F[X]$-модуль.

Эквивалентность 2) $\Leftrightarrow$ 3) вытекает из теоремы 14.

Эквивалентность 3) $\Leftrightarrow$ 4) вытекает из леммы 13, и из того факта, что коммутативная подалгебра совпадает со своим централизатором тогда и только тогда, когда она является максимальным коммутативной подалгеброй.

Эквивалентность 2) $\Leftrightarrow$ 5) вытекает из леммы 22.

2) $\Rightarrow$ 1). Пусть $v_1, \dots, v_k \in V$. Согласно условию п. 2) алгебра $\mathrm{End}_{F[X]}(V)$ коммутативна. Следовательно, согласно лемме 22 для некоторого $v \in V$ имеет место принадлежность $v_1, \dots, v_k \in F[X]v$.

1) $\Rightarrow$ 2). Пусть N – конечно порожденный подмодуль модуля ${}_{F[X]}V$. Согласно условию п. 1) N – подмодуль циклического модуля над коммутативной областью главных идеалов, и, значит, подмодуль N является циклическим. Таким образом, модуль ${}_{F[X]}V$ является модулем Безу, и из леммы 22 вытекает коммутативность алгебры $\mathrm{End}_{F[X]}(V)$. Тогда $C(A) = \mathrm{End}_{F[X]}(V) = Z(\mathrm{End}_{F[X]}(V)) = CC(A)$. □

Следствие 24. *Пусть A – локально нильпотентный линейный оператор, действующий в векторном пространстве V над полем F. Тогда эквивалентны следующие утверждения:*

1) $C(A) = F[[A]]$;
2) $F[[A]]$ *– максимальная коммутативная подалгебра алгебры* $\mathrm{End}_F(V)$;
3) *пространство V является конечномерным или счетномерным, и в некотором базисе пространства V матрица оператора A имеет один из следующих видов соответственно:*

$$J_n(0) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}, \quad J_\infty(0) = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & \dots \\ 0 & 0 & 1 & 0 & \dots & \dots \\ 0 & 0 & 0 & 1 & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots & & \\ \vdots & \vdots & \vdots & \vdots & & \end{pmatrix}.$$

Следствие 25. *Пусть V – векторное пространство над полем F, $A : V \to V$ – локально алгебраический линейный оператор. Тогда равносильны следующие утверждения:*

1) *существует $n \in \mathbb{N}$ и вектор $v \in V$ такие, что $V = \langle v, A(v), \dots, A^{n-1}(v)\rangle$;*
2) *$F[A] = C(A)$;*
3) *$F[A]$ – максимальная коммутативная подалгебра алгебры $\mathrm{End}_F(V)$;*
4) *$V_{F[X]} = \bigoplus\limits_{g \in P_0} V_g$, где P_0 – конечное подмножество множества $P(F[X])$ и каждое подпространство V_g является A-циклическим.*

Доказательство. Эквивалентность 1) ⇔ 4) непосредственно следует из того факта, что модуль над коммутативной областью главных идеалов является циклическим в точности тогда, когда он является конечной прямой суммой своих примарных компонент, каждая из которых является циклическим модулем.

2) ⇒ 3). Согласно [18, лемма 26] $\overline{F[A]} = F[A]$. Так как $\overline{F[A]} = F[A] = C(A)$, то из теоремы 23 вытекает, что $F[A]$ – максимальная коммутативная подалгебра алгебры $\mathrm{End}_F(V)$.

3) ⇒ 2). Из леммы 13 имеем $\overline{F[A]} = F[A]$ и $\overline{F[A]}$ – максимальная коммутативная подалгебра алгебры $\mathrm{End}_F(V)$. Тогда согласно теореме 23 имеет место равенство $F[A] = C(A)$.

2) ⇒ 4). Так как согласно п. 2) и [18, лемма 26] $F[A] = \overline{F[A]}$, то из теоремы 14 вытекает, что A – алгебраический линейный оператор. Поскольку $\overline{F[A]} = F[A] = C(A)$, из теоремы 23 и того факта, что каждый ограниченный модуль является конечной прямой суммой своих ненулевых примарных компонент, получаем утверждение п. 4).

4) ⇒ 2). Из условия п. 4) имеем, что модуль $V_{F[X]}$ ограничен. Согласно теореме 23 кольцо эндоморфизмов модуля $V_{F[X]}$ коммутативно. Тогда из теоремы 14 вытекают равенства $F[A] = \overline{F[A]} = CC(A) = C(A)$. □

Пусть V – векторное пространство. Локально алгебраический линейный оператор $A \in \mathrm{End}(V)$ называется минимальным, если для каждого локально алгебраического линейного оператора $X \in \mathrm{End}(V)$ из включения $C(X) \subseteq C(A)$ следует равенство $C(X) = C(A)$. Из теоремы 19 непосредственно вытекает утверждение.

Теорема 26. *Пусть V – векторное пространство над полем F, $A : V \to V$ – локально алгебраический линейный оператор. Если $\overline{F[A]}$ является максимальной коммутативной подалгеброй алгебры $\mathrm{End}_F(V)$, то A минимален.*

Линейный оператор A, действующий на конечномерном векторном пространстве V, называется несокращаемым, если его минимальный многочлен равен его характеристическому многочлену. Хорошо известно, что линейный оператор A является несокращаемым тогда и только тогда, когда V является A-циклическим пространством.

Следствие 27 ([19, лемма 2.5]). *Пусть $n \geq 2$ и F – произвольное поле. Если матрица $A \in M_n(F)$ является несокращаемой, то A минимальна.*

Доказательство. Утверждение непосредственно вытекает из следствия 25 и теоремы 26. □

Пусть V – векторное пространство над полем F, $A : V \to V$ – локально алгебраический линейный оператор. Тогда имеет место разложение $A = \bigoplus\limits_{g\in P(F[X])} A|_{V_g}$, которое иногда называют грубой канонической формой Жордана. Если $g = x - \alpha$, $\alpha \in F$, то оператор $A|_{V_g} : V_g \to V_g$ будем обозначать как A_α. Определим оператор $A^\beta_\alpha : V_g \to V_g$ в виде

$$A^\beta_\alpha := A_\alpha + (\beta - \alpha)\mathrm{Id}_{V_g}.$$

Так как $A^\beta_\alpha - A^\gamma_\alpha = (\beta-\gamma)\mathrm{Id}_{V_{x-\alpha}} \in Z(\mathrm{End}_F(V_{x-\alpha}))$ для любых $\alpha, \beta, \gamma \in F$ и централизатор элемента кольца не меняется при суммировании этого элемента с любым элементом из центра, то имеет место равенство

$$C(A^\beta_\alpha) = C(A^\gamma_\alpha) \text{ для любых } \alpha, \beta, \gamma \in F. \tag{2}$$

Доказательство следующего утверждения принадлежит А.Д. Маклакову.

Теорема 28 ([20]). *Пусть V – векторное пространство произвольной размерности над алгебраически замкнутым полем F и $A : V \to V$ – локально алгебраический линейный оператор. Тогда A минимален тогда и только тогда, когда $\overline{F[A]}$ является максимальной коммутативной подалгеброй алгебры* $\mathrm{End}_F(V)$.

Доказательство. Достаточность вытекает из теоремы 26. Докажем необходимость. Используя формулу (1), будем рассматривать V как $F[X]$-модуль, и обозначим его как V_A. Поскольку A – локально алгебраический оператор, модуль V_A является периодическим. Предположим, что $\overline{F[A]}$ не является максимальной коммутативной подалгеброй алгебры $\mathrm{End}_F(V)$. Тогда из теоремы 23 вытекает, что модуль V_A содержит некоторую разложимую примарную компоненту $V_{x-\alpha}$, $\alpha \in F$, и с учетом леммы 20 имеем

$$V_A = V_{x-\alpha} \oplus V_4,\ V_4 = \bigoplus_{\beta\in F\setminus\{\alpha\}} V_{x-\beta} \text{ и } V_{x-\alpha} = V_1 \oplus V_2 \oplus V_3, \text{ где}$$
$$V_1 \cong F[X]_{(x-\alpha)^{n_1}},\ V_2 \cong F[X]_{(x-\alpha)^{n_2}},\ n_1, n_2 \in \mathbb{N}\cup\{\infty\}.$$

Значит, $A = A_\alpha \oplus A_4$, где $A_4 = \bigoplus\limits_{\beta\in F\setminus\{\alpha\}} A_\beta$, $A_\alpha = A_1 \oplus A_2 \oplus A_3$ и $A_i = A|_{V_i}$ для $i = 1, \ldots, 4$.

Для $i = 1, \ldots, 4$ обозначим через $\pi_i \in \mathrm{End}_{F[X]}(V_A) \subseteq \mathrm{End}_F(V)$ каноническую проекцию на прямое слагаемое V_i модуля V_A. Тогда, используя разложение Пирса, получаем матричное представление кольца эндоморфизмов модуля V_A:

$$\mathrm{End}_{F[X]}(V_A) = C(A) = \begin{pmatrix} \pi_1C(A)\pi_1 & \pi_2C(A)\pi_1 & \pi_3C(A)\pi_1 & 0 \\ \pi_1C(A)\pi_2 & \pi_2C(A)\pi_2 & \pi_3C(A)\pi_2 & 0 \\ \pi_1C(A)\pi_3 & \pi_2C(A)\pi_3 & \pi_3C(A)\pi_3 & 0 \\ 0 & 0 & 0 & \pi_4C(A)\pi_4 \end{pmatrix}, \text{ где}$$

$$\pi_j C(A)\pi_i \cong \begin{cases} F[X]_{(x-\alpha)^{min(n_j,n_i)}}, & \text{если } n_j, n_i < \infty \\ F[X]_{(x-\alpha)^{n_j}}, & \text{если } n_j < \infty,\ n_i = \infty \\ 0, & \text{если } n_j = \infty,\ n_i < \infty \\ F[[X]]_{(x-\alpha)}, & \text{если } n_j = n_i = \infty \end{cases} \quad \text{для } i,j = 1,2.$$

Для $i, j = 1, \ldots, 4$ имеет место канонический изоморфизм модулей

$$\mathrm{Hom}_{F[X]}(V_j, V_i) \cong \pi_j C(A)\pi_i,$$

который при $i = j$ является также изоморфизмом алгебр $\mathrm{End}_{F[X]}(V_i) = C(A_i) \cong \pi_i C(A)\pi_i$, что позволяет отождествить $\mathrm{Hom}_{F[X]}(V_j, V_i)$ (соответственно $C(A_i)$) с соответствующим подмодулем (подалгеброй) в $C(A)$. Заметим также, что либо $\pi_1 C(A)\pi_2 \neq 0$, либо $\pi_2 C(A)\pi_1 \neq 0$.

Рассмотрим два случая.

1) Существует элемент $\beta_0 \in F\backslash\{\alpha\}$ такой, что $V_{x-\beta_0} = 0$. Определим линейный оператор

$$B = (A_1)_\alpha^{\beta_0} \oplus A_2 \oplus A_3 \oplus A_4.$$

2) $V_{x-\beta} \neq 0$ для любого элемента $\beta \in F$. В силу алгебраической замкнутости F, множество $F\backslash\{\alpha\}$ бесконечно. Пусть I – начальный ординал (с минимальным элементом 0), соответствующий мощности множества $F\backslash\{\alpha\}$, и $\{\beta_i\}_{i<I}$ – I-индексированная последовательность элементов $F\backslash\{\alpha\}$, задающая биекцию между I и $F\backslash\{\alpha\}$. Тогда $A_4 = \bigoplus\limits_{i<I} A_{\beta_i}$. Оператор B зададим следующим образом (используем трансфинитный сдвиг $\{\beta_i\}_{i<I}$, чтобы высвободить элемент β_0):

$$B = (A_1)_\alpha^{\beta_0} \oplus A_2 \oplus A_3 \oplus \acute{A}_4, \text{ где } \acute{A}_4 = \bigoplus_{i<I} A_{\beta_i}^{\beta_{i+1}}.$$

Используя (2), получаем $C\left((A_1)_\alpha^{\beta_0}\right) = C(A_1)$ для случаев 1), 2) и $C(\acute{A}_4) = C(A_4)$ для случая 2). Рассмотрим модуль V_B, соответствующий оператору B. Тогда в силу определения оператора B и формулы (2) имеют место равенства $\pi_i C(A)\pi_i = \pi_i C(B)\pi_i$ для $i = 1, \ldots, 4$, а также $\pi_2 C(A)\pi_3 = \pi_2 C(B)\pi_3$ и $\pi_3 C(A)\pi_2 = \pi_3 C(B)\pi_2$. С учетом выбора β_0 подпространство V_1, рассматриваемое как $F[X]$-модуль, изоморфно $F[X]_{(x-\beta_0)^{n_1}}$ и является $(x - \beta_0)$-примарной компонентой модуля V_B. Тогда кольцо эндоморфизмов модуля V_B в обоих случаях имеет вид

$$\mathrm{End}_{F[X]}(V_B) = C(B) = \begin{pmatrix} \pi_1 C(A)\pi_1 & 0 & 0 & 0 \\ 0 & \pi_2 C(A)\pi_2 & \pi_3 C(A)\pi_2 & 0 \\ 0 & \pi_2 C(A)\pi_3 & \pi_3 C(A)\pi_3 & 0 \\ 0 & 0 & 0 & \pi_4 C(A)\pi_4 \end{pmatrix} \subseteq C(A).$$

Так как либо $\pi_1 C(A)\pi_2 \neq 0$, либо $\pi_2 C(A)\pi_1 \neq 0$, то включение $C(B) \subseteq C(A)$ является строгим, а значит, оператор A не минимален. $\square$

Из теоремы 28 вытекает следующее утверждение, приведенное в [21, лемма 3.2] и [19, предложение 2.3].

Следствие 29. *Пусть V – конечномерное векторное пространство над алгебраически замкнутым полем F, $A : V \to V$ – линейный оператор. Тогда A минимален в точности тогда, когда $F[A]$ является максимальной коммутативной подалгеброй алгебры $\mathrm{End}_F(V)$.*

4. Приложения в теории полей

В настоящем разделе рассмотрим подход Н. Джекобсона к изложению теории Галуа, основанный на использовании соответствия Джекобсона–Бурбаки. Также приведем доказательство теоремы Гильберта 90 и некоторые ее известные обобщения на основе этого подхода.

Пусть P – поле. Множество всех автоморфизмов $\mathrm{Aut}(P)$ поля P является хаусдорфовой топологической группой, топология на которой является ограничением конечной топологии заданной на $\mathrm{End}(P)$. Если F – подполе поля P, то подгруппу $\{g \in \mathrm{Aut}(P) \mid \forall a \in F\ g(a) = a\}$ группы $\mathrm{Aut}(P)$ будем обозначать через $G(P/F)$. Неподвижное подполе подгруппы H группы $\mathrm{Aut}(P)$ обозначается P^H.

Напомним некоторые факты из основ теории полей. Алгебраическое расширение P/K называется расширением Галуа, если $K = P^{G(P/K)}$. Хорошо известно, что расширение P/K является расширением Галуа в точности тогда, когда P – поле разложения некоторого семейства сепарабельных многочленов над полем K. При этом $G(P/K)$ является компактной группой как обратный предел дискретных конечных групп. Если H – компактная подгруппа группы $\mathrm{Aut}(P)$, то P/P^H – расширение Галуа. Действительно, если $a \in P$, то $H = \bigcup\limits_{p \in P} \{h \in H \mid h(a) = p\}$. Так как H – компактная группа, то для некоторого конечного семейства различных элементов $p_1, \ldots, p_k \in P$ имеем $H = \bigcup\limits_{1 \le i \le k} \{h \in H \mid h(a) = p_i\}$. Следовательно, коэффициенты сепарабельного многочлена $(x - p_1) \ldots (x - p_k)$, корнем которого является a, принадлежат подполю P^H.

Отождествим, как и ранее, элементы из поля P с эндоморфизмами из $\mathrm{End}(P)$ с помощью вложения $\iota : P \to \mathrm{End}(P)$, $\alpha \mapsto (x \mapsto \alpha x)$. Для каждой подгруппы H группы $\mathrm{Aut}(P)$ через PH обозначим подкольцо кольца $\mathrm{End}(P)$, порожденное P и H. В силу леммы Артина–Дедекинда любой элемент из PH однозначно представим в виде линейной комбинации $\sum\limits_{g \in H} \alpha_g g$. Также заметим, что в кольце $\mathrm{End}(P)$ для каждых $\alpha \in P$ и $g \in H$ выполнено равенство $g\alpha = g(\alpha)g$.

Через $\mathcal{GR}(P)$ обозначим множество всех подколец кольца $\mathrm{End}(P)$ вида $\overline{PH}$, где H – компактная подгруппа группы $\mathrm{Aut}(P)$. Подмножество множества $\mathcal{GR}(P)$, состоящее из всех подколец кольца $\mathrm{End}(P)$ вида PH, где H – конечная подгруппа группы $\mathrm{Aut}(P)$, обозначим $\mathcal{GR}_f(P)$. Ясно, что $\mathcal{GR}(P) \subseteq \mathcal{R}(P)$ и $\mathcal{GR}_f(P) \subseteq \mathcal{R}_f(P)$. Множество всех подполей

K поля P, для которых P/K является расширением Галуа, обозначим $\mathcal{G}(P)$. Через $\mathcal{G}_f(P)$ обозначим множество всех подполей K поля P, для которых P/K является конечным расширением Галуа.

Пусть H – компактная подгруппа группы $\mathrm{Aut}(P)$. Поле P имеет естественную структуру простого точного левого PH-модуля. Так как $C_{\mathrm{End}(P)}(PH) = \mathrm{End}_{PH}(P) \subseteq \mathrm{End}_P(P) = P$ и для каждых $\alpha \in P$ и $g \in \mathrm{Aut}(P)$ равенство $\alpha g = g\alpha$ в кольце $\mathrm{End}(P)$ равносильно $g(\alpha) = \alpha$, то $C_{\mathrm{End}(P)}(\overline{PH}) = C_{\mathrm{End}(P)}(PH) = P^H \in \mathcal{G}(P)$.

С другой стороны, если $K \in \mathcal{G}(P)$, то $K = P^{G(P/K)}$ и $G(P/K)$ – компактная подгруппа группы $\mathrm{Aut}(P)$. Тогда $C_{\mathrm{End}(P)}(PG(P/K)) = P^{G(P/K)} = K$ и, следовательно, согласно теореме плотности Джекобсона–Шевалле

$$C_{\mathrm{End}(P)}(K) = C_{\mathrm{End}(P)}C_{\mathrm{End}(P)}(PG(P/K)) = \overline{PG(P/K)}. \tag{3}$$

В силу изложенного выше имеют место отображения $\Psi : \mathcal{G}(P) \to \mathcal{GR}(P)$ и $\Phi : \mathcal{GR}(P) \to \mathcal{G}(P)$, действующие соответственно согласно правилам $K \mapsto C_{\mathrm{End}(P)}(K)$ и $\overline{PH} \mapsto C_{\mathrm{End}(P)}(\overline{PH})$ для любых $K \in \mathcal{G}(P)$ и $\overline{PH} \in \mathcal{GR}(P)$. Таким образом, ввиду следствий 6 и 7 справедлива

Теорема 30. *Пусть P – поле. Тогда*

1) *отображения Ψ и Φ являются взаимно обратными антиизоморфизмами между частично упорядоченными множествами $(\mathcal{G}(P), \subseteq)$ и $(\mathcal{GR}(P), \subseteq)$;*
2) *$\Psi(\mathcal{G}_f(P)) = \mathcal{GR}_f(P)$ и отображение Ψ индуцирует антиизоморфизм между частично упорядоченными множествами $(\mathcal{G}_f(P), \subseteq)$ и $(\mathcal{GR}_f(P), \subseteq)$.*

При этом если $K \in \mathcal{G}_f(P)$ и $(P : K) = n$, то $\dim({}_P PG(P/K)) = n$, т. е. $|G(P/K)| = n$.

Лемма 31. *Пусть P – поле и H – компактная подгруппа группы $\mathrm{Aut}(P)$. Тогда для каждой замкнутой подгруппы H' группы $G(P/P^H)$ выполнено равенство*

$$G(P/P^H) \cap \overline{PH'} = H'.$$

Доказательство. Пусть H' – замкнутая подгруппа группы $G(P/P^H)$. Заметим, что так как $G(P/P^H)$ является компактной подгруппой хаусдорфовой топологической группы $\mathrm{Aut}(P)$, то подгруппа $G(P/P^H)$ замкнута и, следовательно, H' также является замкнутой в $\mathrm{Aut}(P)$. Пусть $g \in G(P/P^H) \cap \overline{PH'}$. Рассмотрим произвольную окрестность U элемента g. Эта окрестность содержит окрестность вида $U_0 = \{f \in \mathrm{End}(P) \mid f(x_1) = g(x_1), \ldots, f(x_n) = g(x_n)\}$, где $x_1, \ldots, x_n \in P$. Так как P/P^H – расширение Галуа поля P^H, то $x_1, \ldots, x_n$ – алгебраические элементы над полем P^H. Значит, без ограничения общности можно считать, что система $x_1, \ldots, x_n$ содержит подсистему, которая является базисом векторного пространства ${}_{P^H}P^H(x_1, \ldots, x_n)$. Так как $g \in \overline{PH}$, то для некоторого элемента $\sum\limits_{i=1}^{m} \alpha_i h_i$, где

$\alpha_i \in P, h_i \in H'$ для каждого $1 \leq i \leq m$, имеет место равенство

$$g_{|\{x_1,\ldots,x_n\}} = \left(\sum_{i=1}^{m} \alpha_i h_i\right)_{|\{x_1,\ldots,x_n\}}.$$

В силу того, что

$$g, \sum_{i=1}^{m} \alpha_i h_i \in \mathrm{End}_{P^H}(P),$$

имеем

$$g_{|P^H(x_1,\ldots,x_n)} = \left(\sum_{i=1}^{m} \alpha_i h_i\right)_{|P^H(x_1,\ldots,x_n)}.$$

Тогда из леммы Артина–Дедекинда следует $g_{|P^H(x_1,\ldots,x_n)} = h_{i_0|P^H(x_1,\ldots,x_n)}$ для некоторого $1 \leq i_0 \leq m$. Таким образом, $G(P/P^H) \cap \overline{PH'} \subseteq H'$. Поскольку обратное включение очевидно, то получаем равенство $G(P/P^H) \cap \overline{PH'} = H'$. □

Для произвольного поля P множество всех компактных подгрупп группы $\mathrm{Aut}(P)$ обозначим $\mathcal{K}(\mathrm{Aut}(P))$.

Теорема 32. *Пусть P – поле. Тогда отображения*

$$\begin{array}{cc} \mathcal{G}(P) \to \mathcal{K}(\mathrm{Aut}(P)), & \mathcal{K}(\mathrm{Aut}(P)) \to \mathcal{G}(P), \\ K \mapsto G(P/K), & H \mapsto P^H, \end{array}$$

являются взаимно обратимыми и обращают включения.

Доказательство. Равенство $K = P^{G(P/K)}$ для произвольного поля из $\mathcal{G}(P)$ следует из определения расширения Галуа. Пусть $H \in \mathcal{K}(\mathrm{Aut}(P))$. Согласно теореме плотности Джекобсона-Шевалле и равенствам (3) имеем

$$\overline{PH} = C_{\mathrm{End}(P)}C_{\mathrm{End}(P)}(PH) = C_{\mathrm{End}(P)}(P^H) = \overline{PG(P/P^H)}.$$

Так как $H \leq G(P/P^H)$, то в силу леммы 31

$$H = G(P/P^H) \cap \overline{PH} = G(P/P^H) \cap \overline{PG(P/P^H)} = G(P/P^H).$$

□

Если P/K – расширение Галуа, то через $\mathcal{K}(G(P/K))$ обозначим множество всех компактных подгрупп группы $G(P/K)$, которое, очевидно, совпадает с множеством всех замкнутых подгрупп группы $G(P/K)$. Так как для каждого расширения Галуа P/K и любого его промежуточного подполя F расширение P/F также является расширением Галуа, то из предыдущей теоремы непосредственно вытекает

Теорема 33. *Пусть P/K – расширение Галуа и $\mathcal{G}(P/K)$ – множество всех промежуточных подполей расширения P/K. Тогда отображения*

$$\begin{aligned} \mathcal{G}(P/K) &\to \mathcal{K}(G(P/K)), & \qquad \mathcal{K}(G(P/K)) &\to \mathcal{G}(P/K), \\ F &\mapsto G(P/F), & H &\mapsto P^H, \end{aligned}$$

являются взаимно обратимыми и обращают включения.

Далее нам потребуется следующее хорошо известное утверждение, согласно которому все автоморфизмы и все дифференцирования полной матричной алгебры на полем P являются внутренними. Приведем единообразные и краткие доказательства этих фактов.

Теорема 34. *Пусть P – поле. Тогда*

1) *если Φ – автоморфизм алгебры $M_n(P)$, то существует такая обратимая матрица $A \in M_n(P)$, что $\Phi(X) = AXA^{-1}$ для каждой матрицы X из $M_n(P)$;*
2) *если Ψ – дифференцирование алгебры $M_n(P)$, то существует такая матрица $A \in M_n(P)$, что $\Psi(X) = AX - XA$ для каждой матрицы X из $M_n(P)$.*

Доказательство. Пусть P^n – векторное пространство вектор-столбцов длины n с компонентами из поля P. Для каждого линейного оператора $\Phi \in \mathrm{End}_P(M_n(P))$ и каждых $\overline{a}$ и $\overline{b}$ из P^n через $A_{\Phi,a,b}$ обозначим такую однозначно определенную матрицу из $M_n(P)$, что равенство $\Phi\left(\overline{x}\overline{b}^T\right)\overline{a} = A_{\Phi,a,b}\overline{x}$ выполнено для любого $\overline{x}$ из P^n.

1) Пусть Φ – автоморфизм алгебры $M_n(P)$. Тогда $\Phi\left(\overline{x_0}\overline{b}^T\right)\overline{a} \neq 0$ для некоторых $\overline{x}_0, \overline{a}, \overline{b} \in P^n$. Покажем, что $\Phi(A) = A_{\Phi,a,b}AA^{-1}_{\Phi,a,b}$ для произвольной матрицы A из $M_n(P)$. Действительно, для каждого $\overline{x}$ из P^n имеем

$$A_{\Phi,a,b}A\overline{x} = \Phi\left(A\overline{x}\overline{b}^T\right)\overline{a} = \Phi(A)\Phi\left(\overline{x}\overline{b}^T\right)\overline{a} = \Phi(A)A_{\Psi,a,b}\overline{x}.$$

Следовательно, $A_{\Phi,a,b}A = \Phi(A)A_{\Phi,a,b}$. Так как $A_{\Phi,a,b}\overline{x}_0 = \Phi\left(\overline{x}_0\overline{b}^T\right)\overline{a} \neq 0$, то для произвольного $\overline{c} \in P^n$ существует такая матрица B, что

$$\overline{c} = BA_{\Phi,a,b}\overline{x}_0 = \Phi(\Phi^{-1}(B))A_{\Phi,a,b}\overline{x}_0 = A_{\Phi,a,b}\Phi^{-1}(B)\overline{x}_0.$$

Таким образом, матрица $A_{\Phi,a,b}$ обратима и, значит, $\Phi(A) = A_{\Phi,a,b}AA^{-1}_{\Phi,a,b}$.

2) Пусть Ψ – дифференцирование алгебры $M_n(P)$. Существуют такие вектор-столбцы $\overline{a}$ и $\overline{b}$ из P^n, что $\overline{b}^T\overline{a} = 1$. Покажем, что $\Psi(A) = A_{\Psi,a,b}A - AA_{\Psi,a,b}$ для произвольной матрицы A из $M_n(P)$. Для каждого $\overline{x}$ из P^n имеет место равенство

$$\Psi\left(A\overline{x}\overline{b}^T\right) = \Psi(A)\overline{x}\overline{b}^T + A\Psi\left(\overline{x}\overline{b}^T\right).$$

Следовательно,

$$A_{\Psi,a,b}A\overline{x} = \Psi\left(A\overline{x}\overline{b}^T\right)\overline{a} = \Psi(A)\overline{x}\overline{b}^T\overline{a} + A\Psi\left(\overline{x}\overline{b}^T\right)\overline{a} = \Psi(A)\overline{x} + AA_{\Psi,a,b}\overline{x}.$$

Таким образом, $\Psi(A) = A_{\Psi,a,b}A - AA_{\Psi,a,b}$. □

Замечание 35. Доказательство п. 1) теоремы 34 приведено в работе [22]. Модульный аналог этого доказательства, которое дает широкое обобщение п. 1), приведен в работе [23]. Доказательство п. 2) теоремы 34 основано на идеях доказательства теоремы 5.1 из статьи [24].

Предложение 36. *Пусть P/K – расширение Галуа, $G(P/K) = \langle\sigma\rangle$ – циклическая группа порядка n и $P\langle\sigma\rangle$ – подкольцо кольца* $\mathrm{End}(P)$. *Тогда*

1) *если $\alpha \in P$ и $N_{P/K}(\alpha) = 1$, то отображение $\varphi : P\langle\sigma\rangle \to P\langle\sigma\rangle$, действующее по правилу*

$$\alpha_0+\alpha_1\sigma+\alpha_2\sigma^2+\ldots+\alpha_{n-1}\sigma^{n-1} \mapsto \alpha_0+\alpha\alpha_1\sigma+\alpha\sigma(\alpha)\alpha_2\sigma^2+\ldots+\prod_{k=0}^{n-2}\sigma^k(\alpha)\alpha_{n-1}\sigma^{n-1},$$

где $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in P$, является автоморфизмом K-алгебры $P\langle\sigma\rangle$;

2) *если $\alpha \in P$ и $Tr_{P/K}(\alpha) = 0$, то отображение $\psi : P\langle\sigma\rangle \to P\langle\sigma\rangle$, действующее по правилу*

$$\alpha_0+\alpha_1\sigma+\alpha_2\sigma^2+\ldots+\alpha_{n-1}\sigma^{n-1} \mapsto \alpha\alpha_1\sigma+(\alpha+\sigma(\alpha))\alpha_2\sigma^2+\ldots+\left(\sum_{k=0}^{n-2}\sigma^k(\alpha)\right)\alpha_{n-1}\sigma^{n-1},$$

где $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in P$, является дифференцированием K-алгебры $P\langle\sigma\rangle$.

Доказательство. 1) Для каждого $1 \le i \le n-1$ положим

$$\beta_i = \prod_{k=0}^{i-1}\sigma^k(\alpha),$$

также будем считать, что $\beta_0 = 1$. Пусть $\beta, \beta' \in P$, $1 \le i, j \le n-1$ и r – остаток от деления $i+j$ на n. Имеют место равенства

$$\varphi(\beta\sigma^i\beta'\sigma^j) = \varphi(\beta\sigma^i(\beta')\sigma^r) = \beta_r\beta\sigma^i(\beta')\sigma^r.$$

Так как

$$\prod_{k=1}^{n}\sigma^k(\alpha) = 1,$$

то

$$\varphi(\beta\sigma^i)\varphi(\beta'\sigma^j) = \beta_i\beta\sigma^i\beta_j\beta'\sigma^j = \beta_i\sigma^i(\beta_j)\beta\sigma^i(\beta')\sigma^r = \prod_{k=0}^{i+j-1}\sigma^k(\alpha)\beta\sigma^i(\beta')\sigma^r$$
$$= \sigma^{-1}\left(\prod_{k=1}^{i+j}\sigma^k(\alpha)\right)\beta\sigma^i(\beta')\sigma^r = \sigma^{-1}\left(\prod_{k=1}^{r}\sigma^k(\alpha)\right)\beta\sigma^i(\beta')\sigma^r = \beta_r\beta\sigma^i(\beta')\sigma^r.$$

Таким образом, $\varphi(\beta\sigma^i\beta'\sigma^j) = \varphi(\beta\sigma^i)\varphi(\beta'\sigma^j)$ и поскольку отображение φ, очевидно, является K-линейным, то φ – автоморфизм K-алгебры $P\langle\sigma\rangle$.

2) Доказывается с помощью аналогичных вычислений. □

Пусть P/K – расширение Галуа и $G = G(P/K)$ – конечная группа. Согласно изложенному выше каждый элемент из подкольца $PG \in \mathcal{GR}_f(P)$ кольца $\mathrm{End}(P)$ однозначно представим в виде $\sum\limits_{g\in G} \alpha_g g$ и $g\alpha = g(\alpha)g$ для каждых $g \in G$ и $\alpha \in P$. В частности, PG является скрещенным произведением P на G. Так как для простого левого PG-модуля P имеет место равенство $\mathrm{End}_{PG}(P) = C_{\mathrm{End}(P)}(PG) = K$ и размерность K-алгебры PG равна $(P : K)\,|G| = |G|^2$, то из точности простого левого PG-модуля P вытекает, что алгебра PG является артиновой простой и, значит, $PG \cong M_{|G|}(K)$.

Следствием теоремы 34 и предложения 36 является теорема Гильберта 90, обобщения которой играют важное значение во многих вопросах алгебры и являются источниками глубоких аналогий и связей.

Теорема 37 (теорема Гильберта 90)**.** *Пусть P/K – циклическое расширение Галуа и $\alpha \in P$. Тогда*

1) $N_{P/K}(\alpha) = 1$ *в точности тогда, когда для некоторого ненулевого элемента β из P выполнено равенство $\alpha = \beta\sigma(\beta)^{-1}$;*
2) $\mathrm{Tr}_{P/K}(\alpha) = 0$ *в точности тогда, когда для некоторого элемента β из P выполнено равенство $\alpha = \beta - \sigma(\beta)$.*

Доказательство. 1) Из теоремы 34 следует, что отображение φ из предложения 36 является внутренним автоморфизмом K-алгебры $P\langle\sigma\rangle$. Следовательно, существует такой обратимый элемент $\beta \in P\langle\sigma\rangle$, что $\varphi(x) = \beta x\beta^{-1}$ для каждого $x \in P\langle\sigma\rangle$. Так как $\beta p\beta^{-1} = \varphi(p) = p$ для каждого $p \in P$, то $\beta \in C_{P\langle\sigma\rangle}(P) = P$ и, значит, $\beta \in P$. Поскольку $\alpha\sigma = \varphi(\sigma) = \beta\sigma\beta^{-1} = \beta\sigma(\beta^{-1})\sigma$, то $\alpha = \beta\sigma(\beta^{-1})$.

2) Из теоремы 34 имеем, что отображение ψ из предложения 36 является внутренним дифференцированием K-алгебры $P\langle\sigma\rangle$. Следовательно, существует такой элемент $\beta \in P\langle\sigma\rangle$, что $\psi(x) = \beta x - x\beta$ для каждого $x \in P\langle\sigma\rangle$. Так как $\beta p - p\beta = \psi(p) = 0$ для каждого $p \in P$, то $\beta \in C_{P\langle\sigma\rangle}(P) = P$ и, значит, $\beta \in P$. Поскольку $\alpha\sigma = \psi(\sigma) = \beta\sigma - \sigma\beta = (\beta - \sigma(\beta))\sigma$, то $\alpha = \beta - \sigma(\beta)$. □

Замечание 38. Для того, чтобы подчеркнуть важность предыдущей теоремы, отметим некоторые ее непосредственные и хорошо известные следствия.

Пусть a, b, c – примитивная пифагорова тройка, т. е. $a, b, c \in \mathbb{N}$, $(a, b, c) = 1$ и $a^2+b^2 = c^2$. Предположим, что a нечетно. Так как $G(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle$, где σ – операция сопряжения на $\mathbb{Q}(i)$, и $N_{\mathbb{Q}(i)/\mathbb{Q}}\left(\dfrac{a+ib}{c}\right) = 1$, то из теоремы 37 следует, что для некоторого $p + qi \in \mathbb{Q}(i)$ имеет место равенство $\dfrac{a+ib}{c} = \dfrac{p+iq}{p-iq}$. Без ограничения общности можно считать, что $p, q \in \mathbb{Z}$ и $(p, q) = 1$. Тогда для некоторого $t \in \mathbb{N}$ имеют место равенства $ta = p^2 - q^2$, $tb = 2pq$, $tc = p^2 + q^2$. Так как $(p, q) = 1$, то $t \in \{1, 2\}$. Поскольку a нечетно, $p \not\equiv q \bmod 2$

и, значит, $t = 1$. Таким образом, для всякой примитивной пифагоровой тройки a, b, c существуют такие $p, q \in \mathbb{N}$, что либо $a = p^2 - q^2, b = 2pq, c = p^2 + q^2$, если a нечетно, либо $a = 2pq, b = p^2 - q^2, c = p^2 + q^2$, если a четно.

Пусть $a, b \in \mathbb{F}_{2^n}^*$. Так как $G(\mathbb{F}_{2^n}/\mathbb{F}_2) = \langle \sigma \rangle$, где σ – автоморфизм Фробениуса, то из теоремы 37, п. 2) вытекают эквивалентности

$$\exists \alpha \in \mathbb{F}_{2^n} : \alpha^2 + a\alpha + b = 0 \Leftrightarrow \exists \alpha \in \mathbb{F}_{2^n} : \alpha^2 + \alpha = \frac{b}{a^2} \Leftrightarrow \exists \alpha \in \mathbb{F}_{2^n} : \sigma(\alpha) + \alpha = \frac{b}{a^2}$$
$$\Leftrightarrow \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}} \left(\frac{b}{a^2} \right) = 0.$$

Таким образом, корни алгебраического уравнения $x^2 + ax + b = 0$, где $a, b \in \mathbb{F}_{2^n}^*$, принадлежат полю $\mathbb{F}_{2^n}$ в точности тогда, когда $\sum\limits_{k=0}^{n-1} \left(\frac{b}{a^2} \right)^{2^k} = 0$.

Метод доказательства теоремы 37, приведенный выше, позволяет доказать ряд известных обобщений теоремы Гильберта 90. В работе [25] было доказано следующее обобщение теоремы 37 на случай абелевых расширений Галуа.

Теорема 39 (теорема Гильберта 90 для абелевых расширений)**.** *Пусть P/K – расширение Галуа, $G(P/K) = G_1 \times \ldots \times G_m$, где $G_i = \langle \sigma_i \rangle$ – циклическая группа порядка n_i для каждого $1 \leq i \leq m$, и $a_1, \ldots, a_m \in P^*$. Тогда равенства*

$$N_{P/P^{G_i}}(a_i) = 1, \quad \frac{\sigma_i(a_j)}{a_j} = \frac{\sigma_j(a_i)}{a_i},$$

для каждых $1 \leq i, j \leq m$ имеют место в точности тогда, когда существует такой элемент $a \in P^*$, что

$$a_i = \frac{\sigma_i(a)}{a}, \quad i = 1, \ldots, m.$$

Доказательство. Для каждого $1 \leq i \leq m$ положим $\pi_i = a_i \sigma_i$. Так как каждый элемент из $PG(P/K)$ однозначно представим в виде

$$\sum_{0 \leq i_1 \leq n_1 - 1, \ldots, 0 \leq i_m \leq n_m - 1} \beta_{i_1, \ldots, i_m} \pi_1^{i_1} \ldots \pi_m^{i_m},$$

где $\beta_{i_1, \ldots, i_m} \in P$, и для каждых $1 \leq i, j \leq m$ и $\alpha \in P$ выполнены равенства

$$\pi_i^{n_i} = (a_i \sigma_i)^{n_i} = N_{P/P^{G_i}}(a_i) \sigma_i^{n_i} = 1,$$
$$\pi_i \pi_j = a_i \sigma_i a_j \sigma_j = a_i \sigma_i(a_j) \sigma_i \sigma_j = a_j \sigma_j(a_i) \sigma_i \sigma_j = a_j \sigma_j a_i \sigma_i = \pi_j \pi_i,$$
$$\pi_i \alpha = a_i \sigma_i \alpha = a_i \sigma_i(\alpha) \sigma_i = \sigma_i(\alpha) \pi_i,$$

то отображение $\Phi : PG(P/K) \to PG(P/K)$, действующее по правилу

$$\sum_{0\le i_1\le n_1-1,\ldots,0\le i_m\le n_m-1} \beta_{i_1,\ldots,i_m}\sigma_1^{i_1}\ldots\sigma_m^{i_m} \mapsto \sum_{0\le i_1\le n_1-1,\ldots,0\le i_m\le n_m-1} \beta_{i_1,\ldots,i_m}\pi_1^{i_1}\ldots\pi_m^{i_m},$$

является автоморфизмом K-алгебры $PG(P/K)$. Поскольку $PG(P/K) \cong M_{n_1\cdots n_m}(K)$, из теоремы 34 следует, что отображение Φ является внутренним автоморфизмом K-алгебры $PG(P/K)$ и, значит, существует такой обратимый элемент $a \in PG(P/K)$, что $\Phi(x) = axa^{-1}$ для каждого $x \in PG(P/K)$. Ясно, что $a \in C_{PG(P/K)}(P) = P$. Так как $a_i\sigma_i = \Phi(\sigma_i) = a\sigma_i a^{-1}$ $= a\sigma_i(a_i^{-1})\sigma_i$ для каждого $1 \le i \le m$, то $a_i = a\sigma_i(a^{-1})$. □

Пусть P/K – расширение Галуа. Отображение $f : G(P/K) \to P^*$ называется скрещенным гомоморфизмом, если $f(gg') = f(g)g(f(g'))$ для каждых $g, g' \in G$. Множество всех скрещенных гомоморфизмов, действующих из $G(P/K)$ в P^*, является группой относительно поточечной операции умножения функций. Эта группа обозначается $Z(G(P/K), P^*)$. Если $a \in P^*$, то отображение $f : G(P/K) \to P^*$, действующее согласно правилу $g \mapsto \dfrac{a}{g(a)}$, является скрещенным гомоморфизмом. Множество всех скрещенных гомоморфизмов такого вида образуют подгруппу группы $Z(G(P/K), P^*)$, которая обозначается $B(G(P/K), P^*)$. Фактор-группа $H^1(G(P/K), P^*) = Z(G(P/K), P^*)/B(G(P/K), P^*)$ называется первой когомологической группой $G(L/K)$ с коэффициентами в P^*. Аналогично определяется скрещенный гомоморфизм, действующий из $G(P/K)$ в аддитивную группу поля P, и группа $H^1(G(P/K), P)$. Если P/K – циклическое расширение Галуа и $G(P/K) = \langle\sigma\rangle$ – циклическая группа порядка n, то несложно заметить, что

$$f(\sigma^i) = \prod_{k=0}^{i-1}\sigma^k(f(\sigma)) \text{ для каждого } 1 \le i \le n$$

и отображение $\Phi : Z(G(P/K), P^*) \to \{a \in P \mid N_{P/K}(a) = 1\}$, действующее по правилу $f \mapsto f(\sigma)$, является биекцией. Таким образом, в случае циклических расширений Галуа теорема Гильберта 90 равносильна равенству $H^1(G(P/K), P^*) = 1$. Предыдущее равенство было обобщено на случай произвольных конечных расширений Галуа А. Шпайзером [26] и Э. Нетер [27]. Далее это утверждение будет доказано с помощью теоремы 34. Идея применения п. 1) теоремы 34 для доказательства мультипликативной формы теоремы Гильберта 90 для произвольных конечных расширений Галуа принадлежит Э. Нетер.

Предложение 40. *Пусть P/K – конечное расширение Галуа. Тогда для отображения $f : G(P/K) \to P^*$ равносильны следующие условия:*

1) *f – скрещенный гомоморфизм;*
2) *отображение $\varphi : PG(P/K) \to PG(P/K)$, действующее по правилу*

$$\sum_{g\in G}\alpha_g g \mapsto \sum_{g\in G}\alpha_g f(g)g,$$

где $\alpha_g \in P$ для каждого $g \in G$, является автоморфизмом K-алгебры $PG(P/K)$.

Доказательство. Ясно, что отображения φ является автоморфизмом K-алгебры $PG(P/K)$ в точности тогда, когда для каждых $\alpha, \alpha' \in P$ и $g, g' \in G(P/K)$ выполнено равенство

$$\varphi(\alpha g \alpha' g') = \varphi(\alpha g)\varphi(\alpha' g'). \tag{4}$$

Так как

$$\varphi(\alpha g \alpha' g') = \alpha g(\alpha') f(gg') gg'$$

и

$$\varphi(\alpha g)\varphi(\alpha' g') = \alpha g(\alpha') f(g) g(f(g')) gg',$$

то равенство (4) имеет место для каждых $\alpha, \alpha' \in P$ и $g, g' \in G(P/K)$ в точности тогда, когда $f(gg') = f(g)g(f(g'))$. Таким образом, равенство (4) равносильно тому факту, что f – скрещенный гомоморфизм. □

Аналогично доказывается

Предложение 41. *Пусть P/K – конечное расширение Галуа. Тогда для отображения $f : G(P/K) \to P$ равносильны следующие условия:*

1) *f – скрещенный гомоморфизм из $G(P/K)$ в аддитивную группу поля P;*
2) *отображение $\psi : PG(P/K) \to PG(P/K)$, действующее по правилу*

$$\sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g f(g) g,$$

где $\alpha_g \in P$ для каждого $g \in G$, является дифференцированием K-алгебры $PG(P/K)$.

Теорема 42. *Пусть P/K – конечное расширение Галуа. Тогда*

1) *$H^1(G(P/K), P^*) = 1$, т. е. если $f : G(P/K) \to P^*$ – скрещенный гомоморфизм, то существует такой элемент $a \in P^*$, что $f(g) = \dfrac{a}{g(a)}$ для каждого $g \in G$;*
2) *$H^1(G(P/K), P) = 0$, т. е. если $f : G(P/K) \to P$ – скрещенный гомоморфизм из $G(P/K)$ в аддитивную группу поля P, то существует такой элемент $a \in P$, что $f(g) = a - g(a)$ для каждого $g \in G$.*

Доказательство. 1) Из теоремы 34 имеем, что отображение φ из предложения 40 является внутренним автоморфизмом K-алгебры $PG(P/K)$. Следовательно, существует такой элемент $a \in PG(P/K)$, что $\varphi(x) = axa^{-1}$ для каждого $x \in PG(P/K)$. Ясно, что $a \in P$. Тогда для произвольного $g \in G$ получаем

$$f(g)g = \varphi(g) = aga^{-1} = ag(a^{-1})g$$

и, следовательно, $f(g) = \dfrac{a}{g(a)}$.

2) Доказывается аналогично п. 1). □

Замечание 43. Из предыдущей теоремы можно несложно вывести теорему 39 (см., например, [25]). Доказательства теорем 39 и 42 на основе теоремы 34 приведены в настоящей работе из методических соображений, в качестве иллюстрации связей между автоморфизмами и дифференцированиями матричных алгебр и соответственно мультипликативными и аддитивными формами теоремы Гильберта 90.

Замечание 44. Интересно отметить аналогию между теоремой Гильберта 90 и леммой Пуанкаре, согласно которой всякая замкнутая дифференциальная форма ω степени $q > 0$ на $\mathbb{R}^n$ является точной формой, т. е. $H^q_{DR}(\mathbb{R}^n) = 0$ для каждого $q \geq 1$. Действительно, равенство $H^1_{DR}(\mathbb{R}^n) = 0$ равносильно тому факту, что для каждого семейства $f_1, \ldots, f_n$ C^∞-гладких функций на $\mathbb{R}^n$, удовлетворяющих соотношению $\dfrac{\partial f_i}{\partial x_j} = \dfrac{\partial f_j}{\partial x_i}$ для каждых $1 \leq i, j \leq n$, существует такая функция $f \in C^\infty(\mathbb{R}^n)$, что $f_i = \dfrac{\partial f}{\partial x_i}$ для каждого $1 \leq i \leq n$. Предыдущее утверждение вполне аналогично формулировке теоремы Гильберта 90 в случае абелевых расширений Галуа P/K (теорема 39), которое равносильно равенству $H^1(G(P/K), P^*) = 1$.

Автор благодарит А.Д. Маклакова, С.М. Скрябина, Д.Т. Тапкина и А.А. Туганбаева за постоянное внимание к работе и сделанные полезные замечания.

Список литературы

[1] T. Nakayma, *Über einfache distributive Systeme unendlicher Ränge*, Proc. Imp. Acad.Tokyo **20**, 61–66 (1944).

[2] N. Jacobson, *Structure theory of simple rings without finiteness assumptions*, Trans. Amer. Math. Soc., **57** (2), 228–245 (1945).
DOI: https://doi.org/10.2307/1990204

[3] N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. **37**, AMS, Providence R.I., 1956.

[4] N. Jacobson, *Basic algebra* II*: Second edition*, W.H. Freeman and Company, New York, 1989.

[5] N. Bourbaki, *Elements of the history of mathematics*, Springer-Verlag, Berlin, 1994.

[6] E. Artin, *Galois theory*, Notre Dame Math. Lectures **2**, 1971.

[7] K. Fuller, *Density and equivalence*, J. Algebra **29** (3), 528–550 (1974).
DOI: https://doi.org/10.1016/0021-8693(74)90088-X

[8] B.J. Mùller, *On Morita duality*, Canad. J. Math. **21**, 1338–1347 (1969).
DOI: https://doi.org/10.4153/CJM-1969-147-7

[9] P.A. Krylov, A.A. Tuganbaev, *Modules over discrete valuation domains*, De Gruyter, Berlin, New York, 2008.

DOI: https://doi.org/10.1515/9783110205787

[10] C. Faith, *Algebra: rings, modules and categories* I, Springer-Verlag, Berlin, Heidelberg, 1973.
DOI: https://doi.org/10.1007/978-3-642-80634-6

[11] M.C. Iovanov, Z. Mesyan, M.L. Reyes, *Infinite-Dimensional Diagonalization and Semisimplicity*, Israel J. Math. **215**, 801–855 (2016).
DOI: https://doi.org/10.1007/s11856-016-1395-5

[12] N. Jacobson, *A note on division rings*, Am. J. Math. **69** (1), 27–36 (1947).
DOI: https://doi.org/10.2307/2371651

[13] H. Cartan, *Les principaux théorèmes de la théorie de Galois pour les corps non nécessairement commutatifs*, Comptes rendus de l'Académie des Sciences **224**, 249–251 (1947).

[14] S. Warner, *Topological rings*, North Holland, 1993.

[15] I. Kaplansky, *Infinite abelian groups*, Univ. of Michigan Press, Ann Arbor, MI, 1954.

[16] H. Furstenberg, *On the infinitude of primes*, Am. Math. Mon. **62** (5), 353 (1957).
DOI: https://doi.org/10.2307/2307043

[17] Е.В. Новоселов, *Введение в полиадический анализ*, ПГУ, Петрозаводск, 1982.

[18] Z. Mesyan, *Infinite-dimensional triangularization*, J. Pure Appl. Algebra **222** (7), 1529–1547 (2018).
DOI: https://doi.org/10.1016/j.jpaa.2017.07.010

[19] G. Dolinar, A.E. Guterman, B. Kuzma, P. Oblak, *Extremal matrix centralizers*, Linear Algebra Appl. **438** (7), 2904–2910 (2013).
DOI: https://doi.org/10.1016/j.laa.2012.12.010

[20] A. Abyzov, A. Maklakov, *Locally algebraic linear operators and their centralizers*, Linear Algebra Appl. **662**, 1–17 (2023).
DOI: https://doi.org/10.1016/j.laa.2022.12.022

[21] P. Šemrl, *Non-linear commutativity preserving maps*, Acta Sci. Math. (Szeged) **71** (3–4), 781–819 (2005).

[22] P. Šemrl, *Maps on matrix spaces*, Linear Algebra Appl. **413** (2–3), 364–393 (2006).
DOI: https://doi.org/10.1016/j.laa.2005.03.011

[23] A. Abyzov, A. Maklakov, *Automorphisms of dense subrings of the endomorphism ring of a free module*, Linear Algebra Appl. **679**, 220–230 (2023).
DOI: https://doi.org/10.1016/j.laa.2023.09.021

[24] J. Courtemanche, M. Dugas, *Automorphisms of the endomorphism algebra of a free module*, Linear Algebra Appl. **510**, 79–91 (2016).
DOI: https://doi.org/10.1016/j.laa.2016.08.017

[25] I.G. Connell, *Elementary generalizations of Hilbert's Theorem* 90, Canad. Math. Bull. **8** (6), 749–757 (1965).
DOI: https://doi.org/10.4153/CMB-1965-055-2

[26] A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Zeit. **5**, 1–6 (1919).

[27] E. Noether, *Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper*, Math. Ann. **108**, 411–419 (1933).

Адель Наилевич Абызов
Казанский (Приволжский) федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,
e-mail: Adel.Abyzov@kpfu.ru

Volume 1, Issue 4 UDC 15A27, 12F10, 16S50
pp. 3–34 (2023) MSC 512.64, 512.623, 512.55

Density theorems and its applications

A.N. Abyzov

Abstract. This article is semi-review and is also methodological in nature. The article discusses generalizations of the Jacobson-Chevalley density theorem, on the basis of which a number of results from linear algebra are presented, related to centralizers of locally algebraic linear operators. Also, based on Jacobson's approach to constructing Galois theory based on the density theorem, a proof of Hilbert's theorem 90 and some of its well-known generalizations are given.

Keywords: finite topology, centralizer, locally algebraic operator, Galois extensions.

References

[1] T. Nakayma, *Über einfache distributive Systeme unendlicher Ränge*, Proc. Imp. Acad.Tokyo **20**, 61–66 (1944).

[2] N. Jacobson, *Structure theory of simple rings without finiteness assumptions*, Trans. Amer. Math. Soc., **57** (2), 228–245 (1945).
DOI: https://doi.org/10.2307/1990204

[3] N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. **37**, AMS, Providence R.I., 1956.

[4] N. Jacobson, *Basic algebra* II*: Second edition*, W.H. Freeman and Company, New York, 1989.

[5] N. Bourbaki, *Elements of the history of mathematics*, Springer-Verlag, Berlin, 1994.

[6] E. Artin, *Galois theory*, Notre Dame Math. Lectures **2**, 1971.

[7] K. Fuller, *Density and equivalence*, J. Algebra **29** (3), 528–550 (1974).
DOI: https://doi.org/10.1016/0021-8693(74)90088-X

[8] B.J. Mùller, *On Morita duality*, Canad. J. Math. **21**, 1338–1347 (1969).
DOI: https://doi.org/10.4153/CJM-1969-147-7

[9] P.A. Krylov, A.A. Tuganbaev, *Modules over discrete valuation domains*, De Gruyter, Berlin, New York, 2008.
DOI: https://doi.org/10.1515/9783110205787

Acknowledgements. The work is supported by the Russian Science Foundation (grant no. 22-21-00267) and performed under the development program of Volga Region Mathematical Center (agreement no. 075-02-2023-944).

Received: 07 October 2023. Accepted: 28 November 2023. Published: 26 December 2023.

[10] C. Faith, *Algebra: rings, modules and categories* I, Springer-Verlag, Berlin, Heidelberg, 1973.
DOI: https://doi.org/10.1007/978-3-642-80634-6

[11] M.C. Iovanov, Z. Mesyan, M.L. Reyes, *Infinite-dimensional diagonalization and semisimplicity*, Israel J. Math. **215** (2), 801–855 (2016).
DOI: https://doi.org/10.1007/s11856-016-1395-5

[12] N. Jacobson, *A note on division rings*, Am. J. Math. **69** (1), 27–36 (1947).
DOI: https://doi.org/10.2307/2371651

[13] H. Cartan, *Les principaux théorèmes de la théorie de Galois pour les corps non nécessairement commutatifs*, Comptes rendus de l'Académie des Sciences **224**, 249–251 (1947).

[14] S. Warner, *Topological rings*, North Holland, 1993.

[15] I. Kaplansky, *Infinite abelian groups*, Univ. of Michigan Press, Ann Arbor, MI, 1954.

[16] H. Furstenberg, *On the infinitude of primes*, Am. Math. Mon. **62** (5), 353 (1957).
DOI: https://doi.org/10.2307/2307043

[17] E.V. Novoselov, *Introduction to polyadic analysis*, Petrozavodsk. Gos. Univ., Petrozavodsk, 1982 [in Russian].

[18] Z. Mesyan, *Infinite-dimensional triangularization*, J. Pure Appl. Algebra **222** (7), 1529–1547 (2018).
DOI: https://doi.org/10.1016/j.jpaa.2017.07.010

[19] G. Dolinar, A.E. Guterman, B. Kuzma, P. Oblak, *Extremal matrix centralizers*, Linear Algebra Appl. **438** (7), 2904–2910 (2013).
DOI: https://doi.org/10.1016/j.laa.2012.12.010

[20] A. Abyzov, A. Maklakov, *Locally algebraic linear operators and their centralizers*, Linear Algebra Appl. **662**, 1–17 (2023).
DOI: https://doi.org/10.1016/j.laa.2022.12.022

[21] P. Šemrl, *Non-linear commutativity preserving maps*, Acta Sci. Math. (Szeged) **71** (3–4), 781–819 (2005).

[22] P. Šemrl, *Maps on matrix spaces*, Linear Algebra Appl. **413** (2–3), 364–393 (2006).
DOI: https://doi.org/10.1016/j.laa.2005.03.011

[23] A. Abyzov, A. Maklakov, *Automorphisms of dense subrings of the endomorphism ring of a free module*, Linear Algebra Appl. **679**, 220–230 (2023).
DOI: https://doi.org/10.1016/j.laa.2023.09.021

[24] J. Courtemanche, M. Dugas, *Automorphisms of the endomorphism algebra of a free module*, Linear Algebra Appl. **510**, 79–91 (2016).
DOI: https://doi.org/10.1016/j.laa.2016.08.017

[25] I.G. Connell, *Elementary generalizations of Hilbert's Theorem* 90, Canad. Math. Bull. **8** (6), 749–757 (1965).
DOI: https://doi.org/10.4153/CMB-1965-055-2

[26] A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Zeit. **5**, 1–6 (1919).

[27] E. Noether, *Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper*, Math. Ann. **108**, 411–419 (1933).

Adel Nailevich Abyzov
Kazan Federal University,
18 Kremlyovskaya str., Kazan 420008, Russia,
e-mail: Adel.Abyzov@kpfu.ru