А. Б. Жеглов, О диких алгебрах с делением над полями степенных рядов, *Матем. сб.*, 2004, том 195, номер 6, 21–56

DOI: 10.4213/sm825

УДК 512.552.32

**А. Б. Жеглов**

# О диких алгебрах с делением над полями степенных рядов

В статье изучаются некоторые специальные классы алгебр с делением над полем лорановских степенных рядов с произвольным полем вычетов. Алгебры из таких классов мы называем расщепимыми и хорошо расщепимыми. В статье показано, что эти классы содержат группу ручных алгебр с делением. Для класса хорошо расщепимых алгебр с делением доказана теорема о разложении, которая является обобщением известных теорем Джекоба и Вэдсворта о разложении для ручных алгебр с делением. Для обоих классов мы вводим понятие $\delta$-отображения и развиваем технику $\delta$-отображений для алгебр с делением из этих классов. С помощью этой техники мы доказываем теоремы о разложении, передоказываем несколько старых хорошо известных результатов Салтмана, а также доказываем гипотезу М. Артина о периоде и индексе в локальном случае: экспонента алгебры с делением $A$ над $C_2$-полем $F$ равна ее индексу, если $F = F_1((t))$, где $F_1$ – $C_1$-поле. Кроме этого в работе получены несколько результатов о расщепимых алгебрах с делением, которые, как мы надеемся, помогут дальнейшему исследованию диких алгебр с делением.

Библиография: 13 названий.

## § 1. Введение

В этой работе мы исследуем некоторый класс алгебр с делением над полем степенных рядов от одной переменной с произвольным полем вычетов. А именно мы изучаем тела, удовлетворяющие следующему условию: существует сечение $\overline{D} \hookrightarrow D$ гомоморфизма вычетов $D \to \overline{D}$, где $D$ – центральная алгебра с делением над полным полем дискретного нормирования $F = k((t))$. Такие тела мы будем называть *расщепимыми*. В случае $\operatorname{char} k = 0$ все такие тела являются ручными (см. ниже) и, следовательно, принадлежат подгруппе ручных алгебр в группе Брауэра $\operatorname{Br}(F)$, которая была тщательно изучена в работах [1] и [2] (и даже в намного более общей ситуации гензелева поля $F$ произвольной характеристики). Таким образом, мы будем изучать в основном дикие алгебры с делением.

Дикие алгебры с делением степени $p$ над полным полем $F$ дискретного нормирования ранга 1 с полем вычетов характеристики $\operatorname{char}(\overline{F}) = p$ были исследованы Салтманом в [3] (Тиньоль в [4] исследовал более общий случай бездефектных алгебр с делением степени $p$ над гензелевым полем $F$). В этой работе мы изучаем расщепимые алгебры с делением произвольного индекса. Класс таких тел (который, однако, не является подгруппой в группе Брауэра $\operatorname{Br}(F)$) содержит подкласс

Работа выполнена при поддержке Graduiertenkolleg "Geometrie und Nichtlineare Analisys" фонда DFG.

хорошо расщепимых тел (см. определение в § 3), которые обладают рядом замечательных свойств. В частности, для таких алгебр мы докажем теорему о разложении. Эта теорема является обобщением теорем о разложении для ручных алгебр с делением, доказанных Джэкобом и Вэдсвортом в [1].

Для произвольных расщепимых алгебр с делением мы дадим здесь лишь несколько разрозненных результатов, и кажется, что изучение даже этого класса тел еще далеко от своего завершения. Тем не менее, мы развиваем здесь технику для произвольных расщепимых тел и доказываем несколько фундаментальных свойств таких, например, как соотношение между высотами для расщепимой алгебры с делением (см. § 6). Мы надеемся, что эта техника позволит в дальнейшем ответить на вопрос о цикличности некоторых тел степени $p^k$.

В качестве приложения мы приведем несколько результатов, некоторые из которых уже были известны, а некоторые являются новыми. В частности, мы докажем, что справедлива следующая гипотеза: экспонента алгебры с делением $A$ над $C_2$-полем $F = F_1((t))$, где $F_1$ – $C_1$-поле, равна ее индексу.

Приведем краткое описание результатов статьи.

В § 2 мы даем определение расщепимых и хорошо расщепимых алгебр с делением и доказываем, что все ручные алгебры с делением над $F = k((t))$ хорошо расщепимы.

В § 3 мы развиваем упомянутую выше технику для изучения расщепимых алгебр с делением. Мы вводим понятие $\delta$-отображений и развиваем теорию таких отображений на расщепимых алгебрах. В этом параграфе мы определяем также понятие локальной высоты, которое является одним из возможных обобщений определенного Салтманом уровня.

В § 4 мы доказываем указанную выше гипотезу о периоде и индексе. Параграф содержит также краткую историю вопроса, известную автору. Отметим, что доказательство использует далеко не все результаты из § 3.

В § 5 изучаются хорошо расщепимые тела и доказывается теорема о разложении.

В § 6 мы передоказываем некоторые результаты Салтмана о полуразветвленных алгебрах с делением индекса $p$ над полем $F$, используя технику § 3. Также мы вводим понятие высшего уровня и доказываем несколько общих результатов о расщепимых телах, удовлетворяющих следующему условию: $Z(\overline{D})/\overline{F}$ – простое расширение. В частности, мы доказываем, что высший уровень строго больше высоты, если высота взаимно проста с характеристикой центра тела (теорема 4). В конце параграфа мы указываем некоторые открытые вопросы.

В этой работе мы пользуемся обозначениями из статьи [1]. Всегда $D$ будет обозначать алгебру с делением, конечномерную над своим центром $F = k((t)) = Z(D)$. Напомним, что произвольное гензелево нормирование поля $F$ однозначно продолжается до нормирования тела $D$. Мы будем обозначать через $v$ нормирование на $F$ и через $w$ – его продолжение на $D$.

Мы будем обозначать через $\Gamma_D$ группу значений $w$, через $V_D$ – его кольцо нормирования, через $M_D$ – его максимальный идеал и через $\overline{D} = V_D/M_D$ – тело вычетов.

Известно [5; с. 21], что выполняется следующее фундаментальное неравенство:

$$[D : F] \geqslant |\Gamma_D : \Gamma_F| \cdot [\overline{D} : \overline{F}].$$

Тело $D$ называется *бездефектным над* $F$, если выполняется равенство, и *дефектным* в противном случае. Известно, что тело $D$ бездефектно, если на нем существует дискретное нормирование ранга 1.

В работе [1] авторы ввели понятие основного гомоморфизма

$$\theta_D\colon \Gamma_D/\Gamma_F \to \mathrm{Gal}(Z(\overline{D})/\overline{F}),$$

которое определяется с помощью сопряжения элементами из $D$. Они показали, что $\theta_D$ сюръективен и что $Z(\overline{D})$ является композитом абелева и чисто несепарабельного расширений поля $\overline{F}$.

Алгебра с делением $D$ называется *ручной*, если $\mathrm{char}(\overline{F}) = 0$ или если $\mathrm{char}(\overline{F}) = q \neq 0$, $D$ бездефектна над $F$, $Z(\overline{D})$ сепарабельно над $\overline{F}$ и $q \nmid |\ker(\theta_D)|$. Алгебра $D$ называется *дикой* в противном случае.

Алгебра $D$ называется *инерциально расщепимой*, если поле $Z(\overline{D})$ сепарабельно над $\overline{F}$, отображение $\theta_D$ – изоморфизм и $D$ бездефектна над $F$.

В заключение автор хотел бы поблагодарить А.Н. Паршина, Е.-В. Цинка и М. Грабица за полезные обсуждения и внимание к этой работе. Особую признательность мне хотелось бы выразить А. Вэдсворту за внимательное прочтение и указание ошибки в первой версии этой статьи, а также В.И. Янчевскому за активную совместную работу во время его визита в Берлин.

## § 2. Теорема Коэна

Напомним определение из работы [6].

Определение 1. Алгебру с делением $D$ назовем *расщепимой*, если существует гомоморфизм $\overline{D} \hookrightarrow \mathscr{O}_D \subset D$, являющийся сечением отображения $\mathscr{O}_D \to \overline{D}$.

Возникает естественный вопрос, существует ли обобщение теоремы Коэна, т.е. расщепима ли произвольная центральная алгебра с делением. Это не так, если алгебра с делением не является конечномерной над своим центром, как показывает пример Дубровина в [6]. Это также неверно для некоторых конечномерных алгебр с делением, как видно из примера к теореме 2.7 в [3]. Но ответ на вопрос положителен для диких алгебр с делением над полными дискретно нормированными полями. Это непосредственно следует из результатов Джэкоба и Вэдсворта [1] (ср. с [6; теорема 1]).

Теорема 1. *Пусть $(F, v)$ – поле, полное относительно дискретного нормирования $v$ ранга 1. Пусть $\mathrm{char}\, F = \mathrm{char}\, \overline{F}$, и пусть $D$ – ручная алгебра с делением, $Z(D) = F$ и $[D:F] < \infty$.*

*Тогда существует сечение $\overline{D} \hookrightarrow D$ гомоморфизма вычетов $D \to \overline{D}$.*

Доказательство. Так как $F$ – полное поле, то $F$ является гензелевым, и $v$ однозначно продолжается до нормирования $w$ тела $D$. Так как $D$ – ручная алгебра, то $Z(\overline{D})/\overline{Z(D)}$ есть циклическое расширение Галуа. Тогда существует неразветвленный подъем $Z$ поля $Z(\overline{D})$ над $F$, причем $Z$ есть расширение Галуа над $F$, и по классической теореме Коэна существует сечение $\overline{Z} \hookrightarrow Z$.

Рассмотрим централизатор $C = C_D(Z)$ поля $Z$ в $D$. Тогда имеем $\overline{C} = \overline{D}$.

Действительно, по теореме о централизаторе имеем $[D:F] = [C:F][Z:F]$ и $[Z:F] = |\mathrm{Gal}(Z(\overline{D})/\overline{F})|$. В силу [1; предложение 1.7] гомоморфизм

$$\theta_D\colon \Gamma_D/\Gamma_F \to \mathrm{Gal}(Z(\overline{D})/\overline{F})$$

сюръективен, поэтому для любого параметра $z$ выполняется $\theta_D(w(z)) = \sigma$, где $\langle\sigma\rangle = \mathrm{Gal}(Z(\overline{D})/\overline{F})$. Ясно, что $z \notin C$.

Теперь пусть $u_1, \ldots, u_{[C:F]}$ – $F$-базис $C$. Легко видеть, что элементы $u_j, zu_j, \ldots, z^{n-1}u_j$, $j = 1, \ldots, [C:F]$, где $n = \mathrm{ord}(\sigma)$ – порядок $\sigma$, линейно независимы, т.е. они составляют базис $D$ над $F$. Так как

$$w(F\langle zu_j, \ldots, z^{n-1}u_j,\ j = 1, \ldots, [C:F]\rangle) \cap \Gamma_C = 0,$$

где $F\langle zu_j, \ldots, z^{n-1}u_j,\ j = 1, \ldots, [C:F]\rangle$ обозначает векторное пространство в $D$ над $F$, порожденное элементами $u_j z^i$, то имеем, что для любого элемента $x \in D$ с $w(x) = 0$ можно найти элементы $r_1, \ldots, r_{[C:F]} \in F$ такие, что $x = r_1u_1 + \cdots + r_{[C:F]}u_{[C:F]} \pmod{M_D}$. Отсюда $\overline{C} = \overline{D}$.

Заметим, что $C$ – неразветвленная алгебра с делением. В самом деле, в силу теорем 2.8, 2.9 из [1] $C$ содержит копию неразветвленного подъема максимального сепарабельного подполя в $\overline{C}$. Обозначим ее через $\widetilde{C}$. Тогда централизатор $C_C(\widetilde{C})$ должен быть вполне разветвленной алгеброй с делением, а значит, он тривиален и $\widetilde{C}$ – максимальное подполе. Следовательно, $C$ должна быть неразветвленной алгеброй.

Рассмотрим вложение $i\colon \overline{F} \hookrightarrow F$. Оно может быть расширено до вложения $i'\colon \overline{Z} \hookrightarrow Z$, $i'|_{\overline{F}} = i$, по лемме Гензеля. Теперь рассмотрим алгебру $A = \overline{C} \otimes_{\overline{Z}} Z(C)$. Легко видеть, что $A$ – неразветвленная алгебра с делением и $\overline{A} = \overline{C} = \overline{D}$. Поэтому по [7; теорема 31] имеем $A \cong C$; следовательно, существует сечение $\overline{D} \hookrightarrow C$.

Теорема доказана.

Ниже будет показано, что гораздо больше может быть сказано про хорошо расщепимые алгебры.

Определение 2. Алгебра с делением $D$ называется *хорошо расщепимой*, если существует сечение $s\colon \overline{D} \hookrightarrow D$, согласованное с вложением $i\colon \overline{Z(D)} \hookrightarrow Z(D)$, т.е. $s(\overline{Z(D)}) = i(\overline{Z(D)}) \subset Z(D)$.

Легко видеть, что все ручные алгебры с делением хорошо расщепимы, потому что по лемме Гензеля любое вложение $\overline{Z(D)} \hookrightarrow Z(D)$ однозначно продолжается на любое сепарабельное расширение $Z(D)$.

Возникает естественный вопрос, какие из расщепимых алгебр с делением являются хорошо расщепимыми.

По теореме 3.9 из [3] известно, что даже расщепимая алгебра с делением $D$ степени $p = \mathrm{char}\, D$ не является хорошо расщепимой, если уровень $D$ (определение уровня мы напомним в § 3, см. замечание к лемме 7) делится на $p$. Тем не менее, вопрос является открытым, например для алгебр с делением таких, что $\overline{D} = Z(\overline{D})$, $\overline{D}/\overline{F}$ – простое расширение и локальная высота (см. определение в том же замечании) не делится на $p$. Этот вопрос мы еще обсудим в § 6.

## § 3. Дельта-отображения расщепимых алгебр

В настоящем параграфе мы развиваем некоторые идеи из [6], где были изучены определенные свойства $\delta$-отображений для некоторых видов многомерных локальных тел. Ключевую роль во всех наших дальнейших результатах будут играть технические свойства $\delta$-отображений, поэтому ниже мы перечислим все эти свойства.

Пусть $D$ – конечномерная алгебра с делением над полным нормированным полем $F = k((t))$. Пусть $w$ – единственное продолжение нормирования $v$ на $D$. Через $z$ мы будем обозначать произвольный параметр $D$, т.е. произвольный элемент с $\langle w(z)\rangle = \Gamma_D$. Рассмотрим кольцо $\mathbb{Z}\langle\alpha,\delta\rangle$ некоммутативных полиномов от двух переменных. Для любого слова из $\mathbb{Z}\langle\alpha,\delta\rangle$ определим отображение

$$\sigma\colon \mathbb{Z}\langle\alpha,\sigma\rangle \to \mathbb{Z}\langle\alpha,\delta,\delta_i;\ i\geqslant 1\rangle,$$
$$\sigma(\alpha^{a_1}\delta^{b_1}\dots\alpha^{a_n}\delta^{b_n}) = \alpha^{a_1}\delta_{b_1}\dots\delta_{b_{n-1}}\alpha^{a_n-1}\delta^{b_n},$$

где $a_1, b_n \geqslant 0,\ a_i, b_j \geqslant 1,\ i>1, j<n$.

Пусть $S_i^k \in \mathbb{Z}\langle\alpha,\delta\rangle,\ i\geqslant k, i\geqslant 1$, – полиномы, задаваемые следующей формулой:

$$S_i^k = \sum_{\tau\in S_i/G} \tau(\underbrace{\alpha\dots\alpha}_{i-k}\underbrace{\delta\dots\delta}_{k}),$$

где $S_i$ – группа подстановок и $G$ – изотропная подгруппа.

Лемма 1 [6; лемма 2]. *Полиномы $S_i^k$ удовлетворяют следующему свойству:*

$$S_i^i = \delta^i, \qquad S_i^0 = \alpha^i, \qquad S_{i+1}^{k+1} = \alpha S_i^{k+1} + \delta S_i^k.$$

Для любой расщепимой алгебры с делением можно ввести понятие $\delta$-отображений:

Предложение 1 [6; предложения 1, 2]. *Пусть $D$ – расщепимая алгебра с делением. Зафиксируем параметр $z$ и вложение $u\colon \overline{D} \hookrightarrow D$. Тогда $D$ изоморфна алгебре с делением $\overline{D}((z))$, которую зададим как векторное пространство рядов с умножением, определенным формулой*

$$zaz^{-1} = \alpha(a) + \delta_1(a)z + \delta_2(a)z^2 + \cdots, \qquad a\in\overline{D},$$

*где $\alpha\colon \overline{D}\to\overline{D}$ – автоморфизм и $\delta_i\colon \overline{D}\to\overline{D}$ – линейные отображения такие, что отображение $\delta_i$ удовлетворяет тождеству*

$$\delta_i(ab) = \sum_{k=0}^{i} \sigma(\delta^{i-k}\alpha)(a)\sigma(S_i^k\alpha)(b), \qquad a,b\in\overline{D}.$$

Замечание. Заметим, что значения $\sigma(S_i^k\alpha)$ и $\sigma(\delta^{i-k}\alpha)$ принадлежат подкольцу $\mathbb{Z}\langle\alpha,\delta_i; i\geqslant 1\rangle$, поэтому формула корректно определена. Также заметим, что $\delta$-отображения зависят от выбора параметра и вложения. Автоморфизм $\alpha$, как легко видеть, зависит только от выбора параметра. В предложении мы отождествили $\overline{D}$ с $u(\overline{D})$.

Следствие 1 [6; следствие 1]. *Пусть $\alpha = \mathrm{id}$. Тогда*

$$\delta_i(ab) = \delta_i(a)b + \sum_{k=1}^{i}\delta_{i-k}(a)\sum_{(j_1,\dots,j_l)} C_{i-k+1}^l\delta_{j_1}\cdots\delta_{j_l}(b),$$

*где $\delta_0 = \alpha$ и вторая сумма берется по всем векторам $(j_1,\dots,j_l)$ таким, что $0<l\leqslant\min\{i-k+1,k\}$, $j_m\geqslant 1$, $\sum j_m = k$.*

В дальнейшем нам понадобится еще более общее определение.

Определение 3. В предположениях предложения 1 определим отображения ${}^{(z,u)}_{\;\,m}\delta_i\colon \overline{D}\to\overline{D}$, $m\in\mathbb{Z}, i\in\mathbb{N}$, следующим образом:

$$z^m a z^{-m} = u({}^{(z)}\alpha^m(\bar a)) + u({}^{(z,u)}_{\;\,m}\delta_1(\bar a))z + u({}^{(z,u)}_{\;\,m}\delta_2(\bar a))z^2 + \cdots, \qquad a\in u(\overline{D}).$$

Если $m=0$, положим ${}^{(z,u)}_{\;\,m}\delta_i = 0$.

Заметим, что ${}^{(z)}\alpha\big|_{Z(\overline{D})}$ не зависит от выбора $z$.

Отметим также, что если ${}^{(z)}\alpha=\mathrm{id}$, то ${}^{(z,u)}_{\;\,m}\delta_i = 0$ для $m=p^k$, где $k$ достаточно большое и зависит от $i$. Более того, ${}^{(z,u)}_{\;\,m}\delta_i = {}^{(z,u)}_{m+p^k}\delta_i$ для достаточно больших $k$. В дальнейшем мы будем также иногда использовать следующие обозначения:

$${}^{(z,u)}_{\;\,m}\widetilde{\delta}_i = {}^{(z,u)}_{-m}\delta_i, \qquad {}^{(z,u)}_{\;\,1}\delta_i = {}^{(z,u)}\delta_i.$$

Иногда, если это ясно из контекста, мы будем писать ${}_m\delta_i$ вместо ${}^{(z,u)}_{\;\,m}\delta_i$ и ${}^{(z,u)}_{\;\,m}\delta_i(a)$ вместо $u\big({}^{(z,u)}_{\;\,m}\delta_i(\bar a)\big)$.

Сразу из определения следует

Лемма 2. *В обозначениях определения* 3

i) *для* $|m|>1$ *имеем*

$$\begin{aligned}{}^{(z,u)}_{\;\,m}\delta_i(a) &= {}^{(z)}\alpha^{\mathrm{sign}(m)}\big({}^{(z,u)}_{\mathrm{sign}(m)(|m|-1)}\delta_i(a)\big) + {}^{(z,u)}_{\mathrm{sign}(m)}\delta_i\big({}^{(z)}\alpha^{\mathrm{sign}(m)(|m|-1)}(a)\big)\\ &\quad+\sum_{j=1}^{i-1}{}^{(z,u)}_{\mathrm{sign}(m)}\delta_j\big({}^{(z,u)}_{\mathrm{sign}(m)(|m|-1)}\delta_{i-j}(a)\big),\end{aligned}$$

*где* $\mathrm{sign}(m)=m/|m|$, $a\in\overline{D}$;

ii) *для любого* $m\neq 0$ *имеем*

$${}^{(z)}\alpha^{-m}\big({}^{(z,u)}_{\;\,m}\delta_i\big) + {}^{(z,u)}_{-m}\delta_i\big({}^{(z)}\alpha^m\big) + \sum_{j=1}^{i-1}{}^{(z,u)}_{-m}\delta_j\big({}^{(z,u)}_{\;\,m}\delta_{i-j}\big) = 0.$$

Предложение 2. *Для фиксированных* $z$, $u$ *из предложения* 1 *справедливо следующее*:

i) *отображения* ${}^{(z,u)}_{\;\,m}\delta_i$ *удовлетворяют тождествам*

$${}_m\delta_i(ab) = {}_m\delta_i(a)\alpha^{i+m}(b) + \alpha^m(a){}_m\delta_i(b) + \sum_{k=1}^{i-1}{}_m\delta_{i-k}(a)\,{}_{i-k+m}\delta_k(b);$$

ii) *пусть* $\alpha=\mathrm{id}$, *тогда отображения* ${}^{(z,u)}_{\;\,m}\delta_i$ *удовлетворяют тождествам*

$$\begin{aligned}{}_m\delta_i(ab) &= {}_m\delta_i(a)b + a\,{}_m\delta_i(b)\\ &\quad+\sum_{k=1}^{i-1}{}_m\delta_{i-k}(a)\sum_{(j_1,\dots,j_l)}C^l_{i-k+m}\delta_{j_1}\dots\delta_{j_l}(b),\end{aligned}$$

*где вторая сумма берется по всем векторам* $(j_1,\dots,j_l)$ *таким, что* $0<l\leqslant\min\{i-k+m,k\}$, $j_m\geqslant 1$, $\sum j_m = k$; $C^k_j=0$, *если* $j=0$, *и* $C^k_j = C^k_{j+p^q}$ *для* $q\gg 0$, *если* $j\leqslant 0$.

Доказательство. Для любых $a, b \in \overline{D}$ имеем

$$\begin{aligned}\alpha^m(ab)z^m + {}_m\delta_1(ab)z^{m+1} + {}_m\delta_2(ab)z^{m+2} + \cdots = z^m(ab)\\ = (\alpha^m(a)z^m + {}_m\delta_1(a)z^{m+1} + {}_m\delta_2(a)z^{m+2} + \cdots)b.\end{aligned} \tag{1}$$

Если правую сторону равенства (1) записать в виде ряда с коэффициентами слева и затем сравнить соответствующие коэффициенты в правой и левой частях равенства, то мы получим формулы для ${}_m\delta_i(ab)$. Нам остается только доказать, что эти формулы суть те же самые, что и в предложении.

Пусть

$$z^{i+m-k}b = \alpha^{i+m-k}(b)z^{i+m-k} + \cdots + x'_k z^{i+m} + \cdots$$

и

$$\begin{aligned}(\alpha^m(a)z^m + {}_m\delta_1(a)z^{m+1} + {}_m\delta_2(a)z^{m+2} + \cdots)b\\ = \alpha^m(ab)z^m + y_{m+1}z^{m+1} + y_{m+2}z^{m+2} + \cdots .\end{aligned}$$

Тогда имеем, что

$$y_{i+m} = \alpha^m(a)x'_i + \sum_{k=0}^{i-1} {}_m\delta_{i-k}(a)x'_k.$$

В доказательстве предложения 2 из [6] было показано, что

$$z^{i+1-k}b = \alpha^{i+1-k}(b)z^{i+1-k} + \cdots + \sigma(S_i^k\alpha)(b)z^{i+1} + \cdots .$$

Следовательно, $x'_k = \sigma(S_{i+m-1}^k\alpha)(b)$ для $k < i$. Легко видеть, что $x'_i = {}_m\delta_i(b)$, $x'_0 = \alpha^{i+m}(b)$ и $\sigma(S_{i+m-1}^k\alpha) = {}_{i+m-k}\delta_k$, что доказывает п. i).

Для $\alpha = \mathrm{id}$ в силу следствия 1 имеем

$$\sigma(S_{i+m-1}^k\alpha)(b) = \sum_{(j_1,\dots,j_l)} C_{i-k+m}^l \delta_{j_1}\dots\delta_{j_l}(b),$$

где $l, j_1, \dots, j_l$ были определены в нашем утверждении. Этим доказан п. ii).

Предложение доказано.

Лемма 3 [6; лемма 3]. *В предположениях предложения 1 пусть* ${}^{(z,u)}_{\ \ i}\delta_j$ – *первое отображение такое, что* ${}^{(z,u)}_{\ \ i}\delta_j(a) \neq 0$ *для данного* $a \in \overline{D}$, $i \in \mathbb{Z}\setminus\{0\}$, *т.е.* ${}^{(z,u)}_{\ \ i}\delta_1(a) = \cdots = {}^{(z,u)}_{\ \ i}\delta_{j-1}(a) = 0$, ${}^{(z,u)}_{\ \ i}\delta_j(a) \neq 0$ *(таким образом, имеем отображение* $i \mapsto j(i)$*). Справедливо следующее.*

i) *Для* $z' = z + u(b)z^{q+1}$, $b \in \overline{D}$, *имеем*

$$^{(z')}\alpha^i(a) = {}^{(z)}\alpha^i(a), \qquad {}^{(z',u)}_{\ \ i}\delta_k(a) = {}^{(z,u)}_{\ \ i}\delta_k(a), \quad k < q,$$

*и*

$$^{(z',u)}_{\ \ i}\delta_q(a) = {}^{(z,u)}_{\ \ i}\delta_q(a) + b'\,{}^{(z)}\alpha^{q+i}(a) - {}^{(z)}\alpha^i(a)b',$$

*где* $b' = \sum_{k=0}^{i-1} {}^{(z)}\alpha^k(b)$.

ii) *Предположим, что* ${}^{(z)}\alpha^n\big|_{Z(\overline{D})} = \mathrm{id}$, $n \geqslant 1$, $a \in Z(\overline{D})$ *и*

$$^{(z,u)}_{\ \ 1}\delta_1\big({}^{(z)}\alpha^k(a)\big) = \cdots = {}^{(z,u)}_{\ \ 1}\delta_{j-1}\big({}^{(z)}\alpha^k(a)\big) = 0$$

*для любого* $k$.

*Тогда для* $z' = z + u(b)z^{q+1}$, $b \in \overline{D}$, *имеем*

$$ {}^{(z')}\alpha^i(a) = {}^{(z)}\alpha^i(a), \qquad {}^{(z',u)}_{\ i}\delta_k(a) = {}^{(z,u)}_{\ i}\delta_k(a), \quad k < q+j, $$

*и*

$$ \begin{aligned} {}^{(z',u)}_{\ i}\delta_{q+j}(a) &= {}^{(z,u)}_{\ i}\delta_{q+j}(a) + b'\,{}^{(z)}\alpha^q\big({}^{(z,u)}_{\ i}\delta_j(a)\big) - {}^{(z,u)}_{\ i}\delta_j(a)\,{}^{(z)}\alpha^j(b') \\ &+ b'\sum_{k=1}^{q} {}^{(z)}\alpha^{q-k}\big({}^{(z,u)}\delta_j\big({}^{(z)}\alpha^{k+i-1}(a)\big)\big) - {}^{(z,u)}_{\ i}\delta_j(a)\sum_{k=0}^{j-1} {}^{(z)}\alpha^k(b), \end{aligned} $$

*где* $b' = \sum_{k=0}^{i-1} {}^{(z)}\alpha^k(b)$, *если* $n \mid q$ *или если* ${}^{(z)}\alpha(a) = a$.

*В частности, если* ${}^{(z)}\alpha = \mathrm{id}$ *и* $(i,p) = 1$, *то*

$$ {}^{(z',u)}_{\ i}\delta_{q+j}(a) = {}^{(z,u)}_{\ i}\delta_{q+j}(a) + (q-j)\,{}^{(z,u)}_{\ i}\delta_j(a)b. $$

iii) *Для* $z' = u(b)z$, $b \in Z(\overline{D})$, $b \neq 0$, *имеем*

$$ {}^{(z')}\alpha(a) = {}^{(z)}\alpha(a), \qquad {}^{(z',u)}\delta_k(a) = {}^{(z,u)}\delta_k(a), \quad k < j, $$

*и*

$$ {}^{(z',u)}\delta_j(a) = {}^{(z,u)}\delta_j(a)\,{}^{(z)}\alpha(b^{-1})\cdots{}^{(z)}\alpha^j(b^{-1}), $$

*если* $i = 1$.

Доказательство. i) Имеем

$$ \begin{aligned} z'^i a z'^{-i} &= (1 + b'z^q + \cdots)z^i a z^{-i}(1 + b'z^q + \cdots)^{-1} \\ &= (z^i a z^{-i} + b'z^q z^i a z^{-i} + \cdots)(1 - b'z^q + \cdots) \\ &= (z^i a z^{-i} - z^i a z^{-i} b' z^q + \cdots + b'z^q z^i a z^{-i} - \cdots) \\ &= \big(z^i a z^{-i} - \big({}^{(z)}\alpha^i(a) + {}^{(z,u)}_{\ i}\delta_j(a)z^j + \cdots\big)b'z^q \\ &\quad + b'z^q\big({}^{(z)}\alpha^i(a) + {}^{(z,u)}_{\ i}\delta_j(a)z^j + \cdots\big) + \cdots\big) \\ &= \big(z^i a z^{-i} - \big({}^{(z)}\alpha^i(a)b' + {}^{(z,u)}_{\ i}\delta_j(a)\,{}^{(z)}\alpha^j(b')z^j + \cdots\big)z^q \\ &\quad + b'\,{}^{(z)}\alpha^{q+i}(a)z^q + \cdots\big) \\ &= \big(z^i a z^{-i} + \big(-{}^{(z)}\alpha^i(a)b' + b'\,{}^{(z)}\alpha^{q+i}(a)\big)z^q + \cdots\big) \\ &= {}^{(z)}\alpha^i(a) + \cdots + {}^{(z,u)}_{\ i}\delta_{q-1}(a)z'^{q-1} \\ &\quad + \big({}^{(z,u)}_{\ i}\delta_q(a) + b'\,{}^{(z)}\alpha^{q+i}(a) - {}^{(z)}\alpha^i(a)b'\big)z'^q + \cdots. \end{aligned} $$

ii) Положим $c = z'^i z^{-i} - 1 - b'z^{q+i}$. Тогда $w(c) > q+i$. Заметим, что $c\,{}^{(z)}\alpha^k(a) = {}^{(z)}\alpha^k(a)c$, так как $n \mid q$ или ${}^{(z)}\alpha(a) = a$ и $a \in Z(\overline{D})$. Имеем

$$ \begin{aligned} z'^i a z'^{-i} &= (1 + b'z^q + c)z^i a z^{-i}(1 + b'z^q + c)^{-1} \\ &= (z^i a z^{-i} + b'z^q z^i a z^{-i} + c z^i a z^{-i})(1 + b'z^q + c)^{-1} \end{aligned} $$

$$
\begin{aligned}
&= \big({}^{(z)}\alpha^i(a) + {}^{(z,u)}_{i}\delta_j(a)z^j + \cdots + {}^{(z,u)}_{i}\delta_{q+j}(a)z^{q+j} \\
&\quad + \cdots + b'z^q\big({}^{(z)}\alpha^i(a) + {}^{(z,u)}_{i}\delta_j(a)z^j + \cdots\big)\big)(1+b'z^q+c)^{-1} \\
&= \Bigg({}^{(z)}\alpha^i(a) + b'\,{}^{(z)}\alpha^{q+i}(a)z^q + {}^{(z)}\alpha^i(a)c + {}^{(z,u)}_{i}\delta_j(a)z^j \\
&\quad + \cdots + {}^{(z,u)}_{i}\delta_{q+j}(a)z^{q+j} \\
&\quad + \cdots + b'\sum_{k=1}^{q}\big({}^{(z)}\alpha^{q-k}\big({}^{(z,u)}\delta_j\big({}^{(z)}\alpha^{k+i-1}(a)\big)\big)\big)z^{q+j} \\
&\quad + b'\big({}^{(z)}\alpha^q\big({}^{(z,u)}_{i}\delta_j(a)\big)\big)z^{q+j} + \cdots\Bigg)(1+b'z^q+c)^{-1} \\
&= {}^{(z)}\alpha^i(a) + \Bigg({}^{(z,u)}_{i}\delta_j(a)z^j + \cdots + {}^{(z,u)}_{i}\delta_{q+j}(a)z^{q+j} \\
&\quad + \cdots + b'\sum_{k=1}^{q}\big({}^{(z)}\alpha^{q-k}\big({}^{(z,u)}\delta_j\big({}^{(z)}\alpha^{k+i-1}(a)\big)\big)\big)z^{q+j} \\
&\quad + b'\big({}^{(z)}\alpha^q\big({}^{(z,u)}_{i}\delta_j(a)\big)\big)z^{q+j} + \cdots\Bigg)(1-b'z^q-c+\cdots) \\
&= {}^{(z)}\alpha^i(a) + {}^{(z,u)}_{i}\delta_j(a)z^j + \cdots + {}^{(z,u)}_{i}\delta_{q+j}(a)z^{q+j} \\
&\quad + \cdots + b'\sum_{k=1}^{q}\big({}^{(z)}\alpha^{q-k}\big({}^{(z,u)}\delta_j\big({}^{(z)}\alpha^{k+i-1}(a)\big)\big)\big)z^{q+j} \\
&\quad + b'\big({}^{(z)}\alpha^q\big({}^{(z,u)}_{i}\delta_j(a)\big)\big)z^{q+j} + \cdots - {}^{(z,u)}_{i}\delta_j(a)\,{}^{(z)}\alpha^j(b')z^{q+j} + \cdots \\
&= {}^{(z)}\alpha^i(a) + \cdots + {}^{(z,u)}_{i}\delta_{q+j-1}(a)z'^{q+j-1} \\
&\quad + \Bigg({}^{(z,u)}_{i}\delta_{q+j}(a) + b'\,{}^{(z)}\alpha^q\big({}^{(z,u)}_{i}\delta_j(a)\big) - {}^{(z,u)}_{i}\delta_j(a)\,{}^{(z)}\alpha^j(b') \\
&\quad + b'\sum_{k=1}^{q}{}^{(z)}\alpha^{q-k}\big({}^{(z,u)}\delta_j\big({}^{(z)}\alpha^{k+i-1}(a)\big)\big) \\
&\quad - {}^{(z,u)}_{i}\delta_j(a)\sum_{k=0}^{j-1}{}^{(z)}\alpha^k(b)\Bigg)z'^{q+j} + \cdots,
\end{aligned}
$$

так как $z'^j = z^j + \sum_{k=0}^{j-1}{}^{(z)}\alpha^k(b)z^{q+j} + \cdots$.

iii) В этом случае выполняется

$$
\begin{aligned}
z'az'^{-1} = bzaz^{-1}b^{-1} &= {}^{(z)}\alpha(a) + b\,{}^{(z,u)}\delta_j(a)\,{}^{(z)}\alpha^j(b^{-1})z^j + \cdots \\
&= {}^{(z)}\alpha(a) + {}^{(z,u)}\delta_j(a)\,{}^{(z)}\alpha(b^{-1})\cdots{}^{(z)}\alpha^j(b^{-1})z'^j + \cdots,
\end{aligned}
$$

так как ${}^{(z')}\alpha\big|_{Z(\overline{D})} = {}^{(z)}\alpha\big|_{Z(\overline{D})}$.

Следствие 2. *В обозначениях леммы 3 имеет место равенство*

$$j = j(i) = w(xu(a)x^{-1} - u(a)),$$

*где $x \in D$ есть произвольный элемент с $w(x) = i$, если $a \in Z(\overline{D})$, $\alpha(a) = a$ и $(i,p) = 1$, где $p = \operatorname{char} D$.*

*Если $i = 1$, мы будем обозначать $j$ через $j(u,a)$ или $i(u,a)$.*

Доказательство. Так как для некоторого параметра $z$ выполняется

$$x = b(1 + x_1 z + \cdots)z^i,$$

где $b, x_k \in u(\overline{D})$, то следствие легко вытекает из доказательства п. ii) леммы 3.

В дальнейшем нам понадобится следующее определение.

Определение 4. Пусть $(\alpha, \beta)$ – некоторые эндоморфизмы алгебры с делением $D$. Отображение $\delta\colon D \to D'$, где $D \subset D'$ – некоторые алгебры, называется $(\alpha,\beta)$-*дифференцированием*, если оно линейно и удовлетворяет следующему условию:

$$\delta(ab) = \delta(a)\alpha(b) + \beta(a)\delta(b),$$

где $a, b \in D$.

Будем говорить, что $(\alpha, 1)$-дифференцирование есть $\alpha$-*дифференцирование.*

Лемма 4 (ср. [6; лемма 4]). *Пусть $\delta$ – $(\alpha,\beta)$-дифференцирование произвольной алгебры с делением $D$ такое, что $\alpha, \beta$ сохраняют $Z(D)$ и $\alpha\big|_{Z(D)} \neq \beta\big|_{Z(D)}$.*

*Тогда $\delta$ является внутренним дифференцированием, т.е. существует такой элемент $d \in D$, что*

$$\delta(a) = d\alpha(a) - \beta(a)d$$

*для всех $a \in D$.*

Доказательство. Положим $d = \delta(a)(a^\alpha - a^\beta)^{-1}$, где $a \in Z(D)$ – произвольный элемент такой, что $\alpha(a) \neq \beta(a)$. Положим $\delta_{\rm in}(x) = d\alpha(x) - \beta(x)d$. Мы утверждаем, что $\delta = \delta_{\rm in}$. Действительно, рассмотрим отображение $\overline{\delta} = \delta - \delta_{\rm in}$. Это $(\alpha,\beta)$-дифференцирование. Возьмем произвольный элемент $b \in D$. Тогда $\overline{\delta}(ab) = \overline{\delta}(ba)$. Но у нас

$$\overline{\delta}(ab) = \overline{\delta}(a)\alpha(b) + \beta(a)\overline{\delta}(b) = \beta(a)\overline{\delta}(b)$$

и

$$\overline{\delta}(ba) = \overline{\delta}(b)\alpha(a) + \beta(b)\overline{\delta}(a) = \alpha(a)\overline{\delta}(b).$$

Отсюда $\overline{\delta}(b) = 0$ для любого $b$.

Предложение 3 (ср. [6; лемма 10]). *Пусть $D$ – расщепимая алгебра с делением. Пусть $n = \mathrm{Gal}(Z(\overline{D})/\overline{Z(D)})$. Тогда существует параметр $z'$ такой, что*

$${}^{(z',u)}_{\ \ m}\delta_j = 0$$

*для произвольного $m$, если $n \nmid j$.*

Доказательство. Так как при $n=1$ утверждение в доказательстве не нуждается, предположим, что $n>1$. Пусть $z$ – некий фиксированный параметр. По [1; предложение 1.7] ${}^{(z)}\alpha\big|_{Z(\overline{D})}$ имеет порядок $n$.

По предложению 2 ${}^{(z,u)}\delta_1$ является $({}^{(z)}\alpha^2, {}^{(z)}\alpha)$-дифференцированием. Так как $n>1$, имеем ${}^{(z)}\alpha^2\big|_{Z(\overline{D})} \neq {}^{(z)}\alpha\big|_{Z(\overline{D})}$. Отсюда по лемме 4 ${}^{(z,u)}\delta_1$ – внутреннее дифференцирование и ${}^{(z,u)}\delta_1(a) = d\,{}^{(z)}\alpha^2(a) - {}^{(z)}\alpha(a)d$, $a \in \overline{D}$. Положим $z_1 = z - u(d)z^2$. По лемме 3,i) имеем, что для любого $a\in\overline{D}$ ${}^{(z_1,u)}\delta_1(a)=0$ и ${}^{(z)}\alpha(a) = {}^{(z_1)}\alpha(a)$. Следовательно, ${}^{(z_1,u)}\delta_1 = 0$ и ${}^{(z)}\alpha = {}^{(z_1)}\alpha$.

В силу предложения 2 ${}^{(z_1,u)}\delta_2$ есть $({}^{(z_1)}\alpha^3, {}^{(z_1)}\alpha)$-дифференцирование. Если $n\neq 2$, то оно внутреннее и мы можем применить лемму 3. Действуя по аналогии, получаем, что существует параметр $z_{n-1}$ такой, что ${}^{(z_{n-1},u)}\delta_j = 0$ для $j<n$ и ${}^{(z)}\alpha = {}^{(z_{n-1})}\alpha$. Легко видеть, что тогда ${}^{(z_{n-1},u)}_{\;m}\delta_j=0$ для $j<n$ и всех $m\in\mathbb{Z}$. Заметим, что ${}^{(z_{n-1},u)}\delta_n$ есть $({}^{(z_{n-1})}\alpha^{n+1}, {}^{(z_{n-1})}\alpha) = ({}^{(z_{n-1})}\alpha, {}^{(z_{n-1})}\alpha)$-дифференцирование, т.е. ${}^{(z_{n-1},u)}\delta_n\,{}^{(z_{n-1})}\alpha^{-1}$ – дифференцирование.

Заметим также, что ${}^{(z_{n-1},u)}\delta_{n+1}$ есть $({}^{(z_{n-1})}\alpha^2, {}^{(z_{n-1})}\alpha)$-дифференцирование. Это следует из предложения 2, так как ${}^{(z_{n-1},u)}_{\;m}\delta_j = 0$ для $j<n$ и всех $m\in\mathbb{Z}$. Следовательно, по лемме 4 ${}^{(z_{n-1},u)}\delta_{n+1}$ – внутреннее дифференцирование. Используя лемму 3,i) при $z_{n+1} = z_{n-1} + bz_{n-1}^{n+2}$ для соответствующего $b$, мы имеем, что ${}^{(z_{n+1},u)}\delta_j = 0$ для $j<n+2$, $n\nmid j$ и ${}^{(z)}\alpha = {}^{(z_{n+1})}\alpha$. Более того, ${}^{(z_{n+1},u)}_{\;m}\delta_j=0$ для $j<n+2$, $n\nmid j$ и всех $m\in\mathbb{Z}$. Это легко следует из леммы 2.

Предположим по индукции, что существует такой параметр $z_k$, что ${}^{(z_k,u)}_{\;m}\delta_j=0$ для $j<k+1$, $n\nmid j$ и всех $m\in\mathbb{Z}$ и ${}^{(z)}\alpha = {}^{(z_k)}\alpha$.

Следовательно, по предложению 2, если $n\nmid(k+1)$, имеем, что ${}^{(z_k,u)}\delta_{k+1}$ – внутреннее $({}^{(z_k)}\alpha^{k+2}, {}^{(z_k)}\alpha)$-дифференцирование. И если $n\mid(k+1)$, мы можем с помощью аналогичных рассуждений заключить, что ${}^{(z_k,u)}\delta_{k+2}$ есть $({}^{(z_k)}\alpha^{k+2}, {}^{(z_k)}\alpha)$-дифференцирование. Поэтому по лемме 3 существует параметр $z_{k+1} = z_k + bz_k^{k+2}$ ($z_k + bz_k^{k+3}$, если $n\mid(k+1)$) такой, что ${}^{(z_{k+1},u)}_{\;m}\delta_j = 0$ для $j<k+2$, $n\nmid j$ и всех $m\in\mathbb{Z}$ и ${}^{(z)}\alpha = {}^{(z_{k+1})}\alpha$ (или ${}^{(z_{k+1},u)}_{\;m}\delta_j=0$ для $j<k+3$, $n\nmid j$ и всех $m\in\mathbb{Z}$ и ${}^{(z)}\alpha = {}^{(z_{k+1})}\alpha$, если $n\mid(k+1)$).

Так как $z_{l+1} = (1+b_l z_l^{k_l})z_l$ для любого $l$, последовательность $\{z_l\}_{l=1}^{\infty}$ сходится в $D$, что завершает доказательство утверждения.

Лемма 5. *В ситуации предложения* 1 *пусть $D$ – расщепимая алгебра с делением характеристики $p>0$. Пусть $t\in Z(\overline{D})$ – такой элемент, что $\alpha(t)=t$.*

*Пусть $j=i(u,t)$ – минимальное положительное целое число такое, что ${}^{(z,u)}\delta_j\big|_{\mathbb{F}_p(t)} \neq 0$ (см. следствие 2), и предположим, что $j<\infty$. Тогда отображения ${}^{(z,u)}_{\;n}\delta_m$, $kj\leqslant m<(k+1)j$, $k\in\{1,\dots,p-1\}$, удовлетворяют следующим свойствам.*

i) *Существуют элементы $c_{n,m,k}\in\overline{D}$ такие, что*

$$ {}^{(z,u)}_{\;n}\delta_m\big|_{\mathbb{F}_p(t)} = c_{n,m,1}\delta + \dots + c_{n,m,k}\delta^k, $$

*где $\delta\colon \mathbb{F}_p(t)\to\mathbb{F}_p(t)$ – такое дифференцирование, что $\delta(t)=1$, и*

$$ c_{n,kj,k} = (k!)^{-1}\,{}^{(z,u)}_{\;n}\delta_j(t)\,{}^{(z,u)}_{\;n+j}\delta_j(t)\cdots{}^{(z,u)}_{\;n+(k-1)j}\delta_j(t). $$

ii) *Пусть* $\zeta = \operatorname{ord}({}^{(z)}\alpha\big|_{Z(\overline{D})})$. *Тогда* $\zeta \mid j$ *и* $c_{n,kj,k} \neq 0$, *если* $(n,j)=1$ *и* ${}^{(z)}\alpha({}^{(z,u)}\delta_j(t)) \neq {}^{(z,u)}\delta_j(t)$; $c_{n,kj,k} \neq 0$, *если* ${}^{(z)}\alpha({}^{(z,u)}\delta_j(t)) = {}^{(z,u)}\delta_j(t)$ *и* $n,(n+j),\dots,(n+(k-1)j) \neq 0 \pmod p$.

*Если* ${}^{(z)}\alpha = \mathrm{id}$, *то* $c_{n,kj,k} \neq 0$ *тогда и только тогда, когда* $n,(n+j),\dots,(n+(k-1)j) \neq 0 \pmod p$.

Доказательство. i) Доказываем по индукции по $k$. Пусть $a,b \in \mathbb{F}_p(t)$. Для $k=1$ по предложению 2, ii) имеем, что

$$ {}_n\delta_m(ab) = {}_n\delta_m(a)b + a\,{}_n\delta_m(b), $$

потому что все отображения $\delta_q$, $q<j$, равны на $\mathbb{F}_p(t)$ нулю. Отсюда ${}_n\delta_m$ – дифференцирование на $\mathbb{F}_p(t)$, ${}_n\delta_m\big|_{\mathbb{F}_p(t)} = c_{n,m,1}\delta$ и $c_{n,j,1} = {}_n\delta_j(t)$.

Для произвольного $k$ из предложения 2, i) и по предположению индукции имеем, что

$$ \begin{aligned} {}_n\delta_m(t^q) = q\,{}_n\delta_m(t)t^{q-1} & \\ &+ {}_n\delta_j(t)\biggl(\sum_{l=0}^{q-2}(c_{n+j,m-j,1}\delta + \dots + c_{n+j,m-j,k-1}\delta^{k-1})(t^{q-1-l})t^l\biggr) \\ &+ \dots + {}_n\delta_{m-j}(t)\biggl(\sum_{l=0}^{q-2}(c_{m-j+n,m-s,1}\delta)(t^{q-1-l})t^l\biggr). \end{aligned} \tag{2} $$

Следовательно, ${}_n\delta_m(t^p)=0$, потому что $k \leqslant p-1$ и $\sum_{l=0}^{p-2}\delta^i(t^{p-1-l})t^l = 0$ для $i \leqslant p-2$. Отсюда ${}_n\delta_m\big|_{\mathbb{F}_p(t)} = c_{n,m,1}\delta + \dots + c_{n,m,p-1}\delta^{p-1}$ и нам осталось только показать, что $c_{n,m,q}=0$ при $q>k$.

Используя формулу (2), мы можем вычислить $c_{n,m,j}$. Получаем

$$ \begin{aligned} c_{n,m,1} &= {}_n\delta_m(t), \\ c_{n,m,2} &= \frac{1}{2!}({}_n\delta_m(t^2) - 2c_{n,m,1}t) \\ &= \frac{1}{2}\bigl({}_n\delta_j(t)(c_{n+j,m-j,1}\delta(t)) + \dots + {}_n\delta_s(t)(c_{s+n,m-s,1}\delta(t))\bigr), \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ c_{n,m,q} &= \frac{1}{q!}\biggl({}_n\delta_j(t)\biggl(\sum_{l=0}^{q-2}c_{n+j,m-j,q-1}\delta^{q-1}(t^{q-1-l})t^l\biggr) \\ &\qquad + \dots + {}_n\delta_{m-(q-1)j}(t)\biggl(\sum_{l=0}^{q-2}c_{m+n-(q-1)j,(q-1)j,q-1}\delta^{q-1}(t^{q-1-l})t^l\biggr)\biggr) \\ &= \frac{1}{q}\bigl({}_n\delta_j(t)c_{n+j,m-j,q-1} + \dots + {}_n\delta_{m-(q-1)j}(t)c_{m+n-(q-1)j,(q-1)j,q-1}\bigr). \end{aligned} \tag{3} $$

Отсюда $c_{n,m,k+1} = \dots = c_{n,m,p-1} = 0$ и

$$ c_{n,kj,k} = q^{-1}\,{}_n\delta_j(t)c_{n+j,kj-j,k-1} = (k!)^{-1}\,{}^{(z,u)}_{n}\delta_j(t)\,{}^{(z,u)}_{n+j}\delta_j(t)\cdots{}^{(z,u)}_{n+(k-1)j}\delta_j(t). $$

ii) Сначала докажем, что $\zeta$ делит $i$. В случае, когда $i$ не делится на $\zeta$, по предложению 2 имеем, что

$$\begin{aligned} {}^{(z,u)}\delta_j(tx) &= {}^{(z,u)}\delta_j(t)\,{}^{(z)}\alpha^{j+1}(x) + {}^{(z)}\alpha(t){}^{(z,u)}\delta_j(x) = {}^{(z,u)}\delta_j(xt) \\ &= {}^{(z,u)}\delta_j(x)\,{}^{(z)}\alpha^{j+1}(t) + {}^{(z)}\alpha(x)\,{}^{(z,u)}\delta_j(t), \end{aligned}$$

где $x \in Z(\overline{D})$, $\alpha(x) \neq x$. Но тогда ${}^{(z)}\alpha^{j+1}(x) = {}^{(z)}\alpha(x)$. Противоречие.

Если ${}^{(z)}\alpha = \mathrm{id}$, аналогично получаем, что ${}^{(z,u)}\delta_j(t) \in Z(\overline{D})$.

Если $x \in \overline{D}$ – произвольный элемент, эти формулы показывают, что ${}^{(z)}\alpha^j$ есть внутренний автоморфизм $i_{{}^{(z,u)}\delta_j(t)^{-1}}$. Следовательно,

$${}^{(z)}\alpha^j({}^{(z,u)}\delta_j(t)) = {}^{(z,u)}\delta_j(t).$$

Предположим, что ${}^{(z)}\alpha({}^{(z,u)}\delta_j(t)) \neq {}^{(z,u)}\delta_j(t)$. Очевидно, что

$${}^{(z,u)}_{n+qj}\delta_j(t) = \sum_{l=0}^{n+qj-1} {}^{(z)}\alpha^l({}^{(z,u)}\delta_j(t)) \neq 0,$$

если $(n,j)=1$. Итак, в этом случае $c_{n,kj,k} \neq 0$ по i).

Если же ${}^{(z)}\alpha\bigl({}^{(z,u)}\delta_j(t)\bigr) = {}^{(z,u)}\delta_j(t)$, то ${}^{(z,u)}_{n+qj}\delta_j(t) = (n+qj)\,{}^{(z,u)}\delta_j(t) \neq 0$ тогда и только тогда, когда $p$ не является делителем $(n+qj)$. Следовательно, по i) $c_{n,kj,k} \neq 0$ в этом случае тогда и только тогда, когда $n, (n+j), \dots, (n+(k-1)j) \neq 0 \pmod p$.

Лемма доказана.

Лемма 6. *Пусть $D$ – расщепимая алгебра с делением, как в лемме 5. Пусть $s \in Z(\overline{D})$ – такой элемент, что $\alpha(s) = s$. Пусть $i = i(u,s)$ – минимальное положительное целое число такое, что ${}^{(z,u)}\delta_i(s) \neq 0$ (см. следствие 2).*

*Если $p \mid i$, то для любого целого положительного $k$ существует отображение ${}^{(z,u)}\delta_{j(k)}$ такое, что ${}^{(z,u)}\delta_{j(k)}(s^{p^k}) \neq 0$.*

Доказательство. Мы утверждаем, что ${}^{(z,u)}\delta_{p^q i}$ – первое такое отображение, что ${}^{(z,u)}\delta_{p^q i}\big|_{\mathbb{F}_p(s^{p^q})} \neq 0$. Доказательство проводим по индукции по $q$. Для $q=0$ утверждение в доказательстве не нуждается. Для произвольного $q$ положим $t = s^{p^{q-1}}$. По предложению 2 имеем

$$\begin{aligned} \delta_{p^q i}(t^p) &= \delta_{p^{q-1}i}(t) \sum_{r=0}^{p-2} {}_{1+p^{q-1}i}\delta_{p^{q-1}i(p-1)}(t^{p-1-r})t^r \\ &\quad + \sum_{l=p^{q-1}i+1}^{p^q i-1} \delta_l(t) \sum_{r=0}^{p-2} {}_{1+l}\delta_{p^q i-l}(t^{p-1-r})t^r. \end{aligned}$$

По индукции и лемме 5 ${}_{1+l}\delta_{p^q i-l}|_{\mathbb{F}_p(t)} = c_{1+l,p^q i-l,1}\delta + \dots + c_{1+l,p^q i-1,p-2}\delta^{p-2}$ для $l > p^{q-1}i$. Следовательно, $\sum_{r=0}^{p-2} {}_{1+l}\delta_{p^q i-l}(t^{p-1-r})t^r = 0$. По лемме 5,ii)

$$\begin{aligned}&{}_{1+p^{q-1}i}\delta_{p^{q-1}i(p-1)}|_{\mathbb{F}_p(t)}\\ &\qquad = c_{1+p^{q-1}i,p^{q-1}i(p-1),1}\delta + \dots + c_{1+p^{q-1}i,p^{q-1}i(p-1),p-1}\delta^{p-1},\end{aligned}$$

где $c_{1+p^{q-1}i,p^{q-1}i(p-1),p-1} \neq 0$. Отсюда

$$\delta_{p^q i}(t^p) = -c_{1+p^{q-1}i,p^{q-1}i(p-1),p-1}\delta_{p^{q-1}i}(t) \neq 0.$$

Аналогично получаем, что ${}^{(z,u)}\delta_j(t^p) = 0$ при $j < p^q i$. Итак, ${}^{(z,u)}\delta_{p^q i}$ есть первое ненулевое отображение на $\mathbb{F}_p(s^{p^q})$.

Лемма 7. *Пусть $D$ – расщепимая алгебра с делением. Пусть $z$ – фиксированный параметр и ${}^{(z)}\alpha = \mathrm{id}$, пусть $u$ – некоторое фиксированное вложение $u\colon \overline{D} \hookrightarrow D$.*

*Пусть ${}^{(z,u)}\delta_i$, $i \in \mathbb{N}\cup\infty$, – первое ненулевое отображение на $\overline{D}$. Предположим, что $(i,p) = 1$, где $p = \mathrm{char}\, D$. Пусть ${}^{(z,u)}\delta_j$, $j > i$, $j \in \mathbb{N}\cup\infty$, – первое отображение такое, что ${}^{(z,u)}\delta_j \neq 0$, если $j$ не делится на $i$, и ${}^{(z,u)}\delta_j \neq c_{j/i}{}^{(z,u)}\delta_i^{j/i}$ для некоторого $c_{j/i} \in \overline{D}$ в противном случае. Тогда*

a) *для $k < p = \mathrm{char}\, D$ ($k$ произвольное, если $\mathrm{char}\, D = 0$) имеем ${}^{(z,u)}\delta_{ki} = c_k{}^{(z,u)}\delta_i^k$, где*
$$c_k = \frac{(i+1)\cdots(i(k-1)+1)}{k!}, \tag{4}$$
*если $ki < j$;*

b) *если условие (4) верно для любого $k$ такого, что $ki < j$, то ${}^{(z,u)}_{-i}\delta_q = 0$ для $i < q < j$ и ${}^{(z,u)}_{-i}\delta_j$ – дифференцирование.*

Замечание. Число $i(u,z) = \min_{a\in\overline{D}}\{w(zu(a)z^{-1} - u(a))\}$, определенное в этой лемме, будем называть *локальной высотой*. Число $i = i(z,u)$ в лемме совпадает с уровнем $D$, определенном в [3], если индекс $D$ есть $p = \mathrm{char}\, D$ и $D$ расщепима. Как следует из лемм 3, 10 (см. ниже), $i(z,u)$ в этом случае не зависит от $z$, $u$. Следствие 2 завершает доказательство того факта, что $i$ совпадает с уровнем, определенным Салтманом, в случае расщепимой алгебры $D$. Это число будет играть важную роль в настоящей работе. Оно также было одним из основных параметров в [6]. Напомним определение *уровня*: $h(D) = \min_{a,b\in D}\{w(ab - ba) - w(a) - w(b)\}$.

Доказательство. Сравнивая коэффициенты в формуле для $\delta_{ki}(ab)$ из предложения 2 с коэффициентами в формуле для $\delta_i^k(ab)$, умноженных на $c_k$, получаем

$$c_k k = ((k-1)i + 1)c_{k-1},$$

откуда следует a).

С другой стороны, если ${}_{-i}\delta_q$, $q > i$, – первое ненулевое отображение после ${}_{-i}\delta_i$, то оно должно быть дифференцированием в силу предложения 2,i). Заметим, что в случае характеристики нуль это может иметь место, только если $q \geqslant j$, так как отображение $c\delta_i^k$ не может являться дифференцированием при $k > 1$, что в этом случае доказывает b).

Так как отображения $\delta_q$ однозначно определяются по лемме 2 отображениями $\widetilde{\delta}_l$, $l \leqslant q$, а отображения $\widetilde{\delta}_q$ однозначно определяются отображениями ${}_{-i}\delta_l$, $l \leqslant q$, и ${}_{-i}\delta_q$ являются линейными комбинациями $\delta_l$, $l \leqslant q$, с целыми коэффициентами, получаем, что b) имеет место в случае произвольной характеристики.

Замечание. Итак, мы видим, что отображения ${}_i\delta_q$ в этой лемме удовлетворяют тем же тождествам, что и $\delta_{q/i}$. Это может рассматриваться как возможная редукция с уровня $i$ до уровня 1.

Определение 5. Пусть $D$ – расщепимая алгебра с делением. Пусть $u$ – некоторое фиксированное вложение $u\colon \overline{D} \hookrightarrow D$. Пусть $s \in Z(\overline{D})$ – такой элемент, что $\alpha(s) = s$. Пусть $i = i(u,s)$ – такое минимальное положительное целое число, что ${}^{(z,u)}\delta_i(s) \neq 0$ (следствие 2 показывает, что $i$ не зависит от $z$). Предположим, что $(i,p) = 1$, где $p = \operatorname{char} D$. Определим

$$d(u,s) = \max_z \{w(z^{-i}u(s)z^i - u(s) - u({}^{(z,u)}_{-i}\delta_i(s))z^i)\} \in \mathbb{N} \cup \infty.$$

Легко заметить, что при некоторых условиях $d(u,s)$ можно интерпретировать как число $j$ из леммы 7, b) (т.е. это определение было мотивировано указанной леммой).

Лемма 8. *В предыдущем определении в случае, если $p = \operatorname{char} D > 0$ и ${}^{(z)}\alpha\big|_{Z(\overline{D})} = \mathrm{id}$, имеем*

i) $d(u,s) = 2i \pmod p$, *если* $d(u,s) < \infty$;

ii) *если* ${}^{(z,u)}_{-i}\delta_i(s) \neq 0$, *то для любого* $z$ *отображение* ${}^{(z,u)}_{-i}\delta_{d(u,s)+(p-1)i}$ *есть первое отображение такое, что* ${}^{(z,u)}_{-i}\delta_{d(u,s)+(p-1)i}(s^p) \neq 0$; *в частности, если* $d(u,s) = \infty$, *то* $[u(s^p), z^i] = 0$.

Доказательство. ii) Пусть ${}^{(z,u)}_{-i}\delta_\kappa$ – первое отображение такое, что

$${}^{(z,u)}_{-i}\delta_\kappa(s^p) \neq 0.$$

По следствию 2 $\kappa$ не зависит от $z$. По той же причине для любого $z$ ${}^{(z,u)}_{-i}\delta_i$ есть первое такое отображение, что ${}^{(z,u)}_{-i}\delta_i(s) \neq 0$.

Положим $w := d(u,s) + (p-1)i$ и зафиксируем $u, z$. Из предложения 2 получаем

$$\begin{aligned} {}_{-i}\delta_w(s^p) &= {}_{-i}\delta_{d(u,s)}(s) \sum_{q=0}^{p-2} {}_{d(u,s)-i}\delta_{(p-1)i}(s^{p-1-q})s^q \\ &\quad + \sum_{k=d(u,s)+1}^{w-1} {}_{-i}\delta_k(s) \sum_{q=0}^{p-2} {}_{k-i}\delta_{w-k}(s^{p-1-q})s^q. \end{aligned}$$

По лемме 5 ${}_{k-i}\delta_{w-k}\big|_{\mathbb{F}_p(s)} = c_{k-i,w-k,1}\delta + \dots + c_{k-i,w-k,p-2}\delta^{p-2}$ для $w - k < (p-1)i$ и ${}_{d(u,s)-i}\delta_{(p-1)i}\big|_{\mathbb{F}_p(s)} = c_{d(u,s)-i,(p-1)i,1}\delta + \dots + c_{d(u,s)-i,(p-1)i,p-1}\delta^{p-1}$

с $c_{d(u,s)-i,(p-1)i,p-1} \neq 0$, если $d(u,s)-i = i \pmod p$. Действительно, как было показано при доказательстве леммы 5,ii), $i$ должно делиться на порядок $n$ автоморфизма ${}^{(z)}\alpha$ на ${}^{(z,u)}\delta_i(s)$, поэтому $(n,p)=1$. Теперь возникают две возможности: $n \nmid d(u,s)$ и $n \mid d(u,s)$.

В первом случае, чтобы показать, что $c_{d(u,s)-i,(p-1)i,p-1} \neq 0$, мы можем повторить рассуждения из первого утверждения леммы 5,ii). Во втором случае имеем ${}_{d(u,s)-i+qi}\delta_i(s) = (d(u,s)-i+qi)/(i\,{}_i\delta_i(s)) \neq 0$, если $d(u,s)-i+qi$ не делится на $p$. Следовательно, по лемме 5,i) $c_{d(u,s)-i,(p-1)i,p-1} \neq 0$ тогда и только тогда, когда $d(u,s)-i = i \pmod p$.

Отсюда

$$ {}_{-i}\delta_w(s^p) = -{}_{-i}\delta_{d(u,s)}(s)c_{d(u,s)-i,(p-1)i,p-1} \neq 0, $$

если $d(u,s)-i = i \pmod p$.

Это также показывает, что ${}_{-i}\delta_w$ есть *первое* отображение такое, что

$$ {}_{-i}\delta_w\big|_{\mathbb{F}_p(s^p)} \neq 0, $$

если $d(u,s)-i = i \pmod p$.

i) По теореме Сколема–Нетёр существует такой параметр $z'$ в $D$, что ${}^{(z')}\alpha = \mathrm{id}$. Положим

$$ d'(u,z',s) = w(z'^{-j}u(s)z'^j - u(s) - u({}^{(z',u)}_{-i}\delta_i(s))z'^i). $$

Так как ${}^{(z')}\alpha = \mathrm{id}$, отображение ${}^{(z',u)}\delta_i$ является первым отображением таким, что ${}^{(z',u)}_{-i}\delta_i(s) \neq 0$. Если $d'(u,z',s) \neq 2i \pmod p$, мы можем найти такой параметр $z''$, что $d'(u,z'',s) > d'(u,z',s)$ (используя лемму 3,ii)). Продолжая эту процедуру, мы в конце концов найдем такой параметр $z$, что $d'(u,z,s) = 2i \pmod p$ либо $d'(u,z,s) = \infty$.

Используя рассуждения п. ii), получаем, что отображение ${}^{(z,u)}_{-i}\delta_{d'(u,z,s)+(p-1)i}$ является первым таким, что ${}^{(z,u)}_{-i}\delta_{d'(u,z,s)+(p-1)i}(s^p) \neq 0$ для параметра $z$. Как было замечено в начале доказательства, число $\kappa = d'(u,z,s)+(p-1)i$ не зависит от параметра. Так как $d'(u,z,s) \leqslant d(u,s)$, получаем, что $d'(u,z,s) = d(u,s)$. Иначе мы можем повторить рассуждения п. ii) и получить, что ${}^{(z,u)}_{-i}\delta_{d(u,s)+(p-1)i}(s^p) = 0$. Противоречие. Лемма доказана.

Было бы интересно узнать больше про поведение отображения ${}^{(z,u)}_{m}\delta_j$ относительно вложения $u$. Нами будет рассмотрен один специальный случай, а именно когда $\overline{D} = Z(\overline{D})$ и $Z(\overline{D})/\overline{Z(D)}$ – простое расширение.

Лемма 9. *Пусть $D$ – такая алгебра с делением, что* $\mathrm{char}\, D = p > 0$, $\overline{D} = Z(\overline{D})$, $Z(\overline{D})$ *– несовершенное поле, и пусть $Z(\overline{D})/\overline{Z(D)}$ – простое расширение (таким образом, $D$ расщепима). Пусть $\overline{u}$ – примитивный элемент расширения $Z(\overline{D})/\overline{Z(D)}$ такой, что $\overline{u} \notin (Z(\overline{D}))^p$, и пусть $u$ – произвольный подъем $\overline{u}$ в $D$.*

*Тогда существует такое вложение $u\colon \overline{D} \hookrightarrow D$, что $u(\overline{u}) = u$, и любое отображение ${}^{(z,u)}_{m}\delta_j$ однозначно определяется значениями ${}^{(z,u)}_{m}\delta_j(u^q)$, или, что эквивалентно, значениями ${}^{(z,u)}_{l}\delta_k(u)$, $k \leqslant j$.*

*В частности, если ${}^{(z,u)}_{m}\delta_k(u) = 0$ при $k \leqslant j$, то ${}^{(z,u)}_{m}\delta_j = 0$.*

Доказательство. Рассмотрим поле $Z(D)(u)$. Это также полное поле дискретного нормирования, так как оно есть конечное расширение $Z(D)$. По классической теореме Коэна существует вложение $\overline{Z(D)(u)} = \overline{D} \hookrightarrow Z(D)(u) \subset D$. По [8; леммы 11, 12] вложение полностью определяется $p$-базисом $\Gamma$ поля $\overline{Z(D)(u)}$. То есть для любого подъема $G$ данного $p$-базиса $\Gamma$ существует такое вложение $s$, что $G \subset s(\overline{Z(D)(u)})$.

Покажем, что существует такой $p$-базис $\Gamma$ поля $\overline{D}$, что $\overline{u} \in \Gamma$ и $\Gamma \ni \gamma \in \overline{Z(D)}$, если $\gamma \neq \overline{u}$.

Рассмотрим множество всех непустых множеств $\Gamma'$ элементов $\gamma_\tau \in \overline{D}$, удовлетворяющих следующему свойству:

A) $\overline{u} \in \Gamma'$, $\Gamma' \ni \gamma \in \overline{Z(D)}$, если $\gamma \neq \overline{u}$, и $[\overline{D}^p(\gamma_1, \dots, \gamma_r) : \overline{D}^p] = p^r$ для любых $r$ различных элементов из $\Gamma'$.

Это множество непусто, так как содержит множество $\Gamma' = \{\overline{u}\}$. По лемме Цорна существует некоторое максимальное множество $\Gamma$, $\Gamma' \subset \Gamma$, удовлетворяющее A). Тогда $\overline{D} = \overline{D}^p(\Gamma)$. Действительно, так как $\overline{Z(D)}^p(\overline{u}) \subset \overline{D}^p(\Gamma)$, нам достаточно показать, что любой элемент из $\overline{Z(D)}$ лежит в $\overline{D}^p(\Gamma)$. Предположим, $a \in \overline{Z(D)}$, $a \notin \overline{D}^p(\Gamma)$. Тогда множество $\Gamma' = \{a \cup \Gamma\}$ удовлетворяет A), что противоречит тому, что $\Gamma$ – максимальное множество.

Теперь мы можем выбрать подъем $\Gamma$ следующим образом. Возьмем $u$ в качестве подъема $\overline{u}$ и возьмем подъемы всех остальных элементов так, чтобы они лежали в $Z(D)$. Такой подъем определяет вложение $u\colon \overline{D} \hookrightarrow D$.

Покажем, что любое отображение ${}^{(z,u)}_{\ \ m}\delta_j$ (для некоторого фиксированного $z$) однозначно определяется значениями ${}^{(z,u)}_{\ \ l}\delta_k(u)$, $k \leqslant j$. Имеем, что $u(\overline{D}) = u(\overline{Z(D)})(u)$ и любой элемент $a \in u(\overline{D})$ может быть представлен как многочлен от конечного числа элементов из $\Gamma$ с коэффициентами из $u(\overline{D})^{p^k}$ для любого $k > 0$.

Заметим, что для любого $j$ существует $k > 0$ такое, что для любого $b \in \overline{Z(D)}^{p^k}$ ${}^{(z,u)}_{\ \ l}\delta_q(b) = 0$ для всех $q \leqslant j$ и всех $l$. Действительно, предположим, что ${}^{(z,u)}_{\ \ 1}\delta_q(b) \neq 0$ для некоторых $q \leqslant j$, $b \in \overline{Z(D)}^{p^k}$ и ${}^{(z,u)}_{\ \ l}\delta_s(c) = 0$ для всех $l$, всех $c \in \overline{Z(D)}^{p^k}$ и всех $s < q$. Тогда ввиду ${}^{(z)}\alpha|_{\overline{Z(D)}} = \mathrm{id}$ и по предложению 2 ${}^{(z,u)}_{\ \ l}\delta_s(b^p) = 0$ для всех $b \in \overline{Z(D)}^{p^k}$, всех $l$ и всех $s \leqslant q$.

Далее, так как $u(\overline{D})^{p^k} = u(\overline{Z(D)})^{p^k}(u^{p^k})$, то любой элемент $a \in u(\overline{D})$ может быть представлен в виде многочлена от конечного числа элементов из $\Gamma$ с коэффициентами из $u(\overline{Z(D)})^{p^k}$. Так как все, кроме $u$, элементы из $\Gamma$ принадлежат центру $Z(D)$, то значение ${}^{(z,u)}_{\ \ m}\delta_j(a)$ однозначно определяется значениями ${}^{(z,u)}_{\ \ m}\delta_j(u^l)$, которые, в свою очередь, по предложению 2 однозначно определяются величинами ${}^{(z,u)}_{\ \ l}\delta_k(u)$, $k \leqslant j$.

Замечание. В случае совершенного поля $Z(\overline{D})$ существует единственное вложение $u$, согласованное с вложением $\overline{Z(D)} \hookrightarrow Z(D)$. Таким образом, утверждение леммы в этом случае очевидно.

Лемма 10 (ср. [6; лемма 8]). *В ситуации леммы 9 предположим, что* ${}^{(z,u)}_{\ \ m}\delta_1 = \dots = {}^{(z,u)}_{\ \ m}\delta_{j-1} = 0$, ${}^{(z,u)}_{\ \ m}\delta_j \neq 0$. *Пусть $n$ – порядок* ${}^{(z)}\alpha$. *Справедливо следующее.*

i) *Для* $u'=u+bz^q$, $b\in u(\overline{D})$, $n\mid q$, *имеем* ${}^{(z,u')}_{\ \ m}\delta_l={}^{(z,u)}_{\ \ m}\delta_l$, $l<q$, *и*

$${}^{(z,u')}_{\ \ m}\delta_q(\overline{u})={}^{(z,u)}_{\ \ m}\delta_q(\overline{u})+{}^{(z)}\alpha^m(\overline{b})-\frac{\partial}{\partial\overline{u}}\big({}^{(z)}\alpha^m(\overline{u})\big)\overline{b},$$

*где производная берется в поле* $\overline{D}=\overline{D}^p(\Gamma)$.

ii) *Пусть* ${}^{(z)}\alpha=\mathrm{id}$. *Тогда для* $u'=u+bz^q$, $b\in u(\overline{D})$, *имеем* ${}^{(z,u')}_{\ \ m}\delta_l={}^{(z,u)}_{\ \ m}\delta_l$, $l<q+j$, *и*

$${}^{(z,u')}_{\ \ m}\delta_{q+j}(\overline{u})={}^{(z,u)}_{\ \ m}\delta_{q+j}(\overline{u})+{}^{(z,u)}_{\ \ m}\delta_j(\overline{b})-\frac{\partial}{\partial\overline{u}}\big({}^{(z,u)}_{\ \ m}\delta_j(\overline{u})\big)\overline{b},$$

*где производная берется в поле* $\overline{D}=\overline{D}^p(\Gamma)$.

iii) *Пусть* ${}^{(z)}\alpha=\mathrm{id}$. *Пусть* $\overline{u'}\in\overline{D}$ *– произвольный примитивный элемент расширения* $\overline{D}/\overline{Z(D)}$, *удовлетворяющий условиям леммы* 9, *и пусть* $u'\in D$ *– произвольный подъем* $\overline{u'}$. *Тогда имеем* ${}^{(z,u')}_{\ \ m}\delta_l={}^{(z,u)}_{\ \ m}\delta_l$, $l<j$, *и*

$${}^{(z,u')}_{\ \ m}\delta_j(\,\overline{u'}\,)={}^{(z,u)}_{\ \ m}\delta_j(\overline{u})\frac{\partial}{\partial\overline{u}}(\,\overline{u'}\,),$$

*где производная берется в поле* $\overline{D}=\overline{D}^p(\Gamma)$.

Доказательство. Во-первых, заметим, что существует такое $k\in\mathbb{N}$, что для любого $a\in\overline{Z(D)}^{p^k}$ выполняется $u(a)-u'(a)=0 \pmod{M_D^{q+1}}$, где $u'$ – другое вложение, $q\in\mathbb{N}$ – произвольное заданное число.

Действительно, предположим, что для любого $c\in\overline{Z(D)}^{p^s}$ выполняется $u(c)-u'(c)=0 \pmod{M_D^l}$, т.е. $u(c)=u'(c)+c_lz^l+\cdots$, где $c_l\in u'(\overline{D})$. Тогда $u(c^p)=(u(c))^p=(u'(c))^p+pu'(c)^{p-1}c_lz^l+\cdots$ и $u(c^p)-u'(c^p)=0 \pmod{M_D^{l+1}}$.

Отсюда сразу следует, что $u(a)-u'(a)=0 \pmod{M_D^q}$ для любого $a\in\overline{D}$, если $u'$ определяется элементом $u'=u+bz^q$, потому что $u(\overline{u})-u'(\overline{u})=bz^q$. Более того, если мы представим $a$ в форме некоторого многочлена $P(\gamma_1,\ldots,\gamma_r,\overline{u})$ с коэффициентами из $\overline{Z(D)}^{p^k}$, то станет ясно, что

$$(u(a)-u'(a))z^{-q}=-\frac{\partial}{\partial\overline{u}}(P(\gamma_1,\ldots,\gamma_r,\overline{u}))\overline{b}\pmod{M_D},$$

если $n\mid q$, так как $u(\gamma_l)=u'(\gamma_l)$ для любого $l$ и $z^quz^{-q}=u \pmod{M_D}$. Также ясно, что производную можно брать даже в поле $\overline{D}^p(\Gamma)$. Следовательно, получаем i)

$$\begin{aligned}
z^mu'z^{-m}&=z^m(u+bz^q)z^{-m}\\
&=u\big({}^{(z)}\alpha^m(\overline{u})\big)+u\big({}^{(z,u)}_{\ \ m}\delta_j(\overline{u})\big)z^j+\cdots+\big(u({}^{(z)}\alpha^m(\overline{b}))+u\big({}^{(z,u)}_{\ \ m}\delta_j(\overline{b})\big)z^j+\cdots\big)z^q\\
&=u\big({}^{(z)}\alpha^m(\overline{u})\big)+\cdots+\big(u\big({}^{(z,u)}\delta_q(\overline{u})\big)+u\big({}^{(z)}\alpha^m(\overline{b})\big)\big)z^q+\cdots\\
&=u'\big({}^{(z)}\alpha^m(\overline{u})\big)+\cdots+\Bigg(u'\big({}^{(z,u)}_{\ \ m}\delta_q(\overline{u})\big)+u'\big({}^{(z)}\alpha^m(\overline{b})\big)\\
&\quad-u'\left(\frac{\partial}{\partial\overline{u}}{}^{(z)}\alpha^m(\overline{u})\overline{b}\right)\Bigg)z^q+\cdots.
\end{aligned}$$

ii) Здесь мы имеем, что

$$
\begin{aligned}
z^m u' z^{-m} &= z^m(u+bz^q)z^{-m} \\
&= u(\overline{u}) + u\big({}^{(z,u)}_{\ m}\delta_j(\overline{u})\big)z^j + \cdots + \big(u(\overline{b}) + u\big({}^{(z,u)}_{\ m}\delta_j(\overline{b})\big)z^j + \cdots\big)z^q \\
&= u(\overline{u}) + u\big({}^{(z,u)}_{\ m}\delta_j(\overline{u})\big)z^j + \cdots + \big(u\big({}^{(z,u)}_{\ m}\delta_q(\overline{u})\big) + u(\overline{b})\big)z^q + u\big({}^{(z,u)}_{\ m}\delta_{q+1}(\overline{u})\big)z^{q+1} \\
&\quad + \cdots + u\big({}^{(z,u)}_{\ m}\delta_{q+j-1}(\overline{u})\big)z^{q+j-1} \\
&\quad + \big(u\big({}^{(z,u)}_{\ m}\delta_{q+j}(\overline{u})\big) + u\big({}^{(z,u)}_{\ m}\delta_j(\overline{b})\big)\big)z^{q+j} + \cdots \\
&= u'(\overline{u}) + u'\big({}^{(z,u)}_{\ m}\delta_j(\overline{u})\big)z^j + \cdots + u'\big({}^{(z,u)}_{\ m}\delta_{q+j-1}(\overline{u})\big)z^{q+j-1} \\
&\quad + \left(u'\big({}^{(z,u)}_{\ m}\delta_{q+j}(\overline{u})\big) + u'\big({}^{(z,u)}_{\ m}\delta_j(\overline{b})\big) - u'\left(\frac{\partial}{\partial\overline{u}}\big({}^{(z,u)}_{\ m}\delta_j(\overline{u})\big)\overline{b}\right)\right)z^{q+j} + \cdots .
\end{aligned}
$$

iii) Пусть $u' = u(\,\overline{u'}\,) + a_1 z + \cdots$, где $a_i \in u(\overline{D})$. Так как согласно предложению 2 отображение ${}^{(z,u)}_{\ m}\delta_j$ является дифференцированием, то

$$
\begin{aligned}
z^m u' z^{-m} &= \big(u(\,\overline{u'}\,) + u\big({}^{(z,u)}_{\ m}\delta_j(\,\overline{u'}\,)\big)z^j + \cdots\big) \\
&\quad + \big(a_1 + u\big({}^{(z,u)}_{\ m}\delta_j(a_1)\big)z^j + \cdots\big)z + \cdots \\
&= u' + u\big({}^{(z,u)}_{\ m}\delta_j(\,\overline{u'}\,)\big)z^j + \cdots = u' + u\left({}^{(z,u)}_{\ m}\delta_j(\overline{u})\frac{\partial}{\partial\overline{u}}(\,\overline{u'}\,)\right)z^j + \cdots \\
&= u' + u'\left({}^{(z,u)}_{\ m}\delta_j(\overline{u})\frac{\partial}{\partial\overline{u}}(\,\overline{u'}\,)\right)z^j + \cdots .
\end{aligned}
$$

## § 4. Гипотеза о периоде и индексе

В этом параграфе мы докажем следующую теорему.

Теорема 2. *Гипотеза о том, что для произвольной алгебры с делением $A$ над $C_2$-полем $F$ экспонента $A$ равна ее индексу, верна для $F = F_1((t))$, где $F_1$ – произвольное $C_1$-поле.*

Напомним, что поле $F$ называется *$C_i$-полем*, если всякий однородный многочлен $f(x_1,\dots,x_n)$ степени $d$ от $n > d^i$ переменных с коэффициентами в $F$ представляет (нетривиально) нуль в поле $F$. Некоторые основные свойства $C_i$-полей можно найти, например, в [2].

Эта гипотеза была выдвинута М. Артином и была решена для некоторых других примеров поля $F$ большим числом авторов. Насколько известно автору, положительный ответ для всех алгебр с делением индекса $\operatorname{ind} A = 2^a 3^b$ над произвольным $C_2$-полем был дан в [2], для алгебр с делением над полем $F = k((X))((Y))$, где $k$ – совершенное поле характеристики $p \neq 0$ такое, что $\dim_{\mathbb{F}_p} k/\wp(k) = 1$, был дан Тиньолем в приложении к [9], для алгебр с делением взаимно простого с характеристикой поля $F$ индекса, где $F$ – поле функций поверхности, был дан в [10]. Кажется, что справедливость гипотезы была также известна для алгебр с делением над полем $F = F_1((t))$ характеристики 0. Здесь мы дадим доказательство теоремы для произвольной характеристики.

Доказательство. 1) Напомним, что любое конечное расширение $C_1$-поля является простым. Действительно, предположим, что $E = F_1(u_1, \dots, u_r)$, $r \geqslant 2$. Рассмотрим поле $K = F_1(u_1^p, \dots, u_r^p)$. По теореме Тзена $K$ и $E$ являются $C_1$-полями. Следовательно, форма $x_1^p + x_2^p u_1 + \dots + x_p^p u_1^{p-1} + x_{p+1}^p u_2$ представляет нетривиально нуль в $E$. Но $x_i^p \in K$ и элементы $1, u_1, \dots, u_1^{p-1}, u_2$ линейно независимы над $K$. Противоречие.

2) Предположим, что теорема верна для случая, когда экспонента – простое число. Мы докажем теорему индукцией по $e = \exp A$. Если $e$ – не простое число, то будем писать $e = lm$. По предположению индукции $A^{\otimes m}$ расщепляется расширением $F \subset F'$ поля $F$ степени $l$. Следовательно, экспонента $A_{F'}$ является делителем $m$. Заметим, что $F'$ является также полем лорановских степенных рядов. Применяя предположение индукции к паре $(F', A_{F'})$, получаем, что существует расширение $F' \subset L$ поля $F'$ степени, являющейся делителем $m$, расщепляющее $A_{F'}$. Следовательно, $A$ расщепляется расширением $F \subset L$ степени, являющейся делителем $lm$, и мы получаем утверждение теоремы.

3) Итак, пусть $\exp A = l$ – простое число. По основным свойствам экспоненты и индекса (см., например, [2]) получаем, что $\operatorname{ind} A = l^k$ для некоторого натурального $k$.

Предположим, что $(l, p = \operatorname{char} F) = 1$.

Известно, что гипотеза верна для всех алгебр с делением индекса $\operatorname{ind} A = 2^a 3^b$, поэтому мы можем положить $l \neq 2, 3$. Можем предположить также, что $F$ содержит группу $\mu_l$ корней из единицы степени $l$, так как $[F(\mu_l) : F] < l$, и мы можем, таким образом, свести задачу к алгебре $A \otimes_F F(\mu_l)$. Тогда по теореме Меркурьева–Суслина $A$ подобна тензорному произведению символ-алгебр индекса $l$.

Чтобы получить утверждение теоремы, достаточно доказать, что любые две символ-алгебры $A_1$, $A_2$ содержат $F$-изоморфные максимальные подполя.

Так как любая алгебра с делением над $C_1$-полем тривиальна и любое расширение этого поля простое, то каждая символ-алгебра индекса $l$ над $F$ расщепима. Ввиду того, что $(l, p) = 1$, она хорошо расщепима, и ее поле вычетов есть циклическое расширение поля $\overline{F}$. Следовательно, если $z_i$ – параметр из предложения 3 алгебры $A_i$, то $z_i$ ведет себя на $\overline{A}_i$ как автоморфизм Галуа, и $z_i^l \in F$. Имеем тогда $v(z_i^l) = 1$ (напомним, что $v$ – нормирование на $F$).

Покажем, что $A_1$ содержит корень степени $l$ из любого элемента $u$ в $F$ с $v(u) \neq 0$. Из этого следует, что $A_1$ должна содержать подполе, изоморфное $F(z_2)$. Ввиду того, что для любого элемента $1 + b$, $v(b) > 0$, существует корень степени $l$ $(1+b)^{1/l} \in F$, достаточно показать, что $A_1$ содержит корень степени $l$ из любых элементов вида $ct$, где $c \in u(\overline{F})$, $u$ – некое фиксированное вложение $u\colon \overline{A}_1 \hookrightarrow A_1$.

Положим $z_1^l = c_1 t$, $c_1 \in u(\overline{F})$. Заметим, что для любого элемента $b \in u(\overline{A}_1)$ выполняется $(bz_1)^l = u(N_{\overline{A}_1/\overline{F}}(b)) z_1^l$. Но отображение нормы $N_{\overline{A}_1/\overline{F}}$ сюръективно, так как $\overline{F}$ является $C_1$-полем (см., например, [2; 3.4.2]), поэтому существует такое $b$, что $(bz)^l = ct$.

4) Предположим теперь, что $\exp A = p$. Тогда $\operatorname{ind} A = p^k$.

По теореме Алберта [11] существует поле $F' = F(u_1^{1/p}, \dots, u_k^{1/p})$, расщепляющее $A$. Такими же рассуждениями, что и в п. 1), можно показать, что каждое такое поле имеет максимум два порождающих, скажем $F' = F(u_1^{1/p}, u_2^{1/p})$. Следовательно, $\operatorname{ind} A \leqslant p^2$. Если $\operatorname{ind} A = p$, утверждение не требует доказательства, поэтому можно считать, что $\operatorname{ind} A = p^2$ и $F'$ есть максимальное подполе в $A$.

5) Предположим, что $F_1$ – совершенное поле.

По теореме Алберта $A \cong A_1 \otimes_F A_2$, где $A_1, A_2$ – циклические алгебры степени $p$, $A_1 = (L_1/F, \sigma_1, u_1)$, $A_2 = (L_2/F, \sigma_2, u_2)$. Так как $F_1$ – совершенное поле , то $\overline{A}_1/\overline{F}$, $\overline{A}_2/\overline{F}$ – расширения Галуа. Следовательно, $A_1$, $A_2$ хорошо расщепимы. Покажем теперь, что $A_1$, $A_2$ имеют общее расщепляющее поле степени $p$ над $F$. Это ведет к противоречию.

Согласно предложению 3 существуют параметры $z_1 \in A_1$, $z_2 \in A_2$, ведущие себя на $\overline{A}_1$, $\overline{A}_2$ как автоморфизмы Галуа. Заметим, что $z_1^p, z_2^p \in F$, и покажем, что $F(z_1)$ расщепляет $A_2$.

Рассмотрим централизатор $D = C_A(F(z_1))$ и элемент $t_1 = z_2 z_1^{-1}$. Имеем, что $t_1^p \in F$, $w(t_1) = 0$ (напомним, что под $w$ понимается единственное продолжение нормирования $v$ на $F$). Так как $\overline{D}/\overline{Z(D)}$ – расширение Галуа, то существует такой элемент $b_1 \in F$, что $w(t_1 - b_1) > 0$. Ввиду того, что $(t_1 - b_1)^p \in F$, существует натуральное $k_1$ такое, что $w((t_1 - b_1)z_1^{-k_1}) = 0$. Обозначим $t_2 = (t_1 - b_1)z_1^{-k_1}$. Тогда опять получается, что $t_2^p \in F$. Повторяя рассуждения и используя свойство полноты тела $D \subset A$, получаем

$$z_2 = t_1 z_1 = (t_2 z_1^{k_1} + b_1) z_1 = \cdots = b_1 z_1 + b_2 z_1^{k_1+1} + \cdots ,$$

следовательно, $z_2 \in F(z_1) = Z(D)$.

6) Предположим, что $F_1$ несовершенно.

Так как $F'$ порождается двумя элементами над $F$, оно содержит все корни степени $p$ поля $F$. Тогда любые два элемента $u, z \in F$ такие, что $z^{1/p} \notin F(u^{1/p})$, где $z^{1/p}, u^{1/p} \in F'$, также порождают $F'$ над $F$. Это доказывается такими же рассуждениями, как и в пп. 1), 4).

Теперь возьмем $u \in F_1 \setminus F_1^p$, $z = u + t$. Ясно, что корни степени $p$ из этих элементов порождают $F'$ над $F$. Более того, поля $F(u^{1/p})$, $F(z^{1/p})$ являются *“неразветвленными”* над $F$, т.е.

$$[\overline{F(u^{1/p})} : \overline{F}] = p = [F(u^{1/p}) : F], \qquad [\overline{F(z^{1/p})} : \overline{F}] = p.$$

Обозначим $u_1 = u^{1/p}$, $u_2 = z^{1/p}$ в $F'$. Тогда по теореме Алберта $A \cong A_1 \otimes_F A_2$, где $A_1$, $A_2$ – циклические алгебры степени $p$, $A_1 = (L_1/F, \sigma_1, u)$, $A_2 = (L_2/F, \sigma_2, z)$.

Рассмотрим централизатор $D = C_A(F(u_1))$. Предположим, что $\overline{D}/\overline{Z(D)}$ есть сепарабельное расширение. Тогда существует подъем $u\colon \overline{D} \hookrightarrow D$ произвольного вложения $u'\colon \overline{F(u_1)} \hookrightarrow F(u_1)$. Рассмотрим вложение $u' = u_1$, определенное в лемме 9. Так как $F(u_1)/F$ есть чисто несепарабельное расширение, то $u'$ – хорошее вложение и $u$ – хорошее вложение $\overline{D} = \overline{A}$ в $D \subset A$. Отсюда получаем, что $A$ – хорошо расщепимая алгебра и $u(\overline{A})$ содержит чисто несепарабельный над $F$ элемент. Но это противоречит лемме 6. Следовательно, $\overline{A}/\overline{F}$ не может содержать сепарабельного подрасширения, потому что в этом случае сепарабельное расширение должно существовать у $\overline{D}/\overline{Z(D)}$.

Теперь, для краткости, применим леммы A.4, A.6 Тиньоля из приложения к статье [9]. Эти леммы говорят о том, что тензорное произведение $A_1 \otimes A_2$ любых двух символов $A_1$, $A_2$ подобно либо одному символу в группе $\operatorname{Br}(F)$ (и в этом случае теорема доказана), либо произведению двух символов уровня нуль. Напомним, что из результатов Салтмана в [3] следует, что любая алгебра с делением уровня нуль является ручной, что в нашем случае означает, что тело вычетов есть сепарабельное расширение над $\overline{F}$. Определение уровня уже обсуждалось выше в замечании к лемме 7.

Итак, пусть $A \sim D_1 \otimes D_2$, где $D_1$, $D_2$ – ручные алгебры с делением степени $p$ над $F$. Мы можем считать, что $A$, $D_1 \otimes D_2$ – тела. Тогда $A \cong D_1 \otimes D_2$. Так как $D_1$, $D_2$ ручные, заключаем, что поле $\overline{A}$ должно содержать сепарабельный элемент, что ведет к противоречию.

Теорема доказана.

## § 5. Хорошо расщепимые алгебры

В этом параграфе мы докажем теорему о разложении для хорошо расщепимых алгебр с делением. Эта теорема показывает, как изучение хорошо расщепимых алгебр с делением может быть сведено к изучению алгебр с делением с просто описываемой структурой. Таким образом, хорошо расщепимые алгебры являются наиболее простыми и удобными в изучении алгебрами.

Лемма 11. *Пусть $D$ – хорошо расщепимая алгебра с делением, $F = Z(D)$, и пусть $Z(\overline{D}) = \overline{F}(s)$ – чисто несепарабельное над $\overline{F}$ поле степени $p = \operatorname{char} D > 0$. Пусть $u\colon \overline{D} \hookrightarrow D$ – хорошее вложение.*

*Тогда существует такой параметр $z$, что ${}^{(z,u)}_{-i}\delta_j = 0$ при $j > i$, где $i = i(z,u)$ – локальная высота, и $u({}^{(z,u)}\delta_i(s)) = x$, где $x \in Z(D)$. Более того, $(i,p) = 1$.*

Доказательство. Так как $Z(\overline{D})/\overline{F}$ – чисто несепарабельное расширение, то ${}^{(z)}\alpha\big|_{Z(\overline{D})} = \mathrm{id}$ для любого параметра $z$. По теореме Сколема–Нётер существует такой параметр $z$ в $D$, что ${}^{(z)}\alpha = \mathrm{id}$. Предположим, что ${}^{(z,u)}\delta_i(s) = 0$, где $i = i(z,u)$. Тогда ${}^{(z,u)}\delta_i\big|_{Z(\overline{D})} = 0$, так как $u$ – хорошее вложение и $Z(\overline{D})/\overline{F}$ – простое расширение. Следовательно, по теореме Сколема–Нётер ${}^{(z,u)}\delta_i$ – внутреннее дифференцирование, и по лемме 3,i) существует такой параметр $z'$, что ${}^{(z',u)}\delta_i = 0$, ${}^{(z')}\alpha = \mathrm{id}$.

Следовательно, мы можем предположить, что ${}^{(z,u)}\delta_i(s) \neq 0$ для некоторого параметра $z$. Так как $s^p \in Z(D)$, то по лемме 6 имеем $(i,p) = 1$. Ввиду того, что ${}^{(z,u)}\delta_i$ – дифференцирование, имеем ${}^{(z,u)}\delta_i(s) \in Z(\overline{D})$ (см. рассуждения при доказательстве леммы 5,ii)). Так как $(i,p) = 1$, существует такое $k$, что $p \mid (1 - ki)$. Следовательно, по лемме 3,iii) для параметра $z' = ({}^{(z,u)}\delta_i(s))^k$ имеем ${}^{(z')}\alpha = \mathrm{id}$, ${}^{(z',u)}\delta_i(s) \in \overline{F}$, т.е. $u({}^{(z',u)}\delta_i(s)) \in Z(D)$. Так как $s^p \in Z(D)$, по лемме 8 должно выполняться $d(u,s) = \infty$. При доказательстве леммы 8,i) было показано, что $d(u,s) = d'(u,z,s)$ для некоторого параметра $z$, и конструкция этого элемента использует лемму 3,ii), что гарантирует, что начальные значения ${}^{(z')}\alpha$, ${}^{(z',u)}\delta_i$ сохраняются. Следовательно, ${}^{(z,u)}_{-i}\delta_j = 0$ для $j > i$, и лемма доказана.

Предложение 4. *Пусть $D$ – расщепимая алгебра с делением. Тогда имеем $D \cong D_1 \otimes_F D_2$, где $D_1$, $D_2$ – расщепимые алгебры с делением и $D_1$ – инерциально расщепимая алгебра.*

*Если $D$ – хорошо расщепимая алгебра с делением, то $Z(\overline{D}_2)/\overline{F}$ – чисто несепарабельное расширение и $D_2$ – хорошо расщепимая алгебра ($D_1$ или $D_2$ могут быть тривиальными).*

*Следовательно, $D \sim A \otimes_F B \otimes_F D_2$, где $A$ – циклическая алгебра с делением и $B$ – неразветвленная алгебра с делением.*

Доказательство. Если $\operatorname{char} D = 0$, то утверждение очевидно, поэтому будем считать, что $\operatorname{char} D > 0$.

По [12; с. 261] имеем $D \cong D_1 \otimes_F \cdots \otimes_F D_k$, где $[D : F] = p_1^{r_1} \cdots p_k^{r_k}$ и $[D_i : F] = p_i^{r_i}$. Пусть $p_2 = p$. Так как $D_i$ бездефектны над $F$, то $D_1, D_3, \dots, D_k$ инерциально расщепимы. Следовательно, по теореме 1 алгебра $B = D_1 \otimes D_3 \otimes \cdots \otimes D_k$ хорошо расщепима.

Предположим сначала, что $D$ хорошо расщепима. По предложению 1.7 из [1], если $s \in Z(\overline{D})$ – такой элемент, что $\alpha(s) = s$, то это чисто несепарабельный элемент над $\overline{F}$. Следовательно, если $D$ – хорошо расщепимая алгебра с делением, то по лемме 6 либо $D_2$ является инерциально расщепимой алгеброй, либо $Z(\overline{D}_2)/\overline{F}$ – чисто несепарабельное расширение. Действительно, в противном случае существует описанный выше элемент $s \in Z(\overline{D}_2) \subset Z(\overline{D})$, и в силу предложения 3 $p \mid i(u, s)$ для любого вложения $u$. Если $u$ – хорошее вложение, то $s^{p^k} \in Z(D)$ для некоторого $k$. Противоречие.

Итак, ниже будем предполагать $Z(\overline{D}_2)/\overline{F}$ чисто несепарабельным расширением. Тогда имеем (см., например, [13; теорема 1]), что $\overline{D} \cong \overline{D}_2 \otimes_{\overline{F}} \overline{B}$, и поэтому $u(\overline{D}) \cong u(\overline{D}_2) \otimes_{u(\overline{F})} u(\overline{B})$, где $u$ – хорошее вложение. Следовательно, $E = u(Z(\overline{D}_2))$ – чисто несепарабельное поле над $u(\overline{F}) \subset Z(D)$.

Рассмотрим поле $E' = u(K) \otimes_{u(\overline{F})} F$, где $K$ – некоторое максимальное сепарабельное подполе в $\overline{B}$. Это неразветвленный подъем поля $K$ в $D$. Рассмотрим централизатор $C = C_D(E') \cong D_2 \otimes_F E'$. Пусть $M$ – некоторое максимальное подполе в $\overline{D}_2$. Заметим, что $u(\overline{D}_2) \subset C$, т.е. $L \subset C$, где $L = u(M)F$ – композит $u(M)$ и $F$, и $E \subset L$. Заметим также, что $[L : F] = \operatorname{ind} D_2 = \operatorname{ind} C$. Поле $L$ расщепляет $C$ из соображений размерности. Следовательно, оно должно расщеплять и $D_2$, так как $([E' : F], p) = 1$ и $D_2$ – $p$-алгебра. Отсюда $L$ изоморфно максимальному подполю в $D_2$, значит, $D_2$ содержит копию чисто несепарабельного "неразветвленного" подполя, поле вычетов которого изоморфно $Z(\overline{D}_2)$. Следовательно, $D_2$ – хорошо расщепимая алгебра. Действительно, централизатором этого поля является неразветвленная алгебра с делением, поэтому по теореме 1 он расщепим. Отсюда следует, что $D_2$ хорошо расщепима, если чисто несепарабельное поле хорошо расщепимо. Оно же, в свою очередь, хорошо расщепимо, потому что содержит подполе, изоморфное $u(Z(\overline{D}_2))$ по построению. (Это можно увидеть и другим путем, используя рассуждения леммы 9, чтобы показать, что существует подходящий $p$-базис.)

Пусть $D$ – расщепимая алгебра. Тогда такими же рассуждениями, что и в предыдущем абзаце, можно показать, что $L$ изоморфно максимальному подполю в $D_2$ (не имеет значения, что $Z(\overline{D}_2)/\overline{F}$ может не быть чисто несепарабельным расширением). Далее, композит $EF \subset L$, $EF \neq L$, так как любой элемент из $E$ коммутирует с $u(\overline{D}_2)$, где $u$ есть некое фиксированное вложение. Поэтому должно выполняться $\overline{C_{D_2}(EF)} = \overline{D}_2$ и $C_{D_2}(EF)$ – неразветвленная алгебра с делением. Следовательно, $D_2$ есть расщепимая алгебра с делением.

Теоремы о разложении [1; теоремы 5.6–5.15] завершают доказательство.

Это предложение показывает, что изучение расщепимых алгебр с делением может быть сведено к изучению расщепимых $p$-алгебр. Поэтому далее в этом и следующем параграфах будем рассматривать только $p$-алгебры.

Предложение 5. *Пусть $D$ – хорошо расщепимая алгебра с делением, причем $Z(\overline{D})/\overline{Z(D)}$ – чисто несепарабельное расширение. Тогда $D \cong D_1 \otimes_{Z(D)} D_2$, где $D_1$ – неразветвленная алгебра с делением и $D_2$ – хорошо расщепимая алгебра с делением такая, что $\overline{D_2}$ – поле, $\overline{D}_2/\overline{Z(D)}$ – чисто несепарабельное расширение, $[\overline{D}_2 : \overline{Z(D)}] = [\Gamma_{D_2} : \Gamma_{Z(D)}]$.*

Доказательство. Доказываем по индукции по степени $[Z(\overline{D}) : \overline{Z(D)}]$.

Положим $[Z(\overline{D}) : \overline{Z(D)}] = p$. Пусть ${}^{(z,u)}\delta_i$ – отображение из леммы 11. Тогда ${}^{(z,u)}\delta_i^p$ – дифференцирование, тривиальное на центре $Z(D)$, откуда по теореме Сколема–Нётер следует, что это внутреннее дифференцирование.

Докажем, что $z^p \in Z(D)$. Имеем

$$z^{-i} a z^i = a + {}_{-i}\delta_i(a) z^i, \qquad a \in u(\overline{D}).$$

Следовательно,

$$z^{-pi} a z^{pi} = a + {}_{-i}\delta_i^p(a) z^{pi}, \qquad a \in u(\overline{D}),$$

и

$$z^{pi} a z^{-pi} = a + \delta_1'(a) z^{pi} + {\delta_1'}^2(a) z^{2pi} + \cdots ,$$

где $\delta_1' = (-1)_{-i}\delta_i^p = i^p \delta_i^p$. Отсюда

$$z^p a z^{-p} = a + \frac{1}{i}\delta_1'(a) z^{pi} + c_2 \frac{1}{i^2} {\delta_1'}^2(a) z^{2pi} + \cdots ,$$

где $c_k$ задаются формулой (4) (лемма 7). Следовательно, $z^p \in Z(D)$ тогда и только тогда, когда $\delta_i^p = 0$. Предположим, что $\delta_i^p \neq 0$. Рассмотрим элемент $Y \in Z(D)$, $w(Y) > 0$. Пусть

$$Y = a_1 z^p + \cdots , \qquad a_1 \in u(\overline{D}).$$

Сначала заметим, что

$$Y = a_1 z^p + a_2 z^{2p} + a_3 z^{3p} + \cdots , \qquad a_i \in u(\overline{D}).$$

В самом деле, $Y$ должен удовлетворять $[Y, s] = 0$, где $s$ есть порождающая поля $u(Z(\overline{D}))$ над $u(\overline{Z(D)})$. Так как $s \in u(Z(\overline{D}))$ и $w([z^k, s]) = k + i$ при $(k, p) = 1$ и $w([z^k, s]) = \infty$ в противном случае, имеем, что $[z^{i_k}, s] = 0$ для любого $k$, где

$$Y = \sum_{k=1}^{\infty} a_k z^{i_k}.$$

Следовательно, $p \mid i_k$.

Далее, $Y$ должен удовлетворять $Ya = aY$ для любого $a \in u(\overline{D})$. Поэтому $a_1, \ldots, a_i \in u(Z(\overline{D}))$ и должно выполняться

$$a a_{i+1} - a_{i+1} a = \frac{a_1 \delta_1'(a)}{i}$$

и

$$aa_{2i+1} - a_{2i+1}a = a_i\delta_1'(a) + a_1c_2{\delta_1'}^2(a).$$

Ввиду того, что $\Delta(a) = aa_{2i+1} - a_{2i+1}a$ есть внутреннее дифференцирование, получаем ${\delta_1'}^2 = \delta$, где $\delta$ – дифференцирование, что приводит к противоречию, если $\delta \neq 0$ и $\operatorname{char} D \neq 2$. В последнем случае можно применить те же аргументы для $a_{3i+1}$. Следовательно, ${\delta_1'}^2 = \delta = 0$, $\delta_1' = 0$ и $z^p \in Z(D)$.

Рассмотрим алгебру $W = u(Z(\overline{D}))((z))$. Из того, что $z^p \in Z(D)$ и $u(\overline{Z(D)}) \subset Z(D)$, следует, что $Z(W) = u(\overline{Z(D)})((z^p)) = Z(D)$. Следовательно, по теореме о централизаторе $D \cong W \otimes_F C_D(W)$. Очевидно, что $C_D(W)$ – неразветвленная алгебра с делением.

Предположим теперь, что предложение доказано для $[Z(\overline{D}) : \overline{Z(D)}] = p^{k-1}$. По теореме Алберта [11; теорема 13] $D_2$ является циклической алгеброй как произведение циклических подалгебр $D_i$, где $\overline{D}_i/\overline{F}$ есть простое чисто несепарабельное расширение и $D_i$ – хорошо расщепимая алгебра.

Пусть $[Z(\overline{D}) : \overline{Z(D)}] = p^k$. Для хорошего вложения существует подъем $\widetilde{K}$ такого подполя $\overline{Z(D)} \subset K \subset Z(\overline{D})$, что расширение $K/\overline{Z(D)}$ имеет степень $p$, т.е. $\overline{\widetilde{K}} = K$, $\Gamma_{\widetilde{K}} = \Gamma_{Z(D)}$, $u(K) \subset \widetilde{K}$, $\widetilde{K}/Z(D)$ – чисто несепарабельное расширение степени $p$. По предположению индукции $C_D(\widetilde{K}) \cong A_1 \otimes_{\widetilde{K}} A_2$, где $A_2$ есть циклическая алгебра с делением и $\overline{A}_2$ – поле. Заметим, что $\overline{A}_2 = Z(\overline{D})$.

По теореме 6 из [11] мы можем взять $A_2 = (L/\widetilde{K}, \sigma, a)$, где $a$ порождает $\widetilde{K}$ над $Z(D)$. Итак, $A_2$ содержит максимальное чисто несепарабельное подполе $E = \widetilde{K}(y)$ с $y^{p^{k-1}} = a$, поэтому $E = Z(D)(y)$. По теореме 3 из [11] $L = L_0 \times \widetilde{K}$, где $L_0$ – циклическое поле степени $p^{k-1}$ над $Z(D)$, и $yx_0 = \sigma(x_0)y$, где $x_0 \in L_0$.

Рассмотрим централизатор $B = C_D(L_0)$. Докажем, что $B \cong B_1 \otimes_{L_0} B_2$, где $B_2$ – циклическая алгебра с делением степени $p$ и $B_2$ содержит $\widetilde{K}$.

Заметим, что $B$ содержит $Z(D)(a) = \widetilde{K}$ и $A_1$. Если $\widetilde{K}L_0 = L$ "не разветвлено" над $L_0$, то мы можем применить рассуждения первого шага индукции к алгебре $B$. По построению $B_2$ содержит $L$, поэтому – и $\widetilde{K}$. Предположим, что $L$ вполне разветвлено над $L_0$, и пусть $z$ – параметр $L$, т.е. элемент с наименьшим возможным положительным значением нормирования на $L$. Так как $L$ чисто несепарабельно над $L_0$, то $z^p$ есть параметр $L_0$.

Имеем, что $W := C_B(L) = C_D(L) \cong A_1 \otimes_{\widetilde{K}} L$ – неразветвленная алгебра с делением. Рассмотрим вложение $u' \colon \overline{L} = \overline{L_0} \hookrightarrow L_0$. Как было показано при доказательстве теоремы 1, существует подъем $\widetilde{u'}$ элемента $u'$, $\widetilde{u'} \colon \overline{W} \hookrightarrow W$. Рассмотрим теперь подалгебру $W' = \widetilde{u'}(\overline{W})((z^p))$. Имеем $Z(W') = u'(\overline{L})((z^p)) = L_0$, поэтому $W'$ есть неразветвленная подалгебра в $B$. По теореме о централизаторе $B \cong W' \otimes_{L_0} C_B(W')$, где $C_B(W')$ – алгебра с делением степени $p$, содержащая $L_0(z) = L$, а следовательно, и $\widetilde{K}$, и циклическая по теореме Алберта [11; теорема 12]).

Теперь можно повторить буквально доказательство теоремы 12 из [11], чтобы показать, что существует циклическое расширение Галуа $L'$ поля $L_0$, которое является циклическим над $Z(D)$, и $y$ ведет себя как автоморфизм Галуа на $L'/Z(D)$, порождающий $\operatorname{Gal}(L'/Z(D))$. Следовательно, существует циклическая подалгебра $D_2 = (L'/Z(D), \sigma, y^{p^k})$ в $D$, где $\sigma$ – автоморфизм Галуа поля $L'$, порождаемый внутренним автоморфизмом $i_y$. Заметим, что $A_2 \subset D_2$ и $A_2$ является хорошо расщепимой алгеброй с $[\overline{A}_2 : \overline{Z(A_2)}] = [\Gamma_{A_2} : \Gamma_{Z(A_2)}]$. Так как $\overline{A}_2 = \overline{D}_2$ и $Z(A_2) = \widetilde{K}$ есть чисто несепарабельное расширение $Z(D)$, то $D_2$ – хорошо расщепимая алгебра такая, что $\overline{D}_2$ есть поле и $[\overline{D}_2 : \overline{Z(D)}] = [\Gamma_{D_2} : \Gamma_{Z(D)}]$. По теореме о централизаторе $D \cong D_1 \otimes_{Z(D)} D_2$, где $D_1 = C_D(D_2)$ должна быть неразветвленной алгеброй с делением, что завершает доказательство.

Объединяя все результаты данного параграфа, получаем следующую теорему.

Теорема 3. *Пусть $D$ – конечномерная хорошо расщепимая центральная алгебра с делением над полем $F = k((t))$.*

*Если* $\operatorname{char} F = p > 0$, *то* $D \cong D_1 \otimes_F D_2 \otimes_F A_1 \otimes_F \cdots \otimes_F A_m$, *где* $A_i$ – *такие циклические алгебры с делением, что* $[\overline{A}_i : \overline{Z(D)}] = [\Gamma_{A_i} : \Gamma_{Z(D)}]$ *и* $\overline{A}_i/\overline{Z(D)}$ – *простые чисто несепарабельные расширения,* $D_1$ – *инерциально расщепимая алгебра с делением,* $(\operatorname{ind}(D_1), p) = 1$, $D_2$ – *неразветвленная алгебра с делением* ($D_1$, $D_2$, $A_i$ *могут быть тривиальными*).

*Если* $\operatorname{char} F = 0$, *то* $D$ – *инерциально расщепимая алгебра с делением.*

## § 6. Расщепимость и хорошая расщепимость

В этом параграфе мы приведем некоторые разрозненные результаты, касающиеся взаимосвязи между расщепимыми и хорошо расщепимыми алгебрами с делением. Мы будем рассматривать здесь только алгебры с делением, удовлетворяющие следующему свойству: $Z(\overline{D})/\overline{Z(D)}$ – простое расширение.

Предложение 6. *Пусть $D$ – центральная алгебра с делением над $F$ характеристики* $\operatorname{char} D = p > 0$, *причем* $Z(\overline{D}) = \overline{D}$ *и* $[Z(\overline{D}) : \overline{F}] = p$.

*Тогда $D$ – расщепимая алгебра и локальная высота $i = i(u, z)$ (если она определена, т.е. когда $\alpha = \mathrm{id}$) не зависит от $u$ и $z$. Это хорошо расщепимая алгебра, если $(i, p) = 1$. Если же $p \mid i$, то существует параметр $z$ такой, что $z^p \in Z(D)$, и любое "неразветвленное" максимальное подполе циклическое.*

*Следовательно, в обоих случаях $D$ есть циклическая алгебра с делением степени $p$.*

Доказательство. Так как $\overline{D}/\overline{F}$ – простое расширение, то $[\overline{D} : \overline{F}] = [\Gamma_D : \Gamma_F]$. Действительно, рассмотрим поля $E = F(s)$ и $E' = F(z)$, где $s$ – произвольный элемент такой, что $\overline{s}$ – примитивный элемент расширения $\overline{D}/\overline{F}$, и $z$ – произвольный параметр $D$. Тогда $[\overline{D} : \overline{F}] \leqslant [E : F] \leqslant [D : F]^{1/2} = ([\overline{D} : \overline{F}][\Gamma_D : \Gamma_F])^{1/2}$, поэтому $[\overline{D} : \overline{F}] \leqslant [\Gamma_D : \Gamma_F]$. С другой стороны, $[\Gamma_D : \Gamma_F] \leqslant [E' : F] \leqslant ([\overline{D} : \overline{F}] \times [\Gamma_D : \Gamma_F])^{1/2}$, поэтому $[\overline{D} : \overline{F}] = [\Gamma_D : \Gamma_F]$. Следовательно, $D$ – расщепимая алгебра с делением степени $p$.

Если $Z(\overline{D})/\overline{F}$ – сепарабельное расширение, то по теореме 1 $D$ – хорошо расщепимая алгебра. Поэтому далее будем предполагать, что это чисто несепарабельное расширение, $Z(\overline{D}) = \overline{F}(\overline{u})$. Для любого подъема $u$ элемента $\overline{u}$ будем считать $u$ вложением, построенным по лемме 9, т.е. ${}^{(z,u)}\delta_j$ определяется значениями ${}^{(z,u)}\delta_j(u^k)$ для любого $j$. По следствию 2 локальная высота $i(u, z)$ не зависит от $z$, а по лемме 10 $i(u, z)$ не зависит от $u$. Для произвольного вложения $u'$ отображение ${}^{(z,u')}\delta_{i(u',z)}$ полностью определяется значением в $\overline{u}$, так как ${}^{(z,u')}\delta_{i(u',z)}$ – дифференцирование и $\overline{D}/\overline{F}$ – простое расширение. Следовательно, $i(u', z) = w(zu'(\overline{u})z^{-1} - u'(\overline{u}))$ и $i(u', z)$ полностью определяется подъемом $u'(\overline{u})$.

Но произвольный подъем на $\overline{u}$ задает вложение, от которого, как мы доказали, $i$ не зависит. Соответственно, $i(u,z)$ не зависит от $z$ и $u$.

Предположим теперь, что $p \mid i$.

Используя лемму 3, без ограничения общности можно считать, что ${}^{(z,u)}\delta_j = 0$, если $j$ не делится на $p$.

В самом деле, если ${}^{(z,u)}\delta_j \neq 0$, то можно применить лемму 3,ii), чтобы получить, что существует такой параметр $z_j$, что ${}^{(z_j,u)}\delta_j(u) = 0$ и ${}^{(z_j,u)}\delta_k = {}^{(z,u)}\delta_k$ при $k < j$, ${}^{(z_j)}\alpha = \mathrm{id}$. Так как по предложению 2 и по предположению индукции ${}^{(z_j,u)}\delta_j$ является дифференцированием (аналогичные рассуждения были использованы при доказательстве предложения 3), а также так как оно задается значениями на $u^k$, т.е. значениями на $u$, имеем ${}^{(z,u)}\delta_j = 0$. Ввиду того, что для $j_1 > j_2$ справедливо $w(z_{j_1} - z_{j_2}) > j_1 - i$, последовательность $\{z_j\}$ сходится к параметру $z'$, который удовлетворяет нашему условию.

Следовательно, существует подалгебра $A = u(\overline{D})((z^p))$. Покажем теперь, что $Z(D) \subset A$. Заметим, что любой элемент $a \in D$ может быть записан как $a = a_0 + a_1 z + \dots + a_{p-1} z^{p-1}$, где $a_i \in A$. Заметим также, что $z^k A z^{-k} \subset A$ для любого $k$. Отсюда, если $a \in Z(D)$, то $z a_j z^{-1} = a_j$ и $u a_j z^j u^{-1} = a_j z^j$ для любого $j$. Для $j > 0$ имеем $a_j z^j = \sum_k a_{jk} z^{kp+j}$, поэтому по следствию 2 $u a_j z^j u^{-1} \neq a_j z^j$. Следовательно, $a = a_0 \in A$.

Так как $A \neq D$, $A$ должна быть коммутативной, отсюда $z^p \in Z(D)$. Более того, расширение $A/Z(D)$ циклично. Так как рассуждения верны для любого подъема $u$ элемента $\overline{u}$, то произвольное "неразветвленное" максимальное подполе в $D$ должно бытьциклично над $F$.

Пусть теперь $(i,p) = 1$.

Используя лемму 3,iii), можем найти такие параметр $z$ и примитивный элемент $s \in \overline{D}$, что ${}^{(z,u)}\delta_i(s) = sc$, где $c \in \overline{F}$. В самом деле, так как $(i,p) = 1$, то найдется такое $k$, что $1 - ki$ делится на $p$. Следовательно, по лемме 3,iii) для параметра $z' = u({}^{(z,u)}\delta_i(\overline{u})^k)z$ выполняется ${}^{(z',u)}\delta_i(\overline{u}) \in \overline{F}$, поэтому по лемме 10,iii) ${}^{(z',u)}\delta_i(s) = 1$, где $s = \overline{u}\,{}^{(z',u)}\delta_i(\overline{u})^{-1}$. Это значит, что существует $k_1$ такое, что $-ik_1 - 1$ делится на $p$, поэтому для $z'' = s^{k_1} z'$ выполняется ${}^{(z'',u)}\delta_i(s) = sc$, где $c = s^{-ik_1-1} \in \overline{F}$. Легко видеть, что ввиду $s = \overline{u}a$, где $a \in \overline{F}$, отображение ${}^{(z,u)}\delta_j$ однозначно определяется также по ${}^{(z,u)}\delta_j(s^k)$, т.е. и по ${}^{(z,u)}_{\ \ m}\delta_l(s)$ при $l \leqslant j$. Поэтому без ограничения общности можем считать, что $s = \overline{u}$, $z = z''$.

Используя лемму 10,ii), можем отыскать такую сходящуюся последовательность $\{u_j\}$, $u_j \in D$, $j \geqslant i$, что $u_{j+1} = u_j + b_j z^{j+1-i}$, $u_i = u$, $b_j \in u_j(\overline{D})$ (здесь под $u_j$ понимаем вложение, задаваемое $u_j$, см. лемму 9), и ${}^{(z,u_j)}_{\ \ m}\delta_k(\overline{u})\overline{u}^{-1} \in \overline{F}$ для всех $k \leqslant j$ и всех $m$.

В самом деле, предположим, что это верно для $j \geqslant i$. Пусть ${}^{(z,u_j)}_{\ \ m}\delta_{j+1}(\overline{u}) = a_0 + \dots + a_{p-1}\overline{u}^{p-1}$, $a_k \in \overline{F}$. Так как ${}^{(z,u_j)}_{\ \ m}\delta_i = {}^{(z,u)}_{\ \ m}\delta_i = m\,{}^{(z,u)}\delta_i$, то имеем

$$
{}^{(z,u_j)}_{\ \ m}\delta_i(a_k\overline{u}^k) - \frac{\partial}{\partial \overline{u}}\bigl({}^{(z,u_j)}_{\ \ m}\delta_i(\overline{u})\bigr)a_k\overline{u}^k = (k-1)mca_k\overline{u}^k.
$$

Следовательно, $u_{j+1} = u_j - u_j\bigl(\sum_{k,k\neq 1}(k-1)^{-1}m^{-1}c^{-1}a_k\overline{u}^k\bigr)z^{j+1-i}$ удовлетворяет нашему условию.

Обозначим через $u$ предел последовательности $\{u_j\}$. По индукции и по предложению 2 легко можно показать, что ${}^{(z,u)}_{\ \ m}\delta_j(\overline{u}^k)\overline{u}^{-k} \in \overline{F}$ для любого целого $k$.

Следовательно, существует подалгебра $A = u(\overline{F})((z))$ в $D$. Рассуждениями, аналогичными случаю $p \mid i$, можно показать, что $A$ содержит $Z(D)$. Так как $A \neq D$, она должна быть коммутативной, поэтому $u^p \in Z(D)$. Тогда $u$ – хорошее вложение. Предложение доказано.

Пусть $D$ – расщепимая алгебра с делением, и пусть $Z(\overline{D})/\overline{Z(D)}$ – чисто несепарабельное расширение. Как было показано при доказательстве леммы 11, тогда существует такой параметр $z$ в $D$, что ${}^{(z,u)}\delta_i\big|_{Z(\overline{D})} \neq 0$, где $i = i(u,z)$ – локальная высота. Хотя $D$ может и не являться хорошо расщепимой, рассуждения леммы верны для любой расщепимой алгебры. Мы будем называть такой параметр *подходящим параметром*, а число $i(u) = \max_z i(u,z) = i(u,z)$ для подходящего параметра – *полулокальной высотой*. Теперь докажем следующую простую лемму.

Лемма 12. *Пусть $D$ – расщепимая центральная $p$-алгебра с делением над $F$, где $p = \operatorname{char} D > 0$, и пусть $Z(\overline{D}) = \overline{F}(s)$ – простое расширение над $\overline{F}$. Тогда*

i) *существует такое вложение $u$, что ${}^{(z,u)}_{\;\;l}\delta_j\big|_{Z(\overline{D})}$ определяется значениями ${}^{(z,u)}_{\;\;l}\delta_j(s^k)$ для любых $j$, $l$, $z$ (как в лемме 9);*

ii) $[Z(\overline{D}) : \overline{F}] = [\Gamma_D : \Gamma_F]$;

iii) *если $\alpha\big|_{Z(\overline{D})} \neq \mathrm{id}$ или $i(u)$ делится на $p$, то существует подалгебра $A = u(\overline{D})((z))$ для такого подходящего параметра $z$, что $Z(D) \subset Z(A)$, более того, $Z(A)$ есть циклическое расширение Галуа над $Z(D)$.*

Доказательство. i) Для произвольного вложения $u$ рассмотрим поле $E = u(Z(\overline{D}))F \subset D$ и централизатор $W = C_D(E)$. Тогда $\overline{W} = \overline{D}$ и $Z(\overline{W}) = \overline{E}$. Следовательно, $W$ должна быть неразветвленной алгеброй с делением, и по теореме 1 существует подъем на $\overline{W}$ произвольного вложения $\overline{E} \hookrightarrow E$. Далее, возьмем вложение, определяемое элементом $s$, как в лемме 9. Его подъем будет искомым вложением. Это вложение также будем обозначать через $s$.

ii) По предложению 1.7 из [1] основной гомоморфизм $\theta_D$ (см. введение) сюръективен. Поэтому достаточно доказать утверждение только для централизатора $C_D(K)$, где $K$ – подъем циклического подрасширения расширения $Z(\overline{D})/\overline{F}$. Ниже будем поэтому полагать $Z(\overline{D})/\overline{F}$ чисто несепарабельным расширением.

Рассмотрим максимальное сепарабельное подполе $M$ в $\overline{D}$, и пусть $M'/\overline{F}$ – сепарабельное подрасширение расширения $M/\overline{F}$. Из [1; теоремы 2.8, 2.9] следует, что существует неразветвленный подъем $M'$ в $D$, скажем, $\widetilde{M}$. Рассмотрим централизатор $B = C_D(\widetilde{M})$. Тогда $\overline{B}$ – поле. Требуемое утверждение будет доказано, если удастся доказать его для $B$, так как $[\widetilde{M} : F] = \operatorname{ind}(\overline{D})$ и $[D : F] = \operatorname{ind}(\overline{D})^2[Z(\overline{D}) : \overline{F}][\Gamma_D : \Gamma_F]$. Так как $\overline{B}/\overline{Z(B)}$ – простое расширение, для этого можно повторить рассуждения начала доказательства предложения 6.

iii) Если $\alpha\big|_{Z(\overline{D})} \neq \mathrm{id}$, рассмотрим параметр $z$ из предложения 3. Очевидно, что $A = u(\overline{D})((z))$ – подалгебра с центром $K$, который является неразветвленным подъемом циклического подрасширения расширения $Z(\overline{D})/\overline{F}$.

Предположим, что $\alpha\big|_{Z(\overline{D})} = \mathrm{id}$ и $i(u)$ делится на $p$. Пусть $z$ – подходящий параметр. Используя лемму 3, можно доказать, что ${}^{(z,u)}\delta_j = 0$, если $j$ не делится на $p$.

В самом деле, пусть ${}^{(z,u)}\delta_j \neq 0$ – первое отображение, обладающее этим свойством, и $(j,p)=1$. Если ${}^{(z,u)}\delta_j\big|_{Z(\overline{D})}=0$, то, применяя лемму 3,i), можно показать существование параметра $z_j$ такого, что ${}^{(z_j,u)}\delta_j=0$ и ${}^{(z_j,u)}\delta_k={}^{(z,u)}\delta_k$ для $k<j$, ${}^{(z_j)}\alpha=\mathrm{id}$, так как ${}^{(z,u)}\delta_j$ – дифференцирование по предложению 2 и по индукции (подобные рассуждения уже использовались при доказательстве предложения 3), и, следовательно, по теореме Сколема–Нетёр это – внутреннее дифференцирование.

Если ${}^{(z,u)}\delta_j\big|_{Z(\overline{D})}\neq 0$, то применяем лемму 3,ii) и имеем, что существует параметр $z_j$ такой, что ${}^{(z_j,u)}\delta_j(s)=0$ и ${}^{(z_j,u)}\delta_k={}^{(z,u)}\delta_k$ для $k<j$, ${}^{(z_j)}\alpha=\mathrm{id}$. Так как ${}^{(z_j,u)}\delta_j$ – дифференцирование и его ограничение на $Z(\overline{D})$ определяется значениями на $s^k$, т.е. значениями на $s$, то выполняется ${}^{(z,u)}\delta_j\big|_{Z(\overline{D})}=0$ и задача сводится к предыдущему случаю. Так как при $j_1>j_2$ выполняется $w(z_{j_1}-z_{j_2})>j_1-i$, то последовательность $\{z_j\}$ сходится к параметру $z'$, который удовлетворяет нашему условию.

Следовательно, существует подалгебра $A=u(\overline{D})((z'))$ в $D$. Рассуждениями, аналогичными использованным при доказательстве предложения 6, получаем, что $Z(D)\subset Z(A)$. Так как $z'$ сохраняет $A$, то он сохраняет центр $Z(A)$. С другой стороны, он на нем действует нетривиально. Следовательно, $Z(A)$ есть циклическое расширение Галуа степени $p$ и внутренний автоморфизм $i_{z'}$, ограниченный на $Z(A)$, порождает его группу Галуа.

Эта лемма показывает, что изучение расщепимых $p$-алгебр над $F$ может быть сведено к изучению расщепимых $p$-алгебр с чисто несепарабельным расширением $Z(\overline{D})/\overline{F}$ и $(i(u),p)=1$.

Определение 6. Пусть $D$ – расщепимая $p$-алгебра с делением с чисто несепарабельным расширением $Z(\overline{D})/\overline{F}$. Для любого элемента $a\in\overline{D}$ определим число

$$d_D(a)=\max_{u,z} w\big(z^{-i(u,a)}u(a)z^{i(u,a)}-u(a)-u\big({}^{(z,u)}_{-i(u,a)}\delta_{i(u,a)}(a)\big)z^{i(u,a)}\big)\in\mathbb{N}\cup\infty,$$

где параметры $z$ берутся из множества подходящих параметров, а $i(u,a)$ был определен в следствии 2.

Как нам кажется, число $d_D(a)$ может играть роль уровня высшего порядка в расщепимой алгебре с делением. Ниже мы покажем, что оно содержит в себе часть информации об алгебре с делением.

Лемма 13. *Пусть $D$ – расщепимая $p$-алгебра с делением, $p>2$, с чисто несепарабельным простым расширением $Z(\overline{D})/\overline{F}$.*

*Пусть $u$ – некое фиксированное вложение $u\colon\overline{D}\hookrightarrow D$. Положим $Z(\overline{D})=\overline{F}(a)$, $(i(u,a),p)=1$; $d(u,a)\leqslant 2i(u,a)$.*

*Пусть $z$ – такой параметр, что ${}^{(z,u)}\delta_{i(u,a)}\big({}^{(z,u)}_{-i(u,a)}\delta_{i(u,a)}(a)\big)=0$, ${}^{(z)}\alpha=\mathrm{id}$ и ${}^{(z,u)}_{-i(u,a)}\delta_q\big|_{\mathbb{F}_p(a)}=0$ для $i(u,a)<q<d(u,a)$. Положим $j(k):=i(u,a^{p^k})$.*

*Предположим, что для любого $k\geqslant 1$ параметр $z_k$ такой, что*

$${}^{(z_k,u)}_{-j(k)}\delta_r\big|_{\mathbb{F}_p(a^{p^k})}=0$$

*для* $j(k) < r < d(u,a^{p^k})$, *удовлетворяет условию* ${}^{(z_k,u)}\delta_{i(u,a)} = {}^{(z,u)}\delta_{i(u,a)}$, ${}^{(z_k)}\alpha = {}^{(z)}\alpha$. *Пусть также для любого* $k \geqslant 1$ *выполняется* $d(u,a^{p^k}) - j(k) = d(u,a) - j(0)$.

*Тогда отображения* ${}_{w+(p-1-r)j(k)}^{(z,u)}\delta_\zeta$, $rj(k) < \zeta \leqslant (r-1)j(k) + d(u,a^{p^k})$, $r \in \{1,\dots,p-1\}$, $k \geqslant 0$, *удовлетворяют*

$$
{}_{w+(p-1-r)j(k)}^{(z,u)}\delta_\zeta\big|_{\mathbb{F}_p(a^{p^k})} = c_{w+(p-1-r)j(k),\zeta,1}\delta + \dots + c_{w+(p-1-r)j(k),\zeta,r}\delta^r,
$$

*где дифференцирование* $\delta$ *было определено в лемме* 5, $c_{w+(p-1-r)j(k),\zeta,r} \in Z(\overline{D})$, $c_{w+(p-1-r)j(k),\zeta,r} \neq 0$, *только если* $\zeta = (r-1)j(k) + d(u,a^{p^k})$.

*Более того,* $c_{w+(p-1-r)j(k),(r-1)j(k)+d(u,a^{p^k}),r} \neq 0$, *если* $w = i(u,a) \pmod p$;

$$
\begin{aligned}
&c_{w+(p-1-r)j(k),(r-1)j(k)+d(u,a^{p^k}),r} \\
&\qquad = r!\, c_{w+(p-r)j(k),(r-2)j(k)+d(u,a^{p^k}),r-1}\; {}_{w+(p-1-r)j(k)}\delta_{j(k)}(a^{p^k}),
\end{aligned}
$$

*а* ${}_{w+(p-2)j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}(a^{p^k}) = {}_{-j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}(a^{p^k})$.

Доказательство. Лемма доказывается аналогично лемме 5,i) индукцией по $r$ одновременно для всех $k \geqslant 0$.

Для $r = 1$ легко показать, используя лемму 2, что

$$
{}^{(z_k,u)}\delta_q(a^{p^k}) = -(j(k))^{-1}\, {}_{-j(k)}^{(z_k,u)}\delta_q(a^{p^k})
$$

для $j(k) \leqslant q < d(u,a^{p^k})$ (полагаем здесь $z_0 = z$). По лемме 8,i) имеем, что $d(u,a) - i(u,a) = i(u,a) \pmod p$. По утверждению ii) леммы 8 и по индукции по $k$ тогда получаем $j(k) = j(0) \pmod p$.

Следовательно,

$$
{}_{w+(p-2)j(k)}^{(z_k,u)}\delta_q\big|_{\mathbb{F}_p(a^{p^k})} = 0,
$$

если $j(k) < q < d(u,a^{p^k})$, и

$$
{}_{w+(p-2)j(k)}^{(z_k,u)}\delta_q\big|_{\mathbb{F}_p(a^{p^k})} \neq 0,
$$

только если $q = d(u,a^{p^k})$.

Так как ${}_{-j(k)}^{(z_k,u)}\delta_{j(k)}\big|_{\mathbb{F}_p(a^{p^k})}$ – дифференцирование и по предложению 2,i) отображение ${}_{-j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}\big|_{\mathbb{F}_p(a^{p^k})}$ тоже должно быть дифференцированием, получаем ${}_{w+(p-2)j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}(a^{p^k}) \in Z(\overline{D})$. Действительно, как было показано при доказательстве леммы 5,ii), для любого дифференцирования $\delta$ выполняется $\delta(b) \in Z(\overline{D})$ для любого $b \in Z(\overline{D})$. Так как ${}_{w+(p-2)j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}(a^{p^k}) = q_1\, {}_{-j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}(a^{p^k}) + q_2\, {}_{m}^{(z_k,u)}\delta_{j(0)}\big({}_{-j(k)}^{(z_k,u)}\delta_{j(k)}(a^{p^k})\big)$ для некоторых целых $q_1$, $q_2$, $m$, наше утверждение доказано. Поэтому $c_{w+(p-2)j(k),d(u,a^{p^k}),1} \in Z(\overline{D})$.

Если $w = j(0) \pmod p$, то ${}_{w+(p-2)j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}(a^{p^k}) = {}_{-j(k)}^{(z_k,u)}\delta_{d(u,a^{p^k})}(a^{p^k})$, так как $w + (p-1)j(0) = 0 \pmod p$ и $\operatorname{char} D > 2$. Следовательно, имеем $c_{w+(p-2)j(k),d(u,a^{p^k}),1} \neq 0$.

Положим теперь $t = a^{p^k}$. По предложению 2,i) для любого $r$ имеем

$$\begin{aligned}
{}_{w+(p-1-r)j(k)}^{(z_k,u)}\delta_\zeta(t^q) &= q\, {}_{w+(p-1-r)j(k)}\delta_\zeta(t)t^{q-1} \\
&+ {}_{w+(p-1-r)j(k)}\delta_{j(k)}(t)\sum_{l=0}^{q-2} {}_{w+(p-r)j(k)}\delta_{\zeta-j(k)}(t^{q-1-l})t^l \\
&+ {}_{w+(p-1-r)j(k)}\delta_{d(u,t)}(t)\sum_{l=0}^{q-2} {}_{w+(p-1-r)j(k)+d(u,t)}\delta_{\zeta-d(u,t)}(t^{q-1-l})t^l \\
&+ \sum_{i=d(u,t)+1}^{\zeta-1} {}_{w+(p-1-r)j(k)}\delta_i(t)\sum_{l=0}^{q-2} {}_{w+(p-1-r)j(k)+i}\delta_{\zeta-i}(t^{q-1-l})t^l. \qquad (5)
\end{aligned}$$

С помощью тех же рассуждений, что были использованы при доказательстве леммы 5,i), получаем, что ${}_{w+(p-1-r)j(k)}\delta_\zeta(t^p) = 0$ и

$${}_{w+(p-1-r)j(k)}\delta_\zeta\big|_{\mathbb{F}_p(t)} = c_{w+(p-1-r)j(k),\zeta,1}\delta + \dots + c_{w+(p-1-r)j(k),\zeta,p-1}\delta^{p-1}.$$

Для того чтобы показать, что $c_{w+(p-1-r)j(k),\zeta,i} = 0$ для $i > r$, достаточно с помощью (3) проверить, что все отображения в (5) представляются в виде $c_1\delta + \dots + c_{r-1}\delta^{r-1}$. Сделаем это подробно.

Так как $\zeta - d(u,t) - 1 < (r-1)j(k)$, то по лемме 5,ii) ${}_m\delta_{\zeta-i}\big|_{\mathbb{F}_p(t)} = c_{m,\zeta-i,1}\delta + \dots + c_{m,\zeta-i,r-2}\delta^{r-2}$ для всех $i > d(u,t)$.

Если $w = j(0) \pmod p$, то $w + (p-1-r)j(k) + d(u,t) + (r-2)j(k) = 0 \pmod p$. Так как $\zeta - d(u,t) \leqslant (r-1)j(k)$, по лемме 5,ii) получаем

$$\begin{aligned}
&{}_{w+(p-1-r)j(k)+d(u,t)}\delta_{\zeta-d(u,t)}\big|_{\mathbb{F}_p(t)} \\
&\quad = c_{w+(p-1-r)j(k)+d(u,t),\zeta-d(u,t),1}\delta \\
&\qquad + \dots + c_{w+(p-1-r)j(k)+d(u,t),\zeta-d(u,t),r-2}\delta^{r-2}.
\end{aligned}$$

Если $w \neq j(0) \pmod p$, то оттуда же получаем, что

$$\begin{aligned}
&{}_{w+(p-1-r)j(k)+d(u,t)}\delta_{\zeta-d(u,t)}\big|_{\mathbb{F}_p(t)} \\
&\quad = c_{w+(p-1-r)j(k)+d(u,t),\zeta-d(u,t),1}\delta \\
&\qquad + \dots + c_{w+(p-1-r)j(k)+d(u,t),\zeta-d(u,t),r-1}\delta^{r-1},
\end{aligned}$$

и по лемме 5,i) $c_{w+(p-1-r)j(k)+d(u,t),\zeta-d(u,t),r-1} \in Z(\overline{D})$ как произведение элементов из $Z(\overline{D})$.

Наконец, по предположению индукции

$$\begin{aligned}
&{}_{w+(p-r)j(k)}\delta_{\zeta-j(k)}\big|_{\mathbb{F}_p(t)} \\
&\quad = c_{w+(p-r)j(k),\zeta-j(k),1}\delta + \dots + c_{w+(p-r)j(k),\zeta-j(k),r-1}\delta^{r-1},
\end{aligned}$$

где $c_{w+(p-r)j(k),\zeta-j(k),r-1} \neq 0$, только если $\zeta - j(k) = (r-2)j(k) + d(u,t)$, и $c_{w+(p-r)j(k),\zeta-j(k),r-1} \in Z(\overline{D})$. Так как ${}_{w+(p-1-r)j(k)}\delta_{j(k)}(t) \in Z(\overline{D})$, по формуле (3) получаем $c_{w+(p-1-r)j(k),\zeta,r} \in Z(\overline{D})$, и если $w = j(0) \pmod p$, то $c_{w+(p-1-r)j(k),\zeta,r} \neq 0$ тогда и только тогда, когда $\zeta = (r-1)j(k) + d(u,t)$,

$$\begin{aligned} &c_{w+(p-1-r)j(k),(r-1)j(k)+d(u,t),r} \\ &\qquad = r!\, c_{w+(p-r)j(k),(r-2)j(k)+d(u,t),r-1}\, {}_{w+(p-1-r)j(k)}\delta_{j(k)}(t) \neq 0. \end{aligned}$$

Лемма доказана.

Лемма 14. *Пусть $D$ – алгебра с делением, как в лемме 13. Предположим, что $d(u,a) \leqslant 2i(u,a)$ и $\operatorname{char} D > 2$.*

*Тогда для любого $k$ существует такой параметр $z_k$, что ${}^{(z_k,u)}_{-j(k)}\delta_r\big|_{\mathbb{F}_p(a^{p^k})} = 0$ для $j(k) < r < d(u,a^{p^k})$, и ${}^{(z_k)}\alpha = {}^{(z)}\alpha$, ${}^{(z_k,u)}\delta_{j(l)} = {}^{(z,u)}\delta_{j(l)}$ для всех $l \leqslant k$ (используемые обозначения были введены в лемме 13).*

*Более того, для любого $k \geqslant 1$ выполняется $d(u,a^{p^k}) - j(k) = d(u,a) - j(0)$ и*

$${}^{(z_k,u)}_{-j(k)}\delta_{d(u,a^{p^k})}(a^{p^k}) = -{}^{(z_{k-1},u)}_{-j(k-1)}\delta_{d(u,a^{p^{k-1}})}(a^{p^k})\,c_{d(u,t)-j(k-1),j(k)-j(k-1),p-1},$$

*где $c_{d(u,t)-j(k-1),j(k)-j(k-1),p-1}$ было определено в лемме 13.*

Доказательство. Доказываем индукцией по $k$. По лемме 8 $d(u,a) = 2j(0) \pmod p$ и $j(1) = d(u,a) + (p-1)j(0)$. Поэтому по предположению индукции можем считать, что для произвольного $k$ выполняется $d(u,a^{p^{k-1}}) = 2j(0) \pmod p$ и $j(k-1) = j(0) \pmod p$, $j(k) = d(u,a^{p^{k-1}}) + (p-1)j(k-1)$.

Начнем для удобства с параметра $z = z_0$, удовлетворяющего условиям леммы 13. Покажем, что такой параметр существует. Действительно, выбрав некоторый подходящий параметр $z$ и изменив его, если нужно, на параметр $u(c)z$ для подходящего $c \in Z(\overline{D})$ (как при доказательстве предложения 6), мы можем положить, что ${}^{(z,u)}_{-j(0)}\delta_{j(0)}(a) \in Z(\overline{D})^p$. Далее, используя рассуждения доказательства леммы 8,i), находим искомый параметр $z_0$.

Идея доказательства теперь в следующем: сначала докажем, что

$${}^{(z_{k-1},u)}_{-j(k-1)}\delta_{j(k)+d(u,a)-j(0)}(a^{p^k}) \neq 0.$$

Далее мы докажем существование параметра $z_k$ такого, что ${}^{(z_k,u)}_{-j(k)}\delta_\zeta(a^{p^k}) = 0$ для $j(k) < \zeta < j(k) + d(u,a) - j(0)$ и ${}^{(z_k,u)}_{-j(k)}\delta_{j(k)+d(u,a)-j(0)}(a^{p^k}) \neq 0$. Будет показано, что $z_k$ удовлетворяет условиям леммы.

Итак, предположим, что $j(k) \leqslant \zeta \leqslant j(k) + d(u,a) - j(0) = j(k) + d(u,a^{p^{k-1}}) - j(k-1)$. Положим $t = a^{p^{k-1}}$. По предложению 2,i) имеем

$$\begin{aligned} {}^{(z_{k-1},u)}_{-j(k-1)}\delta_\zeta(t^p) &= {}^{(z_{k-1},u)}_{-j(k-1)}\delta_{d(u,t)}(t) \sum_{l=0}^{p-2} {}^{(z_{k-1},u)}_{d(u,t)-j(k-1)}\delta_{\zeta-d(u,t)}(t^{p-1-l})t^l \\ &\quad + \dots + {}^{(z_{k-1},u)}_{-j(k-1)}\delta_{\zeta-(p-1)j(k-1)}(t) \sum_{l=0}^{p-2} {}^{(z_{k-1},u)}_{\zeta-pj(k-1)}\delta_{(p-1)j(k-1)}(t^{p-1-l})t^l \\ &\quad + \sum_{i=\zeta-(p-1)j(k-1)+1}^{\zeta-1} {}^{(z_{k-1},u)}_{-j(k-1)}\delta_i(t) \sum_{l=0}^{p-2} {}^{(z_{k-1},u)}_{i-j(k-1)}\delta_{\zeta-i}(t^{q-1-l})t^l. \end{aligned}$$

По лемме 5,i) в последней сумме имеем ${}^{(z_{k-1},u)}_{i-j(k-1)}\delta_{\zeta-i}\big|_{\mathbb{F}_p(t)} = c_{i-j(k-1),\zeta-i,1}\delta+\dots+ c_{i-j(k-1),\zeta-i,p-2}\delta^{p-2}$, так как $\zeta - i < (p-1)j(k-1)$. Следовательно, эта сумма равна нулю.

По утверждению ii) леммы 5 имеем

$$\begin{aligned}{}^{(z_{k-1},u)}_{\zeta-pj(k-1)}\delta_{(p-1)j(k-1)}\big|_{\mathbb{F}_p(t)} &= c_{\zeta-pj(k-1),(p-1)j(k-1),1}\delta \\ &\quad+\dots+ c_{\zeta-pj(k-1),(p-1)j(k-1),p-1}\delta^{p-1},\end{aligned}$$

где $c_{\zeta-pj(k-1),(p-1)j(k-1),p-1} \neq 0$, тогда и только тогда, когда $\zeta = j(k-1) = j(0) \pmod p$.

По лемме 5,i) выполняется ${}^{(z_{k-1},u)}_{m}\delta_q\big|_{\mathbb{F}_p(t)} = c_{m,q,1}\delta + \dots + c_{m,q,p-1}\delta^{p-1}$ для $(p-1)j(k-1) < q < (p-1)j(k-1) + d(u,a) - j(0)$, и по лемме 13 $c_{m,q,p-1} = 0$, а также ${}^{(z_{k-1},u)}_{d(u,t)-j(k-1)}\delta_{\zeta-d(u,t)}\big|_{\mathbb{F}_p(t)} = c_{d(u,t)-j(k-1),\zeta-d(u,t),1}\delta + \dots + c_{d(u,t)-j(k-1),\zeta-d(u,t),p-1}\delta^{p-1}$ с $c_{d(u,t)-j(k-1),\zeta-d(u,t),p-1} \neq 0$, если $\zeta - d(u,t) = j(0)$.

Итак, получается следующая картина: ${}^{(z_{k-1},u)}_{-j(k-1)}\delta_\zeta(t^p) \neq 0$, только если $\zeta = j(0) \pmod p$ или если $\zeta = j(k) + d(u,a) - j(0)$. В последнем случае

$${}^{(z_{k-1},u)}_{-j(k-1)}\delta_\zeta(t^p) = -{}^{(z_{k-1},u)}_{-j(k-1)}\delta_{d(u,t)}(t^p)c_{d(u,t)-j(k-1),j(k)-j(k-1),p-1},$$

где $c_{d(u,t)-j(k-1),j(k)-j(k-1),p-1}$ может быть вычислено с помощью леммы 13.

Теперь покажем существование такого параметра $z_k$, что ${}^{(z_k,u)}_{-j(k-1)}\delta_\zeta(t^p) = 0$ для $j(k) < \zeta < j(k) + d(u,a) - j(0)$. По лемме 3,ii) существует такая замена параметров $z_{k-1} \mapsto z' = z_{k-1} + bz_{k-1}^{p+1}$, что ${}^{(z',u)}_{-j(k-1)}\delta_{j(k)+p}(t^p) = 0$. Достаточно доказать, что любая такая замена, как в лемме 3,ii), при $p \mid q$ меняет только значения отображений ${}_{-j(k-1)}\delta_\zeta$, где $\zeta = j(0) \pmod p$. Действительно, если это так, мы можем сделать несколько замен и "убить" все ненулевые отображения ${}^{(z_{k-1},u)}_{-j(k-1)}\delta_\zeta$ при $j(k) < \zeta < j(k) + d(u,a) - j(0)$ ввиду того, что они все являются дифференцированиями и потому полностью определяются их значениями в $t^p$.

Для доказательства этого факта используем вычисления из доказательства п. ii) леммы 3. Так как $d(u,a) - j(0) \leqslant j(0)$, легко видеть, что для замены $z \mapsto z' = z + bz^{kp+1}$, $p > 2$, там выполняется

$$\begin{aligned}z'^{-j(k-1)}t^p z'^{j(k-1)} &= t^p + {}^{(z,u)}_{-j(k-1)}\delta_{j(k)}(t^p)z^{j(k)} \\ &\quad+ \dots + {}^{(z,u)}_{-j(k-1)}\delta_{j(k)+j(0)}(t^p)z^{j(k)+j(0)} + \dots .\end{aligned}$$

Так как $z' = z + bz^{kp+1}$, каждый элемент $z^l$ может быть записан в виде ряда по $z'$, где всякая степень равна $l$ по модулю $p$. Следовательно, эта замена коснется только отображений с правыми индексами, равными $j(k)$ по модулю $p$. Так как ${}^{(z_{k-1},u)}_{-j(k-1)}\delta_\zeta(t^p) \neq 0$, только если $\zeta = j(0) \pmod p$ при $\zeta < j(k) + d(u,a) - j(0)$, наше утверждение доказано.

Итак, существует такой параметр $z_k$, что ${}^{(z_k,u)}_{-j(k-1)}\delta_\zeta(t^p) \neq 0$, только если $\zeta = j(k) + d(u,a) - j(0)$ или $\zeta = j(k)$. Так как $z_k$ был построен как последовательность замен таких, как в лемме 3,ii), то ${}^{(z_k)}\alpha = {}^{(z_{k-1})}\alpha$ и ${}^{(z_k,u)}\delta_{j(q)} = {}^{(z_{k-1},u)}\delta_{j(q)}$ для всех $q \leqslant k$.

Наконец, докажем, что ${}^{(z_k,u)}_{-j(k)}\delta_\zeta(t^p) \neq 0$, только если $\zeta = j(k) + d(u,a) - j(0)$ или $\zeta = j(k)$. Но это следует прямо из определения этих отображений, так как $j(k) = j(k-1) \pmod p$, $d(u,a) - j(0) \leqslant j(0)$ и $\operatorname{char} D > 2$. В частности,

$$
\begin{aligned}
{}^{(z_k,u)}_{-j(k)}\delta_{j(k)}(t^p) &= {}^{(z_k,u)}_{-j(k-1)}\delta_{j(k)}(t^p),\\
{}^{(z_k,u)}_{-j(k)}\delta_{j(k)+d(u,a)-j(0)}(t^p) &= {}^{(z_k,u)}_{-j(k-1)}\delta_{j(k)+d(u,a)-j(0)}(t^p).
\end{aligned}
$$

Лемма доказана.

Теперь мы можем приступить к доказательству следующей теоремы.

Теорема 4. *Пусть $D$ – $p$-алгебра с делением характеристики $\operatorname{char} D = p > 2$ с центром $Z(D) = F$. Предположим, что $Z(\overline{D}) = \overline{D}$ и $\overline{D}/\overline{F}$ – простое чисто несепарабельное расширение, $\overline{D} = \overline{F}(a)$. Предположим, что полулокальная высота $i(u)$, не зависящая в этом случае от вложения $u$, не делится на $p$.*

*Тогда $d_D(a) > i(u)$.*

Доказательство. По лемме 12,ii) $[\overline{D} : \overline{F}] = [\Gamma_D : \Gamma_F]$. Следовательно, поле $F(\widetilde{a})$, где $\widetilde{a}$ – подъем $a$, есть максимальное "неразветвленное" подполе и $D$ – расщепимая алгебра с делением. Очевидно, что $\alpha = \mathrm{id}$.

Так как ${}^{(z,u)}\delta_{i(u,z)}$ – дифференцирование и $\overline{D}/\overline{F}$ – простое расширение, то ${}^{(z,u)}\delta_{i(u,z)}$ полностью определяется значением в $a$. Поэтому по лемме 3 $i(u,z)$ не зависит от $z$, и $i(u,z) = i(u)$. Следовательно, $i(u) = w(zu(a)z^{-1} - u(a))$ и $i(u)$ полностью определяется подъемом $u(a)$. С другой стороны, любой подъем $\widetilde{a}$ элемента $a$ определяет согласно лемме 9 вложение $\widetilde{a}$, и по лемме 10 $i(\widetilde{a})$ не зависит от $\widetilde{a}$. Следовательно, $i(u)$ не зависит от $u$.

Идея доказательства теперь заключается в следующем: мы рассмотрим линейные пространства, являющиеся образами отображений ${}^{(z,u)}\delta_{j(k)}|_{\overline{F}(a^{p^k})}$ в $\overline{D}$, где $j(k)$ были определены в лемме 14 и $z$, $u$ фиксированы. Покажем, что любое такое пространство имеет нулевое пересечение с остальными, если $d_D(a) \leqslant i(u)$. Затем покажем, что этот факт противоречит тому, что $u(a)$ порождает конечномерное пространство над $F$.

Итак, предположим $d_D(a) \leqslant i(u)$. Для вычисления пространств

$$
{}^{(z,u)}\delta_{j(k)}(\overline{F}(a^{p^k})) \in \overline{D}
$$

воспользуемся леммами 8, 13 и 14. Фиксируем параметр $z$, определенный в лемме 13. Согласно леммам 9, 10,iii) можно найти такой примитивный элемент $\overline{u} \in \overline{D}$ расширения $\overline{D}/\overline{F}$, что ${}^{(z,u)}\delta_{j(0)}(\overline{u}) = 1$, где $u$ – вложение, определенное леммой 9 для некоторого подъема $u$ элемента $\overline{u}$. Используя лемму 3,ii), можно найти такое вложение $u$, что ${}^{(z,u)}\delta_{d(u,\overline{u})}(\overline{u}) \notin {}^{(z,u)}\delta_{j(0)}(\overline{D})$. Зафиксируем это вложение. Непосредственно из лемм 3, 10 следует, что $d(u,\overline{u}) = d_D(\overline{u}) = d_D(a)$. Таким образом, без ограничения общности можно положить $a = \overline{u}$.

Положим

$$
J(k) := {}^{(z,u)}\delta_{j(k)}(a^{p^k}), \qquad A(k) := {}^{(z,u)}\delta_{j(k)}(\overline{F}(a^{p^k})),
$$
$$
A'(k) := \overline{F}(a^{p^{k+1}}) \cdot a^{p^k(p-1)} J(k).
$$

Имеем

$$A(k)=\bigoplus_{q=0}^{p-2}\overline{F}(a^{p^{k+1}})\cdot a^{p^k q}J(k),\qquad \overline{D}\cdot J(k)=A(k)\oplus A'(k)$$

как $\mathbb{F}_p$-линейные пространства.

Из леммы 8 следует, что

$$\begin{aligned}{}^{(z,u)}\delta_{j(k)}(a^{p^k})&={}^{(z_k,u)}\delta_{j(k)}(a^{p^k})\\&=q\,{}^{(z_{k-1},u)}_{-j(k-1)}\delta_{d(u,a^{p^{k-1}})}(a^{p^{k-1}})c_{d(u,a^{p^{k-1}})-j(k-1),(p-1)j(k-1),p-1},\end{aligned}$$

где $q\in\mathbb{F}_p^*$, $z_k$ определялись в лемме 13, $c_{d(u,a^{p^{k-1}})-j(k-1),(p-1)j(k-1),p-1}$ вычислялся в лемме 5,i) и он не равен нулю согласно лемме 5,ii), а ${}^{(z_{k-1},u)}_{-j(k-1)}\delta_{d(u,a^{p^{k-1}})}(a^{p^{k-1}})$ вычислялся в лемме 14. По последней лемме имеем

$${}^{(z_{k-1},u)}_{-j(k-1)}\delta_{d(u,a^{p^{k-1}})}(a^{p^{k-1}})=-j(k-1)\,{}^{(z,u)}\delta_{d(u,a^{p^{k-1}})}(a^{p^{k-1}}).$$

Собирая все эти вычисления вместе и используя индукцию, получаем, что $J(k)=q_kJ(k-1)^pJ(1)=\widetilde{q_k}J(1)^{p^{k-1}+p^{k-2}+\dots+1}$ для $k\geqslant 1$, где $q_k\in\mathbb{F}_p$.

Следовательно, имеет место следующая фильтрация:

$$\overline{F}\subset\dots\subset\overline{F}(a^{p^{k+1}})J(k+1)\subset\overline{F}(a^{p^k})J(k)\subset\dots\subset\overline{D}$$

и для любого $k\geqslant 1$ имеем $\overline{F}(a^{p^k})\cdot J(k)\subset A'(k-1)$. Поэтому $A(k)\cap A(k_1)=\{0\}$, если $k\neq k_1$.

Рассмотрим теперь элемент $b\in F$ такой, что $\overline{b}=a^{p^l}$ для некоторого $l>0$. Будем считать $l$ минимальным возможным. Такое число существует, потому что $D$ – конечномерная алгебра с делением над $F$. Пусть $b=u(a^{p^l})+b_1z+\cdots$, где $b_k\in u(\overline{D})$. Пусть $I:=\min_k\{w(zb_kz^{k-1}-b_kz^k)\}$ (предполагаем здесь, что $b_0=u(a^{p^l})$). Заметим, что $I<\infty$, так как по лемме 14 $j(l)<\infty$, т.е. ${}^{(z,u)}\delta_{j(l)}(a^{p^l})\neq 0$. Тогда выполняется

$$zbz^{-1}=\sum_{k=0}^{\infty}zb_kz^{k-1}=b+\sum_r{}^{(z,u)}\delta_{j(r)}(b_{q_r})z^I+\cdots=b,$$

где $b_{q_r}\in\overline{F}(a^{p^r})$ и $b_{q_r}\notin\overline{F}(a^{p^{r+1}})$. Итак, $\sum_r{}^{(z,u)}\delta_{j(r)}(b_{q_r})=0$, но этого не может быть, так как $A(k)\cap A(k_1)=\{0\}$, если $k\neq k_1$. Противоречие.

Теорема доказана.

Замечание. Было бы интересно получить ответы на следующие вопросы.

i) Пусть $D$ – алгебра с делением, как в теореме 4. Существует ли такая пара $(z,u)$, что все ненулевые отображения ${}^{(z,u)}\delta_q$ удовлетворяют условию $i(u)\mid q$? Если да, то должна существовать подалгебра $D'\subset D$ уровня 1 с $[D:D']<\infty$ (см. замечание перед леммой 8). Тогда можно было бы свести изучение алгебры $D$ к изучению алгебры уровня 1.

ii) Верно ли, что $D$ – хорошо расщепимая алгебра, т.е. циклическая? Вероятно, технические результаты из этой статьи помогут дать ответ на этот вопрос, по крайней мере, в случае уровня 1.

## Список литературы


1. *Jacob B., Wadsworth A.* Division algebras over Henselian fields // J. Algebra. 1990. V. 128. P. 126–179.
2. *Платонов В. П., Янчевский В. И.* Конечномерные алгебры с делением // Итоги науки и техники. Совр. проблемы матем. Фундамент. направления. Т. 77. М.: ВИНИТИ, 1991. С. 144–262.
3. *Saltman D. J.* Division algebras over discrete valued fields // Comm. Algebra 1980. V. 8. P. 1749–1774.
4. *Tignol J.-P.* Algebres a division et extensions de corps sauvagement ramifiees de degre premier // J. Reine Angew. Math. 1990. V. 404. P. 1–38.
5. *Schilling O. F. S.* The theory of valuations. Providence, RI: Amer. Math. Soc. 1950. (Math. Surveys Monogr. V. 4.)
6. *Жеглов А. Б.* О классификации двумерных локальных тел // Изв. РАН. Сер. матем. 2001. Т. 65. №1. С. 25–60.
7. *Azumaya G.* On maximally central algebras // Nagoya J. Math. 1951. V. 2. P. 119–150.
8. *Cohen I.* On the structure and ideal theory of complete local rings // Trans. Amer. Math. Soc. 1946. V. 59. P. 54–106.
9. *Aravire R., Jacob B.* $p$-algebras over maximally complete fields // K-theory and algebraic geometry: connections with quadratic forms and division algebras. Summer Research Institute on quadratic forms and division algebras, July 6–24, 1992, University of California, Santa Barbara, CA (USA). / ed. B. Jacob et al. Providence, RI: Amer. Math. Soc., 1995. P. 27–49. (Proc. Symp. Pure Math. V. 58. Part 2.)
10. *de Jong A. J.* The period-index problem for the Brauer group of an algebraic surface // Preprint; `http://www-math.mit.edu/~dejong`.
11. *Albert A. A.* Simple algebras of degree $p^e$ over a centrum of characteristic $p$ // Trans. Amer. Math. Soc. 1936. V. 40. P. 112–126.
12. *Pierce R. S.* Associative algebras. New York: Springer-Verlag, 1982.
13. *Morandi P.* Henselisation of a valued division algebra // J. Algebra. 1989. V. 122. P. 232–243.


Университет Гумбольдта, Берлин, Германия
*E-mail*: `azheglov@mathematik.hu-berlin.de`

Поступила в редакцию
20.05.2003