СЕРИЯ
МАТЕМАТИЧЕСКАЯ
Том 40, № 2, 1976

УДК 513.6

В. П. ПЛАТОНОВ

ПРОБЛЕМА ТАННАКА — АРТИНА И ПРИВЕДЕННАЯ K-ТЕОРИЯ

§ 1. Введение и формулировка основных результатов

Пусть A — простая конечномерная алгебра с центром K, $\mathrm{Nrd}_{A/K}: A \to K$ — приведенная норма A [см. (1), (2)], $SL(1, A) = (a \in A \mid \mathrm{Nrd}_{A/K}(a) = 1)$, $A^{(1)} = [A^*, A^*]$ — коммутант мультипликативной группы A^*.

Следующая очень естественная проблема была поставлена независимо Таннака и Артином в 1943 году [см. (3), (4)]: *будет ли* $SL(1, A) = A^{(1)}$? Так как A является полной матричной алгеброй $M_n(D)$, где D — тело, то из результатов Дьедонне об определителе над телом [см. (5)] легко следует эквивалентность: $SL(1, A) = A^{(1)} \Leftrightarrow SL(1, D) = D^{(1)}$. Хорошо известны и другие формулировки проблемы Таннака — Артина: 1) при $n>1$ фактор-группа группы $SL(1, A) = SL(n, D)$ по центру является простой; 2) при $n>1$ $SL(n, D)$ порождается унипотентными элементами; 3) $A^{(1)}$ является множеством всех K-точек аффинного K-многообразия.

Позднее, в 1963 году, Кнезер и Титс высказали общую гипотезу о том, что для простой односвязной K-изотропной алгебраической группы G группа $G_K/c(G_K)$, где $c(G_K)$ — центр G_K, является простой абстрактной группой [(6); обсуждения этой гипотезы см. в (7) — (10)]. Еще позднее, в 1968 году, в связи с развитием алгебраической K-теории Басс в числе двух важнейших проблем в книге (15), стр. 222, сформулировал проблему Таннака — Артина следующим образом: будет ли всегда приведенная группа Уайтхеда

$$SK_1(A) = SL(1, A)/A^{(1)} = 1?$$

Существовало убеждение, что проблема Таннака — Артина и гипотеза Кнезера — Титса должны иметь положительное решение. Были даже две работы Кодама (13), в которых утверждалось положительное решение проблемы Таннака — Артина, но они оказались ошибочными. Практически после работ Накаяма — Мацусима (3) и Ванга (4) не было никакого прогресса в проблеме Таннака — Артина, несмотря на многочисленные усилия. И даже для тел степени 4 проблема оставалась нерешенной, в то время как для тел простой степени положительное решение проблемы было получено Вангом в 1950 году (4).

Недавно автору в (11), (12) удалось доказать, вопреки ожиданиям, что проблема Таннака — Артина (следовательно, и проблема Басса) имеет отрицательное решение. Это повлекло за собой также опровержение общей гипотезы Кнезера — Титса. Оказалось, что с точки зрения множества полей K равенство $SK_1(A)=1$ является скорее исключением, нежели правилом для тел, индекс которых делится на квадрат простого числа. В существенной мере удалось выяснить и общий механизм отрицательного решения проблемы Таннака — Артина. При этом обнаружились глубокие связи с теорией полей классов и арифметикой вообще (в особенности с арифметикой куммеровых расширений), что дало возможность для широкого класса полей K неожиданным образом вычислить группу $SK_1(A)$.

Цель настоящей работы — подробное изложение основных результатов статей ([11]), ([12]). Я следую, главным образом, статье ([12]), содержащей более общие и законченные результаты.

Во введении формулируются только наиболее существенные результаты, которые располагаются не по степени их важности, а в порядке их последовательного получения в статье.

В дальнейшем, как правило, через A обозначается тело с центром K, $[A:K]=n^2$. $k(x_1, x_2, \ldots, x_m)$ — поле рациональных функций от переменных $x_1, x_2, \ldots, x_m$ с полем констант k; $k\langle x_1, x_2, \ldots, x_m\rangle$ и $k[[x_1, x_2, \ldots, x_m]]$ — соответственно поле и кольцо формальных степенных рядов над k.

Если A — тело над полным дискретно нормированным полем K, то через O_A, O_K обозначается соответственно кольцо целых элементов A и K; $\mathfrak{P}_A$, $\mathfrak{P}_K$ — простые идеалы O_A, O_K; $\bar{A}=O_A/\mathfrak{P}_A$, $\bar{K}=O_K/\mathfrak{P}_K$. Предполагается, что $\bar{A}$ сепарабельно над $\bar{K}$.

КОНГРУЭНЦ-ТЕОРЕМА 3.12. *Если $a\in SL(1, A)$ и $a\equiv 1 \pmod{\mathfrak{P}_A}$, то $a\in A^{(1)}$.*

С л е д с т в и е 3.13. *Для неразветвленного тела A*

$$SK_1(A)\simeq SK_1(\bar{A}).$$

Это следствие показывает, что исследование $SK_1(A)$ для тел A над полными дискретно нормированными полями не является фактически ограничением, ибо тело B над произвольным полем k является телом вычетов $\bar{A}$ для $A=B\otimes k\langle x\rangle$.

Пусть A — циклическая простая алгебра над K, т. е. A есть скрещенное произведение циклического расширения R/K и группы $\mathrm{Gal}(R/K)$. Будем обозначать тогда A через $A(a, R)$, где a — определяющий элемент из K.

Рассмотрим циклические алгебры $A(x, R_1)$ и $A(y, R_2)$ над полем $K=k(x, y)$, где R_1, R_2 — циклические расширения поля k.

ТЕОРЕМА 4.7. *Тензорное произведение $A(x, R_1)\otimes_{k(x,y)}A(y, R_2)$ тогда и только тогда является телом, когда $R_1\otimes_k R_2$ — поле, т. е. R_1 и R_2 линейно разделены над k.*

В ([12]) был введен новый объект в теории полей — *группы специальных проективных конорм*, играющий важную роль в дальнейшем. Пусть $L\supset R\supset k$ — башня нормальных расширений поля k, где R — циклическое расширение k степени n, $\{\sigma\}=\mathrm{Gal}(R/k)$. Рассмотрим фактор-группу

$R^*/k^*N_{L/R}(L^*)$. Элемент $a^* \in R^*/k^*N_{L/R}(L^*)$ называется специальной проективной конормой, если для его представителя $a \in a^*$ $a^{1-\sigma} \in N_{L/R}(L^*)$. Множество всех специальных проективных конорм образует подгруппу $R^*/k^*N_{L/R}(L^*)$, которую будем называть группой специальных проективных конорм, соответствующей башне $L \supset R \supset k$, и обозначать через $\mathcal{P}(L, R, k)$.

Следующая теорема играет центральную роль.

ТЕОРЕМА РЕДУКЦИИ 4.11. *Пусть* $A(R_1, R_2) = A(x, R_1) \underset{k\langle x,y\rangle}{\otimes} A(y, R_2)$ *является телом. Тогда существует сюръективный морфизм*

$$\varphi : SK_1(A(R_1, R_2)) \to \mathcal{P}(R_1R_2, R_2, k).$$

Если $SK_1(\bar{A}(R_1, R_2)) = 1$, *то* φ — *изоморфизм; в частности, если* $[R_1 : k]$ *не делится на квадрат простого числа, то* $SK_1(A(R_1, R_2)) \simeq \mathcal{P}(R_1R_2, R_2, k)$.

Теорема редукции в существенной мере сводит вычисление группы $SK_1(A(R_1, R_2))$ к вычислению группы специальных проективных конорм, а это уже задача теории полей.

В ряде случаев можно непосредственно вычислить группу $\mathcal{P}(R_1R_2, R_2, k)$ и показать, что она далеко не всегда тривиальна. Более эффективной оказывается когомологическая интерпретация группы $\mathcal{P}(R_1R_2, R_2, k)$, которая равносильна интерпретации группы $\mathcal{P}(R_1R_2, R_2, k)$ посредством групп Брауэра *.

Пусть $L = R_1 \otimes_k R_2$. Через $\mathrm{Br}(L/k)$, $\mathrm{Br}(R_1/k)$, $\mathrm{Br}(R_2/k)$ обозначаются подгруппы группы Брауэра $\mathrm{Br}(k)$, состоящие из элементов, разложимых соответственно над L, R_1, R_2. Группы $\mathrm{Br}(R_1/k)$, $\mathrm{Br}(R_2/k)$ канонически вкладываются в $\mathrm{Br}(L/k)$, и мы будем отождествлять их с образами в $\mathrm{Br}(L/k)$. С помощью техники когомологий Галуа доказывается

ТЕОРЕМА 4.17. *Группа* $\mathcal{P}(L, R_2, k) \simeq \mathrm{Br}(L/k)/(\mathrm{Br}(R_1/k)\mathrm{Br}(R_2/k))$.

В качестве одного из следствий этой теоремы получается симметричность группы специальных проективных конорм.

ТЕОРЕМА 5.7. *Пусть* R_1, R_2 — *циклические расширения поля* k, *являющегося глобальным или локально компактным полем. Тогда для тела* $A(R_1, R_2)$ *над* $k\langle x, y\rangle$

$$SK_1(A(R_1, R_2)) \simeq \mathrm{Br}(L/k)/(\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)).$$

Для локально компактного поля k из теорем 4.17, 5.7 и теоремы взаимности локальной теории полей классов следует окончательный результат.

ТЕОРЕМА 5.9. *Если поле* k *локально компактно и* $A(R_1, R_2)$ *является телом, то* $SK_1(A(R_1, R_2))$ — *циклическая группа порядка* $([R_1 : k], [R_2 : k])$.

В случае глобального поля k, т. е. поля алгебраических чисел или поля алгебраических функций одной переменной с конечным полем кон-

* Я признателен профессору Ж. П. Серру, который обратил мое внимание на эффективный характер такой интерпретации.

стант, также получены почти предельные оценки для группы $SK_1(A(R_1, R_2))$ (теоремы 5.15, 5.17).

Мы ограничимся во введении формулировкой только окончательного результата для наиболее существенного случая, когда $[R_1:k]=[R_2:k]=p$, где p — простое число.

ТЕОРЕМА 5.13. *Пусть* $L=R_1\otimes_k R_2$, $[R_1:k]=[R_2:k]=p$, *где* k — *глобальное поле. Тогда для тела* $A(R_1, R_2)$ *группа* $SK_1(A(R_1, R_2))\simeq(Z/pZ)^{d-1}$, *где* $d=d(L/k)$ — *число точек поля* v *на* k, *для которых* $[L_v:k_v]=[L:k]$.

Пусть теперь $A(\sqrt{p}, \sqrt{r})=A(x, Q(\sqrt{p}))\otimes_{Q\langle x,y\rangle}A(y, Q(\sqrt{r}))$, где p, r — различные простые числа. Именно такие тела впервые рассматривались в моей статье ([11]) и именно они доставляют минимальные контрпримеры к проблеме Таннака — Артина. Через $\left(\frac{p}{r}\right)$ обозначается символ Лежандра.

ТЕОРЕМА 5.19. *Группа* $SK_1(A(\sqrt{p}, \sqrt{r}))$ *может быть только трех типов*:

I) $SK_1(A(\sqrt{p}, \sqrt{r}))=1$ *тогда и только тогда, когда выполняется одно из двух условий*:

a) $\left(\frac{p}{r}\right)=\left(\frac{r}{p}\right)=1$;

b) $\left(\frac{p}{r}\right)=-\left(\frac{r}{p}\right)$, $pr\equiv 1 \pmod 8$.

II) $SK_1(A(\sqrt{p}, \sqrt{r}))\simeq Z/2Z$ *тогда и только тогда, когда выполняется одно из двух условий:*

a) $\left(\frac{p}{r}\right)=\left(\frac{r}{p}\right)=-1$, $p\vee r\vee pr\equiv 1 \pmod 8$;

b) $\left(\frac{p}{r}\right)=-\left(\frac{r}{p}\right)$, $pr\not\equiv 1 \pmod 8$.

III) $SK_1(A(\sqrt{p}, \sqrt{r}))\simeq(Z/2Z)^2$ *тогда и только тогда, когда* $\left(\frac{p}{r}\right)=\left(\frac{r}{p}\right)=-1$, $p, r, pr\not\equiv 1 \pmod 8$.

Естественно возникает вопрос: всякая ли конечная абелева группа экспоненты p реализуется в виде $SK_1(A(R_1, R_2))$? Ответ оказывается утвердительным. k_0 обозначает минимальное глобальное поле.

ТЕОРЕМА 6.2. *Для всякой группы* $(Z/pZ)^i$, $i\geqslant 0$, *существуют такие циклические расширения* $R_1^{(i)}/k_0$, $R_2^{(i)}/k_0$ *степени* p, *что*

$$SK_1(A(x, R_1^{(i)})\otimes_{k_0\langle x,y\rangle}A(y, R_2^{(i)}))\simeq(Z/pZ)^i.$$

Следствие 6.3. *Для любого простого* p *существует такое* A *над* $Q\langle x, y\rangle$ *степени* p^2, *что* $SK_1(A)=1$, *но для подходящего поля* r-*адических чисел* Q_r $SK_1(A\otimes_Q Q_r)\simeq Z/pZ$.

Заметим, что на первый взгляд следствие 6.3 кажется удивительным. Истинная причина состоит в том, что не все локальные символы Гильберта поднимаются до глобальных.

Если F — чисто трансцендентное расширение поля K, то канонический морфизм $SK_1(A) \to SK_1(A \otimes_K F)$ является инъективным. Следовательно, результаты статьи сохраняют силу для произвольных полей формальных степенных рядов и полей рациональных функций. Более того, верна следующая заключительная

ТЕОРЕМА 6.7. *Пусть K — конечнопорожденное поле. Если степень трансцендентности K над простым подполем больше единицы при* $\operatorname{char} K = 0$ *и больше двух при* $\operatorname{char} K > 0$, *то для произвольного числа m существует такое тело с центром K, что* $\operatorname{Card} SK_1(A) > m$.

Обсуждение дальнейших перспектив и некоторые гипотезы приведенной K_1-теории содержатся в § 7.

Хотя мы и придаем результатам статьи ([12]) более общую и завершенную форму, достижение максимальной общности не является нашей целью. Это могло бы несколько затушевать возникшие здесь идеи и нестандартные связи.

§ 2. Приведенная группа Уайтхеда над произвольными полями

2.1. Пусть A — центральное тело над K, размерность $[A:K] = n^2$. $\operatorname{Nrd}_{A/K} : A \to K$ — приведенная норма A над K. Тензорное произведение $A \otimes_K F$, где F — расширение поля K, будем обозначать через A_F. Отметим, что для $a \in A$ $\operatorname{Nrd}_{A/K}(a) = \operatorname{Nrd}_{A_F/F}(a)$. $A^{(1)} = [A^*, A^*]$ — коммутант мультипликативной группы A^*,

$$SL(1, A) = (a \in A \mid \operatorname{Nrd}_{A/k}(a) = 1), \quad SK_1(A) = SL(1, A)/A^{(1)}.$$

Непосредственно из теоремы Дьедонне об определителе над телом вытекает следующая лемма [см. ([4])].

ЛЕММА. *Пусть F — конечное расширение поля K степени m. Если $a \in A \cap A_F^{(1)}$, то $a^m \in A^{(1)}$.*

Если, в частности, взять в качестве F максимальное подполе A, то $SL(1, A) = A \cap SL(1, A_F) = A \cap A_F^{(1)}$, ибо $A_F \simeq M_n(F)$ — полная матричная алгебра степени n над F. Поэтому для всякого $a \in SL(1, A)$ $a^n \in A^{(1)}$, т. е. n — экспонента группы $SK_1(A) = SL(1, A)/A^{(1)}$.

2.2. Для всякого конечного расширения F поля K имеем канонический гомоморфизм $\tau_F : SK_1(A) \to SK_1(A_F)$.

ЛЕММА. *Если* $([F:K], n) = 1$, *то отображение* $\tau_F : SK_1(A) \to SK_1(A_F)$ *инъективно.*

Доказательство. Пусть $a \in SK_1(A)$ и $\tau_F(a) = 1$. Из леммы 2.1 следует, что $a^{[F:K]} = a^n = 1$. Тогда $a^{([F:K], n)} = a = 1$.

2.3. Пусть $n = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ — каноническое представление числа n. Тогда существует соответствующее представление A в виде тензорного произведения: $A = \prod_{i=1}^{m} \otimes_K A(p_i)$, где $[A(p_i):K] = p_i^{2d_i}$. Возникает естественный вопрос: в какой мере группа $SK_1(A)$ определяется группами $SK_1(A(p_i))$? В частности, если группы $SK_1(A(p_i)) = 1$, будет ли

$SK_1(A)=1$? Оказывается, все зависит от того, будет ли из $SK_1(A(p_i))=1$ следовать $SK_1(A_F(p_i))=1$ для конечных расширений F поля K.

ЛЕММА. *Если для всякого конечного расширения F поля K $SK_1(A_F(p_i))=1$, $i=1, 2, \ldots, m$, то $SK_1(A)=1$.*

Доказательство. Пусть F_i — максимальное подполе $A(p_i)$, $R_i=\prod\limits_{d\neq i}\otimes_K F_d$. Тогда

$$SK_1(A_{R_i}(p_i))=1\Rightarrow \forall a\in SK_1(A),\quad a^{[R_i:K]}=1.$$

Но все $[R_i:K]$, $i=1, \ldots, m$, в совокупности взаимно просты, значит, $a^{([R_1:K],[R_2:K],\ldots,[R_m:K])}=a=1$.

2.4. Пусть $[A:K]=p^{2\alpha}$, где p — простое число, $a\in SL(1, A)$. Если F — максимальное подполе, содержащее a, то можно считать, что F не чисто несепарабельно над K, в противном случае $\operatorname{char} K=p$ и норма $N_{F/K}(a)=a^{p^\alpha}=1\Rightarrow a=1$.

Пусть F_S — максимальное сепарабельное подполе F и L — его поле разложения. Тогда для силовской p-подгруппы G_p группы $\mathrm{Gal}(L_S/K)$ через $L(G_p)$ обозначим подполе G_p-инвариантных элементов L_S. Так как $(p, [L(G_p):K])=1$, то $A_{L(G_p)}$ будет телом, причем $F\otimes_K L(G_p)$ — его максимальное подполе. $G_p\simeq \mathrm{Gal}(L_S/L(G_p))$, поэтому существует последовательность циклических расширений степени p: $L(G_p)\subset L_1\subset L_2\subset\ldots\subset L_S$, проходящая через $F_S\otimes_K L(G_p)$. Следовательно, в $F\otimes_K L(G_p)$ существует циклическое расширение $L(G_p)$ степени p.

По лемме 2.2 $SK_1(A)\subsetneq SK_1(A_{L(G_p)})$, поэтому иногда можно считать элемент a принадлежащим такому максимальному подполю $F\subset A$, которое обладает циклическим подполем R/K степени p.

2.5. Предложение ([4]). *Экспонента группы $SK_1(A)$ есть $n/p_1p_2\ldots p_m$; в частности, если n не делится на квадрат простого числа, то $SK_1(A)=1$.*

Доказательство. Как в лемме 2.3, все сводится к случаю $n=p_1p_2\ldots p_m$, который в свою очередь сводится к случаю $n=p$. А рассуждение п. 2.4 редуцирует доказательство к следующей ситуации: $a\in SL(1, A)\cap F$, где F/K — циклическое расширение степени p. По теореме 90 Гильберта $a=b^{1-\sigma}$, где $\{\sigma\}=\mathrm{Gal}(F/K)$, $b\in F$. Следовательно, по теореме Сколема — Нетер $a=bgb^{-1}g^{-1}$, $g\in A^*$.

2.6. ЛЕММА. *Пусть φ — автоморфизм тела A. Тогда*

$$(\mathrm{Nrd}_{A/K}(a))^\varphi=\mathrm{Nrd}_{A/K}(a^\varphi)\quad \forall a\in A.$$

Доказательство. Если $f_a(x)=\sum\limits_{i=0}^{d}\alpha_i x^i$ — минимальный многочлен a над K, то $f_{a^\varphi}(x)=\sum\limits_{i=0}^{d}\alpha_i^\varphi x^i$ — минимальный многочлен для a^φ. $\mathrm{Nrd}_{A/K}(a)=(-1)^n\alpha_0^{n/d}$. Тогда

$$\mathrm{Nrd}_{A/K}(a^\varphi)=(-1)^n(\alpha_0^\varphi)^{n/d}=(\mathrm{Nrd}_{A/K}(a))^\varphi.$$

2.7. ЛЕММА. *Пусть F — чисто трансцендентное расширение поля K. Тогда отображение $\tau_F: SK_1(A) \to SK_1(A_F)$ инъективно* *.

Доказательство. Если $a \in SL(1, A) \cap A_F^{(1)}$, то для подходящей K-специализации базиса трансцендентности поля F над K $a \in A^{(1)}$.

2.8. Замечание. Предыдущие леммы показывают важность вопроса о поведении группы $SK_1(A)$ при расширении поля K. На первый взгляд кажется вероятным, что $SK_1(A) = 1 \Rightarrow SK_1(A_F) = 1$ для расширения F поля K. Однако в § 6 будет построен пример, «патологичный» во многих смыслах, дающий отрицательный ответ: существуют такие A, что $SK_1(A) = 1$, но $SK_1(A_F) \neq 1$ для подходящего F.

§ 3. Тела над дискретно нормированными полями

3.1. В этом параграфе будем предполагать, что A — тело над полным дискретно нормированным полем K. Через O_K, O_A обозначается соответственно кольцо целых элементов K, A. $\mathfrak{P}_K$, $\mathfrak{P}_A$ — простые идеалы соответственно O_K и O_A. $\bar{A}$ всегда обозначает тело вычетов $O_A/\mathfrak{P}_A$, $\bar{K} = O_K/\mathfrak{P}_K$. Для $a \in O_A$ через $\bar{a}$ обозначается образ в теле вычетов $\bar{A}$. В дальнейшем предполагается, что центр тела $\bar{A}$ сепарабелен над $\bar{K}$. Основные сведения о структуре тела A содержатся в ([16]), гл. 5, ([17]), гл. 12. Необходимые из них приводятся ниже.

Пусть $Z(\bar{A})$ — центр $\bar{A}$. Тогда $[Z(\bar{A}):\bar{K}] = e(A)$, где $e(A)$ — индекс ветвления A, причем $Z(\bar{A})$ — циклическое расширение $\bar{K}$; $n = re(A)$, где $[\bar{A} : Z(\bar{A})] = r^2$. Если $e(A) = 1$, то тело A называется неразветвленным над K.

Через π_A обозначается простой элемент тела A. π_A определяет на O_A внутренний автоморфизм φ, который индуцирует на $\bar{A}$ автоморфизм $\bar{\varphi}$ порядка $e(A)$, причем его ограничение на $Z(\bar{A})$ порождает $\mathrm{Gal}(Z(\bar{A})/\bar{K})$ [см., например, ([18])].

В A существуют неразветвленные максимальные подполя, которые описываются следующим образом. Тело $\bar{A}$ обладает над $Z(\bar{A})$ сепарабельным максимальным подполем $\bar{F}$, которое будет сепарабельно и над $\bar{K}$. Пусть α — примитивный элемент поля $\bar{F}$ над $\bar{K}$, a — прообраз α при редукции. Тогда $K(a)$ — неразветвленное максимальное подполе A. Индекс ветвления произвольного максимального подполя F тела A делит $e(A)$, причем $\exists F$, $e(F) = e(A)$.

3.2. ЛЕММА. *Если $a \in SL(1, A)$, то* $N_{Z(\bar{A})/\bar{K}}(\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\bar{a})) = 1$.

Доказательство. Пусть F — максимальное подполе A, содержащее a. Тогда $\mathrm{Nrd}_{A/K}(a) = N_{F/K}(a) = 1$. При редукции по модулю $\mathfrak{P}_A$ норма обладает следующим свойством [см. ([14]), гл. 1]:

$$\overline{N_{F/K}(a)} = (N_{\bar{F}/\bar{K}}(\bar{a}))^{e(F)} = 1,$$

где $e(F)$ — индекс ветвления поля F. Если теперь T — максимальное подполе $\bar{A}$, содержащее $\bar{F}$, то $[T:\bar{K}] = n$. Но $[\bar{F}:\bar{K}]e(F) = n$, поэтому $[T:\bar{F}] =$

* В действительности это отображение является изоморфизмом.

$=e(F)$ и транзитивность нормы влечет:

$$N_{Z(\bar{A})/\bar{K}}(\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\bar{a})) = N_{T/\bar{K}}(\bar{a}) = (N_{\bar{F}/\bar{K}}(\bar{a}))^{e(F)} = 1.$$

Лемма доказана.

3.3. ЛЕММА. *Для всякого $\alpha \in \bar{A}$ с условием*

$$N_{Z(\bar{A})/\bar{K}}(\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\alpha)) = 1$$

существует такой элемент $a \in SL(1, A)$, что $\bar{a} = \alpha$.

Доказательство. Пусть b — прообраз α при редукции, т. е. $\bar{b} = \alpha$, $b \in O_A$. Если F — максимальное подполе A, содержащее b, то

$$\overline{\mathrm{Nrd}_{A/K}(b)} = \overline{N_{F/K}(b)} = (N_{\bar{F}/\bar{K}}(\bar{b}))^{e(F)} = N_{Z(\bar{A})/\bar{K}}(\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\alpha)) = 1.$$

Следовательно, $\mathrm{Nrd}_{A/K}(b) \in 1 + \mathfrak{P}_K$. Если L — неразветвленное расширение поля K, то хорошо известно, что $N_{L/K}(1+\mathfrak{P}_L) = 1 + \mathfrak{P}_K$ [см. ([17]), стр. 90]. Но в A существует неразветвленное максимальное подполе R (см. п. 3.1). Поэтому можно выбрать такой элемент $t \in 1 + \mathfrak{P}_R \subset 1 + \mathfrak{P}_A$, что $\mathrm{Nrd}_{A/K}(t) = N_{R/K}(t) = \mathrm{Nrd}_{A/K}(b)$. Отсюда следует, что для $a = bt^{-1}$ имеем: $\mathrm{Nrd}_{A/K}(a) = 1$, $\bar{a} = \alpha$. Лемма 3.3 доказана.

3.4. Предложение. $\overline{SL(1, A)} = (\alpha \in \bar{A} \mid N_{Z(\bar{A})/\bar{K}}(\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\alpha)) = 1)$.

Доказательство немедленно следует из лемм 3.2 и 3.3.

3.5. Предыдущее предложение описывает образ группы $SL(1, A)$ при редукции. Следующее утверждение характеризует образ коммутанта.

Предложение. Пусть $b \in A^{(1)} = [A^*, A^*]$. *Тогда*

$$\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\bar{b}) = \beta^{1-\sigma},$$

где $\beta \in \mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\bar{A})$, σ — *порождающий элемент группы* $\mathrm{Gal}(Z(\bar{A})/\bar{K})$.

Доказательство. Нетрудно видеть, что ввиду мультипликативности приведенной нормы при фиксированном σ достаточно доказать предложение для элемента $b = a_1 a_2 a_1^{-1} a_2^{-1}$, где $a_1, a_2 \in A^*$. Пусть π — простой элемент в A. Тогда $a_1 = \pi^r d_1$, $a_2 = \pi^t d_2$, где $d_1, d_2 \in O_A^*$. Обозначим через φ внутренний автоморфизм A, порождаемый π, и будем считать, что $\sigma = \bar{\varphi}$ (см. п. 3.1). Имеем:

$$[a_1, a_2] = \pi^r d_1 \pi^t d_2 (\pi^r d_1)^{-1} (\pi^t d_2)^{-1} =$$

$$= \pi^r d_1 \pi^t (\pi^r d_1)^{-1} \pi^{-t} [\pi^t (\pi^r d_1) \pi^{-t}, \pi^t d_2 \pi^{-t}] =$$

$$= a_1 (a_1^{-1})^{\varphi^t} [\pi^r d_1^{\varphi^t}, d_2^{\varphi^t}] = a_1 (a_1^{-1})^{\varphi^t} [d_1^{\varphi^{t+r}}, d_2^{\varphi^{t+r}}] d_2^{\varphi^{t+r}} (d_2^{-1})^{\varphi^t} =$$

$$= d_1^{\varphi^r} (d_1^{-1})^{\varphi^{r+t}} [d_1^{\varphi^{t+r}}, d_2^{\varphi^{t+r}}] d_2^{\varphi^{t+r}} (d_2^{-1})^{\varphi^t}.$$

Вычислим теперь $\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}(\overline{[a_1, a_2]})$, применяя лемму 2.6. Для сокращения будем писать Nrd вместо $\mathrm{Nrd}_{\bar{A}/Z(\bar{A})}$:

$$\mathrm{Nrd}(\overline{[a_1, a_2]}) = \mathrm{Nrd}(\bar{d}_1^{\sigma^r} (\bar{d}_1^{-1})^{\sigma^{r+t}} [\bar{d}_1^{\sigma^{r+t}}, \bar{d}_2^{\sigma^{r+t}}] \bar{d}_2^{\sigma^{r+t}} (\bar{d}_2^{-1})^{\sigma^t}) =$$

$$= \mathrm{Nrd}\,(\bar{d}_1^{\sigma^r}(\bar{d}_1^{-1})^{\sigma^{r+t}})\,\mathrm{Nrd}\,(\bar{d}_2^{\sigma^{r+t}}(\bar{d}_2^{-1})^{\sigma^t}) = \mathrm{Nrd}\,(\bar{d}_1^{\sigma^r}\bar{d}_1^{\sigma^{r+1}}\ \ldots\ \bar{d}_1^{\sigma^{r+t-1}})^{1-\sigma}\times$$
$$\times\,\mathrm{Nrd}\,(\bar{d}_2^{-\sigma^t}\bar{d}_2^{-\sigma^{t+1}}\ \ldots\ \bar{d}_2^{-\sigma^{t+r-1}})^{1-\sigma} = \mathrm{Nrd}\,(\bar{d}_1^{\sigma^r+\sigma^{r+1}+\ldots+\sigma^{r+t-1}})^{1-\sigma}\times$$
$$\times\,\mathrm{Nrd}\,((\bar{d}_2^{-1})^{\sigma^t+\sigma^{t+1}+\ldots+\sigma^{t+r-1}})^{1-\sigma} =$$
$$= \mathrm{Nrd}\,(\bar{d}_1^{\sigma^r+\sigma^{r+1}+\ldots+\sigma^{r+t-1}}(\bar{d}_2^{-1})^{\sigma^t+\sigma^{t+1}+\ldots+\sigma^{t+r-1}})^{1-\sigma} = \beta^{1-\sigma}.$$

Предложение доказано.

3.6. ЛЕММА. *Пусть* $A = \prod_{i=1}^{m} \otimes_K A(p_i)$ — *примарное разложение тела* A. *Тогда индекс ветвления* $e(A) = \prod_{i=1}^{m} e(A(p_i))$.

Доказательство. Так как индекс ветвления подтела делит индекс ветвления тела, то $e(A)$ делится на $\prod_{i=1}^{m} e(A(p_i))$, ввиду взаимной простоты чисел $e(A(p_i))$. Но по 3.1

$$[A(p_i):K] = [\overline{A(p_i)} : Z(\overline{A(p_i)})]\, e(A(p_i)),$$
$$\overline{A(p_i)} \otimes_{Z(\overline{A(p_i)})} Z(\bar{A}) \subset \bar{A}.$$

Следовательно, $[\bar{A}:Z(\bar{A})]$ делится на $[\overline{A(p_i)}:Z(\overline{A(p_i)})]$. А это означает, что p_i — часть числа $e(A)$ совпадает с $e(A(p_i))$. Лемма доказана.

3.7. ЛЕММА. *Пусть* L — *циклическое неразветвленное расширение поля* K, $\{\sigma\} = \mathrm{Gal}(L/K)$. *Если* $b \in 1+\mathfrak{P}_L$ *и* $N_{L/K}(b) = 1$, *то существует такое* $a \in 1+\mathfrak{P}_L$, *что* $a^{1-\sigma} = b$.

Доказательство. По теореме 90 Гильберта существует представление $x^{1-\sigma} = b$ для подходящего $x \in L$. Можно считать, что $x \in O_L$. Тогда имеем следующие простые импликации:

$$x = bx^{\sigma} \Rightarrow \bar{x} = \bar{x}^{\bar{\sigma}} \Rightarrow \bar{x} \in \bar{K} \Rightarrow \exists t \in O_K^{\bullet},\quad xt^{-1} \equiv 1 \pmod{\mathfrak{P}_L}.$$

Следовательно, в качестве a можно взять xt^{-1}.

3.8. ЛЕММА. *Пусть* $a \in (1+\mathfrak{P}_A) \cap SL(1, A)$. *Тогда существует такой элемент* $t \in A^{(1)}$, *что* $at \in (1+\mathfrak{P}_A) \cap F$, *где* F — *неразветвленное максимальное подполе в* A.

Доказательство. Если z — такой элемент в O_A, что $K(z)$ — неразветвленное максимальное подполе, то рассмотрим $K(az) = F$. Так как $\overline{az} = \bar{z}$, то F является неразветвленным максимальным подполем, ибо $\bar{F} = \overline{K(z)}$. Пусть $f(x)$ — минимальный многочлен для z над K. По лемме Гензеля в O_F существует корень многочлена $f(x)$, сравнимый с z по модулю идеала $\mathfrak{P}_A$. Обозначим его через b. Так как поля $K(z)$ и $K(b)$ являются K-изоморфными, то существует такой элемент $g \in A^{\bullet}$, что $b = gzg^{-1}$. Тогда при $t = zgz^{-1}g^{-1}$ элемент at удовлетворяет требованиям леммы. Действительно, $at = azgz^{-1}g^{-1} \in F$, ибо az, $gz^{-1}g^{-1} \in F$. Кроме того, $\overline{at} = \overline{az}\,\overline{gz^{-1}g^{-1}} = 1$. Лемма доказана.

3.9. Предложение. *Пусть $[A:K]=p^{\alpha}$, где p — простое число. Тогда всякий элемент $a\in(1+\mathfrak{P}_A)\cap SL(1,A)$ содержится в коммутанте $A^{(1)}$.*

Доказательство. Применяем индукцию по размерности A над центром. Из леммы 3.8 следует, что можно считать $a\in F$, где F — неразветвленное максимальное подполе A. Через L обозначим минимальное нормальное расширение поля K, содержащее F; $G=\mathrm{Gal}(L/K)$, G_p — силовская p-подгруппа G, $L(G_p)$ — подполе G_p-неподвижных элементов в L. Так как $[A:K]$ и $[L(G_p):K]$ взаимно просты, то $A\otimes_K L(G_p)$ является телом, $F\otimes_K L(G_p)=T$ — максимальное подполе $A_{L(G_p)}$. Из конструкции T следует, что в T имеется подполе T_p, являющееся циклическим расширением $L(G_p)$ (см. п. 2.4). Оно соответствует некоторой максимальной подгруппе группы G_p. По построению элемент $a\in(1+\mathfrak{P}_{A_{L(G_p)}})\cap SL(1,A_{L(G_p)})$, $A_{L(G_p)}=A\otimes_K\otimes_K L(G_p)$ и из леммы 2.2 следует, что достаточно доказать предложение для тела $A_{L(G_p)}$. Можно считать поэтому, не ограничивая общности, что поле F содержит циклическое подполе T_p.

Рассмотрим централизатор $\Delta=C_A(T_p)$. Так как $[\Delta:T_p]<[A:K]$, то по предположению индукции для Δ наше утверждение справедливо. Имеем:

$$\mathrm{Nrd}_{A/K}(a)=\mathrm{Nrd}_{F/K}(a)=N_{T_p/K}(N_{F/T_p}(a))=N_{T_p/K}(\mathrm{Nrd}_{\Delta/T_p}(a))=1.$$

Следовательно, $\mathrm{Nrd}_{\Delta/T_p}(a)=b^{1-\sigma}$, где $b\in T_p$, $\{\sigma\}=\mathrm{Gal}(T_p/K)$. Так как $a\in 1+\mathfrak{P}_A$, то $\mathrm{Nrd}_{\Delta/T_p}(a)\in 1+\mathfrak{P}_{T_p}$. По лемме 3.7 можно выбрать $b\in 1+\mathfrak{P}_{T_p}$. Но F — неразветвленное расширение T_p, поэтому $N_{F/T_p}(1+\mathfrak{P}_F)=1+\mathfrak{P}_{T_p}$. Отсюда следует существование такого элемента $t\in 1+\mathfrak{P}_F$, что $\mathrm{Nrd}_{\Delta/T_p}(t)=b$. Как всякий K-изоморфизм, σ продолжается до внутреннего автоморфизма тела A, порождаемого элементом $g\in A^*$. Тогда $b^{1-\sigma}=bgb^{-1}g^{-1}$ и элемент $gtg^{-1}\in\Delta$, ибо $gT_pg^{-1}=T_p$. Для элемента $h=agtg^{-1}t^{-1}\in\Delta$ с учетом леммы 2.6 приведенная норма $\mathrm{Nrd}_{\Delta/T_p}(h)=1$, $t\in 1+\mathfrak{P}_A$, $gtg^{-1}t^{-1}\in 1+\mathfrak{P}_A$, поэтому $h\in(1+\mathfrak{P}_A)\cap SL(1,A)$. Для завершения доказательства необходимо воспользоваться индуктивным предположением. Предложение доказано.

3.10. Пусть D — простая алгебра с центром K. Тогда $D\simeq M_d(\Delta)$, где Δ — алгебра с делением над K. Напомним, как устроены максимальные порядки в D [см. ([16]), ([19])]: всякий максимальный порядок в $M_d(\Delta)$ сопряжен с $M_d(O_\Delta)$; $M_d(\mathfrak{P}_\Delta)$ — единственный простой двусторонний идеал в $M_d(O_\Delta)$. Поэтому естественно простой идеал максимального порядка $H\subset M_d(\Delta)$ обозначать через $\mathfrak{P}_H$. Для простого элемента $\pi\in\Delta$ $\mathfrak{P}_H=\pi H=H\pi$. Если $A=\prod_{i=1}^{m}\otimes_K A(p_i)$ — примарное разложение тела A, то в $A(p_i)$ существует такое максимальное подполе F_i, что $e(F_i)=e(A(p_i))$. Как в п. 2.3, обозначим $R_i=\prod_{r\neq i}\otimes_K F_r$. Тогда

$A_{R_i}\simeq M_{d_i}(A_{R_i}(p_i))$.

3.11. ЛЕММА. *Пусть H_i — максимальный порядок A_{R_i}, содержащий O_A. Тогда $\mathfrak{P}_{H_i} \supset \mathfrak{P}_A$.*

Доказательство. Пусть π — простой элемент в $A_{R_i}(p_i)$. По лемме 3.6 элемент π будет простым элементом в A. Следовательно, в силу п. 3.10, $\mathfrak{P}_{H_i} = \pi H_i \supset \pi O_A = \mathfrak{P}_A$.

3.12. КОНГРУЭНЦ-ТЕОРЕМА. $(1+\mathfrak{P}_A) \cap SL(1, A) \subset A^{(1)}$.

Доказательство. Сохраним обозначения п. 3.10:

$$A = \prod_{i=1}^{m} \otimes_K A(p_i), \quad R_i = \prod_{r \neq i} \otimes_K F_r, \quad A_{R_i} = M_{d_i}(A_{R_i}(p_i)).$$

Пусть элемент $a \in (1+\mathfrak{P}_A) \cap SL(1, A)$. Тогда $a \in H_i$, где H_i — максимальный порядок A_{R_i}, содержащий O_A. Очевидно, что $a \in SL(1, A_{R_i})$. С другой стороны, по лемме 3.11, $a \in 1+\mathfrak{P}_{H_i}$. Так как максимальные порядки в $M_{d_i}(A_{R_i}(p_i))$ сопряжены, то для некоторого $g_i \in A^*_{R_i}$

$$g_i a g_i^{-1} \in (1+M_{d_i}(\mathfrak{P}_{A_{R_i}(p_i)})) \cap SL(1, A_{R_i}).$$

С помощью обобщенной процедуры элементарных преобразований можно показать, что с точностью до элемента из $(1+M_{d_i}(\mathfrak{P}_{A_{R_i}(p_i)})) \cap A^{(1)}_{R_i}$, $i = 1, 2, \ldots, m$,

$$g_i a g_i^{-1} = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & a_i \end{pmatrix},$$

где $a_i \in 1+\mathfrak{P}_{A_{R_i}(p_i)}$. Аналогичный результат справедлив даже в более общей ситуации матричных алгебр над полулокальными кольцами (см. ([15]), стр. 217). Но

$$\mathrm{Nrd}_{A_{R_i}/R_i}(g_i a g_i^{-1}) = \mathrm{Nrd}_{A_{R_i}(p_i)/R_i}(a_i) = 1.$$

Следовательно, к телу $A_{R_i}(p_i)$ и элементу a_i можно применить предложение 3.9. Тогда получим: $a_i \in A^{(1)}_{R_i}(p_i)$, $i = 1, 2, \ldots, m$. Как обычно, отсюда вытекает включение $g_i a g_i^{-1} \in A^{(1)}_{R_i}$, которое в свою очередь дает $a \in A^{(1)}_{R_i}$ для всех R_i. Из леммы 2.1 следует, что

$$a^{[R_i : K]} \in A^{(1)},$$
$$a^{([R_1 : K], [R_2 : K], \ldots, [R_m : K])} = a \in A^{(1)},$$

ибо наибольший общий делитель $([R_1 : K], [R_2 : K], \ldots, [R_m : K]) = 1$. Конгруэнц-теорема доказана.

3.13. Следствие. *Для неразветвленного тела A*

$$SK_1(A) \simeq SK_1(\overline{A}).$$

Доказательство. Ввиду неразветвленности простой элемент π тела A содержится в K. Поэтому для $a, b \in A^*$ элемент $c = aba^{-1}b^{-1} =$

$=\alpha\beta\alpha^{-1}\beta^{-1}$, где α, $\beta\in O_A^*$. Из предложения 3.4 следует, что гомоморфизм $\psi: a\to\bar{a}$ отображает $SL(1, A)$ на $SL(1, \bar{A})$, ибо $Z(\bar{A})=\bar{K}$. Достаточно теперь убедиться, что $\psi^{-1}(\bar{A}^{(1)})=A^{(1)}$. Так как $\bar{c}=\bar{\alpha}\bar{\beta}\bar{\alpha}^{-1}\bar{\beta}^{-1}$, то $\psi^{-1}(\bar{A}^{(1)})\supseteq A^{(1)}$. Если $t\in\psi^{-1}(\bar{A}^{(1)})$, то существует $s\in A^{(1)}$ такое, что $\overline{ts}=1$. По конгруэнц-теореме тогда

$$ts\in A^{(1)}\Rightarrow t\in A^{(1)}.$$

3.14. З а м е ч а н и е. Следствие 3.13 показывает, что рассмотрение $SK_1(A)$ для тел A над полными дискретно нормированными полями не является фактически ограничением, ибо тело B над произвольным полем k получается в качестве тела вычетов неразветвленного тела $B\otimes_k k\langle x\rangle$, где $k\langle x\rangle$ — поле формальных степенных рядов одной переменной.

§ 4. Группы проективных конорм и теорема редукции

4.1. Г р у п п ы с п е ц и а л ь н ы х п р о е к т и в н ы х к о н о р м. Пусть $L\supset R\supset k$ — башня нормальных расширений поля k, где R — циклическое расширение k степени n, $\{\sigma\}=\mathrm{Gal}(R/k)$. Элемент $a^*\in R^*/k^*N_{L/R}(L^*)$ называется специальной проективной конормой, если для его представителя $a\in a^*(a\in R^*)$ $a^{1-\sigma}\in N_{L/R}(L^*)$. Множество всех специальных проективных конорм образует подгруппу в $R^*/k^*N_{L/R}(L^*)$, которую будем называть группой специальных проективных конорм, соответствующей башне $L\supset R\supset k$, и обозначать через $\mathscr{P}(L, R, k)$. Очевидно, что $\mathscr{P}(L, R, k)$ является группой экспоненты $[L:R]$. Для полной корректности определения группы $\mathscr{P}(L, R, k)$ следует отметить, что она не зависит от выбора автоморфизма σ, порождающего группу $\mathrm{Gal}(R/k)$. Действительно, данное выше определение группы специальных проективных конорм эквивалентно следующему: пусть σ^* — автоморфизм, индуцируемый σ в $R^*/N_{L/R}(L^*)$ (так как L нормально над k, то $\sigma(N_{L/R}(L^*))=N_{L/R}(L^*)$), T_{σ^*} — подгруппа σ^*-инвариантных элементов в $R^*/N_{L/R}(L^*)$; тогда $\mathscr{P}(L, R, k)$ получается факторизацией T_{σ^*} по k^*. Теперь ясно, что $\mathscr{P}(L, R, k)$ не зависит от выбора образующей σ, ибо это верно для T_{σ^*}.

Оказывается, группа $\mathscr{P}(L, R, k)$ естественным образом связана с приведенной группой Уайтхеда $SK_1(A)$ и во многих случаях полностью определяет ее. Установление этой связи и является основной целью настоящего параграфа.

4.2. Напомним, что алгебра A называется циклической, если она является скрещенным произведением циклического расширения R поля K, и группы $\mathrm{Gal}(R/K)$. Если $\{\sigma\}=\mathrm{Gal}(R/K)$, то σ индуцируется некоторым внутренним автоморфизмом алгебры A, порождаемым элементом $g\in A^*$, причем $g^{[R:K]}=a\in K$. Общепринято обозначать алгебру A тогда следующим образом: $A=(a, R, \sigma)$. Мы будем обозначать эту циклическую алгебру через $A(a, R)$.

Пусть теперь $K=k\langle x, y\rangle$ — поле формальных степенных рядов от двух переменных с полем констант k, которое будем рассматривать как поле формальных степенных рядов $k\langle x\rangle\langle y\rangle$, т. е. как полное дискретно нормированное поле с кольцом целых элементов $k\langle x\rangle[[y]]$. Если R_1 и R_2 — циклические расширения поля k соответственно степени n_1, n_2, то $KR_1=R_1\langle x, y\rangle$ и $KR_2=R_2\langle x, y\rangle$ — циклические расширения степени n_1 и n_2 поля K. Построим циклические алгебры $A(x, R_1(x, y))$ и $A(y, R_2(x, y))$, которые будем для сокращения обозначать соответственно через $A(x, R_1)$ и $A(y, R_2)$. Рассмотрим тензорное произведение $A(R_1, R_2)=A(x, R_1)\otimes_{k\langle x,y\rangle}A(y, R_2)$. Так как $A(x, R_1)$ и $A(y, R_2)$ определены над полем рациональных функций $k(x, y)$, то имеется в виду, что центр алгебр $A(x, R_1)$, $A(y, R_2)$ сначала расширяется до $k\langle x, y\rangle$. Через R_1R_2 обозначается композит расширений R_1 и R_2 поля k.

4.3. Возникает естественный вопрос: когда $A(R_1, R_2)$ является телом? Необходимое условие очевидно: $R_1R_2\simeq R_1\otimes_k R_2$, т. е. $[R_1R_2:k]=$ $=n_1n_2$. Оказывается, это простое условие является и достаточным, что составляет содержание теоремы существования, доказательство которой опирается на свойства скрещенных произведений.

Пусть D — тело с центром K, $[D:K]=n^2$, $G=\{\sigma\}$ — циклическая группа внешних автоморфизмов порядка m. Обычным образом строится скрещенное произведение $\widetilde{D}$ тела D и группы $G: \widetilde{D}=D*G$. Хорошо известно, что $\widetilde{D}=D*G$ является простой центральной алгеброй над K_σ, где $K_\sigma=(a\in K\,|\,a^\sigma=a)$, причем $[\widetilde{D}:K_\sigma]=n^2m^2$ (см., например, ([20]), стр. 161). Автоморфизм σ в $\widetilde{D}$ реализуется внутренним образом некоторым элементом u_σ, причем $u_\sigma^m=g\in K_\sigma$.

4.4. Предложение. *Если для всякого $t<m$ уравнение*

$$\mathrm{Nrd}_{D/K}(z)\,\mathrm{Nrd}_{D/K}(z^\sigma)\cdots\mathrm{Nrd}_{D/K}(z^{\sigma^{m-1}})=g^{tn}$$

не имеет решения в теле D, то скрещенное произведение $\widetilde{D}=D*G$ является телом.

Доказательство. Предположим, что $\widetilde{D}$ не является телом. Тогда $\widetilde{D}=\sum_{i=1}^{r}\oplus\widetilde{D}_i$, где $\widetilde{D}_i$ — изоморфные минимальные правые идеалы $\widetilde{D}$. Из размерностных соображений следует, что $r=\frac{m}{t}>1$, где правая размерность $\dim_D\widetilde{D}_i=\frac{m}{r}=t$. Пусть $v_1, v_2, \ldots, v_t$ — базис $\widetilde{D}_1$ над D. Рассмотрим представление φ алгебры D правыми сдвигами в $\widetilde{D}_1$. Элементу u_σ в базисе $v_1, v_2, \ldots, v_t$ будет соответствовать матрица $\varphi(u_\sigma)=U\in M_t(D)$. Если $U=(u_{ij})$, $u_{ij}\in D$, то обозначим $U^\sigma=(u_{ij}^\sigma)$. Вычислим теперь матрицу $\varphi(u_\sigma^2)$:

$$v_ju_\sigma^2=(v_ju_\sigma)u_\sigma=\left(\sum_{i=1}^{t}v_iu_{ij}\right)u_\sigma=$$

$$=\sum_{i=1}^{t}v_iu_\sigma u_{ij}^\sigma=\sum_{i=1}^{t}\left(\sum_{s=1}^{t}v_su_{si}\right)u_{ij}^\sigma=\sum_{s=1}^{t}\left(v_s\left(\sum_{i=1}^{t}u_{si}u_{ij}^\sigma\right)\right).$$

Отсюда следует, что $\varphi(u_\sigma^2) = UU^\sigma$. Стандартное индуктивное рассуждение показывает, что u_σ^q соответствует матрица $UU^\sigma \ldots U^{\sigma^{q-1}}$. По теореме Дьедонне об определителе над телом

$$U = (u_{ij}) = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & u_0 \end{pmatrix} T,$$

где $u_0 \in D$, $T \in M_t^{(1)}(D)$. В частности,

$$\mathrm{Nrd}_{M_t(D)/K_\sigma}(U) = \mathrm{Nrd}_{D/K}(u_0).$$

Аналогично,

$$U^{\sigma^q} = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & u_0^{\sigma^q} \end{pmatrix} T^{\sigma^q}, \quad \mathrm{Nrd}_{M_t(D)/K_\sigma}(U^{\sigma^q}) = \mathrm{Nrd}_{D/K}(u_0^{\sigma^q}).$$

Так как $u_\sigma^m = g$, то $\varphi(u_\sigma^m) = UU^\sigma \ldots U^{\sigma^{m-1}} = \begin{pmatrix} g & & 0 \\ & \ddots & \\ 0 & & g \end{pmatrix}$. Поэтому

$$\mathrm{Nrd}_{M_t(D)/K_\sigma}(UU^\sigma \ldots U^{\sigma^{m-1}}) = \mathrm{Nrd}_{D/K}(u_0)\,\mathrm{Nrd}_{D/K}(u_0^\sigma) \ldots \mathrm{Nrd}_{D/K}(u_0^{\sigma^{m-1}}) =$$
$$= (\mathrm{Nrd}_{D/K}(g))^t = g^{tn}.$$

Следовательно, при $t<m$ уравнение в предложении 4.4 имеет решение $u_0 \in D$. Предложение 4.4 доказано.

4.5. Следствие. *Пусть D является полем. Если для всякого $t<m$ $g^t \notin N_{D/D_\sigma}(D)$, то $\tilde{D}=D*G$ является телом.*

Действительно, в этом случае $D=K$, $D_\sigma=K_\sigma$, $\mathrm{Nrd}_{D/K}(z)=z$ и мы получаем уравнение:

$$zz^\sigma \ldots z^{\sigma^{m-1}} = N_{K/K_\sigma}(z) = g^t.$$

4.6. Замечание. Скрещенное произведение $\tilde{D}=D*G$ следующим образом представляется в виде тензорного произведения: $\tilde{D} = D_\sigma \otimes_{K_\sigma} (K*G_0)$, где G_0 — ограничение G на K и определяющий элемент $u_\sigma \in K*G_0$. Это непосредственно следует из определения скрещенного произведения и теоремы о двойном централизаторе в простой алгебре.

4.7. ТЕОРЕМА. $A(R_1, R_2) = A(x, R_1) \otimes_{k\langle x,y\rangle} A(y, R_2)$ *тогда и только тогда является телом, когда $L = R_1 \otimes_k R_2$ — поле, т. е. R_1 и R_2 линейно разделены над k.*

Доказательство. Пусть $L = R_1 \otimes_k R_2$ — поле. Напомним, что R_1, R_2 — циклические расширения поля k, $[R_1 : k] = n_1$, $[R_2 : k] = n_2$. Рассмотрим вначале алгебру $A(x, R_1) \otimes_{k\langle x,y\rangle} R_2\langle x, y\rangle$, которая является циклической алгеброй $A(x, L\langle x, y\rangle)$, соответствующей расширению $L\langle x, y\rangle / R_2\langle x, y\rangle$. Если интерпретировать $R_2\langle x, y\rangle$ как поле $R_2\langle y\rangle\langle x\rangle$, то $L\langle x, y\rangle$ — неразветвленное расширение $R_2\langle x, y\rangle$. Следовательно, если

$N_{L\langle x,y\rangle/R_2\langle x,y\rangle}(a)=x^t$, то t делится на n_1, поэтому из утверждения 4.4 или 4.5 вытекает, что $A(x, L\langle x, y\rangle)$ есть тело.

Обозначим $A(x, R_1)\otimes_{k\langle x,y\rangle}R_2\langle x, y\rangle$ через D. Если $\{\sigma\}=\mathrm{Gal}(R_2\langle x, y\rangle/k\langle x, y\rangle)$, то σ продолжается до автоморфизма $\tilde\sigma$ тела D следующим образом: пусть $d\in D$ и $d=\sum_{i=1}^{n_1^2}\alpha_i v_i$, где (v_i) — базис $A(x, R_1)$, $\alpha_i\in R_2\langle x, y\rangle$. Тогда $\tilde\sigma(d)\overset{\text{def}}{=}\sum_{i=1}^{n_1^2}\sigma(\alpha_i)v_i$. Нетрудно видеть, что циклическая группа $G=\{\tilde\sigma\}$, $\tilde\sigma^{n_2}=1$, является группой внешних автоморфизмов. Алгебра $A(R_1, R_2)$ естественным образом отождествляется со скрещенным произведением $\tilde D=D*G$, где $\tilde\sigma\to\to u_{\tilde\sigma}\in\tilde D$, $u_{\tilde\sigma}^{n_2}=y$. Действительно, согласно 4.6

$$\tilde D=\tilde D_{\tilde\sigma}\otimes_{k\langle x,y\rangle}(R_2\langle x, y\rangle*G_0),$$

где $G_0=\{\sigma\}$. Но $\tilde D_{\tilde\sigma}=A(x, R_1)$, $R_2\langle x, y\rangle*G_0=A(y, R_2)$. К $\tilde D$ можно применить предложение 4.5. Рассматриваем теперь $R_2\langle x, y\rangle$ как $R_2\langle x\rangle\langle y\rangle$. Пусть для $d\in D$

$$\mathrm{Nrd}_{D/R_2\langle x,y\rangle}(d)\,\mathrm{Nrd}_{D/R_2\langle x,y\rangle}(d^{\tilde\sigma})\,\ldots\,\mathrm{Nrd}_{D/R_2\langle x,y\rangle}(d^{\tilde\sigma^{n_2-1}})=y^{\alpha},$$

где $\alpha\neq 0$. Тогда $d=y^r\varepsilon$, где $r\neq 0$, $\varepsilon\in O_D^*$ (O_D — кольцо целых элементов D относительно $R_2\langle x\rangle[[y]]$), ибо приведенная норма единицы кольца O_D является единицей в $R_2\langle x\rangle[[y]]$. Но y лежит в центре $D_{\tilde\sigma}$, $(O_D^*)^{\tilde\sigma}=O_D^*$, поэтому

$$\mathrm{Nrd}_{D/R_2\langle x,y\rangle}(d)\,\mathrm{Nrd}_{D/R_2\langle x,y\rangle}(d^{\tilde\sigma})\,\ldots\,\mathrm{Nrd}_{D/R_2\langle x,y\rangle}(d^{\tilde\sigma^{n_2-1}})=\mathrm{Nrd}(\varepsilon)\,\mathrm{Nrd}(\varepsilon^{\tilde\sigma})\,\ldots$$
$$\ldots\,\mathrm{Nrd}(\varepsilon^{\tilde\sigma^{n_2-1}})\,y^{rn_1n_2}=\theta y^{rn_1n_2}=y^{\alpha},$$

где $\theta\in(R_2\langle x\rangle[[y]])^*$. Следовательно, α делится на n_1n_2 и предложение 4.5 позволяет утверждать, что $\tilde D$ есть тело. Теорема доказана.

4.8. В дальнейшем будем предполагать, что $A(R_1, R_2)$ является телом, что эквивалентно по теореме 4.7 условию $[R_1R_2:k]=n_1n_2$. Через $O_{A(R_1,R_2)}$ обозначается кольцо целых элементов в $A(R_1, R_2)$ относительно $k\langle x\rangle[[y]]$. $\mathfrak{P}_{A(R_1,R_2)}$ — простой идеал $O_{A(R_1,R_2)}$, $\bar A(R_1, R_2)=O_{A(R_1,R_2)}/\mathfrak{P}_{A(R_1,R_2)}$ — тело вычетов. Аналогично, $O_{\bar A(R_1,R_2)}$ обозначает кольцо целых элементов $\bar A(R_1, R_2)$ относительно $k[[x]]$, $\mathfrak{P}_{\bar A(R_1,R_2)}$—простой идеал $O_{\bar A(R_1,R_2)}$, $\bar{\bar A}(R_1, R_2)=O_{\bar A(R_1,R_2)}/\mathfrak{P}_{\bar A(R_1,R_2)}$.

4.9. ЛЕММА. $\bar A(R_1, R_2)\simeq A(x, R_1)\otimes_{k\langle x\rangle}R_2\langle x\rangle$, $\bar{\bar A}(R_1, R_2)\simeq R_1\otimes_k R_2=R_1R_2$, *в частности,* $\bar A(R_1, R_2)$ *сепарабельно над* $k\langle x\rangle$, *а* $\bar{\bar A}(R_1, R_2)$ *сепарабельно над* k.

Доказательство. Первый изоморфизм следует из подсчета размерностей с учетом того, что $\bar A(x, R_1)\simeq A(x, R_1)$ над $k\langle x\rangle$ и индекс ветвления $A(R_1, R_2)$ есть n_2. Для второго рассуждение аналогично, только индекс ветвления $\bar A(R_1, R_2)$ уже равен n_1 (см. п. 3,1).

4.10. ЛЕММА. $\overline{SL(1, A(R_1, R_2))} = (c \in R_1 R_2 \mid N_{R_1R_2/k}(c) = 1)$.

Доказательство. Из предложения 3.4 и леммы 4.9 следует, что

$$\overline{SL(1, A(R_1, R_2))} = (b \in \overline{A}(R_1, R_2) \mid N_{R_2\langle x\rangle/k\langle x\rangle}(\mathrm{Nrd}_{\overline{A}(R_1,R_2)/R_2\langle x\rangle}(b) = 1)).$$

Пусть T — максимальное подполе $\overline{A}(R_1, R_2)$, содержащее b. Тогда (см. доказательство леммы 3.2) $N_{T/k\langle x\rangle}(b) = 1$ и

$$\overline{N_{T/k\langle x\rangle}(b)} = (N_{\overline{T}/k}(\overline{b}))^{e(T)} = N_{R_1R_2/k}(\overline{b}) = 1.$$

Обратное включение доказывается просто: так как $R_1R_2\langle x\rangle$ неразветвленно над $k\langle x\rangle$, то элемент c, $N_{R_1R_2/k}(c) = 1$, поднимается до элемента $b \in R_1R_2\langle x\rangle$, $\overline{b} = c$, $N_{R_1R_2\langle x\rangle/k\langle x\rangle}(b) = 1$; аналогично, элемент b поднимается до элемента $a \in SL(1, A(R_1, R_2))$, $\overline{a} = b$ (подробнее об этом см. доказательство леммы 3.3). Лемма доказана.

4.11. ТЕОРЕМА РЕДУКЦИИ. *Пусть $A(R_1, R_2) = A(x, R_1) \otimes_{k\langle x,y\rangle} A(y, R_2)$ является телом. Тогда существует сюръективный морфизм*

$$\varphi : SK_1(A(R_1, R_2)) \to \mathscr{P}(R_1R_2, R_2, k).$$

Если $SK_1(\overline{A}(R_1, R_2)) = 1$, то φ — изоморфизм; в частности, если $[R_1 : k] = n_1$ не делится на квадрат простого числа, то $SK_1(A(R_1, R_2)) \simeq \simeq \mathscr{P}(R_1R_2, R_2, k)$.

Доказательство. Пусть $a \in SL(1, A(R_1, R_2))$. По лемме 4.10 $N_{R_1R_2/k}(\overline{\overline{a}}) = 1$. Т. 90 Гильберта Следовательно, $N_{R_1R_2/R_2}(\overline{\overline{a}}) = t_a^{1-\sigma}$, где $t_a \in R_2$, $\{\sigma\} = \mathrm{Gal}(R_2/k)$, t_a порождает некоторый элемент $a^* \in \mathscr{P}(R_1R_2, R_2, k)$. Отображение $\tau : a \to a^*$ будет гомоморфизмом. Его сюръективность следует из леммы 4.10. Пусть $a \in A^{(1)}(R_1, R_2)$. Тогда в соответствии с предложением 3.5

$$\mathrm{Nrd}_{\overline{A}(R_1,R_2)/R_2\langle x\rangle}(\overline{a}) = \beta^{1-\widetilde{\sigma}},$$

где $\{\widetilde{\sigma}\} = \mathrm{Gal}(R_2\langle x\rangle/k\langle x\rangle)$, $\beta = \mathrm{Nrd}_{\overline{A}(R_1,R_2)/R_2\langle x\rangle}(b)$. Если $b \in T$ — максимальному подполю $\overline{A}(R_1, R_2)$, то

$$\mathrm{Nrd}_{\overline{A}(R_1,R_2)/R_2\langle x\rangle}(b) = N_{T/R_2\langle x\rangle}(b).$$

Далее,

$$\overline{N_{T/R_2\langle x\rangle}(b)} = (N_{\overline{T}/R_2}(\overline{b}))^{e(T)} = N_{R_1R_2/k}(\overline{b}) = \overline{\beta},$$

$N_{R_1R_2/R_2}(\overline{\overline{a}}) = \overline{\beta}^{1-\sigma}$. Это означает, что $\tau(a) = 1^*$ — единица группы $\mathscr{P}(R_1R_2, R_2, k)$. Таким образом, $\mathrm{Ker}\,\tau \supseteq A^{(1)}(R_1, R_2)$ и τ индуцирует сюръективный морфизм $\varphi : SK_1(A(R_1, R_2)) \to \mathscr{P}(R_1R_2, R_2, k)$.

Пусть теперь $SK_1(\overline{A}(R_1, R_2)) = 1$ и $\tau(a) = 1^*$. Тогда $N_{R_1R_2/R_2}(\overline{\overline{a}}) = t_a^{1-\sigma}$, где $t_a \in N_{R_1R_2/R_2}(R_1R_2)$. Как и выше, $\mathrm{Nrd}_{\overline{A}(R_1,R_2)/R_2\langle x\rangle}(\overline{a}) = s_a^{1-\widetilde{\sigma}}$, где $\overline{s}_a = t_a$ и $\mathrm{Nrd}_{\overline{A}(R_1,R_2)/R_2\langle x\rangle}(h_a) = s_a$. Существует $g_a \in A(R_1, R_2)$, $\overline{g}_a = h_a$. Пусть θ —

внутренний автоморфизм, индуцируемый простым элементом π кольца $O_{A(R_1,R_2)}$. Тогда редукция $\bar{\theta}$ на $R_2\langle x\rangle$ совпадает с $\tilde{\sigma}$ (см. п. 3.1). Имеем:

$$\mathrm{Nrd}_{\bar{A}(R_1,R_2)/R_2\langle x\rangle}\,(\overline{g_a\pi g_a^{-1}\pi^{-1}}) =$$

$$= \mathrm{Nrd}_{\bar{A}(R_1,R_2)/R_2\langle x\rangle}(h_a)\,\mathrm{Nrd}_{\bar{A}(R_1,R_2)/R_2\langle x\rangle}(h_a^{-1})^{\tilde{\sigma}} = s_a^{1-\tilde{\sigma}}.$$

Следовательно,

$$\mathrm{Nrd}_{\bar{A}(R_1,R_2)/R_2\langle x\rangle}\,(\overline{a\,(g_a\pi g_a^{-1}\pi^{-1})^{-1}}) = 1,$$

т. е.

$$\overline{a\,(g_a\pi g_a^{-1}\pi^{-1})^{-1}} \in SL\,(1,\,\bar{A}\,(R_1,\,R_2)).$$

Так как $SK_1(\bar{A}\,(R_1,\,R_2))=1$, то

$$\overline{a\,(g_a\pi g_a^{-1}\pi^{-1})^{-1}} = \prod_{\nu=1}^{r}\,[b_{2\nu-1},\,b_{2\nu}],$$

где $b_i \in \bar{A}^{\bullet}(R_1,\,R_2)$. Существуют такие $a_i \in A\,(R_1,\,R_2)$, что $\bar{a}_i = b_i$ $\forall i$. Тогда

$$\overline{a\left(\prod_{\nu=1}^{r}\,[a_{2\nu-1},\,a_{2\nu}]\,(g_a\pi g_a^{-1}\pi^{-1})\right)^{-1}} = 1.$$

По конгруэнц-теореме 3.12

$$a\left(\prod_{\nu=1}^{r}\,[a_{2\nu-1},\,a_{2\nu}]\,(g_a\pi g_a^{-1}\pi^{-1})\right)^{-1} \in A^{(1)}\,(R_1,\,R_2).$$

Следовательно, $a \in A^{(1)}\,(R_1,\,R_2)$. Тем самым доказано, что

$$\mathrm{Ker}\,\tau = A^{(1)}\,(R_1,\,R_2) \text{ и } SK_1\,(A\,(R_1,\,R_2)) \simeq \mathcal{P}\,(R_1R_2,\,R_2,\,k).$$

Если, наконец, n_1 не делится на квадрат простого числа, то из предложения 2.5 вытекает, что $SK_1(\bar{A}\,(R_1,\,R_2))=1$. Теорема доказана.

4.12. Следствие. *Для тензорного произведения* $A\,(x,\,R_1) \otimes$ $\otimes_{k(x,y)} A\,(y,\,R_2)$ *над полем рациональных функций* $k\,(x,\,y)$

$$\mathrm{Card}\,(SK_1\,(A\,(x,\,R_1) \otimes_{k(x,y)} A\,(y,\,R_2))) \geqslant \mathrm{Card}\,\mathcal{P}\,(R_1R_2,\,R_2,\,k).$$

Доказательство. Пусть $L = R_1R_2$, $L_1 = (a \in L / N_{L/k}(a) = 1)$. Тогда $L_1 \subset SL\,(1,\,A\,(x,\,R_1) \otimes_{k(x,y)} A\,(y,\,R_2))$ и $\tau\,(L_1) = \mathcal{P}\,(L,\,R_2,\,k)$. Следовательно,

$$\varphi\,(SK_1\,(A\,(x,\,R_1) \otimes_{k(x,y)} A\,(y,\,R_2))) = \mathcal{P}\,(L,\,R_2,\,k).$$

4.13. Замечание. В теореме 4.11 предполагалось, что R_1 и R_2 являются циклическими расширениями поля k. Нетрудно видеть, что доказательство сохраняет силу для произвольных циклических расширений R_1 и R_2 поля $k\langle x,\,y\rangle$ при условии, что тела вычетов являются сепарабельными, а поля R_1 и R_2 в группе проективных конорм заменяются соответствующими полями вычетов.

4.14. Теорема редукции показывает, что группа $SK_1(A(R_1, R_2))$ в значительной степени определяется группой $\mathscr{P}(R_1R_2, R_2, k)$. В частности, если $\mathscr{P}(R_1R_2, R_2, k)\neq 1$, то $SK_1(A(R_1, R_2))\neq 1$. Поэтому вычисление группы $\mathscr{P}(R_1R_2, R_2, k)$ имеет важное значение. В ряде случаев группа $\mathscr{P}(R_1R_2, R_2, k)$ может быть вычислена непосредственно. Приведем один из минимальных контрпримеров в проблеме Таннака — Артина.

Пусть $k=Q_p$ — поле p-адических чисел, $R_1=Q_p(\alpha)$, $R_2=Q_p(\sqrt{p})$, где α — единица кольца целых p-адических чисел Z_p, не являющаяся квадратом. Из теорем 4.7 и 4.11 следует, что

$$SK_1(A(Q_p(\sqrt{\alpha}), Q_p(\sqrt{p})))\simeq\mathscr{P}(Q_p(\sqrt{\alpha}, \sqrt{p}), Q_p(\sqrt{p}), Q_p).$$

Нетрудно показать, что $\mathscr{P}(Q_p(\sqrt{\alpha}, \sqrt{p}), Q_p(\sqrt{p}), Q_p)$ является циклической группой второго порядка.

4.15. В общем случае оказывается весьма эффективной когомологическая интерпретация группы $\mathscr{P}(R_1R_2, R_2, k)$, которая равносильна интерпретации посредством групп Брауэра.

В дальнейшем нам понадобятся известные факты о когомологиях конечных групп и группах Брауэра, которые содержатся в ([14]) (гл. 4, 5), ([21]) (гл. 12).

Пусть поле $L\supset R_1, R_2$. Через $\mathrm{Br}(L/k)$, $\mathrm{Br}(R_1/k)$, $\mathrm{Br}(R_2/k)$ обозначаются подгруппы группы Брауэра $\mathrm{Br}(k)$, состоящие из элементов, разложимых соответственно над L, R_1, R_2. В терминах когомологий Галуа

$$\mathrm{Br}(L/k)\simeq H^2(G, L^*),\quad \mathrm{Br}(R_1/k)\simeq H^2(G_2, R_1^*),$$

$$\mathrm{Br}(R_2/k)\simeq H^2(G_1, R_2^*),\quad \text{где } G=\mathrm{Gal}(L/k),$$

$$G_1=\mathrm{Gal}(L/R_1)\overset{\mathrm{Res}}{\simeq}\mathrm{Gal}(R_2/k),\quad G_2=\mathrm{Gal}(L/R_2)\overset{\mathrm{Res}}{\simeq}\mathrm{Gal}(R_1/k)$$

(Res обозначает отображение ограничения).

Группы $\mathrm{Br}(R_1/k)$ и $\mathrm{Br}(R_2/k)$ каноническим образом вкладываются в $\mathrm{Br}(L/k)$ и в случае необходимости мы будем отождествлять их с образами в $\mathrm{Br}(L/k)$. Если $L=R_1\otimes_k R_2$, то через σ_1, σ_2 обозначаются образующие соответственно циклических групп G_1 и G_2; $N_1=N_{L/R_1}$, $N_2=N_{L/R_2}$.

4.16. Предложение. *Пусть* $L=R_1\otimes_k R_2$,

$$T=\{(x_1, z, x_2)\,|\,x_i\in R_i^*,\ z\in L^*,\ N_1(z)=x_1^{1-\sigma_2},\ N_2(z)=x_2^{1-\sigma_1}\},$$

$$T_0=\{(N_1(y_1),\ y_1^{1-\sigma_2}y_2^{1-\sigma_1},\ N_2(y_2))\,|\,y_1, y_2\in L^*\}.$$

Тогда существует изоморфизм групп $\mathrm{Br}(L/k)\overset{\varphi}{\simeq}T/T_0$, *причем по модулю* T_0

$$\varphi(\mathrm{Br}(R_1/k))=\{(d_1, 1, 1)\,|\,d_1\in k^*\},$$

$$\varphi(\mathrm{Br}(R_2/k))=\{(1, 1, d_2)\,|\,d_2\in k^*\}.$$

Доказательство. Пусть $Z[G_1]$, $Z[G_2]$ — целочисленные групповые кольца соответственно для G_1 и G_2. Группы когомологий $H^m(G_1, R_2^*)$,

$H^m(G_2, R_1^{\bullet})$ вычисляются с помощью стандартных резольвент для Z:

$$(B^{(1)}) \ \ldots \xrightarrow{1-\sigma_1} B_2^{(1)} \xrightarrow{N_1} B_1^{(1)} \xrightarrow{1-\sigma_1} B_0^{(1)} \xrightarrow{\varepsilon_1} Z \to 0, \ B_i^{(1)} = Z[G_1],$$
$$i = 0, 1, 2, \ldots,$$
$$(B^{(2)}) \ \ldots \xrightarrow{\sigma_2-1} B_2^{(2)} \xrightarrow{N_2} B_1^{(2)} \xrightarrow{\sigma_2-1} B_0^{(2)} \xrightarrow{\varepsilon_2} Z \to 0, \ B_j^{(2)} = Z[G_2],$$
$$j = 0, 1, 2, \ldots,$$

где при $h \in Z[G_1]$, $\quad N_1(h) = (1 + \sigma_1 + \ldots + \sigma_1^{n_1-1})h$,

$$(1 - \sigma_1)(h) = (1 - \sigma_1)h, \quad \varepsilon_1\left(\sum_j a_j\sigma_1^j\right) = \sum_j a_j,$$

а при $g \in Z[G_2]$, $N_2(g) = (1 + \sigma_2 + \ldots + \sigma_2^{n_2-1})g$,

$$(\sigma_2 - 1)(g) = (\sigma_2 - 1) \cdot g, \quad \varepsilon_2\left(\sum_j b_j\sigma_2^j\right) = \sum_j b_j.$$

Соответствующая резольвента для вычисления $H^m(G, L^*)$, $m \geqslant 0$, строится как тензорное произведение комплексов $B^{(1)}$ и $B^{(2)}$ над Z. А именно, l-тый член B_l комплекса $B = B^{(1)} \otimes_Z B^{(2)}$ есть

$$\sum_{\substack{i+j=l \\ 0 \leqslant i, j \leqslant l}} B_i^{(1)} \otimes B_j^{(2)}.$$

Нетрудно видеть, что $B_l \simeq Z[G]^{l+1}$, где $Z[G]^{l+1}$ обозначает свободный $Z[G]$-модуль с $l+1$ образующими. Граничные дифференциалы $\theta_l : B_l \to B_{l-1}$ получаются стандартными комбинациями из $1 - \sigma_1$, $\sigma_2 - 1$, N_1, N_2. Точнее, если $i + j = l$, $b_i^{(1)} \in B_i^{(1)}$, $b_j^{(2)} \in B_j^{(2)}$, то

$$\theta_l(b_i^{(1)} \otimes b_j^{(2)}) = \delta_i^{(1)}(b_i^{(1)}) \otimes b_j^{(2)} + (-1)^i b_i^{(1)} \otimes \delta_j^{(2)}(b_j^{(2)}),$$

где $\delta_i^{(1)}$, $\delta_j^{(2)}$ — граничные дифференциалы комплексов $B^{(1)}$ и $B^{(2)}$. Наконец, отображение $\varepsilon : b_0^{(1)} \otimes b_0^{(2)} \to \varepsilon_1(b_0^{(1)})\,\varepsilon_1(b_0^{(2)}) \in Z$ завершает построение свободной $Z[G]$-резольвенты для Z.

Для вычисления когомологий надо перейти к комплексу $D = \mathrm{Hom}_{Z[G]}(B, L^*)$, где $D_i = \mathrm{Hom}_{Z[G]}(B_i, L^*)$, а кограничные дифференциалы $d_m : D_{m-1} \to D_m$ индуцируются дифференциалами θ_l. Нас интересует отрезок комплекса $D_1 \xrightarrow{d_2} D_2 \xrightarrow{d_3} D_3$, ибо $\mathrm{Br}(L/k) \simeq H^2(G, L^*) \simeq \mathrm{Ker}\, d_3/\mathrm{Im}\, d_2$. Так как $D_i \simeq (L^*)^{i+1}$, то этот отрезок имеет вид

$$(L^*)^2 \xrightarrow{d_2} (L^*)^3 \xrightarrow{d_3} (L^*)^4.$$

Кроме того, ввиду $B_2 \simeq Z[G]^3$ всякий элемент $h \in D_2 = \mathrm{Hom}_{Z[G]}(B_2, L^*)$ задается своими значениями на базисных элементах, например, на элементах $(1,0,0)$, $(0,1,0)$, $(0,0,1)$. Пусть $h(1,0,0)=x_1$, $h(0,1,0)=z$, $h(0,0,1)=x_2$. Напомним, что

$$B_2 = B_2^{(1)}\otimes B_0^{(2)} + B_1^{(1)}\otimes B_1^{(2)} + B_0^{(1)}\otimes B_2^{(2)},$$

$$B_3 = B_3^{(1)}\otimes B_0^{(2)} + B_2^{(1)}\otimes B_1^{(2)} + B_1^{(1)}\otimes B_2^{(2)} + B_0^{(1)}\otimes B_3^{(2)}$$

и фактически мы отождествляем $(1,0,0)=(1\otimes 1,0,0)$ и т. д.

Пусть теперь $d_3(h)=1$, т. е. $h\in\operatorname{Ker} d_3$. Тогда

$$h(\theta_3(1,0,0,0)) = h(\theta_3(0,1,0,0)) = h(\theta_3(0,0,1,0)) = h(\theta_3(0,0,0,1)) = 1.$$

По определению имеем:

$$h(\theta_3(1,0,0,0)) = h((1-\sigma_1)(1,0,0)) = x_1^{1-\sigma_1} = 1.$$

Это означает, что $x_1 = x_1^{\sigma_1}$, т. е. $x_1\in R_1^*$. Аналогично,

$$h(\theta_3(0,0,0,1)) = x_2^{\sigma_2-1} = 1 \Rightarrow x_2\in R_2^*.$$

Далее,

$$h(\theta_3(0,1,0,0)) = N_1(h(0,1,0))\,x_1^{\sigma_2-1} = 1.$$

Отсюда следует, что $N_1(z) = x_1^{1-\sigma_2}$. Точно так же

$$h(\theta_3(0,0,1,0)) = h((1-\sigma_1)(0,0,1)) - N_2 h(0,1,0) =$$

$$= x_2^{1-\sigma_1}N_2(z)^{-1} = 1 \Rightarrow N_2(z) = x_2^{1-\sigma_1}.$$

Таким образом,

$$\operatorname{Ker} d_3 = T = \{(x_1, z, x_2)\,|\,x_i\in R_i^*,\ z\in L^*,\ N_1(z) = x_1^{1-\sigma_2},\ N_2(z) = x_2^{1-\sigma_1}\}.$$

Совершенно аналогично вычисляется $\operatorname{Im} d_2 = T_0$. Остается только заметить, что при отображении инфляции

$$H^2(G/G_2, R_2^*) \simeq H^2(G_1, R_2^*) \xrightarrow{\mathrm{Inf}} H^2(G, L^*),$$

$$H^2(G/G_1, R_1^*) \simeq H^2(G_2, R_1^*) \xrightarrow{\mathrm{Inf}} H^2(G, L^*).$$

$H^2(G_1, R_2^*)$ и $H^2(G_2, R_1^*)$ переходят по модулю T_0 соответственно в $\{(1,1,d_2)\,|\,d_2\in k^*\}$ и $\{(d_1,1,1)\,|\,d_1\in k^*\}$. Предложение доказано.

4.17. ТЕОРЕМА. *Пусть поле $L=R_1\otimes_k R_2$, где R_1, R_2 — циклические расширения k. Тогда*

$$\mathscr{P}(L, R_2, k) \simeq \operatorname{Br}(L/k)/(\operatorname{Br}(R_1/k)\operatorname{Br}(R_2/k)),$$

т. е.

$$\mathscr{P}(L, R_2, k) \simeq \operatorname{Coker}(\operatorname{Br}(R_1/k)\oplus\operatorname{Br}(R_2/k)\to\operatorname{Br}(L/k)).$$

Доказательство. Рассмотрим отображение $\psi: T\to\mathscr{P}(L, R_2, k)$, сопоставляющее каждой тройке

$$(x_1, z, x_2)\in T \to x_2^*\in\mathscr{P}(L, R_2, k).$$

Очевидно, что ψ — гомоморфизм, причем сюръективный, так как для $x_2\in x_2^*$ $x_2^{1-\sigma_1} = N_2(z)$ для подходящего $z\in L^*$, и, в свою очередь, $N_1(z) =$

$=x_1^{1-\sigma_2}$, где $x_1 \in R_1^*$. Понятно, что $T_0 \subset \operatorname{Ker}\psi$, поэтому ψ индуцирует сюръективный морфизм $T/T_0 \to \mathscr{P}(L, R_2, k)$, который также будем обозначать через ψ.

Пусть $F_1 = \{(d_1, 1, 1) \mid d_1 \in k^*\}$, $F_2 = \{(1, 1, d_2) \mid d_2 \in k^*\}$. Из определения $\mathscr{P}(L, R_2, k)$ следует, что $\operatorname{Ker}\psi \supset F_1F_2$. По предложению 4.16 $\operatorname{Br}(L/k) \overset{\varphi}{\simeq} T/T_0$, $\varphi(\operatorname{Br}(R_1/k)) = F_1$, $\varphi(\operatorname{Br}(R_2/k)) = F_2$. Поэтому достаточно доказать, что $\operatorname{Ker}\psi = F_1F_2$.

Если $t = (x_1, z, x_2) \in \operatorname{Ker}\psi$, то с точностью до элемента из F_2 он имеет вид $(x_1, z, N_2(z_0))$, где $z_0 \in L^*$. С точностью до элемента из T_0 можно считать $t = (x_1, z, 1)$. Тогда $N_2(z) = 1$, поэтому $z = z_0^{1-\sigma_2}$ и умножение t на $(N_1(z_0), z_0^{1-\sigma_2}, 1)^{-1} \in T_0$ приводит к элементу $(x_1, 1, 1) \in F_1$. Теорема доказана.

4.18. Следствие. $\mathscr{P}(L, R_2, k) \simeq \mathscr{P}(L, R_1, k)$.

§ 5. Приведенные группы Уайтхеда и теория полей классов

5.1. В настоящем параграфе разработанный в § 4 метод вычисления группы $SK_1(A(R_1, R_2))$ применяется для наиболее важных полей k. А именно, будут рассматриваться локально компактные или глобальные поля k. При этом возникают глубокие связи с арифметикой и, в особенности, с теорией полей классов, которые непосредственно проявляются уже в теоремах 4.11 и 4.17. На этом пути удается полностью вычислить группу $SK_1(A(R_1, R_2))$.

5.2. Однако прежде чем переходить к наиболее важным результатам этого параграфа, покажем, что использование полей формальных степенных рядов от двух и более переменных вызывается существом дела и для поля $k\langle x\rangle$ от одной переменной проблема Таннака — Артина решается положительно.

Как обычно, глобальным называется поле, являющееся полем алгебраических чисел или полем алгебраических функций одной переменной с конечным полем констант.

5.3. ЛЕММА. *Пусть D — тело над полем алгебраических чисел k, центр $Z(D)$ которого является циклическим расширением k; $\{\sigma\} = \operatorname{Gal}(Z(D)/k)$. Если σ продолжается до автоморфизма $\tilde{\sigma}$ тела D, то для всякого элемента $b^{1-\sigma} \in \operatorname{Nrd}_{D/Z(D)}(D)$, где $b \in Z(D)$, существует $\alpha \in k^*$ со свойством: $\alpha b \in \operatorname{Nrd}_{D/Z(D)}(D)$. При $[Z(D):k] = 2$ условие продолжимости σ можно опустить.*

Доказательство. Обозначим $Z(D) = K$. Пусть $V_\infty = \{v_i\}$ — конечное множество всех вещественных точек поля K, в которых тело D разветвлено. Это означает, что пополнения K_{v_i} являются полем вещественных чисел и $D \otimes_K K_{v_i}$ не есть полная матричная алгебра над K_{v_i}. Такой выбор V_∞ связан с тем, что по теореме Эйхлера о нормах в простых алгебрах (см. ([2]), стр. 279) $\operatorname{Nrd}_{D/K}(D^*)$ состоит из тех элементов K^*, образ которых в K_{v_i} $\forall v_i \in V_\infty$ строго положителен. В частности, если множество V_∞ пусто, то $\mathrm{Nrd}_{D/K}(D^*) = K^*$ и лемма 5.3 заведомо справедлива. Поэтому будем считать, что V_∞ — непустое множество. Пусть $V_\infty^0 = \{v_r^0\}$ — множество всех ограничений V_∞ на k. Тогда V_∞ разбивается на классы, $V_\infty(r)$, состоящие из продолжений одной и той же точки v_r^0 поля k. Так как K/k — циклическое расширение, то все продолжения v_r^0 получаются из одного из них — v_r следующим образом: $v_r, v_r^\sigma, \ldots, v_r^{\sigma^{m-1}}$. Покажем, что элементы $v_r(b)$, $v_r^\sigma(b), \ldots, v_r^{\sigma^{m-1}}(b)$ имеют одинаковый знак, т. е. либо одновременно положительны, либо отрицательны. Так как $b^{1-\sigma} = \mathrm{Nrd}_{D/K}(d)$, то

$$v_r(b^{1-\sigma}) > 0 \Rightarrow v_r(b)\, v_r^\sigma(b) = v_r(b)\, v_r(b^\sigma) > 0.$$

По лемме 2.6

$$b^{\sigma-\sigma^2} = (\mathrm{Nrd}_{D/K}(d))^\sigma = \mathrm{Nrd}_{D/K}(\widetilde{d^\sigma}).$$

Аналогично,

$$v_r(b^{\sigma-\sigma^2}) > 0 \Rightarrow v_r^\sigma(b)\, v_r^{\sigma^2}(b) > 0.$$

И вообще $v_r^{\sigma^s}(b)\, v_r^{\sigma^{s+1}}(b) > 0$. По слабой аппроксимационной теореме существует такой элемент $\alpha \in k^*$, что $v_r^0(\alpha)\, v_r^{\sigma^s}(b) > 0\ \forall s, r$. Тогда $v_l(\alpha b) > 0$ $\forall v_l \in V_\infty$. Следовательно, $\alpha b \in \mathrm{Nrd}_{D/K}(D^*)$. Если $[K:k] = 2$, то $v_r(b)$ и $v_r^\sigma(b)$ имеют одинаковый знак и можно сразу применять аппроксимационную теорему. Лемма доказана.

5.4. ТЕОРЕМА. *Пусть A — тело над локально компактным или глобальным полем K, тогда $SK_1(A) = 1$.*

Доказательство. Из леммы 2.3 и рассуждений п. 2.4 следует, что достаточно доказать теорему для тела A примарной степени: $[A:K] = p^\alpha$, p — простое число. При этом можно считать, что элемент $a \in SL(1, A)$ содержится в таком максимальном подполе $F \subset A$, что в F существует циклическое подполе T_p степени p. Далее практически повторяется индуктивное рассуждение из п. 3.9. Пусть $\Delta = C_A(T_p)$. Имеем:

$$N_{T_p/K}(\mathrm{Nrd}_{\Delta/T_p}(a)) = 1, \quad \mathrm{Nrd}_{\Delta/T_p}(a) = b^{1-\sigma}, \quad b \in T_p, \quad \{\sigma\} = \mathrm{Gal}(T_p/K).$$

Из локально компактных полей K интерес представляют только несвязные поля. Тогда $b = \mathrm{Nrd}_{\Delta/T_p}(h)$, $b^{1-\sigma} = bgb^{-1}g^{-1}$, где $g \in A^*$. $\mathrm{Nrd}_{\Delta/T_p}(aghg^{-1}h^{-1}) = 1$, поэтому по индуктивному предположению $aghg^{-1}h^{-1} \in \Delta^{(1)} \Rightarrow a \in A^{(1)}$. Если же K — глобальное поле, то для $p \neq 2$ непосредственно из теоремы Эйхлера, а для $p = 2$ из леммы 5.3 также следует существование $b \in \mathrm{Nrd}_{\Delta/T_p}(\Delta^*)$, и снова все сводится к телу Δ меньшей степени. Теорема доказана.

5.5. ТЕОРЕМА. *Пусть A — тело над полным дискретно нормированным полем K с сепарабельным телом вычетов $\bar{A}$. Если поле вычетов $\bar{K}$ локально компактно или глобально, то $SK_1(A) = 1$.*

Доказательство. Как обычно, достаточно доказать теорему для тел примарной степени: $[A:K]=p^{\alpha}$. Рассмотрим менее простой случай, когда $\overline{K}$ — глобальное поле. Если $Z(\overline{A})=\overline{K}$, то из утверждения п. 3.13 и теоремы 5.4 следует, что $SK_1(A)=1$. Пусть теперь $Z(\overline{A})\neq\overline{K}$. Тогда $Z(\overline{A})$ — циклическое расширение $\overline{K}$, причем порождающий автоморфизм σ группы $\mathrm{Gal}(Z(\overline{A})/\overline{K})$ продолжается до автоморфизма $\tilde{\sigma}$ тела $\overline{A}$ (см. п. 3.1). Если $a\in SL(1, A)$, то

$$N_{Z(\overline{A})/\overline{K}}(\mathrm{Nrd}_{\overline{A}/Z(\overline{A})}(\overline{a}))=1.$$

По лемме 5.3 $\mathrm{Nrd}_{\overline{A}/Z(\overline{A})}(\overline{a})=\alpha^{1-\sigma}$, где $\alpha=\mathrm{Nrd}_{\overline{A}/Z(\overline{A})}(b)$.

Элемент b поднимается до некоторого элемента $\beta\in A$, $\overline{\beta}=b$. Тогда для простого элемента π тела A

$$\mathrm{Nrd}_{\overline{A}/Z(\overline{A})}\overline{(\beta\pi\beta^{-1}\pi^{-1})}=\mathrm{Nrd}_{\overline{A}/Z(\overline{A})}(\overline{\beta})\mathrm{Nrd}_{\overline{A}/Z(\overline{A})}\overline{(\pi\beta^{-1}\pi^{-1})}=\alpha^{1-\sigma}.$$

Следовательно,

$$\mathrm{Nrd}_{\overline{A}/Z(\overline{A})}\overline{(a\pi\beta\pi^{-1}\beta^{-1})}=1\Rightarrow\overline{a\pi\beta\pi^{-1}\beta^{-1}}\in\overline{A}^{(1)}.$$

Но всякий элемент из $\overline{A}^{(1)}$ поднимается до элемента из $A^{(1)}$, в частности, существует такой элемент $t\in A^{(1)}$, что $\overline{a\pi\beta\pi^{-1}\beta^{-1}t}=1$, т. е. $a\pi\beta\pi^{-1}\beta^{-1}t\in$ $\in 1+\mathfrak{P}_A$. По конгруэнц-теореме 3.12 тогда $a\in A^{(1)}$. Для локально компактного поля $\overline{K}$ доказательство совершенно аналогично. Теорема 5.5 доказана.

5.6. Замечания. Теорема 5.4 для поля K нулевой характеристики впервые доказана Вангом ([4]). Новое доказательство не только проще и короче, но и более по существу. Теорема 5.5 доказана автором совместно с С. И. Янчевским и анонсирована в ([11]). Отметим, что при $\mathrm{char}\,K=\mathrm{char}\,\overline{K}$ поле K является полем формальных степенных рядов $\overline{K}\langle x\rangle$.

5.7. ТЕОРЕМА. *Пусть R_1, R_2— циклические расширения поля k, являющегося глобальным или локально компактным полем. Тогда для тела $A(R_1, R_2)$ над $k\langle x, y\rangle$*

$$SK_1(A(R_1, R_2))\simeq\mathrm{Br}(R_1R_2/k)/(\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)).$$

Доказательство непосредственно следует из теорем 4.11, 4.17, если учесть, что

$$SK_1(\overline{A}(R_1, R_2)_x)=SK_1(\overline{A}(R_1, R_2)_y)=1$$

по теореме 5.5.

5.8. Следствие. *Для поля $k(x, y)$ рациональных функций*

$$\mathrm{Card}\,SK_1(A(x, R_1)\otimes_{k(x,y)}A(y, R_2))\geqslant\mathrm{Card}\,\mathcal{P}(R_1R_2, R_2, k).$$

5.9. ТЕОРЕМА. *Пусть $A(R_1, R_2)=A(x, R_1)\otimes_{k(x,y)}A(y, R_2)$ — тело над локально компактным полем k. Тогда $SK_1(A(R_1, R_2))$ является цикли-*

ческой группой порядка (n_1, n_2); *в частности, если* $[R_1 : k] = [R_2 : k] = n$, *то* $SK_1(A(R_1, R_2))$ — *циклическая группа порядка* n.

Доказательство. Из теорем 4.17 и 5.7 следует, что

$$SK_1(A(R_1, R_2)) \simeq \mathrm{Br}(R_1R_2/k)/(\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)).$$

По теореме взаимности локальной теории полей классов $\mathrm{Br}(R_1R_2/k)$ — циклическая группа порядка n_1n_2, $\mathrm{Br}(R_1/k)$ и $\mathrm{Br}(R_2/k)$ — соответственно циклические группы порядков n_1 и n_2. Отсюда немедленно получается утверждение теоремы.

5.10. Следствие. *Для поля рациональных функций* $k(x, y)$

$$\mathrm{Card}\, SK_1(A(x, R_1) \otimes_{k(x,y)} A(y, R_2)) \geqslant (n_1, n_2).$$

5.11. Следствие. *Для произвольного* n *существует такое тело* $A(R_1, R_2)$, *что*

$$SK_1(A(R_1, R_2)) \simeq Z/nZ.$$

Доказательство. Возьмем такое несвязное локально компактное поле k, которое содержит примитивный корень n-ой степени из единицы. Тогда в качестве R_1 можно взять неразветвленное расширение степени n, а в качестве R_2 — вполне разветвленное расширение $k(\sqrt[n]{\pi})$, где π — простой элемент в k. По теореме 4.7 $A(R_1, R_2)$ является телом.

5.12. Предложение. *Пусть* $L = R_1 \otimes_k R_2$, *где* k — *глобальное поле,* R_1, R_2 — *циклические расширения* k *простой степени* p. *Если* $d = d(L/k)$ — *число всех таких точек поля* k, *что локальная степень* $[L_v : k_v] = [L : k]$, *то*

$$\mathrm{Br}(L/k)/(\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)) \simeq (Z/pZ)^{d-1} \quad \text{при} \quad d > 0,$$
$$\mathrm{Br}(L/k)/(\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2, k)) = (1) \quad \text{при} \quad d = 0.$$

Доказательство. Для всякой точки поля v на k выберем одну из точек поля L, продолжающую v, и будем обозначать ее также через v. Заметим, что при $[L_v : k_v] = [L : k]$ точка поля v имеет единственное продолжение на L. Группа $\mathrm{Br}(L_v/k_v)$ является циклической группой порядка $[L_v : k_v]$. Естественный гомоморфизм $\mathrm{Br}(L/k) \to \mathrm{Br}(L_v/k_v)$ определяет сюръективный морфизм $h_v : \mathrm{Br}(L/k) \to E_v$, где E_v — группа всех корней из единицы степени $[L_v : k_v]$.

Если $b \in \mathrm{Br}(L/k)$, то для почти всех v $h_v(b) = 1$ и можно рассмотреть гомоморфизм

$$h : \mathrm{Br}(L/k) \to \coprod_v E_v,$$

определяемый так: $h(b) = (h_v(b))$.

Одна из основных теорем теории полей классов утверждает, что отображение h инъективно и $h(\mathrm{Br}(L/k))$ состоит из таких элементов $(e_v) \in \coprod\limits_v E_v$, что $\prod\limits_v e_v = 1$. Мы будем отождествлять $\mathrm{Br}(L/k)$ с $h(\mathrm{Br}(L/k))$.

Для произвольного $b \in \mathrm{Br}(L/k)$ только для конечного числа точек поля v локальный инвариант $h_v(b) \neq 1$, причем $h_v(b)$ имеет порядок p и p^2. Разобьем все точки поля v, для которых $h_v(b) \neq 1$ и $h_v(b)^p = 1$, на два класса:

(I) $v_1^{(1)}, v_2^{(1)}, \ldots, v_r^{(1)}$, если $(R_1)_{v_i^{(1)}} = L_{v_i^{(1)}}$;

(II) $v_1^{(2)}, \ldots, v_s^{(2)}$, если $(R_2)_{v_j^{(2)}} = L_{v_j^{(2)}}$ и $v_i^{(1)} \neq v_j^{(2)}$.

Пусть сначала $d=0$, т. е. группы разложения для всех v цикличны. Тогда все точки поля v, для которых $h_v(b) \neq 1$, исчерпываются точками поля этих двух классов. Так как $\prod_v h_v(b) = 1$, то

$$\prod_{i=1}^{r} h_{v_i^{(1)}}(b) = \varepsilon, \quad \varepsilon^p = 1, \quad \prod_{j=1}^{s} h_{v_j^{(2)}}(b) = \varepsilon^{-1}.$$

Для бесконечного множества точек поля w $(R_1)_w = (R_2)_w \neq k_w$. Действительно, если

$$\mathrm{Gal}(L/R_1) = \{\sigma_1\}, \quad \mathrm{Gal}(L/R_2) = \{\sigma_2\},$$

то пусть R_{12} — подполе в L, соответствующее циклической подгруппе $\{\sigma_1\sigma_2\}$. По теореме плотности Чеботарева для бесконечного множества точек поля w $[L_w : (R_{12})_w] = p$, $(R_{12})_w = k_w$. Тогда $(R_1)_w = (R_2)_w \neq k_w$. Элемент $(h_{v_i^{(1)}}(b), e_w^{(1)})$, где $e_w^{(1)} = \varepsilon^{-1}$, есть элемент группы $\mathrm{Br}(R_1/k)$, а $(h_{v_j^{(2)}}(b), e_w^{(2)})$, где $e_w^{(2)} = \varepsilon$, — элемент группы $\mathrm{Br}(R_2/k)$. Следовательно,

$$b = (h_{v_i^{(1)}}(b), h_{v_j^{(2)}}(b)) = (h_{v_i^{(1)}}(b), e_w^{(1)})(h_{v_j^{(2)}}(b), e_w^{(2)}) \in \mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k).$$

Таким образом, при $d=0$ $\mathrm{Br}(L/k) = \mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)$. В действительности доказано больше: группа $\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)$ совпадает с группой таких элементов $(e_v) \in \coprod_v E_v$, для которых $e_v^p = 1$, $\prod_v e_v = 1$.

Пусть теперь $d > 0$. Тогда к классам (I) и (II) добавляются точки третьего класса:

(III) $v_1^{(3)}, v_2^{(3)}, \ldots, v_d^{(3)}$, если $[L_{v_i^{(3)}} : k_{v_i^{(3)}}] = p^2$.

Так как

$$[(R_1)_{v_i^{(3)}} : k_{v_i^{(3)}}] = [(R_2)_{v_i^{(3)}} : k_{v_i^{(3)}}] = p,$$

то, рассматривая в предыдущем рассуждении вместо w любую точку поля $v_i^{(3)}$, получим, что по модулю $\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)$ элемент $b \in \mathrm{Br}(L/k)$ имеет вид: $b = (h_{v_i^{(3)}}(b))$. По модулю элементов вида $(e_{v_i^{(3)}})$, $e_{v_i^{(3)}}^p = 1$, элементы $(h_{v_i^{(3)}}(b))$ образуют группу, изоморфную $(Z/pZ)^d$. Но условие $\prod_v h_v(b) = 1$ показывает, что $\mathrm{Br}(L/k)/(\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k)) \simeq (Z/pZ)^{d-1}$. Предложение доказано.

5.13. ТЕОРЕМА. *Пусть* $A(R_1, R_2)=A(x, R_1)\otimes_{k\langle x,y\rangle}A(y, R_2)$ — *тело над глобальным полем* k, *причем* $[R_1:k]=[R_2:k]=p$ — *простое число*, $L=R_1\otimes_k R_2$. *Тогда* $SK_1(A(R_1, R_2))\simeq(Z/pZ)^{d-1}$, *где* $d=d(L/k)$ — *число таких точек поля* $v_1, v_2, \ldots, v_d$ *на* k, *для которых* $[L_{v_i}:k_{v_i}]=[L:k]$.

Доказательство непосредственно следует из теорем 4.17, 5.7 и предложения 5.12.

5.14. Довольно неожиданная точная формула теоремы 5.13 может быть получена и в общей ситуации, когда $[R_1:k]$ и $[R_2:k]$ являются произвольными числами. Однако окончательный результат формулируется в более громоздкой форме, поэтому мы ограничимся лишь оценкой сверху, которая близка к точной.

Пусть $L=R_1\otimes_k R_2$, где $[R_1:k]=n_1$, $[R_2:k]=n_2$. Все точки поля k разобьем в конечное число классов следующим образом. Точки поля v_1 и v_2 принадлежат одному классу, если

$$[(R_1)_{v_1}:k_{v_1}]=[(R_1)_{v_2}:k_{v_2}],\quad [(R_2)_{v_1}:k_{v_1}]=[(R_2)_{v_2}:k_{v_2}].$$

Наибольший общий делитель $([(R_1)_v:k_v], [(R_2)_v:k_v])$ не зависит от выбора точки поля из данного класса и будет называться степенью класса. Число классов точек поля L на k будем обозначать через $d(L/k)$. Пусть $v_1, v_2, \ldots, v_{d(L/k)}$ — представители всех классов точек поля L/k, $n(v_i)$ — степени классов.

5.15. ТЕОРЕМА. *Пусть* $A(R_1, R_2)=A(x, R_1)\otimes_{k\langle x,y\rangle}A(y, R_2)$ — *тело над глобальным полем* k. *Тогда порядок*

$$\operatorname{Card} SK_1(A(R_1, R_2))\leqslant\prod_{i=1}^{d(L/k)} n(v_i).$$

Доказательство этой теоремы совершенно аналогично доказательству теоремы 5.13 и его можно опустить.

5.16. Для случая $[R_1:k]=[R_2:k]=n$ дадим еще одну оценку для группы $SK_1(A(R_1, R_2))$, которая основывается на аппроксимационных соображениях и представляет независимый интерес.

ЛЕММА. *Пусть* $L\supset R\supset k$ — *башня циклических расширений степени* n, $\{\sigma\}=\mathrm{Gal}(R/k)$. *Если* v — *дискретная точка поля* k, *неразветвленная в* L, w_1, w_2 — *продолжения* v *на* L, *то для всякого* $a\in R^*$ *со свойством* $a^{1-\sigma}\in N_{L/R}(L^*)$

$$w_1(a)\equiv w_2(a)\ (\mathrm{mod}\, m),\ \text{где } m=[L_{w_1}:R_{w_1}].$$

Доказательство. Прежде всего отметим, что для ограничений w_i на R сохраняются те же обозначения. Так как все продолжения v на R имеют вид $w_1^{\sigma^r}$, то можно считать, что

$$w_2(b)=w_1(b^{\sigma^d})\quad\forall\, b\in R.$$

Тогда из $a^{1-\sigma}\in N_{L/R}(L^*)$ следует, что $a(a^\sigma)^{n-1}\in N_{L/R}(L^*)$. Так как расширения L_{w_i} неразветвлены над k_v, простой элемент поля k_v является и простым элементом в L_{w_l}, а всякий элемент на $O^*_{R_{w_l}}$ является нормой элемента из L_{w_l}, то из $[L_{w_1}:R_{w_1}]=[L_{w_2}:R_{w_2}]=m$ следует, что $w_l(a(a^\sigma)^{n-1})=$ $=ml_l$, где m делит n. Пусть $w_1(a^{\sigma^j})=t_j$. Тогда

$$w_1^{\sigma^r}(a(a^\sigma)^{n-1})=w_1(a^{\sigma^r})+w_1((a^{\sigma^{r+1}})^{n-1})=$$
$$=t_r+(n-1)t_{r+1}=ml_{r+1}\Rightarrow t_r-t_{r+1}=ml_{r+1}-nt_{r+1}.$$

Это означает, что $t_r\equiv t_{r+1}(\mathrm{mod}\,m)$, поэтому $t_i\equiv t_j(\mathrm{mod}\,m)$ для всех i, j. В частности, $w_1(a)=t_0\equiv w_2(a)=t_d(\mathrm{mod}\,m)$. Лемма доказана.

5.17. ТЕОРЕМА. *Пусть k — глобальное поле, т. е. конечное расширение k_0, являющегося полем рациональных чисел или полем рациональных функций одной переменной с конечным полем констант. Если $A(R_1, R_2)=A(x, R_1)\otimes_{k(x,y)}A(y, R_2)$ является телом, причем $[R_1:k]=$ $=[R_2:k]=n$, то* $\mathrm{Card}\,SK_1(A(R_1, R_2))\leqslant n^{\delta-1}$, *где δ — число таких ветвящихся над k_0 точек поля $L=R_1\otimes_k R_2$, для которых $L_v\neq(R_2)_v$.*

Доказательство. В силу теоремы 4.11 достаточно доказать, что $\mathrm{Card}\,\mathscr{P}(L, R_2, k)\leqslant n^{\delta-1}$. Обозначим через $T=(w_1, w_2, \ldots, w_\delta)$ множество всех ветвящихся над k_0 точек поля L, для которых $L_{w_l}\neq(R_2)_{w_l}$. Пусть $a^*\in\mathscr{P}(L, R_2, k)$. Покажем, что в a^* можно выбрать такого представителя $a_0\in R_2^*$, что для всякой точки поля $w\notin T$ $a_0\in N_{L_w/(R_2)_w}(L_w)$. По условию для всякого $a\in a^*$ $a^{1-\sigma}\in N_{L/R_2}(L)$, где $\{\sigma\}=\mathrm{Gal}(R_2/k)$. Значит, $a^{1-\sigma}\in$ $\in N_{L_w/(R_2)_w}(L_w)$ для всех точек поля w, причем a определяется с точностью до множителя из k. Достаточно доказать, что $a_0\in N_{L_w/(R_2)_w}(L_w)$ для точек поля w, неразветвленных над k_0.

Так как почти для всех w $a\in O^*_{(R_2)_w}$, то пусть $\Theta=(\theta_1, \theta_2, \ldots, \theta_s)$ — именно те точки поля, для которых a не является единицей в $(R_2)_{\theta_i}$, $i=$ $=1, 2, \ldots, s$. Разобьем точки поля $\theta_1, \theta_2, \ldots, \theta_s$ на классы, состоящие из точек поля, лежащих над одной и той же точкой поля k_0. Для определенности пусть $\theta_1, \theta_2, \ldots, \theta_r$ лежат над точкой поля v. Так как поля L_{θ_i} неразветвлены над $(k_0)_v$, то по лемме 5.16 $a=\pi^{t(v)}\varepsilon_i$, $i=1, 2, \ldots, r$, где $\varepsilon_i\in O^*_{(R_2)_{\theta_i}}$, π — простой элемент кольца $O_{(k_0)_v}$, являющийся также простым элементом кольца O_{k_0}. Такой выбор элемента π всегда возможен, ибо по сильной аппроксимационной теореме O_{k_0} плотно в $O_{(k_0)_v}$ в v-адической топологии и, кроме того, в O_{k_0} разложение на простые множители однозначно. Тогда нетрудно видеть, что для всех других точек поля $w\notin\Theta\bigcup T$ $\pi\in O^*_{(R_2)_w}$ и с учетом неразветвленности $L_w/(R_2)_w$ $\pi\in N_{L_w/(R_2)_w}(L_w)$. Рассмотрим теперь элемент $b=a\pi^{-t(v)}$. Из приведенного выше следует, что для всех $w\notin T$, $w\neq\theta_j$, $j=r+1, \ldots, s$, $b\in N_{L_w/(R_2)_w}(L_w)$. Очевидное индуктивное рассуждение завершает доказательство и в итоге получается такой элемент $a_0\in a^*$, что для $w\notin T$

$$a_0\in N_{L_w/(R_2)_w}(L_w).$$

Образуем теперь группу

$$(R_2^*)_T = (R_2^*)_{w_1} \times (R_2^*)_{w_2} \times \ldots \times (R_2^*)_{w_\delta}$$

и обычным образом отождествим группу R_2^* с ее диагональным вложением в $(R_2^*)_T$. Аналогично строится L_T^*. Из теоремы взаимности локальной теории полей классов следует, что порядок фактор-группы $(R_2^*)_T/N_{L_T/(R_2)_T}(L_T^*)$ не превосходит n^δ. Если $a_0 \in (N_{L_T/(R_2)_T}(L_T^*)) \cap R_2^*$, то по теореме Хассе о норме для циклических расширений $a_0 \in N_{L/R_2}(L^*)$ и элемент $a^* = 1^*$ — единица группы $\mathscr{P}(L, R_2, k)$. Немедленный вывод отсюда — порядок $\mathscr{P}(L, R_2, k)$ не превосходит n^δ. Но по формуле произведения для символа норменного вычета

$$\prod_{w_i \in T} \left(\frac{a_0,\, L/R_2}{w_i}\right) = 1,$$

ибо по построению для $w \notin T$ $\left(\frac{a_0,\, L/R_2}{w}\right) = 1$. Это означает, что не более $\delta - 1$ символов $\left(\frac{a_0,\, L/R_2}{w_i}\right)$ принимают независимые значения, поэтому $\operatorname{Card} \mathscr{P}(L, R_2, k) \leqslant n^{\delta-1}$. Теорема 5.17 доказана.

5.18. В заключение этого параграфа вычислим $SK_1(A(R_1, R_2))$ для тел $A(\sqrt{p}, \sqrt{r}) = A(x, Q(\sqrt{p})) \otimes_{Q\langle x, y\rangle} A(y, Q(\sqrt{r}))$ в элементарной арифметической форме. Именно такие тела впервые рассматривались в статье ([11]). Они представляют особый интерес и потому, что доставляют минимальные контрпримеры к проблеме Таннака — Артина как в смысле степени тела, так и поля $Q\langle x, y\rangle$.

5.19. ТЕОРЕМА. *Группа $SK_1(A(\sqrt{p}, \sqrt{r}))$ может быть только трех типов*:

I) $SK_1(A(\sqrt{p}, \sqrt{r})) = 1$ *тогда и только тогда, когда выполняется одно из следующих условий*:

а) *символ Лежандра* $\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = 1$;

б) $\left(\frac{p}{r}\right) = -\left(\frac{r}{p}\right)$, $pr \equiv 1 \pmod 8$.

II) $SK_1(A(\sqrt{p}, \sqrt{r})) \simeq Z/2Z$ *тогда и только тогда, когда выполняется одно из следующих условий*:

а) $\left(\frac{r}{p}\right) = \left(\frac{p}{r}\right) = -1$ *и хотя бы одно из чисел* $p, r, pr \equiv 1 \pmod 8$;

б) $\left(\frac{p}{r}\right) = -\left(\frac{r}{p}\right)$, $pr \not\equiv 1 \pmod 8$.

III) $SK_1(A(\sqrt{p}, \sqrt{r})) \simeq (Z/2Z)^2$ *тогда и только тогда, когда* $\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = -1$, $p, r, pr \not\equiv 1 \pmod 8$.

Доказательство. Применяем теорему 5.13 в сочетании с квадратичным законом взаимности. Так как для простого числа t равенство $[Q_t(\sqrt{p}, \sqrt{r}) : Q_t] = 4$ возможно лишь для $t = p$, r или 2 (для всех других значений t расширение $Q(\sqrt{p}, \sqrt{r})/Q$ неразветвлено), то $d = d(Q(\sqrt{p}, \sqrt{r})/Q) \leqslant 3$ и либо I) $SK_1(A(\sqrt{p}, \sqrt{r})) = 1$, либо II) $SK_1(A(\sqrt{p}, \sqrt{r})) \simeq Z/2Z$, либо III) $SK_1(A(\sqrt{p}, \sqrt{r})) \simeq (Z/2Z)^2$.

Разберем случай [I). Если $\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = 1$, то $d = d(Q(\sqrt{p}, \sqrt{r})/Q) \leqslant 1$, ибо разве лишь при $t = 2$ $[Q_t(\sqrt{p}, \sqrt{r}) : Q_t] = 4$. При условии I)б из $pr \equiv 1 \pmod 8$ следует, что $[Q_2(\sqrt{p}, \sqrt{r}) : Q_2] \leqslant 2$. Так как одно из чисел $\left(\frac{p}{r}\right)$, $\left(\frac{r}{p}\right)$ равно единице, то и в этом случае $d \leqslant 1$, т. е. $SK_1(A(\sqrt{p}, \sqrt{r})) = 1$. Проверим необходимость этих условий, т. е. теперь предполагается, что $SK_1(A(\sqrt{p}, \sqrt{r})) = 1$. Это означает, что $d \leqslant 1$. Если p или $r \equiv 1 \pmod 4$, то $\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = 1$, в противном случае $\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = -1 \Rightarrow [Q_p(\sqrt{p}, \sqrt{r}) : Q_p] = [Q_r(\sqrt{p}, \sqrt{r}) : Q_r] = 4 \Rightarrow d \geqslant 2$, что невозможно. Остается рассмотреть случай, когда $p \equiv r \equiv 3 \pmod 4$. Тогда по квадратичному закону взаимности одно из чисел $\left(\frac{p}{r}\right)$, $\left(\frac{r}{p}\right)$ равно -1. Пусть $\left(\frac{p}{r}\right) = -1$; легко видеть, что $[Q_r(\sqrt{p}, \sqrt{r}) : Q_r] = 4$. Если теперь $pr \not\equiv 1 \pmod 8$, то $[Q_2(\sqrt{p}, \sqrt{r}) : Q_2] = 4$, следовательно, $d \geqslant 2$, что снова невозможно. Типы II) и III) рассматриваются совершенно аналогично. Например, для типа III) имеем эквивалентность:

$$SK_1(A(\sqrt{p}, \sqrt{r})) \simeq (Z/2Z)^2 \Leftrightarrow d = 3.$$

При $d = 3$

$$[Q_p(\sqrt{p}, \sqrt{r}) : Q_p] = [Q_r(\sqrt{p}, \sqrt{r}) : Q_r] = [Q_2(\sqrt{p}, \sqrt{r}) : Q_2] = 4.$$

Отсюда следует, что $\left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = -1$, $p, r, pr \not\equiv 1 \pmod 8$. Достаточность условий на p и r почти очевидна. Теорема доказана.

5.20. Следствие. *Пусть* $p \equiv r \equiv 3 \pmod 4$, $\left(\frac{p}{r}\right) = 1$, $pr \equiv 1 \pmod 8$. *Тогда* $SK_1(A(\sqrt{p}, \sqrt{r})) = 1$, *но* $SK_1(A(\sqrt{p}, \sqrt{r}) \otimes_{Q\langle x, y\rangle} Q_p\langle x, y\rangle) \simeq Z/2Z$, *т. е. расширение поля* Q *до поля* p*-адических чисел* Q_p *увеличивает группу* $SK_1(A)$.

Доказательство вытекает из I) и теоремы 5.9.

5.21. На первый взгляд следствие 5.20 кажется несколько патологическим, ибо интуиция подсказывает, что при таком большом увеличении поля приведенная группа Уайтхеда $SK_1(A)$ скорее должна уменьшаться. Истинная причина заключается в том, что не все локальные символы Гильберта поднимаются до глобальных. В следующем параграфе будет показано, что аналогичная ситуация имеет место для тел произвольной степени.

§ 6. Обратная задача приведенной K-теории

6.1. В предыдущем параграфе было доказано, что для глобального поля k $SK_1(A(R_1, R_2))$ является конечной абелевой группой. Если же $[R_1 : k] = [R_2 : k] = p$, то $SK_1(A(R_1, R_2))$ будет абелевой группой экспоненты p. Естественно возникает вопрос: всякая ли конечная абелева группа экспоненты p реализуется в виде $SK_1(A(R_1, R_2))$? Ответ утвердителен и в этом состоит один из основных результатов настоящего параграфа, в своей технической части полностью относящийся к теории полей классов.

В дальнейшем через k_0 обозначается минимальное глобальное поле, т. е. поле рациональных чисел или поле рациональных функций одной переменной с конечным полем констант.

6.2. ТЕОРЕМА. *Для всякой группы $(Z/pZ)^i$, $i \geqslant 0$, существуют такие циклические расширения $R_1^{(i)}/k_0$, $R_2^{(i)}/k_0$ степени p, что*

$$SK_1(A(x, R_1^{(i)}) \otimes_{k_0\langle x,y\rangle} A(y, R_2^{(i)})) \simeq (Z/pZ)^i.$$

Доказательство. Из теорем 4.7, 4.11 и 5.13 легко вывести, что утверждение теоремы 6.2 эквивалентно следующему утверждению теории полей классов: для произвольного простого p и неотрицательного i существует такое абелево расширение $L^{[i]}$ поля k_0 типа (p, p), что

$$[L_{v_r}^{[i]} : (k_0)_{v_r}] = [L : k_0]$$

в точности для $i+1$ точек поля $v_1, v_2, \ldots, v_{i+1}$. Так как рассуждения фактически не зависят от характеристики поля k_0, то ограничимся доказательством для случая поля нулевой характеристики, т. е. будем доказывать следующее утверждение для $k_0 = Q$: для произвольного простого p и натурального i существует такое абелево расширение $L^{[i]}/Q$ типа (p, p), что $[L_{p_r}^{[i]} : Q_{p_r}] = [L : Q]$ в точности для $i+1$ простых чисел (точек поля) $p_1, p_2, \ldots, p_{i+1}$.

Пусть $F = \prod\limits_r Z_r^*$, где Z_r^* — мультипликативная группа кольца r-адических чисел Z_r. В соответствии с теорией полей классов все конечные абелевы расширения поля Q находятся во взаимно однозначном соответствии с подгруппами конечного индекса группы F. Пусть M_p — множество простых чисел вида $1 + pn$, которое бесконечно по теореме Дирихле о простых числах в арифметических прогрессиях. Нетрудно видеть, что для любого $q \in M_p$ в группе Z_q^* существует подгруппа $Z_q^*(p)$ индекса p. Выберем $q_1 \in M_p$ и число $t < q_1$, порождающее факторгруппу $Z_{q_1}^*/Z_{q_1}^*(p)$. Тогда существует бесконечное подмножество $M_p(t) \subset M_p$, состоящее из чисел $r \equiv t \pmod{q_1}$. Действительно, в прогрессии $t + q_1(p - t + 1) + pq_1 n$ содержится бесконечное число простых, но всякое простое число из этой прогрессии по построению принадлежит M_p.

Выберем теперь $q_2, \ldots, q_m \in M_p(t)$. В группе

$$D = Z^*_{q_2} \times Z^*_{q_3} \times \ldots \times Z^*_{q_m}$$

существует такая подгруппа H, что $[D : H] = p$ и $[Z^*_{q_j} : (Z^*_{q_j} \cap H)] = p$, т. е. H не содержит элементов групп $Z^*_{q_j}$, $j = 2, \ldots, m$, порождающих $Z^*_{q_j}/Z^*_{q_j}(p)$. Такой выбор подгруппы H действительно возможен. Если x^*_j — независимые образующие группы $D \Big/ \left(\prod\limits_{j=2}^{m} Z^*_{q_j}(p)\right)$, то элементы $x^*_2x^*_3, x^*_3x^*_4, \ldots, x^*_{m-1}x^*_m$ порождают в $D \Big/ \left(\prod\limits_{j=2}^{m} Z^*_{q_j}(p)\right)$ подгруппу индекса p, не содержащую образующих x^*_j. Ее прообраз в D и возьмем в качестве H.

Рассмотрим теперь в группе конечных аделей $A_{Q^*} = Q^* \times \prod\limits_r Z^*_r$ подгруппу $T = Q^* \times Z^*_{q_1}(p) \times H \times \prod\limits_{r \neq q_j} Z^*_r$. По основной теореме теории полей классов существует такое абелево расширение $L^{(m)}/Q$, что $\mathrm{Gal}(L^{(m)}/Q) \simeq A_{Q^*}/T$. По построению A_{Q^*}/T есть группа типа (p, p). Нас особенно интересует локальное поведение $L^{(m)}$. Так как для простых $r \neq q_j$ $Z^*_r \subset T$, то для таких r поле $L^{(m)}_r$ неразветвлено над Q_r. Более того, все простые r, ветвящиеся в $L^{(m)}$, исчерпываются q_j (см. ([2]), гл. XIII). Нам понадобятся известные формулы теории полей классов для вычисления локальной степени $[L^{(m)}_r : Q_r]$ (см. ([2]), гл. XIII, § 10):

$$[L^{(m)}_r : Q_r] = e_r f_r, \quad e_r = [Z^*_r T : T], \quad f_r = [Q^*_r T : Z^*_r T].$$

Покажем, что $[L^{(m)}_{q_j} : Q_{q_j}] = [L^{(m)} : Q] = p^2$, если $j = 2, \ldots, m$. Имеем:

$$Z^*_{q_j} T = Q^* \times Z^*_{q_1}(p) \times (Z^*_{q_j} H) \times \prod_{r \neq q_j} Z^*_r,$$

поэтому

$$[Z^*_{q_j} T : T] = [Z^*_{q_j} H : H] = [Z^*_{q_j} : (Z^*_{q_j} \cap H)] = p.$$

Для доказательства равенства $[Q^*_{q_j} T : Z^*_{q_j} T] = p$, $j = 2, \ldots, m$, достаточно доказать, что $Q^*_{q_j} T \neq Z^*_{q_j} T$. Предположим, что $Q^*_{q_j} T = Z^*_{q_j} T$. Тогда для подходящего $t = (t, t, \ldots, t, \ldots) \in Q^*$

$$t\left(1, \ldots, 1, \frac{1}{q_j}, 1, \ldots, 1, \ldots\right) \in Z^*_{q_1}(p) \times (Z^*_{q_j} H) \times \prod_{\substack{r \neq q_l \\ l = 1, 2, \ldots, m}} Z^*_r,$$

где $\frac{1}{q_j} \in Q^*_{q_j}$. Тогда $\frac{t}{q_j} \in Z^*_{q_j}$, значит, $t = q_j \frac{t_1}{t_2}$, где t_1, t_2 — взаимно простые целые числа, не делящиеся на q_j. Если $t = q_j$, то включение невозможно, ибо $t \in Z^*_{q_1}(p)$, но q_j по построению не содержится в $Z^*_{q_1}(p)$. Следовательно, одно из чисел t_1, t_2 должно делиться на простое число s. Но тогда $t = q_j \dfrac{t_1}{t_2}$ не содержится в Z^*_s, что противоречит первоначальному предположению. Таким образом, $[L^{(m)}_{q_j} : Q_{q_j}] = p^2$, $j = 2, \ldots, m$.

Если $[L^{(m)}_{q_1} : Q_{q_1}] = p^2$, то положим $m = i+1$ и тогда получим поле $L^{[i]} = L^{(i+1)}$, удовлетворяющее нашим требованиям. В случае $[L^{(m)}_{q_1} : Q_{q_1}] = p$ в качестве m возьмем число $i+2$. Теорема доказана.

6.3. Следствие. *Для любого простого p существует такое тело A над $Q\langle x, y\rangle$ степени p^2, что $SK_1(A) = 1$, но для подходящего поля r-адических чисел Q_r*

$$SK_1(A \otimes_Q Q_r) \simeq Z/pZ.$$

Доказательство. Тело A соответствует полю $L^{[0]}$ теоремы 6.2, а r — то единственное простое число, для которого $[L^{[0]}_r : Q_r] = [L : Q]$. Далее применяется теорема 5.9.

6.4. Замечание. Анализ доказательства предыдущей теоремы показывает, что она может быть обобщена на случай абелевых групп произвольной экспоненты, если получить точную формулу для вычисления группы $\mathrm{Br}(L/k)/(\mathrm{Br}(R_1/k)\,\mathrm{Br}(R_2/k))$ в общем случае.

6.5. Теорема 6.2 по своему характеру является теоремой существования. Для $p = 2$ можно дать явную конструкцию полей $R^{(i)}_1$ и $R^{(i)}_2$.

Предложение. *Пусть $p_1, p_2, \ldots, p_i$ — различные простые числа вида $1 + 4n$. Существует бесконечное множество простых $p \equiv 1 \pmod 4$, для которых $\left(\frac{p_l}{p}\right) = -1$, $l = 1, 2, \ldots, i$. Если p — одно из таких простых чисел, то*

$$SK_1(A)(Q(\sqrt{p}, Q(\sqrt{p_1p_2 \ldots p_i}))) \simeq (Z/2Z)^i \vee (Z/2Z)^{i-1}$$

соответственно для нечетного или четного i.

Доказательство. Из китайской теоремы об остатках следует существование такого z, что $z \equiv 1 \pmod 4$, $\left(\frac{z}{p_l}\right) = -1$, $l = 1, 2, \ldots, i$. В арифметической прогрессии $z + 4p_1p_2 \ldots p_in$ существует бесконечное число простых, которые удовлетворяют условиям предложения. Пусть p — одно из них. Применяем к полю $L = Q(\sqrt{p}, \sqrt{p_1p_2 \ldots p_i})$ теорему 5.13. Если i нечетно, то

$$\left(\frac{p_1p_2 \ldots p_l}{p}\right) = -1, \quad \left(\frac{p}{p_l}\right) = -1, \quad l = 1, \ldots, i.$$

Ввиду выбора простых чисел, $[L_2 : Q_2] < 4$, поэтому $d = i + 1$, а значит,

$$SK_1(A(Q(\sqrt{p}), Q(\sqrt{p_1p_2 \ldots p_i}))) \simeq (Z/2Z)^i.$$

Для четного i $\left(\frac{p_1p_2 \ldots p_l}{p}\right) = 1$, поэтому $d = i$. Предложение доказано.

6.6. Результаты этого и предыдущего параграфов убеждают в том, что вычисление группы $SK_1(A)$ в общем случае является малореальной задачей. Поэтому естественно основной проблемой считать проблему характеризации полей K, для которых проблема Таннака — Артина решается положительно или отрицательно. Для полных дискретно нормированных полей почти предельная характеризация следует из теорем 5.5, 5.7, 5.9, 5.13. Теперь уже нетрудно получить решение этой проблемы для конечнопорожденных полей, т. е. полей алгебраических функций конечной степени над простым подполем.

6.7. ТЕОРЕМА. *Пусть K — конечнопорожденное поле. Если степень трансцендентности K над простым подполем больше единицы при* $\operatorname{char} K=0$ *и больше двух при* $\operatorname{char} K>0$, *то для произвольного числа m существует такое тело A с центром K, что* $\operatorname{Card} SK_1(A)>m$.

Доказательство. Так как рассуждения при $\operatorname{char} K=0$ и $\operatorname{char} K>0$ совершенно аналогичны, то ограничимся случаем $\operatorname{char} K=0$. Тогда K является конечным расширением поля рациональных функций $Q(x_1, x_2, \ldots, x_n)$ от n независимых переменных. Пусть p — простое число, не делящее степени $[K:Q(x_1, x_2, \ldots, x_n)]$. Для достаточно большого i $p^i>m$. Так как степень трансцендентности поля K над Q больше единицы, то $n\geqslant 2$. В соответствии с теоремой 6.2 и следствием 4.12 тогда существует тело B с центром $Q(x_1, x_2)$ степени p^2, для которого $\operatorname{Card} SK_1(B)\geqslant p^i$. Пусть $A=B\otimes_{Q(x_1,x_2)}K$. Тогда из лемм 2.7 и 2.2 следует, что $\operatorname{Card} SK_1(A)\geqslant \operatorname{Card} SK_1(B)\geqslant p^i>m$. Теорема доказана.

6.8. Таким образом, для конечнопорожденных полей только в случае алгебраических функций одной переменной неизвестно, может ли приведенная группа Уайтхеда быть нетривиальной. Заметим, что для поля формальных степенных рядов одной переменной с полем алгебраических чисел в качестве поля констант всегда $SK_1(A)=1$.

Аналоги теоремы 6.6 справедливы и для других полей, например, для полей алгебраических функций над локально компактным несвязным полем k.

§ 7. Дальнейшие перспективы

Подводить окончательные итоги развития теории, совершившей довольно неожиданный поворот, пока еще рано. Но уже сейчас можно обсуждать возникшие здесь новые идеи и связи. Для широкого класса алгебр A вычисление группы $SK_1(A)$ редуцировано к задаче теории полей — вычислению группы специальных проективных конорм. Для локальных и глобальных полей вычисление группы специальных проективных конорм доведено почти до конца. Но для других полей положение не столь обнадеживающее. Несомненно, что для полей функций от двух и более переменных арифметические соображения недостаточно эффективны и понадобится привлечение алгебро-геометрических методов. Из принципиальных вопросов, по-видимому, остался нерешенным один*:

* Примечание при корректуре. Этот вопрос уже решен в моей статье «О бесконечности приведенной группы Уайтхеда», Докл. АН СССР, 227, № 2 (1976), где найдены условия бесконечности группы SK_1 (A).

может ли группа $SK_1(A)$ быть бесконечной? Весьма вероятно, что к ответу на этот вопрос приведет вычисление группы специальных проективных конорм над полями функций в самых простых случаях, т. е. вычисление группы $\mathrm{Br}(L/k)/(\mathrm{Br}(R_1/k)\mathrm{Br}(R_2/k))$, где L — композит квадратичных расширений R_1/k, R_2/k.

Хотя окончательного результата о том, что всякая конечная абелева группа реализуется в качестве $SK_1(A)$, пока нет, но в принципе здесь все ясно и это уже задача непосредственно теории полей классов.

Можно ввести различные обобщения группы специальных проективных конорм, связанные с телами над полными дискретно нормированными полями, не являющимися тензорными произведениями. Однако связь этих групп с $SK_1(A)$ оказывается уже не столь полезной и одна из ближайших важных задач — эффективное обобщение конструкции группы специальных проективных конорм. Возможно, что это обобщение лучше искать сразу в терминах групп Брауэра подполей и полей вычетов, связанных с данным дискретно нормированным телом.

При доказательстве теоремы 5.17 обнаруживается некоторая связь порядка группы $SK_1(A)$ с числом классов идеалов поля k. Было бы интересно выявить эту связь в точной форме.

Следствие 6.3 показывает, что при расширении центра K тела A группа $SK_1(A)$ может претерпевать довольно неожиданные изменения. Представляется весьма интересным более тщательное исследование этой ситуации *.

Естественно возникает задача распространения результатов, полученных для $SL(1, A)$, на группы K-точек G_K односвязных простых K-определенных алгебраических групп в связи с гипотезой Кнезера — Титса. В первую очередь, разумеется, надо решить принципиальный вопрос о справедливости гипотезы Кнезера — Титса для других типов простых алгебраических групп, среди которых особый интерес представляют унитарные группы. Недавно в ([23]) показано, по аналогии с ([11]), что для унитарных групп гипотеза Кнезера — Титса решается, вообще говоря, отрицательно, причем с точки зрения типа полей граница между положительным и отрицательным ответом оказывается, с учетом ([9]), ([22]), по-видимому, такой же, как и для группы $SL(1, A)$. Ближайшая задача — построение приведенной унитарной K_1-теории, аналогичной построенной в настоящей статье. Кажется правдоподобным, что приведенная унитарная группа Уайтхеда $SUK_1(A)$ в существенной мере будет определяться группой $SK_1(A)$.

Поступило
27.VI.1975

* **Примечание при корректуре.** Такое исследование проведено в моей статье «Бесконечность приведенной группы Уайтхеда в проблеме Таннака — Артина», Матем. сб.

Литература

1 **Бурбаки Н.,** Алгебра: модули, кольца, формы, М., «Наука», 1966.

2 **Вейль А.,** Основы теории чисел, М., «Мир», 1972.

3 **Nakayama T., Matsushima Y.,** Über die multiplikative Gruppe einer p-adischen Divisionsalgebra, Proc. Imperial Academy of Japan, 19 (1943), 622—628.

4 **Wang S.,** On the commutator group of a simple algebra, Amer. J. Math., 72, № 2 (1950), 323—334.

5 **Артин Э.,** Геометрическая алгебра, М., «Наука», 1969.

6 **Tits J.,** Algebraic and abstract simple groups, Ann. Math., 80, № 2 (1964), 313—329.

7 **Harder G.,** Eine Bemerkung zum sehwachen Approximationssatz, Archiv Math., XIX, 5 (1968), 465—472.

8 **Borel A., Tits J.,** Homomorphismes «abstraits» de groupes algebriques simples, Ann. Math., 97, № 3 (1973), 499—571.

9 **Платонов В. П.,** Проблема сильной аппроксимации и гипотеза Кнезера — Титса, Изв. АН СССР. Сер. матем., 33 (1969), 1211—1220.

10 **Платонов В. П.,** Дополнение к работе «Проблема сильной аппроксимации и гипотеза Кнезера — Титса», Изв. АН СССР. Сер. матем., 34 (1970), 775—777.

11 **Платонов В. П.,** О проблеме Таннака — Артина, Докл. АН СССР, 221, № 5 (1975), 1038—1041.

12 **Платонов В. П.,** Проблема Таннака — Артина и группы проективных конорм, Докл. АН СССР, 222, № 6 (1975), 1299—1302.

13 **Kodama T.,** On the commutator group of normal simple algebra, Mem. Fac. Sci. Kuyshu Univ., Ser. A, 10 (1956), 141—149, 14 (1960), 98—103.

14 Алгебраическая теория чисел (под редакцией Дж. Касселса и А. Фрелиха), М., «Мир», 1969.

15 **Басс Х.,** Алгебраическая K-теория, М., «Мир», 1973.

16 **Schilling O. G.,** The Theory of Valuations, Amer. Math. Soc., v. 17, № 4 (1950), 1—253.

17 **Serre J.-P.,** Corps locaus, Paris, 1962.

18 **Платонов В. П., Янчевский В. И.,** О гипотезе Хардера, Докл. АН СССР, 221, № 4 (1975), 784—787.

19 **Deuring M.,** Algebren, Berlin, 1968.

20 **Джекобсон Н.,** Теория колец, М., ИЛ, 1947.

21 **Картан А., Эйленберг С.,** Гомологическая алгебра, М., ИЛ, 1960.

22 **Платонов В. П.,** Арифметические и структурные проблемы в линейных алгебраических группах, Тр. Международного матем. конгресса в Ванкувере, т. 2 (1975), 39—44.

23 **Платонов В. П., Янчевский В. И.,** О гипотезе Кнезера — Титса для унитарных групп, Докл. АН СССР, 225, № 1 (1975), 48—52.