Ж. Дьёдонне

ГЕОМЕТРИЯ КЛАССИЧЕСКИХ ГРУПП

Перевод с французского
Э. Б. Винберга

Издательство «МИР»
Москва 1974

УДК 519.4

Монография одного из крупнейших французских математиков Жана Дьёдонне содержит систематическое изложение теории классических линейных групп иад произвольным телом. Третье ее издание дополнено новейшими результатами об автоморфизмах классических групп.

Несмотря на то что многие из результатов, излагаемых в книге, могут быть теперь получены методами теории полупростых алгебраических групп, монография Дьёдоние сохраняет свое значение как безукоризненное изложение теории классических групп .классическими методами, преимущество которых состоит в простоте и высокой степени конструктивности.

Изложение носит характер обзора: доказательства, как правило, лишь намечаются. Благодаря этому книга при небольшом объеме содержит очень много результатов.

Книга заинтересует математиков многих специальностей, в первую очередь специалистов по алгебре и топологии. Она будет полезна преподавателям, аспирантам и студентам старших курсов университетов и пединститутов.

Редакция литературы по математическим наукам

Д $\frac{20203-005}{041(01)-74}$ 5—74

ОТ ПЕРЕВОДЧИКА

Книга Ж. Дьёдонне содержит наиболее полное изложение теории классических линейных групп над произвольными телами. Она является как хорошим руководством для изучения предмета, так и незаменимым справочным пособием. Ее автор — крупный французский математик, которому принадлежит много оригинальных работ в этой области.

Название книги, быть может, не дает достаточно ясного представления о ее содержании. Основная ее цель — выяснение алгебраической структуры классических групп; геометрия же, наряду с линейной алгеброй, служит средством для достижения этой цели. Полностью геометрическим вопросам посвящена лишь третья глава, но и она носит скорее вспомогательный характер.

Ко времени выхода второго издания книги теория классических групп в основном закончила свое самостоятельное развитие и влилась в теорию полупростых алгебраических линейных групп, создание которой связано в первую очередь с именами К. Шевалле, А. Бореля и Ж. Титса. Однако классические методы не утратили значения ввиду своей элементарности и высокой степени конструктивности, которую им придает аппарат линейной алгебры, не говоря уже о том, что классические результаты служат образцом для обобщений. Поэтому книга Дьёдонне, зафиксировавшая состояние классической теории линейных групп в высшей фазе ее развития, еще долго сохранит свою ценность.

Э. Б. Винберг

ПРЕДИСЛОВИЕ АВТОРА

В этой книге излагаются примерно те же теории, что и в первой трети труда Ван-дер-Вардена «Группы линейных преобразований», вышедшего раньше в этой серии. В ней дается значительно более развернутое изложение, которое отражает в первую очередь большое число работ на тему книги, появившихся в течение последних двадцати лет и существенно изменивших точку зрения на рассматриваемые в ней вопросы. С другой стороны, хотя в отведенных нам рамках не могло быть и речи о полных доказательствах, мы старались демонстрировать хотя бы основные идеи доказательств значительно чаще, чем это сделано у Ван-дер-Вардена.

Из всех групп линейных преобразований здесь рассматриваются только те, которые называются «классическими». В связи с этим используется лишь «элементарная» часть теории групп, концентрирующаяся вокруг понятий подгруппы и гомоморфизма. Мы не затрагиваем тех частей теории, которые требуют более сложных понятий. Так, мы не касаемся теории линейных представлений групп, а также топологии и дифференциальной геометрии. Поэтому почти единственным средством доказательств остается линейная алгебра в той геометрической форме, которую она приняла в современную эпоху.

Эванстон, 1 октября 1954 г.

Жан Дьёдонне

ПРЕДИСЛОВИЕ КО ВТОРОМУ ИЗДАНИЮ

После выхода в свет в 1955 г. первого издания этой книги было опубликовано довольно много работ о классических группах, внесших значительные улучшения как в методы, так и в результаты. В этом новом издании мы попытались по возможности учесть эти улучшения и привести библиографию в соответствие с сегодняшним днем. Необходимо, однако, указать, что в тексте практически не отражен самый эффектный прогресс, достигнутый в эти последние годы: после решающих работ К. Шевалле, посвященных построению простых групп из простых комплексных алгебр Ли [5] и классификации полупростых алгебраических групп над алгебраически замкнутым полем [6], на первый план вышли методы, заимствованные в значительной степени из теории Ли и алгебраической геометрии и позволяющие трактовать большое число вопросов теории классических групп единым образом, без необходимости изучать группу каждого типа отдельно. Многие математики вслед за К. Шевалле уже с успехом использовали эти общие методы в своей работе, и есть все основания ожидать, что будущее развитие этого направления покроет практически все содержание данной книги. Обзор результатов, достигнутых в этом направлении, должен быть в ближайшее время сделан Ж. Титсом.

Париж, 1 октября 1962 г.

Жан Дьёдонне

Глава I

КОЛЛИНЕАЦИИ И КОРРЕЛЯЦИИ

§ 1. Линейные и полулинейные отображения

В последующем изложении мы предполагаем известными элементарные понятия и результаты линейной алгебры (см., например, монографию Бурбаки [1], обозначениями которой мы пользуемся). Под *векторным пространством* всегда понимается (если не оговорено противное) *конечномерное правое* векторное пространство E над телом K (коммутативным или нет).

Пусть K, K' — два тела, σ — *изоморфизм* тела K на K'. Пусть E — векторное пространство над K и F — векторное пространство над K'. *Полулинейное отображение* пространства E в F *относительно изоморфизма* σ — это такое отображение u, что

$$u(x+y)=u(x)+u(y) \quad \text{при} \quad x \in E,\ y \in E,$$

$$u(x\lambda)=u(x)\lambda^{\sigma} \quad \text{при} \quad x \in E,\ \lambda \in K.$$

Образ при отображении u подпространства из E есть подпространство в F; полный прообраз подпространства из F есть подпространство в E. *Рангом* отображения u называется размерность пространства $u(E)$, равная коразмерности ядра $u^{-1}(0)$ отображения u.

Пусть K'' — третье тело и τ — изоморфизм тела K' на K''. Пусть G — векторное пространство над K'' и v — полулинейное отображение пространства F в G относительно изоморфизма τ. Тогда $w = vu$ есть полулинейное отображение пространства E в G относительно изоморфизма $\sigma\tau$ тела K на K''. Если u биективно, то u^{-1} есть полулинейное отображение пространства F на E относительно изоморфизма σ^{-1}.

В случае когда $K' = K$, *линейное* отображение пространства E в F — это не что иное, как полулинейное отображение, соответствующее тождественному автоморфизму тела K.

Пусть $(a_i)_{1 \leqslant i \leqslant n}$ — базис пространства E. Полулинейное отображение u пространства E в пространство F полностью определяется заданием изоморфизма σ и элементов $z_i = u(a_i)$ $(1 \leqslant i \leqslant n)$ пространства F. В самом деле, при $x = \sum_{i=1}^{n} a_i \xi_i$ имеем $u(x) = \sum_{i=1}^{n} z_i \xi_i^\sigma$. Если $(b_j)_{1 \leqslant j \leqslant m}$ — базис пространства F и $z_i = u(a_i) = \sum_{j=1}^{m} b_j \alpha_{ji}$, то отображение u определяется матрицей $A = (\alpha_{ji})$, имеющей m строк и n столбцов. Матрица A называется матрицей отображения u по отношению к базисам (a_i) и (b_j). Если u биективно (и, значит, $m = n$), то матрицей отображения u^{-1} по отношению к базисам (b_j) и (a_i) служит матрица $(A^{-1})^{\sigma^{-1}}$. Если v — полулинейное отображение F в G относительно изоморфизма τ и B — матрица отображения v по отношению к базису (b_j) пространства F и базису (c_k) пространства G, то матрицей отображения vu по отношению к базисам (a_i) и (c_k) будет матрица BA^τ.

Коллинеацией векторного пространства E над телом K называется всякое *биективное* полулинейное отображение пространства E на себя. Коллинеации пространства E образуют группу. Очевидно, что группы коллинеаций векторных пространств одной размерности над одним телом изоморфны. Обозначим через $\Gamma L_n(K)$ группу коллинеаций фиксированного раз и навсегда n-мерного векторного пространства E над телом K (например, пространства K^n, рассматриваемого как правое векторное пространство над K).

Для всякого $\alpha \in K$, $\alpha \neq 0$, отображение h_α: $x \to x\alpha$ есть коллинеация относительно внутреннего автоморфизма $\xi \to \alpha^{-1}\xi\alpha$ тела K. Говорят, что h_α — *гомотетия* с коэффициентом α. Гомотетии образуют нормальный делитель H_n в группе $\Gamma L_n(K)$, и отображение $\alpha \to h_\alpha$ есть *антиизоморфизм* мультипликативной группы K^* тела K на группу H_n. Гомотетия может быть охарактеризована как коллинеация, относительно которой *инва-*

риантно всякое k-мерное подпространство пространства E (для какого-нибудь *одного* значения k, удовлетворяющего неравенствам $1 \leqslant k < n$).

Коллинеации пространства E, являющиеся *линейными* отображениями[1]), образуют нормальный делитель $GL_n(K)$ в группе $\Gamma L_n(K)$, называемый *полной линейной группой от n переменных над телом K*. Подгруппы H_n и $GL_n(K)$ являются взаимными *централизаторами* в группе $\Gamma L_n(K)$ (см. гл. II, § 1). Их пересечение Z_n есть их общий *центр*. Он изоморфен мультипликативной группе Z^* центра Z тела K и состоит из так называемых *центральных гомотетий* $x \to x\gamma$, где $\gamma \in Z^*$.

Для любых подпространств V и W одинаковой размерности в пространстве E существует такое линейное преобразование $u \in GL_n(K)$, что $u(V) = W$. Иначе говоря, для всякого r, удовлетворяющего неравенствам $1 \leqslant r \leqslant n-1$, группа $GL_n(K)$ *транзитивно* действует на множестве r-мерных подпространств.

Если обозначить через $\varphi(u)$ автоморфизм тела K, соответствующий коллинеации u, то отображение $u \to \varphi(u)$ будет гомоморфизмом группы $\Gamma L_n(K)$ на группу A автоморфизмов тела K. Ядром этого гомоморфизма является $GL_n(K)$, так что $\Gamma L_n(K)/GL_n(K) \simeq A$.

Факторгруппа $P\Gamma L_n(K) = \Gamma L_n(K)/H_n$ может быть отождествлена с группой *проективных коллинеаций* $(n-1)$-мерного правого проективного пространства $P(E) = P_{n-1}(K)$ над K (которое при этом отождествляется с пространством прямых пространства E). Мы будем обозначать через $u \to \bar{u}$ канонический гомоморфизм группы ΓL_n на $P\Gamma L_n$. Проективной коллинеации $\bar{u}$ соответствует не один автоморфизм σ тела K, но целый *класс смежности* группы A по подгруппе I внутренних автоморфизмов (изоморфной K^*/Z^*). Этот класс мы будем обозначать через $\bar{\sigma} = \bar{\varphi}(u)$. Отображение $\bar{\varphi}$ есть гомоморфизм группы $P\Gamma L_n(K)$ на группу A/I. Его ядром является группа $PGL_n(K) = GL_n(K)/Z_n$ проек-

---

[1]) Биективное *линейное* отображение векторных пространств над одним и тем же телом K называется также *изоморфизмом* этих пространств. Таким образом, элементы группы $GL_n(K)$ — это автоморфизмы векторного пространства K^n.

тивных линейных отображений пространства $P_{n-1}(K)$ на себя (так называемая *полная проективная группа* от n переменных над телом K), так что имеем $P\Gamma L_n(K)/PGL_n(K) \simeq A/I$.

§ 2. Растяжения и сдвиги

Мы не будем здесь заниматься проблемой *классификации* коллинеаций векторного пространства E над произвольным телом K. Укажем только, что эта проблема состоит в отыскании условий, при которых коллинеации u и v связаны соотношением $v = tut^{-1}$, где $t \in GL_n(K)$. В случае коммутативного тела K и линейных отображений u проблема решается классической теорией *элементарных делителей* (см., например, Бурбаки [2]). Эта теория обобщена на произвольные коллинеации в работах Джекобсона [1], [2] и [3], Накаямы [1], [2], Асано и Накаямы [1] и Хаантьеса [1]. Мы ограничимся здесь изучением нескольких частных случаев, которые будут использованы в дальнейшем.

Пусть V и W — два дополнительных подпространства размерностей p и $n-p$ $(1 \leqslant p < n)$ в пространстве E. Всякая коллинеация u пространства E, относительно которой инвариантны (в целом) V и W, однозначно определяется своими ограничениями v и w на V и W соответственно. Такие коллинеации образуют группу, изоморфную подгруппе произведения $\Gamma L_p(K) \times \times \Gamma L_{n-p}(K)$, составленной из таких пар (v, w), что автоморфизмы тела K, соответствующие v и w, совпадают. Очевидно, что эта подгруппа содержит в качестве нормального делителя группу $GL_p(K) \times GL_{n-p}(K)$, образованную *линейными* коллинеациями пространства E, относительно которых инвариантны V и W.

В тех же обозначениях рассмотрим коллинеации u, оставляющие на месте *каждый элемент* подпространства V. Ясно, что такая коллинеация должна быть *линейной* и определяется своим ограничением на подпространстве W, дополнительном к V. Для $x \in W$ имеем $u(x) = v(x) + w(x)$, где $v(x) \in V$, $w(x) \in W$. При этом v — произвольное линейное отображение подпространства W в V, а w — произвольное линейное отображение

W *на* себя. Отображения v и w зависят от выбора дополнительного подпространства W, но линейное преобразование, индуцированное w в факторпространстве E/V, зависит только от u.

Рассмотрим частный случай, когда $p = n - 1$, т. е. когда V — *гиперплоскость.* Пусть $W = aK$ — прямая, дополнительная к V. Тогда $w(a) = a\alpha$; элемент $\alpha \in K^*$ определен коллинеацией u с точностью до сопряженности. Обозначим через $\dot\alpha$ *класс сопряженности* элемента α (образованный элементами $\lambda\alpha\lambda^{-1}$). Следует различать два случая в зависимости от того, состоит класс $\dot\alpha$ лишь из единицы 1 тела K или нет. Если $\dot\alpha \neq \{1\}$, то коллинеация u называется *растяжением.* Легко показать, что в этом случае существует единственная прямая $W_0 = a_0K$, дополнительная к V и *инвариантная* (в целом) относительно u. Если $\dot\alpha = \{1\}$ и коллинеация u не тождественна, то она называется *сдвигом* вдоль гиперплоскости V; будем также говорить, что V принадлежит сдвигу u. В этом случае для любого $x \in E$ имеем $u(x) = x + a\rho(x)$, где $a \in V$, а ρ — такая *линейная форма* на E, что $\rho^{-1}(0) = V$. Вектор a и форма ρ определены коллинеацией u с точностью до одновременной замены a на $a\lambda$ и ρ на $\lambda^{-1}\rho$, где $\lambda \in K^*$. Подпространство $V_0 = aK \subset V$ называется прямой, принадлежащей сдвигу u; мы также говорим «сдвиг в направлении прямой V_0». Не существует никакой прямой, инвариантной относительно u и не принадлежащей V.

Растяжения и сдвиги, соответствующие гиперплоскости V, вместе с тождественным отображением образуют подгруппу $D(V)$ группы $GL_n(K)$. Сдвиги вдоль гиперплоскости V вместе с тождественным отображением образуют коммутативный нормальный делитель $T(V)$ в группе $D(V)$, изоморфный аддитивной группе пространства V, т. е. группе K^{n-1}. Факторгруппа $D(V)/T(V)$ изоморфна мультипликативной группе K^*. Группы $D(V)$ и $T(V)$ имеют простую интерпретацию в проективном пространстве $P_{n-1}(K)$: если гиперплоскость пространства $P_{n-1}(K)$, соответствующую пространству V, принять за «бесконечно удаленную», то $D(V)$ будет группой аффинных преобразований пространства K^{n-1}, переводящих каждую прямую в параллельную ей прямую, а $T(V)$ будет группой *параллельных переносов* пространства K^{n-1}.

Два растяжения (соответственно два растяжения, содержащиеся в $D(V)$) сопряжены в группе $GL_n(K)$ (соответственно в группе $D(V)$) тогда и только тогда, когда они соответствуют одному и тому же классу $\dot{\alpha}$ сопряженных элементов в группе K^*. Любые два сдвига сопряжены в группе $GL_n(K)$ $(n \geqslant 2)$; два сдвига, содержащиеся в $T(V)$, сопряжены в группе $D(V)$ тогда и только тогда, когда они соответствуют одной и той же прямой $V_0 \subset V$.

Для того чтобы линейное преобразование $v \in GL_n(K)$ было перестановочно со сдвигом $u \in T(V)$, необходимо и достаточно выполнение следующих условий:

1) $v(V) = V$;

2) $v(V_0) = V_0$, где V_0 — прямая, принадлежащая сдвигу u;

3) если $u(x) = x + a\rho(x)$ и $v(a) = a\lambda$, то $\rho(v(x)) = \lambda\rho(x)$.

Для того чтобы два сдвига были перестановочны, необходимо и достаточно, чтобы прямая каждого из них содержалась в гиперплоскости другого. *Централизатором* группы $T(V)$ в группе $GL_n(K)$ является произведение (прямое) $Z_nT(V)$. В самом деле, относительно преобразования u, перестановочного с любым сдвигом вдоль V, должны быть инвариантны гиперплоскость V и любая прямая этой гиперплоскости. Следовательно, ограничение u на V есть центральная гомотетия h_γ (см. гл. II, § 1). Тогда $h_\gamma^{-1}u \in D(V)$, и легко видеть, что $h_\gamma^{-1}u$ может быть только сдвигом.

§ 3. Инволюции и полуинволюции

Инволюцией в группе $GL_n(K)$ называется такое линейное преобразование u, что $u^2(x) = x$ (мы будем записывать это и так: $u^2 = 1$). Описание таких преобразований различно в случаях, когда характеристика тела отлична от 2 и равна 2.

1°. Если характеристика тела K отлична от 2, то E разлагается в прямую сумму двух подпространств U^+ и U^- (одно из которых может быть нулевым) таким образом, что $u(x) = x$ при $x \in U^+$ и $u(x) = -x$ при $x \in U^-$. Говорят, что U^+ и U^- — это *положительное* и *отрицательное* собственные подпространства инволюции u. Если $\dim(U^+) = p$, то u называется инволюцией типа $(p, n-p)$, или $(p, n-p)$*-инволюцией*. Образ в группе $PGL_n(K)$ инволюции типа $(p, n-p)$ или $(n-p, p)$ $(p \leqslant n/2)$ называется p*-инволюцией*.

2°. Если K — тело характеристики 2, то $u(x) = x + v(x)$, где v — линейное преобразование, удовлетворяющее условию $v^2 = 0$ или, что то же самое, $v(E) \subset v^{-1}(0)$. Говорят, что $v^{-1}(0)$ и $v(E)$ — подпространства, принадлежащие инволюции u (или подпространства этой инволюции). Если $\dim(v(E)) = p$, то $\dim(v^{-1}(0)) = n - p$ и $2p \leqslant n$; в этих обозначениях говорят, что u — инволюция типа $(p, n-p)$, или $(p, n-p)$*-инволюция*, а ее образ в $PGL_n(K)$ называется p*-инволюцией*. В частности, инволюции типа $(1, n-1)$ — это не что иное, как *сдвиги* (см. § 2).

Коллинеация $u \in \Gamma L_n(K)$ будет называться *полуинволюцией*, если соответствующая проективная коллинеация $\bar{u}$ является инволютивным элементом группы $P\Gamma L_n(K)$, т. е. $\bar{u}^2 = 1$. Это равносильно тому, что $u^2(x) = x\gamma$, где $\gamma \in K^*$, для всякого $x \in E$. Если σ — автоморфизм тела K, соответствующий u, то, вычисляя $u^3(x)$ двумя способами, находим, что

$$\gamma^\sigma = \gamma, \tag{1}$$

и, вычисляя $u^2(x\xi)$ двумя способами, — что

$$\xi^{\sigma^2} = \gamma^{-1}\xi\gamma \tag{2}$$

для всех $\xi \in K$. Теперь необходимо рассмотреть два случая:

А) γ *не представляется в виде* $\lambda\lambda^\sigma$, $\lambda \in K$. Тогда можно построить *квадратичное расширение* K_0 тела K, базис которого над K (правый и левый одновременно) состоит из 1 и такого элемента ρ, что $\rho^2 = \gamma$ и $\eta\rho = \rho\eta^\sigma$

для всех $\eta \in K$[1]). Можно, далее, ввести в E структуру правого векторного пространства над K_0, положив $x\zeta = x\xi + u(x)\eta$ при $\zeta = \xi + \rho\eta \in K_0$ $(\xi \in K,\ \eta \in K)$. При этом E будет иметь размерность $n/2$ над K_0, откуда, кстати, следует, что в этом случае n непременно *четно* (ср. Дьёдонне [14][2])).

В) $\gamma = \lambda\lambda^\sigma$, где $\lambda \in K$. Положим тогда $v(x) = u(x)\lambda^{-1}$; это будет полуинволюция относительно автоморфизма τ, определенного равенством $\xi^\tau = \lambda\xi^\sigma\lambda^{-1}$. Имеем $v^2(x) = x$, $\xi^{\tau^2} = \xi$. Пусть K_1 — подтело тела K, образованное элементами, *инвариантными относительно* τ. Возможны два случая:

В1) $K_1 = K$, т. е. τ — тождественный автоморфизм. В этом случае v — инволюция в группе $GL_n(K)$; вид такой коллинеации был определен выше.

В2) K есть *квадратичное расширение* тела K_1. Тогда E есть правое векторное пространство размерности $2n$ над K_1 и v, рассматриваемое как линейное преобразование этого векторного пространства, есть *инволюция* в группе $GL_{2n}(K_1)$. Если характеристика тела K отлична от 2, то K имеет базис над K_1, состоящий из 1 и такого элемента ρ, что $\rho^2 \in K_1$, $\rho^\tau = -\rho$. Пространство E разлагается над K_1 в прямую сумму собственных подпространств V^+ и V^- преобразования v. Так как $v(x\rho) = -v(x)\rho$, то коллинеация $x \to x\rho$ отображает V^+ на V^-. Следовательно, пространства V^+ и V^- имеют одинаковую размерность, равную n, и базис $(e_i)_{1 \leqslant i \leqslant n}$ пространства V^+ над K_1 есть в то же время базис пространства E над K. В этом базисе $u(e_i) = e_i\lambda$ при $1 \leqslant i \leqslant n$.

Если K — тело характеристики 2, то оно имеет над K_1 базис, состоящий из 1 и такого элемента θ, что $\theta^2 + \theta = \beta \in K_1$ и $\theta^\tau = \theta + 1$. В этом случае $v(x) =$

[1]) Если σ — нетождественный автоморфизм тела K, то K_0 *не коммутативно*, даже если K коммутативно. Это с очевидностью показывает необходимость введения некоммутативных тел в теорию.

[2]) Доказательство существования тела K_0, данное на стр. 178—179 этой работы, годится при любой характеристике тела K, но если K имеет характеристику 2 и σ оставляет неподвижным каждый элемент центра тела K, то K_0 не будет расширением Галуа над K.

$= x + w(x)$, где $w(E) \subset w^{-1}(0) = V$, причем размерность p пространства $w(E)$ над K_1 не превосходит n. Легко проверяется, что $w(x\theta) = w(x)\theta + w(x) + x$; в частности, если $x \in V$, то $w(x\theta) = x$. Отсюда следует, что $w(E) = V$ и $p = n$. Так как отображение $x \to x\theta$ является коллинеацией, то размерность подпространства $V\theta$ (над K_1) равна размерности V, т. е. n. Поскольку $V \cap V\theta = \{0\}$, подпространства V и $V\theta$ дополнительны. Таким образом, базис $(e_i)_{1 \leqslant i \leqslant n}$ пространства V над K_1 есть в то же время базис пространства E над K, и в этом базисе $u(e_i) = e_i\lambda$ при $1 \leqslant i \leqslant n$. Мы получили тот же результат, что и в случае, когда характеристика тела K не равна 2.

§ 4. Централизатор проективной инволюции

Изучим *централизатор* $\bar{H}$ инволюции $\bar{u}$ в группе $P\Gamma L_n(K)$, т. е. группу проективных коллинеаций $\bar{v}$, перестановочных с $\bar{u}$. Это равносильно изучению подгруппы H элементов $v \in \Gamma L_n(K)$, соответствующих таким проективным коллинеациям $\bar{v}$. Коллинеации $v \in H$ характеризуются тем, что они *«проективно перестановочны»* с u, т. е. $v(u(x)) = u(v(x))a$, $a \in K$. Допуская некоторую вольность, мы будем записывать это так: $vu = uv \cdot a$. Пусть σ и τ — автоморфизмы тела K, соответствующие u и v. Заменяя в полученном выше соотношении x на $x\xi$, приходим к условию

$$\xi^{\sigma\tau} = a^{-1}\xi^{\tau\sigma}a \tag{3}$$

при всех $\xi \in K$ (мы полагаем, что $\xi^{\sigma\tau} = (\xi^\sigma)^\tau$). Если $u^2(x) = x\gamma$, то для γ имеются условия (1) и (2); кроме того, вычисляя двумя различными способами $u(v(u(x)))$, находим, что

$$\gamma^{-1}\gamma^\tau = a^\sigma a. \tag{4}$$

Заметим, что для решения нашей первоначальной задачи можно по желанию заменять u и v на $u \cdot \alpha$ и $v \cdot \beta$, где α и β — произвольные элементы из K^*; при этом a заменяется на $\alpha^{-1}\beta^{-\sigma}a\alpha^{\tau}\beta$ [1]) и γ — на $\gamma\alpha^{\sigma}\alpha$. В соответствии с § 3 мы будем различать несколько случаев (которые будут обозначаться так же, как и там).

A) γ *не представляется в виде* $\lambda\lambda^{\sigma}$, $\lambda \in K$. Если рассматривать E как векторное пространство размерности $n/2$ над телом K_0, то u будет гомотетией $x \to x\rho$. Соотношения (3) и (4) позволяют продолжить автоморфизм τ на тело K_0 таким образом, чтобы $\rho^{\tau} = \rho a$, и тогда условие $v(x\rho) = v(x)\rho a$ записывается в виде $v(x\rho) = v(x)\rho^{\tau}$. Это означает, что v есть коллинеация векторного пространства E над K_0 относительно автоморфизма τ. Обратно, для того чтобы такая коллинеация v принадлежала группе H, необходимо и достаточно выполнение следующих условий:

1) тело K инвариантно (в целом) относительно τ;
2) $\rho^{\tau} = \rho a$, где $a \in K$.

Таким образом, группа H — это подгруппа группы $\Gamma L_{n/2}(K_0)$, образованная такими коллинеациями, что соответствующий им автоморфизм τ тела K_0 удовлетворяет двум предыдущим условиям. Заметим, что во всяком случае H содержит в качестве нормального делителя *полную линейную группу* $GL_{n/2}(K_0)$.

B) $\gamma = \lambda\lambda^{\sigma}$, где $\lambda \in K^*$. Заменяя u на $u \cdot \lambda^{-1}$, мы сводим дело к случаю $\gamma = 1$, $\sigma^2 = 1$.

B1) Предположим, что σ — тождественный автоморфизм; тогда соотношение (4) приводит к тому, что $a^2 = 1$, т. е. $a = \pm 1$.

α) Пусть вначале характеристика тела K отлична от 2. Если $vu = uv$, то $v(U^+) = U^+$, $v(U^-) = U^-$, и обратно. Если $vu = -uv$, то $v(U^+) = U^-$, $v(U^-) = U^+$; это возможно, только если $n = 2p$ и u есть (p, p)-инволюция. Таким образом, индекс в группе H централизатора H_0 коллинеации u в $\Gamma L_n(K)$ равен 1 или 2, причем второй случай имеет место, лишь если u есть (p, p)-инволюция. Что касается группы H_0, то она изоморфна подгруппе прямого произведения $\Gamma L_p(K) \times \Gamma L_{n-p}(K)$

[1]) Здесь и дальше используется следующее обозначение: если σ_i — автоморфизмы тела K и m_i — целые числа, то $x^{\sum m_i\sigma_i} = \prod (x^{\sigma_i})^{m_i} = \prod (x^{m_i})^{\sigma_i}$ для любого $x \in K$. — *Прим. перев.*

(если u есть $(p, n-p)$-инволюция), образованной такими парами (v_1, v_2), что автоморфизмы тела K, соответствующие v_1 и v_2, совпадают. Группа $GL_p(K) \times \times GL_{n-p}(K)$ есть нормальный делитель в H_0.

β) Пусть теперь K — тело характеристики 2. Тогда $u(x) = x + w(x)$, где $w(E) \subset w^{-1}(0) = U$. Положим $p = = \dim(w(E))$. Централизатор H коллинеации u в группе $\Gamma L_n(K)$ совпадает с централизатором w. Следовательно, U и $w(E) = W$ инвариантны (в целом) относительно всякой коллинеации $v \in H$. Пусть H_0 — нормальный делитель в H, образованный элементами v, для которых полулинейное преобразование, индуцированное в E/U, тождественно. Элементы $v \in H_0$ являются *линейными* преобразованиями. Пусть U' — дополнительное подпространство к U. Для всякого $v \in H$ и $x \in U'$ имеем $v(x) = v_1(x) + v_2(x)$, где $v_1(x) \in U'$ и $v_2(x) \in U$. При $x \in U'$ должно выполняться равенство $w(v_1(x)) = = v(w(x))$. Следовательно, при данном v_1 коллинеация v однозначно определяется в $W = w(U')$ и может быть произвольно задана на векторах подпространства W', дополнительного к W в U (но так, чтобы W' отображалось в U). Отсюда немедленно вытекает, что факторгруппа H/H_0 изоморфна группе $\Gamma L_p(K)$. В группе H_0 можно выделить нормальный делитель H_1, образованный элементами v, оставляющими на месте каждый вектор подпространства U. Легко видеть, что группа H_1 изоморфна аддитивной группе $K^{p(n-p)}$. С другой стороны, поскольку элементы $v \in H_0$ характеризуются тем, что $v(x) = x$ для всех $x \in W$, в каждом классе смежности группы H_0 по H_1 имеется такой элемент v, что $v(x) = x$ для всех $x \in W + U'$. Отсюда следует, что факторгруппа H_0/H_1 изоморфна группе H_0', образованной ограничениями коллинеаций $v \in H_0$ на подпространстве U. В группе H_0' выделяется нормальный делитель H_2', образованный коллинеациями, тождественными на U по модулю W. Легко видеть, что факторгруппа H_0'/H_2' изоморфна группе $GL_{n-2p}(K)$, а группа H_2' изоморфна аддитивной группе $K^{p(n-2p)}$. Обозначим через H_2 полный прообраз группы H_2' в H. Тогда мы имеем следующий нормальный ряд для группы H:

$$H \supset H_0 \supset H_2 \supset H_1 \supset \{1\},$$

последовательные факторы которого изоморфны группам

$$\Gamma L_p(K),\ GL_{n-2p}(K),\ K^{p(n-2p)},\ K^{p(n-p)}.$$

B2) Предположим теперь, что σ — нетождественный автоморфизм, и пусть K_1 — подтело, образованное элементами тела K, инвариантными относительно σ. Из формулы (4) следует, что $a^\sigma a = 1$. Поле $Z(a)$, порожденное элементом a и центром Z тела K, инвариантно относительно автоморфизма σ. Если ограничение автоморфизма σ на $Z(a)$ тождественно, то $a^2 = 1$ и, значит, $a = \pm 1$. В противном случае, поскольку период автоморфизма σ равен 2, существует такой элемент $b \in Z(a)$, что $a = b^{1-\sigma}$; но тогда u и $v \cdot b^{-1}$ коммутируют. Таким образом, всегда можно считать, что $a = \pm 1$.

Условие (3) дает равенство $\xi^{\sigma\tau} = \xi^{\tau\sigma}$ для всех $\xi \in K$. Следовательно, подтело K_1 инвариантно относительно автоморфизма τ тела K.

α) Пусть характеристика тела K не равна 2. Подгруппа $H \subset \Gamma L_n(K)$, образованная такими коллинеациями v, что $vu = \pm uv$[1]), содержит в качестве нормального делителя индекса 2 централизатор H_0 коллинеации u. Мы ограничимся изучением группы H_0. Выше было показано, что пространство E, рассматриваемое как $2n$-мерное векторное пространство над K_1, есть прямая сумма n-мерных подпространств U^+ и U^-, причем $U^- = U^+\rho$. Условие $v \in H_0$ равносильно тому, что $v(U^+) = U^+$, $v(U^-) = U^-$. Ограничение коллинеации v на пространстве U^+ есть коллинеация этого пространства (над K_1). Так как $\rho^{\tau\sigma} = \rho^{\sigma\tau} = -\rho^\tau$, то $\rho^\tau = \rho\alpha$, где $\alpha \in K_1$. Положим $\xi^\omega = \rho^{-1}\xi\rho$ для всякого $\xi \in K_1$; тогда ω — автоморфизм тела K_1, и

$$\xi^{\tau\omega} = \alpha\xi^{\omega\tau}\alpha^{-1}. \tag{5}$$

Кроме того, если $\rho^2 = \beta \in K_1$, то должно быть $\beta^\tau = (\rho^\tau)^2 = \rho\alpha\rho\alpha$, откуда

$$\beta^{-1}\beta^\tau = \alpha^\omega\alpha. \tag{6}$$

---

[1]) Эта подгруппа не совпадает с подгруппой H, определенной в начале этого параграфа; однако ее образ в группе $P\Gamma L_n(K)$ совпадает с $\bar{H}$. — *Прим. перев.*

Обратно, если τ — автоморфизм тела K_1, удовлетворяющий условиям (5) и (6) для некоторого $\alpha \in K_1$, то его можно продолжить до автоморфизма тела K, полагая $\rho^\tau = \rho\alpha$, и всякая коллинеация v пространства U^+ (над K) относительно автоморфизма τ продолжается до коллинеации пространства E (над K). Для этого надо положить $v(x\rho) = v(x)\rho^\tau$. Так как тогда $v(U^-) = U^-$, то $v \in H_0$. Таким образом, группа H_0 изоморфна подгруппе группы $\Gamma L_n(K_1)$, образованной коллинеациями относительно автоморфизмов τ тела K_1, удовлетворяющих условиям (5) и (6) (для некоторого α, зависящего от τ). Заметим, что *полная линейная группа* $GL_n(K_1)$ есть нормальный делитель группы H_0 (и группы H).

β) Пусть теперь K — тело характеристики 2. Выше было показано, что пространство E, рассматриваемое как $2n$-мерное векторное пространство над K_1, есть прямая сумма подпространств $V = w^{-1}(0)$ и $V\theta$, где $\theta^2 + \theta = \beta \in K_1$ и $\theta^\sigma = \theta + 1$. Кроме того (Дьёдонне [14], стр. 181), отображение $\xi \to D\xi = \theta\xi + \xi\theta$ есть дифференцирование тела K_1. Для того чтобы коллинеация v принадлежала H, необходимо и достаточно, чтобы $vw = wv$. В частности, $v(w(x)) = w(v(x))$ при $x \in V$, откуда $v(V) = V$. С другой стороны, $\theta^{\tau\sigma} = \theta^{\sigma\tau} = \theta^\tau + 1$, откуда $\theta^\tau = \theta + \lambda$, $\lambda \in K_1$. Принимая во внимание, что $w(x\theta) = x$ при $x \in V$, легко проверить, что если $v(V) = V$ и $\theta^\tau = \theta + \lambda$ $(\lambda \in K_1)$, то $v(w(x\theta)) = w(v(x\theta))$ при $x \in V$ и, значит, v и w коммутируют. Заметим теперь, что если применить к равенству $D\xi = \theta\xi + \xi\theta$ автоморфизм τ, то получится, что

$$(D\xi)^\tau - D(\xi^\tau) = \lambda\xi^\tau + \xi^\tau\lambda. \tag{7}$$

С другой стороны,

$$\beta^\tau - \beta = \lambda^2 + \lambda. \tag{8}$$

Обратно, если τ — автоморфизм тела K_1, удовлетворяющий условиям (7) и (8) для некоторого $\lambda \in K_1$, то его можно продолжить до автоморфизма тела K, полагая $\theta^\tau = \theta + \lambda$, и всякая коллинеация v пространства V (над K_1) относительно автоморфизма τ продолжается до коллинеации пространства E (над K) таким образом, что $v(x\theta) = v(x)\theta^\tau$. Следовательно, группа H

изоморфна подгруппе группы $\Gamma L_n(K_1)$, образованной коллинеациями относительно автоморфизмов τ тела K_1, удовлетворяющих условиям (7) и (8) (для некоторого λ, зависящего от τ). *Полная линейная группа* $GL_n(K_1)$ является нормальным делителем в группе H.

Что касается изучения централизатора в группе $GL_n(K)$ произвольного линейного преобразования, мы ограничимся ссылкой на работы Шрейера и Ван-дер-Вардена [1] и Дьёдонне [3], где это проделано при некоторых ограничениях на тело K.

§ 5. Корреляции и полуторалинейные формы

Известно, что *сопряженное пространство* E^* к правому векторному пространству E над телом K есть *левое* векторное пространство над K той же размерности, что и E. Как обычно, мы будем употреблять обозначение $\langle x', x\rangle$ вместо $x'(x)$ при $x \in E$ и $x' \in E^*$. Пространство E^* можно рассматривать также как правое векторное пространство над телом K°, *противоположным* телу K. Полулинейное отображение E в E^* может существовать только в том случае, когда тела K и K° изоморфны, т. е. существует такое биективное отображение J тела K на себя, что $(\alpha+\beta)^J = \alpha^J + \beta^J$ и $(\alpha\beta)^J = \beta^J\alpha^J$; такое отображение называется *антиавтоморфизмом* тела K. Заметим, что если K коммутативно, то антиавтоморфизм — это то же самое, что автоморфизм. Отображение φ пространства E в пространство E^* будет полулинейным отображением относительно антиавтоморфизма J тела K, если

$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \text{при} \quad x \in E,\ y \in E,$$

$$\varphi(x\lambda) = \lambda^J\varphi(x) \quad \text{при} \quad x \in E,\ \lambda \in K.$$

Каждому такому полулинейному отображению φ поставим в соответствие отображение $(x, y) \to f(x, y) = \langle\varphi(x), y\rangle$ прямого произведения $E \times E$ в K. Отображение f, очевидно, обладает следующими свойствами:

$$f(x_1+x_2,\ y)=f(x_1,\ y)+f(x_2,\ y),$$
$$f(x,\ y_1+y_2)=f(x,\ y_1)+f(x,\ y_2),$$
$$f(x\lambda,\ y)=\lambda^J f(x,\ y),$$
$$f(x,\ y\lambda)=f(x,\ y)\lambda.$$

Такое отображение будет называться *полуторалинейной формой* на $E\times E$ относительно антиавтоморфизма J. Если K коммутативно и J — тождественный автоморфизм, то f — это обычная *билинейная форма* на $E\times E$.

Обратно, очевидно, что всякая полуторалинейная форма на $E\times E$ однозначно представляется в виде $\langle\varphi(x),\ y\rangle$, где φ — полулинейное отображение пространства E в E^*. Пусть $(e_i)_{1\leqslant i\leqslant n}$ — базис пространства E и $(e'_i)_{1\leqslant i\leqslant n}$ — дуальный базис пространства E^*, такой, что $\langle e'_i,\ e_j\rangle=\delta_{ij}$. Если $\varphi(e_i)=\sum\limits_{j=1}^{n}\alpha_{ij}e'_j$, то $\alpha_{ij}=\langle\varphi(e_i),\ e_j\rangle=f(e_i,\ e_j)$, и для $x=\sum\limits_i e_i\xi_i$, $y=\sum\limits_i e_i\eta_i$ имеем $f(x,\ y)=\sum\limits_{i,j}\xi_i^J\alpha_{ij}\eta_j={}^tx^JAy$, где x и y отождествлены со столбцами своих координат и $A=(\alpha_{ij})$. Матрица A, являющаяся матрицей отображения φ по отношению к базисам (e_i) и (e'_i)[1]), называется также *матрицей* полуторалинейной формы f в базисе (e_i) пространства E. Ее ранг, не зависящий от выбора базиса (e_i) и совпадающий с рангом отображения φ, называется *рангом* полуторалинейной формы f.

Если $(\bar e_i)_{1\leqslant i\leqslant n}$ — другой базис пространства E, P — матрица перехода от (e_i) к $(\bar e_i)$ и A' — матрица формы f в базисе $(\bar e_i)$, то $A'={}^tP^JAP$. В случае, когда K коммутативно, определитель Δ матрицы A называется *дискриминантом* формы f в базисе (e_i). Если Δ' — дискриминант f в базисе $(\bar e_i)$, то $\Delta'=(\delta\delta^J)\Delta$, где $\delta=\det P$.

---

[1]) При том определении матрицы полулинейного отображения, которое было дано в § 1, матрицей отображения φ будет матрица, транспонированная к A. — *Прим. перев.*

Корреляцией пространства E на E^* называется биективное полулинейное отображение E на E^* или, что то же самое, полулинейное отображение, ранг которого равен размерности пространства E. Полуторалинейная форма f на $E \times E$, соответствующая корреляции φ, называется *невырожденной*. Такая форма характеризуется следующим свойством: всякий вектор $x \in E$, для которого $f(x, y) = 0$ при всех $y \in E$, равен 0.

§ 6. Рефлексивные полуторалинейные формы

В дальнейшем, если не будет оговорено противное, мы будем рассматривать только *невырожденные* полуторалинейные формы на $E \times E$ (относительно антиавтоморфизмов тела K). Два вектора x, y пространства E, взятые в данном порядке, называются *ортогональными* в смысле (или относительно) формы f, если $f(x, y) = 0$. Невырожденность формы f означает, что не существует вектора $x \neq 0$, такого, что x и y ортогональны для *любого* $y \in E$. Мы будем говорить, что форма f (или соответствующая корреляция φ) *рефлексивна*, если отношение ортогональности симметрично, т. е. $f(x, y) = 0$ эквивалентно $f(y, x) = 0$. Ниже будут описаны (при $n \geqslant 2$) все рефлексивные полуторалинейные формы (Биркгоф и фон Нейман [1]).

Прежде всего можно ограничиться рассмотрением только *невырожденных* рефлексивных форм. В самом деле, если f рефлексивна и вырожденна, то множество векторов x, ортогональных ко всем векторам из E, является подпространством N пространства E. Если $x \equiv x_1 \pmod N$ и $y \equiv y_1 \pmod N$, то $f(x, y) = f(x_1, y_1)$; следовательно, форма f определяет полуторалинейную форму на факторпространстве E/N (называемую формой, *ассоциированной* с f). Эта форма рефлексивна и *невырожденна*, и она полностью определяет форму f.

Если J — антиавтоморфизм, соответствующий форме f, то предположение о рефлексивности означает, что для всякого вектора $x \neq 0$ пространства E линейные уравнения $f(x, y) = 0$ и $(f(y, x))^{J^{-1}} = 0$ задают одну и ту же гиперплоскость и, значит, $f(y, x) = (f(x, y))^J m(x)$, где $m(x)$ — скаляр, зависящий только от x. Если x_1 и x_2

линейно независимы, то из предыдущего соотношения вытекает, что $m(x_1+x_2)=m(x_1)=m(x_2)$. Следовательно, $f(y, x)=(f(x, y))^J r^{-1}$, где r — скаляр, отличный от 0 и не зависящий от x и y.

Далее, вычисляя двумя способами $(f(y, x))^J$ и учитывая, что $f(x, y)$ может быть произвольным элементом тела K, получаем, что

$$\xi^{J^2}=r^J\xi r \quad \text{для всех} \quad \xi\in K; \tag{9}$$

в частности,

$$rr^J=1. \tag{10}$$

Теперь рассмотрим отдельно два случая:

1) $\xi+\xi^J r^J=0$ для всех $\xi\in K$. Полагая $\xi=1$, находим $r=-1$, откуда $\xi^J=\xi$ при всех ξ. Это возможно, только если тело K *коммутативно* и J есть его *тождественный* автоморфизм. Таким образом, в этом случае

$$f(y, x)=-f(x, y); \tag{11}$$

такая форма f называется *кососимметричной* билинейной формой.

2) Существует такой элемент $\zeta\in K$, что $\zeta+\zeta^J r^J = q\neq 0$. Легко видеть, что $r=q^{-1}q^J$. Положим $\xi^T = (q^{-1}\xi q)^J$ и $g(x, y)=q^J f(x, y)$; тогда

$$\xi^{T^2}=\xi \quad \text{для всех} \quad \xi\in K \tag{12}$$

и

$$g(y, x)=g(x, y)^T. \tag{13}$$

Антиавтоморфизм T, удовлетворяющий условию (12), называется *инволюцией* тела K, а полуторалинейная форма g со свойством (13) называется *эрмитовой* относительно инволюции T. Если тело K коммутативно и T — его тождественный автоморфизм, то соотношение (13) превращается в равенство

$$g(y, x)=g(x, y); \tag{14}$$

в этом случае форма g называется *симметричной* билинейной формой. Если T — нетождественная инволюция, то элементы $\alpha\in K^*$, для которых $\alpha^T=\alpha$, называются *симметричными* относительно T, а элементы, для которых

$\alpha^T = -\alpha$ (такие всегда существуют в силу сделанного предположения) — *кососимметричными*. Если α — симметричный (соответственно кососимметричный) относительно T элемент, то, полагая $\xi^S = \alpha\xi^T\alpha^{-1}$ и $h(x, y) = \alpha g(x, y)$, мы получаем инволюцию S тела K и полуторалинейную форму h относительно инволюции S, удовлетворяющую условию

$$\begin{aligned} &h(y, x) = (h(x, y))^S, && \text{если } \alpha \text{ симметричен,} \\ &h(y, x) = -(h(x, y))^S, && \text{если } \alpha \text{ кососимметричен.} \end{aligned} \tag{15}$$

Во втором случае форма h называется *косоэрмитовой* относительно инволюции S.

Для того чтобы полуторалинейная форма f была эрмитовой (соответственно косоэрмитовой), необходимо и достаточно, чтобы ее матрица A в произвольном базисе пространства E удовлетворяла условию ${}^tA = A^J$ (соответственно ${}^tA = -A^J$).

Это условие может быть выражено другим способом. Если u — полулинейное относительно изоморфизма σ отображение векторного пространства E в векторное пространство F, то отображение $x \to (\langle y', u(x)\rangle)^{\sigma^{-1}}$ будет линейной формой на E для любого элемента y' пространства F^*, сопряженного к F. Следовательно,

$$\langle y', u(x)\rangle = \langle {}^tu(y'), x\rangle^\sigma, \tag{16}$$

где ${}^tu$ — полулинейное отображение F^* в E^* относительно изоморфизма σ^{-1}. Отображение ${}^tu$ называется *транспонированным* к u. В частности, для корреляции φ пространства E на пространство E^* относительно антиавтоморфизма J отображение ${}^t\varphi$ будет корреляцией пространства E на пространство E^* относительно антиавтоморфизма J^{-1}; при этом

$$\langle \varphi(x), y\rangle = \langle {}^t\varphi(y), x\rangle^J. \tag{17}$$

Эрмитовость (соответственно *косоэрмитовость*) полуторалинейной формы f, соответствующей корреляции φ, означает, что ${}^t\varphi = \varphi$ (соответственно ${}^t\varphi = -\varphi$).

Мы доказали, что, умножая произвольную рефлексивную форму на скаляр, можно добиться того, чтобы она стала эрмитовой или косоэрмитовой. Отныне мы будем рассматривать *исключительно* такие формы, и когда мы будем говорить о рефлексивной форме, это всегда будет означать, что она эрмитова или косоэрмитова (и в обоих случаях, что J — инволюция).

§ 7. Ортогональные дополнения и изотропные подпространства

Пусть f — (невырожденная) рефлексивная форма на n-мерном пространстве E. Для всякого подпространства V пространства E множество V^0 всех векторов пространства E, ортогональных ко всем векторам из V, является подпространством в E; оно называется *ортогональным дополнением* к V. В свою очередь V есть ортогональное дополнение к V^0. Если $\dim V = p$, то $\dim V^0 = n - p$. Имеем $(V + W)^0 = V^0 \cap W^0$, $(V \cap W)^0 = V^0 + W^0$ для любых подпространств V, W. Говорят, что подпространство V *изотропно*, если $V \cap V^0 \neq \{0\}$; в этом случае V^0 также изотропно. Это условие эквивалентно тому, что ограничение формы f на $V \times V$ *вырожденно*. Говорят, что подпространство V *вполне изотропно*, если $V \subset V^0$; это эквивалентно тому, что ограничение формы f на $V \times V$ *тождественно равно* 0 (или что любые два вектора из V ортогональны). В этом случае $p \leqslant n - p$, т. е. $2p \leqslant n$. *Индексом* формы f называется *наибольшая размерность* ν вполне изотропных подпространств пространства E; из предыдущего ясно, что $2\nu \leqslant n$. Для любого изотропного подпространства V подпространство $V \cap V^0$ вполне изотропно. Заметим также, что если V — вполне изотропное подпространство и W — вполне изотропное подпространство, содержащееся в V^0, то $V + W$ также вполне изотропно. Отсюда следует, что если $\dim V = \nu$, то всякое вполне изотропное подпространство, содержащееся в V^0, содержится в V.

Неизотропное подпространство V пространства E характеризуется тем свойством, что V^0 является дополнительным подпространством к V. Форма f называется *анизотропной*, если $\nu = 0$.

Вектор $x \neq 0$ называется *изотропным*, если $f(x, x) = 0$ (иначе говоря, если он ортогонален самому себе). Очевидно, что все векторы вполне изотропного подпространства изотропны. Обратно, предположим, что $f(x, x) = 0$ для *всякого* вектора x, принадлежащего подпространству V. Из равенства $f(x+y, x+y) = 0$ при $x \in V$, $y \in V$ следует, что $f(x, y) = \varepsilon(f(x, y))^J$, где $\varepsilon = -1$, если форма f эрмитова, и $\varepsilon = 1$, если форма f косоэрмитова. Если пространство V не вполне изотропно, то, заменяя y на $y\xi$, получаем, что $\xi^J = \lambda\xi\lambda^{-1}$ для некоторого $\lambda \neq 0$ и любого $\xi \in K$. Это возможно, только если K *коммутативно* и J — *тождественный автоморфизм*. Очевидно, что тогда форма f *кососимметрична*. В частности, если $f(x, x) = 0$ для всех векторов $x \in E$, то форма f называется *знакопеременной*. Всякая знакопеременная форма кососимметрична. Обратно, если K — поле *характеристики, не равной* 2, то всякая кососимметричная форма на $E \times E$ знакопеременна.

§ 8. Эквивалентиость рефлексивных полуторалинейных форм

Пусть E и F — два n-мерных векторых пространства над K и u — изоморфизм пространства F на E. Если f — полуторалинейная форма на $E \times E$ (не обязательно невырожденная или рефлексивная), то отображение $(x, y) \to f(u(x), u(y))$ будет полуторалинейной формой на $F \times F$ (относительно того же антиавтоморфизма тела K); говорят, что эта форма f_1 получается *перенесением* формы f посредством изоморфизма u. Если A — матрица формы f в базисе $(e_i)_{1 \leqslant i \leqslant n}$ пространства E, то A будет также матрицей формы f_1 в базисе пространства F, образованном векторами $u^{-1}(e_i)$ $(1 \leqslant i \leqslant n)$. В любом другом базисе пространства F матрица формы f_1 имеет, следовательно, вид ${}^tU^JAU$, где U — обратимая квадратная матрица.

Говорят, что полуторалинейная форма f на $E \times E$ и полуторалинейная форма f_1 на $F \times F$ *эквивалентны*, если f_1 получается из f перенесением посредством изоморфизма u пространства F на пространство E; тогда f получается из f_1 перенесением посредством изоморфизма u^{-1}. Если A и A_1 — матрицы форм f и f_1 в каких-то базисах пространств E и F соответственно, то эквивалентность форм f и f_1 равносильна существованию такой обратимой квадратной матрицы U, что $A_1={}^tU^JAU$. Можно также сформулировать условие эквивалентности форм f и f_1 как существование базисов пространств E и F соответственно, в которых матрицы форм f и f_1 одинаковы.

Проблема нахождения условий, при которых две полуторалинейные формы на $E\times E$ эквивалентны, за исключением одной работы Жордана ([3], т. III, мемуар 69, см. также комментарии к этому тому, стр. XI), рассматривалась только для рефлексивных форм[1]). Резюмируем кратко основные полученные результаты.

Прежде всего две эквивалентные формы должны иметь одинаковый ранг. Легко также установить, что две вырожденные рефлексивные формы эквивалентны тогда и только тогда, когда эквивалентны ассоциированные невырожденные формы (см. § 6). Таким образом, можно ограничиться рассмотрением невырожденных рефлексивных форм.

Проблема эквивалентности полностью решена лишь для *знакопеременных* форм (над коммутативным телом K). Такая форма f может быть невырожденной, только если пространство E имеет *четную* размерность $2m$. В этом случае можно показать, что в пространстве E существует такой базис (называемый *симплектическим базисом* для формы f), что

$$f(e_i, e_j)=0, \quad \text{если} \quad j\neq i+m \quad \text{и} \quad i\neq j+m,$$
$$f(e_i, e_{i+m})=-f(e_{i+m}, e_i)=1 \quad \text{для} \quad 1\leqslant i\leqslant m.$$

(В § 11 будет доказано более общее утверждение.) Таким образом, две знакопеременные формы на $E\times E$, имеющие одинаковый ранг, всегда эквивалентны.

Для прочих рефлексивных форм над произвольным телом известны лишь некоторые необходимые условия эквивалентности. Первое такое условие состоит в равенстве индексов (см. § 7; более точное необходимое

[1]) Автор не совсем прав. См., например, Ходж и Пидо [1*]. — *Прим. перев.*

условие будет найдено в § 11). Во-вторых, если тело K коммутативно, дискриминанты двух эквивалентных форм (см. § 5) должны принадлежать к одному классу мультипликативной группы K^* по модулю подгруппы «норм» $\lambda\lambda^J$.

Если рефлексивная форма f не кососимметрична, то в пространстве E существует *ортогональный базис* для формы f, т. е. такой базис $(e_i)_{1 \leqslant i \leqslant n}$, что

$$f(e_i, e_j) = 0 \quad \text{при} \quad i \neq j.$$

Кроме того, полагая $f(e_i, e_i) = \gamma_i$, получаем, что $\gamma_i^J = \gamma_i$, если форма f эрмитова, и $\gamma_i^J = -\gamma_i$, если форма f косоэрмитова. Доказательство существования такого базиса можно провести индукцией по n: в пространстве E существует неизотропный вектор e_1; гиперплоскость H, ортогональная к e_1, не изотропна и дополнительна к e_1K; так как форма f не кососимметрична, то по предположению индукции существует ортогональный базис для ограничения формы f на H, откуда и вытекает доказываемое утверждение.

Единственный случай, оставшийся в стороне, — случай симметричных, но не знакопеременных форм над телом характеристики 2 — будет рассмотрен в § 10.

Существование ортогональных базисов позволяет в некоторых случаях решить проблему эквивалентности. Например, если K — *алгебраически замкнутое* поле и f — невырожденная симметричная форма на $E \times E$, то существует такой ортогональный базис (e_i) пространства E, что $f(e_i, e_i) = 1$ при $1 \leqslant i \leqslant n$ (такой базис называется *ортонормированным*). Таким образом, в этом случае две симметричные формы одинакового ранга всегда эквивалентны. Если K — *евклидово упорядоченное* поле (т. е. из каждого неотрицательного элемента извлекается квадратный корень) и f — невырожденная симметричная форма на $E \times E$, то существует такой ортогональный базис (e_i) пространства E, что $f(e_i, e_i) = 1$ при $1 \leqslant i \leqslant p$ и $f(e_i, e_i) = -1$ при $p + 1 \leqslant i \leqslant n$. Кроме того, если K — произвольное упорядоченное поле, то при любом ортогональном базисе (e_i) пространства E для невырожденной симметричной формы f число p

таких индексов i, что $\gamma_i = f(e_i, e_i) > 0$, одно и то же (*закон инерции Сильвестра*). Пара $(p, n-p)$ называется в этом случае *сигнатурой* формы f, а число $n-p$ — ее *индексом инерции.* Две эквивалентные формы должны иметь одинаковую сигнатуру; над евклидовым полем это необходимое условие эквивалентности является также и достаточным. В § 11 будет показано, что для упорядоченного поля K всегда имеет место неравенство $\nu \leqslant \mathrm{Min}(p, n-p)$; в случае евклидова поля K оно превращается в равенство.

Если K — *конечное* поле $\mathbf{F}_q$ из q элементов характеристики $\neq 2$, то для всякой симметричной формы f существует такой ортогональный базис (e_i), что $f(e_i, e_i) = 1$ при $1 \leqslant i \leqslant n-1$ и либо $f(e_n, e_n) = 1$, либо $f(e_n, e_n) = \delta$, где δ — элемент, не являющийся квадратом в поле $\mathbf{F}_q$ (известно, что квадраты образуют в мультипликативной группе $\mathbf{F}_q^*$ подгруппу индекса 2; см. Диксон [1], стр. 158). Таким образом, над полем $\mathbf{F}_q$ имеется два класса эквивалентных симметричных форм ранга n. Для форм первого класса дискриминант Δ (относительно произвольного базиса) есть квадрат в поле $\mathbf{F}_q$; для форм второго класса он не является квадратом. Если $n = 2m + 1$ нечетно, то всякая форма второго класса получается из формы первого класса умножением на δ; в этом случае индекс всякой симметричной формы равен $m = [n/2]$. В случае когда $n = 2m$ четно, индекс равен $m = n/2$, если $(-1)^m\Delta$ есть квадрат в $\mathbf{F}_q$, и $m-1$ в противном случае.

Для *поля алгебраических чисел* проблема эквивалентности симметричных форм полностью решена Минковским в [1] и Хассе в [2]. Современная теория симметричных форм над таким полем тесно связана с изучением алгебр Клиффорда (гл. II, § 7). Эта теория и ее обобщения изложены, например, в работе Витта [1] и в книге Эйхлера [2], к которым мы и отсылаем читателя [1]).

Пусть K_0 — *упорядоченное* поле, $K = K_0(\sqrt{-1})$ — квадратичное расширение и J есть K_0-автоморфизм поля K, отличный от тождественного, такой что K_0 есть

---

1) См. также книгу О'Мира [7*]. — *Прим. перев.*

множество элементов, *симметричных* относительно J. Если f — эрмитова форма на $E \times E$ и (e_i) — ортогональный базис пространства E относительно формы f, то число таких индексов i, что $\gamma_i = f(e_i, e_i) > 0$, не зависит от выбора ортогонального базиса (*закон инерции*). Этот результат справедлив также, если K — *обобщенное тело кватернионов* над K_0 и J — его единственная инволюция, множество инвариантных элементов которой совпадает с K_0. Если, кроме того, K_0 — евклидово поле (а K — либо его квадратичное расширение, либо тело кватернионов над K_0), то необходимое и достаточное условие эквивалентности двух *эрмитовых* форм над K состоит в том, чтобы они имели одинаковую сигнатуру. Укажем также, что если K_0 — евклидово поле, а K — тело кватернионов над K_0, то для всякой *косоэрмитовой* формы f на $E \times E$ существует такой ортогональный базис (e_i), что $f(e_i, e_i) = j$ при $1 \leqslant i \leqslant n$, где j — фиксированный кватернион, квадрат которого равен -1. Таким образом, в этом случае две косоэрмитовы формы одного ранга всегда эквивалентны (Дьёдонне [13], стр. 383).

Предположим теперь, что K_0 — произвольное конечное поле $\mathbf{F}_q$, K — его квадратичное расширение $\mathbf{F}_{q^2}$ и J — единственный K_0-автоморфизм $\xi \to \xi^q$ поля K, отличный от тождественного. Тогда для любой эрмитовой формы на $E \times E$ существует *ортонормированный* базис; иначе говоря, две эрмитовы формы одинакового ранга всегда эквивалентны и, следовательно, все эрмитовы формы имеют максимальный возможный индекс $[n/2]$. Это немедленно вытекает из того факта, что каждый элемент поля K_0 является нормой некоторого элемента из K.

Заметим, наконец, что проблема эквивалентности эрмитовых форм над полем алгебраических чисел, а также эрмитовых или косоэрмитовых форм над телом, центром которого служит поле алгебраических чисел, была решена Ландгером [1], [2], Раманатаном [1], Цукамото [1] и Сатаке [1] [1]).

---

[1]) См. также Джекобсон [4*], Шимура [1*], Якобовиц [1]. — *Прим. перев.*

§ 9. Унитарные группы

Пусть f — (невырожденная) рефлексивная форма на $E \times E$, соответствующая инволюции J тела K. Биективные линейные отображения u пространства E на себя, для которых форма f равна своему перенесению посредством u (см. § 8), т. е.

$$f(u(x),\ u(y)) = f(x,\ y) \quad \text{при} \quad x \in E,\ y \in E, \tag{18}$$

называются *унитарными преобразованиями* пространства E относительно формы f. Они образуют подгруппу в группе $GL_n(K)$, которую мы будем обозначать через $U_n(K, f)$ и которая называется *унитарной группой* от n переменных над телом K относительно формы f.

Соотношение (18) может быть записано другим способом. Если φ — корреляция, ассоциированная с формой f, и $\check{u} = {}^t u^{-1}$ — преобразование, *контраградиентное* к u, то соотношение (18) эквивалентно тому, что

$$\langle \varphi(u(x)),\ u(y) \rangle = \langle \varphi(x),\ y \rangle = \langle \check{u}(\varphi(x)),\ u(y) \rangle,$$

и, поскольку $u(y)$ пробегает вместе с y все пространство E, это в свою очередь эквивалентно равенству

$$\varphi(u(x)) = \check{u}(\varphi(x)) \quad \text{для всех} \quad x \in E.$$

Более общо, пусть u — коллинеация пространства E относительно автоморфизма тела K, который мы будем обозначать через σ или σ_u. Мы будем говорить, что корреляция φ и коллинеация u *проективно перестановочны*, если существует такой скаляр r_u, что

$$\varphi(u(x)) = r_u \check{u}(\varphi(x)) \quad \text{для всех} \quad x \in E, \tag{19}$$

где по-прежнему $\check{u} = {}^t u^{-1}$ — коллинеация пространства E^*, *контраградиентная* к u (и соответствующая тому же автоморфизму σ тела K, что и u). Это соотношение эквивалентно тому, что

$$\langle \varphi(u(x)),\ u(y) \rangle = \langle r_u \check{u}(\varphi(x)),\ u(y) \rangle$$

для всех $x \in E$, $y \in E$. В силу формулы (16) это в свою очередь эквивалентно равенству

$$f(u(x),\ u(y)) = r_u (f(x,\ y))^{\sigma}. \tag{20}$$

Для того чтобы коллинеация u удовлетворяла условию этого типа, необходимо и достаточно (при $n \geqslant 2$), чтобы она переводила *ортогональные векторы в ортогональные*. В самом деле, если это свойство имеет место, то для данного $y \in F$ существует такой скаляр m_y, что при любом $x \in E$

$$\langle \varphi(u(x)), u(y) \rangle = m_y \langle \varphi(x), y \rangle^\sigma.$$

Как и в § 6, рассматривая линейно независимые элементы y_1 и y_2, находим, что $m_{y_1+y_2} = m_{y_1} = m_{y_2}$, откуда вытекает соотношение (20).

Заметим, что если в (19) заменить x на $x\xi$, то получится, что

$$\xi^{\sigma J} = r_u \xi^{J\sigma} r_u^{-1} \quad \text{для любого} \quad \xi \in K. \tag{21}$$

Переставляя в (20) x и y и учитывая, что форма f эрмитова или косоэрмитова, находим, что

$$r_u^J = r_u. \tag{22}$$

Мы будем говорить, что коллинеация u, удовлетворяющая условию (20), есть *унитарное полуподобие* (относительно формы f), соответствующее автоморфизму σ_u и *множителю* r_u. Если (e_i) — произвольный базис пространства E, то условие (20) равносильно тому, что

$$f(u(e_i), u(e_j)) = r_u (f(e_i, e_j))^\sigma.$$

Это означает, что матрица U коллинеации u в этом базисе удовлетворяет условию

$${}^tU^J A U = r_u A^\sigma, \tag{23}$$

где A — матрица формы f в этом базисе. Очевидно, что полуподобия (относительно формы f) образуют подгруппу $\Gamma U_n(K, f)$ группы $\Gamma L_n(K)$. Полуподобие, соответствующее тождественному автоморфизму (иначе говоря, линейное), называется также *унитарным подобием* (относительно формы f). Такие преобразования образуют нормальный делитель $GU_n(K, f) = \Gamma U_n(K, f) \cap \cap GL_n(K)$ в группе $\Gamma U_n(K, f)$. *Унитарная группа* $U_n(K, f)$ является нормальным делителем в группе $GU_n(K, f)$, состоящим из подобий с множителем 1, называемых также *унитарными преобразованиями*. Если A — матрица формы f в каком-то базисе пространства E, то вместо $U_n(K, f)$ пишут также $U_n(K, A)$ и аналогично для остальных групп.

Отображение $u \to \sigma_u$ является гомоморфизмом группы $\Gamma U_n(K, f)$ на некоторую подгруппу группы автоморфизмов тела K. Об этой подгруппе в общем случае ничего не известно, кроме того, что она содержит группу внутренних автоморфизмов тела K. Ядром гомоморфизма $u \to \sigma_u$ является группа $GU_n(K, f)$. Для $u \in GU_n(K, f)$ соотношение (21) показывает, что множитель r_u должен лежать в *центре* Z тела K, а из (22) следует, что, кроме того, r_u принадлежит подполю Z_0 поля Z, образованному элементами, инвариантными относительно инволюции J (либо это подполе совпадает с Z, либо Z является его сепарабельным квадратичным расширением). Отображение $u \to r_u$ является гомоморфизмом группы $GU_n(K, f)$ на (абелеву) подгруппу $M(f)$ группы Z_0^*. В общем случае об этой подгруппе известно очень мало (см. гл. II, § 13). Ядром гомоморфизма $u \to r_u$ является унитарная группа $U_n(K, f)$.

Мы будем обозначать через $P\Gamma U_n(K, f)$, $PGU_n(K, f)$, $PU_n(K, f)$ образы групп $\Gamma U_n(K, f)$, $GU_n(K, f)$, $U_n(K, f)$ при каноническом гомоморфизме группы $\Gamma L_n(K)$ на проективную группу $P\Gamma L_n(K)$. Очевидно, что всякая гомотетия $x \to x\lambda$ является унитарным полуподобием с множителем $\lambda^J\lambda$. Отсюда следует, что $P\Gamma U_n \simeq \Gamma U_n/H_n$. Всякая центральная гомотетия является унитарным подобием и, значит, $PGU_n \simeq GU_n/Z_n$. Наконец, $PU_n \simeq U_n/U_1$, где $U_1 = U_n \cap Z_n$ — подгруппа, образованная центральными гомотетиями $x \to x\gamma$, для которых $\gamma^J\gamma = 1$. Позже мы увидим (гл. II, § 3), что группа U_1, как правило, совпадает с центром группы U_n.

Если рефлексивная форма f_1 на $E \times E$ получается перенесением формы f посредством биективного линейного отображения v, то группа $\Gamma U_n(K, f_1)$ (соответственно $GU_n(K, f_1)$, $U_n(K, f_1)$) получается из группы $\Gamma U_n(K, f)$ (соответственно $GU_n(K, f)$, $U_n(K, f)$) при помощи внутреннего автоморфизма $s \to v^{-1}sv$ группы $\Gamma L_n(K)$. С другой стороны, если α — симметричный или кососимметричный (относительно J) элемент тела K, то

$\Gamma U_n(K, \alpha f) = \Gamma U_n(K, f)$, $GU_n(K, \alpha f) = GU_n(K, f)$ и $U_n(K, \alpha f) = U_n(K, f)$.

Если тело K коммутативно и f — *знакопеременная* форма, то прилагательное «унитарный» повсюду в предыдущих определениях заменяют на прилагательное «*симплектический*». Так как две знакопеременные формы одинакового (четного) ранга n эквивалентны, то соответствующие группы обозначают просто через $\Gamma Sp_n(K)$, $GSp_n(K)$ и $Sp_n(K)$, не указывая формы f. (Аналогичные обозначения используются для проективных групп.) Вообще, форма f опускается в обозначении унитарной группы всегда, когда две формы одинакового ранга эквивалентны (в частности, когда $J \neq 1$ и K — конечное поле).

Если K — поле *характеристики* $\neq 2$ и f — *симметричная* форма, то прилагательное «унитарный» заменяют повсюду на «*ортогональный*» и соответствующие группы обозначают через $\Gamma O_n(K, f)$, $GO_n(K, f)$ и $O_n(K, f)$ (и соответствующим образом обозначаются проективные группы). Для полей характеристики 2 определение ортогональных групп совершенно иное и будет дано в § 16.

§ 10. *T*-формы

Пусть f — *эрмитова* форма на $E \times E$; мы будем говорить, что f есть *T-форма*, если для всякого $x \in E$ элемент $f(x, x)$ есть «след» в K, т. е. представляется в виде $\lambda + \lambda^J$ для некоторого $\lambda \in K$. Так как элемент $\gamma = f(x, x)$ симметричен, то это условие всегда выполняется, если *характеристика поля K отлична от* 2; в самом деле, в этом случае достаточно взять $\lambda = \gamma/2$. Это условие выполняется также, если характеристика поля K равна 2, но подполе Z_0 симметричных элементов центра Z тела K отлично от Z (в таком случае говорят, что J — инволюция *второго рода*; это бывает всегда, когда тело K коммутативно и J не есть тождественный автоморфизм). Действительно, тогда существует такой элемент $\gamma \in Z$, что $\gamma^J \neq \gamma$ и, значит, $\alpha = \gamma + \gamma^J \neq 0$. Если μ — произвольный симметричный элемент тела K, то $(\alpha^{-1}\mu)^J = \alpha^{-1}\mu$, поскольку $\alpha \in Z$, и $\mu = \gamma(\alpha^{-1}\mu) + \gamma^J(\alpha^{-1}\mu)^J =$

$= (\gamma\alpha^{-1}\mu) + (\gamma\alpha^{-1}\mu)^J$. Напротив, никакой симметричный элемент, отличный от 0, не является «следом», если K коммутативно (характеристики 2) и J — тождественный автоморфизм. В этом случае T-формы — это *знакопеременные* формы. Можно привести и другие примеры, когда не все симметричные элементы являются следами. Существует, например, некоммутативное тело размерности 4 над своим центром, обладающее этим свойством (см. Дьёдонне [4], стр. 73).

Изучение унитарных групп относительно произвольных эрмитовых форм может быть в основном сведено к изучению унитарных групп относительно T-форм (Дьёдонне [16]). В самом деле, если f — любая эрмитова форма на $E \times E$, то множество V векторов $x \in E$, для которых $f(x, x)$ есть след, является подпространством. Положим $V_1 = V \cap V^0$ (это вполне изотропное подпространство), и пусть V_2 и V_3 — подпространства, дополнительные к V_1 в пространствах V и V^0 соответственно. Нетрудно показать, что существует такой базис $(e_i)_{1 \leqslant i \leqslant 2q}$ пространства $(V_2 + V_3)^0 = V_2^0 \cap V_3^0$, что векторы e_i, $i \leqslant q$, образуют базис пространства V_1 и $f(e_i, e_{q+j}) = 0$ при $i \neq j$, $f(e_i, e_{q+i}) = 1$ при $1 \leqslant i \leqslant q$. Если V_4 — подпространство, порожденное векторами e_{q+i} $(1 \leqslant i \leqslant q)$, то E есть прямая сумма подпространств V_1, V_2, V_3 и V_4. Анализ условий, которым должно удовлетворять унитарное преобразование u, показывает, что группа $U_n(K, f)$ обладает нормальным рядом

$$U_n \supset \Gamma_0 \supset \Gamma \supset \{1\},$$

в котором группы Γ_0/Γ и Γ абелевы, а фактор U_n/Γ_0 изоморфен унитарной группе $U_m(K, f_2)$, где f_2 — ограничение формы f на $V_2 \times V_2$ и $m = \dim V_2$ [1]). По построению f_2 — невырожденная *Т-форма.*

Такое же разложение пространства E позволяет доказать существование ортогонального базиса в случае,

---

[1]) Это следует из того, что группа $U_n(K, f)$ тождественно действует на E/V. В самом деле, пусть $u \in U_n(K, f)$, $x \in E$. Тогда имеем $f(u(x), u(x)) = f(x, x)$ и $f(u(x) + x, u(x) + x) = f(u(x), x) + f(u(x), x)^J$; следовательно, $u(x) + x \in V$, т. е. $u(x) \equiv x \pmod V$. — *Прим. перев.*

который мы не разобрали в § 8, а именно, когда K — поле характеристики 2 и f — симметричная, но не знакопеременная форма. В предыдущих обозначениях множество $V \cup V^0$ не может совпадать со всем пространством E и, если $a \notin V \cup V^0$, то a — неизотропный вектор и в ортогональной к нему гиперплоскости H существуют неизотропные векторы (так как иначе $H = V$ и $a \in V^0$). Такое же рассуждение по индукции, как и в § 8, позволяет установить существование ортогонального базиса (Алберт [1]).

§ 11. Свойства T-форм

Начиная с этого места, мы будем предполагать, что все рассматриваемые эрмитовы формы являются *невырожденными T-формами*. Для таких форм справедлива прежде всего следующая лемма: *каковы бы ни были изотропный вектор $a \in E$ и содержащая его неизотропная плоскость P, существует второй изотропный вектор $b \in P$, для которого $f(a, b) = 1$*. В самом деле, можно взять такой вектор $c \in P$, что $f(c, a) = \alpha \neq 0$, и искать вектор b в виде $b = c + a\xi$ так, чтобы $f(b, b) = 0$. При этом получается уравнение $\alpha\xi + \xi^J\alpha^J = -f(c, c)$, и так как $-f(c, c) = \lambda + \lambda^J$, то можно положить $\xi = \alpha^{-1}\lambda$. При этом $f(a, b) = \alpha^J \neq 0$. Умножая b на α^{-J}, получаем требуемое соотношение.

Из этого результата получаются два следствия.

1) *Для всякого вполне изотропного подпространства V пространства E существует второе вполне изотропное подпространство W той же размерности, такое, что $V \cap W = \{0\}$ и никакой вектор из V не ортогонален к W. Кроме того, для всякой пары вполне изотропных подпространств, удовлетворяющих этому условию и имеющих одинаковую размерность p, существует базис $(e_i)_{1 \leqslant i \leqslant p}$ пространства V и базис $(e_{p+i})_{1 \leqslant i \leqslant p}$ пространства W, такие, что $f(e_i, e_{p+j}) = \delta_{ij}$.*

Это утверждение можно доказать индукцией по размерности пространства V при помощи предыдущей леммы. Заметим, что для пары вполне изотропных подпространств размерности p, равной *индексу* ν формы f, из соотношения $V \cap W = \{0\}$ вытекает, что никакой вектор из V не ортогонален к W.

2) *Если $\nu \geqslant 1$, то существует базис пространства E, составленный из изотропных векторов.* В самом деле, существует изотропный вектор $a \in E$ и второй изотропный вектор b, такой, что $f(a, b) = 1$. Плоскость P, определенная векторами a и b, неизотропна. Пусть $(c_i)_{1 \leqslant i \leqslant n-2}$ — базис ортогонального дополнения P^0. Поскольку $f(b, a + c_i) \neq 0$, в плоскости, определенной векторами b и $a + c_i$, существует такой изотропный вектор e_i, что $f(b, e_i) = 1$. Векторы a, b и e_i $(1 \leqslant i \leqslant n-2)$ образуют искомый базис.

Два подпространства V, W одинаковой размерности не всегда, вообще говоря, можно перевести одно в другое унитарным преобразованием пространства E. Условие существования такого преобразования дается следующей фундаментальной теоремой, принадлежащей Витту [1] (см. также Полл [1] и Капланский [1]):

Для того чтобы существовало такое унитарное преобразование $u \in U_n(K, f)$, что $u(V) = W$, необходимо и достаточно, чтобы ограничения формы f на $V \times V$ и $W \times W$ были эквивалентны.

Доказательства требует лишь достаточность этого условия. Пусть v — такое линейное отображение пространства V на пространство W, что $f(v(x), v(y)) = f(x, y)$ при $x, y \in V$. Достаточно доказать, что отображение v может быть *продолжено до преобразования* $u \in U_n$. Доказательство, которое мы наметим, принадлежит Шевалле [1]. Будем доказывать теорему индукцией по размерности m подпространств V и W. Применяя предположение индукции к $(m-1)$-мерному подпространству U пространства V, мы можем с самого начала считать, что $v(x) = x$ при $x \in U$. Рассмотрим, далее, подпространство U_1 наибольшей размерности среди подпространств, содержащих U и обладающих следующим свойством: отображение v может быть продолжено до такого линейного отображения w подпространства $V + U_1$, что $f(w(x), w(y)) = f(x, y)$ при $x, y \in V + U_1$ и $w(x) = x$ при $x \in U_1$. Заменив V на $V + U_1$, можно предполагать, что $U_1 = U$, т. е. что отображение v не может быть продолжено на подпространство

$V_1 \supset V$ таким образом, чтобы $f(v(x), v(y)) = f(x, y)$ при $x, y \in V_1$ и чтобы в V_1 существовали векторы, инвариантные относительно v и не лежащие в U. Поскольку результат очевиден при $U = V$, можно предполагать, что $V = U + aK$, где $a \notin U$. Положим $b = v(a)$; ясно, что $b \notin U$. Можно также считать, что $V \neq E$. Попытаемся продолжить v на подпространство размерности $m+1$. Для этого нужно найти векторы $z \notin V$, $z' \notin W$, удовлетворяющие следующим условиям:

(A) $z' - z$ ортогонален к U, $f(z, a) = f(z', b)$ и $f(z, z) = f(z', z')$.

Тогда можно будет продолжить отображение v на подпространство $V + zK$, положив $v(z) = z'$.

Заметим, что из-за *максимальности* подпространства U невозможно, чтобы условия (A) удовлетворялись при $z' = z$, т. е. чтобы вектор $z' = z$, не принадлежащий ни V, ни W, был ортогонален к $b - a$. Отсюда следует, что гиперплоскость H, ортогональная к $b - a$, содержится в V или в W. Это означает, в частности, что $m = n - 1$. Предположим для определенности, что $H = V$. Тогда $f(a, b - a) = 0$ и $f(a, b) = f(a, a) = f(b, b)$, так что $f(b, b - a) = 0$ и, значит, $b \in H$ и $H = W$.

Таким образом, доказательство свелось к случаю, когда подпространства V и W совпадают с гиперплоскостью H, ортогональной к $b - a$. В этом случае $b - a$ — изотропный вектор, ортогональный к векторам a и b и к подпространству U. Попытаемся сделать так, чтобы выполнялись условия (A), взяв в качестве z произвольный вектор, не лежащий в V. Будем искать вектор z' в виде $z' = z + c + (b - a)\xi$, определяя c и ξ с помощью условия (A). Прежде всего, вектор c должен быть ортогонален к U. Из условия $f(z', b) = f(z, a)$ получаем $f(c, b) = -f(z, b - a) = \beta \neq 0$. Так как $b \notin U$, то существует вектор $c \in U^0$, для которого $f(c, b) = \beta$. Этот вектор не может быть ортогонален к a, так как в этом случае он был бы ортогонален и к гиперплоскости $H = U + aK$ и, следовательно, к b; значит, $f(c, a) = \alpha \neq 0$. Итак, $f(z', b - a) = f(z, b - a) + f(c, b - a) = -f(c, a) = -\alpha \neq 0$, откуда видно, что $z' \notin H$ при любом ξ. Остается определить ξ из условия $f(z', z') = f(z, z)$. Поскольку f есть T-форма, получаем следующее соотношение: $\alpha\xi+\xi^J\alpha^J=f(z+c,z+c)-$ $-f(z,z)=\lambda+\lambda^J$, так что можно взять $\xi=\alpha^{-1}\lambda$.

Перед тем как делать выводы из теоремы Витта, укажем, что для того, чтобы подпространство V могло быть преобразовано в W посредством унитарного подобия, необходимо и достаточно, чтобы ограничение формы f на $W\times W$ было эквивалентно ее ограничению на $V\times V$, умноженному на элемент μ из *группы множителей* $M(f)$ (см. § 9).

Из теоремы Витта получаются следующие результаты:

3) *Если V и W — два вполне изотропных подпространства одинаковой размерности, то существует такое преобразование $u\in U_n(K,f)$, что $u(V)=W$.*

4) *Всякое вполне изотропное подпространство V пространства E содержится во вполне изотропном подпространстве максимальной размерности ν.*

В самом деле, пусть W — вполне изотропное подпространство размерности ν и V_1 — подпространство в W, размерность которого равна размерности V. Тогда существует такое преобразование $u\in U_n(K,f)$, что $u(V_1)=V$. Подпространство $u(W)$ удовлетворяет поставленным условиям.

5) Пусть V, W — вполне изотропные подпространства максимальной размерности ν, причем $V\cap W=\{0\}$. Тогда подпространство $M=V+W$ неизотропно (размерности 2ν), поскольку всякий изотропный вектор, ортогональный к V, содержится в V (см. § 7). По той же причине подпространство M^0 (размерности $n-2\nu$) не содержит никакого изотропного вектора. Если теперь V_1, W_1 — два других вполне изотропных подпространства размерности ν, для которых $V_1\cap W_1=\{0\}$, то *существует такое унитарное преобразование u, что $u(V)=V_1$ и $u(W)=W_1$*. Это следует из теоремы Витта и из существования базисов подпространств $V+W$ и V_1+W_1 описанного в п. 1 типа. Так как $u(M^0)=M_1^0$, то ограничения формы f на $M^0\times M^0$ и на $M_1^0\times M_1^0$ эквивалентны. Ограничение формы f на $M^0\times M^0$, которое определено, таким образом, однозначно с точностью до эквивалентности, называется *приведенной* анизотропной

формой формы f. Для того чтобы две эрмитовы формы были эквивалентны, необходимо и достаточно, чтобы они имели одинаковый индекс и чтобы их приведенные анизотропные формы были *эквивалентны*.

Если K — упорядоченное поле (по необходимости нулевой характеристики) и f — симметричная форма, то элементы $c_i = {}^1/_2(e_i + e_{i+\nu})$, $c_{i+\nu} = {}^1/_2(e_i - e_{i+\nu})$ $(1 \leqslant \leqslant i \leqslant \nu)$ образуют ортогональный базис подпространства $M = V + W$, причем $f(c_i, c_i) = {}^1/_2$ и $f(c_{i+\nu}, c_{i+\nu}) = = -{}^1/_2$ при $1 \leqslant i \leqslant \nu$. Дополняя систему $(c_i)_{1 \leqslant i \leqslant 2\nu}$ до ортогонального базиса пространства E при помощи ортогонального базиса $(c_i)_{2\nu < i \leqslant n}$ подпространства M^0, мы видим, что $\nu \leqslant \mathrm{Min}\,(p, n-p)$, где p — число таких индексов i, что $f(c_i, c_i) > 0$. Если, кроме того, поле K евклидово, то можно считать, что $f(c_i, c_i) = 1$ при всех $i > 2\nu$ или $f(c_i, c_i) = -1$ при всех $i > 2\nu$, поскольку M^0 не содержит изотропных векторов. В таком случае $\nu = \mathrm{Min}\,(p, n-p)$. Эти результаты легко распространяются на эрмитовы формы в случае, когда K — квадратичное расширение упорядоченного поля или обобщенное тело кватернионов над упорядоченным полем.

Заметим, наконец, что теорема Витта и утверждения 1)—4) этого параграфа справедливы также для *знакопеременной* формы f.

§ 12. Квазиотражения и сдвиги в унитарных группах

Проблема *классификации* преобразований, принадлежащих группе $U_n(K, f)$ или $GU_n(K, f)$, или $\Gamma U_n(K, f)$, состоит в отыскании условий, при которых два преобразования u, v, принадлежащие одной из этих групп, *сопряжены* в этой группе. Мы изучим только частные случаи этой проблемы. Более полное исследование проведено в работах Жордана ([3], т. III), Спрингера [1], Якобинского [1] и Уолла [2].

Заметим вначале, что если подпространство V пространства E инвариантно (в целом) относительно некоторого преобразования из $\Gamma U_n(K, f)$, то его ортогональное дополнение V^0 также инвариантно (в целом) относительно этого преобразования. Если V неизотропно, то такое преобразование определяется своими ограничениями на дополнительных подпространствах V, V^0, и множество этих преобразований является группой, изоморфной подгруппе группы $\Gamma U_p(K, f_1) \times \Gamma U_{n-p}(K, f_2)$, образованной такими парами (v, w), для которых автоморфизмы тела K и множители, соответствующие v и w, одинаковы. (Здесь $p = \dim V$, f_1 и f_2 — ограничения формы f на $V \times V$ и $V^0 \times V^0$ соответственно.)

Рассмотрим теперь преобразования из $\Gamma U_n(K, f)$, оставляющие на месте *каждый элемент* подпространства V. Такое преобразование u должно принадлежать группе $GU_n(K, f)$, а если V не вполне изотропно, то группе $U_n(K, f)$. Пусть $V_1 = V \cap V^0$ и U — дополнительное подпространство к V_1 в V. Тогда преобразование u однозначно определяется своим ограничением на неизотропном подпространстве U^0, в котором оно должно оставлять на месте все элементы подпространства V_1. Если $V_1 = \{0\}$ (т. е. V неизотропно), то такие преобразования u образуют группу, изоморфную группе $U_{n-p}(K, f_2)$ (в тех же обозначениях, что и выше). Другой крайний случай — это когда V вполне изотропно. Ограничимся случаем, когда V — вполне изотропное подпространство максимальной размерности ν, причем $2\nu = n$. Пусть W — вполне изотропное подпространство, дополнительное к V, и $(e_i)_{1 \leqslant i \leqslant 2\nu}$ — базис пространства E описанного в п. 1 § 11 типа. Положим $u(x) = x + v(x)$. Из соотношения $f(u(x), u(y)) = f(x, y)$ получаем прежде всего, что $f(x, v(y)) = 0$ при $x \in V$, $y \in W$. Это означает, что v — линейное отображение, аннулирующее V и отображающее W в V. Далее, при $x \in W$, $y \in W$ получаем (для эрмитовой формы f) соотношение $f(x, v(y)) + f(y, v(x))^J = 0$. Матрица преобразования u в базисе (e_i) имеет вид

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix},$$

где ${}^tS = -S^J$ (иначе говоря, S — *косоэрмитова* матрица порядка ν и *произвольного* ранга $\leqslant \nu$). Если исходить из косоэрмитовой формы f, то S будет *эрмитовой* матрицей. Следовательно, подгруппа группы $U_n(K, f)$, оставляющая на месте все элементы подпространства

V, в рассматриваемом случае изоморфна аддитивной группе косоэрмитовых (соответственно эрмитовых) матриц порядка ν. Унитарные преобразования того типа, который мы только что рассматривали, называются *специальными* преобразованиями. Легко видеть, что для того, чтобы два таких преобразования u_1, u_2 были *сопряжены* в группе $U_n(K, f)$, необходимо и достаточно, чтобы соответствующие матрицы S_1 и S_2 (или, что то же самое, косоэрмитовы формы $f(x, v_1(y))$ и $f(x, v_2(y))$ в пространствах W_1 и W_2 соответственно) были *эквивалентны*.

Рассмотрим унитарные преобразования, оставляющие на месте все элементы *гиперплоскости* V, т. е. унитарные растяжения и сдвиги (см. § 2). Если V *неизотропно* и a — вектор, ортогональный к V, то $u(a) = a\alpha$ и $\alpha^J f(a, a)\alpha = f(a, a)$. Такое преобразование u называется *квазиотражением* относительно гиперплоскости V. Для данной неизотропной гиперплоскости V всегда существует квазиотражение, отличное от тождественного. Если характеристика тела K не равна 2, то можно взять $\alpha = -1$ (тогда получается *отражение* относительно V). Если характеристика тела K равна 2, то при $f(a, a) = \lambda + \lambda^J$ возьмем $\alpha = \lambda^{-1}\lambda^J$; тогда $\alpha^J\lambda\alpha = \lambda$ и $\alpha^J\lambda^J\alpha = \lambda^J$, так что α удовлетворяет нужному условию; кроме того, $\alpha \neq 1$, так как $\lambda^J \neq \lambda$. Заметим, что в ортогональной группе $O_n(K, f)$ (где K — поле характеристики $\neq 2$) единственным квазиотражением относительно гиперплоскости V, отличным от тождественного, является отражение относительно V. Симплектическая группа $Sp_n(K)$ является *единственной* унитарной группой, в которой нет квазиотражений (потому что нет неизотропных гиперплоскостей).

Что касается *унитарных сдвигов*, то они существуют, только если гиперплоскость V *изотропна*; вектор a сдвига является при этом изотропным вектором, ортогональным к V. Такой сдвиг представляется в виде $x \to x + a\lambda f(a, x)$, где λ — кососимметричный элемент тела K, если форма f эрмитова, и симметричный, если она косоэрмитова. При замене вектора a на $a\mu^{-1}$ коэффициент λ заменяется на $\mu\lambda\mu^J$. Для того чтобы два унитарных сдвига вдоль гиперплоскости V были сопряжены в группе U_n, необходимо и достаточно, чтобы их коэффициенты λ, λ' были связаны соотношением $\lambda' = \mu^J\lambda\mu$ при подходящем μ. Заметим, что, коль скоро в пространстве E имеются изотропные векторы, существуют унитарные сдвиги; исключением является лишь ортогональная группа $O_n(K, f)$ (где K — поле характеристики $\neq 2$), поскольку в K в этом случае нет кососимметричного элемента, отличного от 0.

§ 13. Полуинволюции в унитарных группах и их централизаторы. Первый случай

Пусть u — некоторая полуинволюция в группе $\Gamma U_n(K, f)$ относительно автоморфизма σ тела K. Пусть $u^2(x) = x\gamma$ и $f(u(x), u(y)) = e(f(x, y))^\sigma$. Перепишем в этом случае соотношения (1), (2), (21) и (22):

$$\gamma^\sigma = \gamma, \ \xi^{\sigma^2} = \gamma^{-1}\xi\gamma, \ \xi^{\sigma J} = e\xi^{J\sigma}e^{-1}, \ e^J = e. \tag{24}$$

Кроме того, вычисляя $f(u^2(x), u^2(y))$ двумя способами, находим, что

$$\gamma^J\gamma = ee^\sigma. \tag{25}$$

Мы будем предполагать в этом параграфе, что γ *не представляется в виде* $\lambda\lambda^\sigma$ (случай А) § 3). Образуем квадратичное расширение $K_0 = K(\rho)$ тела K, в котором $\rho^2 = \gamma$ и $\eta\rho = \rho\eta^\sigma$ при $\eta \in K$, и превратим пространство E в векторное пространство размерности $n/2$ над K_0, полагая $x\zeta = x\xi + u(x)\eta$ при $\zeta = \xi + \rho\eta \in K_0$ и $x \in E$. Полученное векторное пространство обозначим через E_0. Легко видеть, что существует взаимно однозначное соответствие $x' \leftrightarrow x'_0$ между пространством E^*, двойственным к E, и пространством E_0^*, двойственным к E_0, при котором

$$\langle x'_0, x\rangle = \langle x', x\rangle + \rho\langle x', u(x)\rangle^\sigma\gamma^{-1} \tag{26}$$

для всякого $x \in E$. Кроме того, при помощи формул (24) и (25) можно показать, что инволюция J может быть распространена на K_0 таким образом, что $\rho^J = \rho e^\sigma\gamma^{-1}$. В соответствии с формулой (26), корреляции

φ (ассоциированной с формой f) отвечает отображение φ_0 пространства E_0 в E_0^*, определяемое формулой

$$\langle \varphi_0(x),\ y\rangle = \langle \varphi(x),\ y\rangle + \rho\,\langle \varphi(x),\ u(y)\rangle^{\sigma}\gamma^{-1}. \qquad (27)$$

Из (24) и (25) выводится, что $\varphi_0(x\zeta) = \zeta^J\varphi_0(x)$ при любом $\zeta \in K_0$; иначе говоря, φ_0 есть *корреляция*. Далее, если ${}^t\varphi = \varepsilon\varphi$, $\varepsilon = \pm 1$, то и ${}^t\varphi_0 = \varepsilon\varphi_0$. В самом деле, из формулы (27) следует, что

$$\langle \varphi_0(x),\ y\rangle^J - \varepsilon\,\langle \varphi_0(y),\ x\rangle \in \rho K$$

при любых $x, y \in E_0$; однако это выражение является линейной функцией от x (над K_0) и не может принимать значения только в ρK, не будучи тождественно равным нулю.

Из (27) получаем следующую формулу для рефлексивной формы $f_0(x, y)$, ассоциированной с корреляцией φ_0:

$$f_0(x,\ y) = f(x,\ y) + \rho\,(f(x,\ u(y)))^{\sigma}\gamma^{-1}. \qquad (28)$$

Найдем теперь группу H полуподобий, *проективно перестановочных* с полуинволюцией u. Это равносильно изучению *централизатора* инволюции $\bar{u} \in P\Gamma U_n$ в проективной группе $P\Gamma U_n$ (см. § 4). Преобразование $v \in H$, соответствующее автоморфизму τ, удовлетворяет условию $vu = uv\cdot a$ $(a \in K)$, из которого вытекают соотношения (3) и (4); кроме того, $\varphi(v(x)) = h\check{v}(\varphi(x))$, где h — симметричный элемент тела K. Известно (см. § 4), что можно распространить автоморфизм τ на тело K_0 таким образом, что v будет коллинеацией пространства E_0 относительно полученного автоморфизма. Если это сделать, то из формулы (28) будет следовать, что $f_0(v(x),\ v(y)) - h(f_0(x, y))^{\tau} \in \rho K$ при любых $x \in E_0$, $y \in E_0$; но так как это выражение при фиксированном x полулинейно по y, все его значения могут лежать в ρK, только если оно тождественно равно нулю. Следовательно, v принадлежит группе $\Gamma U_{n/2}(K_0, f_0)$. Обратно, элемент v этой группы проективно перестановочен с u, если соответствующий ему автоморфизм τ тела K_0 сохраняет (в целом) K и удовлетворяет условию $\rho^{\tau} = \rho a$ (где $a \in K$) и если его множитель принадлежит K. Заметим, что подгруппа H группы $\Gamma U_{n/2}(K_0, f_0)$, определенная этим условием, содержит в качестве нормального делителя *унитарную группу* $U_{n/2}(K_0, f_0)$.

§ 14. Полуинволюции в унитарных группах и их централизаторы. Второй случай

В обозначениях § 13 предположим теперь, что $\gamma = \lambda\lambda^{\sigma}$. Заменяя u на $u \cdot \lambda^{-1}$ (что приводит к изменению автоморфизма и множителя, соответствующих u), можно добиться того, чтобы $\gamma = 1$, откуда $\sigma^2 = 1$ и $ee^{\sigma} = 1$. Рассмотрим отдельно два случая в зависимости от того, тождествен автоморфизм σ или нет.

А) $\sigma = 1$ и, значит, $e^2 = 1$. Есть три возможности:

А1) Характеристика тела K не равна 2 и $e = 1$; тогда u — инволютивный элемент группы $U_n(K, f)$. Легко видеть, что всякий вектор из U^+ ортогонален ко всякому вектору из U^-. Отсюда вытекает, что подпространства U^+, U^- неизотропны; каждое из них есть ортогональное дополнение к другому. Обратно, для всякой пары дополнительных ортогональных неизотропных подпространств V, W линейное преобразование u, определенное равенствами $u(x) = x$ при $x \in V$ и $u(x) = -x$ при $x \in W$, является инволютивным элементом группы $U_n(K, f)$.

Пусть v — полуподобие с множителем h, соответствующее автоморфизму τ тела K, и пусть $vu = uv \cdot a$. Из условия (4) находим, что $a^2 = 1$, т. е. $a = \pm 1$. Случай $vu = -uv$ возможен, только если U^+ и U^- имеют одинаковую размерность. Если H — группа полуподобий, проективно перестановочных с u, и H_0 — централизатор элемента u в ΓU_n, то H_0 — подгруппа индекса 1 или 2 в H. Группа H_0 изоморфна подгруппе прямого произведения $\Gamma U_p(K, f_1) \times \Gamma U_{n-p}(K, f_2)$ (где $p = \dim U^+$, f_1 и f_2 — ограничения f на $U^+ \times U^+$ и $U^- \times U^-$ соответственно), образованной такими парами полуподобий, что входящие в одну пару полуподобия имеют одинаковые автоморфизмы и множители.

А2) Характеристика тела K не равна 2 и $e = -1$. Из соотношения $f(u(x), u(y)) = -f(x, y)$ немедленно следует, что U^+ и U^- — дополнительные *вполне* *изотропные* подпространства и, значит, $n = 2m$ и $\dim U^+ = \dim U^- = m = \nu$. Обратно, если $n = 2\nu$ и V, W — дополнительные вполне изотропные подпространства максимальной размерности ν, то линейное преобразование u, определенное равенствами $u(x) = x$ при $x \in V$ и $u(x) = -x$ при $x \in W$, удовлетворяет условию $f(u(x), u(y)) = -f(x, y)$ при любых $x \in E$, $y \in E$.

Если $v \in \Gamma U_n$ и $vu = uv \cdot a$, то, как и в предыдущем случае, $a^2 = 1$. Предполагая, что форма f эрмитова, можно выбрать в пространстве E базис описанного в п. 1 § 11 типа, и тогда преобразование v, определенное равенствами $v(e_i) = e_{i+m}$ и $v(e_{i+m}) = e_i$ при $1 \leqslant i \leqslant m$, принадлежит подгруппе H, причем $vu = -uv$. Следовательно, централизатор H_0 инволюции u в группе ΓU_n в этом случае всегда является подгруппой индекса 2 в группе H. Таким образом, можно ограничиться рассмотрением H_0. Пусть $v \in H_0$ — полуподобие, соответствующее автоморфизму τ, и h — его множитель. Соотношение $vu = uv$ показывает, что $v(U^+) = U^+, v(U^-) = U^-$, а соотношение $f(v(x), v(y)) = h(f(x, y))^\tau$ при $x \in U^+$ и $y \in U^-$ показывает, что действие преобразования v в U^- однозначно определяется действием v в U^+, причем соответствующий автоморфизм τ обладает тем свойством, что антиавтоморфизмы τJ и $J\tau$ отличаются на внутренний автоморфизм тела K. Непосредственно проверяется, что, обратно, всякая коллинеация пространства U^+ относительно автоморфизма τ, обладающего этим свойством, продолжается до коллинеации v пространства E, принадлежащей H_0. Таким образом, группа H_0 может быть отождествлена с подгруппой группы $\Gamma L_{n/2}(K)$, образованной такими коллинеациями, что соответствующие им автоморфизмы обладают указанным выше свойством. Заметим, что H_0 содержит в качестве нормального делителя *полную линейную* группу $GL_{n/2}(K)$.

A3) Характеристика тела K равна 2 и $e = 1$. Тогда (см. § 3) $u(x) = x + w(x)$, где $w(E) \subset w^{-1}(0) = U$. Записывая условие унитарности для u, находим, что $w(E)$ ортогонально к U; так как $w(E)$ имеет ту же размерность, что и U^0, то $w(E) = U^0 \subset U$ — вполне изотропное подпространство. Если полуподобие $v \in$

$\in \Gamma U_n(K, f)$ проективно перестановочно с u, то оно принадлежит централизатору H инволюции u в группе $\Gamma U_n(K, f)$, поскольку в рассматриваемом случае из $a^2 = 1$ следует $a = 1$. Следовательно, $v(U) = U$ и $v(U^0) = U^0$. Обозначим через V (неизотропное) подпространство, дополнительное к U^0 в U. Тогда V^0 будет неизотропным подпространством размерности $2p$, где $p = \dim U^0$. Оно содержит U^0, и в нем можно найти p-мерное вполне изотропное подпространство W, дополнительное к U^0 в V^0 (см. § 11).

Пусть H_1 — нормальный делитель группы H, образованный такими v, что $v(x) \equiv x (\operatorname{mod} U)$ при всех $x \in E$ и $v(y) \equiv y (\operatorname{mod} U^0)$ при всех $y \in U$. Из этих условий следует, что v — *линейное* преобразование. Если $V \neq \neq \{0\}$, то его множитель равен 1; иначе говоря, $v \in U_n(K, f)$. Из равенства $f(v(x), v(y)) = f(x, y)$ при $x \in W$ и $y \in U^0$ получаем $f(x, v(y) - y) = 0$ и, так как $W^0 = V + W$ и $v(y) - y \in U^0$, то $v(y) = y$ при $y \in U^0$. Если $V = \{0\}$, то таким же образом получаем, что $v(y) = yh$ при $y \in U^0$, где h — множитель v (принадлежащий центру тела K).

Пусть H_2 — подгруппа группы H_1, оставляющая на месте каждый элемент из U. Так как любое преобразование $v \in H_2$ оставляет на месте все элементы подпространства V, то оно полностью определяется своим ограничением на $V^0 = U^0 + W$, которое является унитарным преобразованием этого пространства, оставляющим на месте все элементы вполне изотропного подпространства U^0, и, следовательно, — специальным преобразованием (см. § 12). Это показывает, что H_2 — *абелева* группа, изоморфная аддитивной группе косоэрмитовых или эрмитовых матриц порядка p в зависимости от того, эрмитова или косоэрмитова форма f.

Группа H_1/H_2 изоморфна группе H_1' ограничений преобразований $v \in H_1$ на U. Если $V \neq \{0\}$, положим $v(y) = y + v''(y)$, где $v''(y) \in U^0$, при $y \in V$; с другой стороны, положим $v(x) = x + v'(x)$, где $v'(x) \in U$, при $x \in W$. Соотношение $f(v(x), v(y)) = f(x, y)$ дает тогда $f(v'(x), y) + f(x, v''(y)) = 0$ при $x \in W$, $y \in V$. Выбирая каким-либо образом базисы в V и в $V^0 = U^0 + W$ (например, ортогональный или симплектический базис в V и базис описанного в п. 1) § 11 типа в V^0), нетрудно установить, что для всякого линейного отображения v'' пространства V в пространство U^0 существует единственное линейное отображение v' пространства W в пространство V, удовлетворяющее предыдущему условию. Это показывает, что группа H_1/H_2 изоморфна аддитивной группе матриц, имеющих p строк и $n-2p$ столбцов, т. е. группе $K^{p(n-2p)}$. Если $V=\{0\}$, то $v(y)=$ $=yh$ при $y\in U^0=U$, и можно положить $v(x)=x$ при $x\in W$. Следовательно, в этом случае группа H_1/H_2 изоморфна мультипликативной группе Z_0^* поля симметричных элементов центра тела K.

Определим, наконец, H/H_1. Для всякого $v\in H$ положим $v(x)=v_1(x)+v'(x)$, где $v_1(x)\in W$, $v'(x)\in U$, при $x\in W$, и $v(y)=v_2(y)+v''(y)$, где $v_2(y)\in V$, $v''(y)\in U^0$, при $y\in V$. Определим коллинеацию $\tilde{v}$ следующим образом: $\tilde{v}(x)=v_1(x)$ при $x\in W$, $\tilde{v}(y)=v_2(y)$ при $y\in V$ и $\tilde{v}(z)=v(z)$ при $z\in U^0$. Можно проверить, что $\tilde{v}$ принадлежит группе $\Gamma U_n(K,f)$ (и ей соответствует тот же автоморфизм τ и множитель h, что и v) и что v коммутирует с u тогда и только тогда, когда $\tilde{v}$ коммутирует с u. Таким образом, отображение $v\to\tilde{v}$ является гомоморфизмом группы H на ее подгруппу $\tilde{H}$, причем ядром этого гомоморфизма служит H_1. Группа $\tilde{H}$, тем самым, изоморфна H/H_1. Выберем в пространстве $V^0=U^0+W$ базис описанного в п. 1) § 11 типа. Тогда матрица ограничения коллинеации $\tilde{v}$ на V^0 будет иметь вид $\begin{pmatrix}\check{A}^J h & 0\\ 0 & A\end{pmatrix}$, где A — квадратная матрица порядка p. Матрица ограничения отображения u на V^0 имеет вид $\begin{pmatrix} I & S\\ 0 & I\end{pmatrix}$, где S — косоэрмитова или эрмитова матрица порядка p в зависимости от того, эрмитова или косоэрмитова форма f. Условие перестановочности u и $\tilde{v}$ в V_0 записывается тогда в виде ${}^tA^JSA=hS^\tau$; иначе говоря, ограничение $\tilde{v}$ на V^0 может быть отождествлено с элементом группы $\Gamma U_p(K,S)$. С другой стороны, ограничение $\tilde{v}$ на V есть элемент группы $\Gamma U_{n-2p}(K,f_1)$, где f_1 — невырожденная форма, являющаяся ограничением f на $V\times V$. Окончательно, группа

$\bar{H} \simeq H/H_1$ *изоморфна подгруппе группы* $\Gamma U_{n-2p}(K, f_1) \times \times \Gamma U_p(K, S)$, *образованной парами коллинеаций с одинаковыми автоморфизмами и множителями.* Заметим, что рефлексивная форма, определяемая матрицей S, невырожденна, но может *не быть* T-*формой* (см. § 10).

В) $\sigma \neq 1$. Обозначим через K_1 подтело тела K, образованное элементами, инвариантными относительно σ. (Отметим, что, вообще говоря, K_1 не инвариантно относительно J.) Известно, что множество U^+ элементов $x \in E$, для которых $u(x) = x$, есть n-мерное подпространство над K_1, причем базис U^+ над K_1 есть в то же время базис E над K (см. § 3). Имеем $f(x, y) = ef(x, y)^\sigma$ при $x \in U^+$, $y \in U^+$. Заменяя x на $x\xi$, где $\xi \in K_1$, получаем, что $\xi^J = e\xi^{J\sigma}e^{-1}$. Отсюда следует, что если $e = \pm 1$, то K_1 инвариантно относительно J. Мы сейчас покажем, что, умножая форму f на подходящий симметричный или кососимметричный элемент, можно добиться того, чтобы $e = 1$. Предположим вначале, что $r = 1 + e \neq 0$; тогда $r^J = r$ и $r^\sigma = re^{-1}$, т. е. $e = r^{1-\sigma}$. Форма $g(x, y) = = r^{-1}f(x, y)$ будет эрмитовой (соответственно косоэрмитовой) относительно инволюции $\xi \to \xi^T = r^{-1}\xi^J r$, если f — эрмитова (соответственно косоэрмитова) относительно J. При этом $g(u(x), u(y)) = (g(x, y))^\sigma$. Остается рассмотреть случай, когда $e = -1$ и характеристика K отлична от 2. Имеем $K = K_1(\rho)$, $\rho^\sigma = -\rho$. Возьмем $r = = \rho^J \pm \rho$, выбрав знак так, чтобы $r \neq 0$. Тогда $r^J = \pm r$ и $r^\sigma = -r$, так что $e = r^{1-\sigma}$, и дальше можно рассуждать так же, как и выше.

В дальнейшем будем считать, что $e = 1$. Тогда при $x, y \in U^+$ имеем $f(x, y) = (f(x, y))^\sigma$ и, следовательно, $f(x, y) \in K_1$. Поскольку базис пространства U^+ над K_1 есть в то же время базис пространства E над K, ограничение формы f на $U^+ \times U^+$ будет *невырожденной* рефлексивной формой.

Известно (см. § 4), что при изучении коллинеаций v, проективно перестановочных с u, всегда можно, умножив v на скаляр, свести дело к случаю, когда $vu = = \pm uv$, и в этом случае K_1 инвариантно относительно автоморфизма τ тела K, соответствующего v. Рассмотрим отдельно две возможности:

B1) Характеристика тела K не равна 2. Тогда $K = K_1(\rho)$, где $\rho^\sigma = -\rho$. В силу формулы (24) $\rho^{\sigma J} = \rho^{J\sigma}$. Следовательно, $\rho^{J\sigma} = -\rho^J$, так что $\rho^J = \rho\delta$, где $\delta \in K_1$ [1]). Ограничимся рассмотрением централизатора H_0 инволюции u в $\Gamma U_n(K, f)$, являющегося подгруппой индекса 1 или 2 в группе H элементов $v \in \Gamma U_n(K, f)$, для которых $vu = \pm uv$. Ограничение преобразования $v \in H_0$ на U^+ принадлежит группе $\Gamma U_n(K_1, f_1)$, где f_1 — ограничение формы f на $U^+ \times U^+$. Автоморфизм τ тела K_1, соответствующий v, должен удовлетворять условиям (5) и (6) § 4. Кроме того, если h — множитель v (который должен принадлежать K_1), то, записывая условие $\rho^{\tau J} = h\rho^{\tau J}h^{-1}$, находим, что [2])

$$\alpha^{J\omega}\delta h = h^\omega \alpha \delta^\tau. \tag{29}$$

Обратно, если эти условия выполнены, то можно продолжить коллинеацию $v \in \Gamma U_n(K_1, f_1)$ до коллинеации пространства E, полагая $v(x\rho) = v(x)\rho^\tau$ (§ 4), и при этом $f(v(x\rho),\ v(y\rho)) = h(f(x\rho, y\rho))^\tau$ для любых $x,\ y \in U^+$, так что $v \in \Gamma U_n(K, f)$. Так как $U^- = U^+\rho$ и $v(U^-) = U^-$, то при этом также v принадлежит H_0. Итак, группа H_0 изоморфна подгруппе группы $\Gamma U_n(K_1, f_1)$, образованной такими полуподобиями, что соответствующие им автоморфизм τ и множитель h удовлетворяют условиям (5), (6) и (29) (для некоторого $\alpha \in K_1$, зависящего от v). Заметим, что эта подгруппа содержит в качестве нормального делителя *унитарную группу* $U_n(K_1, f_1)$.

B2) Характеристика тела K равна 2. Тогда (см. § 4) $K = K_1\theta$, где $\theta^\sigma = \theta + 1$, и соотношение $\theta^{J\sigma} = \theta^{\sigma J}$ дает, что $\theta^{J\sigma} = \theta^J + 1$. Следовательно, $\theta^J = \theta + \delta$, где $\delta \in K_1$. Группа H в данном случае совпадает с централизатором элемента u в $\Gamma U_n(K, f)$. Так же, как и в B1), ограничение коллинеации v на U^+ принадлежит группе $\Gamma U_n(K_1, f_1)$, причем ее автоморфизм τ должен удовлетворять условиям (7) и (8) § 4. Кроме того, множитель

---

[1]) Если $\rho^2 = \beta \in K_1$ и $\rho^{-1}\xi\rho = \xi^\omega$ при $\xi \in K_1$, то обязательно $\xi^{\omega J} = \mu\xi^{J\omega}\mu^{-1}$, где $\mu \in K_1$, $\mu^J = \mu$, $\beta^\omega = \beta$, $\beta^J\beta = \mu\mu^\omega$; тогда $\delta = \mu^{-1}\beta^J = \mu^\omega\beta^{-1}$.

[2]) См. обозначения п. B2α) § 4. — *Прим. перев.*

$h \in K_1$ полуподобия v должен удовлетворять условию $\theta^{\tau J} = h\theta^{J\tau}h^{-1}$, откуда[1])

$$Dh + h(\lambda + \delta^{\tau}) + (\delta + \lambda^{J})h = 0. \qquad (30)$$

Как и в B1), делаем вывод, что группа H изоморфна подгруппе группы $\Gamma U_n(K_1, f_1)$, образованной полуподобиями, автоморфизм и множитель которых удовлетворяет условиям (7), (8) и (30) (для некоторого $\lambda \in K_1$, зависящего от v). Она содержит в качестве нормального делителя *унитарную группу* $U_n(K_1, f_1)$.

§ 15. Перестановочные корреляции

Мы определили понятие коллинеации, ***проективно перестановочной*** с какой-либо коллинеацией (§ 4) или корреляцией (§ 9). Если теперь φ и ψ — две корреляции пространства E на пространство E^*, то $\varphi^{-1}\psi$ будет коллинеацией пространства E; мы скажем, что корреляции φ и ψ ***проективно перестановочны***, если $\varphi^{-1}\psi$ — ***полуинволюция*** (§ 3), т. е. существует такой элемент $\gamma \in K$, что

$$\varphi^{-1}(\psi(x)) = \psi^{-1}(\varphi(x))\gamma \qquad (31)$$

для всех $x \in E$.

Очевидно, что это свойство не зависит от порядка, в котором берутся φ и ψ. Кроме того, определенные нами в трех случаях понятия «проективной перестановочности» *когерентны* в следующем смысле: если коллинеация u (соответственно корреляция θ) проективно перестановочна с двумя корреляциями φ, ψ, то она проективно перестановочна с коллинеацией $\varphi^{-1}\psi$; если коллинеация u проективно перестановочна с коллинеацией v и с корреляцией φ, то она проективно перестановочна с корреляцией φv; наконец, если корреляция ψ проективно перестановочна с коллинеацией v и с корреляцией φ, то она проективно перестановочна с корреляцией φv.

Описание централизатора инволюции в группе $P\Gamma L_n$ (§ 4) или в группе $P\Gamma U_n$ (§ 13 и 14) есть

[1]) См. обозначения п. B2β) § 4. — *Прим. перев.*

частный случай следующей общей проблемы, с другими частными случаями которой мы встретимся в § 8 гл. IV. *Дано некоторое число полуинволюций* $u_i \in \Gamma L_n(K)$ $(1 \leqslant i \leqslant q)$ *и рефлексивных корреляций* φ_j $(1 \leqslant j \leqslant r)$, *попарно проективно перестановочных. Требуется найти все коллинеации* v, *проективно перестановочные с* u_i $(1 \leqslant i \leqslant q)$ *и* φ_i $(1 \leqslant j \leqslant r)$. Предыдущие замечания позволяют свести вопрос к случаю, когда $r = 0$ или $r = 1$ (заменяя $r - 1$ из корреляций φ_j коллинеациями $\varphi_1^{-1}\varphi_j$).

Если характеристика тела K не равна 2, то можно использовать результаты § 4, 13 и 14 для определения группы H коллинеаций v, проективно перестановочных с полуинволюциями u_i и корреляцией φ, при помощи *рекуррентного процесса* по числу q (Дьёдонне [14]). Возьмем для этого полуинволюцию u_1 и рассмотрим несколько случаев[1]).

1) u_1 удовлетворяет условиям § 13. Тогда (в обозначениях этого параграфа) полуинволюции u_i $(2 \leqslant i \leqslant q)$ могут рассматриваться как $q - 1$ полуинволюций в группе $\Gamma U_{n/2}(K_0, f_0)$, а коллинеация v — как элемент этой группы, проективно перестановочный с ними и такой, что его автоморфизм и множитель удовлетворяют условиям, указанным в § 13.

2) u_1 удовлетворяет условиям случая B) § 14. Тогда полуинволюции u_i $(2 \leqslant i \leqslant q)$, умноженные, если нужно, на подходящие скаляры, могут рассматриваться как $q - 1$ полуинволюций в группе $\Gamma U_n(K_1, f_1)$, а v — как элемент этой группы, проективно перестановочный с ними и такой, что его автоморфизм и множитель удовлетворяют условиям, указанным в § 14.

3) u_1 удовлетворяет условиям случая A1) § 14. Если подпространства U^+ и U^- имеют различную размерность, то они инвариантны относительно преобразований u_i $(2 \leqslant i \leqslant q)$, а также любого элемента v группы H, и, с точностью до условий на множитель и автоморфизм,

[1]) В дальнейшем предполагается, что f — эрмитова или косоэрмитова форма, определяемая корреляцией φ в пространстве E. Условие проективной перестановочности коллинеации v с φ означает, что $v \in \Gamma U_n(K, f)$. — *Прим. перев.*

соответствующие коллинеации v, дело сводится к первоначальной задаче для каждого из подпространств U^+, U^-, но уже для $q-1$ полуинволюций u_i. Так же обстоит дело и тогда, когда U^+ и U^- имеют одинаковую размерность, но $u_iu_1 = u_1u_i$ при $2 \leqslant i \leqslant q$, с той только разницей, что мы переходим от группы H к ее подгруппе H_0 индекса 2. Если, наконец, $u_2u_1 = -u_1u_2$, то, заменив, если нужно, u_i на u_2u_i, можно предполагать, что $u_iu_1 = u_1u_i$ при $i \geqslant 3$. Тогда $u_2(U^+) = U^-$, $u_2(U^-) = U^+$, $u_i(U^+) = U^+$ и $u_i(U^-) = U^-$ при $i \geqslant 3$. Переходя к подгруппе H_0 индекса 2, можно ограничиться случаем, когда $vu_1 = u_1v$, и тогда $v(U^+) = U^+$, $v(U^-) = U^-$. Ограничение v' коллинеации v на подпространстве U^+ принадлежит группе $\Gamma U_{n/2}(K, f')$ (где f' — ограничение формы f на $U^+ \times U^+$) и проективно перестановочно с ограничениями на U^+ полуинволюций u_i $(3 \leqslant i \leqslant q)$. Обратно, можно проверить, что хотя и не всякое такое преобразование v' пространства U^+ продолжается до коллинеации $v \in H_0$, но это всегда имеет место, если v' принадлежит группе $U_{n/2}(K, f')$ и перестановочно с u_i $(i \geqslant 3)$.

4) u_1 удовлетворяет условиям случая A2) § 14. Если $u_iu_1 = u_1u_i$ при $2 \leqslant i \leqslant q$, то преобразования u_i сохраняют подпространства U^+ и U^-, и, перейдя к подгруппе H_0 индекса 2 в группе H, можно предполагать, что тем же свойством обладает преобразование v. Ограничение v на U^+ является коллинеацией этого пространства, проективно перестановочной с ограничениями на U^+ полуинволюций u_i $(2 \leqslant i \leqslant q)$. Такая коллинеация не всегда продолжается до коллинеации $v \in H_0$; однако это верно для линейных коллинеаций $v' \in GL_{n/2}(K)$, перестановочных с u_i $(i \geqslant 2)$.

Если $u_2u_1 = -u_1u_2$, то можно предполагать, что $u_iu_1 = u_1u_i$ при $i \geqslant 3$. Если τ — автоморфизм, соответствующий u_2, то полуторалинейная форма $f'(x, y) = f(u_2(x), y)$, определенная при $x \in U^+$, $y \in U^+$, рефлексивна относительно антиавтоморфизма τJ. В этом случае ограничение v' коллинеации v на U^+ должно принадлежать группе $\Gamma U_{n/2}$ (K, f') и быть проективно перестановочно с ограничениями на U^+ полуинволюций u_i $(3 \leqslant i \leqslant q)$. Обратное опять-таки верно не всегда, но во всяком случае верно для коллинеаций v', принадлежащих группе $U_{n/2}(K, f')$ и перестановочных с u_i $(i \geqslant 3)$.

§ 16. Квадратичные формы и ортогональные группы над полем характеристики 2

Если K — поле характеристики $\neq 2$ и f — симметричная билинейная форма на $E \times E$, то *квадратичной формой*, ассоциированной с f, называют отображение $x \to Q(x) = f(x, x)$ пространства E в K. Непосредственно проверяется, что

$$Q(\lambda x + \mu y) = \lambda^2 Q(x) + \mu^2 Q(y) + 2\lambda\mu f(x, y) \qquad (32)$$

для любых скаляров λ, μ. В частности, отсюда следует, что $f(x, y) = {}^1/_2(Q(x + y) - Q(x) - Q(y))$. Обратно, если отображение Q пространства E в K удовлетворяет тождеству (32), где f — билинейная форма на $E \times E$, то f — симметричная форма, $Q(\lambda x) = \lambda^2 Q(x)$ и $Q(x) = f(x, x)$.

Предположим теперь, что K — поле *характеристики* 2. В этом случае *квадратичной формой* называют отображение Q пространства E в K, удовлетворяющее тождеству вида

$$Q(\lambda x + \mu y) = \lambda^2 Q(x) + \mu^2 Q(y) + \lambda\mu f(x, y), \qquad (33)$$

где f — билинейная форма на $E \times E$. Эта форма однозначно определяется по Q, поскольку из (33) вытекает, что

$$f(x, y) = Q(x + y) + Q(x) + Q(y). \qquad (34)$$

Кроме того, $Q(\lambda x) = \lambda^2 Q(x)$ и, следовательно, $f(x, x) = 0$; таким образом, f — *знакопеременная* форма. Пусть $2p \leqslant n$ — ранг формы f и E^0 есть $(n - 2p)$-мерное подпространство, ортогональное к E. Если обозначить через h ограничение формы Q на E^0, то при $x \in E^0$, $y \in E^0$ имеем

$$h(\lambda x + \mu y) = \lambda^2 h(x) + \mu^2 h(y). \qquad (35)$$

Отображение $\xi \to \xi^2$ является изоморфизмом поля K на подполе K^2; формула (35) означает, что h есть *полулинейное* отображение векторного пространства E^0 над полем K в векторное пространство K над полем K^2 относительно изоморфизма $\xi \to \xi^2$. Следовательно, ядро F отображения h есть q-мерное подпространство пространства E^0, где $q \leqslant n-2p$, а его образ $M = h(E^0)$ есть подпространство пространства K (над K^2) размерности $n-2p-q=d$. Ясно, что $d \leqslant [K:K^2]$; в частности, если поле K *совершенно* (т. е. $K=K^2$), то $d=0$ или $d=1$. Число $n-q$ называется *рангом* формы Q. Пусть U есть $2p$-мерное подпространство, дополнительное к E^0 в E, и V есть d-мерное подпространство, дополнительное к F в E^0. Если $(e_i)_{1 \leqslant i \leqslant 2p}$ — симплектический базис пространства U (относительно формы f), $(e_i)_{2p+1 \leqslant i \leqslant 2p+d}$ — какой-нибудь базис пространства V и $(e_i)_{2p+d+1 \leqslant i \leqslant n}$ — какой-нибудь базис пространства F, то форма $Q(x)$ при $x = \sum_{i=1}^{n} e_i\xi_i$ записывается в виде $\sum_{i=1}^{p} (\alpha_i\xi_i^2 + \beta_i\xi_i\xi_{p+i} + \gamma_i\xi_{p+i}^2) + \sum_{i=2p+1}^{2p+d} \delta_i\xi_i^2$, причем соотношение $\sum_{i=2p+1}^{2p+d} \delta_i\xi_i^2 = 0$ влечет за собой $\xi_i = 0$ при $2p+1 \leqslant i \leqslant 2p+d$. Мы будем говорить, что форма Q *невырожденна*, если $q=0$; число $d=n-2p$ в этом случае называется *дефектом* формы Q, и, если $d>0$, форма Q называется *дефектной* (что всегда имеет место, если пространство E нечетномерно). Начиная с этого места, мы будем предполагать, что форма Q *невырожденна*. Ее ограничение на любом подпространстве U, дополнительном к E^0, *недефектно*.

Ненулевой вектор $x \in E$ называется *особым*, если $Q(x)=0$. Подпространство V пространства E называется *особым*, если $Q(x)=0$ при всех $x \in V$. Так как $Q(x) \neq 0$ для любого ненулевого вектора из E^0, то для любого особого подпространства V имеем $V \cap E^0 = \{0\}$, так что V содержится в некотором подпространстве E_1, дополнительном к E^0. В силу формулы (34) V *вполне изотропно* по отношению к форме f и, следовательно,

$\dim V \leqslant p$. *Индексом* формы Q называется максимальная размерность ν *особых* подпространств пространства E. Из предыдущего следует, что $\nu \leqslant p$ и что можно выбрать дополнительное к E^0 подпространство E_1, содержащее особое подпространство максимальной размерности ν. Предположим отныне, что такое подпространство E_1 выбрано раз и навсегда; *ортогональность* в E_1 будет всегда пониматься в смысле знакопеременной формы f. Имеет место лемма, аналогичная первой лемме § 11: *для всякого особого вектора $a \in E_1$ и неизотропной плоскости P, содержащей a, в плоскости P существует единственный особый вектор b, такой, что* $f(a, b) = 1$. В самом деле, если $f(a, c) \neq 0$, то условие $Q(c + a\xi) = 0$ записывается в виде $f(a, c)\xi + Q(c) = 0$. Из этой леммы следует, что утверждения 1) и 2) § 11 будут справедливы, если заменить E на E_1 и слова «изотропный» и «вполне изотропный» — на «особый». Заметим также, что если $V \subset E_1$ — особое подпространство и W — особое подпространство, содержащееся в V^0 (ортогональном дополнении к V *в* E_1), то $V + W$ — также особое подпространство; следовательно, если V имеет максимальную размерность ν, то всякий особый вектор, содержащийся в V^0, принадлежит V.

Если E и F — векторные пространства одинаковой размерности над K и u — изоморфизм F на E, то функция $x \to Q(u(x))$ на пространстве F, очевидно, является квадратичной формой. Говорят, что эта форма получается *перенесением* формы Q посредством изоморфизма u. Соответствующая знакопеременная форма получается перенесением формы f посредством u. Две квадратичные формы называются *эквивалентными*, если они получаются одна из другой перенесением; в этом случае они имеют одинаковый ранг и индекс, а ассоциированные с ними знакопеременные формы имеют одинаковый ранг.

Проблема эквивалентности решена лишь в небольшом числе случаев. Мы ограничимся рассмотрением невырожденных форм. Если поле K *алгебраически замкнуто*, то $p = \nu$, поскольку квадратное уравнение всегда имеет решение в K. Кроме того, $d = 0$ или 1. Поэтому существует такой базис $(e_i)_{1\leqslant i\leqslant n}$ пространства E, что

$$Q(x)=\xi_1\xi_{p+1}+\ldots+\xi_p\xi_{2p},\qquad \text{если}\quad n=2p,$$
$$Q(x)=\xi_1\xi_{p+1}+\ldots+\xi_p\xi_{2p}+\xi_{2p+1}^2,\qquad \text{если}\quad n=2p+1.$$

Если $K=\mathbf{F}_q$ $(q=2^s)$, то всегда существует такой базис (e_i) пространства E, что

$$Q(x)=\xi_1\xi_{p+1}+\ldots+\xi_p\xi_{2p}+\xi_{2p+1}^2,\qquad \text{если}\quad n=2p+1,$$
$$Q(x)=\xi_1\xi_{p+1}+\ldots+\xi_{p-1}\xi_{2p-2}+$$
$$+\left(\alpha\xi_p^2+\xi_p\xi_{2p}+\alpha\xi_{2p}^2\right),\qquad \text{если}\quad n=2p,$$

где во втором случае $\alpha=0$ или α таково, что полином $\alpha X^2+X+\alpha$ неприводим над K (Диксон [1], стр. 197—199). В первом случае $d=1$, $\nu=p$; во втором случае $d=0$, $\nu=p$ или $\nu=p-1$, если $\alpha=0$ или $\alpha\neq 0$ соответственно.

О других результатах по проблеме эквивалентности см. Арф [1].

Ортогональным полуподобием относительно квадратичной формы Q называется коллинеация u пространства E, удовлетворяющая условию

$$Q(u(x))=r_u(Q(x))^{\sigma}\quad \text{для всех}\quad x\in E, \tag{36}$$

где $\sigma=\sigma_u$ — автоморфизм поля K, соответствующий коллинеации u, а $r_u\in K^*$ называется *множителем* u. Формула (34) показывает, что, если форма Q не дефектна, u является *симплектическим* полуподобием с тем же множителем. Ортогональные полуподобия образуют подгруппу в группе $\Gamma L_n(K)$, обозначаемую через $\Gamma O_n(K, Q)$. Преобразования, принадлежащие нормальному делителю $GO_n(K, Q)=\Gamma O_n(K, Q)\cap GL_n(K)$, называются *подобиями* (относительно Q), а подобия с множителем 1 — *ортогональными преобразованиями*. Ортогональные преобразования образуют нормальный делитель $O_n(K, Q)$ в группе $GO_n(K, Q)$, называемый *ортогональной группой* (относительно Q). Отображение $u\to\sigma_u$ является гомоморфизмом группы $\Gamma O_n(K, Q)$ на подгруппу группы автоморфизмов поля K; ядром этого гомоморфизма служит группа $GO_n(K, Q)$. Отображение

$u \to r_u$ является гомоморфизмом группы $GO_n(K, Q)$ на подгруппу мультипликативной группы K^*; его ядром служит группа $O_n(K, Q)$. Очевидно, что $Z_n = H_n \subset \subset GO_n(K, Q)$, причем множитель гомотетии $x \to x\gamma$ равен γ^2. Образы $P\Gamma O_n(K, Q)$ и $PGO_n(K, Q)$ групп ΓO_n и GO_n в проективной группе $P\Gamma L_n(K)$ изоморфны соответственно $\Gamma O_n/Z_n$ и GO/Z_n. Далее, $Z_n \cap O_n = \{1\}$ и, следовательно, группа O_n изоморфна проективной группе PO_n, являющейся ее образом в $P\Gamma L_n$.

Ортогональные группы, соответствующие двум эквивалентным квадратичным формам, изоморфны. Для любого $\alpha \in K^*$ имеем $\Gamma O_n(K, \alpha Q) = \Gamma O_n(K, Q)$, $GO_n(K, \alpha Q) = GO_n(K, Q)$ и $O_n(K, \alpha Q) = O_n(K, Q)$.

Если u — ортогональное преобразование, то легко видеть, что $u(E^0) = E^0$ и что ограничение u на E^0 *тождественно* (потому что равенство $Q(u(x)) = Q(x)$, если $x \in E^0$, можно записать в виде $Q(u(x) - x) = 0$). Следовательно, u однозначно определяется своим ограничением на E_1. При $x \in E_1$ положим $u(x) = u_1(x) + u_2(x)$, где $u_1(x) \in E_1$, $u_2(x) \in E^0$. Ясно, что преобразование u_1 должно принадлежать *симплектической группе* $Sp_{2p}(K)$; кроме того, оно должно быть таким, чтобы $Q(u_1(x)) + Q(x) \in M$ *при любом* $x \in E_1$. Обратно, если u_1 обладает этими двумя свойствами, то существует единственное отображение u_2, для которого $u_1 + u_2 \in O_n(K, Q)$ (Дьёдонне [4], стр. 53—54). Группа $O_n(K, Q)$ может рассматриваться, таким образом, как *подгруппа группы* $Sp_{2p}(K)$, *образованная такими преобразованиями* v, *что* $Q(v(x)) + Q(x) \in M$ *при всех* $x \in E_1$. Если форма Q недефектна, то это последнее условие сводится, очевидно, к тому, что $Q(v(x)) = Q(x)$.

Если K — *совершенное* поле, то невырожденная форма Q недефектна, если n четно, и имеет дефект 1, если n нечетно. В последнем случае группа $O_n(K, Q)$ *совпадает* с симплектической группой $Sp_{2p}(K)$.

Для случая, когда форма Q *недефектна*, Арф [1] получил следующее обобщение теоремы Витта:

Для того чтобы существовало такое ортогональное преобразование $u \in O_n(K, Q)$, что $u(V) = W$, необходимо и достаточно, чтобы ограничения формы Q на V и W были эквивалентны.

Доказательство теоремы Витта, принадлежащее Шевалле (§ 11), применимо к данному случаю со следующими модификациями. Прежде всего в условиях (А) нужно заменить $f(z, z) = f(z', z')$ на $Q(z) = Q(z')$. Затем в конце доказательства следует заметить, что поскольку $f(a, a) = 0$, то $f(a, b) = f(a, b - a) = 0$, откуда $Q(b - a) = Q(b) + Q(a) = 0$ в силу сделанного предположения. Тогда условие $Q(z + c + (b - a)\xi) = Q(z)$ сводится к уравнению

$$\alpha\xi = Q(z + c) + Q(z),$$

из которого определяется ξ, поскольку $\alpha \neq 0$.

Из этого результата немедленно вытекает, что утверждения 3), 4) и 5) § 11 остаются справедливыми, если заменить слова «вполне изотропный» на «особый».

Сдвиг в ортогональной группе $O_n(K, Q)$ (рассматриваемой как подгруппа симплектической группы $Sp_{2p}(K)$) есть симплектический сдвиг $x \to x + \lambda f(x, a) a$, где вектор a должен быть изотропен; условие ортогональности приводит к тому, что $\lambda + \lambda^2 Q(a) \in M$.

§ 17. Обобщения

Часть определений, данных в этой главе, распространяется на случай, когда K есть коммутативное кольцо A, а E — свободный модуль конечного типа над A. В частности, на этот случай переносятся понятия ортогональной и унитарной групп. Изучение этих групп существенно зависит от природы кольца A. Существенные результаты имеются только в случае, когда A — *локальное* кольцо или кольцо целых элементов поля алгебраических чисел. Мы не можем углубляться в эти вопросы и отсылаем читателя к следующей литературе: Эйхлер [2], Клингенберг [1], [2], Лакруа [1], Реге [1], Рим [2], [3], [4], О'Мира и Поллак [1], [2], Поллак [3], [4], Борель [1], Райнер [1], [2], Хуа и Райнер [1], [2], [3], Ландин и Райнер [1], [2], [3] [1]).

[1]) См. также О'Мира [7*]. — *Прим. перев.*

Глава II

СТРУКТУРА КЛАССИЧЕСКИХ ГРУПП

§ 1. Центр и коммутант группы $GL_n(K)$

Рассмотрим n-мерное векторное пространство E над K. Всякая коллинеация u пространства E, перестановочная со всеми линейными преобразованиями, перестановочна, в частности (при $n > 1$), со сдвигами (гл. I, § 2), и, следовательно, каждая прямая пространства E инвариантна относительно нее. Выбрав какой-нибудь базис пространства E, легко доказать, что u — гомотетия. Это показывает, что *централизатор* группы $GL_n(K)$ в $\Gamma L_n(K)$ совпадает с группой H_n гомотетий. При $n = 1$ это утверждение тривиально.

При $n \geqslant 2$ *специальной линейной группой*, или *унимодулярной группой* (от n переменных над телом K) называют подгруппу $SL_n(K)$ группы $GL_n(K)$, порожденную сдвигами. Очевидно, что это нормальный делитель. *Группа $SL_n(K)$ совпадает с коммутантом группы $GL_n(K)$, кроме случая, когда $n = 2$ и тело K есть поле $\mathbf{F}_2$ из двух элементов* (Дьёдонне [1]). Доказательство этого факта проводится в несколько этапов.

а) Отождествляя группу $GL_n(K)$ с группой обратимых матриц порядка n, начнем с того, что представим всякую матрицу A в виде произведения сдвигов и растяжения. Для этого обозначим через I единичную матрицу и через E_{ij} — матрицу, у которой все элементы, кроме стоящего в i-й строке в j-м столбце, равны нулю, а этот элемент равен 1. Тогда $B_{ij}(\lambda) = I + \lambda E_{ij}$ $(i \neq j)$ будет матрицей сдвига, а $D(\mu) = I + (\mu - 1) E_{nn}$ — матрицей растяжения. Матрица $B_{ij}(\lambda) A$ получается из A прибавлением к i-й строке j-й строки, умноженной слева на λ. Если $P_{ij} = B_{ij}(1) B_{ji}(-1) B_{ij}(1)$, то матрица $P_{ij}A$ получается из A заменой i-й строки на j-ю и j-й строки на i-ю, умноженную на -1. Используя эти замечания, легко представить всякую обратимую матрицу A в виде $A = BD(\mu)$, где $B \in SL_n(K)$ — матрица, являющаяся произведением некоторого числа матриц $B_{ij}(\lambda)$ (такое разложение, конечно, неоднозначно; см. Диксон [1]). Заметим мимоходом, что если тело K коммутативно, то минимальное число членов в разложении произвольного преобразования из $SL_n(K)$ в произведение сдвигов равно n, если данное преобразование не есть гомотетия, и $n+1$ в противном случае (Дьёдонне [19]).

b) Покажем, далее, что группа $SL_n(K)$ в любом случае содержит коммутант группы $GL_n(K)$, т. е. что группа GL_n/SL_n *абелева*. Как легко видеть, для любой матрицы B, являющейся произведением некоторого числа матриц $B_{ij}(\lambda)$, имеет место равенство $D(\mu)B = B'D(\mu)$, где $B' \in SL_n$. Поэтому из a) следует, что достаточно проверить включение $D(\lambda\mu\lambda^{-1}\mu^{-1}) \in SL_n(K)$. Поскольку $D(\lambda\mu\lambda^{-1}\mu^{-1}) = D(\lambda)(D(\mu\lambda\mu^{-1}))^{-1}$, достаточно доказать, что два растяжения, принадлежащие к одному классу сопряженности (гл. I, § 2), *сопряжены в группе* $SL_n(K)$. Это легко выводится из следующих двух замечаний:

1°. Для любых двух ненулевых векторов a, b пространства E существует линейное преобразование, являющееся сдвигом или произведением двух сдвигов и переводящее a в b.

2°. Для любых двух гиперплоскостей H_1, H_2 и для любого вектора a, не принадлежащего ни H_1, ни H_2, существует сдвиг, оставляющий на месте a и переводящий H_1 в H_2.

c) Поскольку любые два сдвига сопряжены в группе $GL_n(K)$, всякий гомоморфизм θ этой группы на абелеву группу переводит все сдвиги в один элемент σ. Так как $B_{12}(\lambda)B_{12}(\mu) = B_{12}(\lambda+\mu)$, то $\sigma^2 = \sigma$ и, значит, $\sigma = 1$, если только в K существует два таких элемента λ, $\mu \neq 0$, что $\lambda + \mu \neq 0$; это условие всегда выполняется, если $K \neq \mathbf{F}_2$. Если $K = \mathbf{F}_2$ и $n > 2$, то сдвиги вдоль гиперплоскости H образуют (вместе с тождественным преобразованием) группу $T(H)$, изоморфную K^{n-1} (гл. I, § 2) и, следовательно, содержащую более двух элементов. Рассматривая в этом случае образ при гомоморфизме θ произведения двух сдвигов из $T(H)$, отличных от единицы, получаем опять-таки, что $\sigma^2 = \sigma$. Случай, когда $n=2$ и $K=\mathbf{F}_2$, — особый. В этом случае нет растяжений, отличных от тождественного, и, следовательно, $GL_2(\mathbf{F}_2)=SL_2(\mathbf{F}_2)$; группа $GL_2(\mathbf{F}_2)$ изоморфна симметрической группе $\mathfrak{S}_3$ и, будучи разрешимой, не совпадает со своим коммутантом.

Если тело K коммутативно и содержит по меньшей мере 4 элемента, то всякое преобразование $u\in SL_n(K)$ является *коммутатором* $vwv^{-1}w^{-1}$ двух элементов этой группы, кроме, быть может, того случая, когда u — гомотетия и характеристика поля K равна 0 (Томсон [1], [2], [3]).

Обозначим через C коммутант мультипликативной группы K^*. При $n\geqslant 2$ *факторгруппа* $GL_n(K)/SL_n(K)$ *изоморфна абелевой группе* K^*/C (Дьёдонне [1]). В случае когда K коммутативно, эта теорема немедленно следует из существования определителя, осуществляющего гомоморфизм группы $GL_n(K)$ на K^*. В общем случае поступают так же, определяя для всякой обратимой матрицы A порядка n элемент $\det(A)$ *группы* K^*/C, называемый по-прежнему *определителем матрицы* A, таким образом, что отображение $A\to\det(A)$ является гомоморфизмом группы $GL_n(K)$ *на* K^*/C с ядром $SL_n(K)$. Построение $\det(A)$ проводится индукцией по n. Пусть φ — каноническое отображение группы K^* на K^*/C. Если $A=(a_{ij})$ и $a_{i1}\neq 0$, то обозначим через A' матрицу, получаемую из A вычитанием из строк с номерами $j\neq i$ подходящих кратных i-той строки таким образом, чтобы все элементы первого столбца, кроме a_{i1}, *стали равными* 0. Положим $\det(A)=\varphi((-1)^{i+1}a_{i1})\det(A'_{i1})$, где A'_{i1} — матрица, получаемая из A' вычеркиванием первого столбца и i-той строки. Индукцией по n доказывается, что это определение не зависит от выбора индекса i (такого, что $a_{i1}\neq 0$), что значение $\det(A)$ не изменяется при переходе от A к $B_{ij}(\lambda)A$ и, наконец, что $\det(A)$ умножается на $\varphi(\mu)$ при умножении какой-либо строки матрицы A слева на μ (подробное доказательство см. у Артина [3]). Для матрицы $A=BD(\mu)$, где B — произведение матриц $B_{ij}(\lambda)$, из этих свойств определителя следует, что $\det(A)=\varphi(\mu)$. Отсюда в свою очередь немедленно следует, что отображение $X\to\det(X)$ является гомоморфизмом на K^*/C с ядром $SL_n(K)$.

Из предыдущего следует также, что если V и W — два подпространства одинаковой размерности в E, то существует такое преобразование $u \in SL_n(K)$, что $u(V) = W$.

§ 2. Структура группы $SL_n(K)$

Рассуждение, проведенное в начале § 1, позволяет также утверждать, что централизатор группы $SL_n(K)$ в $\Gamma L_n(K)$ совпадает с группой H_n гомотетий. *Центром* группы $SL_n(K)$ является, следовательно, группа $SL_n(K) \cap Z_n$, образованная центральными гомотетиями $x \to x\gamma$, определитель которых (в смысле § 1) есть единичный элемент группы K^*/C, т. е. γ^n принадлежит коммутанту C группы K^*. Факторгруппа группы $SL_n(K)$ по центру изоморфна ее образу $PSL_n(K)$ при каноническом гомоморфизме в полную проективную группу $PGL_n(K)$. Группа $PSL_n(K)$ называется *специальной*, или *унимодулярной*, *проективной группой* (от n переменных над телом K).

Структура группы $PSL_n(K)$ выясняется следующей теоремой: *при $n \geqslant 2$ группа $PSL_n(K)$ проста, за исключением случая, когда $n = 2$ и $K = \mathbf{F}_2$ или $\mathbf{F}_3$* (Диксон [1], Ивасава [1], Абе [1], Дьёдонне [1], Хуа [8]).

Изложенный ниже способ доказательства принадлежит Ивасаве [1] и опирается на следующие леммы из теории групп, где Γ обозначает группу перестановок множества E.

1) *Если Γ по меньшей мере дважды транзитивна, то она примитивна.*

2) *Всякий нормальный делитель $\neq \{e\}$ примитивной группы перестановок транзитивен.*

3) *Если N — транзитивная подгруппа группы Γ, то для всякого $x \in E$ имеет место равенство $\Gamma = NS_x$, где S_x — стационарная подгруппа элемента x.*

Это классические леммы.

4) *Предположим, что группа Γ примитивна и удовлетворяет следующим условиям:*

a) *Γ совпадает со своим коммутантом;*

b) *для всякого $x \in E$ стационарная подгруппа S_x содержит абелеву подгруппу H_x, являющуюся нормальным* *делителем в S_x и такую, что сопряженные к ней подгруппы sH_xs^{-1} $(s \in \Gamma)$ порождают Γ.*

Тогда группа Γ проста.

В самом деле, пусть N — нормальный делитель группы Γ, отличный от $\{e\}$. Всякий элемент $s \in \Gamma$ может быть представлен в виде $\prod_{i=1}^{n} s_i h_i s_i^{-1}$, где $h_i \in H_x$, и, согласно леммам 2) и 3), $s_i = t_i u_i$, где $t_i \in N$, $u_i \in S_x$. Пользуясь тем, что H_x — нормальный делитель в S_x, получаем $s = t'h'$, где $t' \in N$ и $h' \in H_x$. Таким образом, $\Gamma = NH_x$. Так как N — нормальный делитель, а группа H_x абелева, то отсюда легко выводится, что коммутант группы Γ содержится в N и, следовательно, $N = \Gamma$, что и доказывает утверждение леммы.

Чтобы применить эти леммы, заметим, что группа $PSL_n(K)$ *по меньшей мере дважды транзитивна* (в действительности, в точности дважды транзитивна, если только $n > 2$) в проективном пространстве $P_{n-1}(K)$ при $n \geqslant 2$, поскольку две пары различных прямых в K^n всегда могут быть преобразованы одна в другую преобразованием из группы $SL_n(K)$. Согласно 1), отсюда следует, что группа $PSL_n(K)$ *примитивна*, и остается проверить условия a) и b) леммы 4). Займемся вначале условием b). Пусть $z \in P_{n-1}(K)$ и $a \in K^n$ — вектор, канонический образ которого есть z. Возьмем в качестве H_z канонический образ подгруппы сдвигов вида $x \to x + a\rho(x)$. Так как $tH_zt^{-1} = H_{t(z)}$ для всякого $t \in PSL_n(K)$ и группа PSL_n транзитивна, то H_z удовлетворяет условиям b). (Напомним, что по определению группа $SL_n(K)$ порождается сдвигами.) Остается доказать, что группа $SL_n(K)$ в рассматриваемых случаях *совпадает со своим коммутантом.* Для этого достаточно проверить, что *всякий сдвиг является коммутатором* в группе $SL_n(K)$. Более того, поскольку любые два сдвига сопряжены в группе $GL_n(K)$, а группа $SL_n(K)$ является нормальным делителем в группе $GL_n(K)$, достаточно проверить, что какой-нибудь один сдвиг t является коммутатором в $SL_n(K)$. Если $n \geqslant 3$, возьмем в качестве t сдвиг вдоль гиперплоскости $H = \sum_{i \neq 3} e_i K$ в направлении вектора $a = e_1 - e_2$, нормированный так, чтобы $t(e_3) = e_3 + a$

(здесь (e_i) — базис пространства K^n). Пусть тогда t_1 — сдвиг вдоль гиперплоскости H в направлении вектора e_1, нормированный так, чтобы $t_1(e_3) = e_3 + e_1$, и s — преобразование из $SL_n(K)$, определяемое равенствами $s(e_1) = e_2$, $s(e_2) = -e_1$ и $s(e_i) = e_i$ при $i \geqslant 3$. Непосредственно проверяется, что $t = t_1 s t_1^{-1} s^{-1}$. Если $n = 2$, достаточно рассмотреть матрицу $B_{12}(\lambda)$ при $\lambda \neq 0$. Пусть $A = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}$. Тогда $AB_{12}(1)A^{-1}B_{12}(-1) = B_{12}(\mu^2 - 1)$. Единственными телами, в которых $\mu^2 = 1$ при всех $\mu \in K^*$, являются $\mathbf{F}_2$ и $\mathbf{F}_3$.

Остается изучить особые случаи $K = \mathbf{F}_2$ и $K = \mathbf{F}_3$. Вообще, порядок группы $GL(\mathbf{F}_q)$ равен

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}).$$

В самом деле, это есть число базисов пространства $\mathbf{F}_q^n$. Группа GL_n/SL_n, изоморфная $\mathbf{F}_q^*$, содержит $q - 1$ элементов; отсюда следует, что порядок группы $SL_n(\mathbf{F}_q)$ равен

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{n-2})\, q^{n-1}.$$

Центр группы $SL_n(\mathbf{F}_q)$, изоморфный подгруппе группы $\mathbf{F}_q^*$, образованной корнями n-й степени из единицы, есть циклическая группа порядка d, где d — наибольший общий делитель чисел $q - 1$ и n. Следовательно, порядок группы $PSL_n(\mathbf{F}_q)$ равен

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{n-2})\, q^{n-1}/d.$$

В частности, $PSL_2(\mathbf{F}_2)$ есть группа порядка 6 и $PSL_2(\mathbf{F}_3)$ — группа порядка 12. Обе эти группы разрешимы (см. также гл. IV § 8). За этими двумя исключениями, группы $PSL_n(\mathbf{F}_q)$ образуют последовательность (зависящую от двух параметров n, q, где q — степень простого числа) *простых конечных групп* (см. Диксон [1], стр. 309—310).

Заметим, что рассуждения, проведенные в этом параграфе, показывают также, что всякий нормальный делитель группы $GL_n(K)$, не содержащийся в ее центре Z_n, *содержит* унимодулярную группу $SL_n(K)$, кроме, может быть, тех случаев, когда группа $PSL_n(K)$ не проста. Заметим также, что при $n \geqslant 3$ любые два сдвига сопряжены *в группе* $SL_n(K)$. В самом деле, они сопряжены в $GL_n(K)$, и легко видеть, что для любого сдвига u существует преобразование из GL_n, перестановочное с u и имеющее *произвольный* определитель (см. гл. I, § 2). Напротив, при $n = 2$ не всякие два сдвига сопряжены *в* $SL_2(K)$. Можно показать, что классы сопряженных сдвигов в $SL_2(K)$ взаимно однозначно соответствуют элементам группы K^*/K^{*2}, где K^{*2} обозначает мультипликативную группу, порожденную *квадратами* элементов группы K^*.

§ 3. Образующие и центр унитарной группы

В дальнейшем, когда будет идти речь об унитарных группах $U_n(K, f)$, симплектические и ортогональные группы (последние — над полем характеристики $\neq 2$) будут подразумеваться как частные случаи, если не оговорено противное. Всегда будем предполагать, что $n \geqslant 2$ и, в случае когда характеристика K равна 2, что f есть T-форма.

Если унитарная группа $U_n(K, f)$ не является симплектической группой (иными словами, если f — не знакопеременная форма), то она *порождается квазиотражениями* (гл. I, § 12), *за исключением группы* $U_2(\mathbf{F}_4)$ (Дьёдонне [16]). Доказательство проводится индукцией по n. При $u \in U_n$ для любого неизотропного вектора $x \in E$ хотя бы один из векторов $u(x) - x$, $u(x) + x$ (если характеристика K не равна 2) неизотропен, и существует квазиотражение относительно гиперплоскости, ортогональной этому вектору, преобразующее x в $u(x)$ или $-u(x)$. Во втором случае другое квазиотражение преобразует $-u(x)$ в $u(x)$. Таким образом, всегда существует такое произведение s квазиотражений, что преобразование $s^{-1}u$ оставляет на месте вектор x и поэтому может рассматриваться как унитарное преобразование в гиперплоскости, ортогональной x. Применяя предположение индукции, получаем требуемое утверждение. Случай, когда характеристика тела K равна 2, требует более тонкого исследования. Можно, далее, показать, что всякий элемент ортогональной группы $O_n(K, f)$ есть произведение не более чем n отражений (Э. Картан [2], Дьёдонне [4], Шерк [1]); всякий элемент произвольной группы $U_n(K, f)$, за исключением, само собой разумеется, группы $U_2(\mathbf{F}_4)$, есть произведение не более чем $n+1$ квазиотражений (Дьёдонне [19]), причем эта оценка является точной.

Коммутант C группы K^*, очевидно, инвариантен (в целом) относительно антиавтоморфизма J тела K, и тем самым J индуцирует инволютивный автоморфизм (который мы также будем обозначать через J) фактор-группы K^*/C. Из предыдущего результата легко вывести, что определитель (см. § 1) всякого преобразования из унитарной группы, не являющейся ортогональной, имеет вид $\gamma^J\gamma^{-1}$, где $\gamma \in K^*/C$ [1]). Что касается ортогональных групп, то легко видеть, что определитель любого преобразования из этих групп равен $+1$ или -1.

Всякое преобразование из $\Gamma L_n(K)$, принадлежащее централизатору унитарной группы $U_n(K, f)$, перестановочно, в частности, со всеми квазиотражениями и, следовательно, сохраняет (в целом) всякую неизотропную гиперплоскость. Оно перестановочно также со всеми унитарными сдвигами, если такие сдвиги существуют, и сохраняет всякую изотропную прямую. Отсюда вытекает, что если группа U_n не является ортогональной, то ее централизатор совпадает с группой гомотетий H_n, а ее центр есть группа $U_n \cap Z_n$, состоящая из центральных гомотетий $x \to x\gamma$, для которых $\gamma^J\gamma = 1$.

Что касается ортогональной группы $O_n(K, f)$, то ее централизатор также совпадает с H_n при $n \geqslant 3$. Это вытекает из изложенных выше соображений и из следующей леммы:

1) *При $n \geqslant 3$ всякая изотропная прямая пространства E является пересечением двух неизотропных плоскостей.*

В самом деле, если x — изотропный вектор, y — вектор, ортогональный к x и не коллинеарный ему, и z — неизотропный вектор, не ортогональный к x, то плоскость, натянутая на векторы x и z, и плоскость, натянутая на векторы x и $y+z$, удовлетворяют поставленным требованиям.

---

[1]) В частности, определитель всякого преобразования из симплектической группы равен 1 (см. § 5). — *Прим. перев.*

Остается рассмотреть группы $O_2(K, f)$. Пусть (e_1, e_2) — ортогональный базис пространства E. Если поле K (характеристика которого $\neq 2$) содержит более 3 элементов, то существует такой элемент $\alpha \in K^*$, что вектор $e_1 + e_2\alpha$ неизотропен. Преобразование $u \in \Gamma L_2$, принадлежащее централизатору группы O_2, должно сохранять прямую, содержащую вектор $e_1 + e_2\alpha$, а также оси координат. Следовательно, $u(e_1) = e_1\gamma_1$, $u(e_2) = e_2\gamma_2$ и $\alpha^\sigma = \alpha\mu$, где $\mu = \gamma_1\gamma_2^{-1}$ (здесь σ — автоморфизм поля K, соответствующий преобразованию u). Заметим теперь, что имеется не более двух значений α, при которых вектор $e_1 + e_2\alpha$ изотропен. Если K^* содержит хотя бы 6 элементов, то существуют два элемента $\alpha, \beta \in K^*$, такие, что векторы $e_1 + e_2\alpha$, $e_1 + e_2\beta$, $e_1 + e_2\alpha\beta$ неизотропны. Из равенств $\alpha^\sigma = \alpha\mu$, $\beta^\sigma = \beta\mu$ и $(\alpha\beta)^\sigma = (\alpha\beta)\mu$ следует, что $\mu = 1$ и $\alpha^\sigma = \alpha$ для всех элементов $\alpha \in K^*$, кроме, быть может, двух. Однако, если σ не есть тождественный автоморфизм, то подгруппа элементов из K^*, инвариантных относительно σ, содержит не более половины всех элементов группы K^*. Значит, если K содержит не менее 7 элементов, то σ тождествен, а u — гомотетия. Это же сраведливо и для $K = \mathbf{F}_5$, ибо поле $\mathbf{F}_5$ не допускает нетождественного автоморфизма. Для $K = \mathbf{F}_3$ следует различать два случая: $f(e_1, e_1) = f(e_2, e_2)$ и $f(e_1, e_1) = -f(e_2, e_2)$. В первом случае индекс ν формы f равен 0, изотропных векторов нет и, следовательно, u — гомотетия. Во втором случае, напротив, $\nu = 1$, оси координат суть единственные неизотропные прямые пространства E и $O_2(\mathbf{F}_3, f)$ является абелевой группой порядка 4 (прямым произведением двух циклических групп порядка 2), совпадающей со своим собственным централизатором в группе $\Gamma L_2(\mathbf{F}_3) = GL_2(\mathbf{F}_3)$.

В случае когда $\nu \geqslant 1$, мы будем называть *гиперболической плоскостью* неизотропную плоскость, содержащую хотя бы один изотропный вектор. В любой гиперболической плоскости существуют два изотропных вектора a, b, образующих базис этой плоскости и удовлетворяющих условию $f(a, b) = 1$. Если U_n — ортогональная группа, то в такой плоскости имеется только две изотропные прямые; в остальных случаях, напротив, имеется по меньшей мере *три* такие прямые. Мы будем называть преобразование $u \in U_n$ *гиперболическим*, если оно оставляет на месте все векторы $(n-2)$-мерного подпространства, ортогонального к некоторой гиперболической плоскости.

2) *Если* $\nu = 1$, *то всякое преобразование из* $U_n(K, f)$ *есть произведение гиперболических преобразований.* Это очевидно при $n = 2$. Если $n > 2$ и f — не знакопеременная форма, то достаточно заметить, что всякое квазиотражение s относительно (неизотропной) гиперплоскости H есть гиперболическое преобразование. В самом деле, пусть a — ненулевой вектор, ортогональный к H. Существует изотропный вектор b, не ортогональный к a (см. гл. I, § 11, п. 2)). Плоскость P, натянутая на векторы a и b, гиперболическая, и преобразование s оставляет на месте все векторы из P^0. Тем самым s — гиперболическое преобразование. Что касается симплектической группы $Sp_n(K)$, то для нее утверждение вытекает из того факта, что она порождается симплектическими сдвигами (см. § 5).

3) *При* $\nu \geqslant 1$ *и* $n \geqslant 3$ *всякая неизотропная прямая есть пересечение двух гиперболических плоскостей, кроме того случая, когда* $U_n(K, f)$ *есть ортогональная группа* $O_3(\mathbf{F}_3, f)$. В самом деле, если x — неизотропный вектор, то существует изотропный вектор y, не ортогональный к x (см. гл. I, § 11, п. 2)). Пусть z — вектор, ортогональный к x, но не ортогональный к y и не лежащий в плоскости P, проходящей через x и y. Тогда плоскость Q, содержащая y и z, является гиперболической. Если U_n — не ортогональная группа, то плоскость Q содержит хотя бы один изотропный вектор y', не коллинеарный ни y, ни z и, следовательно, не ортогональный к x. Плоскость P', содержащая x и y', отлична от P. Прямая, содержащая x, есть пересечение плоскостей P и P'. Если U_n — ортогональная группа, отличная от указанной выше исключительной группы, то всегда можно выбрать вектор z неизотропным, и далее рассуждать таким же способом.

§ 4. Структура группы $U_n(K, f)$

(f есть T-форма индекса $\geqslant 1$; ортогональные группы не рассматриваются.)

I. Группа $T_n(K, f)$

При изучении структуры унитарных групп важно различать два случая: когда $\nu \geqslant 1$ и когда $\nu = 0$ (см. § 12). *В этом и следующем параграфах мы будем всегда предполагать, что* $\nu \geqslant 1$. Поскольку мы исключаем ортогональные группы, в группе $U_n(K, f)$ есть унитарные сдвиги. Мы будем считать форму f *косоэрмитовой*, что не приводит к ограничению общности (см. гл. I, § 6). При этом предположении унитарный сдвиг имеет вид $x \to x + a\lambda f(a, x)$, где a — изотропный вектор и λ — симметричный элемент тела K (гл. I, § 12). Обозначим через $T_n(K, f)$ нормальный делитель группы $U_n(K, f)$, *порожденный унитарными сдвигами*. Для изучения структуры группы $T_n(K, f)$ используются следующие леммы.

1) *Если тело K не коммутативно, то оно порождается множеством S симметричных элементов, за исключением того случая, когда K есть тело обобщенных кватернионов характеристики $\neq 2$, а S совпадает с его центром Z* (Дьёдонне [13]). Если K коммутативно и $J \neq 1$, то, очевидно, S есть такое подполе поля K, что K является его сепарабельным квадратичным расширением.

2) *Если a и b — два неколлинеарных изотропных вектора, то существует такое преобразование $u \in T_n$, что векторы $u(a)$ и b коллинеарны.* Пусть сначала $f(a, b) \neq 0$. Положим $\mu = (f(a, b))^{-1}$. Тогда вектор $c = a - b\mu$ изотропен и сдвиг $x \to x + cf(c, x)$ удовлетворяет поставленному условию. Пусть теперь $f(a, b) = 0$. Тогда плоскость, натянутая на a и b, вполне изотропна, так что $n \geqslant 3$, и существует такой вектор z, что $f(a, z) \neq 0$ и $f(b, z) \neq 0$. Плоскость, натянутая на a и z, гиперболична и содержит изотропный вектор a_1, не коллинеарный вектору a и, следовательно, не ортогональный к b. Так как $f(a, a_1) \neq 0$ и $f(a_1, b) \neq 0$, то доказательство сводится к первому случаю.

При $n = 2$ пространство E есть гиперболическая плоскость. В качестве ее базиса можно выбрать два изотропных вектора e_1, e_2, таких, что $f(e_1, e_2) = 1$. При таком базисе (и в обозначениях § 1) имеет место следующая лемма:

3) *Группа $T_2(K, f)$ порождается унитарными сдвигами $B_{12}(\lambda)$ и $B_{21}(\mu)$*, где λ и μ пробегают множество *симметричных* элементов тела K. Достаточно заметить, что условие изотропности вектора $x = e_1\alpha + e_2\beta$ записывается в виде $\alpha^J\beta - \beta^J\alpha = 0$, что при $\beta \neq 0$ означает симметричность элемента $\alpha\beta^{-1}$. Сдвиг $B_{12}(-\alpha\beta^{-1})$ преобразует такой вектор x в вектор, коллинеарный e_2. Следовательно, всякий сдвиг в направлении вектора x при трансформации посредством $B_{12}(-\alpha\beta^{-1})$ преобразуется в сдвиг вида $B_{21}(\lambda)$. Отсюда и следует утверждение леммы.

Эти леммы позволяют, прежде всего, установить, что *центр группы T_n есть ее пересечение $W_n = T_n \cap Z_n$ с центром группы $GL_n(K)$*. Действительно, преобразование из T_n, перестановочное с любым сдвигом из T_n, сохраняет каждую изотропную прямую и, следовательно, каждую гиперболическую плоскость. Ввиду леммы 3 из § 3 отсюда следует, что при $n \geqslant 3$ такое преобразование сохраняет каждую прямую. При $n = 2$ преобразование из центра группы T_n должно коммутировать со сдвигами $B_{12}(\lambda)$ и $B_{21}(\mu)$, откуда следует, что его матрица имеет вид $\begin{pmatrix} \alpha & 0 \\ 0 & (\alpha^{-1})^J \end{pmatrix}$, где $\alpha\lambda = \lambda(\alpha^{-1})^J$ для любого симметричного элемента λ тела K[1]. Лемма 1 показывает тогда, что α принадлежит центру тела K, за исключением, быть может, случая, когда K есть тело обобщенных кватернионов характеристики $\neq 2$, а множество S совпадает с центром Z тела K. Но в этом последнем случае элементы матриц $B_{12}(\lambda)$ и $B_{21}(\mu)$ лежат *в* Z и в силу леммы 3 элементы всех матриц из T_2 также лежат в Z; в частности, $\alpha \in Z$, откуда и следует в этом случае доказываемое утверждение.

Структура группы T_n/W_n выясняется следующими теоремами (Дьёдонне [13]; см. также Хуа [10]).

А) *Если группа T_2/W_2 проста, то группа $T_n(K, f)/W_n$ проста при $n \geqslant 3$* (для всякой T-формы f индекса $\nu \geqslant 1$). Заметим, что унитарные сдвиги, вообще говоря, не являются попарно сопряженными *в группе T_n*. Однако из

---

[1]) При $\lambda = 1$ получаем, что $\alpha = (\alpha^{-1})^J$ и, значит, $\alpha\lambda = \lambda\alpha$ для любого симметричного элемента λ. — *Прим. перев.*

леммы 2 следует, что если нормальный делитель G группы T_n содержит *все* сдвиги, соответствующие какому-либо одному вектору a, то он содержит вообще все сдвиги и, следовательно, совпадает с T_n. Поэтому достаточно проверить, что этим свойством обладает произвольный нормальный делитель G группы T_n, не содержащийся в W_n. Пусть $u \in G$, $u \notin W_n$. Существует такой изотропный вектор $x \in E$, что x и $u(x)$ не коллинеарны (иначе в силу леммы 3 § 3 преобразование u было бы гомотетией). Предположим сначала, что $f(x, u(x)) = 0$. Существует вектор z, ортогональный к $u(x)$, но не ортогональный к x. Плоскость P, содержащая x и z, будет гиперболической. В ней имеется изотропный вектор y, не коллинеарный x. Лемма 2 показывает, что существует сдвиг v, преобразующий x в $y\lambda$, причем вектор этого сдвига содержится в плоскости P. Тогда $v(u(x)) = u(x)$, так что преобразование $u_1 = vu^{-1}v^{-1}u$, принадлежащее G, переводит x в $y\lambda$. Следовательно, можно ограничиться случаем, когда $f(x, u(x)) \neq 0$. Если тогда w — сдвиг в направлении вектора x, то uwu^{-1} — сдвиг в направлении вектора $u(x)$, не коммутирующий с w (см. § 1). Обозначим через Q гиперболическую плоскость, определяемую векторами x и $u(x)$. Преобразование $u_2 = w^{-1}uwu^{-1}$ принадлежит G и оставляет на месте каждый вектор подпространства Q^0, ортогонального к плоскости Q. Его можно рассматривать как элемент группы $U_2(K, f_1)$, где f_1 — ограничение формы f на Q. С другой стороны, будучи произведением двух сдвигов из $U_2(K, f_1)$, оно принадлежит группе $T_2(K, f_1)$, но не лежит в центре этой группы, поскольку не коммутирует с w. В силу сделанного предположения отсюда следует, что G содержит все преобразования из $T_2(K, f_1)$ и, в частности, все сдвиги в направлении вектора x. Тем самым теорема доказана.

В) *Если тело K содержит более* 25 *элементов, то группа $T_2(K, f)/W_2$ проста* (для всякой T-формы f индекса $\nu \geqslant 1$). Доказательство аналогично доказательству простоты группы $PSL_2(K)$, данному в § 2. Группу T_2/W_2 следует рассмотреть как группу подстановок множества *C изотропных прямых.* Лемма 2 показывает, что эта группа транзитивна; для того чтобы доказать, что она дважды транзитивна, достаточно проверить, что сдвиги $B_{12}(\lambda)$ (где λ — симметричный элемент тела K) преобразуют прямую e_2K в любую изотропную прямую, отличную от e_1K, что очевидно. Проверка условия b) леммы 4 § 2 производится так же, как для группы $SL_n(K)$, но используется определение группы $T_n(K, f)$. Остается, таким образом, доказать, что (исключая особые случаи) группа T_2/W_2 совпадает со своим коммутантом. Из сделанного относительно K предположения вытекает в силу леммы 1, что S содержит хотя бы один элемент, отличный от 0 и ± 1. Элементарное вычисление с матрицами (Ван [1]) показывает, что всякая матрица $B_{12}(\lambda)$, где $\lambda \in S$, принадлежит коммутанту группы T_2, что завершает доказательство.

C) Предположим, что K *коммутативно*. Если $J = 1$, то всякий элемент поля K симметричен. Согласно лемме 3, группа $T_2(K, f)$ порождается матрицами $B_{12}(\lambda)$ и $B_{21}(\mu)$, где $\lambda \in K$, $\mu \in K$, и, следовательно, совпадает с *унимодулярной группой* $SL_2(K)$. Если $J \neq 1$, то множество симметричных элементов есть подполе K_0 поля K, такое, что K является его сепарабельным квадратичным расширением. В этом случае по тем же соображениям группа $T_2(K, f)$ совпадает *с унимодулярной группой* $SL_2(K_0)$. Из этих замечаний и результатов § 2 следует, что если поле K содержит не более 25 элементов, то группа T_2/W_2 не будет простой только в следующих случаях:

a) $J = 1$, $K = \mathbf{F}_2$ или $\mathbf{F}_3$;

b) $J \neq 1$, $K = \mathbf{F}_4$ или $\mathbf{F}_9$.

В силу теоремы A) мы получаем, что, *за исключением этих четырех случаев, группа T_n/W_n проста при $n \geqslant 2$*. В особых случаях рассуждение, проведенное при доказательстве теоремы A), показывает, что если группа T_h/W_h проста при некотором $h > 2$, то группа T_n/W_n проста при всех $n \geqslant h$. Если применять к группе T_h/W_h метод п. B), то выясняется, что рассматриваемая группа подстановок не будет дважды транзитивна, если $h \geqslant 4$ (поскольку поле K конечно и, следовательно, $\nu \geqslant 2$ (гл. I, § 8)). Однако таким же методом, что в § 9, леммы 7, 8 и 9, можно установить, что она *примитивна*.

Тем самым все сводится к тому, чтобы посмотреть, совпадает ли группа T_h/W_h со своим коммутантом Γ.

а) $J = 1$ (симплектические группы). Заметим, что в этом случае $T_n(K, f) = Sp_n(K, f)$ (см. § 5). Если $K = \mathbf{F}_3$, то можно взять $h = 4$. В самом деле, специальное преобразование u (см. гл. I, § 12), соответствующее матрице $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, есть произведение двух сопряженных сдвигов и, следовательно, является коммутатором. То же самое относится к специальному преобразованию, соответствующему матрице $S' = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$, поскольку эта матрица эквивалентна матрице S (см. гл. I, § 12). Следовательно, коммутант Γ группы T_4 содержит специальное преобразование, соответствующее матрице $S - S' = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}$, и, так как последняя эквивалентна матрице $S'' = \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}$, то и специальное преобразование, соответствующее матрице $S' + S'' = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}$. Последнее преобразование есть сдвиг t. Группа Γ содержит также t^2, а всякий сдвиг сопряжен с t или t^2. Значит $\Gamma = T_4$.

Если $K = \mathbf{F}_2$, то группа T_4/W_4 содержит простую подгруппу индекса 2 (см. гл. IV, § 8). В этом случае можно взять $h = 6$. Действительно, специальное преобразование u, соответствующее матрице $S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, является, как и выше, произведением двух сопряженных сдвигов и, значит, лежит в Γ. Матрица S эквивалентна двум симметричным матрицам

$$S_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{и} \quad S_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Следовательно, Γ содержит также специальное преобразование, соответствующее матрице

$$S' = S_1 + S_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

а также эквивалентной ей матрице $S'' = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Отсюда получаем, что Γ содержит специальное преобразование, соответствующее матрице $S + S''$, которое является сдвигом.

b) $J \neq 1$ (унитарные группы). Если исключить случай $K = \mathbf{F}_4$ и $n = 3$, то $T_n(K, f) = U_n^+(K, f)$ (см. § 5). Если $K = \mathbf{F}_9$, то можно взять $h = 3$. Действительно, пусть t — унитарный сдвиг. Тогда $t^3 = 1$, и достаточно найти такой элемент $s \in U_3^+$, что $sts^{-1} = t^{-1}$, поскольку тогда $sts^{-1}t^{-1} = t^{-2} = t$, и тем самым будет доказано, что $t \in \Gamma$. Пусть (e_1, e_2, e_3) — базис пространства E, образованный не ортогональными друг другу изотропными векторами e_1, e_2 и вектором e_3, ортогональным к гиперболической плоскости $P = e_1K + e_2K$. Можно считать, что t есть сдвиг в направлении вектора e_1, так что его матрица имеет вид $\begin{pmatrix} B_{12}(\lambda) & 0 \\ 0 & 1 \end{pmatrix}$. Существует такой элемент $\alpha \in K$, что $\alpha\alpha^J = -1$. Автоморфизм s пространства E, матрица которого есть $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & -\alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}$, удовлетворяет нужным условиям.

Наконец, при $K = \mathbf{F}_4$ группа $T_3(\mathbf{F}_4)$ имеет нормальный ряд $T_3 \supset T_3' \supset W_3 \supset \{1\}$, где группа T_3/T_3' изоморфна симметрической группе $\mathfrak{S}_3$, а группа T_3'/W_3 циклическая порядка 3. В этом случае можно взять $h = 4$. В самом деле, специальное преобразование u, соответствующее эрмитовой матрице $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, является произведением двух сопряженных сдвигов и, значит, содержится в Γ. Но все эрмитовы матрицы ранга 2 над $\mathbf{F}_4$ эквивалентны (см. гл. I, § 8). Следовательно, Γ содержит также специальные преобразования, соответствующие матрицам $S' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и $S'' = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, а значит, и матрице $S + S' + S'' = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Это последнее преобразование является сдвигом.

Предыдущие рассуждения позволяют утверждать, что в тех случаях, когда группа T_n/W_n проста, всякий нормальный делитель группы $U_n(K, f)$, не содержащийся в ее центре, содержит группу $T_n(K, f)$.

§ 5. Структура группы $U_n(K, f)$

(f есть T-форма индекса $\geqslant 1$; ортогональные группы не рассматриваются.)

II. Группа $U_n(K, f)/T_n(K, f)$

Структура группы $U_n(K, f)/T_n(K, f)$ была определена Уоллом [1]. Обозначим через Σ подгруппу группы K^*, порожденную ее симметричными элементами, и через Ω — подгруппу, порожденную элементами $\lambda \in K^*$, обладающими следующим свойством: существует вектор $x \in E$, ортогональный к некоторой гиперболической плоскости и такой, что $f(x, x) = \lambda - \lambda^J$. Подгруппы Σ и Ω являются нормальными делителями в K^* [1]). Обозначим через $[K^*, \Omega]$ подгруппу группы K^*, порожденную коммутаторами $\lambda\omega\lambda^{-1}\omega^{-1}$, где $\lambda \in K^*$ и $\omega \in \Omega$. В этих обозначениях *группа* $U_n(K, f)/T_n(K, f)$ *при* $n \geqslant 2$ *изоморфна факторгруппе* $K^*/\Sigma[K^*, \Omega]$, *за исключением случая, когда* $n = 3$ *и* $K = \mathbf{F}_4$.

Метод Уолла основан на следующих предварительных рассмотрениях, проводимых при *единственном* предположении, что f — невырожденная косоэрмитова форма

[1]) Легко видеть, что $\Sigma \subset \Omega$. — *Прим. перев.*

(не обязательно T-форма и, может быть, анизотропная). Пусть $a \neq 0$ — вектор пространства E. Обозначим через Ω_a подгруппу группы K^*, порожденную элементами $\lambda \in K^*$, для которых существует такой вектор $x \in E$, ортогональный к a, что $f(x, x) = \lambda - \lambda^J$. Положим $\Gamma_a = \Sigma [K^*, \Omega_a]$. Легко видеть, что Ω_a и Γ_a — нормальные делители группы K^*, причем $\Sigma \subset \Gamma_a \subset \Omega_a$. Определим следующим образом гомоморфизм N_a: $U_n(K, f) \to K^*/\Gamma_a$ (*норму Уолла*). Для всякого $u \in U_n$ обозначим через V_u подпространство пространства E, являющееся образом эндоморфизма $x \to x - u(x)$. Если $\dim(V_u) = r$, то преобразование u может быть представлено в виде $u = s_1 s_2 \ldots s_r$, где $s_i \in U_n$, $\dim(V_{s_i}) = 1$ и V_u есть *прямая сумма* V_{s_i}. Каждое из преобразований s_i является квазиотражением или сдвигом и записывается в виде

$$s_i(x) = x - a_i \omega_i f(a_i, x),$$

где $\omega_i^{-1} - \omega_i^{-J} = f(a_i, a_i)$, причем каждый из векторов a_i может быть выбран так, чтобы $f(a, a_i) = 0$ или 1. Тогда образ в K^*/Γ_a элемента $\omega_1 \omega_2 \ldots \omega_r$ *не зависит от рассматриваемого разложения преобразования* u, и если обозначить его через $N_a(u)$, то N_a будет гомоморфизмом.

Теперь для доказательства теоремы Уолла зафиксируем изотропный вектор $e \in E$ и обозначим через N норму Уолла N_e. Пусть P_0 — гиперболическая плоскость, содержащая e. Теорема Уолла доказывается сначала для случая $P_0 = E$. В общем случае рассматривается подгруппа U_n^0 группы U_n, образованная гиперболическими преобразованиями, соответствующими плоскости P_0. Доказывается, что ограничение N на U_n^0 *сюръективно*, и завершается доказательство при помощи следующей леммы (использующей частный случай теоремы при $n = 2$).

1) *Если P_1 и P_2 — две гиперболические плоскости, то существует такое преобразование $w \in T_n$, что $w(P_1) = P_2$ (случай, когда $n = 3$ и $K = \mathbf{F}_4$, исключается).*

Из теоремы Уолла, в частности, выводится следующее утверждение:

2) *Если* $\nu \geqslant 2$, *то группа* $T_n(K, f)$ *совпадает с коммутантом группы* $U_n(K, f)$ [1].

В самом деле, в этом случае очевидно, что $\Omega = K^*$ [2].

Ван [2] определил во всех случаях коммутант группы $U_2(K, f)$ при $\nu = 1$.

Предположим теперь, что K — тело *конечной* размерности m^2 над своим центром Z. Можно показать, что тогда для инволюции J возможны три случая:

I. J оставляет на месте все элементы из Z, и размерность (над Z) пространства S симметричных элементов равна $m(m+1)/2$.

II. J оставляет на месте все элементы из Z, и размерность (над Z) пространства S симметричных элементов равна $m(m-1)/2$.

III. Ограничение J на Z не тождественно, симметричные элементы из Z образуют такое подполе Z_0, что Z является его сепарабельным квадратичным расширением; пространство S имеет размерность m^2 над Z_0.

В случаях I и II говорят, что J — инволюция *первого рода*, в случае III — *второго рода* (очевидно, что именно этот случай имеет место, если K коммутативно и $J \neq 1$). Заметим, что если J — инволюция типа I и $\alpha^J = -\alpha$, то $\xi \to \alpha\xi^J\alpha^{-1}$ — инволюция типа II.

Если J — инволюция типа I, *то* $U_n(K, f) = T_n(K, f)$ (Дьёдонне [13], стр. 379). Это относится, в частности, к *симплектическим группам* ($J = 1$). Таким образом, проективная группа $PSp_n(K)$, факторгруппа группы $Sp_n(K)$ по ее центру (состоящему из одного или двух элементов в зависимости от того, равна или не равна 2 характеристика тела K), *проста*, за исключением случая, когда $K = \mathbf{F}_3$, $n = 2$, и случая, когда $K = \mathbf{F}_2$, $n = 2$ или 4 (Диксон [1]). Кроме того, *всякое симплектическое преобразование есть произведение симплектических сдвигов.*

---

[1] Кроме случая, когда $U_n = Sp_4(\mathbf{F}_2)$. — *Прим. перев.*

[2] В силу теоремы Уолла из этого следует, что группа U_n/T_n коммутативна и, значит, T_n содержит коммутант группы U_n. С другой стороны, из результатов § 4 вытекает, что при $\nu \geqslant 2$ во всех случаях, кроме оговоренного в предыдущем примечании, T_n содержится в коммутанте группы U_n. — *Прим. перев.*

Можно показать, что число множителей при этом может быть сделано не превосходящим $n+1$, причем эта оценка является точной (Дьёдонне [19]).

Уолл [1] вывел из своей теоремы такое следствие:

3) *Если K — тело, конечномерное над своим центром, $n \geqslant 3$ и группа T_n/W_n проста, то T_n совпадает с коммутантом группы U_n.*

Напротив, при $n=2$, если K — тело обобщенных кватернионов и J — инволюция типа II, то T_2 не совпадает с коммутантом группы U_2 (см. гл. IV, § 8).

Обозначим через $U_n^+(K, f)$ (без ограничений на форму f, которая, в частности, может быть индекса 0) нормальный делитель группы $U_n(K, f)$, образованный преобразованиями, определитель которых (см. § 1) равен 1, и через $PU_n^+(K, f)$ — образ $U_n^+(K, f)$ в $PGL_n(K)$ при каноническом отображении. Если тело K конечномерно над своим центром и J — инволюция типа I, то из сказанного выше следует, что $U_n^+ = U_n$. Можно доказать то же самое в случае, когда J — инволюция типа II, поскольку в обоих случаях автоморфизм группы K^*/C, индуцированный J, тождествен[1]). Напротив, если J — инволюция типа III, то всегда $U_n^+ \neq U_n$ (Дьёдонне [13], стр. 384). Если K не коммутативно, строение группы U_n^+ в этом случае не известно[2]). Для коммутативного тела K имеет место следующее утверждение (Диксон [1, 3], Дьёдонне [4], стр. 66—71):

4) *Если K коммутативно, $\nu \geqslant 1$ и $J \neq 1$, то $U_n^+(K, f) = T_n(K, f)$ при $n \geqslant 2$, кроме случая $n=3$, $K = \mathbf{F}_4$.*

В особом случае U_3^+/T_3 есть группа порядка 4, произведение двух циклических групп порядка 2.

Таким образом, если K коммутативно, группа $PU_n^+(K, f)$ изоморфна T_n/W_n, за исключением случая

[1]) Если J — инволюция типа I, то $U_n^+ = T_n$. Напротив, как доказал Платонов, если J — инволюция типа II и Z — конечно порожденное поле, то $U_n^+ \neq T_n$. — *Прим. перев.*

[2]) Для глобальных полей Z (в частности, для полей алгебраических чисел) Платонов и Янчевский [1*] доказали, что в этом случае $U_n^+ = T_n$. — *Прим. перев.*

группы $U_3(\mathbf{F}_4)$; во всех случаях группа U_n/U_n^+ изоморфна группе элементов поля K, норма которых равна 1 (относительно поля инвариантов K_0 инволюции J).

Добавим, наконец, что порядок симплектической группы $Sp_{2m}(\mathbf{F}_q)$ над конечным полем равен

$$(q^{2m}-1)\,q^{2m-1}\,(q^{2m-2}-1)\,q^{2m-3}\,\ldots\,(q^2-1)\,q,$$

а порядок унитарной группы $U_n(\mathbf{F}_{q^2})$ равен

$$q^n-(-1)^n)\,q^{n-1}\left(q^{n-1}-(-1)^{n-1}\right)q^{n-2}\,\ldots\,(q^2-1)\,q\,(q+1).$$

(Диксон [1], стр. 94 и 134).

§ 6. Группа $O_n(K, f)$ (характеристика K не равна 2): группа вращений и коммутант

Отображение $u \to \det(u)$ есть гомоморфизм группы $O_n(K, f)$ на группу $\{-1, +1\}$, так что ортогональные преобразования с определителем 1 образуют нормальный делитель индекса 2 в $O_n(K, f)$. Этот нормальный делитель обозначается через $O_n^+(K, f)$ и называется *группой вращений*. Элементы группы O_n, не принадлежащие O_n^+, называются *переворачиваниями*. Вращение (соответственно переворачивание) является произведением *четного* (соответственно *нечетного*) числа отражений, причем это число всегда можно сделать $\leqslant n$. Поэтому, если *n нечетно* (соответственно *четно*), всякое вращение (соответственно переворачивание) *оставляет на месте* хотя бы один вектор $\neq 0$.

Для подпространства V пространства E всегда существуют ортогональные преобразования с определителем -1, сохраняющие V (в целом), *за исключением* случая, когда $n=2m$, $\nu=m$ и V есть m-мерное вполне изотропное подпространство. Ввиду теоремы Витта отсюда следует, что если V и W — два таких подпространства E, что ограничения формы f на $V \times V$ и на $W \times W$ эквивалентны, то всегда существует такое вращение u, что $u(V)=W$, кроме случая, когда V и W — вполне изотропные подпространства размерности $n/2$. Что касается вполне изотропных подпространств размерности $n/2$, то они разбиваются на *два* класса транзитивности относительно группы O_n^+. Более точно, если V и W — два таких подпространства, то для любого отражения s имеем $\dim(V \cap s(W)) = \dim(V \cap W) \pm 1$, так что V и W принадлежат к *одному* классу тогда и только тогда, когда $\dim(V \cap W)$ имеет *ту же четность, что* $n/2$.

Инволюция типа $(n-2, 2)$ в группе $O_n(K, f)$ называется *инверсией*. Очевидно, что инверсия является вращением.

1) *При $n \geqslant 3$ всякое вращение представляется в виде произведения инверсий.*

Это утверждение доказывается индукцией по n. Пусть x — неизотропный вектор. Тогда существует инверсия, преобразующая x в $-x$. Если u — произвольное вращение, то хотя бы один из векторов $u(x)-x$, $u(x)+x$ неизотропен. Если таковым является вектор $u(x)+x$, то существует ортогональная к нему неизотропная плоскость P, содержащая вектор $u(x)-x$; инверсия, для которой P служит отрицательным подпространством, переводит тогда x в $u(x)$. Если вектор $u(x)-x$ неизотропен, то аналогично строится инверсия, переводящая x в $-u(x)$, и затем применяется инверсия, переводящая $-u(x)$ в $u(x)$. Таким образом, всегда можно свести доказательство к случаю, когда u оставляет на месте неизотропный вектор x. Рассматривая ограничение преобразования u на гиперплоскости, ортогональной к x, путем индуктивного рассуждения доказательство приводится к случаю $n = 3$. В этом случае, поскольку всякое вращение из группы O_2 есть произведение не более чем двух отражений, всякое вращение из группы O_3, оставляющее на месте некоторый неизотропный вектор, есть произведение не более чем двух инверсий.

2) *При $n \geqslant 3$ центр группы $O_n^+(K, f)$ состоит лишь из единицы, если n нечетно, и из единицы и преобразования $x \to -x$, если n четно.* Действительно, полулинейное преобразование, перестановочное со всеми инверсиями, сохраняет все неизотропные плоскости. Но очевидно, что всякая неизотропная прямая есть пересече-

ние двух неизотропных плоскостей. В силу леммы 1 § 3 то же самое справедливо в отношении изотропных прямых. Следовательно, централизатором группы O_n^+ в ΓL_n является группа гомотетий $H_n = Z_n$, откуда и вытекает доказываемое утверждение. Если n нечетно, то группа O_n есть *прямое произведение* группы O_n^+ и центра $Z_n \cap O_n$ группы O_n.

3) *При $n = 2$ группа $O_2^+(K, f)$ коммутативна.* Более точно, возможны два случая:

a) если $\nu = 1$, то, выбирая в пространстве E базис из двух изотропных векторов, мы видим, что преобразования из O_2^+ записываются матрицами вида $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, где $\lambda \in K^*$. Следовательно, группа $O_2^+(K, f)$ в этом случае *изоморфна* K^*;

b) если $\nu = 0$, то выбрав в пространстве E ортогональный базис, можно предполагать, что $f(x, x) = \xi_1^2 + \alpha\xi_2^2$, где $-\alpha$ не является квадратом в K. Пусть $K_1 = K(\omega)$ — квадратичное расширение поля K, полученное присоединением квадратного корня ω из $-\alpha$. Пространство E может быть отождествлено с K_1 таким образом, что вектор $(1, 0)$ отождествляется с единицей поля K_1. Заметим, что если $\zeta = \xi + \omega\eta$, то $\bar{\zeta} = \xi - \omega\eta$ и $\zeta\bar{\zeta} = \xi^2 + \alpha\eta^2$. Вращение $u \in O_2^+(K, f)$ переводит единицу поля K_1 в элемент γ, норма которого равна 1, и поэтому совпадает с преобразованием $\zeta \to \gamma\zeta$ поля K_1. Таким образом, в этом случае группа $O_2^+(K, f)$ *изоморфна группе элементов с нормой* 1 *поля* K_1.

Обозначим через $\Omega_n(K, f)$ *коммутант* ортогональной группы $O_n(K, f)$.

4) *Группа $\Omega_n(K, f)$ порождается произведениями $s(wsw^{-1})$ двух сопряженных отражений. Она также порождается квадратами элементов группы O_n* (Диксон [1], стр. 218; Дьёдонне [4], стр. 23). Чтобы доказать, что всякий коммутатор $uvu^{-1}v^{-1}$ является произведением преобразований вида $s(wsw^{-1})$, где s — отражение, можно рассуждать индукцией по числу отражений, в произведение которых разлагается v (§ 3). Тем же методом доказывается, что всякий квадрат v^2 принадлежит группе

Ω_n [1]). Отсюда вытекает, что *всякий отличный от* 1 *элемент группы* O_n/Ω_n *имеет период* 2. Тем самым строение этой группы полностью определяется кардинальным числом ее элементов (которое может быть либо конечным вида 2^k, либо бесконечным).

5) *При* $n \geqslant 3$ *группа* Ω_n *является также коммутантом группы* O_n^+. Для доказательства достаточно использовать свойство 1). Рассуждая как в п. 4), мы видим, что коммутант группы O_n^+ порождается квадратами ее элементов [2]). С другой стороны, легко доказать, что группа Ω_n порождается коммутаторами $sts^{-1}t^{-1} = (st)^2$ всевозможных пар отражений s, t. Следовательно, Ω_n содержится в коммутанте группы O_n^+ и, значит, совпадает с ним. При $n = 2$ $\Omega_2 \subset O_2^+$, однако, равенства нет, поскольку группа O_2^+, как мы видели, абелева.

Таким образом, при $n \geqslant 3$ мы имеем следующий нормальный ряд в группе $O_n(K, f)$:

$$O_n \supset O_n^+ \supset \Omega_n \supset \Omega_n \cap Z_n \supset \{1\}. \tag{1}$$

Если *n нечетно*, то, как мы видели, группа $O_n^+ \cap Z_n$ содержит только 1. Тем более, $\Omega_n \cap Z_n = \{1\}$. В любом случае группа $\Omega_n \cap Z_n$ совпадает с *центром* группы Ω_n. В самом деле, полулинейное преобразование u, коммутирующее со всеми элементами из Ω_n, коммутирует, в частности, с квадратами v^2 преобразований v, оставляющих на месте все элементы какого-либо неизотропного $(n-2)$-мерного подпространства Q. Эти преобразования можно рассматривать как ортогональные преобразования плоскости Q^0, ортогональной к Q. За исключением случая, когда $K = \mathbf{F}_3$ и Q^0 — гиперболическая плоскость, существуют преобразования v такого вида, для которых $v^2 \neq 1$. Следовательно, все неизотропные $(n-2)$-мерные подпространства и, значит, все неизотропные прямые должны быть инвариантны отно-

[1]) Обратно, если O_n^2 — группа, порожденная квадратами, то факторгруппа O_n/O_n^2 абелева, поскольку в ней квадраты всех элементов равны 1. Следовательно, $O_n^2 \supset \Omega$. — *Прим. перев.*

[2]) Это верно для любой группы, порожденной элементами периода 2. — *Прим. перев.*

сительно u. Как и в п. 3), отсюда вытекает, что u — гомотетия. Если $K = \mathbf{F}_3$, то u должно сохранять все *эллиптические плоскости* (в которых ограничение формы $f(x, x)$ в некотором ортогональном базисе записывается в виде $\xi_1^2 + \xi_2^2$). При $n \geqslant 4$ всякая неизотропная прямая есть пересечение двух эллиптических плоскостей, откуда и следует в этом случае доказываемое утверждение. Наконец, при $n = 3$ в пространстве E существует такой базис, что три координатные плоскости, и только они, являются эллиптическими. Преобразование u должно либо оставлять без изменения, либо умножать на -1 каждый из векторов этого базиса. Легко видеть, что среди таких преобразований только тождественное коммутирует со всеми преобразованиями из Ω_3.

Через $PO_n^+(K, f)$, $P\Omega_n(K, f)$ обозначаются канонические образы групп $O_n^+(K, f)$, $\Omega_n(K, f)$ в $PGL_n(K)$. Они изоморфны факторгруппам $O_n^+/(O_n^+ \cap Z_n)$ и $\Omega_n/(\Omega_n \cap Z_n)$ соответственно.

В последующих параграфах мы изложим известные результаты о факторах описанного выше нормального ряда ортогональной группы.

§ 7. Алгебра Клиффорда квадратичной формы
(K — поле характеристики $\neq 2$.)

Как и выше, мы обозначаем через $f(x, y)$ невырожденную симметричную билинейную форму на n-мерном векторном пространстве E над полем K. Рассмотрим в тензорной алгебре $T(E)$ над E двусторонний идеал $\mathfrak{a}$, порожденный элементами вида $x \otimes y - y \otimes x - 2f(x, y)$. Факторалгебра $C(f) = T(E)/\mathfrak{a}$ называется *алгеброй Клиффорда* формы f (Клиффорд [1], [2], Липшиц [1]). Пусть $(a_i)_{1 \leqslant i \leqslant n}$ — ортогональный базис пространства E. Обозначим через e_i класс элемента a_i по модулю $\mathfrak{a}$, рассматриваемый как элемент алгебры $C(f)$. Для всякого подмножества H множества чисел $1, 2, \ldots, n$ положим $e_H = e_{i_1} e_{i_2} \ldots e_{i_p}$, где $(i_k)_{1 \leqslant k \leqslant p}$ — последовательность всех элементов из H, расположенных в возрастающем порядке (если H пусто, то $e_H = 1$). Можно доказать (Шевалле [1], Бурбаки [3]), что 2^n элементов e_H образуют *базис* алгебры $C(f)$ над K с таблицей умножения

$$e_A e_B = \gamma_{A,B} e_{A \triangle B}, \tag{2}$$

где $A \triangle B$ обозначает сумму в булевой алгебре подмножеств множества чисел $1, 2, \ldots, n$ (иначе говоря, характеристическая функция подмножества $A \triangle B$ есть сумма по модулю 2 характеристических функций подмножеств A и B). При этом

$$\gamma_{A,B} = (-1)^{\rho(A,B)} \prod_{i \in A \cap B} f(a_i, a_i), \tag{3}$$

где $\rho(A, B)$ есть «число инверсий» в последовательности, полученной приписыванием B к A. Если обозначить через $\rho(A, j)$ число элементов из A, бо́льших j, то

$$\rho(A, B) = \sum_{j \in B} \rho(A, j). \tag{4}$$

В частности, $e_i e_j = -e_j e_i$ при $j \neq i$ и $e_i^2 = f(a_i, a_i)$ при любом i.

Множество L_p линейных комбинаций элементов e_H, соответствующих множествам H, содержащим *не более* p элементов $(0 \leqslant p \leqslant n)$, есть подпространство алгебры $C(f)$, не зависящее от выбора базиса (a_i). В частности, пространство E может быть отождествлено с подпространством элементов алгебры $C(f)$, являющихся линейными комбинациями элементов e_i. При этом вектор a_i отождествляется с e_i. Для каждой пары элементов x, y пространства E в алгебре $C(f)$ имеет место равенство

$$xy + yx = 2f(x, y) \tag{5}$$

и, в частности,

$$x^2 = f(x, x). \tag{6}$$

Очевидно, что элементы e_i вместе с единицей *порождают* алгебру $C(f)$.

1) *Центр алгебры $C(f)$ совпадает с K, если n четно, и равен $K + Ke_1e_2 \ldots e_n$, если n нечетно.* Действительно,

если записать условие, что элемент $z = \sum_A \gamma_A e_A$ перестановочен с e_i, то получится что $\gamma_A = 0$ для всех множеств A, содержащих нечетное число элементов, отличных от i. Отсюда и вытекает сформулированное утверждение.

Линейные комбинации элементов e_H, соответствующих подмножествам H, содержащим *четное* число элементов, образуют подалгебру $C^+(f)$ алгебры $C(f)$, не зависящую от выбора базиса (a_i). Ее размерность над K равна 2^{n-1}. Как алгебра она порождается произведениями $e_i e_j$ $(i < j)$ и единицей. Линейные комбинации элементов e_H, соответствующих подмножествам H, содержащим *нечетное* число элементов, образуют подпространство $C^-(f)$ алгебры $C(f)$, дополнительное к $C^+(f)$ и не зависящее от выбора базиса (a_i). Для краткости элементы из $C^+(f)$ называют элементами *четной степени*, а элементы из $C^-(f)$ — элементами *нечетной степени*.

2) *Центр алгебры $C^+(f)$ совпадает с K, если n нечетно, и равен $K + Ke_1 \ldots e_n$, если n четно.* В предыдущих обозначениях, если записать, что элемент $z \in C^+(f)$ коммутирует с $e_i e_j$, то получится, что $\gamma_A = 0$ для всех таких множеств A, что $j \in A$, но $i \notin A$. Отсюда и получается сформулированный результат.

Более глубокое алгебраическое исследование алгебры Клиффорда и описание ее связи со «спинорным представлением» ортогональной группы $O_n(K, f)$ читатель может найти в работах Шевалле [1] и Эйхлера [2]. Для целей приложения алгебры $C(f)$ к изучению структуры группы $O_n(K, f)$ мы используем элементарный метод, не требующий этих результатов. Мы будем следовать в основном изложению Эйхлера [2].

3) *Для всякого ортогонального преобразования $u \in O_n(K, f)$ существует обратимый элемент $s_u \in C(f)$, удовлетворяющий одному из следующих условий:*

а) *если u — вращение, то s_u — элемент четной степени и*

$$u(x) = s_u x s_u^{-1} \tag{7}$$

для любого $x \in E$;

b) *если u — переворачивание, то s_u — элемент нечетной степени и*

$$u(x) = -s_u x s_u^{-1} \tag{8}$$

для любого $x \in E$.

Эти условия определяют элемент s_u однозначно с точностью до пропорциональности.

В самом деле, предположим вначале, что u — отражение относительно гиперплоскости, ортогональной неизотропному вектору $a \in E$. Тогда в силу (5) и (6)

$$u(x) = x - 2\frac{f(x, a)}{f(a, a)}a = x - (ax + xa)a^{-2}a = -axa^{-1}. \tag{9}$$

Пусть теперь $u = v_1 v_2 \ldots v_p$, где v_i — отражение относительно гиперплоскости, ортогональной к неизотропному вектору a_i. Тогда

$$u(x) = (-1)^p (a_1 a_2 \ldots a_p)\, x\, (a_1 a_2 \ldots a_p)^{-1},$$

и можно взять $s_u = a_1 a_2 \ldots a_p$. Если t — другой элемент, удовлетворяющий условию (7) или (8), то элемент $s_u^{-1}t$ лежит в $C^+(f)$ и коммутирует со всеми элементами из E и, значит, со всеми элементами из $C(f)$. Из п. 1) следует, что $s_u^{-1}t \in K$.

4) *Обратно, если s — такой обратимый элемент алгебры $C(f)$, что $sEs^{-1} = E$, то преобразование $x \to sxs^{-1}$ содержится в группе $O_n(K, f)$; если, кроме того, $s \in C^+(f)$, то это преобразование является вращением.*

Первое утверждение немедленно вытекает из (5). С другой стороны, если $s \in C^+(f)$, но преобразование $x \to v(x) = sxs^{-1}$ является переворачиванием, то в силу 3) существует такой обратимый элемент $t \in C^-(f)$, что $v(x) = -txt^{-1}$. Положим $r = t^{-1}s$. Тогда $rxr^{-1} = -x$ для всякого $x \in E$. Пусть $r = \sum_A \gamma_A e_A$. Из условия $re_ir^{-1} = -e_i$, $1 \leqslant i \leqslant n$, вытекает, что $\gamma_A = 0$, если A содержит четное число индексов $\neq i$. Следовательно, $r = \gamma e_1 e_2 \ldots e_n$, причем n четно; но это противоречит тому, что $r \in C^-(f)$.

Заметим теперь, что линейное преобразование J тензорной алгебры $T(E)$, определяемое условием $(x_1 \otimes x_2 \otimes \ldots \otimes x_p)^J = x_p \otimes x_{p-1} \otimes \ldots \otimes x_1$, является антиавтоморфизмом. Очевидно, что J сохраняет идеал $\mathfrak{a}$ и, следовательно, индуцирует *инволютивный антиавтоморфизм алгебры Клиффорда* $C(f)$, который мы будем обозначать также через J. Имеем

$$(x_1x_2 \ldots x_p)^J = x_px_{p-1} \ldots x_1 \tag{10}$$

при $x_i \in E$, $1 \leqslant p \leqslant n$. Ясно, что J сохраняет $C^+(f)$ и $C^-(f)$.

Пусть теперь u — произвольное вращение, произведение $2p$ отражений относительно гиперплоскостей, ортогональных к неизотропным векторам $a_1, \ldots, a_{2p}$. Тогда для $s_u = a_1a_2 \ldots a_{2p}$ справедлива формула (7). В силу (6)

$$s_us_u^J = a_1a_2 \ldots a_{2p}a_{2p} \ldots a_2a_1 =$$
$$= f(a_1, a_1) f(a_2, a_2) \ldots f(a_{2p}, a_{2p}) \neq 0$$

Если заменить s_u на λs_u, где $\lambda \in K^*$, то скаляр $s_us_u^J$ умножится на λ^2. Из 3) следует, что *класс элемента* $s_us_u^J$ *по модулю группы* K^{*2} квадратов элементов группы K^* зависит только от u. Обозначим этот класс через $\theta(u)$. Для двух вращений u, v из 3) следует, что s_{uv} и s_us_v отличаются только скалярным множителем. Отсюда получаем

$$\theta(uv) = \theta(u)\theta(v). \tag{11}$$

Другими словами, θ — *это гомоморфизм группы* O_n^+ *на подгруппу* Γ *группы* K^*/K^{*2}, *порожденную классами элементов вида* $f(x, x)f(y, y)$, где x и y — произвольные неизотропные векторы пространства E. Говорят, что $\theta(u)$ есть *спинорная норма* вращения u (Липшиц [1], [2], [3], Эйхлер [2]). Определение Липшица дает также метод вычисления $\theta(u)$ через элементы матрицы преобразования u в ортогональном базисе.

Ядро $O_n'(K, f) = \theta^{-1}(1)$ *содержит коммутант* $\Omega_n(K, f)$ *группы* $O_n(K, f)$. Это очевидно при $n \geqslant 3$, поскольку тогда $\Omega_n(K, f)$ совпадает с коммутантом группы $O_n^+(K, f)$. Это верно также при $n = 2$; в самом деле, если s, s' — два сопряженных отражения относительно гиперплоскостей, ортогональных векторам a, a', то можно считать, что

$f(a, a) = f(a', a')$ и тогда $\theta(ss') = (f(a, a))^2 \bmod K^{*2} = 1$.

Мультипликативная группа таких обратимых элементов $s \in C(f)$, что $sEs^{-1} = E$, называется *группой Клиффорда* формы f. Ее подгруппа, образованная элементами $s \in C^+(f)$, для которых $ss^J = 1$, обозначается через $\mathrm{Spin}_n(K, f)$. Ставя в соответствие каждому элементу $s \in \mathrm{Spin}_n(K, f)$ элемент $x \to sxs^{-1}$ группы $O_n^+(K, f)$, получаем гомоморфизм, ядро которого есть $\{-1, +1\}$, а образ — группа $O'_n(K, f)$. Иначе говоря, имеется каноническая *точная последовательность* гомоморфизмов групп

$$1 \to \{-1, +1\} \to \mathrm{Spin}_n(K, f) \to O_n^+(K, f) \xrightarrow{\theta} \Gamma \to 1.$$

§ 8. Структура группы $O_n(K, f)$

(K — поле характеристики $\neq 2$, f — форма индекса $\nu \geqslant 1, n \geqslant 2$.)

I. Структура групп O_n^+/Ω_n и $\Omega_n \cap Z_n$

1) *Пусть P — гиперболическая плоскость. Всякое ортогональное преобразование (соответственно вращение) u может быть представлено в виде $u = sv$, где s — гиперболическое преобразование (соответственно гиперболическое вращение), связанное с плоскостью P, а $v \in \Omega_n$.*

Это очевидно, если u — гиперболическое преобразование, связанное с плоскостью P', так как в силу теоремы Витта существует такое преобразование $t \in O_n$, что $t(P) = P'$, и тогда $u = tst^{-1} = s(s^{-1}tst^{-1})$, где s — гиперболическое преобразование, связанное с плоскостью P. В общем случае u разлагается в произведение p гиперболических преобразований, и доказательство может быть проведено индукцией по p. Наконец, если u — вращение, то, поскольку и v — вращение, s — также вращение.

Другое доказательство этого утверждения см. у Шевалле [1], стр. 53—55.

2) *Если P и P' — две гиперболические плоскости, то существует такое преобразование $v \in \Omega_n(K, f)$, что $v(P) = P'$.* Это очевидно при $n = 2$. При $n > 2$ в силу

теоремы Витта существует такое преобразование $u \in O_n$, что $u(P) = P'$. Согласно 1), имеем тогда представление $u = sv$, где $v \in \Omega_n$, а s — гиперболическое преобразование, связанное с плоскостью P'. Ясно, что тогда $v(P) = P'$.

Эти результаты позволяют доказать следующую теорему (Эйхлер [2]):

Если $\nu \geqslant 1$ и $n \geqslant 2$, то спинорная норма θ есть гомоморфизм группы O_n^+ на группу K^*/K^{*2}, ядром которого является коммутант Ω_n группы O_n.

В самом деле, из 1) получаем, что $\theta(u) = \theta(s)\theta(v) = \theta(s)$, поскольку Ω_n содержится в ядре гомоморфизма θ. Поэтому доказательство сводится к случаю $n = 2$, $\nu = 1$. В этом случае в базисе, составленном из изотропных векторов e_1, e_2, для которых $f(e_1, e_2) = 1$, вращение s записывается матрицей $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ и является произведением двух отражений, одного — относительно прямой, ортогональной к вектору $e_1 - e_2$, другого — относительно прямой, ортогональной к вектору $\alpha e_1 - e_2$. Так как $f(e_1 - e_2, e_1 - e_2) = -2$, $f(\alpha e_1 - e_2, \alpha e_1 - e_2) = -2\alpha$, то $\theta(s) = \hat{\alpha}$ (класс элемента $\alpha \in K^*$ по модулю K^{*2}). Отсюда немедленно вытекает доказываемая теорема, ибо если $\theta(s) = 1$, то $\alpha = \beta^2$ и s является квадратом вращения $\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}$, так что $s \in \Omega_n$ (см. § 6).

Из этой теоремы получаются следствия:

a) *Если $n \geqslant 2$ и $\nu \geqslant 1$, то группа $O_n^+(K, f)/\Omega_n(K, f)$ изоморфна K^*/K^{*2}.*

b) *Если $n \geqslant 2$ и $\nu \geqslant 1$, то симметрия $x \to -x$ принадлежит группе $\Omega_n(K, f)$ тогда и только тогда, когда n четно и дискриминант формы f является квадратом в поле K.* Действительно, симметрия $x \to -x$ есть произведение n отражений относительно координатных гиперплоскостей в ортогональном базисе для формы f. Спинорная норма этого преобразования есть, следовательно, класс по модулю K^{*2} дискриминанта формы f в этом базисе. Заметим, что условие «дискриминант формы f является квадратом» в любом случае является *необходимым и достаточным условием* для того, чтобы преобразование $x \to -x$ принадлежало группе O'_n (даже если $\nu = 0$).

§ 9. Структура группы $O_n(K, f)$

(K — поле характеристики $\neq 2$, f — форма индекса $\geqslant 1$, $n \geqslant 3$.)

II. Структура группы $\Omega_n/\Omega_n \cap Z_n = P\Omega_n(K, f)$

Особое строение алгебр Клиффорда при $n = 3$ и $n = 4$ дает важные сведения о структуре соответствующих ортогональных групп (см. также гл. IV, § 8), и мы начнем с изучения этих двух случаев, *без ограничения на индекс* ν (который, таким образом, может равняться нулю.)

А) $n = 3$. Пусть $(e_i)_{1 \leqslant i \leqslant 3}$ — ортогональный базис пространства E. Подалгебра $C^+(f)$ имеет в этом случае размерность 4. Ее базис составляют единица 1 и три элемента

$$i_1 = e_2 e_3, \quad i_2 = e_3 e_1, \quad i_3 = -\alpha_3 e_1 e_2 \tag{12}$$

с таблицей умножения

$$\begin{gathered} i_1 i_2 = i_3, \quad i_h i_k = -i_k i_h \quad \text{при} \quad h \neq k, \\ i_1^2 = \beta_1, \quad i_2^2 = \beta_2, \quad i_3^2 = -\beta_1 \beta_2, \end{gathered} \tag{13}$$

где $\alpha_k = f(e_k, e_k)$, $\beta_1 = -\alpha_2 \alpha_3$, $\beta_2 = -\alpha_3 \alpha_1$. Таким образом, $C^+(f)$ — это *обобщенная алгебра кватернионов* над K, соответствующая элементам $\beta_1 \in K$, $\beta_2 \in K$. Результаты § 7 уточняются следующим образом:

1) *Для всякого вращения* $u \in O_3^+$ *элемент* s_u *есть обратимый кватернион, и, обратно, всякий обратимый кватернион есть элемент вида* s_u.

Первая часть этого утверждения была доказана в § 7. Для доказательства обратного утверждения можно рассуждать следующим образом (Эйхлер [2]). Будем говорить, что кватернион z *чистый*, если он не содержит скалярной компоненты. Антиавтоморфизм J алгебры $C^+(f)$ (см. § 7) есть единственный антиавтомофизм этой алгебры, оставляющий на месте только элементы из K, и чистые кватернионы z могут быть определены условием $z^J = -z$. Положим, далее, $j = e_1e_2e_3$. Если рассматривать пространство E как вложенное в $C(f)$, то отображение $x \to xj$ отображает его изоморфно на пространство чистых кватернионов. Из того что $N(t) = tt^J = t^Jt \in K$ для любого кватерниона t, легко следует, что если z — чистый кватернион и t — любой обратимый кватернион, то tzt^{-1} — чистый кватернион. Для любого $x \in E$ теперь $txt^{-1} = t(xj)t^{-1}j^{-1}$, так что $txt^{-1} \in E$, откуда и вытекает доказываемое утверждение (см. п. 4) § 7) [1]).

Из этого результата немедленно получается следствие:

2) *Группа* $O_3^+(K, f)$ *изоморфна факторгруппе* C^{+*}/K^*; *где* C^{+*} *обозначает группу обратимых элементов алгебры* $C^+(f)$ (*кватернионов*). *Группа* $O_3'(K, f)$ *изоморфна факторгруппе группы кватернионов* t, *норма* $N(t)$ *которых равна* 1, *по подгруппе* $\{-1, +1\}$.

Известно, что условие обратимости кватерниона z состоит в том, что его норма $N(z) = zz^J$ должна быть отлична от нуля. Легко видеть, что на пространстве чистых кватернионов билинейная форма $xy^J + yx^J$ эквивалентна форме f с точностью до множителя и что, если $N(z) = 0$ для какого-то кватерниона $z \neq 0$, существует *чистый* кватернион $z' \neq 0$, для которого $N(z') = 0$. Следовательно, если $\nu = 0$, то $C^+(f)$ — *тело*. Напротив, если $\nu = 1$, то в $C^+(f)$ имеются делители нуля; в этом случае $C^+(f) = K_{(2)}$ где $K_{(2)}$ — алгебра матриц порядка 2 над K. Группа C^{+*} в этом случае изоморфна группе $GL_2(K)$. Отсюда получаем (см. § 2):

3) *Если* $\nu = 1$, *то группа* $O_3^+(K, f)$ *изоморфна проективной группе* $PGL_2(K)$, *а ее коммутант* $\Omega_3(K, f)$ — *группе* $PSL_2(K)$; *группа* $\Omega_3(K, f)$ *проста, если только* $K \neq \mathbf{F}_3$.

Для случая когда $\nu = 0$ и K — не диадическое *локальное поле*, Поллак [3] нашел все нормальные делители группы $\Omega_3(K, f)$.

---

[1]) Элементы $x \in E$ могут быть при $n \leqslant 4$ охарактеризованы как такие элементы из $C^-(f)$, что $x^J = x$. Этим можно воспользоваться для более непосредственного доказательства того, что $txt^{-1} \in E$. — *Прим. перев.*

В) $n=4$. В этом случае центр T алгебры $C^+(f)$ есть прямая сумма K и $Ke_1e_2e_3e_4$, где $(e_i)_{1\leqslant i\leqslant 4}$ — ортогональный базис пространства E. Кроме того, $(e_1e_2e_3e_4)^2=\Delta$, где Δ — дискриминант формы f в базисе (e_i). В зависимости от того, является Δ квадратом в K или нет, алгебра T есть либо прямая сумма двух полей, изоморфных K, либо квадратичное расширение поля K. Заметим, что при $\nu=2$ всегда имеет место первый случай, при $\nu=1$ — второй случай; при $\nu=0$ могут представиться оба случая.

Элементы i_h, определенные равенствами (12), порождают подалгебру L в алгебре $C^+(f)$, являющуюся обобщенной алгеброй кватернионов над K. Поскольку $T\cap L=K$ и всякий элемент из T коммутирует со всеми элементами из L, алгебра $C^+(f)$ может быть отождествлена с *тензорным произведением* $T\otimes L$ (над K). Положим $j=e_1e_2e_3e_4$; тогда

$$ji_1=-\alpha_2\alpha_3e_1e_4,\quad ji_2=-\alpha_3\alpha_1e_2e_4,\quad ji_3=\alpha_1\alpha_2\alpha_3e_3e_4.$$

Для $t=\lambda_0+\lambda_1i_1+\lambda_2i_2+\lambda_3i_3\in C^+(f)$, где $\lambda_k\in T$, имеем $t^J=\lambda_0-\lambda_1i_1-\lambda_2i_2-\lambda_3i_3$, поскольку J оставляет на месте все элементы из T. Отсюда получается, что $N(t)=tt^J=\lambda_0^2-\lambda_1^2\beta_1-\lambda_2^2\beta_2+\lambda_3^2\beta_1\beta_2\in T$.

4) *Обратимый элемент $t\in T\otimes L$ является элементом вида s_u, где $u\in O_4^+$, тогда и только тогда, когда $N(t)\in K$* (Эйхлер [2]).

Действительно, в § 7 мы видели, что если $t=s_u$, то $N(t)\in K$. Обратно, пусть $N(t)\in K$. Тогда $y=txt^{-1}=txt^J/N(t)$ для всякого $x\in E$, так что $y^J=y$. С другой стороны, ясно, что $y\in C^-(f)$. Следовательно, $y\in E$. Ввиду утверждения 4) § 7 этого достаточно для доказательства.

Из предыдущего следует, что *группа $O_4'(K, f)$ изоморфна факторгруппе группы кватернионов $t\in T\otimes L$, удовлетворяющих условию $N(t)=1$, по подгруппе* $\{-1, +1\}$.

Рассмотрим теперь отдельно два описанных выше случая.

BI) *Δ не является квадратом в K.* Если обозначить через $f_1(x, y)$ ограничение формы $f(x, y)$ на гиперплоскости H, ортогональной к e_4, то из 2) следует, что *группа*

$O_4'(K, f)$ изоморфна группе $O_3'(K(\sqrt{\Delta}), f_1)$. Если индекс ν формы f равен 1, то можно считать, что индекс формы f_1 также равен 1. Ввиду 3) отсюда получается такое следствие:

5) *Если $\nu = 1$, то группа $\Omega_4(K, f)$ проста и изоморфна группе $PSL_2(K(\sqrt{\Delta}))$.* (Заметим, что если K конечно, то $K(\sqrt{\Delta})$ содержит не менее 9 элементов.)

Если $\nu = 0$, то форма f_1 также имеет *индекс* 0 над $K(\sqrt{\Delta})$. В самом деле, если бы в H нашлись такие два ненулевых вектора x, y, что $f(x + \sqrt{\Delta}\, y,\ x + \sqrt{\Delta}\, y) = 0$, то x и y должны были бы быть ортогональны друг другу и имело бы место равенство $f(x, x) = -\Delta f(y, y)$. Но из определения Δ тогда следовало бы, что в плоскости, ортогональной к x и y, существует изотропный вектор (для формы f), что противоречит предположению.

BII) *Δ является квадратом в K*; скажем, $\Delta = \omega^2$, где $\omega \in K$. Пусть $c' = {}^1/_2(1 + \omega^{-1}j)$, $c'' = {}^1/_2(1 - \omega^{-1}j)$, тогда c' и c'' — два ортогональных идемпотента в $C^+(f)$, так что алгебра $C^+(f)$ есть прямая сумма двух алгебр кватернионов Lc' и Lc'', каждая из которых изоморфна L, с центрами Kc' и Kc'' соответственно. Всякий обратимый элемент алгебры $C^+(f)$ представляется в виде $t = ac' + bc''$, где a и b — обратимые элементы алгебры L. Условие $N(t) \in K$ означает, что $N(a) = N(b)$; при этом $N(t) = N(a) = N(b)$. В частности, $N(t) = 1$ тогда и только тогда, когда $N(a) = N(b) = 1$. Учитывая, что $O_4' \cap Z_4$ состоит из двух элементов (см. § 7), получаем, что группа *$O_4'/(O_4' \cap Z_4)$ изоморфна прямому произведению $O_3'(K, f_1) \times O_3'(K, f_1)$*. В частности,

6) *Если $\nu = 2$, то группа $\Omega_4/(\Omega_4 \cap Z_4)$ изоморфна прямому произведению $PSL_2(K) \times PSL_2(K)$* (множители которого *просты*, если $K \neq \mathbf{F}_3$).

Эти результаты можно уточнить следующим образом. Для всякого $x \in E$ имеем $xj = -jx$, так что $c'x = xc''$, $c''x = xc'$. Если $t = ac' + bc''$ $(a \in L,\ b \in L)$, то $t^{-1} = a^{-1}c' + b^{-1}c''$ и

$$txt^{-1} = c'(axb^{-1}) + c''(bxa^{-1}).$$

Предположим для простоты, что $f(e_4, e_4) = 1$ (этого всегда можно добиться, умножив форму f на константу).

Всякий элемент $x \in E$ однозначно представляется в виде $x = e_4\alpha + j_0 z$, где $\alpha \in K$, $j_0 = e_1e_2e_3$, а $z \in L$ — чистый кватернион. Сопоставим вектору x кватернион $\tilde{x} = \alpha + \omega z$. Учитывая, что $j = j_0 e_4 = \omega(c' - c'')$ и что e_4 коммутирует со всеми кватернионами, легко проверить, что

$$\tilde{x} = c'xe_4 + c''e_4x = c'xe_4 + e_4c'x.$$

Из этого выводится, что вектору txt^{-1} соответствует кватернион $a\tilde{x}b^{-1}$. Таким образом, если отождествить E с L посредством линейного отображения $x \to \tilde{x}$, то *всякое вращение пространства E представится в виде $y \to ayb^{-1}$, где a и b — такие кватернионы, что $N(a) = N(b)$, и, обратно, всякое такое преобразование будет вращением.*

C) $n \geqslant 5$. Имеется следующая фундаментальная теорема (Диксон [1], [2], [3], Дьёдонне [4]):

Если $n \geqslant 5$ и $\nu \geqslant 1$, то группа $\Omega_n/(\Omega_n \cap Z_n)$ проста.

Принцип приводимого ниже доказательства принадлежит Тамагаве [1]; оно использует идею Ивасавы, уже применявшуюся нами в § 2 и 4. Мы ограничимся для простоты случаем, когда $K \neq \mathbf{F}_3$, и затем укажем (не входя в детали), каким образом Тамагава избегает этого исключительного случая. Доказательство основывается на нескольких предварительных леммах.

7) *Пусть D, D', D_1, D'_1 — четыре изотропные прямые, причем D и D' не ортогональны друг другу и D_1 и D'_1 также не ортогональны друг другу. Тогда существует такой элемент $v \in \Omega_n$, что $v(D) = D_1$ и $v(D') = D'_1$.*

Пусть P (соответственно P_1) — гиперболическая плоскость, определяемая прямыми D и D' (соответственно D_1 и D'_1). Тогда существует такое преобразование $w \in \Omega_n$, что $w(P) = P_1$ (см. § 8, 2)). Поэтому можно считать, что $P = P_1$. Далее, поскольку гиперболическая плоскость содержит только две изотропные прямые, то доказательство сводится к случаю, когда $D_1 = D'$, $D'_1 = D$. Пусть a — неизотропный вектор, ортогональный к P. В плоскости P существуют векторы x с любым наперед заданным значением $f(x, x) \in K$ и, в частности, вектор b, для которого $f(b, b) = f(a, a)$. В силу теоремы Витта существует такое преобразование $t \in O_n$, что $t(a) = b$. Обозначим через s отражение относительно гиперплоскости, ортогональной к a. Тогда $s(D) = D$, $s(D') = D'$. Преобразование $s' = tst^{-1}$ будет отражением относительно гиперплоскости, ортогональной к b, и $s'(D) = D'$, $s'(D') = D$. Преобразование $v = s's = tst^{-1}s^{-1} \in \Omega_n$ будет искомым.

Заметим, что эта лемма справедлива при любых $n \geqslant 3$ и $\nu \geqslant 1$ (мы используем это в лемме 8).

8) *Пусть a, b, b' — три различных изотропных вектора, причем $f(a, b) = f(a, b') = 0$. Тогда существует такой элемент $v \in \Omega_n$, что $v(a) = a$ и $v(b) = b'$.*

Предположим сначала, что $f(b, b') \neq 0$. Пусть P — гиперболическая плоскость, определяемая векторами b и b'. Существует четвертый изотропный вектор a', такой, что $f(a, a') \neq 0$, $f(a', b) = f(a', b') = 0$ (гл. I, п. 1 § 11). Ортогональное дополнение R в E к плоскости, определяемой векторами a и a', неизотропно и имеет размерность $\geqslant 3$. Обозначим через f_1 ограничение формы f на R. Из 7) следует, что существует такое преобразование $v' \in \Omega_{n-2}(K, f_1)$, что $v'(b) = b'$. Продолжим v' до преобразования пространства E, тождественного на ортогональном дополнении к R. Полученное преобразование $v \in \Omega_n(K, f)$ и будет искомым.

Если $f(b, b') = 0$, рассмотрим такой изотропный вектор a', что $f(a, a') \neq 0$, и определим подпространство R так же, как и выше. Обозначим через b_1 и b'_1 ненулевые векторы, содержащиеся в пересечениях подпространства R с вполне изотропными плоскостями $Ka + Kb$ и $Ka + Kb'$ соответственно. Пусть c — изотропный вектор, лежащий в R и не ортогональный к b_1; тогда c не ортогонален и к b, поскольку $f(a, c) = 0$. Применяя дважды первую часть доказательства, находим такое преобразование $v_1 \in \Omega_n$, что $v_1(a) = a$, $v_1(b) = b_1$. Поступая так же с векторами b' и b'_1, мы приходим в конце концов к тому, что достаточно найти преобразование $w \in \Omega_n$, для которого $w(a) = a$, $w(b_1) = b'_1$. Для этого возьмем такое преобразование $w' \in \Omega_{n-2}(K, f_1)$, что $w'(b_1) = b'_1$, и продолжим его до преобразования $w \in \Omega_n(K, f)$, тождественного на ортогональном дополнении к R.

Из п. 3) § 3 немедленно вытекает, что группа PO_n (и, *тем более*, $P\Omega_n$) действует *точно* на множестве C изотропных прямых пространства E.

9) *Группа $P\Omega_n$, рассматриваемая как группа перестановок множества C, примитивна.*

Предположим противное, т. е. что C допускает нетривиальное разбиение, совместимое с действием группы $P\Omega_n$. Пусть M — одно из множеств такого разбиения и D, D' — два его различных элемента. Можно считать, что прямые D и D' не ортогональны. В самом деле, если бы они были ортогональны, то из 8) следовало бы, что M содержит все изотропные прямые, ортогональные к D *или* D'. Существует изотропная прямая D'', ортогональная к D, но не ортогональная к D' (гл. I, п. 1, § 11). Тогда $D'' \in M$, и пару (D, D') можно заменить на пару (D'', D').

Итак, предположим, что прямые D и D' не ортогональны. Из 7) следует, что M содержит все изотропные прямые, не ортогональные к D *или* D'. Если $\nu = 1$, то из этого уже следует, что $M = C$. Если $\nu > 1$, то существует изотропная прямая D_1, ортогональная к D, отличная от D и не ортогональная к D' (гл. I, п. 1, § 11). Согласно предыдущему, $D_1 \in M$. В силу 8) существует преобразование из Ω_n, оставляющее на месте прямую D и переводящее прямую D_1 в любую изотропную прямую, ортогональную к D и отличную от нее. Следовательно, M содержит все изотропные прямые, ортогональные к D, и, значит, $M = C$.

Покажем теперь, что к примитивной группе $P\Omega_n$ применима лемма 4 § 2, если определить подходящим образом группы H_x.

10) *Пусть a — изотропный вектор, L — изотропная гиперплоскость, ортогональная к a. Для всякого вектора $y \in L$ сдвиг $t_a: z \to z + af(z, y)$ в гиперплоскости L однозначно продолжается до ортогонального преобразования $\rho_{a,y}$ пространства E.*

Существование преобразования $\rho_{a,y}$ вытекает из теоремы Витта, если проверить, что t_a является ортогональным преобразованием гиперплоскости L; но это немедленно следует из того, что $f(a, z) = 0$ для всех $z \in L$. Для доказательства единственности рассмотрим изотропный вектор b, не ортогональный к a. Пусть P — гиперболическая плоскость, содержащая a и b. Если два ортогональных преобразования u, u' совпадают с t_a на L, то они совпадают с t_a на подпространстве P^0. Преобразование $u'u^{-1}$ оставляет неподвижными все векторы из P^0 и, следовательно, сохраняет плоскость P. Более того, $u'u^{-1}$ оставляет на месте изотропный вектор $a \in P$. Следовательно, $u'u^{-1}$ — тождественное преобразование.

11) *В обозначениях* п. 10)

$$\rho_{a,y}\rho_{a,y'} = \rho_{a,y+y'} \quad \text{при} \quad y \in L,\ y' \in L,$$

$$\rho_{a,\lambda y} = \rho_{\lambda a,y} \quad \text{при} \quad \lambda \in K,\ \lambda \neq 0,$$

$$v\rho_{a,y}v^{-1} = \rho_{v(a),v(y)} \quad \text{для любого} \quad v \in O_n(K, f).$$

В самом деле, для доказательства этих равенств достаточно проверить совпадение значений их членов на векторах из L или, для третьего равенства, из $v(L)$; но это очевидно.

Из соотношений 11) следует, что для данного изотропного вектора a преобразования $\rho_{a,y}$, где y пробегает L, образуют *абелеву подгруппу* H_a в группе O_n. При этом $H_{\lambda a} = H_a$, так что H_a зависит только от $x = Ka \in C$. Образ группы H_a в PO_n, очевидно, изоморфен H_a; обозначим его через H_x. Для всякого $v \in O_n$ имеем $vH_av^{-1} = H_{v(a)}$. Отсюда следует, в частности, что *H_x является нормальным делителем стационарной подгруппы точки x в PO_n.*

12) *Группа $P\Omega_n$ порождается своими подгруппами H_x, $x \in C$.*

Докажем вначале, что $H_x \in P\Omega_n$ при любом $x \in C$. В обозначениях доказательства утверждения 10) достаточно показать, что $\rho_{a,y} \in \Omega_n$ для всех векторов y некоторого *ортогонального базиса* пространства P^0. Поэтому можно ограничиться случаем, когда вектор y *не изотропен.* При этом условии сдвиг t_a совпадает с ограничением на L произведения ss' отражений относительно гиперплоскостей, ортогональных к векторам y и $y' = y - {}^1/_2 f(y, y)a$. Так как $f(y', y') = f(y, y)$, то по теореме Витта существует такое преобразование $u \in O_n$, что $u(y) = y'$. Тогда имеем $s' = usu^{-1}$, и $\rho_{a,y}$ совпадает на L с $susu^{-1}$. Ввиду 10) отсюда следует, что $\rho_{a,y} = susu^{-1} \in \Omega_n$. Заметим теперь, что группа Ω_n порождается произведениями вида $susu^{-1}$, где s — отражение относительно неизотропной гиперплоскости V, а $u \in O_n$ (§ 6, п. 4).

Пусть z — вектор, ортогональный к V. Если плоскость P, определяемая векторами z и $u(z)$, изотропна и a — изотропный вектор этой плоскости (определенный однозначно с точностью до пропорциональности), то $susu^{-1} \in H_a$ в силу предыдущего вычисления. Предположим теперь, что плоскость P неизотропна. Тогда существует 3-мерное неизотропное подпространство W, содержащее плоскость P и изотропный вектор c. Это очевидно, если P — гиперболическая плоскость: тогда можно взять $c \in P$. В противном случае, поскольку изотропные векторы не могут лежать в одной гиперплоскости, существует изотропный вектор $c \notin P$, не ортогональный к P; в этом случае в качестве W можно взять $P + Kc$. (Действительно, $W = P + Kc$ не может содержать вполне изотропной плоскости, так как она имела бы изотропное пересечение с P; с другой стороны, в силу выбора c невозможно, чтобы $W \cap W^0 = Kc$.) Обозначим через f_1 ограничение формы f на W. Согласно 3), коммутант группы $O_3(K, f_1)$ прост. Следовательно, ограничение преобразования $susu^{-1}$ на W есть произведение ограничений на W преобразований вида $\rho_{a,y}$, где a и y *принадлежат* W (поскольку в простой группе подгруппы, сопряженные к любой неединичной подгруппе, порождают всю группу). Так как эти преобразования тождественны на W^0, то и на всем пространстве E преобразование $susu^{-1}$ есть произведение преобразований вида $\rho_{a,y}$.

13) *Группа $P\Omega_n$ совпадает со своим коммутантом.*

Достаточно показать, что каждая из подгрупп H_x содержится в коммутанте группы $P\Omega_n$. Возьмем такое $\lambda \in K$, что $\lambda \neq 0$ и $\lambda^2 \neq 1$. Пусть a, b — два изотропных вектора, причем $f(a, b) = 1$. Обозначим через P гиперболическую плоскость, определяемую этими векторами, и через v — вращение плоскости P, для которого $v(a) = \lambda a$, $v(b) = \lambda^{-1}b$. Мы знаем, что $v^2 \in \Omega_n$ (§ 6, п. 4)). Из соотношений 11) следует, что для всякого вектора y, ортогонального к a,

$$v^2\rho_{a,y}v^{-2}\rho_{a,y}^{-1} = \rho_{a,(\lambda^2-1)y}\ ^{1)}.$$

[1]) Поскольку $\rho_{a,y+\mu a} = \rho_{a,y}$, можно считать, что y ортогонален к b; тогда $v(y) = y$. — *Прим. перев.*

Так как $\lambda^2 - 1 \neq 0$, то тем самым доказано, что всякий элемент подгруппы H_a является коммутантом в Ω_n.

Таким образом, все условия для применения леммы 4 § 2 выполнены, что и требовалось доказать.

Оригинальное доказательство Тамагавы несколько отлично от приведенного выше. Он сразу рассматривает группу Ω'_n, *порожденную преобразованиями* $\rho_{a,y}$ *в группе* $O_n(K, f)$, и *непосредственно* показывает, что группа $P\Omega'_n$ *примитивна*. Затем он доказывает, что $\Omega'_n = \Omega_n$, и заканчивает доказательство так же, как и выше. Поскольку простота группы $PSL_2(K)$ при этом не используется, случай $K = \mathbf{F}_3$ не является для него исключительным нигде, кроме доказательства утверждения 13), которое в этом случае может быть проверено простым вычислением, использующим предположение, что $n \geqslant 5$.

В действительности проведенное нами доказательство позволяет утверждать, что *всякий нормальный делитель группы* $O_n^+(K, f)$ $(n \geqslant 5, \nu \geqslant 1)$, *не содержащийся в* Z_n, *содержит* $\Omega_n(K, f)$.

Заметим, наконец, что число элементов группы вращений $O_n^+(\mathbf{F}_q, f)$ равно

$$(q^{n-1} - 1)\, q^{n-2} (q^{n-3} - 1)\, q^{n-4} \ldots (q^2 - 1)\, q$$

при *нечетном* n (в этом случае все ортогональные группы от n переменных над полем $\mathbf{F}_q$ изоморфны) и при *четном* $n = 2m$ —

$$(q^{2m-1} - \varepsilon q^{m-1})(q^{2m-2} - 1)\, q^{2m-3} \ldots (q^2 - 1)\, q,$$

где $\varepsilon = 1$, если $(-1)^m \Delta$ есть квадрат в поле $\mathbf{F}_q$, и $\varepsilon = -1$ в противном случае (Диксон [1], стр. 160). Так как для конечного поля K индекс формы f всегда $\geqslant 1$ при $n \geqslant 3$ и группа K^*/K^{*2} состоит из 2 элементов, то $\Omega_n(\mathbf{F}_q, f)$ — подгруппа *индекса* 2 в $O_n^+(\mathbf{F}_q, f)$ (см. § 8), и при четном n группа $\Omega_n \cap Z_n$ содержит 2 или 1 элементов в зависимости от того, является дискриминант Δ квадратом в $\mathbf{F}_q$ или нет.

§ 10. Группа $O_n(K, Q)$

(K — поле характеристики 2, форма Q не дефектна.)

Напомним, что $n = 2m$ четно и группа $O_n(K, Q)$ является подгруппой симплектической группы $Sp_{2m}(K)$, соответствующей билинейной форме f, ассоциированной с квадратичной формой Q (гл. I, § 16).

Централизатор группы $O_n(K, Q)$ *в* $\Gamma L_n(K)$ находится так же, как в § 3 (с заменой отражений ортогональными сдвигами и изотропных векторов — особыми). Таким образом устанавливается, что этот централизатор совпадает с группой гомотетий H_n, за исключением следующих двух случаев:

1°. $n=2$, $K=\mathbf{F}_4$, $\nu=1$. В этом случае централизатор содержит, помимо гомотетий, полулинейное преобразование, меняющее местами два особых вектора e_1, e_2, таких, что $f(e_1, e_2)=1$.

2°. $n=2$, $K=\mathbf{F}_2$, $\nu=1$. В этом случае $O_n(K, Q)$ есть группа порядка 2, совпадающая со своим централизатором.

Таким образом, кроме этого последнего случая, *центр* группы $O_n(K, Q)$ состоит лишь из единицы.

Каждой недефектной форме Q ставится в соответствие *алгебра Клиффорда* $C(Q)$ (Арф [1], Шевалле [1]). Это факторалгебра тензорной алгебры $T(E)$ по двустороннему идеалу $\mathfrak{a}_1$, порожденному элементами вида $x\otimes x - Q(x)$ (и содержащему идеал, порожденный элементами $x\otimes y + y\otimes x - f(x, y)$). Алгебра $C(Q)$ имеет размерность 2^{2m} над K. Пространство E может быть отождествлено с подпространством элементов первой степени алгебры $C(Q)$. При этом для любых $x\in E$, $y\in E$ имеем

$$xy+yx=f(x, y), \tag{14}$$

$$x^2=Q(x). \tag{15}$$

В частности, если $(e_i)_{1\leqslant i\leqslant 2m}$ — *симплектический базис* пространства E (относительно формы f), т. е. $f(e_i, e_j)=f(e_{m+i}, e_{m+j})=0$ и $f(e_i, e_{m+j})=\delta_{ij}$ при $1\leqslant i\leqslant m$, $1\leqslant j\leqslant m$, то

$$\begin{gathered} e_i^2=Q(e_i), \qquad e_{m+i}^2=Q(e_{m+i}), \\ e_ie_j=e_je_i, \quad e_{m+i}e_{m+j}=e_{m+j}e_{m+i}, \\ e_ie_{m+j}+e_{m+j}e_i=\delta_{ij} \end{gathered} \tag{16}$$

при $1\leqslant i\leqslant m$, $1\leqslant j\leqslant m$. *Центр* алгебры $C(Q)$ совпадает с K.

Линейные комбинации элементов e_H (определенные, как в § 7), соответствующих множествам H, состоящим из четного числа элементов (элементы *четной степени* в $C(Q)$), образуют подалгебру $C^+(Q)$ размерности 2^{2m-1} над K. Она порождается произведениями $e_ie_j(1 \leqslant i \leqslant \leqslant j \leqslant 2m)$ и единицей. Центр T алгебры $C^+(Q)$ двумерен; его базис составляют 1 и элемент

$$\zeta = e_1e_{m+1} + e_2e_{m+2} + \ldots + e_me_{2m}, \tag{17}$$

удовлетворяющий условию

$$\zeta^2 + \zeta = \Delta(Q), \tag{18}$$

где

$$\Delta(Q) = Q(e_1)Q(e_{m+1}) + \ldots + Q(e_m)Q(e_{2m}). \tag{19}$$

Говорят, что $\Delta(Q)$ — *псевдодискриминант* формы Q относительно симплектического базиса $(e_i)_{1 \leqslant i \leqslant 2m}$ (Арф [1], Кнезер [2]). Пусть u — симплектическое преобразование. Положим

$$u(e_i) = \sum_{j=1}^{m} a_{ij}e_j + \sum_{j=1}^{m} b_{ij}e_{m+j},$$

$$u(e_{m+i}) = \sum_{j=1}^{m} c_{ij}e_j + \sum_{j=1}^{m} d_{ij}e_{m+j}.$$

Обозначим через $\Delta(Q_1)$ псевдодискриминант формы Q_1, определяемой равенством $Q_1(x) = Q(u(x))$, относительно того же базиса (e_i). Тогда

$$\Delta(Q_1) = \Delta(Q) + \wp(D(u)), \tag{20}$$

где $\wp(\xi) = \xi + \xi^2$, а $D(u)$ — *инвариант Диксона* преобразования u, определяемый формулой

$$D(u) = \sum_{i,j} (\alpha_j a_{ij} c_{ij} + \beta_j b_{ij} d_{ij} + b_{ij} c_{ij}), \tag{21}$$

в которой $\alpha_i = Q(e_i)$, $\beta_i = Q(e_{m+i})$ (Диксон [1], стр. 206; Дьёдонне [20]). Если u — *ортогональное преобразование*, то $D(u) = 0$ или $D(u) = 1$. Кроме того, отображение $u \to D(u)$ является гомоморфизмом группы $O_n(K, Q)$ в аддитивную группу поля K. Ортогональные преобразования u, для которых $D(u) = 0$, образуют *подгруппу индекса* 2 в $O_n(K, Q)$, называемую *группой вращений* и обозначаемую через $O_n^+(K, Q)$. Для ортогонального *сдвига* t всегда $D(t) = 1$.

1) *Всякое преобразование из* $O_n(K, Q)$ *есть произведение ортогональных сдвигов, кроме случая, когда* $K = \mathbf{F}_2$, $n = 4$ *и* $\nu = 2$ (Дьёдонне [4]; другое доказательство у Шевалле [1], стр. 20—21). Более того, можно показать, что, за вышеупомянутым исключением, всякое ортогональное преобразование представляется в виде произведения не более чем n ортогональных сдвигов (Дьёдонне [19]). При этом вращения могут быть охарактеризованы как такие ортогональные преобразования, которые представляются в виде произведения *четного* числа ортогональных сдвигов. Замечания, сделанные в § 6, о возможности преобразовать с помощью вращения данное подпространство V в другое данное подпространство W (такое, что ограничения формы Q на V и W эквивалентны) сохраняют силу, если заменить слова «вполне изотропный» на «особый» (даже в указанном выше исключительном случае).

2) *При* $n \geqslant 4$ *центр группы* $O_n^+(K, Q)$ *состоит лишь из единицы*. Доказательство может быть проведено так же, как в § 6, если заметить, что для всякой неизотропной плоскости P существует вращение (произведение двух ортогональных сдвигов в направлении векторов, лежащих в P), подпространством неподвижных точек которого является P^0.

3) *Группа* $O_2^+(K, Q)$ *коммутативна*. Следует различать два случая, в зависимости от индекса ν формы Q.

a) Если $\nu = 1$, то в базисе, составленном из особых векторов, матрицы преобразований из O_2^+ имеют вид $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, где $\lambda \in K^*$. Таким образом, в этом случае группа $O_2^+(K, Q)$ *изоморфна* K^*.

b) Если $\nu = 0$, то в симплектическом базисе $Q(x) = \xi_1^2 + \xi_1\xi_2 + \alpha\xi_2^2$ [1]), где многочлен $X^2 + X + \alpha$ неприводим над K. Пусть $K_1 = K(\omega)$ — сепарабельное квадратичное

[1]) Точнее, этого можно добиться, умножая форму Q на скаляр. — *Прим. перев.*

расширение поля K, получаемое присоединением к K корня ω этого многочлена. Отождествим пространство E с K_1 так, чтобы вектор $(1, 0)$ отождествлялся с единицей поля K_1. Если $\zeta = \xi + \omega\eta$, то $\bar{\zeta} = \xi + \eta + \omega\eta$ и $\zeta\bar{\zeta} = \xi^2 + \xi\eta + \alpha\eta^2$. С другой стороны, легко видеть, что всякое вращение, оставляющее на месте единицу поля K_1, тождественно. Так как всякое вращение $u \in O_2^+(K, Q)$ переводит единицу поля K_1 в элемент γ, равный 1 по норме, то оно совпадает с преобразованием $\zeta \to \gamma\zeta$. Таким образом, в этом случае группа $O_2^+(K, Q)$ *изоморфна группе элементов с нормой* 1 *в поле* K_1.

Обозначим через $\Omega_n(K, Q)$ *коммутант* ортогональной группы $O_n(K, Q)$.

4) *Группа* $\Omega_n(K, Q)$ *порождается произведениями* $t(wtw^{-1})$ *двух сопряженных ортогональных сдвигов. Она также порождается квадратами элементов группы* O_n. Доказательство такое же, как и п. 4) § 6, кроме особого случая $K = \mathbf{F}_2$, $n = 4$, $\nu = 2$, который требует специального изучения (Дьёдонне [4], стр. 45).

В оставшейся части этого параграфа мы *исключаем* из рассмотрения, если не будет оговорено противное, особый случай $K = \mathbf{F}_2$, $n = 4$, $\nu = 2$.

5) *При* $n \geqslant 4$ *группа* Ω_n *совпадает с коммутантом группы вращений* O_n^+. Доказательство, данное в п. 5) § 6, не проходит, но можно доказать это утверждение непосредственно, проверив, что коммутатор $sts^{-1}t^{-1}$ произвольных ортогональных сдвигов s, t содержится в коммутанте группы O_n^+.

Центр группы Ω_n сводится к единице (и тем самым равен $\Omega_n \cap Z_n$) при $n = 4$. Доказательство совершенно аналогично данному в § 6 для полей характеристики $\neq 2$. Правда, здесь имеется особый случай $K = \mathbf{F}_2$. В этом случае рассматриваются *эллиптические* плоскости, т. е. такие плоскости, ограничение формы $Q(x)$ на которых в симплектическом базисе записывается в виде $\xi_1^2 + \xi_1\xi_2 + \xi_2^2$. Доказывается, что всякая неособая прямая является пересечением двух эллиптических плоскостей (исключая случай, когда $n = 4$, $\nu = 2$).

6) *Для всякого ортогонального преобразования* $u \in O_n(K, Q)$ *существует такой обратимый элемент* $s_u \in$

$\in C(Q)$, определенный с точностью до скалярного множителя, что $u(x) = s_u x s_u^{-1}$ при любом $x \in E$. Преобразование u является вращением тогда и только тогда, когда s_u — элемент четной степени. Обратно, для всякого обратимого элемента s, такого, что $sEs^{-1} = E$, преобразование $x \to sxs^{-1}$ пространства E принадлежит группе $O_n(K, Q)$.

Доказательство проводится так же, как в § 7, п. 3) и 4), с заменой отражений ортогональными сдвигами.

Далее, как и в § 7, для всякого вращения $u \in O_n^+$ определяется *спинорная норма* $\theta(u) \in K^*/K^{*2}$. Образом группы O_n^+ при гомоморфизме θ является подгруппа группы K^*/K^{*2}, порожденная классами произведений $Q(x)Q(y)$, а его ядро $O'_n(K, Q) = \theta^{-1}(1)$ содержит группу $\Omega_n(K, Q)$. Заметим, что если поле K *совершенно* (в частности, если оно *конечно*), то $O'_n = O_n^+$.

Назовем *гиперболической плоскостью* всякую неизотропную плоскость, содержащую особую прямую (и, значит, содержащую ровно две такие прямые). Назовем также *гиперболическим преобразованием* (соответственно *гиперболическим вращением*) всякое ортогональное преобразование (соответственно *вращение*), оставляющее неподвижными все элементы ортогонального дополнения к гиперболической плоскости.

7) *Пусть P — гиперболическая плоскость. Всякое ортогональное преобразование (соответственно всякое вращение) может быть представлено в виде $u = sv$, где s — гиперболическое преобразование (соответственно гиперболическое вращение), связанное с плоскостью P, а $v \in \Omega_n$. Если P' — вторая гиперболическая плоскость, то существует такое преобразование $w \in \Omega_n$, что $w(P) = P'$.* Доказательство (для ортогональных преобразований) проводится так же, как в § 8, п. 2), если заметить, что ортогональный сдвиг является гиперболическим преобразованием. Далее, если u — вращение и $u = sv$, где $v \in \Omega_n$, то s также должно быть вращением. Вторая часть утверждения доказывается так же, как в § 8, п. 3).

8) *Если $n \geqslant 2$ и $\nu \geqslant 1$ (особый случай $K = \mathbf{F}_2$, $n = 4$, $\nu = 2$ исключается), то спинорная норма есть гомоморфизм группы O_n^+ на группу K^*/K^{*2}, ядром которого*

является коммутант Ω_n. Факторгруппа O_n^+/Ω_n тем самым изоморфна группе K^*/K^{*2}.

Доказательство проводится так же, как в § 8.

Изучение алгебры Клиффорда при $n=4$, как и в § 9, позволяет определить структуру групп $O_4(K, Q)$. Пусть $(e_i)_{1\leqslant i\leqslant 4}$ — симплектический базис, т. е. $f(e_1, e_3) = f(e_2, e_4) = 1$ и $f(e_i, e_j) = 0$ для любой другой пары индексов. Положим $Q(e_1) = \alpha$, $Q(e_2) = \beta$, $Q(e_3) = \gamma$, $Q(e_4) = \delta$. Центр T алгебры $C^+(Q)$ есть прямая сумма K и $K\zeta$, где $\zeta = e_1e_3 + e_2e_4$. При этом $\zeta^2 + \zeta = \Delta$, где $\Delta = \alpha\gamma + \beta\delta$ — псевдодискриминант формы Q. В зависимости от того, имеет Δ вид $\wp(\rho)$ при $\rho \in K$ или нет, алгебра T есть либо сумма двух полей, изоморфных K, либо сепарабельное квадратичное расширение поля K. По теореме Витта при $\nu = 2$ всегда имеет место первый случай (и можно считать, что $\alpha = \beta = \gamma = \delta = 0$); при $\nu = 1$ всегда имеет место второй случай (и можно считать, что $\beta = \delta = 0$, а $\alpha\gamma$ не имеет вида $\wp(\rho)$). При $\nu = 0$ могут представиться оба случая.

Определим инволюцию J алгебры $C(Q)$, как в § 7. Имеет место следующий критерий, доказываемый так же, как в случае характеристики $\neq 2$ (§ 9, п. 4)).

9) *Для того чтобы обратимый элемент t алгебры $C^+(Q)$ был элементом вида s_u, где $u \in O_4^+$, необходимо и достаточно, чтобы элемент $N(t) = tt^J$ принадлежал полю K.*

Из этого вытекает, что *группа $O_4'(K, Q)$ изоморфна группе обратимых элементов алгебры $C^+(Q)$ с нормой $N(t)$, равной* 1.

Рассмотрим отдельно несколько случаев.

I. $\nu=2$. Тогда алгебра $C^+(Q)$ является прямой суммой двух простых алгебр с центрами $(1+\zeta)K$ и ζK соответственно. Базис первой составляют элементы $1+\zeta$, e_1e_2, e_3e_4 и $j = e_1e_2e_3e_4$, базис второй — элементы e_1e_4, e_2e_3, $e_1e_3\zeta = j + e_1e_3$ и $e_2e_4\zeta = j + e_2e_4$. Легко видеть, что каждая из этих двух алгебр изоморфна алгебре матриц порядка 2 над K и при отождествлении ее с этой алгеброй[1]) норма $N(t)$ совпадает с определителем. Отсюда получаем

[1]) Причем ее центр отождествляется с K. — *Прим. перев.*

10) *Если* $\nu = 2$, $K \neq \mathbf{F}_2$, *то группа* $\Omega_4(K, Q)$ *изоморфна прямому произведению* $SL_2(K) \times SL_2(K)$ (каждый множитель которого является *простой* группой (§ 2)).

В исключительном случае, когда $\nu = 2$, $K = \mathbf{F}_2$, группа O_4^+ [1]) изоморфна группе элементов $t \in C^+(Q)$ с нормой $N(t)$, равной 1, и, значит, изоморфна прямому произведению $SL_2(\mathbf{F}_2) \times SL_2(\mathbf{F}_2)$, множители которого суть разрешимые группы порядка 6. Группа Ω_4, порожденная произведениями пар сдвигов (Дьёдонне [4], стр. 45), является в данном случае подгруппой индекса 2 в O_4^+, а коммутант группы O_4^+ является подгруппой индекса 2 в Ω_4. Эта последняя подгруппа есть прямое произведение двух циклических групп порядка 3.

II. $\nu = 1$. Центр T алгебры $C^+(Q)$ является в данном случае сепарабельным квадратичным расширением поля K. Элементы 1, e_1e_2, e_3e_4 и $j = e_1e_2e_3e_4$ образуют базис алгебры $C^+(Q)$ над T. Легко видеть, что алгебра $C^+(Q)$ изоморфна алгебре матриц порядка 2 над T, и при отождествлении ее с этой алгеброй норма $N(t)$ совпадет с определителем. Отсюда получаем

11) *Если* $\nu = 1$, *то группа* $\Omega_4(K, Q)$ *изоморфна группе* $SL_2(T)$ *и, значит, проста* (поскольку T содержит не менее 4 элементов; см. § 2).

III. $\nu = 0$. Как указывалось выше, здесь могут быть два случая.

а) $\Delta = \wp(\rho)$, где $\rho \in K$. Тогда $C^+(Q)$ изоморфна прямой сумме двух простых алгебр с центрами $(\rho + \zeta)K$ и $(1 + \rho + \zeta)K$ соответственно (если $\Delta = 0$, то возьмем $\rho = 1$). Первая из них имеет в качестве базиса элементы $\rho + \zeta$, $(\rho + \zeta)e_1e_2$, $(\rho + \zeta)e_3e_4$, $(\rho + \zeta)e_1e_2e_3e_4$. Она изоморфна алгебре кватернионов A_1 над K с таблицей умножения

$$i_1^2 = \alpha\beta, \quad i_2^2 = \gamma\delta, \quad i_2 i_1 = i_1 i_2 + \rho.$$

Вторая имеет в качестве базиса элементы $\rho + \zeta + 1$, $(\rho+\zeta+1)e_1e_4$, $(\rho+\zeta+1)e_2e_3$ и $(\rho+\zeta+1)(e_1e_3+e_1e_2e_3e_4)$ и изоморфна алгебре кватернионов A_2 над K с таблицей умножения

$$j_1^2 = \alpha\delta, \quad j_2^2 = \beta\gamma, \quad j_2 j_1 = j_1 j_2 + \rho.$$

[1]) Совпадающая с O_4'. — *Прим. перев.*

Из предположения $\nu = 0$ следует, что обе эти алгебры являются *телами*. В самом деле, норма элемента $x = x_0 + x_1 i_1 + x_2 i_2 + x_3 i_1 i_2$ алгебры A_1 представляется квадратичной формой

$$x_1^2 + \rho x_0 x_3 + \alpha\beta\gamma\delta x_3^2 + \alpha\beta x_1^2 + \rho x_1 x_2 + \gamma\delta x_2^2,$$

которая с точностью до множителя эквивалентна форме

$$Q(z) = \alpha z_1^2 + z_1 z_3 + \gamma z_3^2 + \beta z_2^2 + z_2 z_4 + \delta z_4^2,$$

где $z = \sum_{i=1}^{4} z_i e_i$. Эквивалентность осуществляется подстановкой

$$z_1 = x_0 + \alpha\gamma x_3, \quad z_2 = \alpha x_1 + \delta x_2, \quad z_3 = \alpha\rho x_3, \quad z_4 = \rho x_2.$$

Так же исследуется алгебра A_2. Таким образом, если обозначить через N_1 (соответственно N_2) *группу элементов алгебры* A_1 (*соответственно* A_2) *с нормой* 1, *то группа* $\Omega_4(K, Q)$ *изоморфна прямому произведению* $N_1 \times N_2$.

b) Δ *не представляется в виде* $\wp(\rho)$. Тогда T есть сепарабельное квадратичное расширение поля K, и алгебра $C^+(Q)$ является алгеброй кватернионов над T, имеющей в качестве базиса элементы 1, e_1e_2, e_3e_4 и $e_1e_2e_3e_4$. Таблица умножения этой алгебры такая же, как у A_1, с заменой ρ на $1 + \zeta$, а норма с точностью до множителя эквивалентна форме $Q(z)$, рассматриваемой как *квадратичная форма над* T. Из предположения $\nu = 0$ следует так же, как и в случае характеристики $\neq 2$, что форма $Q(z)$ имеет *индекс* 0 *над* T. Действительно, пусть $Q(x + \zeta y) = 0$. Тогда $Q(x) = \Delta Q(y)$ и $Q(y) = f(x, y)$. Пользуясь определением псоевдодискриминанта Δ, отсюда легко вывести, что в плоскости, ортогональной к $xK + yK$, имеется особый вектор $\neq 0$. Таким образом, $C^+(Q)$ — *тело кватернионов* над T и группа $\Omega_4(K, Q)$ изоморфна *группе его элементов с нормой* 1.

Для $n \geqslant 6$ имеется следующая теорема (Диксон [1], Дьёдонне [4]):

12) *Если* $n \geqslant 6$ *и* $\nu \geqslant 1$, *то группа* $\Omega_n(K, Q)$ *проста.* (Напомним, что форма Q не дефектна).

Доказательство Тамагавы для поля характеристики $\neq 2$ проходит здесь *без изменений* (если повсюду вместо изотропных векторов рассматривать особые), исключая доказательство леммы 13 § 9 в случае $K = \mathbf{F}_2$, когда требуется небольшое специальное рассуждение, использующее предположение $n \geqslant 6$.

Это доказательство позволяет, кроме того, утверждать, что всякий нормальный делитель группы $O_n^+(K, Q)$ ($n \geqslant 6$, $\nu \geqslant 1$) содержит ее коммутант $\Omega_n(K, Q)$.

Заметим, наконец, что число элементов группы вращений $O_{2m}^+(\mathbf{F}_q, Q) = \Omega_{2m}(\mathbf{F}_q, Q)$, где $q = 2^h$, равно

$$(q^m - 1)(q^{2(m-1)} - 1)\, q^{2(m-1)} \ldots (q^2 - 1)\, q^2,$$

если $\nu = m$ и

$$(q^m + 1)(q^{2(m-1)} - 1)\, q^{2(m-1)} \ldots (q^2 - 1)\, q^2,$$

если $\nu = m - 1$ (Диксон [1], стр. 206).

§ 11. Группа $O_n(K, Q)$

(K — поле характеристики 2, форма Q дефектна.)

Напомним (гл. I, § 16), что дефект d формы Q обладает тем свойством, что $n - d = 2p$ — четное число и что всегда можно рассматривать группу $O_n(K, Q)$ как подгруппу симплектической группы $Sp_{2p}(K)$, образованную такими преобразованиями u, что $Q(u(x)) + Q(x) \in M$, где M — подпространство поля K, рассматриваемого как векторное пространство над K^2; при этом можно предполагать, что M содержит единицу. Поэтому единственный случай, который нуждается в рассмотрении, — это когда $M \neq K$, т. е. поле K *несовершенно* (и, значит, *бесконечно*). Кроме того, ограничение Q_1 формы Q на $2p$-мерном подпространстве E_1 не дефектно, а условие $\nu \geqslant 1$ влечет за собой, что в E_1 существуют особые векторы $\neq 0$. Так как группа $O_{2p}(K, Q_1)$ является подгруппой группы $O_n(K, Q)$, то *центр* группы $O_n(K, Q)$ состоит лишь из единицы (§ 10).

Вектор $a \in E_1$ называется *полуособым*, если $Q(a) \in M$. Преобразования из группы $O_n(K, Q)$ переводят полуособые векторы в полуособые. Ортогональный сдвиг (гл. I, § 16) в направлении полуособого вектора называется *полуособым*. Такой сдвиг $x \to x + \lambda f(x, a) a$ характеризуется условием $\lambda \in M$ (автоматически выполняющимся при $\lambda = 1$).

1) *Всякое ортогональное преобразование является произведением ортогональных сдвигов.* Доказательство проводится так же, как в случае недефектных форм, причем предположение о бесконечности K исключает все особые случаи (Дьёдонне [4], стр. 55).

2) *При $2p \geqslant 2$ и $\nu \geqslant 1$ группа $\Omega_n(K, Q)$, порожденная полуособыми сдвигами, проста.* Доказательство совершенно аналогично доказательству простоты группы $T_n(K, f)$, порожденной унитарными сдвигами (Дьёдонне [4], стр. 55—58).

3) *Группа $\Omega_n(K, Q)$ (при $2p \geqslant 2$, $\nu \geqslant 1$) является коммутантом группы $O_n(K, Q)$.* Доказательство, имеющееся у Дьёдонне [4], стр. 59—60, не применимо в случае $2p = 4$, $\nu = 2$. Чтобы исследовать и этот случай, достаточно (см. там же) доказать, что если P, P' — две гиперболические плоскости в подпространстве E_1, то существует преобразование из группы Ω_n, преобразующее P в P'. Используя предположение $\nu = 2$, можно доказать это утверждение, следуя, с небольшой модификацией, методу, примененному в работе Дьёдонне [13], стр. 380—382, для унитарной группы. Модификация состоит в следующем. Пусть $(e_i)_{1 \leqslant i \leqslant 4}$ — симплектический базис пространства E_1, образованный особыми векторами, удовлетворяющими условиям: $f(e_1, e_2) = f(e_3, e_4) = 1$ и $f(e_i, e_j) = 0$ для остальных пар индексов $(i \leqslant j)$. Доказывается, что произведение *и трех* (а не *двух*) ортогональных сдвигов в направлении векторов $a_k = \lambda_k e_2 + \mu_k e_3$ сохраняет (в целом) плоскости $e_1 K + e_3 K$ и $e_2 K + e_4 K$ и что $u(e_1) = e_1 + e_3 \alpha$, где $\alpha \neq 0$. Для этого достаточно заметить, что в поле K можно найти шесть элементов λ_k, μ_k $(1 \leqslant k \leqslant 3)$, таких, что

$$\lambda_1 + \lambda_2 + \lambda_3 = 0, \ \mu_1 + \mu_2 + \mu_3 = 0, \ \lambda_1\mu_1 + \lambda_2\mu_2 + \lambda_3\mu_3 \neq 0$$

§ 12. Унитарные и ортогональные группы, соответствующие анизотропным формам

Бóльшая часть полученных в § 4—11 результатов о строении ортогональных и унитарных групп перестает быть справедливой, когда рассматриваемые квадратичные или полулинейные формы *анизотропны*.

Рассмотрим, например, рациональное *p-адическое поле* $\mathbf{Q}_p$. Пусть f — невырожденная симметричная билинейная форма индекса 0 от $n=3$ или 4 переменных над $\mathbf{Q}_p$. Тогда можно найти такой ортогональный базис пространства E, что *всякое* преобразование из $O_n(\mathbf{Q}_p, f)$ записывается в этом базисе матрицей, все элементы которой — *целые p-адические числа* (Эйхлер [2], стр. 57). Пусть G_k — множество преобразований $u \in O_n$, матрица которых имеет вид $1+p^kV$, где V — матрица с целыми p-адическими элементами. Предыдущее замечание показывает, что G_k — *нормальный делитель группы* O_n. Легко доказывается, что G_k/G_{k+1} — *абелева* p-группа, не равная единице, и что пересечение подгрупп G_k содержит только единичный элемент группы O_n (Дьёдонне [11]). Сравнение с § 9 показывает, что этот случай в некотором роде противоположен случаю $\nu \geqslant 1$.

Аналогичные примеры можно привести для ортогональных групп $O_n(K, f)$ от *произвольного* числа переменных, так же как и для ортогональных групп $O_n(K, Q)$ над полем характеристики 2 и для унитарных групп $U_n(K, f)$ (Дьёдонне [4]). Результаты § 8 о группах O_n^+/Ω_n и $\Omega_n \cap Z_n$ также перестают быть справедливыми для анизотропных форм. Например, при $K=\mathbf{R}$ (поле действительных чисел) для положительно определенной формы f имеем $\Omega_n = O_n^+$, хотя группа $\mathbf{R}^*/\mathbf{R}^{*2}$ состоит из 2 элементов. Можно привести пример анизотропной симметричной билинейной формы f от 4 переменных над полем $\mathbf{Q}$ рациональных чисел, дискриминант которой есть квадрат, но для которой симметрия $x \to -x$ не принадлежит коммутанту Ω_n (Дьёдонне [9], стр. 93). Можно также привести пример унитарной группы $U_n(K, f)$ от 2 переменных над полем $\mathbf{Q}(\sqrt{2})$, для которой группа U_n^+ не совпадает со своим коммутантом, в противоположность результатам § 5 (Дьёдонне [10], стр. 948).

Предыдущие примеры строились для специальных полей K. Легко устанавливается, что строение, например, группы $O_n(K, f)$ для анизотропной формы f *существенно зависит от основного поля* K. Так, хорошо известно, что группа $O_n^+(\mathbf{R}, f)$, где f — анизотропная форма, *проста* при $n \geqslant 3$ и $n \neq 4$, в то время как строение ортогональных групп от 3 переменных над p-адическими полями, как было показано выше, совершенно иное.

Единственными типами полей, которые хорошо изучены с этой точки зрения, являются *локально компактные нормированные поля* (характеристики $\neq 2$) и *поля алгебраических чисел*. Что касается первых, то описанная выше ситуация, имеющая место для p-адических полей, является общей для этого типа полей (Дьёдонне [11], Эйхлер [2], стр. 57). Для p-адических и $\mathfrak{p}$-адических полей встречаются только случаи $n = 3$ и $n = 4$, поскольку при $n \geqslant 5$ всякая симметричная билинейная форма над таким полем имеет индекс $\geqslant 1$ (Витт [1], стр. 40).

Изучение ортогональных групп над *полем алгебраических чисел* K тесно связано с теорией эквивалентности квадратичных форм над таким полем (гл. I, § 8). Не входя в детали этой теории, укажем, что она основана на изучении квадратичных форм $f_\mathfrak{p}$, получаемых из формы f *расширением поля K до каждого из его локальных полей* $K_\mathfrak{p}$ (где $\mathfrak{p}$ — архимедово или неархимедово нормирование поля K). Ее главные результаты выражаются удивительнейшим образом в виде принципа *«перехода от локального к глобальному»* [1]). Например, для того чтобы форма f имела индекс $\geqslant 1$, необходимо и достаточно, чтобы она обладала этим свойством над *каждым* из полей $K_\mathfrak{p}$ [2]). Это приводит к предположению, что аналогичный принцип должен управлять строением ортогональных групп. Это предположение частично подтверждается работами Кнезера [1], основной результат которых (улучшающий результаты, полученные ранее Дьёдонне [9], [10], [12] ме-

---

[1]) Этот принцип называют иногда «принципом Хассе». — *Прим. перев.*

[2]) То есть чтобы этим свойством обладала каждая из форм $f_\mathfrak{p}$. — *Прим. перев.*

нее мощным методом) состоит в доказательстве (при $\nu = 0$) следующих трех теорем:

A) *Пусть* $\mathfrak{p}_i$ $(1 \leqslant i \leqslant r)$ — *вещественные нормирования поля* K, *для которых форма* $f_{\mathfrak{p}_i}$ *имеет индекс* 0. *Тогда при* $n \geqslant 3$ *спинорная норма определяет изоморфизм группы* O_n^+/O_n' *на подгруппу группы* K^*/K^{*2}, *образованную классами чисел поля* K, *положительных в каждом из полей* $K_{\mathfrak{p}_i}$.

B) *При* $n \geqslant 2$ *и* $n \neq 4$ *имеем* $O_n' = \Omega_n$.

C) *При* $n \geqslant 5$ *группа* $P\Omega_n = \Omega_n/(\Omega_n \cap Z_n)$ *проста.*

Для доказательства теоремы A) заметим, что образ пространства $K_{\mathfrak{p}}^n$ при отображении $x \to f_{\mathfrak{p}}(x, x)$ есть все $K_{\mathfrak{p}}$ для любого нормирования $\mathfrak{p}$ поля K, отличного от нормирований $\mathfrak{p}_i$ и (при $n = 3$) от конечного числа неархимедовых нормирований $\mathfrak{q}_j$, для которых форма $f_{\mathfrak{q}_j}$ имеет индекс 0. Для каждого j образ пространства $K_{\mathfrak{q}_j}^n$ при отображении $x \to f_{\mathfrak{q}_j}(x, x)$ есть дополнение к классу по модулю $K_{\mathfrak{q}_j}^{*2}$ элемента δ_j. Пусть теперь $\gamma \in K$ таково, что $\gamma > 0$ в каждом из полей $K_{\mathfrak{p}_i}$. Существует элемент $\alpha \in K$, представляемый при любом i формой $f_{\mathfrak{p}_i}$ и не принадлежащий ни при каком j ни классу δ_j, ни классу $\gamma\delta_j^{-1}$ по модулю $K_{\mathfrak{q}_j}^{*2}$. Элементы α и $\beta = \alpha^{-1}\gamma$ представляются тогда формой $f_{\mathfrak{p}}$ при любом $\mathfrak{p}$ и, значит, формой f в силу принципа перехода от локального к глобальному. Отсюда следует, что класс γ по модулю K^{*2} является спинорной нормой произведения двух отражений. Тем самым теорема A) доказана.

Для доказательства теоремы B) рассмотрим сначала случай $n \leqslant 3$. Всякое преобразование $t \in O_n^+$ представляется тогда в виде произведения двух отражений s_a и s_b относительно гиперплоскостей, ортогональных к векторам a и b соответственно. При $t \in O_n'$ можно считать, что $f(a, a) = f(b, b)$, и из теоремы Витта следует тогда, что s_a и s_b сопряжены в группе O_n и, значит, $t \in \Omega_n$. Пусть теперь $n \geqslant 5$. Элемент $t \in O_n^+$ представляется в виде произведения отражений s_{a_i} $(1 \leqslant i \leqslant m)$. Затем ищется плоскость $P \subset K^n$, содержащая такие векторы b_i, что $f(b_i, b_i) = f(a_i, a_i)$ при любом i. Отражения s_{a_i} и s_{b_i} будут тогда сопряжены в группе O_n. Поэтому если обозначить через t' произведение отражений s_{b_i}, то $t't^{-1} \in \Omega_n$, и если $t \in O'_n$, то и $t' \in O'_n$. Но t' можно рассматривать как вращение в плоскости P, и доказательство сводится к первому случаю. Таким образом, остается доказать существование плоскости P. С этой целью строится квадратичная форма $g(y, y) = f(a_1, a_1)(\eta_1^2 - \delta\eta_2^2)$ в пространстве K^2, принимающая значения $f(a_i, a_i)$ $(1 \leqslant i \leqslant \leqslant m)$, для чего достаточно взять в качестве δ норму элемента λ расширения L поля K, порожденного квадратными корнями $\sqrt{f(a_i, a_i)/f(a_1, a_1)}$ при $2 \leqslant i \leqslant m$. Далее, нужно показать, что в K^n существует плоскость P, ограничение на которой формы f эквивалентно g. В силу принципа перехода от локального к глобальному это достаточно проверить над каждым из полей $K_\mathfrak{p}$. Для неархимедовых нормирований $\mathfrak{p}$ это вытекает из предположения $n \geqslant 5$. Небольшое дополнительное рассуждение показывает, что это верно также и для архимедовых нормирований.

Доказательство теоремы C) намного сложнее. Оно состоит из двух частей. Сначала для произвольного нормального делителя N группы Ω_n, не содержащегося в ее центре, доказывается, что

I) *N содержит нормальный делитель группы O_n, не содержащийся в ее центре.*

С этой целью доказывается, прежде всего, что

1) *N содержит плоское вращение, отличное от* 1. В самом деле, пусть $u \in N$ — элемент, не лежащий в центре группы Ω_n. Тогда существует такая плоскость T, что $u(T) \neq T$. Пусть t — вращение плоскости T, принадлежащее группе Ω_n. Тогда преобразование $v = t^{-1}utu^{-1}$ принадлежит N, отлично от 1 и оставляет неподвижными векторы из подпространства V размерности $\geqslant n - 4$. Пусть $x \in V$, y ортогонален к V и s — вращение плоскости $S = Kx + Ky$, принадлежащее группе Ω_n и такое, что $s^2 \neq 1$. Тогда $w = s^{-1}vsv^{-1}$ будет искомым плоским вращением.

Пусть W — плоскость вращения w. Предположим сначала, что для всякого вещественного нормирования $\mathfrak{p}$ форма $f_{\mathfrak{p}}$ и ее ограничение на подпространстве W^0, ортогональном к W, либо обе имеют индексы 0, либо обе имеют положительный индекс. Тогда теоремы A) и B), примененные к W^0 и к K^n, показывают, что $O_n(K, f) = \Omega_n(K, f) O_{n-2}(K, g)$, где g — ограничение формы f на W^0, и, значит, всякое преобразование вида sws^{-1}, где $s \in O_n$, представляется также в виде twt^{-1}, где $t \in \Omega_n$. Отсюда следует, что нормальный делитель группы O_n, порожденный w, удовлетворяет требованиям предложения I.

Если вращение w не удовлетворяет предыдущему условию, то можно построить другое плоское вращение $u \in N$, которое ему удовлетворяет. Для этого рассмотрим 3-мерное подпространство V, содержащее W. Пусть h — ограничение формы f на V. Рассмотрим вещественные нормирования $\mathfrak{p}$, для которых форма $f_{\mathfrak{p}}$ имеет положительный индекс. Легко видеть, что для каждого такого нормирования в пространстве $V \otimes_K K_{\mathfrak{p}}$ существует плоскость $U_{\mathfrak{p}}$, ортогональное дополнение $U_{\mathfrak{p}}^0$ к которой в пространстве $K_{\mathfrak{p}}^n$ содержит изотропные векторы. Пусть $u_{\mathfrak{p}}$ — вращение плоскости $U_{\mathfrak{p}}$, отличное от 1. Из простоты группы $O_3^+(\mathbf{R}, h_{\mathfrak{p}}) = \Omega_3(\mathbf{R}, h_{\mathfrak{p}})$ вытекает, что $u_{\mathfrak{p}}$ разлагается в произведение элементов вида $sws^{-1}tw^{-1}t^{-1}$, где s и t принадлежат $\Omega_3(\mathbf{R}, h_{\mathfrak{p}})$, поскольку эти произведения образуют нормальный делитель группы $\Omega_3(\mathbf{R}, h_{\mathfrak{p}})$, не равный единице. Пусть $\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$ — рассматриваемые вещественные нормирования. Тогда при любом i элемент $u_{\mathfrak{p}_i}$ может быть представлен в виде

$$u_{\mathfrak{p}_i} = s_{i1} w s_{i1}^{-1} t_{i1} w^{-1} t_{i1}^{-1} \ldots s_{ik} w s_{ik}^{-1} t_{ik} w^{-1} t_{ik}^{-1},$$

с *одним и тем же* k (поскольку всегда можно взять несколько из элементов s_{ij}, t_{ij} равными 1), причем s_{ij} и t_{ij} принадлежат $\Omega_3(\mathbf{R}, h_{\mathfrak{p}_i})$ при $1 \leqslant j \leqslant k$. Затем можно использовать следующую *аппроксимационную лемму*:

2) *Пусть заданы конечное число нормирований* $\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$ *поля* K *и для каждого* i *элемент* v_i *группы* $O_n^+(K_{\mathfrak{p}_i}, f_{\mathfrak{p}_i})$ (*соответственно* $\Omega_n(K_{\mathfrak{p}_i}, f_{\mathfrak{p}_i})$). *Тогда суще-*

ствует последовательность $(v^{(n)})$ *элементов группы* $O_n^+(K, f)$ *(соответственно* $\Omega_n(K, f)$*), которая при каждом* i *сходится к* v_i *в группе* $O_n(K_{\mathfrak{p}_i}, f_{\mathfrak{p}_i})$.

Эта лемма легко выводится из обычной аппроксимационной теоремы для поля K с помощью представления преобразований v_i в виде произведения отражений.

Возвращаясь к доказательству утверждения I, применим лемму 2) к элементам s_{ij} и t_{ij} при каждом j. Тогда мы получим элемент $u \in N \cap \Omega_3(K, h)$, сколь угодно близкий к элементу $u_{\mathfrak{p}_i}$ в группе $\Omega_3(\mathbf{R}, h_{\mathfrak{p}_i})$ при $1 \leqslant i \leqslant m$. Легко видеть, что при этом можно добиться того, чтобы элемент u удовлетворял нашим требованиям.

Таким образом, можно предполагать, что N — нормальный делитель *в группе* O_n. Точнее, нужно доказать следующее утверждение.

II) *Всякий нормальный делитель* N *группы* O_n, *не содержащийся в ее центре, но содержащийся в группе* Ω_n, *совпадает с* Ω_n.

Говорят, что гиперплоскость H пространства K^n *универсальна*, если образы H и K^n при отображении $x \to f(x, x)$ одинаковы. В силу принципа перехода от локального к глобальному это условие при $n \geqslant 5$ равносильно тому, что если a — вектор, ортогональный к H, то $f_{\mathfrak{p}}(a, a) > 0$ (соответственно < 0) для всякого такого вещественного нормирования $\mathfrak{p}$, что сигнатура формы $f_{\mathfrak{p}}$ равна $(n-1, 1)$ (соответственно $(1, n-1)$). Справедливо следующее утверждение:

3) *Группа* Ω_n *порождается произведениями отражений* $s_x^{-1}s_y s_x s_y^{-1}$, *для которых гиперплоскость, ортогональная к* x, *универсальна.*

Достаточно (§ 6, п. 4) показать, что всякое произведение $u = s^{-1}tst^{-1}$ (s и t — отражения) представляется в виде $s_x^{-1}s_y s_x s_y^{-1}$, где x удовлетворяет условию нашего утверждения. Преобразование u является плоским вращением. В его плоскости имеется вектор x, ортогональный к некоторой универсальной гиперплоскости. Это следует из предыдущей характеризации таких векторов и из аппроксимационной теоремы для поля K. Тогда $u = s_x s_z$, причем можно считать, что $f(x, x) = f(z, z)$, поскольку спинорная норма u равна 1. Пусть s_y — отражение, переставляющее x и z. Тогда $u = s_x^{-1} s_y s_x s_y^{-1}$, что и требовалось доказать.

Таким образом, достаточно доказать, что образующие группы Ω_n, рассмотренные в лемме 3, принадлежат N. Это вытекает из следующей леммы:

4) *Если a и b — два таких вектора пространства K^n, что $a \neq \pm b$, $f(a, a) = f(b, b)$, и если гиперплоскость H отражения, переставляющего a и b, универсальна, то существует такой элемент $t \in N$, что $t(a) = b$.*

Действительно, предположим, что эта лемма доказана. В обозначениях леммы 3 ограничимся случаем, когда $s_x(y) \neq \pm y$ (иначе $s_x^{-1} s_y s_x s_y^{-1} = 1$), и применим лемму 4 к векторам y и $s_x(y)$. Тогда получим $s_x(y) = t(y)$, где $t \in N$. Преобразование $t^{-1} s_x = u$ перестановочно с s_y, так что $s_x^{-1} s_y s_x s_y^{-1} = u^{-1} (t^{-1} s_y t s_y^{-1}) u \in N$.

Лемма 4) будет вытекать из следующей леммы:

5) *В предположениях леммы 4 существуют такие элементы $u \in N$ и $c \in K^n$, что $f(c, c) = f(a, a)$, $f(a, c) = f(b, c) = f(a, u(a))$.*

В самом деле, тогда в силу теоремы Витта существуют такие преобразования v, w из O_n, что $v(a) = a$, $v(u(a)) = c$, $w(a) = b$, $w(u(a)) = c$ и элемент $t = (wuw^{-1})^{-1} (vuv^{-1})$ удовлетворяет требованиям леммы 4).

Доказательство самой леммы 5) разбивается на несколько этапов.

6) *Существует такое преобразование $v \in \Omega_n$, что $v(a) \in H$ (т. е. $f(a, v(a)) = f(b, v(a))$) и $v(a)$ не лежит в плоскости $P = Ka + Kb$.*

В силу предположения относительно H существует такой вектор $e \in H$, что $f(e, e) = f(a, a)$, и по теореме Витта существует такое преобразование $v_1 \in O_n$, что $v_1(a) = e$. Умножив v_1 в случае необходимости на отражение относительно H, можно считать, что $v_1 \in O_n^+$. Обозначим через g ограничение формы f на H. Из предположения об универсальности H вытекает, что группы спинорных норм для f и для g одинаковы. Следовательно, существует такое преобразование $v_2 \in O_{n-1}(K, g)$, что $v_2 v_1 \in O'_n(K, f) = \Omega_n(K, f)$ (в силу теоремы В)), если рассматривать v_2 как элемент группы $O_n(K, f)$, считая, что оно тождественно на векторах, ортогональных к H.

Наконец, можно найти такое преобразование $v_3 \in \in O_{n-1}(K, g)$, что $v_3(v_2(v_1(a))) \notin P$. Обозначая той же *буквой* v_3 продолжение v_3 до преобразования пространства K^n, видим, что преобразование $v = v_3 v_2 v_1$ удовлетворяет требованиям леммы 6.

Рассмотрим теперь подпространство P^0, ортогональное к P, и пусть $\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$ — нормирования (архимедовы или неархимедовы), для которых ограничение формы $f_{\mathfrak{p}_i}$ на $P^0 \otimes_K K_{\mathfrak{p}_i}$ анизотропно (таких нормирований имеется конечное число, поскольку $\dim P^0 \geqslant 3$). Так как $n \geqslant 5$, то группы $P\Omega_n(K_{\mathfrak{p}_i}, f_{\mathfrak{p}_i})$, как известно, просты. Если w — элемент из N, не содержащийся в центре группы O_n, то при каждом i имеем

$$v = s_{i1} w s_{i1}^{-1} t_{i1} w^{-1} t_{i1}^{-1} \ldots s_{ik} w s_{ik}^{-1} t_{ik} w^{-1} t_{ik}^{-1},$$

где s_{ij} и t_{ij} лежат в $\Omega_n(K_{\mathfrak{p}_i}, f_{\mathfrak{p}_i})$. Применяя к s_{ij} и t_{ij} лемму 2), можно сделать вывод о существовании элемента $u \in N$, сколь угодно близкого к v *в каждой из групп* $\Omega_n(K_{\mathfrak{p}_i}, f_{\mathfrak{p}_i})$. Теперь можно применить следующую *лемму непрерывности*:

7) *Пусть L — не дискретное полное нормированное поле характеристики $\neq 2$ и $g(x, x) = \sum_{i,j} \alpha_{ij}\xi_i\xi_j$ — невырожденная квадратичная форма в пространстве L^n. Тогда существует такое $\varepsilon > 0$, что из соотношений $|\alpha'_{ij} - \alpha_{ij}| \leqslant \varepsilon$ для любой пары (i, j) следует, что квадратичная форма $g'(x, x) = \sum_{i,j} \alpha'_{ij}\xi_i\xi_j$ эквивалентна форме $g(x, x)$.*

Этот результат легко получается из возможности извлечь квадратный корень в L из всякого элемента, достаточно близкого к 1.

Пусть теперь $g(x, x)$ — квадратичная форма в пространстве K^3, определяемая для векторов канонического базиса (a', b', c') равенствами $g(a', a') = g(b', b') = g(c', c') = f(a, a)$, $g(a', b') = f(a, b)$, $g(a', c') = g(b', c') = f(a, u(a))$. С помощью леммы 7) устанавливается, что если взять преобразование u достаточно близким к v в каждой из групп $\Omega_n(K_{\mathfrak{p}_i}, f_{\mathfrak{p}_i})$, то форма $g_{\mathfrak{p}_i}$ *при любом i* будет *эквивалентна ограничению формы* $f_{\mathfrak{p}_i}$ *на* *подпространстве* $Q_i \subset K^n_{\mathfrak{p}_i}$, *порожденном векторами* a, b *и* $v(a)$. Пусть d' — вектор пространства K^3, ортогональный (относительно g) векторам a' и b'. Из предыдущего следует, что для любого i существует такой вектор $d_i \in P^0 \otimes_K K_{\mathfrak{p}_i}$, что $f_{\mathfrak{p}_i}(d_i, d_i) = g_{\mathfrak{p}_i}(d', d')$. С другой стороны, для любого нормирования $\mathfrak{p}$, отличного от $\mathfrak{p}_i$, ограничение формы $f_{\mathfrak{p}}$ на $P^0 \otimes_K K_{\mathfrak{p}}$ имеет положительный индекс и, значит, существует такой вектор $d_{\mathfrak{p}} \in P^0 \otimes_K K_{\mathfrak{p}}$, что $f_{\mathfrak{p}}(d_{\mathfrak{p}}, d_{\mathfrak{p}}) = g_{\mathfrak{p}}(d', d')$. Согласно принципу перехода от локального к глобальному, существует такой вектор $d \in P^0$, что $f(d, d) = g(d', d')$. В силу определения формы g отсюда немедленно следует, что существует вектор c, удовлетворяющий требованиям леммы 5. Этим завершается доказательство теоремы C).

Таким образом, для поля алгебраических чисел K остается только выяснить структуру группы $O_3(K, f)$ при $\nu = 0$ (поскольку структура группы $O_4(K, f)$ будет тогда ясна ввиду результатов § 9). На этот счет имеются результаты только для случая, когда K есть поле $\mathbf{Q}$ рациональных чисел или, более общо, поле, имеющее *только одно вещественное нормирование.* А именно, тогда можно доказать, используя структуру ортогональной группы от 3 переменных над p-адическим полем, что при $\nu = 0$ группа $O_3(K, f)$ допускает *такую убывающую последовательность нормальных делителей* G_k, *что группы* G_k/G_{k+1} *абелевы и пересечение всех* G_k *есть единица* (Дьёдонне [11]).

Укажем, что Кнезер [1] получил аналогичные результаты для унитарных групп над полями алгебраических чисел.

§ 13. Группы подобий $GU_n(K, f)$

Мы ограничимся случаем, когда тело K *коммутативно.* Пусть Δ и r — определитель и множитель подобия $u \in GU_n(K, f)$. Из соотношения (23) § 9 гл. I получаем

$$\Delta\Delta^J = r^n.$$

Если $n = 2m + 1$ *нечетно,* то, полагая $\Delta = r^m \mu$, из предыдущего соотношения находим, что $r = \mu\mu^J$ и, значит, перобразование $h_\mu^{-1}u$, где h_μ — гомотетия $x \to x\mu$, принадлежит группе $U_n(K, f)$. Таким образом, в этом случае группа $GU_n(K, f)$ есть *произведение* (вообще говоря, не прямое) *группы* Z_n *гомотетий и унитарной группы* $U_n(K, f)$. Что касается ортогональных групп над полем K характеристики $\neq 2$, группа $GO_n(K, f)$ при нечетном n есть *прямое произведение* группы Z_n и *группы вращений* $O_n^+(K, f)$ (см. § 6, п. 2).

Если $n = 2m$ *четно*, то $\Delta = \mu r^m$, где $\mu\mu^J = 1$. Подобия, для которых $\Delta = r^m$, называются *прямыми подобиями* и образуют нормальный делитель $GU_n^+(K, f)$ в группе $GU_n(K, f)$. Если $J \neq 1$, то факторгруппа GU_n/GU_n^+ изоморфна группе элементов поля K с нормой 1, поскольку в группе $U_n(K, f)$ существуют преобразования с определителем, равным любому элементу с нормой 1.

Из предыдущего следует, что группа $M(f)$ *множителей подобий* одинакова для GU_n и для GU_n^+. Кроме того, если f_0 — приведенная анизотропная форма для формы f (от $2(m - \nu)$ переменных; см. гл. I, § 11), то $M(f) = M(f_0)$. В частности, для *симплектической группы* $M(f) = K^*$; вообще, это верно, если $\nu = m$. Структура группы $M(f)$ для четного $n = 2m$ и *анизотропной* формы f в общем случае не известна. Можно только доказать (Дьёдонне [21]), что $M(f)$ есть *подгруппа* группы $N(\Delta)$ элементов поля K_0 (поля инвариантов инволюции J), имеющих вид $aa^J + (-1)^{m-1}\Delta bb^J$; но, вообще говоря, $M(f) \neq N(\Delta)$ [1]. В случае, когда K — *поле алгебраических чисел*, можно полностью описать подгруппу $M(f)$ в группе $N(\Delta)$ (см. там же) как для унитарных групп ($J \neq 1$), так и для ортогональных.

Для группы $GO_n(K, f)$ ортогональных подобий (над полем K характеристики $\neq 2$) можно представить ее элементы при помощи алгебры Клиффорда (Эйхлер [1], [2]). Для всякого подобия u с множителем r_u и для всякого произведения $x_1x_2 \ldots x_{2k}$ четного числа векторов пространства E (погруженного в $C(f)$) положим

[1]) Здесь Δ — дискриминант формы f. — *Прим. перев.*

$\tilde{u}(x_1 \ldots x_{2k}) = r_u^{-k} u(x_1) \ldots u(x_{2k})$. Можно доказать, что это определение не зависит от представления данного элемента в виде произведения векторов пространства E и что определенное таким образом преобразование $\tilde{u}$ алгебры $C^+(f)$ является ее автоморфизмом. Для того чтобы u было прямым подобием (в случае, когда $n = 2m$), необходимо и достаточно, чтобы $\tilde{u}$ было тождественно на элементах центра T алгебры $C^+(f)$. В этом случае $\tilde{u}$ является внутренним автоморфизмом $z \to s_u z s_u^{-1}$, где s_u — элемент алгебры $C^+(f)$, определенный с точностью до множителя из T. Кроме того, $s_u s_u^I$ содержится в T, и даже в K, если m нечетно. Более детальное изучение подобий с этой точки зрения см. в работе Воненбургера [2].

Глава III

ГЕОМЕТРИЧЕСКАЯ ХАРАКТЕРИЗАЦИЯ КЛАССИЧЕСКИХ ГРУПП

§ 1. Основная теорема проективной геометрии

Пусть E, E' — правые векторные пространства одинаковой размерности n над телами K, K' соответственно. Если K и K' изоморфны, то всякое биективное полулинейное отображение u пространства E на пространство E' определяет посредством факторизации биективное отображение $\bar{u}$ проективного пространства $P(E)$ на проективное пространство $P(E')$, преобразующее каждое проективное линейное многообразие в проективное линейное многообразие той же размерности. «Основная теорема проективной геометрии» является обращением этого утверждения. Более точно, ее формулировка такова:

1) *Пусть φ — биективное отображение пространства $P(E)$ на пространство $P(E')$, преобразующие любые три коллинеарные точки пространства $P(E)$ в три коллинеарные точки пространства $P(E')$. Тогда, если $n \geqslant 3$, тела K и K' изоморфны и $\varphi = \bar{u}$, где u — биективное полулинейное отображение пространства E на пространство E'.*

Заметим вначале, что из предположения, сделанного относительно φ, следует, что для всякого проективного линейного многообразия $V \subset P(E)$ размерности $p \leqslant n-1$ множество $\varphi(V)$ также является p-мерным проективным линейным многообразием. В самом деле, пусть a_iK $(1 \leqslant i \leqslant p+1)$ — проективно независимые точки пространства $P(E)$, порождающие многообразие V. Тогда $\varphi(V)$ содержится в проективном линейном многообразии V', порожденном точками $\varphi(a_iK)$ $(1 \leqslant i \leqslant p+1)$. Дополним систему $(a_i)_{1 \leqslant i \leqslant p+1}$ до базиса $(a_i)_{1 \leqslant i \leqslant n}$ пространства E. Поскольку $\varphi(P(E)) = P(E')$ содержится в проективном линейном многообразии, порожденном n точками $\varphi(a_i K)$ $(1 \leqslant i \leqslant n)$, эти точки проективно независимы. Тем более проективно независимы $p+1$ точек $\varphi(a_i K)$, $1 \leqslant i \leqslant p+1$. Если бы множество $\varphi(V)$ было отлично от V', то нашлась бы такая точка aK пространства $P(E)$, не принадлежащая

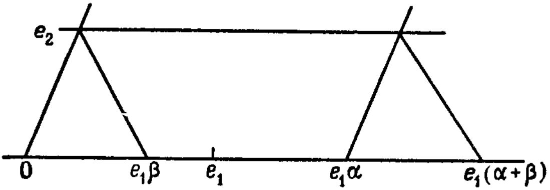

Рис. 1.

многообразию V, что $\varphi(aK) \in V'$, и тогда $(p+1)$-мерное многообразие V_1, порожденное V и aK, при отображении φ переходило бы в множество, лежащее в p-мерном многообразии V', что, как мы только что видели, невозможно.

Рассмотрим теперь базис $(e_i)_{1 \leqslant i \leqslant n}$ пространства E, точки $e_1 K$, $e_2 K$ и $e_n K$ пространства $P(E)$ и их образы $e_1' K' = \varphi(e_1 K)$, $e_2' K' = \varphi(e_2 K)$ и $e_n' K' = \varphi(e_n K)$ в пространстве $P(E')$. Векторы e_1', e_2' и e_n' линейно независимы в пространстве E'. Обозначим через D проективную прямую, порожденную точками $e_1 K$ и $e_2 K$, и через F — проективную плоскость, порожденную D и $e_n K$. Положим $D' = \varphi(D)$, $F' = \varphi(F)$. Всякая точка плоскости F, не лежащая на прямой D, единственным образом представляется в виде $(e_1\alpha_1 + e_2\alpha_2 + e_n)K$, так что дополнение к D в F может быть отождествлено с векторным пространством $L = e_1 K + e_2 K$. Всякой прямой плоскости F, отличной от D, соответствует прямая пространства L, причем любым двум прямым плоскости F, точка пересечения которых принадлежит D, соответствуют параллельные прямые пространства L (т. е. прямые, получающиеся одна из другой параллельным переносом). Отождествляя аналогичным образом дополнение к прямой D' в плоскости F' с векторным пространством $L' = e_1' K' + e_2' K'$, получаем, исходя из отображения φ, биективное отображение g пространства L на пространство L', преобразующее всякую прямую в прямую и любые две параллельные прямые в параллельные прямые. Кроме того, $g(0)=0$, и можно считать, что $g(e_1)=e'_1$, $g(e_2)=e'_2$.

Как показано на рисунках 1 и 2, при помощи проведения параллельных прямых в пространстве L можно,

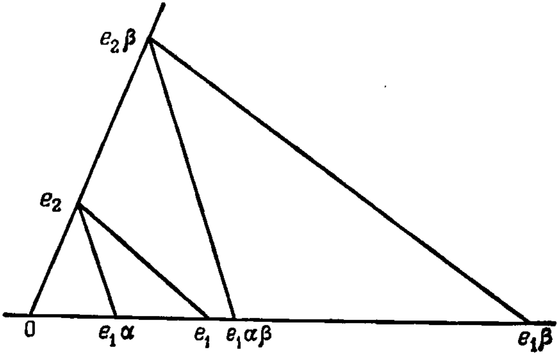

Рис. 2.

исходя из данных элементов α, β тела K, получить элементы $\alpha+\beta$ и $\alpha\beta$ как абсциссы точек прямой e_1K.

Следовательно, $g(e_1\xi)=e'_1\xi^\sigma$, где $\xi\to\xi^\sigma$ — такое биективное отображение тела K на тело K', что $(\xi+\eta)^\sigma=\xi^\sigma+\eta^\sigma$ и $(\xi\eta)^\sigma=\xi^\sigma\eta^\sigma$. Иначе говоря, σ — *изоморфизм* тела K на тело K'. Далее, поскольку прямая, соединяющая точки $e_1\xi$ и $e_2\xi$ в пространстве L, параллельна прямой, соединяющей точки e_1 и e_2, то $g(e_2\xi)=e'_2\xi^\sigma$. Наконец, точка $e_1\alpha+e_2\beta$ пространства L получается как пересечение прямых, проведенных через $e_1\alpha$ и $e_2\beta$ параллельно прямым e_2 и e_1 соответственно [1]). Следовательно, $g(e_1\alpha+e_2\beta)=e'_1\alpha^\sigma+e'_2\beta^\sigma$, так что g — полули-

[1]) То есть прямым, проведенным через 0 и e_2 и через 0 и e_1 соответственно. — *Прим. перев.*

нейное (относительно изоморфизма σ) отображение пространства L на пространство L'.

Это рассуждение применимо к любой паре точек $(e_i K,\ e_j K)$, где $1 \leqslant i < j \leqslant n-1$. Обозначим через u полулинейное относительно изоморфизма σ отображение пространства E на пространство E', определяемое равенствами $u(e_i) = e'_i$ $(1 \leqslant i \leqslant n)$[1]. Если $\bar{u}$ — соответствующее отображение пространства $P(E)$ на пространство $P(E')$, то $\bar{u}^{-1}\varphi$ будет преобразованием пространства $P(E)$, переводящим прямые в прямые и оставляющим на месте все точки каждой из прямых, соединяющих две точки $e_i K$, $e_j K$. Индукцией по p отсюда легко выводится, что это преобразование оставляет на месте все точки p-мерного линейного многообразия, определяемого любыми $p+1$ точками из числа $e_i K$. При $p = n-1$ получаем $\varphi = \bar{u}$.

Имеется следующий вариант основной теоремы:

2) *Пусть φ — биективное отображение пространства $P(E)$ на пространство $P(E')$, при котором образ любого p-мерного проективного линейного многообразия (где p — фиксированное целое число, удовлетворяющее неравенствам $1 \leqslant p \leqslant n-2$) содержится в p-мерном проективном линейном многообразии. Тогда справедливо заключение теоремы* 1).

Случай, когда $p = 1$, составляет содержание теоремы 1). Доказательство теоремы 2) можно свести к этому случаю путем постепенного понижения размерности p, если доказать, что в условиях теоремы образ всякого $(p-1)$-мерного линейного многообразия V содержится в $(p-1)$-мерном линейном многообразии.

Многообразие V есть пересечение содержащих его p-мерных многообразий. Их образы при отображении φ не могут содержаться в одном и том же p-мерном многообразии, так как тогда $\varphi(P(E))$ не совпадало бы с $P(E')$. Пусть W_1 и W_2 — два таких p-мерных многообразия, что $V = W_1 \cap W_2$ и $\varphi(W_1) \subset W'_1$, $\varphi(W_2) \subset W'_2$, где W'_1

---

[1] Векторы e'_i $(1 \leqslant i \leqslant n-1)$ необходимо предварительно нормировать таким образом, чтобы $\varphi((e_i + e_n)K) = (e'_i + e'_n)K'$. — *Прим. перев.*

и W'_2 — различные p-мерные многообразия. Тогда $\varphi(V)\subset W'_1 \cap W'_2$, откуда и вытекает доказываемое утверждение.

При $E = E'$ предыдущие теоремы дают геометрическую характеризацию коллинеаций пространства E, т. е. элементов группы $P\Gamma L_n(K)$. Они, очевидно, неверны при $n = 2$[1]. В этом случае коллинеации (или корреляции) можно охарактеризовать как отображения, сохраняющие двойные отношения, равные какому-либо элементу центра тела K, отличному от 0 и 1 и инвариантному относительно соответствующего автоморфизма (или антиавтоморфизма). См. по этому поводу Анкочеа [1], Хуа [7], Бэр [3], стр. 78—93.

При $n \geqslant 3$ основная теорема дает также характеризацию корреляций, если взять в качестве E' пространство E^*, *дуальное к* E.

§ 2. Преобразования, сохраняющие «соседство»

1. Преобразования грассманианов

В обозначениях § 1 пусть $G_r(E)$ — множество r-мерных проективных линейных многообразий пространства $P(E)$ $(0 \leqslant r \leqslant n-1)$. Тогда $G_0(E) = P(E)$; при $r > 0$ множество $G_r(E)$ называется *грассманианом* индекса r пространства E. Всякое биективное полулинейное отображение u пространства E на пространство E' (если оно существует, т. е. если тела K и K' изоморфны) определяет биективное отображение $\bar{u}_r$ множества $G_r(E)$ на множество $G_r(E')$ (в частности, $\bar{u}_0$ — это отображение, обозначавшееся в § 1 через $\bar{u}$). Кроме того, при $2r = n-2$ можно определить следующим образом биективное отображение ω_r множества $G_r(E)$ на множество $G_r(E^*)$ (где E^* — пространство, дуальное к E). Всякое r-мерное проективное линейное многообразие V пространства $P(E)$ представляется в виде $V = P(W)$, где $W \subset E$ — подпространство размерности $r+1 = n/2$. Пусть $W' \subset E^*$ — «ортогональное» ему подпростран-

---

[1]) Точнее, теорема 1) неверна, а теорема 2) бессодержательна. — *Прим. перев.*

ство, образованное линейными формами, обращающимися в 0 на W. Это левое векторное пространство над K, или правое векторное пространство над K°, размерности $n/2$. Множество $P(W')$ будет r-мерным проективным линейным многообразием в пространстве $P(E^*)$. В этих обозначениях положим $\omega_r(V) = P(W')$.

Желательно получить «геометрическую» характеризацию отображений $\bar{u}_r$ и ω_r при $r \neq 0$, подобную той, какую дает основная теорема проективной геометрии для отображений $\bar{u}_0$. С этой целью вводится понятие *отклонения* двух многообразий V_1, V_2, принадлежащих $G_r(E)$. Отклонение считается равным t, если пересечение $V_1 \cap V_2$ имеет размерность $r - t$. Это равносильно тому, что наименьшее линейное многообразие, содержащее V_1 и V_2, имеет размерность $r + t$. Два r-мерных линейных многообразия V_1, V_2 называются *соседними*, если их отклонение равно 1. Отклонение двух линейных многообразий $V_1 \in G_r(E)$, $V_2 \in G_r(E)$ может быть определено также как наименьшее целое число t, для которого существует такая конечная последовательность (U_i), состоящая из $t+1$ элементов множества $G_r(E)$, что $U_1 = V_1$, $U_{t+1} = V_2$ и многообразия U_i, U_{i+1} являются соседними при $1 \leqslant i \leqslant t$.

Это последнее замечание показывает, что если φ — биективное отображение множества $G_r(E)$ на $G_r(E')$, то φ *сохраняет отклонение любых двух многообразий* тогда и только тогда, когда φ *и* φ^{-1} *преобразуют любые два соседних многообразия в соседние многообразия.* Искомая характеризация отображений $\bar{u}_r$ дается следующей теоремой (Чоу [1]).

При $n \geqslant 3$ и $0 < r < n - 2$ всякое биективное отображение φ множества $G_r(E)$ на множество $G_r(E')$, сохраняющее отклонение любых двух многообразий, является отображением вида $\bar{u}_r$, где u — биективное полулинейное отображение пространства E на пространство E', либо (при $2r = n - 2$) — отображением вида $\bar{v}_r \circ \omega_r$, где v — биективное полулинейное отображение пространства E^* на пространство E'.

Мы ограничимся тем, что наметим в общих чертах доказательство этой теоремы.

a) В $G_r(E)$ рассматриваются максимальные подмножества, состоящие из *попарно соседних* многообразий. Доказывается, что всякое такое множество состоит либо из всех r-мерных линейных многообразий, содержащих некоторое $(r-1)$-мерное линейное многообразие (множество первого типа), либо из всех r-мерных линейных многообразий, содержащихся в некотором $(r+1)$-мерном линейном многообразии (множество второго типа).

b) Образ при отображении φ максимального множества первого типа есть максимальное множество в $G_r(E')$, которое *априори* может быть первого или второго типа. Но если для какого-нибудь *одного* максимального множества $\mathfrak{M}$ первого типа $\varphi(\mathfrak{M})$ есть множество первого типа, то образ при отображении φ *любого* другого максимального множества $\mathfrak{M}_1$ первого типа есть также множество первого типа. Доказательство этого утверждения сводится к случаю, когда $\mathfrak{M}$ и $\mathfrak{M}_1$ соответствуют соседним $(r-1)$-мерным линейным многообразиям. В этом случае достаточно заметить, что пересечение $\mathfrak{M} \cap \mathfrak{M}_1$ содержит только один элемент, в то время как пересечение максимального множества первого типа и максимального множества второго типа, если оно не пусто, содержит не менее двух элементов.

c) Ввиду описания максимальных множеств, данного в п. a), из п. b) получаем биективное отображение φ_1 множества $G_{r-1}(E)$ на $G_{r-1}(E')$ или на $G_{r+1}(E')$. Так как два $(r-1)$-мерных (соответственно $(r+1)$-мерных) линейных многообразия являются соседними тогда и только тогда, когда соответствующие им максимальные множества имеют общий элемент, то отображения φ_1 и φ_1^{-1} преобразуют соседние многообразия в соседние.

d) Если $2r \neq n-2$, то из изложенного выше следует, что φ_1 отображает $G_{r-1}(E)$ на $G_{r-1}(E')$. В самом деле, если $2r < n-2$, то отклонение двух $(r-1)$-мерных линейных многообразий не превосходит r, в то время как два $(r+1)$-мерных линейных многообразия могут иметь отклонение $r+1$. Аналогично, если

$2r > n-2$, от отклонение двух $(r+1)$-мерных линейных многообразий не превосходит $n-r-2$, в то время как существуют $(r-1)$-мерные линейные многообразия, имеющие отклонение не менее $n-r-1$. Постепенным понижением размерности получается в конце концов такое биективное отображение ψ пространства $P(E)$ на пространство $P(E')$, что $\psi(V)=\varphi(V)$ для любого r-мерного линейного многообразия $V \subset P(E)$. Утверждение 2) § 1 позволяет вывести отсюда заключение теоремы.

e) Если $2r = n-2$ и φ отображает каждое максимальное множество первого типа в максимальное множество второго типа, то $\varphi \circ \omega_r^{-1}$ отображает всякое максимальное множество первого типа в $G_r(E^*)$ в максимальное множество первого типа в $G_r(E')$, и доказательство сводится к рассмотренному выше случаю.

§ 3. Преобразования, сохраняющие «соседство»

1. Преобразования пространств изотропных многообразий

Предположим теперь, что в пространстве E задана невырожденная полуторалинейная форма $f(x, y)$, эрмитова или косоэрмитова. Если характеристика тела K равна 2, мы будем предполагать, что f есть T-форма (гл. I, § 10). Кроме того, мы будем предполагать, что *индекс* $r+1$ формы f не меньше 1. Линейное многообразие V пространства $P(E)$ будем называть *изотропным* (соответственно *вполне изотропным*), если оно имеет вид $P(W)$, где W — изотропное (соответственно вполне изотропное) подпространство пространства E (относительно формы f). Через $N_s(E)$ (или N_s) мы будем обозначать множество *s-мерных* вполне изотропных многообразий пространства $P(E)$. Всякое полуподобие $u \in \Gamma U_n(K, f)$ определяет очевидным образом биективное преобразование $\bar{u}_r$ множества N_r. Желательно было бы получить геометрическую характеризацию таких преобразований. Эта характеризация дается следующей теоремой, аналогичной теореме § 2 (Чоу [1], Дьёдонне [8]):

При $2 \leqslant r \leqslant \left[\frac{n-2}{2}\right]$ (*и, значит,* $n \geqslant 6$) *всякое биективное преобразование* φ *множества* $N_r(E)$, *обладающее тем свойством, что* φ *и* φ^{-1} *преобразуют любые два соседних многообразия в соседние, имеет вид* $\bar{u}_r$, *где* u — *некоторое полуподобие.*

Свойства вполне изотропных подпространств (гл. I, § 11) позволяют, прежде всего, доказать следующие две леммы:

a) Пусть V_1, V_2 — два вполне изотропных многообразия одинаковой размерности $s \leqslant r$. Тогда существуют два вполне изотропных многообразия W_1, W_2 максимальной размерности r, такие, что $V_1 \subset W_1$, $V_2 \subset W_2$ и $W_1 \cap W_2 = V_1 \cap V_2$.

b) Пусть V_1, V_2 — два вполне изотропных многообразия одинаковой размерности $s \leqslant r$, и пусть $s-t$ — размерность их пересечения. Тогда существует такая конечная последовательность $(W_k)_{1 \leqslant k \leqslant t+1}$ вполне изотропных многообразий размерности s, что $W_1 = V_1$, $W_{t+1} = V_2$ и многообразия W_k, W_{k+1} являются соседними при $1 \leqslant k \leqslant t$.

Далее, как и в § 2, рассматриваются максимальные множества попарно соседних r-мерных вполне изотропных многообразий. Последовательно проверяются следующие свойства:

c) Всякое максимальное множество есть множество всех вполне изотропных многообразий, содержащих некоторое вполне изотропное многообразие размерности $r-1$.

d) Так как преобразование φ, а также φ^{-1} переводит всякое максимальное множество в максимальное множество, то, ввиду c), возникает биективное преобразование φ_1 множества $N_{r-1}(E)$ вполне изотропных многообразий размерности $r-1$. Используя a), можно показать, что φ_1 и φ_1^{-1} переводят любые два соседних многообразия в соседние и что $(r-1)$-мерные вполне изотропные многообразия, содержащиеся в r-мерном вполне изотропном многообразии V, при преобразовании φ_1 переходят в $(r-1)$-мерные вполне изотропные многообразия, содержащиеся в $\varphi(V)$.

e) Постепенно понижая размерность s, можно таким образом определить биективное преобразование φ_{r-s} множества $N_s(E)$, такое, что φ_{r-s} и φ_{r-s}^{-1} переводят соседние многообразия в соседние. При $s = 0$ получается биективное преобразование $g = \varphi_r$ множества $N_0(E)$ *изотропных точек* пространства $P(E)$. Это преобразование обладает тем свойством, что если $V = P(W)$ — вполне изотропное многообразие размерности $s \leqslant r$, то множество $g(V)$, состоящее из образов точек из V при преобразовании g, совпадает с $\varphi_{r-s}(V)$. Предположение $r \geqslant 2$ позволяет тогда применить основную теорему проективной геометрии (§ 1). Это дает следующее свойство преобразования g: если $V = P(W)$ есть r-мерное вполне изотропное многообразие и $\varphi(V) = P(W')$, то ограничение g на V имеет вид $\bar{u}_W$, где u_W — биективное *полулинейное отображение* пространства W на пространство W'. Кроме того, для всех $V \in N_r(E)$ автоморфизм тела K, соответствующий отображению u_W, *один и тот же* с точностью до внутреннего автоморфизма и, следовательно, может быть сделан одинаковым для всех $V \in N_r(E)$. Это доказывается сначала для двух соседних многообразий V_1, V_2, а затем применяется b).

Если n четно и форма f *знакопеременная*, то $N_0(E) = P(E)$ и g есть тогда биективное преобразование пространства $P(E)$, преобразующее любые две ортогональные (в смысле формы f) точки в ортогональные. Так как всякая гиперплоскость пространства $P(E)$ образована точками, ортогональными к одной из ее точек, то преобразование g переводит гиперплоскости в гиперплоскости. Основная теорема проективной геометрии показывает тогда, что $g = \bar{u}$, где u — полулинейное преобразование пространства E. Выбрав в E симплектический базис и записав условие того, что u преобразует ортогональные векторы в ортогональные, легко показать, что u — полуподобие.

f) В общем случае рассмотрим два многообразия $V_1 \in N_r(E)$, $V_2 \in N_r(E)$, не имеющие общих точек. Пусть $U_0 = P(W_0)$ — $(2r+1)$-мерное проективное линейное многообразие, которое ими порождается. Можно показать, что существует такое биективное полулинейное отображение v_0 пространства W_0 на $(2r+2)$-мерное подпространство пространства E, что $\bar{v}_0(x) = g(x)$ для любой изотропной точки $x \in U_0$ (Чоу [1], стр. 47). Затем образуется возрастающая последовательность $U_0, U_1, \ldots$ $\ldots, U_{n-2r-2}$ проективных линейных многообразий пространства $P(E)$ таким образом, что многообразие U_{k+1} порождается многообразием U_k и изотропной точкой, не ортогональной к U_k. Пусть $U_k = P(W_k)$. Рекуррентным образом строится такая последовательность $v_0, v_1, \ldots$ $\ldots, v_{n-2r-2} = u$ биективных полулинейных отображений, что v_k определено на W_k, v_{k+1} продолжает v_k и $\bar{v}_k(x) =$ $= g(x)$ для всякой изотропной точки $x \in U_k$ (Дьёдонне [8], стр. 298—299). Тогда u будет биективным полулинейным преобразованием пространства E, причем $\bar{u}(V) = \varphi(V)$ для любого многообразия $V \in N_r(E)$. Кроме того, показывается, что u преобразует ортогональные векторы в ортогональные. Для этого используется тот факт, что изотропная, но не вполне изотропная прямая характеризуется тем, что она содержит только одну изотропную точку и, следовательно, переходит при преобразовании $\bar{u}$ в прямую того же типа. Окончание доказательства проводится так же, как в п. е).

Замечания. 1) Пусть E' — второе пространство той же размерности, что и E, и f' — эрмитова или косоэрмитова невырожденная полуторалинейная форма на $E' \times E'$, имеющая тот же индекс $r+1$, что и f. Вместо сохраняющих соседство биективных отображений множества $N_r(E)$ на себя можно рассматривать такие биективные отображения φ множества $N_r(E)$ на множество $N_r(E')$, что φ и φ^{-1} сохраняют соседство. Таким же образом доказывается, что тела скаляров K, K' пространств E, E' изоморфны и что $\varphi = \bar{u}_r$, где u — такое биективное полулинейное отображение пространства E на пространство E', что $f'(u(x), u(y)) = \mu(f(x, y))^{\sigma}$, где σ — изоморфизм тела K на тело K', соответствующий отображению u, а μ — отличный от нуля элемент тела K'.

2) Предыдущие рассуждения легко распространяются на случай, когда характеристика тела K равна 2, а в пространстве E задана недефектная квадратичная форма Q индекса $r+1 \geqslant 1$. Будем называть *особыми* про-

ективные линейные многообразия $V = P(W)$ пространства $P(E)$, для которых W — особое подпространство в E (относительно формы Q). Обозначим через $N_s(E)$ множество особых многообразий размерности $s \leqslant r$. Тогда теорема, сформулированная в начале этого параграфа, остается справедливой, а ее доказательство — неизменным, с точностью до того, что нужно повсюду заменить вполне изотропные многообразия на особые (Дьёдонне [8]).

3) Теорема, доказанная выше при условии $r \geqslant 2$, неверна при $r = 0$, поскольку тогда любые два элемента из $N_r(E)$ будут соседними. Она также неверна при $r = 1$, $n = 4$, когда K коммутативно и f — симметричная билинейная форма. Это следует из того, что множество N_r (E) является тогда объединением двух таких подмножеств N_r^+ и N_r^-, что два многообразия, принадлежащие одному из них, никогда не являются соседними, в то время как многообразие из N_r^+ и многообразие из N_r^- — всегда соседние (классические свойства «прямолинейных образующих» квадрик; см. § 6 гл. II и § 4 этой главы). Всякое преобразование φ, переставляющее произвольным образом элементы множества N_r^+, с одной стороны, и элементы множества N_r^- — с другой, удовлетворяет условию теоремы. Неизвестно, справедлива ли теорема в других случаях, когда $r = 1$.

4) Из результатов Чоу вытекают как частные случаи многочисленные теоремы, доказанные ранее Хуа [1], [2], [4], [6] и выраженные на языке теории матриц. Рассмотрим, например, случай, когда пространство E имеет четную размерность $2m$, а форма f знакопеременна (и, значит, тело K коммутативно). Пусть $(e_i)_{1 \leqslant i \leqslant 2m}$ — симплектический базис пространства E относительно формы f. Используя обозначения Хуа, сопоставим каждому вектору пространства E строку из его $2m$ координат в базисе (e_i). Для m векторов $z_1, \ldots, z_m$ матрицу, составленную из соответствующих им строк, запишем в виде (X, Y), где X и Y — квадратные матрицы порядка m. Если $z'_1, \ldots, z'_m$ — другие m векторов и (X', Y') — соответствующая матрица, то непосредственно проверяется,

что матрица $(f(z_i, z'_j))$ равна

$$F(X, Y, X', Y') = (X, Y)\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}\begin{pmatrix} {}^tX' \\ {}^tY' \end{pmatrix}.$$

Следовательно, условие «$f(z_i, z_j) = 0$ для всех i, j» может быть записано в виде

$$F(X, Y, X, Y) = 0. \tag{1}$$

При этом, для того чтобы вполне изотропное подпространство W, порожденное векторами z_i, имело размерность m, необходимо и достаточно, чтобы ранг матрицы (X, Y) равнялся m. Пару (X, Y) квадратных матриц порядка m, удовлетворяющую этим условиям, Хуа называет *симметричной парой*. Это название объясняется тем, что если, например, матрица Y обратима, то условие (1) может быть записано в виде $(Y^{-1}X) = {}^t(Y^{-1}X)$ и означает, таким образом, что матрица $Z = Y^{-1}X$ симметрична. Для того чтобы две симметричные пары (X, Y) и (X_1, Y_1) определяли одно и то же вполне изотропное подпространство W, необходимо и достаточно, чтобы существовала такая обратимая квадратная матрица Q порядка m, что $(X_1, Y_1) = Q(X, Y)$. В случае когда матрицы Y и Y_1 обратимы, это означает, что $Y_1^{-1}X_1 = Y^{-1}X$. Множество $N_{m-1}(E)$ может быть, таким образом, отождествлено с множеством классов симметричных пар относительно указанного выше отношения эквивалентности или с множеством симметричных матриц порядка m, пополненным «бесконечно удаленными» элементами (соответствующими симметричным парам, в которых матрица Y необратима). Далее, показывается, что отклонение двух многообразий $V = P(W)$, $V_1 = P(W_1)$, соответствующих симметричным парам (X, Y), (X_1, Y_1), равно рангу квадратной матрицы $F(X, Y, X_1, Y_1)$ (или, в случае когда матрицы Y и Y_1 обратимы, рангу разности $Z_1 - Z$ соответствующих симметричных матриц). В этих терминах легко интерпретировать теорему Чоу. Интересно отметить, что преобразование φ записывается в «неоднородных координатах» в виде

$$Z \to a(AZ^{\sigma} + B)(CZ^{\sigma} + D)^{-1},$$

где $a \in K$, а квадратные матрицы A, B, C, D удовлетворяют условиям

$$A \cdot {}^tB = B \cdot {}^tA, \quad C \cdot {}^tD = D \cdot {}^tC, \quad A \cdot {}^tD - B \cdot {}^tC = I.$$

§ 4. Преобразования, сохраняющие «соседство»

II. Преобразования пространств изотропных многообразий (продолжение)

В обозначениях § 3 предположим, что K — поле характеристики $\neq 2$, f — симметричная билинейная форма, *n четно* и r равно своему *максимальному* возможному значению $(n-2)/2$. В § 6 гл. II было указано, что множество $N_r(E)$ распадается тогда на два класса транзитивности $N_r^+(E)$, $N_r^-(E)$ относительно группы вращений $O_n^+(K, f)$ (или, точнее, ее образа в проективной группе). При этом многообразия $V_1 \in N_r(E)$, $V_2 \in N_r(E)$ принадлежат одному классу транзитивности тогда и только тогда, когда $\dim(V_1 \cap V_2) = r - 2k$ (k целое). В этом случае будем говорить, что многообразия V_1 и V_2 *соседние*, если $k = 1$, т. е. $\dim(V_1 \cap V_2) = r - 2$. При таком определении справедлива следующая теорема (Чоу [1]):

При $r \geqslant 4$ всякое биективное преобразование φ множества $N_r^+(E)$, такое, что φ и φ^{-1} преобразуют любые два соседних многообразия в соседние, имеет вид $\bar{u}_r$, где u — полуподобие.

Для доказательства так же, как и выше, рассматриваются максимальные множества *попарно соседних* линейных многообразий в $N_r^+(E)$. Последовательно устанавливаются следующие свойства:

а) Всякое максимальное множество образовано либо многообразиями из $N_r^+(E)$, имеющими $(r-1)$-мерное пересечение с некоторым многообразием из $N_r^-(E)$ (множество первого типа), либо многообразиями из $N_r^+(E)$, содержащими некоторое $(r-3)$-мерное вполне изотропное многообразие (множество второго типа).

b) Максимальное множество первого типа при преобразовании φ переходит в максимальное множество, которое *априори* может быть либо первого, либо второго типа. Однако если для какого-нибудь *одного* максимального множества $\mathfrak{M}$ первого типа $\varphi(\mathfrak{M})$ есть множество первого типа, то это верно и для любого *другого* максимального множества первого типа.

c) Если $r \geqslant 4$, то образ максимального множества первого типа не может быть множеством второго типа. Отсюда выводится, что преобразование φ может быть продолжено до преобразования всего множества $N_r(E)$, удовлетворяющего условиям теоремы § 3. Применение этой теоремы завершает доказательство.

Следующие соображения позволяют описать полуподобия u, для которых $\bar{u}_r$ сохраняет множество $N_r^+(E)$. Легко видеть, что если $V \in N_r^+(E)$, то существует полуподобие v с тем же множителем и автоморфизмом, что и u, относительного которого V инвариантно. Тогда $v^{-1}u$ есть ортогональное преобразование, переводящее V в другое многообразие из $N_r^+(E)$ и, значит, являющееся *вращением.*

Замечания. 1) Предыдущий результат можно распространить на случай, когда рассматриваются два различных пространства E, E' и отображение φ множества $N_r^+(E)$ на множество $N_r^+(E')$ (см. § 3).

2) Если K — поле характеристики 2, Q — недефектная квадратичная форма максимального индекса на E, то множество $N_r(E)$ также распадается на два класса транзитивности $N_r^+(E)$, $N_r^-(E)$ относительно группы вращений $O_n^+(K, Q)$ (гл. II, § 10). Предыдущие результаты переносятся без изменений на преобразования множества $N_r^+(E)$.

3) При $r = 1$ и $r = 2$ теорема Чоу неверна, поскольку тогда любые два многообразия из $N_r^+(E)$ соседние. Случай $r = 3$ также исключительный. В этом случае из теории «тройственности» (Шевалле [1], гл. IV) вытекает существование биективного отображения множества $N_3^-(E)$ на множество $N_0(E)$, преобразующего любые два соседних многообразия в две ортогональные изотропные

точки. При помощи этого отображения определяется биективное преобразование φ_0 множества $N_3^+(E)$, переводящее всякое максимальное множество первого типа в максимальное множество второго типа. Отсюда немедленно вытекает, что всякое преобразование φ, удовлетворяющее условиям теоремы, есть либо преобразование вида $\bar{u}_r$, либо преобразование вида $\varphi_0\bar{u}_r$.

4) Переводя теорему этого параграфа на язык матриц, получаем на этот раз теорему о множестве кососимметричных матриц, пополненном подходящим образом бесконечно удаленными элементами.

5) Если K — поле характеристики $\neq 2$, то грассманианы $G_r(E)$, пространства $N_r^+(E)$ при $n = 2r + 2$ в случае симметричной формы f и пространства $N_r(E)$ во всех остальных случаях являются неособыми *неприводимыми алгебраическими многообразиями*, которые могут быть погружены в проективное пространство S. Чоу [1] доказал, что все *бирегулярные бирациональные* преобразования этих многообразий индуцируются преобразованиями из $GL(E)$, за исключением $N_3^+(E)$. Идея доказательства состоит в том, чтобы перевести понятия «соседства», введенные в § 2—4, на язык геометрии пространства S. А именно, две точки из $G_r(E)$ или $N_r(E)$ будут соседними тогда и только тогда, когда прямая, соединяющая их в пространстве S, целиком лежит в $G_r(E)$ (соответственно в $N_r(E)$); две точки из $N_r^+(E)$ будут соседними тогда и только тогда, когда они лежат на плоской кривой 2-го порядка, содержащейся в $N_r^+(E)$. После этого все сводится к доказательству того, что всякое бирегулярное бирациональное преобразование рассматриваемого многообразия переводит прямую в прямую (соответственно плоскую кривую 2-го порядка — в плоскую кривую 2-го порядка). Последнее проводится при помощи изучения полных линейных систем без базисной точки на этих многообразиях и, в частности, системы, порожденной гиперплоскими сечениями.

В случае когда K — поле комплексных чисел, можно вместо бирегулярных бирациональных преобразований рассматривать биективные аналитические преобразования. Доказательство проводится аналогично, с заменой полных линейных систем на классы гомологий (Чоу [1]).

§ 5. Другие характеризации классических групп

Пусть K — поле характеристики $\neq 2$, E — векторное пространство размерности $n \geqslant 2$ над K, $f(x, y)$ — невырожденная симметричная билинейная форма на E. Для того чтобы элемент $f(x, x)$ был *квадратом* в K при любом $x \in E$, необходимо и достаточно, чтобы поле K было *пифагоровым* (т. е. чтобы сумма двух квадратов была квадратом) и чтобы существовал такой ортогональный базис $(e_i)_{1 \leqslant i \leqslant n}$ пространства E, что $f(e_i, e_i) = 1$ при $1 \leqslant i \leqslant n$. При этом, для того чтобы форма f была *анизотропной*, необходимо и достаточно, чтобы -1 не была квадратом в K, т. е. чтобы поле K было *упорядочиваемым.* Обычная евклидова геометрия над полем действительных чисел служит типичным примером, когда эти условия выполнены. Из этих условий вытекает свойство «свободной подвижности» в пространстве E, которое можно сформулировать следующим образом. Пусть K *упорядочено.* Будем называть *i-мерной цепью инцидентных полупространств* последовательность $(H_k)_{1 \leqslant k \leqslant i}$, определенную, исходя из линейно независимой системы векторов $(a_k)_{1 \leqslant k \leqslant i}$, таким образом, что H_k есть множество линейных комбинаций $\sum_{j=1}^{k} \lambda_j a_j$, в которых *последний* коэффициент λ_k неотрицателен. Свойство «свободной подвижности» состоит в том, что при перечисленных выше условиях для любых двух *n-мерных* цепей инцидентных полупространств *существует единственное преобразование* из группы $O_n(K, f)$, преобразующее первую из этих цепей во вторую. «Проблема Гельмгольца» заключается в том, чтобы найти все подгруппы группы $GL_n(K)$, обладающие свойством свободной подвижности. Эта проблема неоднократно исследовалась для поля действительных чисел, большей частью инфинитезимальными методами (см. библиографию у Пиккерта [1]). В наиболее общем виде она была решена Бэром [1], который в предположении, что K — упорядоченное, но не обязательно коммутативное тело, доказал следующую теорему:

Если подгруппа G группы $GL_n(K)$ (при $n \geqslant 3$) обладает свойством свободной подвижности, то тело K коммутативно и пифагорово, а G есть ортогональная группа $O_n(K, f)$ относительно такой анизотропной симметричной билинейной формы $f(x, y)$, что элемент $f(x, x)$ является квадратом в K при любом $x \in E$.

Идея доказательства состоит в том, чтобы, используя свойство свободной подвижности, доказать, что для всякого подпространства $V \subset E$ существует единственная инволюция $u \in G$, для которой V служит положительным подпространством. Ставя в соответствие подпространству V отрицательное подпространство этой инволюции, получаем «отношение ортогональности» между подпространствами пространства E, которое определяет, в частности, биективное отображение множества прямых пространства E на множество гиперплоскостей, или, иными словами, биективное отображение пространства $P(E)$ на пространство $P(E^*)$ (где E^* — пространство, дуальное к E). Так как это отображение переводит прямые пространства $P(E)$ в прямые пространства $P(E^*)$, то применима основная теорема проективной геометрии, показывающая, что определенная выше «ортогональность» совпадает с ортогональностью относительно некоторой рефлексивной полуторалинейной формы $f(x, y)$ на E. Эта форма должна быть анизотропной. Кроме того, из свойства свободной подвижности довольно легко выводится, что любые две прямые пространства E могут быть преобразованы одна в другую произведением инволюций, принадлежащих группе G. Более тонкое рассуждение показывает, что форма f симметрична и, следовательно, тело K коммутативно и пифагорово. Доказательство заканчивается замечанием, что инволюции из группы G являются ортогональными преобразованиями относительно формы f.

Теорема остается справедливой при $n = 2$, если предположить, что K — *евклидово* упорядоченное поле, т. е. что всякий неотрицательный элемент является квадратом в K (Бэр [1]).

Кроме того, Бэр [1] доказал, что свойство, аналогичное свойству «свободной подвижности», но в котором n-мерные цепи заменены $(n-1)$-мерными, характеризует при $n \geqslant 3$ *подгруппы вращений* $O_n^+(K, f)$ ортогональных групп $O_n(K, f)$, обладающих свойством свободной подвижности. Пример Пиккерта [1], стр. 498, показывает, что это перестает быть верным при $n = 2$.

Рассматривая проективную группу $PGL_2(K)$ над полем K как группу перестановок проективной прямой $P_1(K)$, Титс [1] получил характеризацию этих групп посредством свойств *транзитивности*. Эти группы *трижды транзитивны* в том смысле, что для любых двух троек (a, b, c) и (a', b', c') различных точек проективной прямой $P_1(K)$ существует *ровно одно* преобразование из группы, которое переводит a в a', b в b' и c в c'. Одного этого условия недостаточно для характеризации групп $PGL_2(K)$, однако в той же работе Титса указаны различные дополнительные условия, которые вместе с условием троекратной транзитивности позволяют утверждать, что рассматриваемая группа изоморфна группе $PGL_2(K)$. Эти условия подсказаны классическими определениями и построениями проективной геометрии. Например, трижды транзитивная группа G перестановок множества E изоморфна группе $PGL_2(K)$, если для всякой пары различных элементов a, b множества E группа преобразований из G, оставляющих a и b на месте, коммутативна. Помимо этого, методы Титса позволили ему найти все конечные трижды транзитивные группы (см. там же). Он распространил затем свои результаты на проективные группы $PGL_n(K)$ от любого числа переменных над полем K (Титс [2]). Группа G перестановок множества E называется *почти n-кратно транзитивной*, если в множестве E выделены так называемые «реперы», состоящие из n точек и обладающие тем свойством, что для произвольных реперов (a_i) и (b_i) существует единственное преобразование из группы G, переводящее a_i в b_i при $1 \leqslant i \leqslant n$[1]. Глубокое изучение этого понятия позволило Титсу охарактеризовать группы $PGL_n(K)$ среди всех почти $(n+1)$-кратно транзитивных групп.

Другую характеризацию групп $PGL_2(K)$ (K — поле характеристики $\neq 2$) дал Бахман [1]. Она основывается на том факте, что всякий элемент такой группы является произведением двух инволюций. Это немедленно следует из того, что группа $PGL_2(K)$ изоморфна группе вращений $O_3^+(K, f)$, где f — форма индекса 1 (см. § 9 гл. II), и из того, что всякое вращение является в этом случае произведением двух инверсий (гл. II, § 6). Бахман показал, как можно охарактеризовать группы $PGL_2(K)$ среди групп, обладающих указанным выше свойством, четырьмя дополнительными условиями, в формулировке которых участвуют только инволюции и их произведения и свойство такого произведения быть или не быть инволюцией. Шмидт [1] и Бахман [1] дали аналогичные характеризации групп $O_3^+(K, f)$, где K — поле характеристики $\neq 2$ и f — форма индекса 0. (Эти группы можно рассматривать как группы движений эллиптической неевклидовой геометрии.) Бэр [2] охарактеризовал эти группы множеством других систем условий, также использующих инволюции. Наиболее замечательная из них, несомненно, следующая. Каждой группе G поставим в соответствие два множества: P (множество «точек») и H (множество «гиперплоскостей»), каждое из которых находится во взаимно однозначном соответствии с множеством инволюций в группе G. Далее определяется отношение «точка p принадлежит гиперплоскости h» условием, что ph — инволюция в G (здесь p и h отождествляются с соответствующими элементами группы G). Это позволяет определить понятие «линейной зависимости» в P: точка p линейно зависит от множества точек S, если она принадлежит всякой гиперплоскости, содержащей все точки из S. Затем определяются «линейные многообразия» в P как такие подмножества

[1]) Помимо этого свойства, множество «реперов» должно, конечно, обладать некоторыми свойствами, обеспечивающими его «обильность». — *Прим. перев.*

M, что всякая точка, линейно зависящая от M, содержится в M. При таких определениях «линейные многообразия» в P удовлетворяют аксиомам n-мерной проективной геометрии для некоторого $n > 1$ тогда и только тогда, когда группа G изоморфна группе движений эллиптической геометрии, и в этом случае $n = 3$.

Глава IV

АВТОМОРФИЗМЫ И ИЗОМОРФИЗМЫ КЛАССИЧЕСКИХ ГРУПП

§ 1. Автоморфизмы групп $GL_n(K)$

До 1966 г. бо́льшая часть методов определения автоморфизмов классических групп основывалась на изучении инволюций в этих группах и на том факте, что при автоморфизме инволюция переходит в инволюцию. Изучение инволюций в классических группах, предпринятое в гл. I, показывает, что им можно внутренним образом поставить в соответствие *подпространства* того пространства, в котором действует группа; автоморфизм группы индуцирует преобразование множества этих подпространств, и в большинстве случаев основная теорема проективной геометрии (гл. III, § 1) позволяет установить, что это преобразование происходит из коллинеации или корреляции, что и дает описание автоморфизмов данной группы.

В настоящей главе будут изложены результаты, полученные этими методами. Краткое описание новых методов см. в приложении.

Начнем с изучения автоморфизмов группы $GL_n(K)$, где K — произвольное тело (не обязательно коммутативное). Из-за того, что инволюции в группе $GL_n(K)$ устроены различным образом в случаях, когда характеристика тела K отлична от 2 и равна 2, нужно рассмотреть отдельно эти два случая.

I. $n \geqslant 3$, *характеристика тела K не равна* 2. Мы будем называть $(p, n-p)$-инволюцию (гл. I, § 3) *экстремальной*, если $p = 1$ или $p = n-1$. Первый шаг состоит в доказательстве следующего утверждения:

1) *Всякий автоморфизм φ группы $GL_n(K)$ переводит экстремальную инволюцию в экстремальную инволюцию.*

Для доказательства достаточно охарактеризовать экстремальные инволюции среди всех инволюций в группе

$GL_n(K)$ свойствами, зависящими только от структуры группы $GL_n(K)$, а не от ее определения при помощи n-мерного векторного пространства E, в котором она действует. Это можно сделать несколькими способами, развивая идеи, восходящие к работе Макки [1]. Наиболее быстрый способ, несомненно, следующий (Дьёдонне [7], стр. 5): в группе $GL_n(K)$ рассматриваются *максимальные множества попарно коммутирующих сопряженных инволюций*. Используя тот факт, что линейное преобразование, коммутирующее с инволюцией, сохраняет собственные подпространства этой инволюции, легко показать, что если такое множество инволюций состоит из $(p, n-p)$-инволюций, то оно содержит $\binom{n}{p}$ элементов, и что всякая $(p, n-p)$-инволюция принадлежит хотя бы одному такому множеству. Отсюда и получается искомая характеризация экстремальных инволюций.

Другой способ, предложенный Риккартом [1], также исходя из идей Макки [1], больше связан со следующими этапами доказательства и применим, как мы увидим ниже (§ 3, 4 и 7), к другим классическим группам. Для любого множества S инволюций группы $GL_n(K)$ обозначим через $c(S)$ множество инволюций, коммутирующих со всеми инволюциями из S. Для двух *коммутирующих* инволюций u, v обозначим через $\nu(u, v)$ число элементов в $c(c(u, v))$. Наконец, для всякой инволюции u обозначим через $\nu(u)$ максимум из чисел $\nu(u, v)$, когда v пробегает множество инволюций, коммутирующих с u. Можно показать при $n > 3$, что $\nu(u) = 16$, если инволюция u не экстремальна, и $\nu(u) = 8$ в противном случае. Это дает новую характеризацию экстремальных инволюций. (При $n = 2$ и $n = 3$ всякая инволюция экстремальна.)

Следующий шаг состоит в рассмотрении, согласно Макки, *минимальных пар* экстремальных инволюций. По определению две экстремальные инволюции u, v образуют минимальную пару, если они не коммутируют и имеют общее собственное подпространство. Доказывается следующее утверждение:

2) *Всякий автоморфизм φ группы $GL_n(K)$ переводит минимальную пару экстремальных инволюций в минимальную пару.*

Как и выше, достаточно охарактеризовать минимальные пары свойствами, зависящими только от структуры группы. Способ Макки (см. там же) основывается на следующем свойстве: две *не коммутирующие* экстремальные инволюции u и v образуют минимальную пару тогда и только тогда, когда $c(c(u,v)) = c(c(u',v'))$ для всякой пары не коммутирующих экстремальных инволюций u', v', содержащихся в $c(c(u,v))$.

Далее, можно рассуждать двумя различными способами (при $n \geqslant 3$). Первый способ состоит в том, чтобы сопоставить каждой экстремальной инволюции пару (D, H), образованную собственными подпространствами этой инволюции, где D — прямая, H — гиперплоскость и $D \oplus H = E$. Автоморфизм φ определяет тогда перестановку ψ множества этих пар. Будем называть две минимальные пары (u_1, v_1), (u_2, v_2) экстремальных инволюций *подобными*, если размерности общих собственных подпространств инволюций u_1, v_1, с одной стороны, и u_2, v_2— с другой, равны. Легко доказать, что φ преобразует любые две подобные минимальные пары в подобные (Риккарт [1], стр. 459). Поэтому совокупность пар (D, H) с фиксированной прямой D при преобразовании ψ переходит либо в совокупность пар с общей прямой, либо в совокупность пар с общей гиперплоскостью, причем для всех прямых D имеет место один и тот же случай. Тем самым преобразование ψ определяет биективное отображение θ пространства $P(E)$ либо на себя, либо на пространство $P(E^*)$. Кроме того, легко видеть, что если D_1, D_2, D_3 —три различные прямые пространства E, лежащие в одной плоскости, H — гиперплоскость, не содержащая ни одной из этих прямых, и u_i $(i = 1, 2, 3)$ обозначает инволюцию, соответствующую паре (D_i, H), то каждая из инволюций u_i принадлежит множеству $c(c(u_j, u_k))$, определенному двумя другими инволюциями. Отсюда без труда выводится, что точки D_1, D_2, D_3 пространства $P(E)$, лежащие на одной прямой, переходят при отображении θ в три точки, лежащие на одной прямой. Согласно основной теореме проективной геометрии (гл. III, § 1), существует либо такая коллинеация g пространства E, что $\bar{g} = \theta$, либо такая корреляция h пространства E на пространство E^*, что $\bar{h} = \theta$. В первом случае φ совпадает на множестве экстремальных инволюций с автоморфизмом $u \to gug^{-1}$, во втором — с автоморфизмом $u \to h^{-1}\check{u}h$, где $\check{u}$ обозначает преобразование, контраградиентное к u. Предположим для определенности, что имеет место первый случай. Так как всякий сдвиг является произведением двух экстремальных инволюций и группа $SL_n(K)$ порождается сдвигами, то автоморфизмы φ и $u \to gug^{-1}$ совпадают на $SL_n(K)$. Рассмотрим автоморфизм φ_0: $u \to g^{-1}\varphi(u)g$. Он оставляет на месте все сдвиги. Если t — какой-нибудь сдвиг, а u — любое преобразование из $GL_n(K)$, то utu^{-1} — также сдвиг, и поэтому $\varphi_0(u)t\varphi_0(u)^{-1} = utu^{-1}$. Это означает, что преобразование $u^{-1}\varphi_0(u)$ перестановочно со всеми сдвигами и, следовательно, относительно него инвариантна любая прямая пространства E. Значит, $\chi(u) = u^{-1}\varphi_0(u)$ есть *центральная гомотетия*. Очевидно, что отображение $u \to \chi(u)$ является гомоморфизмом группы $GL_n(K)$ в ее центр Z_n. Окончательно получаем, что в рассматриваемом случае

$$\varphi(u) = \chi(u)\, gug^{-1}, \tag{1}$$

где χ — гомоморфизм группы $GL_n(K)$ в ее центр Z_n, а g — коллинеация пространства E. Записывая условие того, что ограничение автоморфизма φ на Z_n биективно, находим следующее необходимое условие на гомоморфизм χ: из равенства $\chi(\zeta) = \zeta^{-1}$ должно следовать $\zeta = 1$. Ясно, что это условие и достаточно [1]).

Во втором случае

$$\varphi(u) = \chi(u)\, h^{-1}\check{u}h, \tag{2}$$

где χ — гомоморфизм группы $GL_n(K)$ в ее центр Z_n, а h — корреляция пространства E на пространство E^*.

Второй способ получения этих результатов состоит в использовании упомянутого выше факта: всякий сдвиг есть произведение двух экстремальных инволюций, образующих минимальную пару, и обратно. Отсюда следует, что автоморфизм φ переводит любой сдвиг в сдвиг. Затем используется рассуждение Шрейера и Ван-дер-Вардена [1], стр. 315—316, основанное на том, что произве-

[1]) Достаточно для инъективности, но не для сюръективности, как показывает пример $K = \mathbf{Q}$, $\chi(u) = (\det(u))^2$. — *Прим. перев.*

дение двух сдвигов t_1, t_2 является сдвигом только тогда, когда t_1 и t_2 имеют либо общую гиперплоскость, либо общую прямую. Всякая подгруппа группы $GL_n(K)$, состоящая только из сдвигов (и тождественного преобразования), содержится либо в группе $T(H)$ всех сдвигов вдоль некоторой гиперплоскости H, либо в группе $T(D)$ всех сдвигов в направлении некоторой прямой D. Пересечение $T(D) \cap T(H)$ содержит сдвиг только тогда, когда $D \subset H$; подгруппа вида $T(D)$ не сопряжена подгруппе вида $T(H)$ в группе $GL_n(K)$. Из этих замечаний следует, что автоморфизм φ определяет биективное отображение θ пространства $P(E)$ на пространство $P(E)$ или $P(E^*)$. При этом точки, лежащие в одной гиперплоскости, преобразуются отображением θ в точки, лежащие в одной гиперплоскости, что позволяет закончить доказательство так же, как и выше.

II. $n \geqslant 3$, *характеристика тела K равна* 2. В этом случае сдвиги являются $(1, n-1)$-инволюциями в группе $GL_n(K)$, и достаточно отличить их (при $n \geqslant 4$) от других инволюций свойствами, использующими только структуру группы; метод Шрейера и Ван-дер-Вардена, описанный выше, позволит тогда сделать то же заключение, что и в случае 1. При $n \geqslant 6$ искомое различение достигается замечанием, что произведение двух коммутирующих сдвигов есть либо сдвиг, либо $(2, n-2)$-инволюция, в то время как при $p > 1$ произведение двух коммутирующих $(p, n-p)$-инволюций может принадлежать более чем двум классам сопряженных элементов в группе $GL_n(K)$ (Дьёдонне [7], стр. 14). При $n = 4$ и $n = 5$ нужно различить два класса C_1, C_2 инволюций в группе $GL_n(K)$. С этой целью для всякой инволюции u рассмотрим множество $P^*(u)$ инволюций, коммутирующих с u и не принадлежащих тому классу, которому принадлежит u, затем множество $P^{**}(u)$ инволюций, коммутирующих со всеми инволюциями из $P^*(u)$ и принадлежащих тому же классу, что u. Если u — сдвиг, то произведение любых двух различных элементов из $P^{**}(u)$ лежит в том же классе, что u; но это не так, если u — не сдвиг. Отсюда и получается искомое различение.

III. $n = 2$. Если характеристика тела K равна 2, то по тем же соображениям, что и в случае II, получаем, что автоморфизм φ переводит сдвиги в сдвиги и тем самым определяет биективное преобразование проективной прямой $P_1(K)$ на себя. Можно предполагать, что это преобразование оставляет на месте точку (которую можно считать «бесконечно удаленной») и, значит, индуцирует биективное преобразование $t \to t^\sigma$ тела K. Можно, далее, добиться того, чтобы $0^\sigma = 0$, $1^\sigma = 1$. Используя тот факт, что если s и t — сдвиги, то sts^{-1} — также сдвиг, легко доказать соотношения $(x+y)^\sigma = x^\sigma + y^\sigma$ и $(xyx)^\sigma = x^\sigma y^\sigma x^\sigma$ (Шрейер и Ван-дер-Варден [1], стр. 317—318). Из теоремы Хуа [7] следует тогда, что отображение $t \to t^\sigma$ обязательно является автоморфизмом или антиавтоморфизмом тела K, откуда уже легко выводится, что φ задается формулой (1) или (2).

Тот же метод был применен Шрейером и Ван-дер-Варденом для *коммутативного* тела K характеристики $\neq 2$. Однако их рассуждение содержит ошибку в доказательстве того, что автоморфизм φ преобразует сдвиги в сдвиги. Этот факт был доказан Хуа [5], стр. 756, который заметил, что сдвиги можно охарактеризовать следующим образом. Если характеристика поля K равна $p \neq 0$, то сдвиги t характеризуются свойством $t^p = 1$. Если характеристика поля K равна 0, то сдвиги являются единственными преобразованиями $t \in SL_2(K)$, для которых существует бесконечно много преобразований из $SL_2(K)$, сопряженных с t и коммутирующих с t. Представление автоморфизма φ формулой (1) или (2) сохраняется и в этом случае.

Наконец, опираясь на этот последний результат, Хуа [9] смог доказать, что для произвольного (не обязательно коммутативного) тела K любой автоморфизм группы $GL_2(K)$ задается одной из формул (1) и (2). Таким образом, проблема определения всех автоморфизмов группы $GL_n(K)$ полностью решена.

Замечания. 1) Автоморфизмы группы $\Gamma L_n(K)$ коллинеаций пространства E при $n \geqslant 3$ также задаются формулами (1) и (2), причем χ в этом случае есть отображение группы $\Gamma L_n(K)$ в группу Z_n, удовлетворяющее условию $\chi(u_1u_2) = \chi(u_1)\chi(u_2)^{\sigma_1}$, где σ_1 — автоморфизм тела K, соответствующий коллинеации u_1 (Риккарт [3]). В самом деле, достаточно показать, что при любом автоморфизме группы $\Gamma L_n(K)$ экстремальные инволюции из группы $GL_n(K)$ переходят в экстремальные инволюции. Предположим вначале, что характеристика тела K отлична от 2. Используя описание инволюций в группе $\Gamma L_n(K)$, данное в § 3 гл. I, легко убедиться, что для всякой инволюции $u \in \Gamma L_n(K)$, не принадлежащей группе $GL_n(K)$, существует система из 2^n попарно коммутирующих инволюций, сопряженных к u в $\Gamma L_n(K)$ (Дьёдонне [7], стр. 9). Этого достаточно для отличения этих инволюций от экстремальных. В случае когда характеристика тела K равна 2, достаточно заметить, что если u_1, u_2 — коммутирующие сопряженные инволюции в группе $\Gamma L_n(K)$, не принадлежащие группе $GL_n(K)$, то их произведение принадлежит группе $GL_n(K)$ и, значит, не может быть сопряжено инволюции u_1, в противоположность тому, что бывает, когда u_1, u_2 — сдвиги (Дьёдонне [7], стр. 17). Это последнее рассуждение применимо также при $n = 2$ и дает описание автоморфизмов группы $\Gamma L_2(K)$ для тела K характеристики 2.

2) Риккарт [1], [3] распространил эти методы на задачу определения автоморфизмов группы $GL(E)$ линейных преобразований бесконечномерного векторного пространства E над телом K характеристики $\neq 2$. Впрочем, метод «минимальных пар» был изобретен Макки [1] именно при решении подобной задачи (в случае когда K — поле действительных или комплексных чисел).

Укажем также на другое обобщение, принадлежащее Эрлиху [1], при котором группа $GL_n(K)$ заменяется группой обратимых элементов «регулярного» кольца, ассоциированного с «непрерывной геометрией» фон Неймана.

§ 2. Автоморфизмы групп $SL_n(K)$

Очевидно, что автоморфизм φ группы $GL_n(K)$, задаваемый формулой (1) или (2), индуцирует автоморфизм группы $SL_n(K)$, если только ограничение гомоморфизма χ на $SL_n(K)$ является гомоморфизмом этой группы в ее центр. Так как группа $SL_n(K)$ совпадает со своим коммутантом, кроме случаев, когда $n = 2$, а $K = \mathbf{F}_2$ или $K = \mathbf{F}_3$ (гл. II, § 2), то $\chi = 1$ на $SL_n(K)$, за исключением, быть может, этих двух случаев. Однако центр группы $SL_2(\mathbf{F}_2)$ равен единице, а центр группы $SL_2(\mathbf{F}_3)$

состоит из двух элементов, в то время как ее коммутант является подгруппой индекса 3. Это показывает, что $\chi = 1$ во всех случаях.

Мы покажем теперь, что *всякий автоморфизм группы $SL_n(K)$ индуцируется автоморфизмом группы $GL_n(K)$*, за исключением одного случая, для которого вопрос остается открытым.

Прежде всего, если характеристика тела K отлична от 2 и *n нечетно*, то группа $SL_n(K)$ содержит $(1, n-1)$-инволюции, и рассуждения § 1 применимы при $n \geqslant 3$. Эти рассуждения применимы также, если K — некоммутативное тело характеристики $\neq 2$ и -1 содержится в коммутанте группы K^* (например, это справедливо для тела кватернионов), поскольку в этом случае любая инволюция из $GL_n(K)$ содержится в $SL_n(K)$. Наконец, если характеристика тела K равна 2, то сдвиги принадлежат группе $SL_n(K)$, однако метод, описанный в § 1, использует тот факт, что инволюции одного типа $(p, n-p)$ (где $2p \leqslant n$) сопряжены, что верно в группе $SL_n(K)$, если $2p < n$, и не всегда верно, если $2p = n$. Тем не менее доказательство того, что автоморфизм группы $GL_n(K)$ преобразует сдвиги в сдвиги, переносится без изменений на автоморфизмы группы $SL_n(K)$, кроме случая $n = 4$. В этом последнем случае нужно использовать другой метод доказательства этого утверждения. Метод, указанный в работе Дьёдонне [7], стр. 19, содержит ошибку, исправленную Хуа и Ванем [1]. Учитывая все эти результаты, получаем, что для тела K характеристики 2 автоморфизм группы $SL_n(K)$ индуцируется автоморфизмом $GL_n(K)$ при любом $n \geqslant 2$.

Остается рассмотреть случай, когда n четно, характеристика тела K не равна 2 и -1 не принадлежит коммутанту C группы K^*. В этом случае экстремальные инволюции не принадлежат группе $SL_n(K)$. При $n \geqslant 6$ методы, аналогичные методам § 1, могут быть применены к $(2, n-2)$-инволюциям (которые всегда принадлежат группе $SL_n(K)$), и это позволяет доказать, что и в этом случае всякий автоморфизм группы $SL_n(K)$ индуцируется автоморфизмом группы $GL_n(K)$ (Дьёдонне [7], стр. 20—21). Тот же результат получен Хуа [9] для $n = 4$ совершенно другим методом: вначале он изучает автоморфизмы группы $SL_n^+(K)$, образованной линейными преобразованиями, определитель которых равен единице или образу -1 в группе K^*/C, и показывает, что эти автоморфизмы индуцируются автоморфизмами группы $GL_n(K)$; затем, опираясь на этот результат, с помощью довольно сложного рассуждения он определяет в рассматриваемом случае все автоморфизмы группы $SL_4(K)$.

Что касается группы $SL_2(K)$, то она не содержит инволюций, отличных от единицы[1]). Для определения ее автоморфизмов достаточно было бы охарактеризовать сдвиги свойствами, зависящими только от структуры группы. В конце § 1 мы видели, что это возможно, если K коммутативно. Хуа и Вань [1] доказали, что если K — произвольное тело характеристики $p > 0$, то сдвиги — это все элементы порядка p в группе $SL_2(K)$. Таким образом, проблема остается открытой только в том случае, когда K — некоммутативное тело характеристики 0 и -1 не принадлежит коммутанту группы K^*.

§ 3. Автоморфизмы групп $Sp_{2m}(K)$

Симплектическая группа $Sp_2(K)$ тождественна унимодулярной группе $SL_2(K)$ (гл. II, § 4). Поскольку тело K коммутативно, ее автоморфизмы известны, согласно § 2[2]). Таким образом, можно ограничиться размерностями $2m \geqslant 4$. При этом справедливо следующее утверждение:

Всякий автоморфизм φ *симплектической группы* $Sp_{2m}(K)$ *может быть представлен в виде* $\varphi(u) = gug^{-1}$, *где* $g \in \Gamma Sp_{2m}(K)$ (гл. I, § 9), *за исключением случая, когда* $m = 2$ *и характеристика поля* K *равна* 2[3]).

---

[1]) Имеется в виду случай, когда характеристика тела K не равна 2. — *Прим. перев.*

[2]) В этом случае всякий автоморфизм может быть задан формулой (1) (с $\chi = 1$). В самом деле, пусть h_0 — корреляция, соответствующая инвариантной знакопеременной форме. Тогда $\varphi_0(u) = h_0^{-1}\check{u}h_0 = u$ при любом $u \in Sp_2(K) = SL_2(K)$. С другой стороны, всякий автоморфизм, задаваемый формулой (2), есть композиция автоморфизма φ_0 и автоморфизма, задаваемого формулой (1). — *Прим. перев.*

[3]) Как следует из предыдущего примечания, это утверждение справедливо и при $m = 1$. — *Прим. перев.*

Способы доказательства зависят от того, равна или не равна 2 характеристика поля K.

I. *Характеристика поля K не равна* 2. Первый способ доказательства использует инволюции в группе $Sp_{2m}(K)$. Инволюция типа $(2, 2m-2)$ или $(2m-2, 2)$ называется *экстремальной.* Инволюции типа $(2p, 2m-2p)$ отличаются тем, что максимальная система попарно коммутирующих инволюций такого типа (которые всегда сопряжены) содержит $\binom{m}{p}$ элементов. Другой способ отличить экстремальные инволюции состоит в рассмотрении числа $\nu(u)$, определенного в § 1. При $2m \geqslant 8$ можно показать, что $\nu(u) = 16$, если инволюция u не экстремальна, и $\nu(u) = 8$ в противном случае (Риккарт [2]). (При $2m=4$ и $2m = 6$ все инволюции экстремальны.)

Затем вводится понятие *минимальной пары* экстремальных инволюций. При $2m \geqslant 6$ это пары (u, v), образованные экстремальными инволюциями, двумерные собственные подпространства которых имеют одномерное пересечение. Доказывается, что критерий Макки (для минимальных пар в группе $GL_n(K)$) и в этом случае характеризует минимальные пары, и, следовательно, всякий автоморфизм группы $Sp_{2m}(K)$ переводит минимальные пары в минимальные пары (Дьёдонне [7], стр. 26; Риккарт [2], стр. 710). При $2m = 4$ *минимальной парой* называется такая пара (u, v) некоммутирующих инволюций, что одно из собственных подпространств инволюции u имеет одномерное пересечение с одним из собственных подпространств инволюции v. Характеризация минимальных пар в этом случае состоит в том, что централизатор пары инволюций (u, v) разрешим тогда и только тогда, когда эта пара минимальна (в случае $K = \mathbf{F}_3$ минимальная пара отличается порядком централизатора).

Используя полученную характеризацию минимальных пар, показывается затем, что множество $I(D)$ экстремальных инволюций, двумерное собственное подпространство которых содержит прямую D, при любом автоморфизме группы $Sp_{2m}(K)$ переходит в множество вида $I(D')$. Это устанавливается довольно легко при $2m \geqslant 6$ (Дьёдонне [7], стр. 26—27; Риккарт [2], стр. 711—712) и отдельным, гораздо более длинным рассуждением при $2m = 4$ (Дьёдонне [7], стр. 29—30). Полагая затем

$\psi(D)=D'$, мы получаем биективное преобразование ψ пространства $P(E)$, которое переводит любые две ортогональные прямые пространства E в ортогональные прямые и, следовательно, любые точки пространства $P(E)$, лежащие в одной гиперплоскости, — в точки, лежащие в одной гиперплоскости. Применение основной теоремы проективной геометрии (гл. III, § 1) немедленно приводит тогда к окончательному результату.

Хуа [5] получил этот же результат совершенно другим методом — индукцией по m с использованием описания автоморфизмов группы $SL_2(K)$, полученным в § 2. Поскольку всякий автоморфизм φ группы $Sp_{2m}(K)$ переводит экстремальные инволюции в экстремальные, доказательство можно свести к случаю, когда φ оставляет на месте одну экстремальную инволюцию и, следовательно, ее централизатор Γ, который является прямым произведением группы $Sp_2(K)=SL_2(K)$ и группы $Sp_{2m-2}(K)$. Далее доказательство сводится к случаю, когда φ оставляет на месте все элементы группы $Sp_{2m-2}(K)$. Окончательный результат получается с помощью исследования действия φ на некоторые подгруппы группы Γ.

II. *Характеристика поля K равна* 2. В этом случае нужно выделить с помощью групповых свойств сдвиги среди всех инволюций в группе $Sp_{2m}(K)$. При $m \geqslant 3$ это достигается изучением централизатора инволюции в группе $Sp_{2m}(K)$ (гл. I, § 14) и доказательством (индукцией по m) того, что группа $Sp_{2m}(K)$ не может быть изоморфна группе $Sp_{2q}(K)$ при $q < n$. Заканчивается доказательство так же, как и в § 1.

Если K — совершенное поле характеристики 2, то теорема, вообще говоря, перестает быть справедливой при $m=2$. Предположим, что существует такой автоморфизм σ поля K, что σ^2 совпадает с автоморфизмом $x \to x^2$. Тогда можно показать (Титс [4]), что существуют автоморфизмы группы $Sp_4(K)$, переводящие сдвиги в (2,2)-инволюции. (Доказательство несуществования таких автоморфизмов, данное Дьёдонне [7], стр. 37—38, ошибочно.) В частности, поле K, состоящее из 2^n элементов, обладает автоморфизмом σ с указанным выше свойством тогда и только тогда, когда *n нечетно.* В этом случае можно доказать, что упомянутые выше особые автоморфизмы вместе с автоморфизмами, описанными в начале этого параграфа, порождают группу всех автоморфизмов группы $Sp_4(K)$ (Стейнберг [1]). Для других полей характеристики 2 полное описание автоморфизмов группы $Sp_4(K)$, по всей видимости, получено только в случае, когда поле K алгебраически замкнуто (Стейнберг [1]), стр. 614).

Учитывая, что симметрическая группа $\mathfrak{S}_6$ изоморфна группе $Sp_4(\mathbf{F}_2)$, мы получаем известный факт, что группа $\mathfrak{S}_6$ имеет внешние автоморфизмы.

§ 4. Автоморфизмы групп $U_n(K, f)$

(*K* — тело характеристики $\neq 2$.)

Предположим, что f — эрмитова T-форма над телом *K характеристики* $\neq 2$. При этих условиях справедлива теорема:

При $n \geqslant 3$ всякий автоморфизм унитарной группы $U_n(K, f)$ может быть представлен в виде $\varphi(u) = \chi(u)gug^{-1}$, где $g \in \Gamma U_n(K, f)$, а χ — гомоморфизм группы $U_n(K, f)$ в ее центр.

Первый этап доказательства, как и в предыдущих параграфах, состоит в характеризации экстремальных инволюций группы $U_n(K, f)$. Экстремальными инволюциями в данном случае называются *отражения* относительно неизотропных гиперплоскостей пространства E. При $n = 3$ всякая инволюция экстремальна. При $n \geqslant 4$ характеризация экстремальных инволюций получается методом Макки — Риккарта, описанным в § 1. А именно, если инволюция $u \in U_n(K, f)$ экстремальна, то $\nu(u) = 16$; если она не экстремальна, то $\nu(u) = 8$. Таким образом, всякий автоморфизм φ группы $U_n(K, f)$ преобразует отражения в отражения и тем самым определяет биективное преобразование ψ множества неизотропных прямых пространства E, которое переводит любые две ортогональные прямые в ортогональные прямые. Если индекс формы f равен 0, то можно применить к ψ основную теорему проективной геометрии (гл. III, § 1) и получить отсюда окончательный результат так же, как в предыдущих параграфах (Риккарт [2]).

Если в пространстве E имеются изотропные прямые, то можно продолжить ψ на все пространство $P(E)$ таким образом, чтобы любые две ортогональные прямые пространства E по-прежнему переходили в ортогональные прямые. С этой целью заметим прежде всего, что множество неизотропных прямых, принадлежащих одной неизотропной плоскости P, может быть охарактеризовано как множество неизотропных прямых, ортогональных к некоторой системе из $n-2$ попарно ортогональных неизотропных прямых пространства E, и, следовательно, переводится преобразованием φ в множество неизотропных прямых некоторой неизотропной плоскости, которую мы обозначим через $\psi(P)$. Аналогичным образом показывается, что если P_1, P_2 — неизотропные плоскости, пересечение которых изотропно, а сумма (имеющая размерность 3) неизотропна, то их образы $\psi(P_1)$, $\psi(P_2)$ обладают теми же свойствами.

Предположим теперь, что $n \geqslant 4$, и пусть Δ — изотропная прямая. Докажем, что если плоскость P пробегает множество $I(\Delta)$ неизотропных плоскостей, содержащих Δ, то плоскости $\psi(P)$ содержат некоторую изотропную прямую $\psi(\Delta)$. Это вытекает из следующего предложения (Дьёдонне [7], стр. 48—49): если P — неизотропная плоскость, D — неизотропная прямая, содержащаяся в P, и a, b, c — три различные точки на прямой D, то существует четвертая точка $d \in P$, такая, что $d \notin D$ и векторы $d-a$, $d-b$, $d-c$ не изотропны. При доказательстве этого предложения можно считать, что $c=0$, и тогда в качестве d можно взять вектор, ортогональный к D, если только функция $\xi \to \xi\alpha\xi^J$ (где $\alpha \neq 0$ — симметричный элемент тела K) принимает более двух отличных от 0 значений в теле K. Рассуждение, аналогичное тому, которое проведено в работе Дьёдонне [13], стр. 374, показывает, что это последнее свойство всегда имеет место, если тело K бесконечно (если K не коммутативно, то следует рассмотреть централизатор элемента α), а также если K конечно и подтело K_0 симметричных элементов содержит более 5 элементов. Случай $K_0 = \mathbf{F}_5$ разбирается сходным образом; случай $K_0 = \mathbf{F}_3$ требует других методов (Дьёдонне [7], стр. 50—51 и 76—77) для доказательства существования прямой

$\psi(\Delta)$. После того как существование этой прямой доказано, окончательный результат, как и выше, получается применением основной теоремы проективной геометрии.

Пусть, наконец, $n = 3$. Если $J \neq 1$, то геометрическое рассуждение позволяет продолжить преобразование ψ на всю плоскость $P(E)$, если только K содержит более 25 элементов (Дьёдонне [7], стр. 77—78). Аналогичное рассуждение применимо и к ортогональным группам, если K содержит достаточно много элементов; однако проще воспользоваться тем, что группа $O_3^+(K, f)$ изоморфна группе $PGL_2(K)$, и применить результаты § 6. Относительно автоморфизмов оставшихся групп $U_3(\mathbf{F}_9)$ и $U_3(\mathbf{F}_{25})$ см. § 7.

Автоморфизмы унитарных и ортогональных групп над бесконечным телом характеристики 2 не определены.

§ 5. Автоморфизмы групп $U_n^+(K, f)$

(K — поле характеристики $\neq 2$.)

Если n нечетно, то инволюции типа $(1, n-1)$ принадлежат группе $U_n^+(K, f)$, и рассуждения § 4 применимы без всяких изменений. Напротив, если n четно, то экстремальные инволюции не принадлежат более группе $U_n^+(K, f)$, и приходится рассматривать инволюции типа $(2, n-2)$ или $(n-2, 2)$. Критерий, использующий функцию $\nu(u)$, не отличает, вообще говоря, эти инволюции от других, поскольку могут существовать инволюции других типов, для которых $\nu(u) = 8$. В общем случае не известно никакого критерия, отличающего эти инволюции от других. Однако, если *индекс* формы f *положителен*, можно охарактеризовать инволюции типа $(2, n-2)$ или $(n-2, 2)$, у которых $(n-2)$-мерное собственное подпространство *содержит изотропные векторы*, рассматривая их централизаторы в группе $U_n^+(K, f)$ и показывая (с помощью результатов о структуре унитарных групп, полученных в гл. II), что такой централизатор не изоморфен централизатору инволюции типа $(p, n-p)$ при $2 < p < n-2$ (Дьёдонне [7], стр. 52—53 и 79—80). Дополнительное рассуждение (использующее условие перестановочности двух инволюций) показывает, что автоморфизм группы $U_n^+(K, f)$ переводит *всякую* инволюцию типа $(2, n-2)$ или $(n-2, 2)$ в инволюцию одного из этих типов (там же, стр. 53—54).

Предположим теперь, что $n \geqslant 6$. Пусть S — множество инволюций типа $(2, n-2)$ или $(n-2, 2)$. Пусть, далее, u, v — две коммутирующие инволюции из S, U^+, V^+ (соответственно U^-, V^-) — их 2-мерные (соответственно $(n-2)$-мерные) собственные подпространства. Тогда либо $U^+ \cap V^+$ одномерно, либо $U^+ \subset V^-$ и $V^+ \subset \subset U^-$. В первом случае говорят, что инволюции u и v *иррегулярно перестановочны*, во втором — что они *регулярно перестановочны*. Для различения этих двух сортов перестановочности при $n > 6$ заметим, что uv принадлежит S тогда и только тогда, когда u и v иррегулярно перестановочны; при $n = 6$ необходимо другое рассуждение (Дьёдонне [7], стр. 54 и 80). Назовем теперь *минимальной парой* элементов множества S пару инволюций, 2-мерные собственные подпространства которых имеют одномерное пересечение. Для любых двух инволюций u, v из S обозначим через $c'(u, v)$ множество инволюций из S, регулярно перестановочных с u и v, и через $c'(c'(u, v))$ — множество инволюций из S, регулярно перестановочных со всеми инволюциями из $c'(u, v)$. При таких изменениях критерий Макки (§ 1) будет характеризовать минимальные пары.

Далее, исходя из автоморфизма φ группы $U_n^+(K, f)$, так же, как и для группы $Sp_{2m}(K)$ в § 3, определяется биективное преобразование пространства $P(E)$, и легко показывается, что оно переводит любые две ортогональные прямые пространства E в ортогональные прямые. Как и в предыдущих параграфах, отсюда получается окончательный результат:

При четном $n \geqslant 6$ всякий автоморфизм группы $U_n^+(K, f)$, где K — поле характеристики $\neq 2$, а f — эрмитова (или симметричная) форма индекса $\geqslant 1$, индуцируется автоморфизмом группы $U_n(K, f)$.

Автоморфизмы группы $U_2^+(K, f)$ $(J \neq 1)$ для формы f *индекса* 1 могут быть определены из результатов § 2, если воспользоваться тем, что эта группа изоморфна группе $SL_2(K_0)$, где K_0 — поле инвариантов антиавтоморфизма J (гл. II, § 4 и 5). Отсюда легко получить описание автоморфизмов группы $U_2(K, f)$ в этом же случае, используя тот факт, что ее коммутантом является как раз группа $U_2^+(K, f)$. Для формы f индекса 0 автоморфизмы группы $U_2^+(K, f)$ не определены.

Автоморфизмы группы $U_4^+(K, f)$, где $J \neq 1$ и K — бесконечное поле характеристики $\neq 2$, не известны. То же относится к группе $O_4^+(K, f)$ для формы f индекса 0.

Напротив, для формы f индекса 2 автоморфизмы группы $O_4^+(K, f)$ можно определить. В самом деле, известно (гл. II, § 9), что преобразования из $O_4^+(K, f)$ можно отождествить с преобразованиями $X \to UXV^{-1}$ в пространстве матриц 2-го порядка над K, где U и V — такие обратимые матрицы, что $\det(U) = \det(V)$ (при этом форма $f(x, x)$ отождествляется с $\det(X)$). При таком представлении коммутант $\Omega_4(K, f)$ группы $O_4^+(K, f)$ отождествляется с группой преобразований описанного выше вида, для которых $\det(U)$ является квадратом в K. Поскольку всем парам вида $(\lambda U, \lambda V)$, где $\lambda \neq 0$, соответствует одно и то же преобразование из O_4^+, группа Ω_4 изоморфна группе пар (U, V) с $\det(U) = \det(V) = 1$, рассматриваемых с точностью до одновременного умножения U и V на -1. Обозначим через G_1 (соответственно G_2) подгруппу группы Ω_4, образованную парами (U, I) (соответственно (I, V)), где U (соответственно V) — унимодулярная матрица. Подгруппы G_1, G_2 поэлементно перестановочны; их пересечение $G_1 \cap G_2$ совпадает с центром S группы Ω_4 (а также группы O_4), состоящим из двух элементов; каждая из них изоморфна группе $SL_2(K)$. Следовательно, группа Ω_4 изоморфна факторгруппе $(G_1 \times G_2)/S$ (но не прямому произведению группы S и двух экземпляров группы $PSL_2(K)$, как ошибочно утверждает Хуа в [9], стр. 118). Подгруппа G_1 (соответственно G_2) может быть интерпретирована как подгруппа группы O_4, сохраняющая все вполне изотропные плоскости, принадлежащие одному из двух классов транзитивности группы вращений (см. гл. II, § 6 и гл. III, § 4). Для всякого отражения $s \in O_4$ имеем $sG_1s^{-1} = G_2$.

Если поле K содержит более 3 элементов, то (гл. II, § 2) группа $SL_2(K)$ не имеет нетривиальных нормальных делителей, кроме центра. Отсюда немедленно следует, что в этом случае подгруппами G_1, G_2 и S исчерпываются все нетривиальные нормальные делители группы Ω_4 и, значит, всякий автоморфизм φ группы O_4^+ либо оставляет на месте каждую из подгрупп G_1, G_2, либо переставляет их. Комбинируя автоморфизм φ с внутренним автоморфизмом группы O_4, порожденным отражением, можно добиться того, чтобы он оставлял на месте G_1 и G_2.

Заметим теперь, что для любого автоморфизма σ поля K и любых обратимых матриц A, B преобразование $X \to AX^\sigma B^{-1}$ пространства матриц 2-го порядка отождествляется с полуподобием $g \in \Gamma O_4(K, f)$ (оно преобразует $\det(X)$ в $(\det(A))(\det(B))^{-1}(\det(X))^\sigma$. Из вида автоморфизмов группы $SL_2(K)$ (см. § 2)[1]) следует, что, комбинируя автоморфизм φ с автоморфизмом $u \to gug^{-1}$, можно добиться того, чтобы он *оставлял на месте все элементы подгруппы* G_2. Рассмотрим, далее, какой-нибудь автоморфизм τ поля K и такой эндоморфизм θ группы K^*, что $\theta(\xi)^2 = \xi^{1-\tau}$ для любого $\xi \in K^*$. Определим автоморфизм группы O_4^+, ставя в соответствие каждой паре (U, V) (такой, что $\det(U) = \det(V)$) пару $(\theta(\det(U))U^\tau, V) = (U_1, V_1)$. Так как паре $(\lambda U, \lambda V)$ при этом ставится в соответствие пара $(\lambda U_1, \lambda V_1)$, то это отображение при факторизации корректно определяет автоморфизм группы O_4^+, тождественный на подгруппе G_2 и совпадающий с преобразованием $U \to U^\tau$ на подгруппе G_1 (отождествленной с $SL_2(K)$). Используя описание автоморфизмов группы $SL_2(K)$ (§ 2), можно доказать, что, комбинируя автоморфизм φ с таким автоморфизмом и с автоморфизмом $u \to gug^{-1}$, где g — полуподобие $X \to AX$, можно добиться того, чтобы он *оставлял на месте все элементы подгрупп* G_1 *и* G_2. Но тогда он будет оставлять на месте все элементы из Ω_4, и, поскольку квадрат любого элемента $u \in O_4^+$ лежит в Ω_4 (гл. II, § 6), такой автоморфизм должен иметь вид

[1]) См. также примечание 2 на стр. 153. — *Прим. перев.*

$u \to \chi_0(u)u$, где χ_0 — гомоморфизм группы O_4^+ в ее центр S. Это завершает описание всех автоморфизмов группы O_4^+ (Хуа [9]).

§ 6. Автоморфизмы групп $PGL_n(K), PSL_n(K), PSp_{2m}(K)$

Принципиальная трудность применения предыдущих методов к проективным группам состоит в наличии в этих группах инволюций, которые происходят не из инволюций в группе $GL_n(K)$, а из *полуинволюций* в этой группе (гл. I, § 3). Поэтому нужно, прежде всего, отличить (групповыми свойствами) эти инволюции «второго рода» от тех, которые происходят от инволюций в $GL_n(K)$.

Рассмотрим вначале проективную группу $PGL_n(K)$, где $n \geqslant 3$ и K — тело характеристики $\neq 2$. *Экстремальные* инволюции в этой группе (происходящие из экстремальных инволюций в $GL_n(K)$) можно отличить от других инволюций первым методом, указанным в § 1, а именно, рассматривая максимальные множества коммутирующих сопряженных инволюций (Дьёдонне [7]). Исключение составляет случай, когда $n = 4$ и -1 не является квадратом в K. В этом случае экстремальные инволюции можно отличить от инволюций второго рода, заметив, что если u, v, u', v' — четыре сопряженные инволюции второго рода (соответствующие элементу $\gamma \in K$, не являющемуся квадратом), причем u перестановочно с v, а u' — с v', то произведения uv и $u'v'$ не обязательно сопряжены в группе $PGL_n(K)$. После того как получена характеризация экстремальных инволюций, методом § 1 устанавливается, что *всякий автоморфизм группы $PGL_n(K)$ получается посредством факторизации из автоморфизма группы* $GL_n(K)$. Результат остается справедливым при $n = 2$ (если характеристика тела K отлична от 2). Это доказал Хуа [9] теми же методами, которые он использовал при определении автоморфизмов группы $GL_2(K)$.

Если характеристика тела K равна 2, то инволюции второго рода в группе $PGL_n(K)$ $(n \geqslant 2)$ легко отличить от остальных, заметив, что если u, v — две коммутирующие сопряженные инволюции второго рода, то произведение uv никогда не сопряжено с u, в противоположность тому, что имеет место для инволюций из $GL_n(K)$. После этого применимы методы § 1, и сформулированный выше результат, следовательно, справедлив и в этом случае.

Аналогичные методы применимы и к группе $PSL_n(K)$, за исключением случая, когда n четно, характеристика тела K не равна 2 и -1 не принадлежит коммутанту группы K^* (Дьёдонне [7], стр. 19). В этом последнем случае, чтобы отличить 2-инволюции от инволюций второго рода (при $n \geqslant 4$), используют свойства централизаторов этих инволюций в группе $PSL_n(K)$ (гл. I, § 4). Затем применяются методы § 2. Получаемый результат состоит в том, что во всех случаях, когда известны автоморфизмы группы $SL_n(K)$, все автоморфизмы группы $PSL_n(K)$ получаются из них посредством факторизации.

Аналогичный результат получается и для проективных симплектических групп $PSp_{2m}(K)$. В этом случае также все сводится к отличению экстремальных инволюций от инволюций второго рода, что делается путем изучения централизаторов этих инволюций (см. гл. I, § 13 и 14, и Дьёдонне [7], стр. 32—34).

§ 7. Автоморфизмы групп $PU_n(K, f)$, $PU_n^+(K, f)$ и $P\Omega_n(K, f)$

Трудности, связанные с инволюциями второго рода, возникают и при определении автоморфизмов группы $PU_n(K, f)$. Положение осложняется тем, что методы § 6 применимы лишь при специальных предположениях относительно тела K или формы f. Тем не менее Уолтеру [1] удалось определить все автоморфизмы группы $PU_n(K, f)$ при $n \geqslant 5$ для любого тела K характеристики $\neq 2$, содержащего более 3 элементов. При этих условиях *всякий автоморфизм группы* $PU_n(K, f)$ *получается факторизацией из автоморфизма группы* $U_n(K, f)$ (эти автоморфизмы описаны в § 4). Основная трудность состоит в том, чтобы отличить экстремальные инволюции в группе $PU_n(K, f)$ от других инволюций, после чего рассуждения § 4 проходят без существенных изменений.

Метод Уолтера является развитием метода Риккарта (§ 1). Он основан в первую очередь на рассмотрении числа $\nu(\bar{u})$ для произвольной инволюции $\bar{u} \in PU_n(K, f)$. Этого, однако, недостаточно, так как $\nu(\bar{u}) = 4$ не только для экстремальных инволюций, но и для некоторых инволюций второго рода. Уолтер рассматривает, далее, множество $\bar{M}$ всех инволюций в группе $PU_n(K, f)$, для которых $\nu(\bar{u}) = 4$, и для любых трех различных коммутирующих инволюций $\bar{u}$, $\bar{v}$, $\bar{w}$ из $\bar{M}$ рассматривает число $\omega(\bar{u}, \bar{v}, \bar{w})$ элементов множества $c(c(\bar{u}, \bar{v}, \bar{w}))$ (где $c(S)$ имеет тот же смысл, что и в § 1, но в применении к рассматриваемой группе $PU_n(K, f)$). Пусть $\omega(\bar{u})$ обозначает максимум из чисел $\omega(\bar{u}, \bar{v}, \bar{w})$ для всевозможных $\bar{v}$, $\bar{w}$, удовлетворяющих предыдущим условиям. Детальное изучение множества $\bar{M}$ (основанное на результатах § 13 и 14 гл. I) позволило Уолтеру доказать, что условие $\omega(\bar{v}) = 8$ выделяет экстремальные инволюции среди всех элементов множества $\bar{M}$, исключая случаи, когда $n = 8$ и $n = 12$, которые исследуются особыми методами (см. там же).

Еще раньше Дьёдонне [7], стр. 55—57, нашел все автоморфизмы группы $PO_n(K, f)$ в предположениях, что f — симметричная форма *индекса* $\geqslant 1$, K — произвольное поле характеристики $\neq 2$ и $n \geqslant 3$. При нечетном n группа $PO_n(K, f)$ изоморфна группе $O_n^+(K, f)$, и ее автоморфизмы найдены в § 5. При четном n метод состоит в отличении неэкстремальных инволюций от таких экстремальных инволюций, собственная гиперплоскость которых содержит изотропные прямые, при помощи свойств централизаторов этих инволюций. Это делается достаточно легко путем рассмотрения первых двух коммутантов централизатора и использования того факта, что квадрат всякого элемента группы $O_n(K, f)$ принадлежит ее коммутанту. Окончательный результат состоит в том, что всякий автоморфизм группы $PO_n(K, f)$ получается факторизацией из автоморфизма группы $O_n(K, f)$.

Аналогичным методом определены автоморфизмы группы $PO_n^+(K, f)$ при $n = 6$ и любом четном $n \geqslant 10$ для формы f индекса $\geqslant 1$ (Дьёдонне [7], стр. 57—60).

В этом случае требуется проверить, что централизатор 2-инволюции, $(n-2)$-мерное собственное подпространство которой содержит изотропные прямые, не может быть изоморфен централизатору инволюции второго рода. Это делается путем рассмотрения в этих двух централизаторах *максимальных систем коммутирующих инволюций* и доказательства того, что они состоят из разного числа элементов. В рассматриваемых случаях автоморфизмы группы $PO_n^+(K, f)$ также получаются факторизацией из автоморфизмов группы $O_n^+(K, f)$ (определенных в § 5 при тех же предположениях). Используя особую структуру группы $O_4^+(K, f)$, такими же рассуждениями, как в § 5, можно показать, что этот результат справедлив и при $n = 4$ (исключая, быть может, случай, когда $K = \mathbf{F}_3$ и f — форма индекса 2).

Воненбургер [4] распространил предыдущие методы и результаты на группы $PO_n^+(K, f)$ для формы f индекса 0 при $n \geqslant 5$. При $n = 8$ происходят особенные явления, связанные с так называемой «тройственностью» (см. Э. Картан [2], Шевалле [1], Спрингер и Ван-дер-Блей [1]). А именно, могут существовать автоморфизмы группы $PO_8^+(K, f)$, преобразующие 2-инволюции в инволюции второго рода. Для того чтобы это было возможно, необходимо и достаточно, чтобы поле K было пифагоровым и чтобы для подходящего α форма αf обладала ортонормированным базисом (Воненбургер [5]).

Кажется правдоподобным, что, комбинируя метод, используемый для отличения инволюций второго рода от 2-инволюций в группе $PO_n^+(K, f)$, с методом, позволяющим отличать инволюции типов $(2, n-2)$ и $(n-2, 2)$ от других инволюций в группе $U_n^+(K, f)$ (§ 5), можно получить описание всех автоморфизмов группы $PU_n^+(K, f)$ в случае, когда K — произвольное поле характеристики $\neq 2$, $J \neq 1$ и f — форма индекса $\geqslant 1$.

Стейнберг [1] полностью описал автоморфизмы групп $PU_n^+(K, f)$ и $P\Omega_n(K, f)$ для *конечного* поля K в тех случаях, когда эти группы *простые* (см. гл. II, § 3, 4, 9 и 10). Мы не можем здесь привести его метод, который основан на теории групп Ли и совершенно отличен от методов этой книги. Во всех этих случаях (при $n \neq 8$) из результатов Стейнберга легко получается описание автоморфизмов групп $U_n(K, f)$ и $U_n^+(K, f)$. Для этого достаточно заметить, что всякий такой автоморфизм φ сохраняет центр и коммутант группы и, следовательно, определяет автоморфизм $\bar{\varphi}$ группы $PU_n^+(K, f)$, который по теореме Стейнберга происходит из автоморфизма ψ группы $U_n(K, f)$, имеющего вид, описанный в § 4. После этого все сводится к тому очевидному факту, что если $\bar{\varphi} = 1$, то $\varphi(u) = \chi(u)u$, где χ имеет тот же смысл, что и в § 4.

Автоморфизмы группы $\Omega_n(K, f)$ для бесконечного поля K в общем случае не известны (см., однако, частный случай в работе Дьёдонне [9], стр. 91—92). То же самое относится к группе $P\Omega_n(K, f)$ [1]).

Укажем, наконец, что Воненбургер [4] определил также автоморфизмы проективных групп подобий $PGO_n(K, f)$ и $PGO_n^+(K, f)$ при $n \geqslant 4$ для поля K характеристики $\neq 2$.

§ 8. Изоморфизмы классических групп

Классическая группа $G(n, K, f)$ зависит от тела K, целого числа n (размерности пространства, где действует группа) и, возможно, полуторалинейной формы f (или квадратичной формы Q) данного индекса. Мы будем называть изоморфизм группы $G(n, K, f)$ на группу $G'(n', K', f')$ *типовым*, если его определение не зависит от специальных свойств тела K (кроме, быть может, его коммутативности) и, тем самым, для любого (быть может, любого коммутативного) тела K имеет место изоморфизм соответствующих групп (при этом K', конечно, зависит от K). В противном случае мы будем говорить об *особом* изоморфизме.

Мы уже встречались с типовыми изоморфизмами. Таковыми являются изоморфизм группы $Sp_2(K)$ на группу $SL_2(K)$, где K — произвольное поле, и изоморфизм группы $U_2^+(K, f)$ на группу $SL_2(K_0)$, где K — поле,

[1]) См. приложение. — *Прим. перев.*

$J \neq 1$, f — форма индекса 1 и K_0 — поле инвариантов антиавтоморфизма J (гл. II, § 4 и 5). Бо́льшая часть других известных типовых изоморфизмов (с некоторыми из которых мы встречались, когда изучали группы O_3 и O_4 в § 9 гл. II) связывается с одним-единственным из них, следуя методу, систематически развитому Ван-дер-Варденом [1], стр. 18—28.

Этот метод исходит из следующих соображений. Пусть вначале K — поле характеристики $\neq 2$. Рассмотрим векторное пространство $F = K^4$ и пространство E *бивекторов* над F. Размерность пространства E равна 6; если $(e_i)_{1 \leqslant i \leqslant 4}$ — базис пространства F, то бивекторы $e_i \wedge e_j$ $(i < j)$ составляют базис пространства E. Внешнее произведение двух бивекторов x, y представляется в виде $f(x, y) e_1 \wedge e_2 \wedge e_3 \wedge e_4$, где $f(x, y)$ — невырожденная симметричная билинейная форма на E, *индекс которой равен* 3. Соотношение $f(x, x) = 0$ означает, что x — разложимый бивектор (соответствующий 2-мерному подпространству пространства F). Следовательно, грассманиан $G_1(F)$ может быть отождествлен с квадрикой в 5-мерном проективном пространстве $P(E)$, определяемой уравнением $f(x, x) = 0$. Пусть теперь v — произвольное полулинейное преобразование пространства F и $u = v^{(2)}$ — его вторая внешняя степень, т. е. такое полулинейное преобразование пространства E, что $u(s \wedge t) = v(s) \wedge v(t)$ для любых векторов s, t. Непосредственно можно проверить, что $f(u(x), u(y)) = (\det(v))(f(x, y))^{\sigma}$, где σ — автоморфизм поля K, соответствующий преобразованию v [1]). Иначе говоря, u — это полуподобие относительно формы f. Обратно, если u — такое полуподобие, то соответствующее проективное преобразование $\bar{u}$ отображает грассманиан $G_1(F)$ в себя. При этом, поскольку «соседние» точки множества $G_1(F)$ (в смысле § 2 гл. III) характеризуются тем, что прямая, соединяющая их в $P(E)$, лежит в $G_1(F)$, преобразования $\bar{u}$ и $\bar{u}^{-1}$ переводят соседние точки

[1]) Под $\det(v)$ здесь понимается определитель матрицы преобразования v в базисе (e_i) (или в любом базисе, для которого определитель матрицы перехода от базиса (e_i) равен 1). — *Прим. перев.*

в соседние. Следовательно, можно применить теорему Чоу (гл. III, § 2), которая позволяет заключить, что если $\bar{u}$ не переставляет два класса плоскостей $N_2^+(E)$, $N_2^-(E)$ квадрики $G_1(F)$, то существует такое полулинейное преобразование v пространства F, что преобразование $v^{(2)}u^{-1}$ оставляет на месте все точки пространства $P(E)$ и, значит, является гомотетией. Иначе говоря, в этом случае $u = \mu v^{(2)}$, где $\mu \in K^*$. Кроме того, легко видеть, что если $\mu v^{(2)} = \mu_1 v_1^{(2)}$, то $v_1 = \lambda v$ и $\mu = \lambda^2 \mu_1$, где $\lambda \in K^*$. Если, напротив, $\bar{u}$ переставляет $N_2^+(E)$ и $N_2^-(E)$, то преобразование u является произведением второй внешней степени полулинейного отображения пространства F на пространство F^* (т. е. корреляции пространства F) и канонического отображения (определенного с точностью до множителя) пространства бивекторов над F^* на пространство бивекторов над F. В первом случае, если v линейно, то u является *прямым подобием*[1]) относительно формы f, и обратно. Таким образом, отображение $(\mu, v) \to \mu v^{(2)}$ является *гомоморфизмом* прямого произведения $K^* \times GL_4(K)$ *на* группу $GO_6^+(K, f)$ прямых подобий относительно формы f; ядро этого гомоморфизма образовано элементами $(\lambda^2, \lambda^{-1})$, где $\lambda \in K^*$; множитель подобия $\mu v^{(2)}$ равен $\mu^2 \det(v)$. Поскольку *всякая* невырожденная симметричная билинейная форма *индекса* 3 на E *эквивалентна форме* f (гл. I, § 11), тем самым получается типовой изоморфизм для ортогональных групп таких форм.

Помимо этого, метод Ван-дер-Вардена основывается на следующих двух замечаниях:

1°. Пусть f — невырожденная симметричная билинейная форма на n-мерном векторном пространстве E над полем K и H — неизотропная гиперплоскость в пространстве E. Обозначим через f_1 ограничение формы f на H. Тогда группа $O_{n-1}^+(K, f_1)$ естественным образом отождествляется с подгруппой группы $O_n^+(K, f)$ (или группы $GO_n^+(K, f)$), сохраняющей ту линейную форму u,

---

[1]) См. § 13 гл. II. Утверждение вытекает из того, что $\det(v^2) = (\det v))^3$. — *Прим. перев.*

для которой уравнение $u(x) = 0$ определяет гиперплоскость H.

2°. Пусть K_1 — такое подполе поля K, что $[K: K_1] = 2$, и σ — нетождественный K_1-автоморфизм поля K. Тогда группа $GO_n^+(K_1, f)$ естественным образом отождествляется с подгруппой группы $GO_n^+(K, f)$, образованной преобразованиями, коммутирующими с полуинволюцией $(\xi_i) \to (\xi_i^\sigma)$, принадлежащей группе $\Gamma O_n(K, f)$ (где ξ_i — координаты точки пространства E в некотором базисе[1])).

Всякая невырожденная симметричная билинейная форма после некоторого числа последовательных *квадратичных* расширений становится формой *максимального индекса*. Поэтому для любой группы O_n^+ при $n \leqslant 6$ можно получить некоторый канонический изоморфизм, если *перевести* предыдущие условия на язык фактор-группы $K^* \times GL_4(K)$, изоморфной группе $GO_6^+(K, f)$ посредством описанного выше изоморфизма (для формы f индекса 3).

Таким образом получается 18 типовых изоморфизмов для групп O_n^+ при $3 \leqslant n \leqslant 6$. Они были частично перечислены Ван-дер-Варденом (см. [1], стр. 18—28, где можно также найти список предыдущих работ по этому вопросу) и полностью — Дьёдонне ([14], стр. 200—225). При этом используется, помимо прочего, общая процедура, описанная в § 15 гл. I.

Мы ограничимся здесь указанием получаемых таким образом типовых изоморфизмов между *простыми* или *полупростыми* группами (следовательно, для ортогональных групп, соответствующих формам индекса $\geqslant 1$).

1) $n = 6$, *f — форма индекса* 3. Отождествим форму f с рассматривавшейся выше формой в пространстве E бивекторов над пространством K^4. Гомоморфизм $v \to v^{(2)}$ посредством факторизации определяет изоморфизм *группы $PSL_4(K)$ на группу $P\Omega_6(K, f)$*.

2) $n = 6$, *f — форма индекса* 2. В некотором базисе пространства E форма f записывается в виде $f(x, x) =$

[1]) Предполагается, что коэффициенты билинейной формы f в этом базисе принадлежат полю K_1. — *Прим. перев.*

$= a_1\xi_1^2 + a_4\xi_4^2 - \xi_2\xi_5 + \xi_3\xi_6$, где элемент $-a_4/a_1$ не является квадратом в K. Дискриминант $\Delta = a_1a_4$ формы f обладает тем свойством, что $-\Delta$ *не является квадратом* в K. Пусть $K_1 = K(\sqrt{-\Delta})$ — квадратичное расширение поля K, получаемое присоединением корня ω многочлена $a_1X^2 + a_4$. Рассмотрим косоэрмитову форму $g(z, z) = \bar{\zeta}_1\zeta_2 - \bar{\zeta}_2\zeta_1 - a_1(\bar{\zeta}_3\zeta_4 - \bar{\zeta}_4\zeta_3)$ индекса 2 в пространстве K_1^4. Имеется *изоморфизм группы* $PU_4^+(K_1, g)$ *на группу* $P\Omega_6(K, f)$, определяемый следующим образом: каждому элементу $v \in U_4^+(K_1, g)$ сопоставляется матрица преобразования $v^{(2)}$ в базисе $(e_i')_{1 \leqslant i \leqslant 6}$ пространства E бивекторов над K_1^4, задаваемом формулами

$$e_1' = (\omega e_1 \wedge e_2 + e_3 \wedge e_4)/2\omega a_1, \quad e_2' = e_1 \wedge e_3, \quad e_3' = e_1 \wedge e_4,$$

$$e_4' = (\omega e_1 \wedge e_2 - e_3 \wedge e_4)/2\omega, \quad e_5' = e_2 \wedge e_4, \quad e_6' = e_2 \wedge e_3.$$

где $(e_i)_{1 \leqslant i \leqslant 4}$ — канонический базис пространства K_1^4 над K_1; далее производится факторизация по центрам.

3) $n = 6$, f — *форма индекса* 1 с таким дискриминантом Δ, что $-\Delta$ *является квадратом* в поле K. В некотором базисе пространства E форма f записывается в виде $f(x, x) = a_1\xi_1^2 + a_4\xi_4^2 - a_2\xi_2^2 - a_5\xi_5^2 + \xi_3\xi_6$, где $a_1a_5 = a_2a_4$. Пусть $K_1 = K(\omega)$, где ω имеет тот же смысл, что в 2), и K_2 — тело кватернионов над K, соответствующее паре $(-a_4/a_1, a_1a_2)$. Тело K_2 можно рассматривать как 2-мерное правое векторное пространство над K_1; при этом его базис составляют единица и такой элемент ρ, что $\rho^2 = a_1a_2$ и $\zeta\rho = \rho\bar{\zeta}$ для всякого $\zeta \in K_1$. В этих обозначениях имеется *изоморфизм группы* $PSL_2(K_2)$ *на группу* $P\Omega_6(K, f)$, который строится следующим образом. Будем рассматривать пространство $(K_2)_d^2$ как 4-мерное векторное пространство F над K_1. Пусть $(e_i)_{1 \leqslant i \leqslant 2}$ — канонический базис пространства $(K_2)_d^2$; тогда векторы e_1, e_2, $e_1\rho$, $e_2\rho$ составляют базис пространства F. Каждому элементу $v \in SL_2(K_2)$, рассматриваемому как линейное преобразование пространства F, поставим в соответствие матрицу преобразования $v^{(2)}$ в базисе

$(e'_i)_{1\leqslant i\leqslant 6}$ пространства E бивекторов над F, задаваемом формулами

$$e'_1=(\omega e_1\wedge e_2-a_2^{-1}e_1\rho\wedge e_2\rho)/2\omega a_1,$$
$$e'_4=(\omega e_1\wedge e_2+a_2^{-1}e_1\rho\wedge e_2\rho)/2\omega,$$
$$e'_2=(a_2^{-1}\omega e_1\wedge e_2\rho-e_1\rho\wedge e_2)/2\omega a_2,$$
$$e'_5=(a_2^{-1}\omega e_1\wedge e_2\rho+e_1\rho\wedge e_2)/2\omega,$$
$$e'_3=e_1\wedge e_1\rho,\quad e'_6=a_2^{-1}e_2\wedge e_2\rho.$$

Далее произведем факторизацию по центрам.

4) $n=6$, f — *форма индекса* 1 с таким дискриминантом Δ, что $-\Delta$ *не является квадратом* в K (этот случай не может представиться, если K — поле действительных чисел). В некотором базисе форма f записывается так же, как в 3), но без условия на коэффициенты a_i. Обозначим через ω, как и выше, корень многочлена $a_1X^2+a_4$ и через ω' — корень многочлена $a_2X^2+a_5$. Положим $K_1=K(\omega)$, $K'_1=K(\omega')$. Расширения K_1, K'_1 линейно свободны над K и, следовательно, их композит $K_3=K(\omega,\omega')$ является расширением Галуа 4-й степени над K; оно содержит поле $K_0=K(\sqrt{-\Delta})=K(\omega\omega')$. Пусть L — тело кватернионов над K_0, соответствующее паре $(-a_4/a_1,\ a_1a_2)$. Его можно рассматривать как 2-мерное правое векторное пространство над K_3; при этом его базис составляют единица и такой элемент ρ, что $\rho^2=$ $=a_1a_2$ и $\zeta\rho=\rho\bar{\zeta}$ для всякого $\zeta\in K_3$, где $\zeta\to\bar{\zeta}$ есть K-автоморфизм поля K_3, меняющий знаки у ω и ω'. Определим инволюцию J тела L таким образом, чтобы $\omega^J=$ $=-\omega$, $\omega'^J=\omega'$, $\rho^J=\rho$. Заметим, что это инволюция *второго рода* (гл. II, § 5). Рассмотрим на L_d^2 косоэрмитову форму индекса 1, записывающуюся в виде $g(z,z)=\zeta_1^J\zeta_2-\zeta_2^J\zeta_1$. Тогда имеется *изоморфизм группы* $T_2(L,g)/W_2$ (см. § 4 гл. II) *на группу* $P\Omega_6(K,f)$, который строится следующим образом. Пространство L_d^2 рассматривается как 4-мерное векторное пространство F над K; если при этом $(e_i)_{1\leqslant i\leqslant 2}$ — канонический базис пространства L_d^2 над L, то векторы e_1, e_2, $e_1\rho$, $e_2\rho$ составляют базис пространства F над K_3. Каждому элементу

$v \in T_2(L, g)$, рассматриваемому как линейное преобразование пространства F, ставится в соответствие матрица преобразования $v^{(2)}$ в базисе $(e'_i)_{1 \leqslant i \leqslant 6}$ пространства E бивекторов над F, образованном элементами

$$e'_1 = (\omega e_1 \wedge e_2 - a_2^{-1} e_1\rho \wedge e_2\rho)/2\omega a_1,$$
$$e'_4 = (\omega e_1 \wedge e_2 + a_2^{-1} e_1\rho \wedge e_2\rho)/2\omega,$$
$$e'_2 = (a_2^{-1}\omega' e_1 \wedge e_2\rho - e_1\rho \wedge e_2)/2\omega' a_2,$$
$$e'_5 = (a_2^{-1}\omega' e_1 \wedge e_2\rho + e_1\rho \wedge e_2)/2\omega',$$
$$e'_3 = e_1 \wedge e_1\rho, \quad e'_6 = a_2^{-1} e_2 \wedge e_2\rho.$$

Далее производится факторизация по центрам.

5) $n = 5$, f — *форма индекса* 2. Можно считать, что в некотором базисе пространства E форма f записывается в виде $f(x, x) = \xi_1\xi_4 - \xi_2\xi_5 + \xi_3^2$. Рассмотрим на K^4 знакопеременную форму $g(x, y) = \xi_1\eta_4 - \xi_4\eta_1 + \xi_3\eta_2 - \xi_2\eta_3$. Имеется *изоморфизм группы* $PSp_4(K, g)$ *на группу* $P\Omega_5(K, f)$, определяемый следующим образом. Для каждого элемента $v \in Sp_4(K, g)$ рассматривается матрица преобразования $v^{(2)}$ в базисе $(e'_i)_{1 \leqslant i \leqslant 6}$ пространства E' бивекторов над K^4, образованном бивекторами

$$e'_1 = e_1 \wedge e_2, \quad e'_2 = e_1 \wedge e_3, \quad e'_3 = (e_1 \wedge e_4 + e_2 \wedge e_3)/2,$$
$$e'_4 = e_3 \wedge e_4, \quad e'_5 = e_2 \wedge e_4, \quad e'_6 = (e_1 \wedge e_4 - e_2 \wedge e_3)/2,$$

где $(e_i)_{1 \leqslant i \leqslant 4}$ — канонический базис пространства K^4. Преобразование $v^{(2)}$ сохраняет подпространство, порожденное бивекторами e'_i с индексами $i \leqslant 5$, которое отождествляется с пространством E. Элементу v ставится в соответствие матрица ограничения преобразования $v^{(2)}$ на подпространстве E в базисе $(e'_i)_{1 \leqslant i \leqslant 5}$. Затем производится факторизация по центрам.

6) $n = 5$, f — *форма индекса* 1. Можно считать, что в некотором базисе пространства E форма f записывается в виде $f(x, x) = a_1\xi_1^2 + a_4\xi_4^2 - \xi_2\xi_5 + \xi_3^2$, причем элемент $-a_4/a_1$ не является квадратом в K. Положим $K_1 = K(\omega)$, где ω, как и выше, — корень многочлена $a_1X^2 + a_4$. Пусть, с другой стороны, L — тело кватернионов

над K, соответствующее паре $(-a_4/a_1, -a_1)$. Его можно рассматривать как 2-мерное правое векторное пространство над K_1, базис которого составляют единица и такой элемент ρ, что $\rho^2 = -a_1$ и $\zeta\rho = \rho\bar{\zeta}$ для любого $\zeta \in K_1$. Рассмотрим на пространстве L_d^2 косоэрмитову форму $g(z, z) = \zeta_1^J\zeta_2 - \zeta_2^J\zeta_1$ индекса 1, на этот раз относительно инволюции J *первого рода*, определенной так, чтобы $\omega^J = -\omega$, $\rho^J = \rho$ (инволюция типа I в классификации § 5 гл. II). В этих обозначениях имеется *изоморфизм группы* $T_2(L, g)/W_2$ *на группу* $P\Omega_5(K, f)$, который строится следующим образом. Пространство L_d^2 рассматривается как 4-мерное векторное пространство F над K_1; при этом если $(e_i)_{1 \leqslant i \leqslant 2}$ — канонический базис пространства L_d^2, то векторы e_1, e_2, $e_1\rho$, $e_2\rho$ составляют базис пространства F. Для каждого элемента $v \in T_2(L, g)$, рассматриваемого как линейное преобразование пространства F, строится матрица преобразования $v^{(2)}$ в базисе $(e'_i)_{1 \leqslant i \leqslant 6}$ пространства E' бивекторов над F, составленном из бивекторов

$$e'_1 = e_1 \wedge e_2, \qquad e'_2 = e_1 \wedge e_1\rho, \quad e'_3 = (e_1 \wedge e_2\rho - e_1\rho \wedge e_2)/2,$$

$$e'_4 = e_1\rho \wedge e_2\rho, \quad e'_5 = e_2 \wedge e_2\rho, \quad e'_6 = (e_1 \wedge e_2\rho + e_1\rho \wedge e_2)/2.$$

Преобразование $v^{(2)}$ сохраняет подпространство, порожденное бивекторами e'_i с номерами $i \leqslant 5$, которое отождествляется с пространством E. Элементу v сопоставляется матрица ограничения преобразования $v^{(2)}$ на подпространстве E в базисе $(e'_i)_{1 \leqslant i \leqslant 5}$. Затем производится факторизация по центрам.

7) $n = 4$, f — *форма индекса* 2. В некотором базисе пространства E форма f записывается в виде $f(x, x) = \xi_1\xi_4 - \xi_2\xi_3 = \det(X)$, где $X = \begin{pmatrix} \xi_1 & \xi_2 \\ \xi_3 & \xi_4 \end{pmatrix}$. Отождествив пространство E с пространством матриц 2-го порядка над K, мы можем построить *изоморфизм группы* $PSL_2(K) \times \times PSL_2(K)$ *на группу* $P\Omega_4(K, f)$. Для этого каждой паре (U_1, U_2) унимодулярных матриц 2-го порядка на K поставим в соответствие линейное преобразование

$X \to U_1 X U_2^{-1}$ пространства E (см. Дьёдонне [5]); затем профакторизуем по центрам.

8) $n = 4$, f — *форма индекса* 1. В некотором базисе форма f записывается в виде $f(x, x) = \xi_1\xi_4 \dot{-} (a_2\xi_2^2 + a_3\xi_3^2)$, где элемент $-a_3/a_2$, а значит, и дискриминант $\Delta = -a_2a_3$, *не является квадратом* в K. Пусть $K_1 = K(\sqrt{\Delta})$ — квадратичное расширение посредством присоединения к K корня ω многочлена $a_2X^2 + a_3$. В этих обозначениях имеется *изоморфизм группы* $PSL_2(K_1)$ *на группу* $P\Omega_4(K, f)$, который строится следующим образом. Пространство K_1^4 отождествляется с пространством матриц 2-го порядка над K_1, и для каждой матрицы $U \in SL_2(K_1)$ рассматривается линейное преобразование этого пространства, определяемое формулой $X \to UX(P\bar{U}P^{-1})$, где $P = \begin{pmatrix} 1 & 0 \\ 0 & a_2^{-1} \end{pmatrix}$, а $\zeta \to \bar{\zeta}$ — нетождественный K-автоморфизм поля K_1. Матрице U сопоставляется тогда матрица этого линейного преобразования в базисе $(e_i')_{1 \leqslant i \leqslant 4}$ пространства K_1^4, составленном из векторов

$$e_1' = e_1, \quad e_2' = (\omega e_2 + e_3)/2\omega a_2, \quad e_3' = (\omega e_2 - e_3)/2\omega, \quad e_4' = e_4,$$

где $(e_i)_{1 \leqslant i \leqslant 4}$ — канонический базис этого пространства. Далее производится факторизация по центрам.

9) $n = 3$, f — *форма индекса* 1. Можно считать, что в некотором базисе пространства E форма f записывается в виде $f(x, x) = \xi_1\xi_2 - \xi_3^2 = \det(X)$, где $X = \begin{pmatrix} \xi_1 & \xi_3 \\ \xi_3 & \xi_2 \end{pmatrix}$. Отождествив пространство E с пространством симметричных матриц 2-го порядка над K, мы можем построить *изоморфизм группы* $PSL_2(K)$ *на группу* $P\Omega_3(K, f)$. Для этого каждой матрице $U \in SL_2(K)$ поставим в соответствие линейное преобразование $X \to UX^tU$ пространства E, а затем профакторизуем по центрам.

Некоторые из изложенных выше результатов для размерностей 5 и 6 могут быть получены рассмотрением алгебр Клиффорда так же, как для размерностей 3 и 4

(Эйхлер [2], стр. 33—35, и Шевалле [1], стр. 102—105).

Среди изоморфизмов, получаемых этими методами (и не указанных в § 9 гл. II) упомянем еще изоморфизм между ортогональной группой $O_3^+(K, f)$, где f — форма *индекса* 0, и факторгруппой по группе гомотетий группы прямых унитарных подобий $GU_2^+(K_1, g)$, где K_1 — квадратичное расширение поля K, а g — эрмитова форма *индекса* 0 над K_1.

Для поля K характеристики 2 так же, как и выше, получается гомоморфизм группы $K^* \times GL_4(K)$ на группу $GO_6^+(K, Q)$, где Q — недефектная квадратичная форма индекса 3 (гл. I, § 16). Исходя из этого гомоморфизма, метод Ван-дер-Вардена с некоторыми естественными модификациями (например, дискриминант заменяется на псевдодискриминант, определенный в § 10 гл. II) легко перенести на поля характеристики 2. Изоморфизмы, получаемые таким способом (для размерностей $n = 4$ и $n = 6$), полностью определены Охарой [1].

Рассматривая другие типы полуинволюций в группе $\Gamma O_6(K, f)$, (где f — форма индекса 3), тем же методом можно получить изоморфизмы для унитарных групп над обобщенным телом кватернионов. Пусть L — такое тело (характеристики $\neq 2$), Z — его центр (обязательно бесконечный), J — его единственная инволюция, множество инвариантов которой совпадает с Z. Пусть ω — какой-либо элемент тела L, удовлетворяющий условию $\omega^J = -\omega$; тогда $\omega^2 \in Z$. Обозначим через K поле $Z(\omega)$. Известно, что в L существует такой элемент ρ, что $\rho^J = -\rho$, $\omega\rho = -\rho\omega$, $\rho^2 = \gamma \in Z$. Тело L можно рассматривать как правое векторное пространство над K; при этом элементы 1, ρ составляют его базис. Для любого $\xi \in K$ имеем $\rho^{-1}\xi\rho = \bar{\xi}$ (где $\xi \to \bar{\xi}$ — единственный нетождественный Z-автоморфизм поля K). Пусть теперь E есть правое n-мерное векторное пространство над L и f — невырожденная косоэрмитова форма на $E \times E$. Форма f может быть представлена в виде

$$f(x, y) = \overline{f_0(x, u_0(y))} + \rho f_0(x, y),$$

где f_0 — невырожденная симметричная билинейная форма на пространстве E, рассматриваемом как $2n$-мерное векторное пространство над K, а u_0 — полулинейное преобразование этого пространства (относительно автоморфизма $\xi \to \bar{\xi}$), определяемое равенством $u_0(x) = x\rho$, так что $u_0^2(x) = \gamma x$; при этом $f_0(u_0(x), u_0(y)) = -\gamma \overline{f_0(x, y)}$. Группа $U_n(L, f)$ интерпретируется тогда как подгруппа группы $O_{2n}(K, f_0)$, образованная преобразованиями, коммутирующими с u_0 (гл. I, § 13). При $n = 3$ и $n = 2$ это дает изоморфизмы групп $U_n(L, f)$ на другие классические группы (Дьёдонне [17]). Ограничимся случаем, когда f — форма индекса 1, и укажем получаемые при этом изоморфизмы для групп $T_n(L, f)$ (см. § 4 гл. II).

10) $n = 3$. Можно предполагать, что в некотором базисе $(c_k)_{1 \leqslant k \leqslant 3}$ пространства E (над L) форма f записывается в виде $f(z, z) = -{}^1/_2(\zeta_1^J \omega \zeta_1 + \zeta_2^J \zeta_3 - \zeta_3^J \zeta_2)$. Рассмотрим в пространстве K^4 косоэрмитову форму

$$g(x, x) = \bar{\xi}_1 \xi_2 - \bar{\xi}_2 \xi_1 - \omega(\bar{\xi}_3 \xi_3 - \gamma \bar{\xi}_4 \xi_4)$$

индекса 1. Имеется *изоморфизм группы* $PU_4^+(K, g)$ *на группу* $T_3(L, f)/W_3$, который строится следующим образом. Каждому элементу $v \in U_4^+(K, g)$ ставится в соответствие матрица преобразования $v^{(2)}$ в базисе (e_i') пространства бивекторов над K^4, определяемом формулами

$$e_1' = (e_1 \wedge e_2)/\omega, \quad e_2' = e_1 \wedge e_3, \quad e_3' = e_1 \wedge e_4,$$
$$e_4' = e_3 \wedge e_4, \quad e_5' = e_2 \wedge e_4, \quad e_6' = e_2 \wedge e_3,$$

где $(e_i)_{1 \leqslant i \leqslant 4}$ — канонический базис пространства K^4. При отождествлении базиса (e_i') с базисом пространства E над K, образованном векторами c_k и $c_k\rho$ ($1 \leqslant k \leqslant 3$), полученная матрица естественным образом интерпретируется как матрица из ортогональной группы, соответствующей форме f_0, ассоциированной с формой f указанным выше способом. Далее производится факторизация по центрам.

11) $n = 2$. В некотором базисе пространства E (над L) форма f представляется в виде $f(z, z) = -{}^1/_2(\zeta_2^J \zeta_3 - \zeta_3^J \zeta_2)$. Если обозначить через f' (соответственно через E') форму, обозначавшуюся в 10) через f (соответственно через E), то группа $U_2(L, f)$ может рассматриваться

как подгруппа группы $U_3(L, f')$, сохраняющая подпространство, задаваемое уравнением $\zeta_1 = 0$. Используя гомоморфизм, описанный в 10), преобразования из $U_2(L, f)$ можно отождествить с преобразованиями вида $\mu v^{(2)}$ (где $v \in GU_4(K, g)$), сохраняющими бивекторы $e_1 \wedge e_2$, $e_3 \wedge e_4$; это означает, что в пространстве K^4 преобразование v сохраняет плоскости $P' = Ke_1 + Ke_2$ и $P'' = Ke_3 + Ke_4$. Пусть v' и v'' — ограничения преобразования v на эти плоскости. Можно доказать, что в качестве v' можно взять любой элемент из $GL_2(Z)$, и тогда преобразование v'' должно иметь такой же определитель, как и v', и принадлежать группе $GU_2^+(K, g'')$ (где g'' — ограничение формы g на P''), изоморфной мультипликативной группе L^* отличных от 0 кватернионов. Окончательно мы видим, что группа $U_2(L, f)$ изоморфна факторгруппе подгруппы Γ *группы* $L^* \times GL_2(Z)$, образованной парами (q, v'), для которых $qq^J = \det(v')$, по подгруппе (изоморфной группе Z^*), образованной парами (λ, λ), где $\lambda \in Z^*$. При таком представлении группа $T_2(L, f)$ отождествляется с группой $PSL_2(Z)$, и ясно, что факторгруппа U_2/T_2 *не коммутативна* (выбирая подходящим образом тело L, можно добиться того, чтобы композиционный ряд группы U_2/T_2 содержал некоммутативные простые факторы).

Упомянем, наконец, что те же методы позволяют получить изоморфизмы для некоторых групп $PU_4(L, f)$. В самом деле, такая группа интерпретируется как подгруппа группы $PO_8^+(K, f_0)$. Изоморфизмы, о которых идет речь, получаются в случае, когда группа $PO_8^+(K, f_0)$ допускает особые автоморфизмы (см. § 7). Если φ — такой автоморфизм, он преобразует группу $PU_4(L, f)$ в подгруппу группы $PO_8^+(K, f_0)$, образованную элементами, инвариантными относительно автоморфизма $\varphi\psi_0\varphi^{-1}$, где ψ_0 — автоморфизм $v \to u_0 v u_0^{-1}$ группы $PO_8^+(K, f_0)$.

Помимо типовых изоморфизмов, о которых только что шла речь, известно некоторое число *особых* изоморфизмов между *конечными* группами типов $PSL_n(K)$, $PSp_{2m}(K)$, $PU_n^+(K, f)$, к которым здесь удобно присоединить симметрические группы $\mathfrak{S}_n$ и знакопеременные группы $\mathfrak{A}_n$. Эти изоморфизмы, открытые Жорданом [1] и Диксоном [1], суть следующие:

1) группа $PSL_2(\mathbf{F}_2)$ изоморфна симметрической группе $\mathfrak{S}_3$;

2) группа $PSL_2(\mathbf{F}_3)$ изоморфна знакопеременной группе $\mathfrak{A}_4$;

3) группы $PSL_2(\mathbf{F}_4)$ и $PSL_2(\mathbf{F}_5)$ обе изоморфны знакопеременной группе $\mathfrak{A}_5$;

4) группы $PSL_2(\mathbf{F}_7)$ и $PSL_3(\mathbf{F}_2)$ суть изоморфные простые группы порядка 168;

5) группа $PSL_2(\mathbf{F}_9)$ изоморфна знакопеременной группе $\mathfrak{A}_6$;

6) группа $PSL_4(\mathbf{F}_2)$ изоморфна знакопеременной группе $\mathfrak{A}_8$;

7) симплектическая группа $PSp_4(\mathbf{F}_2)$ изоморфна симметрической группе $\mathfrak{S}_6$;

8) группы $PSp_4(\mathbf{F}_3)$ и $PU_4^+(\mathbf{F}_4)$ суть изоморфные простые группы порядка 25920.

Метод, при помощи которого Жордан и Диксон установили эти изоморфизмы, состоит в том, что в рассматриваемых конечных группах, изоморфизм которых доказывается, выбираются системы образующих, содержащие одинаковое количество элементов и удовлетворяющие одинаковым соотношениям. Можно, однако, получить эти особые изоморфизмы другими методами, которые больше учитывают геометричесую природу рассматриваемых групп (Дьёдонне [18], Эдж [1, 2, 3]).

§ 9. Изоморфизмы классических групп (продолжение)

Естественно поставить вопрос, существуют ли изоморфизмы (типовые или особые) между классическими группами, кроме тех, которые описаны в § 8. Этот вопрос еще не решен каким-либо определенным образом. Мы укажем здесь основные результаты, полученные в этом направлении.

Прежде всего *группы* $PSL_n(K)$ *и* $PSL_m(K')$ $(n \geqslant 2, m \geqslant 2)$ *могут быть изоморфны только при* $n = m$, *за исключением групп* $PSL_2(\mathbf{F}_7)$ *и* $PSL_3(\mathbf{F}_2)$; *кроме того, при* $n = m > 2$ *изоморфизм возможен, только если тела* K *и* K' *изоморфны или антиизоморфны. Это же верно* *при $n = m = 2$, если тела K и K' коммутативны, за исключением случая, когда $K = \mathbf{F}_4$, $K' = \mathbf{F}_5$.*

Это утверждение было доказано в несколько этапов. Вначале Шрейер и Ван-дер-Варден [1] доказали его для *коммутативных тел* K и K'. Затем Дьёдонне ([7], стр. 22—25 и [6], стр. 91—94) дал доказательство для произвольных тел K и K', за исключением нескольких случаев, которые были разобраны Хуа и Ванем [1].

Следует различать два случая в зависимости от того, конечны тела K и K' или бесконечны. В первом случае метод Шрейера и Ван-дер-Вардена состоит в доказательстве того, что при $n \geqslant 3$ сдвиги могут быть охарактеризованы как элементы, отличные от единицы, централизатор которых имеет *максимальный порядок*. Метод, примененный в § 1 для определения автоморфизмов группы $GL_n(K)$, позволяет тогда доказать, что при $n \geqslant 3$ и $m \geqslant 3$ изоморфизм группы $PSL_n(K)$ на группу $PSL_m(K')$ определяет полулинейное отображение пространства K^n на пространство K'^m или дуальное к нему; отсюда и получается требуемое заключение. Остается исследовать случай, когда одно из чисел n, m равно 2. В этом случае используется тот факт, что в группе $PSL_2(K)$ над конечным полем K централизатор любого элемента, отличного от единицы, разрешим; далее рассматриваются порядки конечных групп, встречающихся в рассуждении.

В случае когда оба тела K, K' бесконечны, общим методом является изучение инволюций в рассматриваемых группах. Прежде всего тела K и K' должны иметь характеристику, равную 2 или не равную 2 одновременно. Это следует из того, что если характеристика тела K равна 2, то в группе $PSL_n(K)$ существуют бесконечные системы коммутирующих сопряженных инволюций, в противоположность случаю, когда характеристика не равна 2. Предположим, что характеристика тел K и K' не равна 2. Рассматривая число элементов в максимальных системах коммутирующих сопряженных инволюций в группе $PSL_n(K)$, можно тогда, вообще говоря, доказать, что $m = n$. Для малых значений m и n в некоторых случаях требуются дополнительные рассуждения; наиболее трудный случай, разобранный Хуа и Ванем

[1], — это когда $n = 2$, $m = 3$. После того как установлено равенство $m = n$, методы § 6 позволяют при $m = n > 2$ доказать, что тела K и K' изоморфны или антиизоморфны.

Если характеристика тела K равна 2 и $n \geqslant 6$, то сдвиги в группе $PSL_n(K)$ характеризуются свойством, не зависящим от n (§ 1 и 6). Следовательно, если характеристика тел K и K' равна 2, то при $n \geqslant 6$ и $m \geqslant 6$ всякий изоморфизм группы $PSL_n(K)$ на группу $PSL_m(K')$ должен переводить сдвиги в сдвиги; отсюда легко получается требуемый результат. Если одно из чисел n и m меньше 6, то требуются дополнительные рассуждения. Наиболее трудные случаи, соответствующие парам (2, 3) и (4, 5), разобраны Хуа и Ванем (см. там же).

Что касается симплектических групп, можно доказать, что *группы $PSp_{2m}(K)$ и $PSp_{2n}(K')$ могут быть изоморфны, только если $m = n$ и тела K и K' изоморфны, за исключением случая $m = n = 1$, $K = \mathbf{F}_4$, $K' = \mathbf{F}_5$* (Дьёдонне [7], стр. 39—41). Для доказательства так же, как и выше, изучаются централизаторы инволюций в рассматриваемых группах.

Возможные изоморфизмы между классической группой вида $P\Omega_n(K, f)$ или $PU_n^+(K, f)$ (где K коммутативно) и другой классической группой в общем случае не найдены. Однако это может быть сделано полностью в случае *конечного* поля K. При помощи арифметического изучения формул для *порядков* классических групп над конечными полями Артин [1, 2] показал, что конечные группы типов $PSL_n(K)$, $PSp_{2m}(K)$, $P\Omega_q(K, f)$, $PU_r^+(K)$ (где поле K не фиксировано), $\mathfrak{S}_h$ и $\mathfrak{A}_h$ имеют попарно *различные* порядки, за исключением пар, для которых имеется типовой или особый изоморфизм, пары групп $PSL_3(\mathbf{F}_4)$ и $PSL_4(\mathbf{F}_2)$, которые, как мы видели выше, не изоморфны, и, наконец, пар групп $PSp_{2m}(\mathbf{F}_q)$ и $P\Omega_{2m+1}(\mathbf{F}_q)$ (q нечетно, $m \geqslant 3$). Последнее совпадение порядков заметил Диксон [1], который доказал, что две такие группы не изоморфны (см. там же); другое доказательство см. у Дьёдонне [7], стр. 73—74. Таким образом, *между рассматриваемыми простыми конечными* *группами нет никаких изоморфизмов, кроме изоморфизмов (типовых и особых), указанных в* § 8. Можно также заключить, что для групп вида $P\Omega_n(K, f)$, где f — форма индекса $\geqslant [(n-2)/2]$, и $PU_n^+(K, f)$, где f — форма индекса $[n/2]$, нет других *типовых* изоморфизмов, кроме указанных в § 8, поскольку такой изоморфизм должен был бы тогда существовать и для *конечных* групп этих типов.

ПРИЛОЖЕНИЕ

Методы, использовавшиеся в § 1—7 гл. IV, основываются главным образом на изучении *инволюций* в рассматриваемых группах; это предполагает, с одной стороны, что в группе имеется «достаточно много» инволюций и, с другой стороны, что известно их явное описание. В 1967 г. О'Мира [4] придумал совершенно новый метод, не использующий инволюций и позволяющий разрешать многочисленные вопросы, не поддававшиеся решению прежними методами. А именно, в работе [4] О'Мира нашел своим методом автоморфизмы групп $\Omega_n(K, f)$ и $O'_n(K, f)$ при $n \geqslant 7$ и $n \neq 8$ для поля K характеристики $\neq 2$, содержащего более 3 элементов. Он показал, что для некоторых полей может случиться, что в группе Ω_n нет *ни одной* инволюции, отличной от 1, так что его результат не может быть получен прежними методами.

Основная идея этой работы состоит в рассмотрении *плоских вращений* в изучаемой группе Δ (равной O'_n или Ω_n). Под плоским вращением автор понимает преобразование из группы Δ, подпространство P неподвижных точек которого имеет размерность $n-2$, причем может быть изотропным; вращение называется регулярным, если это подпространство не изотропно; в любом случае плоскость R, ортогональная к P, называется *базисной* плоскостью вращения. Цель состоит в том, чтобы доказать, что автоморфизм σ группы Δ индуцирует перестановку плоскостей пространства K^n с обычными свойствами инцидентности, позволяющими применить, как в § 1—7, основную теорему проективной геометрии. Для этого доказывается, что всякая плоскость R является базисной плоскостью некоторого плоского вращения, принадлежащего группе Δ и преобразуемого автоморфизмом σ в плоское вращение. Доказательство очень технично, причем наиболее труден случай, когда плоскость P не изотропна. Свойство, на которое в конечном счете опирается автор, состоит в том, что регулярные плоские вращения с данной базисной плоскостью образуют коммутативную группу. Если для всякого подмножества $X \subset \Delta$ обозначить через $C(X)$ его централизатор в Δ, а через DH обозначить коммутант группы H, то можно доказать, что для любого плоского вращения u при $k \geqslant 2$ группа $DCD^kC(u)$ коммутативна. Так как это свойство чисто групповое, то тем же свойством обладает элемент $\sigma(u)$. В предположении, что $n \geqslant 5$, автор выводит отсюда сначала, что $\sigma(u)$ есть вращение, подпространство неподвижных точек которого имеет размерность, равную $n-2$ или одному из чисел 0, 1, 2. Затем при помощи ряда довольно тонких геометрических рассуждений он исключает последние три случая (при $n \geqslant 7$ и $n \neq 8$) и доказывает, что определяемое автоморфизмом σ взаимно однозначное преобразование множества плоскостей пространства K^n обладает обычными свойствами инцидентности.

Этот метод интересен тем, что он применим во многих других случаях. Например, в ранней работе [2] О'Мира, используя сдвиги, определил при $n \geqslant 3$ автоморфизмы групп $GL_n(A)$ и $SL_n(A)$ для произвольного *целостного кольца* A. Данное в этой работе доказательство того, что всякий автоморфизм переводит сдвиги в сдвиги, было длинным и трудным. В работе [6] О'Мира значительно упростил это доказательство, рассмотрев упомянутые выше группы как подгруппы группы $GL_n(K)$ (где K — поле частных кольца A) и охарактеризовав сдвиги, принадлежащие любой подгруппе $\Delta \subset GL_n(K)$, содержащей «достаточно много» сдвигов (в том смысле, что для всякой гиперплоскости H и для всякой прямой $D \subset H$ в группе Δ имеется сдвиг вдоль H в направлении D), при помощи групп $CDC(u)$ для некоторых элементов $u \in \Delta$.

Аналогичным способом можно определить автоморфизмы ортогональных групп над локальными или дедекиндовыми кольцами, а также их «конгруэнц-подгрупп» (О'Мира [5], О'Мира и Цассенхауз [1]) и автоморфизмы унитарных групп над телом характеристики 2 (Джонсон [3]).

Упомянем, наконец, другое направление, использующее гомологии групп и теорию групп Ли (Борель [1]), но охватывающее только подгруппы полупростых вещественных групп Ли [1]).

---

[1]) Абстрактные изоморфизмы изотропных простых алгебраических групп над произвольными полями (в частности, классических групп, соответствующих формам индекса $\geqslant 1$) найдены Борелем и Титсом (Borel A., Tits J., Homomorfhismes «abstraits» de groupes algébriques simples, *Ann. Math.*, 97 (1973), 499—571).

Об изоморфизмах классических групп над целостными кольцами см. Hahn A. J., The isomorphisms of certain subgroups of the isometry groups of reflexive spaces, *J. Algebra*, 27 (1973), 205—242. — *Прим. перев.*

СПИСОК ЛИТЕРАТУРЫ[1]

Эта библиография совершенно не претендует на полноту в отношении работ, появившихся до 1935 г. Список этих работ читатель может найти в книге Ван-дер-Вардена [1].

Абе (Abe M.)

1. Projective transformation groups over non-commutative fields, Sijo-Sûgaku-Danwakai, 240 (1942).

Алберт (Albert A. A.)

1. Symmetric and alternate matrices in an arbitrary field, I, *Trans. Amer. Math. Soc.*, 43 (1938), 386—436.

Аллен (Allen H. P.)

1. Hermitian forms, *Trans. Amer. Math. Soc.*, 138 (1969), 199—210; *J. Algebra*, **10** (1968), 503—515.

Анкочеа (Ancochea G.)

1. Le théorème de von Staudt en géométrie projective quaternionienne, *J. reine angew. Math.*, 184 (1942), 193—198.

Артин (Artin E.)

1. The orders of the linear groups, *Comm. Pure Appl. Math.*, 8 (1955), 355—366;
2. The orders of the classical simple groups, *Comm. Pure Appl. Math.*, 8 (1955), 455—472.
3. Geometric algebra. Interscience Tracts n° 3, New York — London, Interscience Publ., 1957. [Русский перевод: Артин Э., Геометрическая алгебра, «Наука», М., 1969.]

Арф (Arf C.)

1. Untersuchungen uber quadratische Formen in Körpern der Charakteristik 2, I, *J. reine angew. Math.*, 183 (1941), 148—167.

Асано, Накаяма (Asano K., Nakayama T.)

1. Über halblineare Transformationen, *Math. Ann.*, **115** (1937), 87—114.

---

[1]) Звездочкой отмечены работы, добавленные при переводе. — *Прим. перев.*

Бахман (Bachmann F.)

1. Eine Kennzeichnung der Gruppe der gebrochen-linearen Transformationen, *Math. Ann.*, **126** (1953), 79—92.

Беге (Böge S.)

1. Schiefhermitesche Formen uber Zahlkörpern und Quaternionenschiefkörpern, *J. reine angew. Math.*, **221** (1966), 85—112.

Биркгоф, фон Нейман (Birkhoff G., von Neumann J.)

1. The logic of quantum mechanics, *Ann. of Math.*, **37** (1936), 823—843.

Болт, Рум, Уолл (Bolt B., Room T. G., Wall G. E.)

1. On the Clifford collineation transformation and similarity group, I, II, *J. Austr. Math. Soc.*, **2** (1961), 60—96.

Борель (Borel A.)

1. On the automorphisms of certain subgroups of semi-simple Lie groups. Algebraic geometry (Papers presented at the Bombay Colloquium, 1968), Tata Institute of fundamental research, 43—73.

Бреннер (Brenner J.)

1. The linear homogeneous group, *Ann. of Math.*, **39** (1938), 472—493.
2. The linear homogeneous group, II, *Ann. of Math.*, **45** (1944), 100—109.

Бурбаки (Bourbaki N.)

1. Algèbre, chap. II: Algèbre linéaire, Actual. Scient. et Ind., 3e ed., n° 1236, Paris: Hermann, 1962. [Русский перевод: в книге Бурбаки Н., Алгебра. Алгебраические структуры. Линейная и полилинейная алгебра, Физматгиз, М., 1962.]
2. Algèbre, chap. VII: Modules sur les anneaux principaux, Actual. Scient. et Ind., n° 1179, Paris: Herman 1952. [Русский перевод в книге Бурбаки Н., Алгебра. Модули, кольца, формы, «Наука», М., 1966.]
3. Algèbre, chap. IX, Actual. Scient. et Ind., n° 1272, Paris: Hermann, 1959. [Русский перевод там же.]

Бэр (Baer R.)

1. Free mobility and Orthogonality, *Trans. Amer. Math. Soc.*, **68** (1951), 439—460.
2. The group of motions of a two-dimensional elliptic geometry, *Comp. Math.*, **9** (1951), 271—288.
3. Linear algebra and projective geometry, New York: Acad. Press, 19—52. [Русский перевод: Бэр Р., Линейная алгебра и проективная геометрия, ИЛ, М., 1955.]

Ван-дер-Варден (Van der Waerden B. L.)

1. Gruppen von linearen Transformationen, Berlin: Julius Springer 1935.

Ван-Дрооге (Van Drooge D. C.)

1. Spinor theory of quadratic quaternion forms, *Koninkl. Ned. Akad. Wetenschap. Proc.*, Ser. A, **70** (1967), 487—523.

Вань (Wan Z.-X., иное написание Wan C.-H.)

1. On the automorphisms of linear groups over a non-commutative Euclidean ring of characteristic 2, *Sci. Rec.*, **1** (1957), 5—8.
2. On the commutator subgroup of the unitary group, *Sci. Rec.*, **4** (1960), 343—348.

Вань, Ван (Wan Z.-X., Wang Y.-X.)

1. On the automorphisms of symplectic groups over a field of characteristic 2, *Sci. Sinica* **12** (1963), 289—315.

Веблен, Янг (Veblen O., Young J. W.)

1. Projective geometry. 2 vol., 2nd ed., Boston, 1918—1938.

Вейль (Weil A.)

1. Algebras with involutions and the classical groups, *J. Ind. Math. Soc.*, **24** (1961), 589—623. [Русский перевод: Вейль А., Алгебры с инволюциями и классические группы, в сб. «Математика», 7 : 4 (1963), 31—55.]

Витт (Witt E.)

1. Theorie der quadratischen Formen in beliebigen Körpern, *J. reine angew. Math.*, **176** (1937), 31—44.
2. Über eine Invariante quadratischer Formen mod. 2, *J. reine angew. Math.*, **193** (1954), 119—120.
3. Verschiedene Bemerkungen zur Theorie des quadratischen Formen über einem Körper, Centre Belge Rech. math., Colloque d'Alg. sup. Bruxelles (1957), 245—250.

Витт, Клингенберг (Witt E., Klingenberg W.)

1. Über die Arfsche Invariante quadratischer Formen mod. 2. *J. reine angew. Math.*, **193** (1954), 121—122.

Вольфхардт (Wolffhardt K.)

1. Über eine Charakterisierung der Determinante, *Math. Z.*, **103** (1968), 259—267.

Воненбургер (Wonenburger M.)

1. Study of a semi-involutive similitude, *Rev. Mat. Hisp. Am.*, Ser. 4, **20**, n° 1 (1960).
2. The Clifford algebra and the group of similitudes, *Canad. J. Math.*, **14** (1962), 45—59.
3. Study of certain similitudes, *Canad. J. Math.*, **14** (1962), 60—68.
4. The automorphisms of the group of simiitudes and some related groups, *Amer. J. Math.*, **84** (1963), 600—614.
5. The automorphisms of $PO_8^+(Q)$ and $PS_8^+(Q)$, *Amer. J. Math.*, **84** (1963), 635—641.
6. The automorphisms of the group of rotations and its projective group corresponding to quadratic forms of any index, *Canad. J. Math.*, **15** (1963), 302—303.

Гётцки (Götzky M.)

1. Über die Erzeugenden der engeren unitären Gruppen, *Arch. d. Math.*, **19** (1968), 383—389.
2. Unverkürzbare Produkte und Relationen in unitaren Gruppen, *Math. Z.*, **104** (1968), 1—15.

Джекобсон (Jacobson N.)

1. Pseudo-linear transformations, *Ann. of Math.*, **38** (1937), 484—507.
2. Normal semi-linear transformations, *Amer. J. Math.*, **61** (1939), 45—58.
3. Theory of rings, Math. Surveys, n°2, New York, 1943. [Русский перевод: Джекобсон Н., Теория колец, ИЛ, М., 1947.]

4*. A note on hermitian forms, *Bull. Amer. Math. Soc.*, **46** (1950), 265—268.

Джонсон (Johnson A. A.)

1. Integral representations of hermitian forms over local fields, *Bull. Amer. Math. Soc.*, **72** (1966), 118—121.
2. Integral representations of hermitian forms over local fields, *J. reine angew. Math.*, **229** (1968), 57—80.
3. The automorphisms of unitary groups over a field of characteristic 2, *Amer. J. Math.*, **93** (1971), 367—384.

Диксон (Dickson L. E.)

1. Linear groups, Leipzig: B. G. Teubner, 1901.
2. Theory of linear groups in an arbitrary field, *Trans. Amer. Math. Soc.*, 2 (1901), 363—394.
3. Linear groups in infinite field, *Proc. Lond. Math. Soc.*, **34** (1902), 185—205.

Дьёдонне (Dieudonné J.)

1. Les déterminants sur un corps non commutatif, *Bull. Soc. Math. France*, **71** (1943), 27—45.
2. Compléments à trois articles antérieurs, *Bull. Soc. Math. France*, **74** (1946), 59—68.
3. Sur la réduction canonique des couples de matrices, *Bull. Soc. Math. France*, **74** (1946), 130—146.
4. Sur les groupes classiques, Actual. Scient. et Ind., n°1040, Paris: Hermann, 1948.
5. Sur une généralisation du groupe orthogonal à quatre variables, *Arch. d. Math.*, **1** (1949), 282—287.
6. Sur les systèmes maximaux d'involutions conjuguées et pertables dans les groupes projectifs, *Summa Bras. Math.*, **2**, (1950) 59—94;
7. On the automorphisms of the classical groups, *Memoirs Amer. Math. Soc.*, n°2 (1951), 1—95.
8. Algebraic homogeneous spaces over fields of characterististic two, *Proc. Amer. Math. Soc.*, 2 (1951), 295—304.
9. On the orthogonal groups over the rational field, *Ann. of Math.*, **54** (1951), 85—93.

10. Orthogonal and unitary groups over the rational field, *Amer. J. Math.*, **73** (1951), 940—948.
11. Sur les groupes orthogonaux rationnels à trois et quatre variables, *C. r. Acad. Sci.* (Paris), **233** (1951), 541—543.
12. On the orthogonal groups over an algebraic number field, *Proc. Lond. Math. Soc.* (3), **2** (1952), 245—256.
13. On the structure of unitary groups, *Trans. Amer. Math. Soc.*, **72** (1952), 367—385.
14. Les extensions quadratiques des corps non commutatifs et leurs applications, *Acta Math.*, **87** (1952), 175—242.
15. A problem of Hurwitz and Newman, *Duke Math. J.*, **20** (1953), 381—390.
16 On the structure of unitary groups (II). *Amer. J. Math.*, **75** (1953), 665—678.
17 Sur les groupes unitaires quaternioniques à deux et à trois variables, *Bull. Sci. Math.*, **77** (1953), 195—213.
18 Les isomorphismes exceptionnels entre les groupes clasciques finis, *Canad. d. of Math.*, **6** (1954), 305—315.
19. Sur les générateurs des groupes classiques, *Summa Bras. Math.*, **3** (1955), 149—178.
20. Pseudodiscriminant and Dickson invariant, *Pacif. J. Math.*, **5** (1955), 907—910.
21. Sur les multiplicateurs des similitudes, *Rend. Circ. Math. Palermo* (2), **3** (1954), 398—408.
22. Sur la représentation paramétrique de Cayley, *Arch. d. Math.*, **9** (1958), 39—41.

Жордан (Jordan C.)

1. Traité des substitutions et des équations algébriques, Paris: Gauthier-Villars, 1870.
2. Sur les groupes linéaires (mod. p) à invariant quadratique, *J. de Math.* (7), **2** (1916), 253—280.
3. Mémoire sur les formes bilinéaires, *J. de Math.* (2), **19** (1874), 35—54 (=Oeuvres, vol. III, Paris, Gauthier — Villars, 1962).

Ивасава (Iwasawa K.)

1. Über die Einfachheit der speziellen projektiven Gruppen, *Proc. Imp. Acad. Tokyo*, **17** (1941), 57—59.

Капланский (Kaplansky I.)

1. Forms in infinite-dimensional spaces, *Anals Acad. Bras. Ci.*, **22** (1950), 1—17.
2. Orthogonal similarity in infivite-dimensional spaces, *Proc. Amer. Math. Soc.*, **3** (1952), 16—25.
3. Quadratic forms, *J. Math. Soc. Japan*, **5** (1953), 200—207 (cf. *Math. Rev.*, **15** (1954), 500).

Картан (Cartan E.)

1. Lecons sur la géométrie projective complexe, Paris: Gauthier — Villars, 1931.
2 Lecons sur la théorie des spineurs, vol. II, Actual. Scient. et Ind., n°701, Paris: Hermann, 1938. [Русский перевод: Картан Э., Теория спиноров, ИЛ, М., 1947.]

Клингенберг (Klingenberg W.)
1. Lineare Gruppen über lokalen Ringen, *Amer. J. Math.*, **83** (**1961**), 137—153.
2. Orthogonale Gruppen über lokalen Ringen, *Amer. Math.*, **83** (1961), 281—320.
3. Symplectic groups over local rings, *Amer. J. Math.*, 85 (1963), 232—240.

Клиффорд (Clifford W. K.)
1. Applications of Grassmann's extensive algebra, Math. Papers, 266—276, London: Macmillan, 1882.
2. On the classification of geometric algebras, Math. Papers, 397—401, London: Macmillan, 1882.

Кнезер (Kneser M.)
1. Orthogonale Gruppen über algebraischen Zahlkörpern, *J. reine angew. Math.*, **196** (1956), 213—220.
2. Bestimmung des Zentrums der Cliffordschen Algebren einer quadratischen Form uber einem Körper der Charakteristik 2, *J. reine angew. Math.*, **193** (1954), 123—125.
3. Über die Ausnahme — Isomorphismen zwischen endlichen klassischen Gruppen, *Abn. Math. Sem. Hamburg Univ.*, **31** (1967), 136—140.

Лакруа (Lacroix N. H. J.)
1. Two-dimensional linear groups over local rings, *Canad. J. Math.*, **21** (1969), 106—135.

Ландгерр (Landherr W.)
1. Äquivalen Hermitescher Formen über einem beliebigen algebraischen Zahlkörper, *Abh. Math. Sem. Hamburg. Univ.*, **11** (1935), 245—248.
2. Liesche Ringe vom Typus A über einem algebraischen Zahlkörper (Die lineare Gruppe) und hermitesche Formen über einem Schiefkörper, *Abn. Math. Sem. Hamburg Univ.*, **12** (1938), 200—241.

Ландин, Райнер (Landin J., Reiner I.)
1. Automorphisms of the general linear group over a principal ideal domain, *Ann. of Math.*, **65** (1957), 519—526.
2. Automorphisms of the Gaussian modular group, *Trans. Amer. Math. Soc.*, **87** (1958), 76—89.
3. Automorphisms of the two-dimensional general linear group over a Euclidean ring, *Proc. Amer. Math. Soc.*, **9** (1958), 209—216.

Лингенберг (Lingenberg R.)
1. Die orthogonalen Gruppen O_3 (K, Q) über Körpern von Char. 2, *Math. Nachr.*, **21** (1960), 371—380.

Липшиц (Lipschitz R.)

1. Untersuchungen über die Summen von Quadraten, Bonn, 1886.
2. Analyse francaise du mémoire précédent, *Bull. Sci. Math.* (2), **10** (1886), 163—183.
3. Correspondence, *Ann. of Math.*, **69** (1959), 247—251.

Макки (Mackey G. W.)

1. Isomorphisms of normed linear spaces, *Ann. of Math.*, **43** (1942), 244—260.

Маркус, Хан (Marcus M., Khan N. A.)

1. A note on a group defined by a quadratic form, *Canad. Math. Bull.*, 3 (1960), 143—148.

Минковский (Minkowski H.)

1. Über die Bedingungen, unter welchen zwei quadratische Fermen mit rationalen Koeffizienten rational einander transformiert werdn können, *J. reine angew. Math.*, **106** (1850), 5—26. (=*Ges. Abh.*, **1** (1914), 219).

Нагао (Nagao H.)

1. On $GL(2, k[x])$, *J. Inst. Poly. Osaka*, **10** (1959), 117—121.

Накаяма (Nakayama T.)

1. Über die Klassifikation halblinearer Transformationen, *Proc. Phys. Math. Soc. Japan*, **19** (1937), 99—107.
2. A note on the elementary divisor theory in non-commutative domains, *Bull. Amer. Math. Soc.*, **44** (1938), 719—723.

Настольд (Nastold H. J.)

1. Über mehrfach metrische Räume, *Arch. der Math.*, **9** (1958), 256—261.

О'Мира (O'Meara O. T.)

1. On the finite generation of linear groups over Hasse domains, *J. reine angew. Math.*, **217** (1965), 79—108.
2. The automorphisms of the linear groups over any integral domain, *J. reine angew. Math.*, **223** (1966), 56—100.
3. The automorphisms of the standard symplectic group over any integral domain, *J. reine angew. Math.*, **230** (1968), 104—138.
4. The automorphisms of the orthogonal groups $\Omega_n(V)$ over fields, *Amer. J. Math.*, **90** (1968), 1260—1306.
5. The automorphisms of the orthogonal groups and their congruence subgroups over arithmetic domains, *J. reine angew. Math.*, **238** (1969), 169—206.
6. Group-theoretic characterization of transvections using CDC, *Math. Z.*, **110** (1969), 385—394.

7*. Introduction to quadratic forms, Springer — Verlag, 1963.

О'Мира, Поллак (O'Meara O. T., Pollak B.)

1. Generation of local integral orthogonal groups, *Math. Z.*, **87** (1965), 385—400.
2. Generation of local integral orthogonal groups, II, *Math. Z.*, **93** (1966), 171—188.

О'Мира, Цассенхауз (O'Meara O. T., Zassenhaus H.)

1. The automorphisms of the linear congruence groups over Dedekind domains, *J. Number Theory*, **1** (1969), 211—221.

Оно (Ono T.)

1. Arithmetic of Orthogonal Groups, *J. Math. Soc. Japan*, **7** (1955), 79—91.
2. Arithmetic of Orthogonal Groups (II), *Nagoya Math. J.*, **9** (1955), 129—146.

Охара (Ohara A.)

1. La structure du groupe des similitudes directes $GO_6^+(Q)$ sur un corps de caractéristique 2, *Osaka Math. J.*, **10** (1958), 239—257.

Пиккерт (Pickert G.)

1. Elementare Behandlung des Helmholtzschen Raumproblems, *Math. Ann.*, **120** (1948), 492—501.

Платонов В. П., Янчевский В. И.

1*. Структура унитарных групп и коммутант простой алгебры над глобальными полями, *ДАН СССР*, **208**, 3 (1973), 541—544.

Полл (Pall G.)

1. Hermitian quadratic forms in a quasi-field, *Bull. Amer. Math. Soc.*, **51** (1945), 889—893.

Поллак (Pollak B.)

1. The equation $\bar{t}at=b$ in a quaternion algebra, *Duke Math. J.*, **27** (1960), 261—272.
2. The equation $\bar{t}at=b$ in a composition algebra, *Duke Math. J.*, **29** (1962), 225—230.
3. On the structure of local orthogonal groups, *Amer. J. Math.*, **88** (1966), 763—780.
4. Generation of local integral orthogonal groups in characteristic 2, *Canad. J. Math.*, **20** (1968), 1178—1191.

Райнер (Reiner I.)

1. Automorphisms of the symplectic modular group, *Trans. Amer. Soc.*, **80** (1955), 35—50.
2. A new type of automorphism of the general linear group over a ring, *Ann. of Math.*, **66** (1957), 461—466.

Раманатан (Ramanathan K. G.)

1. Quadratic forms over involutorial division algebras, *J. Indian Math. Soc.*, **20** (1956), 227—257.
2. A note on symplectic complements, *J. Indian Math. Soc.*, **18** (1954), 115—125.

Ридж (Rege N. S.)

1. On certain classical groups over Hasse domains, *Math. Z.*, **102** (1967), 120—157.

Риккарт (Rickart C. E.)
1. Isomorphic groups of linear transformations, *Amer. J. Math.*, **72** (1950), 451—464.
2. Isomorphic groups of linear transformations, II, *Amer. J. Math.*, **73** (1951), 697—716.
3. Isomorphisms of infinite-dimensional analogues of the classical groups, *Bull. Amer. Math. Soc.*, **57** (1951), 435—448.

Рим (Riehm C. R.)
1. Integral representations of quadratic forms in characteristic 2, *Amer. J. Math.*, **87** (1965), 32—64.
2. The structure of the symplectic group over a discrete valuation ring, *Amer. J. Math.*, **88** (1966), 106—128.
3. Orthogonal groups over the integers of a local field, I. *Amer. J. Math.*, 88 (1966), 553—561.
4. Orthogonal groups over the integers of a local field, II, *Amer. J. Math.*, **89** (1967), 549—577.

Са (Sah C.-H.)
1. Quadratic forms over fields of characteristic 2, *Amer. J. Math.*, **82** (1960), 812—830.

Сатаке (Satake I.)
1. Some remarks to the preceding paper of Tsukamoto, *J. Math. Soc. Japan*, **13** (1961), 401—409.

Сегье (de Séguier J. A.)
1. Sur les groupes à invariant bilinéaire ou quadratique dans un champ de Galois, *J. de Math.* (7), **2** (1916), 281—366.
2. Les substitutions d'ordre 2 des groupes linéaire, hermitien, gauche et quadratique dans un champ de Galois, I, *Ann. Écol. Norm. Sup.*, **50** (1933), 217—243 II, **51** (1934), 79—140.

Сейп-Хорникс (Seip-Hornix E. A. M.)
1. Clifford algebras of quadratic quaternion forms, *Koninkl. Ned. Akad. Wetenschap. Proc.*, Ser. A, **68** (1965), 326—363.

Сёда (Shoda K.)
1. Einige Sätze über Matrizen, *Jap. J. Math.*, **13** (1937), 361—365.
2. Über den Kommutator der Matrizen, *J. Math. Soc. Japan*, 3 (1951), 78—81.

Спрингер (Springer T.)
1. Over symplectische Transformaties, Diss. Univ. Leiden, 1951.
2. Sur les formes quadratiques d'indice zéro, *C. r. Acad. Sci.* (Paris), **234** (1952), 1517—1519.
3. On the equivalence of quadratic forms, *Konink. Ned. Akad. Wetenschap Proc.*, Ser. A, **62** (1969), 241—253.
4. Quadratic forms over fields with a discrete valuation, *Konink. Ned. Akad. Wetenschap. Proc.*, Ser. A, **58** (1955), 352—362.

Спрингер, Ван-дер-Блей (Springer T., van der Blij R.)
1. Octaves and Triality, New Arch. voor Wisk (3) (1960), 158—169.

Станек (Stanek P.)

1. Concerning a theorem of L. K. Hua and I. Reiner, *Proc. Amer. Math. Soc.*, **14** (1963), 751—753.

Стейнберг (Steinberg R.)

1. Automorphisms of finite linear groups, *Canad. J. Math.*, **10** (1960), 606—615.

Сю (Xu C.-H.)

1. On the automorphisms of orthogonal groups over perfect fields of characteristic 2, *Chinese Math.*, **8** (1966), 475—523.

Тамагава (Tamagawa T.)

1. On the structure of orthogonal groups, *Amer. J. Math.*, **80** (1958), 191—197.

Титс (Tits J.)

1. Généralisations des groupes projectifs, *Acad. Roy. Belgique Bull. Cl. Sci.*, **35** (1949), 197—208, 224—233, 568—589, 756—773.
2. Généralisations des groupes projectifs besées sur leurs propriétés de transitivité, *Acad. roy. Belgique, Mém. Cl. Sci.*, **27** (1952), fasc. 2.
3. Le plan projectif des octaves et les groupes de Lie exceptionnels, *Acad. roy. Belgique, Bull. Cl. Sci.*, **39** (1953), 309—329.
4. Les groupes simples de Suzuki et Ree, Sem. Bourbaki, 13-e année, exposé 210 (1960—1961).
5. Formes quadratiques, groupes orthogonaux et algèbres de Clifford, *Invent. Math.*, **5** (1968), 19—41.

Томсон (Thompson R. C.)

1. Commutators in the special and general linear groups, *Trans. Amer. Math. Soc.*, **101** (1961), 16—33.
2. Commutators of matrices with coefficients from the field of two elements, *Duke J. Math.*, **29** (1962), 367—374.
3. Commutators of matrices with coefficients from the field of three elements, *Port. Math.* (1963).

Тояма (Toyama H.)

1. On commutators of matrices, Kodai Math. Sem. Rep., n°5—6 (1949).

Уолл (Wal G. E.)

1. The structure of a unitary factor group, Publ. math. Inst Hautes Etudes Scient., n° 1 (1959).

Уолтер (Walter J. H.)

1. Isomorphisms between projective unitary groups, *Amer. J. Math.*, **77** (1955), 805—844.

Фрейденталь (Freudenthal H.)

1. Oktaven, Ausnahmegruppen und Oktavengeometrie, Utrecht 1951. [Русский перевод: Фрейденталь Г., Октавы, особые группы и октавная геометрия, в сб. «*Математика*», **1 : 1** (1957), 117—153.

2. Sur le groupe exceptionnel E_7, *Indag. Math.*, **15** (1953), 81—89.
3. Sur le groupe exceptionnel E_8, *Indag. Math.*, **15** (1953), 95—98.

Хаантьес (Haantjes J.)

1. Halblineare Transfermationen, *Math. Ann.*, **114** (1937), 293—304.

Хассе (Hasse H.)

1. Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, *J. reine angew. Math.*, **153** (1924), 113—130.
2. Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper, *J. reine angew. Math.*, **154** (1924), 158—162.

Хаттори (Hattori A.)

1. On the multiplicative group of simple algebras and orthogonal groups of three dimensions, *J. Math. Soc. Japan*, **4** (1952), 205—217.

Ходж, Пидо (Hodge W. V. D., Pedoe D.)

1*. Methods of algebraic geometry, vol. I. Cambridge, 1947. [Русский перевод: Ходж В., Пидо Д., Методы алгебраической геометрии, т. I, ИЛ, М., 1954.]

Хуа (Hua L.-K.)

1. Geometries of Matrices: I, Generalizations of von Staudt's theorem, *Trans. Amer. Math. Soc.*, **57** (1945), 441—481.
2. Geometries of Matrices: I_1, Arithmetical constructions, *Trans. Amer. Math. Soc.*, **57** (1945), 482—580.
3. On the extended space of several complex variables (1): The space of complex spheres, *Quart. J. Math.*, **17** (1946), 214—222.
4. Geometries of Matrices: III, Fundamental theorem in the geometry of symmetric matrices, *Trans. Amer. Math. Soc.*, **61** (1947), 229—255.
5. On the automorphisms of the symplectic group over any field, *Ann. of Math.*, **49** (1948), 739—759.
6. Geometry of symmetric matrices over any field with characteristic other than two, *Ann. of Math.*, **50** (1949), 8—31.
7. On the automorphisms of a field, *Proc. Nat. Acad. Sci. USA*, **35** (1949), 386—389.
8. Some properties to a field, *Proc. Nat. Acad. Sci. USA*, **35** (1949), 533—537.
9. Supplement to the paper of Dieudonné on the automorphisms of classical groups, *Mem. Amer. Math. Soc.*, № 2 (1951), 96—122.
10. A generalization of Hamiltonian matrices, *Acta Sci. Sinica* 2, № 1 (1953), 1—58.

Хуа, Вань (Hua L.-K., Wan C.-H.)

1. On the automorphisms and isomorphisms of linear groups, *J. Chinese Math. Soc.*, **2** (1953), 1—32.

Хуа, Райнер (Hua L.-K., Reiner I.)

1. On the generators of the symplectic modular group, *Trans. Amer. Math. Soc.*, **65** (1949), 415—426.

2. Automorphisms of the unimodular group, *Trans. Amer. Math. Soc.*, **71** (1951), 331—348.
3. Automorphisms of the projective unimodular group, *Trans. Amer. Math. Soc.*, 72 (1952), 467—473.

Цассенхауз (Zassenhaus H.)

1. Characterization of unipotent matrices, *J. Number Theory*, **1** (1969), 222—230.

Цукамото (Tsukamoto T.)

1. On the local theory of quaternionic anti-hermitian forms, *J. Math. Soc. Japan*, **13** (1961), 387—400.

Чоу (Chow W. L.)

1. On the geometry of algebraic homogeneous spaces, *Ann. of Math.*, **50** (1949), 32—67.

Швердтфегер (Schwerdtfeger H.)

1. Skew-symmetric matrices and projective geometry, *Amer. Math. Monthly*, **51** (1944), 137—148.
2. Symplectic groups and null systems, Courant anniversary volume, 1948, 371—382.

Шевалле (Chevalley C.)

1. The algebraic theory of spinors, New York, Columbia Univ. Press, 1954.
2. Théorie des groupes de Lie, t. II, Groupes algébriques, Actual. Scient. et Ind., № 1152, Paris: Hermann 1951. [Русский перевод: Шевалле К., Теория группы Ли, т. II, Алгебраические группы, ИЛ, М., 1958.]
3. Sur le groupe exceptionnel (E_6), *C. r. Acad. Sci.*, (Paris), **232** (1951), 1991—1993.
4. Sur une variété algébrique liée l'étude du groupe (E_6), *C. r. Acad. Sci.* (Paris), **232** (1951), 2168—2170.
5. Sur certains groupes simples, Tôhoku Math. J., (2), **7** (1955), 14—66. [Русский перевод: Шевалле К., О некоторых простых группах, в сб. «*Математика*», **2** : 1 (1958), 3—53.]
6. Classification des groupes de Lie algébriques, 2 vol., Séminaire 1956—1958, Paris: Secr. math., 11, R. P. Curie, 1958.

Шерк (Scherk P.)

1. On the decomposition of orthogonalities into symmetries, *Proc. Amer. Math. Soc.*, **1** (1950), 481—491.
2. On regular bilinear forms, Ann. di Mat. (4), **47** (1959), 391—400.
3. Similarities over fields of characteristic two, *Trans. Roy. Soc. Canada*, **53** (1959), 15—20.

Шимура (Shimura G.)

1* Arithmetic of unitary groups. *Ann. of Math.*, **79** (1964), 369—409.

Шмидт (Schmidt A.)

1. Über die Bewegungsgruppe der ebenen elliptischen Geometrie, *J. reine angew. Math.*, **186** (1949), 230—240.

Шпигель (Spiegel E.)

1. On the automorphisms of the unitary group over a field of characteristic 2, *Amer. J. Math.*, **89** (1967), 43—50.
2. On the automorphisms of the projective unitary group over a field of characteristic 2, *Amer. Math.*, **89** (1967), 51—55.

Шрейер, Ван-дер-Варден (Schreier O., van der Waerden B. L.)

1. Die Automorphismen der projektiven Gruppen, *Abh. Math. Sem. Hamburg Univ.*, **6** (1928), 303—322.

Эдж (Edge W. L.)

1. Geometry in three dimensions over GF (3), *Proc. Roy. Soc. A* (London), **222** (1953), 262—286.
2. The geometry of the linear fractional group LF (4, 2), *Proc. Lond. Math. Soc.* (3), **4** (1954), 317—342.
3. The projective orthogonal and linear fractional representations of the simple group of order 360, Proc. Internat. Math. Congress, Amsterdam, Sept. 1954, vol. II.

Эйхлер (Eichler M.)

1. Idealtheorie der quadratischen Formen, *Abh. Math. Sem. Hamburg Univ.*, **18** (1952), 14—37.
2. Quadratische Formen und Orthogonale Gruppen: Berlin, J. Springer, 1952.

Эрлих (Ehrlich G.)

1. The structure of continuous rings, Diss. Univ. of Tennessee, Knoxville, 1953.

Якобинский (Jacobinski H.)

1. Über die Automorphismen einer quadratischen Form, *Kungl. Fysiogr. Sällsk. Förh.*, **19**, № 8 (1949).

Якобовиц (Jacobowitz R.)

1. Hermitian forms over local fields, *Amer. J. Math.*, **84** (1962), 441—465.

СПИСОК ОБОЗНАЧЕНИЙ

А) Обозначения, использующиеся во всей книге:

ξ^σ ($\xi \in K$, σ — автоморфизм тела K или его изоморфизм на тело K'), A^σ (матрица (α_{ij}^σ), если $A = (\alpha_{ij})$).

K° (тело, противоположное телу K), J (изоморфизм тела K на тело K°), ξ^J ($\xi \in K$), A^J (матрица (α_{ij}^J), если $A = (\alpha_{ij})$).

$\xi^{\sigma\tau} = (\xi^\sigma)^\tau$, $\xi^{\sigma J} = (\xi^\sigma)^J$, $\xi^{J\sigma} = (\xi^J)^\sigma$.

$\langle x', x\rangle = x'(x)$ (x — элемент векторного пространства E, x' — элемент дуального пространства E^*).

${}^t u$, $\check{u} = {}^t u^{-1}$ (u — полулинейное отображение) гл. I, § 6.

${}^t A$ (матрица (α_{ji}), транспонированная по отношению к матрице $A = (\alpha_{ij})$).

$f(x, y)$, f (полуторалинейная форма) гл. I, § 5.

V^0 (ортогональное дополнение к подпространству V) гл. I, § 7.

ν (индекс формы f, в гл. I и II) гл. I, § 7.

$M(f)$ (группа множителей формы f) гл. I, § 9.

$\Gamma L_n(K)$, $GL_n(K)$, H_n, Z_n гл. I, § 1.

h_α (гомотетия с коэффициентом α) гл. I, § 1.

$\bar{u}$ (u — коллинеация) гл. I, § 1.

$P(E)$, $P_{n-1}(K)$ гл. I, § 1.

$P\Gamma L_n(K)$, $PGL_n(K)$ гл. 1, § 1.

$SL_n(K)$, $PSL_n(K)$ гл. II, § 1.

$\Gamma U_n(K, f)$, $GU_n(K, f)$, $U_n(K, f)$, $U_n(K, A)$, $U_n(K)$ гл. I, § 9.

$GU_n^+(K, f)$ гл. II, § 13.

$U_n^+(K, f)$ гл. II, § 5.

$T_n(K, f)$, W_n гл. II, § 4.

$P\Gamma U_n(K, f)$, $PGU_n(K, f)$, $PU_n(K, f)$ гл. I, § 9.

$PU_n^+(K, f)$ гл. II, § 5.

$\Gamma Sp_n(K)$, $GSp_n(K)$, $Sp_n(K)$ гл. I, § 9.

$P\Gamma Sp_n(K)$, $PGSp_n(K)$, $PSp_n(K)$ гл. I, § 9.

$\Gamma O_n(K, f)$, $GO_n(K, f)$, $O_n(K, f)$ гл. I, § 9.

$O_n^+(K, f)$, $\Omega_n(K, f)$ гл. II, § 6.

$O_n'(K, f)$ гл. II, § 7.

$P\Gamma O_n(K, f)$, $PGO_n(K, f)$, $PO_n(K, f)$ гл. I, § 9.

$PO_n^+(K, f)$, $P\Omega_n(K, f)$ гл. II, § 6.

$Q(x)$, Q (квадратичная форма над полем характеристики 2) гл. I, § 16.

$\Gamma O_n(K, Q)$, $GO_n(K, Q)$, $O_n(K, Q)$ гл. I, § 16.

$P\Gamma O_n(K, Q)$, $PGO_n(K, Q)$, $PO_n(K, Q)$ гл. I, 16.

$O_n^+(K, Q)$, $Q_n'(K, Q)$, $\Omega_n(K, Q)$ гл. II, § 10 и § 11.

$\mathbf{F}_q$ — конечное поле из q элементов.

$\mathbf{Q}$ — поле рациональных чисел.

$\mathbf{R}$ — поле действительных чисел.

B) Специальные обозначения для некоторых разделов книги:

U^+, U^- (собственные подпространства инволюции) гл. I, § 3, 4, 14, 15.

$B_{ij}(\lambda)$ (матрицы сдвигов) гл. II, § 1 и 2.

$C(f)$, $C^+(f)$, $C^-(f)$, e_H, J (инволюция алгебры Клиффорда), s_u, θ (спинорная норма) гл. II, § 7.

$C(Q)$, $C^+(Q)$, s_u, $\wp(\rho)$ гл. II, § 10.

$G_r(E)$, $\bar{u}_r$, ω_r гл. III, § 2.

$N_s(E)$ гл. III, § 3; $N_r^+(E)$, $N_r^-(E)$ гл. III, § 4.

$c(S)$, $\nu(u, v)$, $\nu(u)$ гл. IV, § 1.

УКАЗАТЕЛЬ ТЕРМИНОВ И ОСНОВНЫХ ТЕОРЕМ

(Цифры указывают главу, параграф и страницу)

ОГЛАВЛЕНИЕ

В 1975 г. В ИЗДАТЕЛЬСТВЕ «МИР» ГОТОВИТСЯ К ВЫПУСКУ

БУРБАКИ Н. **Группы и алгебры Ли** (гл. I—III), *пер. с франц., 32 л.*

Книга входит в завоевавшую мировое признание энциклопедию современной математики «Основы математики», созданную группой французских ученых, выступающих под коллективным псевдонимом Н. Бурбаки.

В 1972 г. издательством «Мир» был выпущен перевод гл. IV—VI книги «Группы и алгебры Ли», а сейчас предлагается перевод ее начальных глав (в таком же порядке выходили французские издания). Книга отражает самые современные результаты в этой области. В ней имеется обширный материал по теории алгебр Ли, свободных алгебр Ли и групп Ли.

Книга предназначена для широкого круга математиков различных специальностей — от студентов до научных работников.

Если Вы желаете приобрести эту книгу, оставьте в книжном магазине предварительный заказ. Своевременное оформление заказа гарантирует Вам приобретение нужной книги.