Оглавление

Глава 1. Линейные группы

§1 Основные определения

Пусть $\mathbb{F}$ — некоторое поле и V — векторное пространство над полем $\mathbb{F}$ конечной размерности n.

Определение 1.1.1. Отображение A векторного пространства V в себя называется *линейным преобразованием*, если для любых двух векторов $u, v \in V$ и любых скаляров $\alpha, \beta \in \mathbb{F}$ справедливо равенство $(\alpha u + \beta v)A = \alpha(uA) + \beta(vA)$.

Обозначим множество всех линейных преобразований пространства V через $\mathrm{M}(V)$. Хорошо известно, что множество $\mathrm{M}(V)$ образует кольцо относительно сложения, заданного правилом $u(A+B) = uA + uB$, и умножения, заданного правилом $u(A \cdot B) = (uA)B$ (суперпозиция).

Определение 1.1.2. Подмножество всех обратимых преобразований в $\mathrm{M}(V)$ является группой, обозначается $\mathrm{GL}(V)$ и называется *общей линейной группой*.

Зафиксируем базис $e_1, \ldots, e_n$ пространства V, пусть $[A]$ — матрица преобразования A в данном базисе. Отображение, сопоставляющее каждому преобразованию его коэффициенты в данном базисе, является изоморфизмом кольца $\mathrm{M}(V)$ на кольцо всех квадратных матриц $\mathrm{M}_n(\mathbb{F})$ степени n с коэффициентами из поля $\mathbb{F}$. Его ограничение на группу $\mathrm{GL}(V)$ дает нам изоморфизм группы всех обратимых линейных преобразований на группу всех обратимых квадратных матриц степени n над полем $\mathbb{F}$, обозначаемую $\mathrm{GL}_n(\mathbb{F})$ и также называемую общей линейной группой. С другой стороны, любую квадратную матрицу степени n можно рассматривать как линейное преобразование пространства строк $\mathbb{F}^n$ длины n с коэффициентами из поля $\mathbb{F}$, которое каноническим образом изоморфно пространству V. Потому в дальнейшем мы будем отождествлять элементы из $\mathrm{GL}(V)$ с матрицами из $\mathrm{GL}_n(\mathbb{F})$, предполагая базис $e_1, \ldots, e_n$ пространства V фиксированным и соответствующим каноническому базису строк в пространстве $\mathbb{F}^n$, т. е. вектор e_i соответствует строчке с единицей на месте i и нулями на остальных местах.

Определение 1.1.3. Подгруппа G группы $\mathrm{GL}_n(\mathbb{F})$ называется *линейной группой*, а пространство V, на котором действует группа G называется G-модулем.

Определение 1.1.4. Подпространство W пространства V называется *G-подмодулем* G-модуля V, если $WG = \{wg | w \in W, g \in G\} \subseteq W$.

В дальнейшем, если понятно о какой группе идет речь, мы будем говорить просто о модулях и подмодулях.

Определение 1.1.5. Для любой группы G всегда существуют два подмодуля, а именно V и $\{0\}$. Эти подмодули называются *тривиальными*. Все остальные подмодули называются *нетривиальными*. Если группа G не имеет нетривиальных подмодулей, то она называется *неприводимой*, а модуль V называется *неприводимым G-модулем*. В противном случае группа называется *приводимой* и модуль V называется *приводимым*.

***Упражнение* 1.1.6.** Пусть $G \leq \mathrm{GL}(V)$ и v — произвольный вектор из V. Всегда ли линейная оболочка множества $vG = \{vg | g \in G\}$ является G-модулем? неприводимым G-модулем?

Определение 1.1.7. Подмодуль U модуля V называется *дополнением* подмодуля W, если $V = U \oplus W$ является прямой суммой подмодулей U и W. Если для модуля W существует дополнение, то он называется *дополнимым*. Группа G называется *вполне приводимой*, если каждый G-подмодуль дополним.

Определение 1.1.8. Если R — некоторое кольцо, которое одновременно является векторным пространством над полем $\mathbb{F}$ и при этом для любого $\alpha \in \mathbb{F}$ и для любых $a, b \in R$ справедливо

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

то R называется $\mathbb{F}$-алгеброй.

Очевидно, что $\mathrm{M}_n(\mathbb{F})$ является $\mathbb{F}$-алгеброй размерности n^2. Если у нас есть подгруппа G группы $\mathrm{GL}_n(\mathbb{F})$, можно рассмотреть подалгебру, порождённую группой G, а именно $\mathcal{L}_{\mathbb{F}}(G) = \mathcal{L}(G)$ — множество $\mathbb{F}$-линейных комбинаций элементов из G. Как и для группы G, для алгебры $\mathcal{L}(G)$ можно определить неприводимый, приводимый и вполне приводимый модули. Соответственно, алгебра $\mathcal{L}(G)$ называется неприводимой, приводимой и вполне приводимой, если модуль, на котором она действует является неприводимым, приводимым или вполне приводимым.

Лемма 1.1.9. *G-модуль V является неприводимым (соотв. приводимым, вполне приводимым) в том и только в том случае, когда V является неприводимым (соотв. приводимым, вполне приводимым) $\langle G\rangle$-модулем.*

Доказательство. Поскольку $G \subseteq \mathcal{L}(G)$, достаточность очевидна. С другой стороны, если W — произвольный G-подмодуль, то очевидно, что он инвариантен относительно любой $\mathbb{F}$-линейной комбинации элементов из G. Действительно,

$$W(\alpha_1 g_1 + \ldots + \alpha_k g_k) = W(\alpha_1 g_1) + \ldots + W(\alpha_k g_k) \subseteq W + \ldots + W = W.$$

Следовательно, W является также и $\mathcal{L}(G)$-подмодулем. □

***Пример* 1.1.10.** Рассмотрим симметрическую группу степени n — Sym_n. Пусть V — n-мерное векторное пространство над полем $\mathbb{F}$ и $e_1, \ldots, e_n$ — некоторый базис пространства V. Если σ — произвольная подстановка из Sym_n, то мы можем задать действие σ на базисе $e_1, \ldots, e_n$ правилом $e_i\sigma = e_{i\sigma}$ и продолжить его линейно на все пространство. Таким образом, мы получаем линейное действие группы Sym_n на пространстве V. В данном базисе в матрице элемента σ в i-ой строке стоит 1 на месте $(i, i\sigma)$ и нули на остальных местах. Такие матрицы в дальнейшем мы будем называть *подстановочными матрицами*. Поскольку любая конечная группа изоморфна некоторой подгруппе группы подстановок, данное вложение показывает, что любая конечная группа может быть изоморфно вложена в общую линейную группу подходящей степени над произвольным полем $\mathbb{F}$.

***Упражнение* 1.1.11.** Найти все неприводимые подмодули группы Sym_n из примера 1.1.10 (рассмотреть поля как нулевой, так и положительной характеристики). Всегда ли группа Sym_n будет вполне приводимой?

***Пример* 1.1.12.** Пусть теперь S — группа подстановочных матриц из предыдущего примера и H — подгруппа всех диагональных матриц в $\mathrm{GL}_n(\mathbb{F})$. Тогда S нормализует H и мы можем рассмотреть группу $M = H \leftthreetimes S$. Подгруппа M называется *мономиальной подгруппой* группы $\mathrm{GL}_n(\mathbb{F})$ и состоит из матриц, у которых в каждой строке и в каждом столбце находится ровно один ненулевой элемент.

Определение 1.1.13. Пусть G — группа. Гомоморфизм из группы G в линейную группу $\mathrm{GL}_n(\mathbb{F})$ называется *представлением* группы G над полем $\mathbb{F}$. Представление называется *точным*, если ядро гомоморфизма тривиально. В этом случае модуль $\mathbb{F}^n = V$ называется *точным*.

Определение 1.1.14. Пусть R — кольцо и $\mathbb{F}$ — его подполе, лежащее в центре кольца R. Тогда R можно рассмотреть как векторное пространство над полем $\mathbb{F}$ и через $[R : \mathbb{F}]$ мы будем обозначать размерность этого векторного пространства.

Определение 1.1.15. Пусть G — конечная группа, R — кольцо. Тогда мы можем построить кольцо RG, состоящая из сумм вида

$$\sum_{g \in G} r_g g,$$

где $r_g \in R$. Кольцо RG называется *групповым кольцом*. Если R — поле, то кольцо RG становится *групповой алгеброй* над полем R.

Определение 1.1.16. Пусть V^* — множество линейных отображений $V \to \mathbb{F}$. Тогда V^* называется *дуальным пространством* пространства V. Если $e_1, \ldots, e_n$ — базис пространства V, то определим e_i^* по правилу

$$e_j \cdot e_i^* = \begin{cases} 1 \text{ если } i = j, \\ 0 \text{ если } i \neq j. \end{cases}$$

Функции e_i^* образуют базис пространства V^*, называемый *дуальным базисом*. В частности $V \simeq V^*$.

***Упражнение* 1.1.17.** Пусть G — абелева подгруппа группы $\mathrm{GL}_n(\mathbb{F})$ и поле $\mathbb{F}$ алгебраически замкнуто. Доказать, что существует G-инвариантное подпространство размерности 1, в частности, абелева группа неприводима в том и только в том случае, когда $n = 1$.

§2 Теоремы Шура и Машке

Теорема 1.2.1. (Лемма Шура) *Если A — некоторая $\mathbb{F}$-алгебра и V — неприводимый A-модуль, то централизатор алгебры A в $\mathrm{M}(V)$ $(C_{\mathrm{M}(V)}(A))$ — тело. Здесь*

$$C_{\mathrm{M}(V)}(A) = \{x \in \mathrm{M}(V) |\ \textit{для всех } a \in A,\ \textit{справедливо } xa = ax\}.$$

Доказательство. Пусть $x \in C_{\mathrm{M}(V)}(A)$ и рассмотрим подпространство $W = \{v \in V | vx = 0\}$ пространства V. Имеем $0 = w(xa) = w(ax) = (wa)x$ для любого $w \in W$ и любого $a \in A$. Следовательно, W является A-подмодулем. Поскольку алгебра A неприводима, отсюда следует, что либо $W = \{0\}$, либо $W = V$. В первом случае x обратим, во втором $x = 0$. □

Лемма 1.2.2. *Если $\mathbb{F}$ — алгебраически замкнутое поле и G — неприводимая линейная группа, то*

$$C_{\mathrm{GL}(V)}(G) = Z(\mathrm{GL}(V)) = \mathbb{F}^* E.$$

Доказательство. Пусть $x \in C_{\mathrm{GL}(V)}(G)$. Так как поле $\mathbb{F}$ алгебраически замкнуто, существует собственный вектор v с собственным значением α для x. Рассмотрим подпространство $V_\alpha = \{v \in V | vx = \alpha v\}$ пространства V. Тогда для любого $g \in G$ и любого $x \in V_\alpha$ справедливо $\alpha v g = v(xg) = v(gx) = (vg)x$, т. е. V_α является G-подмодулем. Так как группа G неприводима и $V_\alpha \neq \{0\}$, получаем $V_\alpha = V$, т. е. x — скалярная матрица. □

***Упражнение* 1.2.3.** Верно ли утверждение леммы 1.2.2 если поле $\mathbb{F}$ не является алгебраически замкнутым?

Теорема 1.2.4. (Теорема Машке) *Если $G \leq \mathrm{GL}_n(\mathbb{F})$ — конечная группа и $(|G|, \mathrm{char}(\mathbb{F})) = 1$ или $\mathrm{char}(\mathbb{F}) = 0$, то группа G вполне приводима.*

Доказательство. Пусть W — некоторый G-подмодуль в V и U_0 — некоторое подпространство пространства V такое, что $V = W \oplus U_0$. Пусть φ — проекция на подпространство W параллельно U_0, т. е. если $v = w + u_0$ — единственное разложение вектора v в виде суммы векторов из W и U_0, то $v\varphi = w$. Ясно, что φ — линейное преобразование. Определим преобразование $\vartheta : V \to W$ следующим образом:

$$v\vartheta = \frac{1}{|G|} \sum_{g \in G} ((vg)\varphi) g^{-1}.$$

Очевидно, что ϑ также является линейным преобразованием. Теперь для любого $h \in G$ имеем

$$(vh)\vartheta = \frac{1}{|G|} \sum_{g \in G} ((vhg)\varphi) g^{-1} = \frac{1}{|G|} \sum_{g \in G} ((vhg)\varphi)(hg)^{-1} h = (v\vartheta)h.$$

Если $w \in W$, то для любого $g \in G$ имеем $wg \in W$, следовательно, $(wg)\varphi = wg$ и $w\vartheta = w$. Поскольку для любого $v \in V$ и любого $h \in G$ справедливо $(vh)\vartheta = (v\vartheta)h$, то $U = \mathrm{Ker}(\vartheta)$ (ядро преобразования θ) — это G-подмодуль модуля V. Имеем также $v\vartheta \in W$, значит, $(v\vartheta)\vartheta = v\vartheta$ и $(v - v\vartheta)\vartheta = v\vartheta - v\vartheta = 0$. Таким образом, $v = v\vartheta + (v - v\vartheta) \in W + U$ и $V = W + U$. Очевидно, что $U \cap W = \{0\}$, потому $V = U \oplus W$, т. е. G-подмодуль W дополним. □

***Упражнение* 1.2.5.** Пусть G — конечная группа. Всегда ли для неё существует точное неприводимое представление $G \to \mathrm{GL}(V)$, где V — векторное пространство над полем $\mathbb{C}$

Теорема 1.2.6. *Если G — линейная группа с модулем V, то модуль V вполне приводим тогда и только тогда, когда V порождён своими неприводимыми подмодулями.*

Доказательство. Пусть $V = \sum_\alpha V_\alpha$, где V_α — неприводимые G-подмодули. Рассмотрим подмодуль W модуля V. Размерность модуля V конечна, следовательно, существует такой максимальный подмодуль U, что $W \cap U = \{0\}$. Если $W + U \neq V$, следовательно, существует $V_\alpha \not\leq W + U$. Поскольку подмодуль V_α неприводим, то $(W + U) \cap V_\alpha = \{0\}$. Тогда $W \cap (U + V_\alpha) = \{0\}$, что противоречит максимальности U. Значит, $U + W = V$.

Обратно, пусть модуль V вполне приводим и S — сумма всех его неприводимых подмодулей. В силу полной приводимости модуля V, имеем $V = S \oplus T$. Если $T \neq \{0\}$, то T содержит неприводимый подмодуль, т. е. $S \cap T \neq \{0\}$. □

Лемма 1.2.7. *Пусть G — линейная группа с модулем V и $V = \sum_\alpha V_\alpha$, где все подмодули V_α неприводимы. Тогда V является прямой суммой некоторых из V_α.*

Доказательство. Пусть S — подмодуль модуля V максимальной размерности, являющийся прямой суммой некоторых из V_α. Если $S \neq V$, то существует V_β такой, что $V_\beta \nleq S$. Тогда $V_\beta \cap S$ является подмодулем и $V_\beta \cap S = \{0\}$ ввиду неприводимости V_β. Следовательно, $S_1 = S \oplus V_\beta$ — это подмодуль модуля V, являющийся прямой суммой некоторых из V_α и $\dim S_1 > \dim S$. Последнее неравенство противоречит тому, что мы выбрали S максимальной размерности, следовательно, $S = V$. □

§3 Примитивность, теорема Клиффорда

Определение 1.3.1. Рассмотрим линейную группу G, действующую на V. Если существуют подпространства $W_1, \ldots, W_k$ $(k > 1)$ пространства V такие, что $V = \oplus_{i=1}^k W_i$ и для любого $g \in G$, для любого $i \in \{1, \ldots, k\}$ существует такое $j \in \{1, \ldots, k\}$, что $W_i g = W_j$, то группа G называется *импримитивной* и $W_1, \ldots, W_k$ называется *системой импримитивности.* Если таких подпространств не существует, то модуль V и группа G называются *примитивными.*

Если линейная группа G импримитивна и $W_1, \ldots, W_k$ — некоторая система импримитивности, можно рассмотреть подгруппы $H_i = St_G(W_i) = \{x \in G | W_i x = W_i\}$, называемые *стабилизаторами* подпространств W_i. Ясно, что $H_i|_{W_i} = G_i \leq \mathrm{GL}(W_i) = \mathrm{GL}_{n/k}(\mathbb{F})$. Если группа G неприводима, значит, G действует транзитивно на множестве $W_1, \ldots, W_k$, следовательно, существуют элементы $g_1 = e, g_2, \ldots, g_k$ такие, что $W_1 g_i = W_i$. Очевидно, что $\{g_1, \ldots, g_k\}$ — трансверсаль (представители смежных классов) подгруппы H_1 в G.

Лемма 1.3.2. *Если G — линейная неприводимая импримитивная группа с системой импримитивности $W_1, \ldots, W_k$, то группы G_i, определённые выше, неприводимы для всех i.*

Доказательство. Пусть R_1 — некоторый G_1-подмодуль в W_1. Рассмотрим $R = R_1 g_1 + \ldots + R_k g_k$. Очевидно, что R является G-подмодулем модуля V. Но группа G неприводима, значит, $R = \{0\}$ или $R = V$. В первом случае $R_1 = \{0\}$, во втором случае $R_1 = W_1$. □

Предположим, что группа G неприводима и импримитивна. Если G_1 также импримитивна и $W_{1,1}, \ldots, W_{1,m}$ — её система импримитивности, значит, $W_{1,1}, \ldots, W_{k,m}$ — система импримитивности группы G. Здесь $W_{i,j} = W_{1,j} g_i$. Действительно, пусть $g \in G$. Тогда $W_{i,j} g = W_{1,j} g_i g = W_{1,j} h g_l$ для некоторого $h \in H_1$ и $l \in \{1, \ldots, k\}$. Следовательно, $W_{i,j} g = W_{1,t} g_l = W_{l,t}$. Таким образом, мы доказали следующую лемму.

Лемма 1.3.3. *Пусть G — линейная неприводимая группа. Тогда существует такая (минимальная) система импримитивности, что все группы G_i, определённые выше, примитивны.*

Теорема 1.3.4. (Теорема Клиффорда) *Пусть $H \trianglelefteq G$ и G — неприводимая линейная группа с модулем V. Рассмотрим неприводимый H-подмодуль W. Тогда справедливы следующие утверждения:*

(а) *$V = \oplus_{i=1}^k W_i$, где W_i — неприводимые H-подмодули (в частности, H вполне приводима).*

(б) *Каждый из W_i имеет вид $W_i = W g_i$ для некоторого $g_i \in G$.*

(в) *Рассмотрим V как H-модуль. Если $V_j, j = 1, \ldots, m, m \leqslant k$ — подмодули, порождённые изоморфными H-подмодулями, то $\{V_j\}$ — система импримитивности группы G*

Доказательство. (а), (б) Очевидно, что $\sum_{g \in G} Wg$ является ненулевым G-подмодулем, следовательно, $V = \sum_{g \in G} Wg$. Кроме того, для любого g, модуль Wg является неприводимым H-подмодулем. В силу следствия 1.2.7, V является прямой суммой некоторых из Wg.

(в) Рассмотрим $V_1 = W_1 \oplus \ldots \oplus W_l$, где V_1 — H-модуль, порождённый всеми H-подмодулями, изоморфными W_1 (изоморфными как H-модули). Если $R \leq V$ и $R \simeq W_1$ (как H-модуль), то $R \leq V_1$ по построению. Заметим, что если $R_1 \simeq R_2$ и $g \in G$, то $R_1 g \simeq R_2 g$. Действительно, по условию существует изоморфизм $\varphi : R_1 \to R_2$ такой, что $r_1^\varphi = r_2$ и $(r_1 h)^\varphi = r_2 h$ для любых $r_1 \in R_1$, $h \in H$ и подходящего $r_2 \in R_2$. Определим $\varphi_g : R_1 g \to R_2 g$ правилом $(r_1 g)^{\varphi_g} = r_2 g$. Имеем

$$((r_1 g)h)^{\varphi_g} = ((r_1 h^g)g)^{\varphi_g} = (r_2 h^g)g = (r_2 g)h.$$

Далее рассмотрим $V_1 g$, где $g \in G$. В силу доказанного выше и поскольку $W_1 \leq V_1$, следовательно, $W_1 g \leq V_1 g$. Таким образом, если для некоторого $1 \leqslant f \leqslant m$, H-модуль V_f содержит $W_1 g$, то $V_1 g \leq V_f$. В силу симметрии $V_f g^{-1} \leq V_1$, следовательно, $V_1 g = V_f$. □

***Упражнение* 1.3.5.** Доказать, что мономиальная подгруппа группы $\mathrm{GL}_n(\mathbb{C})$, построенная в примере 1.1.11, является неприводимой, но не является примитивной и найти систему импримитивности этой подгруппы.

§4 Вспомогательные результаты из теории колец

Ввиду леммы 1.1.9 существует тесная связь между линейными группами и алгебрами, порождёнными этими группами. В данном разделе мы приведем классические результаты из теории колец, которые будем неоднократно использовать в дальнейшем. Более подробное изложение результатов данного параграфа можно найти в [7, §§23–26]. Везде в данном параграфе мы считаем, что R — некоторое подкольцо в $\mathrm{M}_n(\mathbb{F})$ для некоторого поля $\mathbb{F}$, т. е. R является конечномерной $\mathbb{F}$-алгеброй, и $\mathbb{F}^n$ — некоторый R-модуль.

Определение 1.4.1. Элемент x алгебры R называется *нильпотентным*, если $x^n = 0$ для некоторого натурального n. Идеал J алгебры R называется *нильпотентным*, если $J^n = 0$ для некоторого n (т. е. произведение любых n элементов идеала J равно 0). Элемент $a \neq 0$ алгебры R называется *идемпотентом*, если $a^2 = a$.

Определение 1.4.2. Будем говорить, что алгебра R удовлетворяет *условию минимальности* или *условию обрыва убывающих цепей*, если любая убывающая цепь правых идеалов $I_1 \geq I_2 \geq \ldots$ на некотором шаге стабилизируется.

Теорема 1.4.3. [7, Теорема (24.2)] *В алгебре R с условием минимальности каждый ненильпотентный правый идеал I содержит идемпотент.*

Доказательство. Множество ненильпотентных правых идеалов кольца R, содержащихся в идеале I непусто (оно содержит I), следовательно, существует минимальный ненильпотентный правый идеал I_1, содержащийся в I. Тогда $I_1^2 \subseteq I_1$ и, так как I_1 ненильпотентный и минимальный правый идеал, $I_1^2 = I_1$.

Рассмотрим множество M всех правых идеалов L кольца R, для которых справедливо

$$(1) LI_1 \neq \{0\},$$

$$(2) L \subseteq I_1.$$

Поскольку множество M непусто ($I_1 \in M$), мы можем выбрать минимальный элемент $L_1 \in M$. Поскольку $L_1 I_1 \neq \{0\}$, то найдется такой элемент $x \in L_1$, что $xI_1 \neq \{0\}$. Поскольку идеал L_1 минимален и xI_1 — правый идеал кольца R, то $xI_1 = L_1$. Следовательно, существует такой элемент $a \in I_1$, что $x = xa = xa^2 = \ldots$. Таким образом, I_1 содержит ненильпотентный элемент a и $x(a^2 - a) = 0$. Пусть

$$N = \{u \in I_1 | xu = 0\} \subseteq I_1.$$

Так как $xI_1 = L_1 \neq \{0\}$, то $N \neq I_1$ и, следовательно, N — нильпотентный идеал кольца R. Положим теперь $n_1 = a^2 - a \in N$. Если $n_1 = 0$, то теорема доказана. Пусть $n_1 \neq 0$ и $a_1 = a + n_1 - 2an_1 \in I_1$. Элементы a_1, a, n_1 коммутируют друг с другом, поэтому если a_1 нильпотентен, то нильпотентен также элемент $a = a_1 - n_1 + 2an_1$, что невозможно. Следовательно, элемент $a_1 \in I_1$ ненильпотентен. Непосредственными вычислениями проверяется, что

$$n_2 = a_1^2 - a_1 = 4n_1^3 - 3n_1^2 = n_1^2(4n_1 - 3).$$

Элемент n_2 нильпотентен, коммутирует с a_1 и содержит элемент n_1^2 в качестве множителя. Повторяя указанную выше процедуру, мы получаем набор ненильпотентных элементов a_i с условием, что $a_i^2 - a_i$ содержит элемент $n_1^{2^i}$ в качестве множителя. Так как элемент n_1 нильпотентен, получаем $a_i^2 - a_i = 0$ для некоторого i. □

Лемма 1.4.4. *Сумма конечного числа нильпотентных правых идеалов нильпотентна.*

Доказательство. Пусть N_1 и N_2 — нильпотентные правые идеалы кольца R. Сумма $N_1 + N_2$ также является правым идеалом. Пусть $N_1^n = N_2^m = \{0\}$. Тогда каждый элемент идеала $(N_1 + N_2)^{n+m}$ является суммой произведений вида

$$(x_1 + y_1) \cdot (x_2 + y_2) \cdot \ldots \cdot (x_{n+m} + y_{n+m}).$$

После раскрытия скобок мы получим сумму всевозможных произведений элементов из N_1 и N_2 длины $n+m$. Поскольку N_1 и N_2 — правые идеалы, элементы вида $x_i y_j$ лежат в N_1, а элементы вида $y_j x_i$ лежат в N_2. Таким образом, в каждом из произведений присутствует либо произведение n элементов из N_1, либо произведение m элементов из N_2. Следовательно, каждое из произведений равно нулю, т. е. $(N_1 + N_2)^{n+m} = \{0\}$. Индукция по числу слагаемых завершает доказательство леммы. □

Теорема 1.4.5. [7, Теорема (24.4)] *В алгебре R с условием минимальности сумма всех нильпотентных правых идеалов образует нильпотентный двусторонний идеал $J(R)$, называемый* радикалом Джекобсона *алгебры R или просто* радикалом *(в конечномерном случае). Радикал $J(R)$ содержит также и все левые нильпотентные идеалы, а фактор-алгебра $R/J(R)$ не содержит отличных от нуля нильпотентных идеалов.*

Доказательство. Очевидно, что $J(R)$ — правый идеал кольца R. Если $J(R)$ не является нильпотентным, то по теореме 1.4.3 он должен содержать идемпотент e. Но тогда элемент e принадлежит сумме конечного числа нильпотентных идеалов и потому, по лемме 1.4.4, нильпотентен, что невозможно. Следовательно, $J(R)$ нильпотентен.

Рассмотрим теперь двусторонний идеал $RJ(R)$. Для каждого i справедливо

$$(RJ(R))^i = R(J(R)R)(J(R)R)\dots(J(R)R)J(R) \leq RJ(R)^i.$$

Поэтому $RJ(R)$ — нильпотентный левый идеал и, значит, $RJ(R) \leq J(R)$. Обратное включение очевидно, поэтому $RJ(R) = J(R)$, т. е. $J(R)$ является двусторонним нильпотентным идеалом кольца R.

Наконец, любой правый идеал кольца $R/J(R)$ представим в виде $I/J(R)$, где I — правый идеал кольца R. Если идеал $(I/J(R))$ нильпотентен в кольце $R/J(R)$, то тогда идеал I нильпотентен в R, т. е. $I \leq J(R)$. □

Определение 1.4.6. Кольцо R с условием минимальности называется *полупростым*, если $J(R) = \{0\}$.

Пусть кольцо R полупросто и L — минимальный правый идеал кольца R (по включению). В силу теоремы 1.4.3, существует идемпотент $e \in L$. Тогда eR — правый идеал кольца R и $eR \leq L$. В силу минимальности идеала L получаем, что $eR = L$. Будем говорить, что идемпотент e *порождает* идеал L. Пусть теперь

$$L' = (1-e)R = \{x \in R | ex = 0\}.$$

Очевидно, что $L \cap L' = \{0\}$. Кроме того, так как каждый элемент x из R представим в виде

$$x = ex + x - ex = ex + (1-e)x,$$

то мы получаем, что $R = L \oplus L'$. Далее мы можем выбрать минимальный левый идеал $L_1 \leq L'$ кольца R. Для суммы $L \oplus L_1$ существует левый идеал L'' такой, что $L'' \oplus (L \oplus L_1) = R$. Повторяя данную процедуру, мы получаем цепочку идеалов $R \geq L' \geq L'' \geq \dots$. Поскольку кольцо R удовлетворяет условию минимальности, данная цепочка на некотором шаге стабилизируется. Ясно, что последним элементом цепочки должен быть $\{0\}$, так как в противном случае мы могли бы повторить шаг и получить продолжение цепочки. Таким образом, мы получили следующую теорему.

Теорема 1.4.7. *Пусть R — полупростое кольцо с условием минимальности. Тогда существует разложение $R = L_1 \oplus \dots \oplus L_k$ кольца R в прямую сумму минимальных правых идеалов. Более того, существуют такие идемпотенты $e_1, \dots, e_k$, что $L_i = e_i R$ для всех i и $e_i e_j = 0$ при $i \neq j$.*

Заметим также, что мы доказали следующее утверждение. Пусть $L = eR$ — минимальный левый идеал кольца R, порождённый идемпотентом e. Тогда $ex = x$ для любого $x \in L$.

Определение 1.4.8. Идемпотенты $\{e_1, \dots, e_n\}$, удовлетворяющие условию $e_i e_j = 0$ при $i \neq j$ называются *ортогональными*.

Лемма 1.4.9. *Минимальные правые идеалы L и L' изоморфны (как правые R-модули) тогда и только тогда, когда $L' = a'L$ для некоторого элемента $a' \in L'$.*

Доказательство. Если $L' = a'L$, то соответствие $\varphi : x \mapsto a'x$ будет R-изоморфизмом L на L'. $L_y = \{x \in L | a'(x-y) = 0\}$ — это правый идеал в L и потому он либо нулевой, либо совпадает с L. Совпадать с L он не может, так как в этом случае $a'L = \{0\}$, следовательно, $L_y = \{0\}$ для любого $y \in L$, откуда следует инъективность. Сюръективность нам дана по условию, поэтому отображение φ является биекцией. Далее $(x+y)\varphi = a'(x+y) = a'x + a'y = x\varphi + y\varphi$ и $(xr)\varphi = axr' = \varphi(x)r$.

Обратно, пусть существует изоморфизм $\varphi : L \to L'$. Тогда $(ex)\varphi = (e)\varphi x$ для любого элемента $x \in R$. Если $x \in L$, то в силу доказанного ранее $x = ex$ и $x\varphi = ax$, где $a = e\varphi$. □

Следствие 1.4.10. *$L \simeq L'$ тогда и только тогда, когда $L'L = L'$.*

Определение 1.4.11. Кольцо называется *простым*, если оно не содержит нетривиальных двусторонних идеалов.

Теорема 1.4.12. *Пусть R — полупростое кольцо, а L — минимальный правый идеал этого кольца. Сумма B_L всех минимальных правых идеалов кольца R, изоморфных идеалу L, является простым кольцом и двусторонним идеалом кольца R. Более того, кольцо R разлагается в прямую сумму идеалов B_L, где L пробегает полное множество попарно неизоморфных правых идеалов этого кольца.*

Доказательство. Пусть L и L' — минимальные правые идеалы кольца R. Если $L \not\simeq L'$, то по следствию 1.4.10 имеем $L'B_L = B_L L' = \{0\}$. Если же $L \simeq L'$, то $L' \leq B_L$ и $L'B_L, B_L L' \leq B_L$. Поскольку кольцо R является прямой суммой минимальных правых идеалов, то отсюда следует, что B_L — двусторонний идеал кольца R и тот факт, что кольцо R разлагается в прямую сумму идеалов B_L. Заметим, что $B_L B_{L'} = \{0\}$ если идеалы L и L' неизоморфны. Потому любой двусторонний идеал в B_L является двусторонним идеалом кольца R. Но B_L не содержит собственных двусторонних идеалов кольца R по построению. Следовательно, B_L не содержит собственных двусторонних идеалов, т. е. простое кольцо. □

Теорема 1.4.13. *Правый идеал L полупростого кольца R, порождённый идемпотентом e, минимален в том и только в том случае, когда eRe — тело.*

Доказательство. Заметим, что eRe — ненулевое подкольцо кольца R с единицей e. Если x — необратимый (по умножению) элемент кольца eRe, то $xeRe$ — собственный правый идеал кольца eRe. С другой стороны, в теле не содержится собственных идеалов. Поэтому достаточно доказать, что eRe не содержит собственных правых идеалов.

Пусть L_1 — произвольный ненулевой правый идеал кольца eRe. Тогда

$$L_1 R \leq eReR \leq eR = L$$

и, следовательно, $L_1 R = L$. Так как идемпотент e является двусторонней единицей кольца eRe, то

$$eRe = Le = L_1 Re = L_1 eRe \leq L_1,$$

откуда $L_1 = eRe$. Следовательно, в кольце eRe нет собственных идеалов и оно является телом.

Обратно, предположим, что идеал L не является минимальным. Так как правый R-модуль R вполне приводим, то имеет место разложение $L = L_2 \oplus L_3$, где L_2, L_3 — ненулевые правые идеалы кольца R. Тогда $e = e_2 + e_3$ — представление идемпотента e в виде суммы двух ортогональных идемпотентов. Ясно, что $e_2, e_3 \in eRe$, т. е. eRe содержит делители нуля и не может быть телом. □

Теорема 1.4.14. (теорема плотности) *Пусть R — кольцо и V — точный неприводимый R-модуль размерности n над телом $B = C_{\mathrm{M}(V)}(R)$. Тогда для любых линейно независимых $v_1, \ldots, v_k$ и любых $w_1, \ldots, w_k$ существует $r \in R$ переводящий v_i в w_i.*

Доказательство. Заметим, что для доказательства теоремы достаточно доказать следующее утверждение: если U — подпространство пространства V и $w \in V \setminus U$, то существует $r \in R$ такой, что $Ur = \{0\}$ и $wr \neq 0$.

Действительно, пусть всегда можно отыскать такой элемент r. Тогда $wrR \neq \{0\}$ и в силу неприводимости модуля V, справедливо $wrR = V$. Следовательно, мы можем найти такой элемент $s \in R$, что wrs — любой наперед заданный элемент из V, в то время как $Urs = \{0\}$. Если даны линейно независимые элементы $v_1, \ldots, v_k \in V$ и произвольные элементы $w_1, \ldots, w_k \in V$, то мы можем найти элементы $r_i, s_i \in R$ для которых $v_i r_i s_i = w_i$ и $v_j r_i s_i = 0$ для всех $j \neq i$. Тогде элемент $r = r_1 s_1 + \ldots + r_k s_k$ переводит v_i в w_i.

Докажем теперь, что если U — подпространство пространства V и $w \in V \setminus U$, то существует такой $r \in R$, что $Ur = \{0\}$, а $wr \neq 0$. Доказательство будем вести индукцией по размерности подпространства U.

Утверждение тривиально, если $\dim U = 0$, т. е. $U = \{0\}$. Пусть $U = U_0 + uB$, где $\dim U_0 = \dim U - 1$ и $u \in U \setminus U_0$. Пусть $A(U_0) = \{r \in R | U_0 r = \{0\}\}$. По предположению индукции для любого $x \notin U_0$ существует такой $r \in A(U_0)$, что $xr \neq \{0\}$, т. е. $xA(U_0) = \{0\}$ тогда и только тогда, когда $x \in U_0$.

Множество $A(U_0)$ является правым идеалом в R, и так как $u \notin U_0$, то $uA(U_0) \neq \{0\}$. Так как $uA(U_0)$ — подмодуль модуля V, то $uA(U_0) = V$. Допустим, что существует элемент $x \in V \setminus U$ такой, что из равенства $Ur = \{0\}$ следует $xr = 0$. Определим отображение $\tau : V \to V$, полагая $v\tau = xa$ для любого $v \in V$, если $v = ua$, где $a \in A(U_0)$. Ясно, что τ сохраняет линейность. Поэтому для проверки корректности достаточно показать, что $0\tau = 0$. Пусть $v = 0 = ua$. Тогда $Ua = \{0\}$, следовательно, по построению элемента x, $xa = 0$.

Далее, если $v = ua$, где $a \in A(U_0)$, то для любого $r \in R$ имеем $vr = (ua)r = u(ar)$, где $ar \in A(U_0)$. Следовательно, $(vr)\tau = x(ar) = (xa)r = (v\tau)r$. Отсюда $\tau \in B = C_{\mathrm{M}(V)}(R)$. Но тогда для любого элемента $a \in A(U_0)$ справедливы соотношения $xa = (ua)\tau = (u\tau)a$, $(x - u\tau)a = 0$. По предположению индукции последнее соотношение влечёт, что $x - u\tau \in U_0$, т. е.

$$x \in U_0 + u\tau \subseteq U_0 + uB = U.$$

Полученное противоречие завершает доказательство теоремы. □

Теорема 1.4.15. (Веддерберн) *Пусть A — простое кольцо с условием минимальности. Тогда существует такое конечномерное векторное пространство V над телом B, что $A \simeq \mathrm{M}(V) \simeq \mathrm{M}_n(B)$. Размерность $n = \dim V$ и тело B определяются кольцом A однозначно.*

Доказательство. Пусть $V = eA$ — минимальный правый идеал кольца A и A_L — кольцо эндоморфизмов аддитивной группы идеала V, задаваемое правилом для любого $a \in A$ отображение a_L — это правое умножение: $a_L : v \to va, v \in V$. Отображение $a \to a_L$ — это гомоморфизм кольца A, ядро которого — это двусторонний идеал в A. Поскольку A простое, получаем, что $A \simeq A_L$.

Так как A-модуль V неприводим, то по лемме Шура 1.2.1, $B = C_{\mathrm{M}(V)}(A)$ — тело. Будем рассматривать $\lambda \in B$ как левые векторные операторы на V. Тогда V превращается в векторное пространство над телом B и для каждого элемента $a_L \in A_L$ справедливо $(\lambda v)a_L = \lambda(va_L)$, где $v \in V$ и $\lambda \in B$. Следовательно, $\mathrm{M}(V) \simeq \mathrm{M}_n(B)$, где $n = dim(V)$ над телом B. Таким образом, мы показали, что A изоморфна некоторому подкольцу кольца $\mathrm{M}(V) \simeq \mathrm{M}_n(B)$. Равенство $A = \mathrm{M}(V)$ сразу следует из теоремы плотности 1.4.14.

Покажем теперь, что размерность модуля и тело определены единственным образом с точностью до изоморфизма. Предположим, что $A \simeq \mathrm{M}_n(\Delta)$ для некоторого тела Δ. Тогда, ввиду 1.4.12 все минимальныеправые идеалы кольца A изоморфны, они изоморфны $V = eA$ с одной стороны и изоморфны множеству матриц с ненулевой первой строкой и нулями на всех остальных местах с другой стороны. При этом тело $D \simeq eAe \simeq \Delta$, откуда следует единственность. □

§5 Следствия для полупростых колец.

Везде в данном параграфе R — это кольцо с условием минимальности и содержащее 1.

Определение 1.5.1. Пусть R — некоторое кольцо и $Hom(R, R)$ — множество гомоморфизмов аддитивной группы кольца R в себя. Тогда можно рассмотреть вложение $\varphi : R \to Hom(R, R)$, заданное правилом: для любых $s, r \in R$, справедливо $s(r\varphi) = sr$. Кольцо R, рассматриваемое как правый R-модуль будет обозначаться R_R, вложение φ называется *правым регулярным представлением* кольца R. Аналогично определяется *левое регулярное представление* и левый R-модуль ${}_RR$.

Теорема 1.5.2. *Кольцо R с условием минимальности и единицей полупросто тогда и только тогда, когда модуль R_R вполне приводим.*

Доказательство. Полная приводимость модуля R_R для полупростого кольца следует из теоремы 1.4.7. Обратно, предположим, что модуль R_R вполне приводим. Пусть $N = J(R)$ — радикал кольца R. Тогда N является подмодулем модуля R_R, следовательно, $R = N \oplus N'$, где N' — правый идеал кольца R. Рассмотрим разложение $1 = x + x'$, где $x \in N$, $x' \in N'$. Тогда $x - x^2 = x' - x'^2 \in N \cap N' = \{0\}$. Следовательно, $x = x^2 = \ldots = 0$. Значит, $x' = 1 \in N'$ и $N' = R$. □

Теорема 1.5.3. *Кольцо R с условием минимальности и единицей полупросто тогда и только тогда, когда каждый R-модуль вполне приводим.*

Доказательство. Ввиду предыдущей теоремы достаточно показать, что любой R-модуль M полупростого кольца R вполне приводим. Рассмотрим разложение $1 = e_1 + e_2 + \ldots + e_k$ в виде суммы ортогональных идемпотентов, где e_iR — минимальный правый идеал для каждого i. Тогда имеет место равенство

$$M = \sum_{m \in M} \sum_{i=1}^{k} m(e_iR).$$

Очевидно, me_iR — подмодуль модуля M для каждого элемента $m \in M$. Зададим R-гомоморфизм $e_iR \to me_iR$ правилом $e_ix \mapsto me_ix$. Так как e_iR — минимальный правый идеал, то ядро этого гомоморфизма равно $\{0\}$ или

e_iR. Следовательно, подмодуль me_iR или неприводим, или равен нулю. Таким образом, модуль M порождён неприводимыми подмодулями, значит, по теореме 1.2.6, модуль M вполне приводим. □

Лемма 1.5.4. *Если кольцо R полупросто, то каждый неприводимый R-модуль изоморфен некоторому минимальном правому идеалу в R.*

Доказательство. В доказательстве предыдущей теоремы достаточно предположить, что модуль M неприводим. □

Следствие 1.5.5. *Кольцо R является простым в том и только в том случае, когда существует точный неприводимый R-модуль.*

Рассмотрим теперь алгебру $\mathbb{C}G$, где G — конечная группа. Ввиду теоремы Машке 1.2.4, любой $\mathbb{C}G$-модуль вполне приводим, следовательно, $\mathbb{C}G$ — полупростая алгебра над полем $\mathbb{C}$. Следовательно, $\mathbb{C}G$ представима в виде прямой суммы простых алгебр $\mathrm{M}_{n_1}(\mathbb{C}) \oplus \ldots \oplus \mathrm{M}_{n_k}(\mathbb{C})$ для подходящих n_i. Кроме того, любой неприводимый $\mathbb{C}G$-модуль изоморфен $\mathbb{C}^{n_i}$ для некоторого $i \in \{1, \ldots, k\}$. Таким образом, мы доказали следующее равенство

$$|G| = \sum_{i=1}^{k} n_i^2,$$

где n_i пробегают размерности всех представителей классов изоморфизмов неприводимых $\mathbb{C}G$-модулей.

Теорема 1.5.6. *Пусть G — конечная группа, $\mathbb{F}$ — поле, $Cl_1, \ldots, Cl_s$ — классы сопряженных элементов группы G и*

$$C_i = \sum_{x \in Cl_i} x.$$

Тогда элементы $C_1, \ldots, C_s$ образуют $\mathbb{F}$-базис центра групповой алгебры $\mathbb{F}G$.

Доказательство. Очевидно, что элементы C_i принадлежат центру групповой алгебры $\mathbb{F}G$. Более того, они линейно независимы над $\mathbb{F}$, поскольку являются суммой элементов из непересекающихся подмножеств группы G. Пусть элемент $y = \sum a_g g$ принадлежит центру групповой алгебры $\mathbb{F}G$. Тогда для каждого элемента $h \in G$ справедливо

$$\sum a_g g = y = h^{-1}yh = \sum a_g h^{-1}hg.$$

Сравнивая коэффициенты при элементах $g \in G$ в правой и левой частях последнего равенства, получим, что $a_{h^{-1}gh} = a_g$ для всех $g \in G$.

Таким образом, если элементы $g, g' \in G$ лежат в одном классе сопряженных элементов, то $a_g = a_{g'}$, и, значит, элемент y является $\mathbb{F}$-линейной комбинацией элементов из $\{C_i\}$. □

Теорема 1.5.7. *Пусть G — конечная группа. Тогда число неизоморфных неприводимых $\mathbb{C}G$-модулей равно числу классов сопряженных элементов группы G.*

Доказательство. Пусть $\mathbb{C}G = A_1 \oplus \ldots \oplus A_k$ — представление кольца $\mathbb{C}G$ в виде прямой суммы простых алгебр. Поскольку они аннулируют друг друга, справедливо $Z(\mathbb{C}G) = Z(A_1) \oplus \ldots \oplus Z(A_k)$. Но $A_i \simeq \mathrm{M}_{n_i}(\mathbb{C})$ для подходящего n_i, следовательно, $Z(A_i) \simeq \mathbb{C}$ и его размерность равна 1, т. е. размерность центра алгебры $\mathbb{C}G$ равна k и равна количеству неизоморфных неприводимых $\mathbb{C}G$-модулей. В силу предыдущей теоремы 1.5.6 мы знаем, что элементы C_i образуют базис центра кольца $\mathbb{C}G$, следовательно, k равно количеству классов сопряженных элементов группы G. □

В конце данного параграфа мы сформулируем одну теорему, которая не является прямым следствием изложенных выше результатов, но довольно просто доказывается с использованием групповых колец. Элемент $x \in \mathrm{GL}_n(\mathbb{F})$ называется *унипотентным*, если $x - e$ — нильпотентный элемент алгебры $\mathrm{M}_n(\mathbb{F})$. Подгруппа U группы $\mathrm{GL}_n(\mathbb{F})$ называется *унипотентной*, если она состоит из унипотентных элементов. Матрица называется *унитреугольной*, если она треугольная и по диагонали у неё стоят 1. Группа всех верхних унитреугольных матриц обозначается через $\mathrm{UT}_n(\mathbb{F})$.

Теорема 1.5.8. *Пусть U — унипотентная подгруппа группы $\mathrm{GL}_n(\mathbb{F})$. Тогда U подобна подгруппе группы верхних унитреугольных матриц $\mathrm{UT}_n(\mathbb{F})$. В частности, группа U нильпотентна*

Доказательство. Пусть $\mathfrak{U} = \langle U \rangle$. Очевидно, что $\mathfrak{U}$ — подалгебра алгебры $\mathrm{M}_n(\mathbb{F})$. Покажем, что $\mathfrak{U}$ нильпотентна. Действительно, если $\mathfrak{U}$ не является нильпотентной, то переходя, если нужно, к фактор алгебре $\mathfrak{U}/I(\mathfrak{U})$, можно считать, что $\mathfrak{U}$ полупроста. По теореме 1.4.12 любая полупростая алгебра является прямой суммой простых алгебр, следовательно, вновь переходя, если нужно, к фактор алгебре, можно считать, что $\mathfrak{U}$ проста. По теореме Веддерберна 1.4.15 алгебра $\mathfrak{U}$ изоморфна $\mathrm{M}_n(D)$ для некоторого тела D. Следовательно, $X = \mathrm{diag}(1, 0, \ldots, 0) \in \mathfrak{U}$. С другой стороны, $X = \sum_i \alpha_i(x_i - e)$, где все $(x_i - e)$ нильпотентны. Значит, справедливы равенства $1 = \mathrm{tr}(X) = \mathrm{tr}(\sum_i \alpha_i(x_i - e)) = \sum_i \alpha_i \mathrm{tr}(x_i - e) = 0$, противоречие.

Таким образом, алгебра $\mathfrak{U}$ нильпотентна. В частности, существует такое k, что для любых $y_1, \ldots, y_k \in \mathfrak{U}$ справедливо $y_1 \cdot \ldots \cdot y_k = 0$. Пусть k — наименьшее натуральное число, удовлетворяющую этому условию и рассмотрим $\mathfrak{Z} = \{\sum_i \alpha_i(x_i - e)^{k-1}\}$. Ясно, что $\mathfrak{Z}$ — подалгебра алгебры $\mathfrak{U}$ и для всех $z \in \mathfrak{Z}, u \in \mathfrak{U}$ справедливо $zu = uz = 0$. Таким образом, $\mathfrak{Z}$ — нетривиальная центральная подалгебра, следовательно, пространство $W = \{x \in V | xz = 0 \text{ для всех } z \in \mathfrak{Z}\}$ является собственным $\mathfrak{U}$-подмодулем в V. По лемме 1.1.9 мы получаем, что W — собственный U-подмодуль в V. Ясно, что ограничение $U\mid_W$ является унипотентной подгруппой группы $\mathrm{GL}(W)$. Индукция по размерности пространства завершает доказательство. □

***Упражнение* 1.5.9.** Пусть $\mathbb{F}$ — произвольное поле. Доказать, что группа унитреугольных матриц $\mathrm{UT}_n(\mathbb{F})$ нильпотентна.

§6 Нильпотентные подгруппы симметрических групп

Определение 1.6.1. Подгруппа H симметрической группы Sym_n называется *транзитивной*, если для любых $i, j \in \{1, \ldots, n\}$ существует элемент $h \in H$ такой, что $i^h = j$. Подгруппа H симметрической группы Sym_n называется *k-транзитивной*, если для любых наборов попарно различных элементов $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $\{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}$ существует такой $h \in H$, что $i_1^h = j_1, \ldots, i_k^h = j_k$. Заметим, что порядок транзитивной подгруппы группы Sym_n всегда делится на n, так как индекс стабилизатора точки $St_H(i) = \{h \in H | i^h = i\}$ в группе H равен n.

Лемма 1.6.2. *Пусть N — транзитивная нильпотентная подгруппа группы Sym_n. Тогда любой простой делитель порядка группы N делит n.*

Доказательство. Поскольку стабилизатор точки в транзитивной подгруппе имеет индекс n, получаем, что n делит $|N|$.

С другой стороны, пусть p — некоторый простой делитель $|N|$ и P — силовская p-подгруппа группы N. Пусть $x \in Z(P)$ — некоторый элемент порядка p из центра группы P. Обозначим через $\Omega_1, \ldots, \Omega_s$ орбиты элемента x. Тогда, в силу транзитивности группы N, $|\Omega_1| = \ldots = |\Omega_s| = p$ и $\Omega_1 \cup \ldots \cup \Omega_s = \{1, \ldots, n\}$. Поэтому $n = p \cdot s$, значит, p делит n. □

Лемма 1.6.3. *Пусть N — максимальная нильпотентная транзитивная подгруппа группы Sym_{p^n}, где p — простое число. Тогда N является силовской p-подгруппой группы Sym_{p^n}.*

Доказательство. Пусть N — максимальная транзитивная нильпотентная подгруппа группы Sym_{p^n}. Ввиду леммы 1.6.2 её порядок может делиться лишь на одно простое число, p. Ввиду максимальности группы N получаем, что она должна совпадать с силовской p-подгруппой группы Sym_{p^n}. Нетрудно показать, что силовская p-подгруппа группы Sym_{p^n} является транзитивной. □

Предположим теперь, что $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ — разложение числа n по степеням простых чисел Любой элемент множества $\{1, \ldots, n\}$ может быть записан в виде $\xi = [\xi_1, \ldots, \xi_k]$, где $\xi_i \in \{1, \ldots, p_i^{\alpha_i}\}$. Если $N^{(j)}$ — это силовская p_i-подгруппа группы $\mathrm{Sym}_{p_i^{\alpha_i}}$, определим группу N_{p_i} правилом

$$N_{p_i} = \{x \in \mathrm{Sym}_n | \xi^x = [\xi_1, \ldots, \xi_i^{\varphi}, \ldots, \xi_k] \text{ для некоторого } \varphi \in N^{(i)}\}.$$

Очевидно, что $N_n = N_{p_1} \times \ldots \times N_{p_k}$ транзитивна и нильпотентна. Далее мы докажем, что любая транзитивная нильпотентная подгруппа группы Sym_n сопряжена с некоторой подгруппой группы N_n.

Ввиду леммы 1.6.2 каждая транзитивная нильпотентная подгруппа $N \leq \mathrm{Sym}_n$ имеет порядок $p_1^{\nu_1} \cdot \ldots \cdot p_k^{\nu_k}$ и $\nu_i \geqslant \alpha_i$. Мы можем записать N в виде $N = H \times F$, где $|H| = p_1^{\nu_1}$ и $|F| = p_2^{\nu_2} \cdot \ldots \cdot p_k^{\nu_k}$.

Лемма 1.6.4. *Символы, переставляемые группой N можно занумеровать парами $[x, y]$ так, что для любого $h \in H$ и $f \in F$, справедливо*

$$[x, y]^h = [x^{\psi}, y], \ [x, y]^f = [x, y^{\phi}],$$

где $x \in \{1, \dots, p_1^{\alpha_1}\}$, $y \in \{1, \dots, p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}\}$.

Доказательство. Число n не делит порядок $|F|$, значит, F нетранзитивна. Пусть $\Omega_1, \dots, \Omega_l$ — орбиты группы F. Имеем $F \trianglelefteq N$ и N транзитивна, следовательно, $\Omega_1, \dots, \Omega_l$ — это система импримитивности для N. Значит, $|\Omega_1| = \dots = |\Omega_l| = r$ и группа F содержится в прямом произведении l нильпотентных транзитивных подгрупп группы Sym_r. Таким образом, порядок $|F|$ и r имеют одинаковые простые делители $p_2, \dots, p_k$. Далее, группа N транзитивна и F оставляет неподвижным каждое из Ω_i, поэтому H переставляет орбиты Ω_i транзитивно. Значит, l делит $|H|$ и $l = p_1^{\beta_1}$. Но $lr = n$, значит, $l = p_1^{\alpha_1}$, $r = p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Рассмотрим $\{1, 2, \dots, r\} = \Omega_1$. Группа H действует транзитивно, следовательно, каждая орбита Ω_x может быть записана как $\{x_1, x_2, \dots, x_r\}$, где $x_j = j^{h_x}$ для подходящего $h_x \in H$. Если $j^f = i_j$ то $x_j^f = j^{h_x f} = j^{f h_x} = x_{i_j}$. Поэтому для записи $\Omega_x = \{[x,1], [x,2], \dots, [x,r]\}$ справедливо $[x,y]^f = [x, y^{\phi}]$.

Рассмотрим теперь $[x,y]^h$. Достаточно показать, что $[1,y]^h = [x,y]$. Предположим, что $[1,y]^h = [x,y_1]$ и $y \neq y_1$. Тогда существует h_x такой, что $[1,y]^{hh_x^{-1}} = [1,y_1]$. Значит, $(hh_x^{-1})|_{\Omega_1} = h_0$ — это подстановка на орбите $\Omega_1 = \{[1,1], \dots, [1,r]\}$. Рассмотрим $F_0 = F|_{\Omega_1}$. Очевидно, h_0 централизует F_0, следовательно $\langle h_0, F_0 \rangle$ — это нильпотентная транзитивная подгруппа группы Sym_l. Ввиду леммы 1.6.2, каждый простой делитель поряка $|\langle h_0, F_0 \rangle|$ лежит в $p_2, \dots, p_k$. Но $|h_0| = p_1^{\gamma_1}$, значит $h_0 = e$. Следовательно, $y = y_1$ $[x,y]^h = [x^{\psi}, y]$ для всех $x \in \{1, \dots, l\}$. □

Теорема 1.6.5. *Любая транзитивная нильпотентная подгруппа N группы Sym_n сопряжена с некоторой подгруппой группы N_n.*

Доказательство. Пусть $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Если $k = 1$, то теорема доказана (лемма 1.6.3). Предположим, что $k > 1$ и проведем доказательство по индукции. Имеем $N = H \times F$. По индукции подгруппа F сопряжена с некоторой подгруппой группы $N_{n/p_1^{\alpha_1}} = N_{p_2^{\alpha_2} \dots p_k^{\alpha_k}}$. Поэтому $N = H \times F$ сопряжена с некоторой подгруппой группы N_n. □

§7 Неприводимые нильпотентные подгруппы конечных линейных групп

Определение 1.7.1. Неприводимая подгруппа G группы $\mathrm{GL}_n(\mathbb{F})$ называется *абсолютно неприводимой*, если G неприводима в группе $\mathrm{GL}_n(\overline{\mathbb{F}})$, где $\overline{\mathbb{F}}$ — алгебраическое замыкание поля $\mathbb{F}$.

Лемма 1.7.2. *Пусть G — нильпотентная неприводимая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$, где $\mathbb{F}$ — произвольное поле и $Z_1 = Z(G)$. Тогда группу G можно вложить в $\mathrm{GL}_r(\Delta)$ таким образом, что $Z_1 \leq Z(\mathrm{GL}_r(\Delta)) = \Delta^* E$. Здесь Δ — алгебраическое расширение поля $\mathbb{F}$, удовлетворяющее условию $n = r[\Delta : \mathbb{F}]$. Более того, G является абсолютно неприводимой подгруппой группы $\mathrm{GL}_r(\Delta)$.*

Доказательство. Ввиду леммы Шура 1.2.1 получаем, что $C_{\mathrm{M}_n(\mathbb{F})}(G)$ — тело. Далее $Z_1 \leq \mathcal{L}_{\mathbb{F}}(Z_1) \leq C_{\mathrm{M}_n(\mathbb{F})}(G)$ и кольцо $\mathbb{F}Z_1$ коммутативно, значит, $\mathbb{F}Z_1$ является полем, которое обозначается Δ. Поскольку $Z_1 \trianglelefteq G$ и G неприводима, значит, по теореме Клиффорда 1.3.4, справедливо $V = \mathbb{F}^n = Q_1 \oplus \dots \oplus Q_r$, где все Q_i являются неприводимыми Z_1-подмодулями размерности m. Таким образом, $Q_i = u_i \Delta$, $u_i \in Q_i$ и V можно рассматривать как пространство над Δ размерности r. Наконец, $Z_1 = Z(G)$, поэтому $G \leq \mathrm{GL}_r(\Delta)$. Кроме того, $\dim Q_i = [\Delta : \mathbb{F}]$, следовательно, $n = r[\Delta : \mathbb{F}]$.

Докажем теперь, что G является абсолютно неприводимой подгруппой группы $\mathrm{GL}_r(\Delta)$. Заметим, что достаточно доказать равенство $\mathcal{L}_{\Delta}(G) = \mathrm{M}_r(\Delta)$, поскольку это влечёт $\mathcal{L}_{\overline{\Delta}}(G) = \mathrm{M}_r(\overline{\Delta})$ для алгебраического замыкания $\overline{\Delta}$ поля Δ. Поскольку $\mathcal{L}_{\Delta}(G)$ неприводима, $\mathcal{L}_{\Delta}(G)$ — это простая алгебра. Следовательно, по лемме Шура 1.2.1, её централизатор в $\mathrm{M}_r(\Delta)$ — тело. По построению Δ, имеем $\Delta E = C_{\mathrm{M}_r(\Delta)}(G)$. Значит, $\mathcal{L}_{\Delta}(G)$ — это простая алгебра над Δ (см. доказательство теоремы Веддерберна 1.4.15) и совпадает с $\mathrm{M}_r(\Delta)$. □

Лемма 1.7.3. *Рассмотрим подгруппу* $L = \left\{ \mathrm{diag}(\underbrace{A, \dots, A}_{l \text{ раз}}) \mid A \in G \right\}$ *группы $\mathrm{GL}_n(\mathbb{F})$, где G — абсолютно неприводимая подгруппа группы $\mathrm{GL}_{n/l}(\mathbb{F})$. Тогда $C_{\mathrm{GL}_n(\mathbb{F})}(L) = M$, где $M \simeq \mathrm{GL}_l(\mathbb{F})$.*

Доказательство. Пусть $B = \{B_{i,j}\}_{i,j=1}^{l} \in C_{\mathrm{GL}_n(\mathbb{F})}(L)$, где $B_{i,j}$ — блоки размера $(n/l) \times (n/l)$ (т. е. того же размера, что и блоки, стоящие по диагонали в матрицах из группы L). Для любого элемента $x =$

$\mathrm{diag}(A,\dots,A)\in L$ справедливо

$$xB=\mathrm{diag}(A,\dots,A)B=\{AB_{i,j}\}_{i,j=1}^{l}=Bx=\{B_{i,j}A\}_{i,j=1}^{l}.$$

Поскольку группа G абсолютно неприводима, её централизатор в группе $\mathrm{GL}_{n/l}(\overline{\mathbb{F}})$ является полем. Поэтому каждый из блоков $B_{i,j}$ является скалярной матрицей. $\square$

Теорема 1.7.4. *Пусть $\mathbb{F}$ — алгебраически замкнутое поле, G — конечная нильпотентная неприводимая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$. Тогда существует базис $u_1,\dots,u_n$ пространства $V=\mathbb{F}^n$ такой, что для любого $g\in G$ справедливо:*

$$u_1^g=\lambda_1u_{i_1},\dots,u_n^g=\lambda_nu_{i_n},\ \lambda_j\in\mathbb{F},$$

где $\{i_1,\dots,i_n\}=\{1,\dots,n\}$, т. е. G сопряжена с мономиальной подгруппой группы $\mathrm{GL}_n(\mathbb{F})$.

Доказательство. Ввиду леммы 1.3.3 существуют подпространства $W_1,\dots,W_r$ пространства $V=\mathbb{F}^n$ такие, что $\{W_1,\dots,W_r\}$ является системой импримитивности группы G и каждая из G_i примитивна и нильпотентна. Если группа G_i неабелева, то существует абелева нормальная максимальная подгруппа A_i группы G_i, значит, $A_i\not\leq\mathbb{F}E=Z(G)=Z(\mathrm{GL}_n(\mathbb{F}))$. Ввиду теоремы Клиффорда 1.3.4(в), группа G_i непримитивна. Таким образом, мы доказали что все группы G_i абелевы, следовательно, $\dim W_i=1$. $\square$

Следствие 1.7.5. *Если $\mathbb{F}$ — алгебраически замкнутое поле, то фактор-группа неприводимой нильпотентной подгруппы группы $\mathrm{GL}_n(\mathbb{F})$ по произвольной максимальной нормальной абелевой подгруппе изоморфна транзитивной подгруппе симметрической группы Sym_n.*

Лемма 1.7.6. *Пусть $\mathbb{F}$ — конечное поле, G — нильпотентная абсолютно неприводимая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$. Тогда n и $|G/Z(G)|$ имеют одинаковый набор простых делителей.*

Доказательство. Рассмотрим абелеву максимальную нормальную подгруппу H группы G. Ввиду следствия 1.7.5 имеем, что G/H является нильпотентной транзитивной подгруппой группы Sym_n. По лемме 1.6.2, $|G/H|$ и n имеют одинаковый набор простых делителей. Поэтому, любой простой делитель числа n делит $|G/Z(G)|$.

Обратно, предположим, что существует простой делитель r порядка $|G/Z(G)|$, который не делит n. Следовательно, существует элемент $x\in G\setminus Z(G)$ порядка $|x|=r^\nu$. Возьмем произвольную абелеву нормальную максимальную подгруппу H группы G. Поскольку $|G/H|$ и n имеют одни и те же простые делители, значит, $x\in H$. Далее, $x\notin Z(G)$, следовательно, существует $y\in G\setminus C_G(x)$ порядка $|y|=s^\mu$, где s простое. Как мы отметили выше, любой r-элемент группы G содержится в H, значит, перестановочен с x. Таким образом, $s\neq r$ и группа $\langle x,y\rangle$ не является нильпотентной. $\square$

Следствие 1.7.7. *Если p — это характеристика поля $\mathbb{F}$ и p делит n, то $\mathrm{GL}_n(\mathbb{F})$ не содержит абсолютно неприводимых нильпотентных подгрупп.*

Лемма 1.7.8. *Пусть G — абсолютно неприводимая максимальная нильпотентная подгруппа группы $\mathrm{GL}_{r^k}(p^\alpha)$. Тогда $G=RZ(\mathrm{GL}_{r^k}(p^\alpha))$, где R — это силовская r-подгруппа группы $\mathrm{GL}_{r^k}(p^\alpha)$. В частности, все абсолютно неприводимые нильпотентные максимальные подгруппы группы $\mathrm{GL}_{r^k}(p^\alpha)$ сопряжены и*

$$C_{\mathrm{GL}_{r^k}(p^\alpha)}(G)=Z(G)=Z(\mathrm{GL}_{r^k}(p^\alpha)).$$

Доказательство. Немедленно следует из леммы 1.7.6. $\square$

Далее, аналогично тому, как это было проделано для симметрических групп, мы определим некоторые «канонические» максимальные неприводимые нильпотентные подгруппы в группе $\mathrm{GL}_n(\overline{\mathbb{F}})$ и докажем, что любая нильпотентная неприводимая подгруппа содержится (с точностью до сопряжения) в одной из таких «канонических» подгрупп.

Пусть $n=r_1^{\nu_1}\cdot\ldots\cdot r_k^{\nu_k}$ — разложение числа n в произведение простых множителей. Определим нильпотентную абсолютно неприводимую подгруппу N_n группы $GL_n(p^\alpha)$ следующим образом. Рассмотрим группу

$$L_1=\left\{\mathrm{diag}(\underbrace{A,\dots,A}_{l\text{ раз}})\mid A\in\mathrm{GL}_{r_1^{k_1}}(p^\alpha),\ \text{где } l=r_2^{\nu_2}\cdot\ldots\cdot r_m^{\nu_m}\right\}.$$

Возьмем $N_1 = R_1 Z(L_1)$, где R_1 — это силовская r_1-подгруппа группы L_1. По лемме 1.7.3,

$$C_{\mathrm{GL}_n(p^\alpha)}(L_1) \simeq \mathrm{GL}_{r_2^{\nu_2} \ldots r_k^{\nu_k}}(p^\alpha).$$

По лемме 1.7.8, $C_{L_1}(N_1) = Z(N_1) = Z(L_1)$, значит, $C_{\mathrm{GL}_n(p^\alpha)}(N_1) = C_{\mathrm{GL}_n(p^\alpha)}(L_1) \simeq \mathrm{GL}_{r_2^{\nu_2} \ldots r_k^{\nu_k}}(p^\alpha)$ (Лемма 1.7.3). Далее действуем по индукции. В конце получаем $N_n \simeq (R_1 \times \ldots \times R_k)Z(\mathrm{GL}_n(p^\alpha))$. По построению, группа N_n нильпотентна и абсолютно неприводима.

Теорема 1.7.9. [16] *Пусть G — абсолютно неприводимая максимальная нильпотентная подгруппа группы $\mathrm{GL}_n(p^\alpha)$ и $n = r_1^{\nu_1} \ldots r_k^{\nu_k}$. Тогда $G/Z(G) = R_1 \times \ldots \times R_k$, где R_i — это силовская r_i-подгруппа группы $\mathrm{GL}_{r_i^{\nu_i}}(p^\alpha)/Z(\mathrm{GL}_{r_i^{\nu_i}}(p^\alpha))$ и все абсолютно неприводимые максимальные нильпотентные подгруппы группы $\mathrm{GL}_n(p^\alpha)$ сопряжены.*

Доказательство. Пусть G — нильпотентная абсолютно неприводимая подгруппа группы $\mathrm{GL}_n(p^\alpha)$, покажем, что G сопряжена с некоторой подгруппой группы N_n.

Ввиду леммы 1.7.6, имеем $G = (Q_1 \times \ldots \times Q_k)Z(G)$, где Q_i — это нетривиальная силовская r_i-подгруппа группы G и (см. леммы 1.7.2 и 1.7.8) $Z(G) \leq Z(\mathrm{GL}_n(p^\alpha))$. Ввиду теоремы Машке 1.2.4, группа Q_1 вполне приводима, следовательно, пространство V представимо в виде $V = W_1 \oplus \ldots \oplus W_k$. Ввиду теоремы Клиффорда 1.3.4 для каждого $i \in \{1, \ldots, k\}$ существует $g_i \in G$ такой, что $W_i = W_1 g_i$. Поскольку группа G нильпотентна и для любого $h \in Q_1$ справедливо $W_1 h = W_1$ можно считать, что $|g_i|$ не делится на r_1 и g_i централизует Q_1. Поэтому отображение $W_1 \to W_i$, заданное правилом $w_1 \mapsto w_1 g_i$ является изоморфизмом Q_1-модулей и все W_i изоморфны как Q_1-модули. Значит, можно найти такой базис пространства V, в котором справедливо $Q_1 \leq \left\{ diag(\underbrace{A, \ldots, A}_{k \text{ раз}}) \mid A \in \mathrm{GL}_{n/k}(p^\alpha) \right\}$. Далее, $Q_1|_{W_1}$ — нильпотентная неприводимая подгруппа группы $\mathrm{GL}_{n/k}(p^\alpha)$. Кроме того $Z(Q_1) \leq Z(G) \leq Z(\mathrm{GL}_n(p^\alpha))$, следовательно, по лемме 1.7.2, группа $Q_1|_{W_1}$ абсолютно неприводима. Значит, $n/k = r_1^\lambda$ (см. лемму 1.7.6). Теперь $Q_2 \times \ldots \times Q_k$ — нильпотентная абсолютно неприводимая подгруппа группы $\mathrm{GL}_k(p^\alpha)$, значит, $(k, r_1) = 1$. Поэтому $n/k = r_1^{\nu_1}$, подгруппа Q_1 сопряжена с некоторой подгруппой группы $R_1 \leq N_n$ и можно использовать индукцию. □

Следствие 1.7.10. *Пусть N и M — максимальные нильпотентные неприводимые подгруппы группы $\mathrm{GL}_n(q)$. Они сопряжены тогда и только тогда, когда сопряжены их центры.*

Доказательство. Часть «тогда» очевидна. В обратную сторону, если центры сопряжены, то можно считать, что они совпадают. Тогда нильпотентные подгруппы сопряжены ввиду леммы 1.7.2 и теоремы 1.7.9. □

§8 Разрешимые подгруппы линейных групп

Лемма 1.8.1. *Пусть G — примитивная разрешимая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$ и H — абелева нормальная подгруппа группы G. Тогда H изоморфна подгруппе мультипликативной группы некоторого поля K, содержащегося в $\mathrm{M}_n(\mathbb{F})$ и $[K : \mathbb{F}]$ делит n.*

Доказательство. По условию, H является нормальной подгруппой некоторой примитивной группы, значит, по теореме Клиффорда 1.3.4 и лемме 1.3.3 имеем, что $\mathcal{L}_{\mathbb{F}}(H)$ — это простая коммутативная подалгебра алгебры $\mathrm{M}_n(\mathbb{F})$. По теореме 1.4.15, $K = \mathcal{L}_{\mathbb{F}}(H)$ является коммутативным телом, т. е. полем.

Теперь $\mathbb{F}^n$ — это прямая сумма неприводимых K-подмодулей

$$\mathbb{F}^n = W_1 \oplus \ldots \oplus W_k, \quad \dim(W_i) = \frac{n}{k}.$$

Если $w_i \in W_i$ и $w_i \neq 0$, то $w_i K = W_i$. Следовательно $[K : \mathbb{F}] = \dim(W_i) = \frac{n}{k}$. □

Если теперь K^* — мультипликативная подгруппа поля $K = \mathcal{L}_{\mathbb{F}}(H)$, то $gK^*g^{-1} = K^*$ для всех элементов $g \in G$. Следовательно, $GK^* = K^*G$ — разрешимая группа и K^* — абелева нормальная подгруппа группы GK^*. Таким образом, мы получили следующую теорему.

Теорема 1.8.2. *Максимальная абелева нормальная подгруппа линейной максимальной разрешимой примитивной группы является мультипликативной подгруппой некоторого поля K, содержащегося в $\mathrm{M}_n(\mathbb{F})$ и $[K : \mathbb{F}]$ делит n.*

Лемма 1.8.3. *Если G — примитивная разрешимая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$ и H — это абелева нормальная подгруппа группы G, то $\mathrm{GL}_n(\mathbb{F})$ содержит разрешимую подгруппу $L \geq G$ такую, что некоторая максимальная абелева нормальная подгруппа D группы L содержит H и D является мультипликативной подгруппой некоторого поля $K \leq \mathrm{M}_n(\mathbb{F})$, где $[K : \mathbb{F}]$ делит n.*

Доказательство. Имеем $G \leq G_1 = GF_1$, где F_1 — мультипликативная подгруппа поля $K_1 = \mathcal{L}_{\mathbb{F}}(H)$. Если F_1 — максимальная абелева нормальная подгруппа группы G_1, то лемма доказана. В противном случае рассмотрим нормальную максимальную абелеву подгруппу H_1 группы G_1, удовлетворяющую условию $F_1 \leq H_1$. Далее построим группу $G_2 = G_1F_2$, где $F_2 = (\mathcal{L}_{\mathbb{F}}(H_1))^*$. Ясно, что $K_1 < K_2 = \mathcal{L}_{\mathbb{F}}(H_2)$. Продолжая данный процесс, получим ряд вложенных полей $K_1 < K_2 \ldots$ и $[K_i : \mathbb{F}]$ делит n. Значит, данный ряд конечен, что завершает доказательство леммы. □

Рассмотрим теперь примитивную разрешимую подгруппу G группы $\mathrm{GL}_n(\mathbb{F})$, содержащую абелеву нормальную подгруппу H такую, что H является мультипликативной подгруппой некоторого поля $K < \mathrm{M}_n(\mathbb{F})$ и $[K : \mathbb{F}] = m$ делит n. Рассмотрим $M = C_G(H)$.

Теорема 1.8.4. *Фактор группа G/M изоморфна некоторой разрешимой подгруппе группы $Gal(K : F)$.*

Доказательство. Предположим, что $g \in G$, $x, y \in K$, тогда $g^{-1}xg = x^g \in K$, $(x+y)^g = x^g + y^g$, $(xy)^g = x^g y^g$, $(\lambda E)^g = \lambda E$ для любого $\lambda \in \mathbb{F}$. Следовательно, $x \to x^g$ является изоморфизмом поля K и g оставляет неподвижным поле $\mathbb{F}$. Значит, мы можем рассмотреть гомоморфизм $\varphi : G \to Gal(K : F)$. Ядро данного гомоморфизма, очевидно, $C_G(K) = M$. □

Следствие 1.8.5. $|G : M| \leq |Gal(K : F)| \leq [K : \mathbb{F}]! = m!$.

Ввиду теоремы Клиффорда 1.3.4 мы имеем, что $\mathbb{F}^n = V = W_1 \oplus \ldots \oplus W_r$, где все W_i являются изоморфными неприводимыми H-подмодулями. Если $w_i \in W_i \setminus \{0\}$, то $W_i = w_i H = w_i K$, значит, $W_i \simeq K$ как векторное пространство над $\mathbb{F}$. Таким образом, $\mathbb{F}^n = K^r$ и $M \leq \mathrm{GL}_r(K)$. Действительно, если $x, y \in K^r$, $\alpha \in K$, то для любого $m \in M$ справедливо $(x+y)m = xm + ym$ и $(\alpha v)m = \alpha(vm)$, поскольку $M \leq C_{\mathrm{M}_n(\mathbb{F})}(H) = C_{\mathrm{M}_n(\mathbb{F})}(K)$.

Предположим теперь, что $M \neq H$ и рассмотрим абелеву подгруппу $A/H \leq M/H$ такую, что $A/H \trianglelefteq G/H$. Очевидно, что $H \leq Z(A)$. Однако мы выбрали H максимальной, значит, $H = Z(A)$.

Лемма 1.8.6. *Порядок любого элемента в фактор группе A/H является делителем числа $r = n/m$. Если aH — некоторый элемент из A/H порядка ν, то A содержит элемент b такой, что $|[a, b]| = |a^{-1}b^{-1}ab| = \nu$.*

Доказательство. Для любых $a, b \in A$ имеем $ab = hba$, $a^k b = h^k ba^k$, где $h \in H$. Также справедливо $\det(ab) = \det(hba)$, значит, $h^r = 1$, $a^r b = ba^r$, $a^r \in H$. Таким образом, $a^r \in Z(A) = H$ и $(aH)^r = H$.

Предположим теперь, что $|aH| = \nu$. Очевидно, что если $c, d \in A$, то $[a, c][a, d] = [a, cd]$. Кроме того, $[a, c] \in K$ и $[a, c]^r = 1$. Следовательно, $\langle [a, c] | c \in A \rangle$ является циклической конечной группой порядка τ и $[a^\tau, c] = [a, c]^\tau = 1$. Значит, ν делит τ. Обратно, $[a, c]^\nu = [a^\nu, c] = 1$, значит, τ делит ν и $\nu = \tau$. □

Лемма 1.8.7. $|A : H| = [\mathcal{L}(A) : K]$.

Доказательство. Если $a_1, \ldots, a_k$ — линейно независимые над K элементы из A, то они содержатся в различных смежных классах, поэтому $[\mathcal{L}_K(A) : K] \leqslant |A : H|$.

Рассмотрим теперь представителей различных смежных классов $d_1, d_2, \ldots, d_l$. Мы хотим показать, что они линейно независимы над K. Для любого $a \in A$ справедливо $a^{-1}d_i a = h_i d_i$, где $h_i \in H$. Кроме того, если $i \neq j$ можно найти $a \in A$, удовлетворяющий условию $h_i \neq h_j$. Действительно, предположим, что для любого $a \in A$ выполнено $h_i = h_j$, т. е. $h_i = d_i^{-1}a^{-1}d_i a = d_j^{-1}a^{-1}d_j a = h_j$. Значит, $[a, d_j^{-1}d_i] = 1$ и $d_j^{-1}d_i \in H$. Но это противоречит тому, что $d_1, \ldots, d_l$ — это представители различных смежных классов.

Предположим теперь, что $d_1, d_2, \ldots, d_l$ линейно зависимы над K. Возьмем нетривиальную линейную комбинацию $\lambda_1 d_1 + \lambda_2 d_2 + \ldots + \lambda_l d_l = 0$, в которой количество ненулевых коэффициентов минимально. Можно предполагать, что $\lambda_1 \neq 0$ и $\lambda_2 \neq 0$. Рассмотрим $a \in A$, удовлетворяющий условию $[a, d_1] = f_1 \neq f_2 = [a, d_2]$. Тогда

$$f_1(\lambda_1 d_1 + \lambda_2 d_2 + \ldots + \lambda_l d_l) - a^{-1}(\lambda_1 d_1 + \lambda_2 d_2 + \ldots + \lambda_l d_l)a = \\ = \lambda_2(f_1 - f_2)d_2 + \ldots + \lambda_l(f_1 - f_l)d_l = 0,\ \lambda_2(f_1 - f_2) \neq 0,$$

что противоречит выбору минимального количества ненулевых коэффициентов. □

Теорема 1.8.8. *Существуют элементы $a_1, b_1, a_2, b_2, \dots, a_t, b_t \in A$ такие, что:*
(i) $[a_i, b_i] = \epsilon_i$, где $\epsilon_i \in H$, $|\epsilon_i| = \nu_i = |a_iH| = |b_iH|$;
(ii) $[a_i, a_j] = [a_i, b_j] = [b_i, b_j] = 1$ если $i \neq j$;
(iii) для каждого $a \in A$ существует единственное представление в виде

$$a = h \cdot a_1^{\alpha_1} \cdot b_1^{\beta_1} \cdot \ldots \cdot a_t^{\alpha_t} \cdot b_t^{\beta_t}, h \in H, 0 \leqslant \alpha_i, \beta_i < \nu_i.$$

Доказательство. Рассмотрим $\nu_1 = \min\{|aH|, aH \in A/H \setminus H\}$. Тогда A содержит элементы a_1, b_1 такие, что $[a_1, b_1] = \epsilon_1$, где $|\epsilon_1| = \nu_1 = |a_1H| = |b_1H|$ (см. лемму 1.8.6). Далее A можно записать в виде $A = \langle a_1\rangle\langle b_1\rangle A_1$, где $A_1 = C_A(\langle a_1, b_1\rangle)$. Действительно, существует ν_1 элементов, сопряженных с a_1 и также существует ν_1 элементов, сопряженных с b_1. Следовательно, $|A : A_1| \leqslant \nu_1^2$. С другой стороны, все элементы $a_1^{\alpha_1}b_1^{\beta_1}$, $0 \leqslant \alpha_1, \beta_1 < \nu_1$ содержатся в различных смежных классов группы A относительно подгруппы A_1, поэтому $[a_1^{\alpha_1}b_1^{\beta_1}, b_1] = \epsilon_1^{\alpha_1}$ и $[a_1, a_1^{\alpha_1}b_1^{\beta_1}] = \epsilon^{\beta_1}$. Значит, $|A : A_1| = \nu_1^2$ и $A = \langle a_1\rangle\langle b_1\rangle A_1$. Если группа A_1 абелева, то $A_1 = H$, и теорема доказана.

Предположим, что $A_1 \neq H$ и $\nu_2 = \min\{|aH|, aH \in A_1/H \setminus H\}$. Ввиду леммы 1.8.6, существуют элементы $a_2, b_2 \in A_1$ такие, что $[a_2, b_2] = \epsilon_2$, где $\epsilon_2 \in H$ и $|\epsilon_2| = \nu_2$. Как и раньше мы имеем, что $A_1 = \langle a_2\rangle\langle b_2\rangle A_2$, где $A_2 = C_{A_1}(a_2, b_2)$. Группа A/H является конечной, следовательно, после конечного числа шагов мы получим $A = \langle a_1\rangle\langle b_1\rangle \ldots \langle a_t\rangle\langle b_t\rangle H$. □

Предположим теперь, что A/H — это нормальная максимальная абелева подгруппа группы G/H, удовлетворяющая условию $A/H \leq M/H$.

Теорема 1.8.9. *Если A/H — это нормальная максимальная абелева подгруппа группы G/H, удовлетворяющая условию $A/H \leq M/H$, то $C_{M/H}(A/H) = A/H$.*

Доказательство. Ввиду теоремы 1.8.8 мы имеем, что $A = \langle a_1\rangle\langle b_1\rangle \ldots \langle a_t\rangle\langle b_t\rangle H$, $[a_i, b_i] = \epsilon_i$, $[a_i, a_j] = [a_i, b_j] = [b_i, b_j] = 1$ если $i \neq j$, $|a_iH| = |b_iH| = |\epsilon_i| = \nu_i$. Рассмотрим $B/H = C_{M/H}(A/H)$ и $C = C_M(A)$. Очевидно, что $B > C \geq H$. Теперь покажем, что $B = AC$. Если $b \in B$, то $[a_i, b] \in H$. Следовательно, $[a_i^{\nu_i}, b] = [a_i, b]^{\nu_i} = 1$. Также, как и в доказательстве леммы 1.8.6, что $\{[a_i, x] | x \in B\}$ и $\{[b, b_i] | b \in B\}$ — это циклические группы, поэтому $[a_i, b] = \epsilon_i^{\beta_i}$ и $[b, b_i] = \epsilon_i^{\alpha_i}$, $i = 1, 2, \dots, t$.

С другой стороны, для $a = a_1^{\alpha_1}b_1^{\beta_1} \ldots a_t^{\alpha_t}b_t^{\beta_t}$ мы имеем $[a_i, a] = \epsilon_i^{\beta_i}$, $[a, b_i] = \epsilon_i^{\alpha_i}$, т. е. $[a_i, b] = [a_i, a]$ и $[b, b_i] = [a, b_i]$. Значит, $[a_i^{-1}, ab^{-1}] = [b_i, ab^{-1}] = 1$, $i = 1, \dots, t$. Следовательно, $a^{-1}b \in C$ и $B = AC$.

Предположим теперь, что $B/H > A/H$. Значит, существует нормальная подгруппа $D > A$ группы B такая, что фактор группа D/A абелева. Группа A/H является нормальной максимальной абелевой подгруппой, т. е. фактор группа D/H неабелева. Значит, существуют элементы $d, d_1 \in D$ такие, что $[d, d_1] \notin H$. Далее, $d = ac$, $d_1 = a_1c_1$, где $a, a_1 \in A$, $c, c_1 \in C$. Значит, $[d, d_1] = [ac, a_1c_1] = [a, a_1][c, c_1] \in C$. Кроме того, $[d, d_1] \in A$, значит мы имеем, что $[d, d_1] \in C \cap A = H$. Полученное противоречие завершает доказательство. □

Теорема 1.8.10. *Если G — разрешимая неприводимая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$, то существует нормальная абелева подгруппа H группы G такая, что $|G : H| < \infty$.*

Доказательство. Если G импримитивна, рассмотрим систему импримитивности $W_1, \dots, W_t$ такую, что все $G_1, \dots, G_t$ примитивны. Рассмотрим $L = \{g \in G | \forall i, W_ig = W_i\}$. Ясно, что $L \trianglelefteq G$, $L|_{W_i} \simeq G_i$ и $G/L \leq \mathrm{Sym}_t$. Если мы сумеем найти нормальные абелевы подгруппы A_i в группах G_i, удовлетворяющие условию $|G_i : A_i| < \infty$, то подгруппа $A \leq L$, удовлетворяющая условию $A|_{W_i} = A_i$ будет нормальной абелевой подгруппой группы G конечного индекса. Поэтому мы можем считать группу G примитивной.

Рассмотрим нормальную максимальную абелеву подгруппу X группы G. Ввиду леммы 1.8.3 существует примитивная разрешимая подгруппа D с нормальной абелевой подгруппой H такая, что $D \geq G$, $H \geq X$ и $H = K^*$ для некоторого поля $\mathrm{M}_n(\mathbb{F}) > K \geq \mathbb{F}$. Кроме того, по построению, $|D : H| \geq |G : X|$. Теперь $|D : H| = |D : M| \cdot |M : A| \cdot |A : H|$, где $M = C_D(H)$ и A/H — это абелева нормальная максимальная подгруппа группы M. Ввиду следствия 1.8.5 мы имеем, что $|D : M| < \infty$. Используя леммы 1.8.6 и 1.8.7, получаем, что $|A : H| < \infty$. Далее, по теореме 1.8.9, фактор группа M/A является подгруппой в $Aut(A/H)$, где A/H — абелева конечная группа. Следовательно, $|M : A| < \infty$ и $|D : H| < \infty$. □

Теорема 1.8.11. (Ли-Колчин-Мальцев). *Если $G \leq \mathrm{GL}_n(\mathbb{F})$ — разрешимая группа и поле $\mathbb{F}$ алгебраически замкнуто, то существует нормальная подгруппа H группы G конечного индекса, сопряженная с подгруппой группы треугольных матриц.*

Доказательство. Мы можем найти базис пространства V, в котором группа G будет иметь вид:

$$G = \left\{ \begin{pmatrix} G_1 & A_{1,2} & \dots & A_{1,t} \\ 0 & G_2 & A_{2,3} & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & G_t \end{pmatrix} \right\},$$

где все группы G_i неприводимы и разрешимы. Рассмотрим группы $L_i \leq \mathrm{GL}_n(\mathbb{F})$ такие, что $L_i|_{W_i} = G_i$ и $L_i|W_j = 1$. Ясно, что $L = L_1 \times \ldots \times L_t$ — это разрешимая подгруппа и $G^L = G$. Следовательно, GL — разрешимая группа и GL содержит матрицы того же вида, что и G. Следовательно, мы можем заменить группу G на GL. Ввиду теоремы 1.8.10, группа L содержит абелеву нормальную подгруппу A конечного индекса и, по теореме Клиффорда 1.3.4, группа A вполне приводима. Но $\mathbb{F}$ — алгебраически замкнутое поле, следовательно, группа A диагональна. Теперь рассмотрим унипотентный радикал $R_u(G) = U$ группы G. Имеем $GL/U \simeq L$. Следовательно $|G : AU| < \infty$. Но AU — это некоторая подгруппа группы треугольных матриц. $\square$

Глава 2. Системы корней и группы Вейля

В данной главе мы будем в основном следовать [3, Глава 2].

§1 Системы корней

Определение 2.1.1. Пусть V — это евклидово пространство размерности ℓ. Тогда для каждого ненулевого вектора $r \in V$ через w_r мы обозначим *отражение относительно гиперплоскости ортогональной вектору* r. Это линейное преобразование определённое правилом $w_r(r) = -r$ и $w_r(x) = x$ для всех векторов x ортогональных вектору r. Для произвольного вектора $v \in V$ мы имеем

$$w_r(x) = x - \frac{2(r,x)}{(r,r)} \cdot r.$$

Определение 2.1.2. Подмножество Φ евклидового пространства V называется *корневой системой* если выполнены следующие аксиомы:

1. Φ является конечным множеством ненулевых векторов.
2. Φ порождает пространство V.
3. Если $r, s \in \Phi$, то $w_r(s) \in \Phi$.
4. Если $r, s \in \Phi$, то $2(r,s)/(r,r)$ целое.
5. Если $r, \lambda r \in \Phi$, где $\lambda \in \mathbb{R}$, то $\lambda = \pm 1$.

Заметим, что из третьей аксиомы следует что если $r \in \Phi$, то и $-r \in \Phi$. Элементы корневой системы Φ называются *корнями*. Размерность ℓ векторного пространства V называется *рангом* корневой системы Φ.

Пусть Φ — корневая система. Через $W(\Phi)$ обозначим группу порождённую отражениями w_r для всех $r \in \Phi$. Группа $W(\Phi)$ называется *группой Вейля* корневой системы Φ. Ввиду третьей аксиомы, каждый элемент из $W(\Phi)$ оставляет корневую систему Φ инвариантной. Кроме того, ввиду второй аксиомы, $W(\Phi)$ действует точно на Φ. Поскольку Φ — конечное множество, отсюда следует, что $W(\Phi)$ — конечная группа.

Далее мы построим в корневой системе Φ подмножество Π, которое состоит из линейно независимых векторов и любой корень из Φ представим в виде линейной комбинации элементов из Π, все коэффициенты которой либо неотрицательны, либо неположительны. Такая подсистема Π называется *фундаментальной системой* .

Снабдим пространство V полным порядком, удовлетворяющим следующим условиям:

1. Если $v \in V^+$ и $\lambda > 0$, то $\lambda v \in V^+$.
2. Если $v_1, v_2 \in V^+$, то и $v_1 + v_2 \in V^+$.
3. Для любого $v \in V$ либо $v \in V^+$, либо $v \in (-V^+) = V^-$, либо $v = 0$.

Подобное упорядочение можно взять, например, выбрав базис $v_1, \ldots, v_\ell$ пространства V и положив $v \in V^+$ в том и только в том случае, когда первый из ненулевых коэффициентов в разложении $v = \lambda_1 v_1 + \ldots + \lambda_\ell v_\ell$ больше нуля.

Определим теперь порядок $\succ$, полагая $v_1 \succ v_2$ если $v_1 - v_2 \in V^+$. Ясно что $\succ$ дает нам линейный порядок на V согласованный со сложением и умножением на скаляр из $\mathbb{R}$. Подмножество $\Phi \cap V^+$ назовем *положительной системой корней* и обозначим её через Φ^+. Теперь мы докажем существование фундаментальной системы корней в Φ.

Лемма 2.1.3. *Любая положительная система корней в Φ содержит фундаментальную систему.*

Доказательство. Пусть Φ^+ — это положительная система в Φ. Тогда существует некоторый полный порядок на V для которого $\Phi^+ = \Phi \cap V^+$. Пусть Π — это подмножество множества Φ^+, удовлетворяющее условиям:

1. Любой корень в Φ^+ является линейной комбинацией корней из Π с неотрицательными коэффициентами.

2. Никакое подмножество множества Π не удовлетворяет (1).

Такое подмножество существует, поскольку само множество Φ^+ удовлетворяет (1). Мы покажем, что подмножество Π, удовлетворяющее (1) и (2) является фундаментальной системой. Для этого достаточно доказать, что Π линейно независимо.

Докажем сначала, что $(r, s) \leqslant 0$ для любых двух различных корней r, s из Π. Предположим противное: $(r, s) > 0$. Тогда $w_r(s) = s - \lambda r$ для некоторого $\lambda > 0$. Если $w_r(s) \in \Phi^+$ мы имеем $w_r(s) = \sum_{r_i \in \Pi} \alpha_i r_i$, где каждый $\alpha_i \geqslant 0$. Таким образом, $s = \lambda r + \sum_{r_i \in \Pi} \alpha_i r_i$, $\lambda > 0$, $\alpha_i \geqslant 0$. Коэффициент, стоящий перед s в правой части должен быть меньше 1, так как в противном случае $0 = \lambda r + \sum_{r_i \in \Pi} \alpha_i r_i - s \in V^+$. Следовательно, s представим в виде линейной комбинации остальных корней из Π с неотрицательными коэффициентами, что противоречит минимальности Π.

Если теперь $-w_r(s) = \sum_{r_i \in \Pi} \alpha_i r_i$ с неотрицательными α_i, то $\lambda r = s + \sum_{r_i \in \Pi} \alpha_i r_i$, $\lambda > 0$, $\alpha_i \geqslant 0$ и мы вновь приходим к противоречию с минимальностью Π.

Если теперь некоторая линейная комбинация элементов из Π равна 0, то её можно записать в виде $\sum \alpha_i r_i = \sum \beta_i s_i$, где $\alpha_i > 0$, $\beta_i > 0$ и r_i, s_i — различные элементы из Π. Пусть $v = \sum \alpha_i r_i = \sum \beta_i s_i$. Тогда $(v, v) = \sum_{i,j} \alpha_i \beta_j (r_i, s_j) \leqslant 0$. Следовательно, $v = 0$. Поскольку $r_i, s_i \in V^+$ это сразу влечёт, что $\alpha_i = 0$ и $\beta_j = 0$ для всех i, j, так как в противном случае $0 = \sum_i \alpha_i r_i \in V^+$. $\square$

Лемма 2.1.4. *Любая положительная система корней из Φ содержит в точности одну фундаментальную систему. Таким образом, существует взаимнооднозначное соответствие между положительными системами и фундаментальными системами в Φ.*

Доказательство. Пусть $\{r_1, r_2, \ldots, r_\ell\}$ и $\{s_1, s_2 \ldots, s_\ell\}$ — две фундаментальные системы в Φ^+. Тогда $r_i = \sum_{j=1}^{\ell} \alpha_{ij} s_j$, $s_i = \sum_{j=1}^{\ell} \beta_{ij} r_j$, где $\alpha_{ij} \geqslant 0$, $\beta_{ij} \geqslant 0$ и матрицы, составленные из α_{ij} и β_{ij} являются взаимно обратными. Для любого i существует j такое, что $\alpha_{ij} \neq 0$. Поскольку $\sum_{m=1}^{\ell} \alpha_{im} \beta_{mk} = 0$ для всех $k \neq i$, мы имеем, что $\beta_{jk} = 0$ для всех $k \neq i$. Следовательно, $\beta_{ji} \neq 0$. В силу симметрии отсюда следует, что $\alpha_{ik} = 0$ для $k \neq j$. Таким образом, (α_{ij}) — мономиальная матрица. После перенумерации корней $s_1, s_2, \ldots, s_\ell$ можно считать, что (α_{ij}) — диагональная матрица. Поскольку $r_i, s_i \in \Phi^+$, мы имеем $\alpha_{ii} > 0$ для всех i. В силу свойства (5) корневых систем мы имеем $\alpha_{ii} = 1$ для всех i. $\square$

Следствие 2.1.5. *Если $\Pi = \{r_1, r_2, \ldots, r_\ell\}$ — фундаментальная система в Φ, то $(r_i, r_j) \leqslant 0$ для всех $i \neq j$.*

Доказательство. Следствие справедливо для фундаментальной системы, построенной при доказательстве леммы 2.1.3. Ввиду леммы 2.1.4 любая фундаментальная система получается таким образом. $\square$

Выберем теперь фундаментальную систему Π и соответствующую положительную систему Φ^+, и зафиксируем их для последующих рассуждений. Корни из Φ^+ будут называться *положительными корнями*, а остальные корни будут называться *отрицательными*. Корни из Π будут называться *фундаментальными*. Множество отрицательных корней обозначим через Φ^-.

Лемма 2.1.6. *Пусть $r \in \Pi$. Тогда w_r переводит r в $-r$, но любой другой положительный корень переводит в положительный корень.*

Доказательство. Пусть $s \in \Phi^+$ и $s \neq r$. Тогда $s = \sum_{r_i \in \Pi} \alpha_i r_i$ и $\alpha_i \geqslant 0$. Ввиду пятого свойства системы корней, существует $r_i \neq r$ для которого $\alpha_i > 0$. Коэффициент корня r_i в $w_r(s)$, следовательно, также положительный. Значит, $w_r(s) \in \Phi^+$. $\square$

Лемма 2.1.7. *Любой корень из Φ является линейной комбинацией корней из Π с целыми коэффициентами.*

Доказательство. Лемму достаточно доказать лишь для векторов из Φ^+. Пусть $r \in \Phi^+$. Если $r \in \Pi$, то результат, очевидно, верен, поэтому мы предполагаем, что $r \notin \Pi$. Тогда $r = \sum_{r_i \in \Pi} \lambda_i r_i$, где все $\lambda_i \geqslant 0$ и по крайней мере два из них положительные. Далее существует $r_i \in \Pi$ для которого $(r_i, r) > 0$. Действительно, если бы для всех r_i выполнялось $(r_i, r) \leqslant 0$, мы бы получили $(r, r) = \sum \lambda_i (r_i, r) \leqslant 0$, т. е. $r = 0$. Выберем теперь $r_i \in \Pi$ удовлетворяющий условию $(r_i, r) > 0$. Тогда $w_{r_i}(r) = r - \frac{2(r_i, r)}{(r_i, r_i)} r_i$. Корень $w_{r_i}(r)$ представленный в виде линейной комбинации фундаментальных корней, отличается от r лишь в одном коэффициенте. Следовательно, по крайней мере один из коэффициентов корня $w_{r_i}(r)$ положительный и, значит, $w_{r_i}(r) \in \Phi^+$.

Определим *высоту корня* r через $h(r) = \sum \lambda_i$. Тогда $h(w_{r_i}(r)) < h(r)$. Таким образом, для каждого положительного корня, неявляющегося фундаментальным, существует другой положительный корень меньшей высоты. Следовательно, положительные корни минимальной высоты — это в точности фундаментальные корни и их высота равна 1.

Докажем теперь лемму индукцией по высоте корня. Она, очевидно, выполняется для корней высоты 1. Для данного корня $r \in \Phi^+ \setminus \Pi$ выберем как и раньше $r_i \in \Pi$ такой, что $(r, r_i) > 0$. Тогда $w_{r_i}(r)$ является целочисленной комбинацией корней из Π по индукции. Следовательно, r также является целочисленной комбинацией корней из Π, поскольку $r = w_{r_i}(r) + \frac{2(r_i, r)}{(r_i, r_i)} r_i$ и $\frac{2(r_i, r)}{(r_i, r_i)}$ целое ввиду свойства (4) системы корней. □

Следствие 2.1.8. *В базисе* Π *пространства* V *каждый элемент из* W *представим в виде матрицы с целыми коэффициентами.*

Доказательство. Если $r_i \in \Pi$, то $w(r_i) \in \Phi$, следовательно, является линейной комбинацией фундаментальных корней с целыми коэффициентами. □

Лемма 2.1.9.

1. *Любой корень из* Φ *является образом некоторого корня из* Π *относительно некоторого элемента из* W.
2. W *порождена отражениями* $w_r, r \in \Pi$.

Отражения $w_r, r \in \Pi$ называются *фундаментальными отражениями*.

Доказательство. Пусть W_0 — подгруппа группы W, порождённая фундаментальными отражениями. Мы покажем, что каждый корень из Φ имеет вид $w(s)$ для некоторого $w \in W_0$, $s \in \Pi$. Пусть $r \in \Phi^+$. Если $h(r) = 1$, доказывать нечего. Если теперь $h(r) > 1$, то существует корень $r_i \in \Pi$ такой, что $(r_i, r) > 0$. Тогда $w_{r_i}(r) \in \Phi^+$ и $h(w_{r_i}(r)) < h(r)$ (см. доказательство леммы 2.1.7). По индукции $w_{r_i}(r) = w'(s)$ для некоторого $w' \in W_0$ и $s \in \Pi$. Следовательно, $r = w_{r_i} w'(s)$ и $w_{r_i} w \in W_0$. Отрицательные корни можно записать следующим образом: $-r = w_{r_i} w'(-s) = w_{r_i} w' w_s(s)$ и $w_{r_i} w' w_s \in W_0$.

Покажем теперь, что $W_0 = W$. Поскольку W порождена отражениями w_r при $r \in \Phi$, достаточно доказать, что $w_r \in W_0$. В силу доказанного выше, $r = w(s)$ для некоторого $s \in \Pi$, $w \in W_0$. Следовательно, $w_r = w w_s w^{-1}$. Действительно,

$$w w_s w^{-1}(x) = w\left(w^{-1}(x) - \frac{2(s, w^{-1}(x))}{(s, s)} s\right) = x - \frac{2(r, x)}{(r, r)} r = w_r(x).$$

Следовательно, $w_r \in W_0$. □

§2 Функция длины

В лемме 2.1.9 мы доказали, что любой элемент из W может быть представлен в виде произведения фундаментальных отражений w_r, где $r \in \Pi$. Обозначим через $l(w)$ минимальную длину такого представления. Определим также функцию $n(w) = |\Phi^+ \cap \Phi^- w^{-1}|$, т. е. $n(w)$ — это количество положительных корней, которые элемент w переводит в отрицательные. Наша задача доказать, что $n(w) = l(w)$.

Лемма 2.2.1. *Пусть* $r \in \Pi$ *и* $w \in W$. *Тогда*

1. $n(w_r w) = n(w) + 1$ *если* $w^{-1}(r) \in \Phi^+$.
2. $n(w_r w) = n(w) - 1$ *если* $w^{-1}(r) \in \Phi^-$.
3. $n(w w_r) = n(w) + 1$ *если* $w(r) \in \Phi^+$.
4. $n(w w_r) = n(w) - 1$ *если* $w(r) \in \Phi^-$.

Доказательство. Ввиду леммы 2.1.6, элемент w_r меняет знак лишь у двух корней: r и $-r$. Таким образом, $n(w_r w) = n(w) \pm 1$ и $n(ww_r) = n(w) \pm 1$. Далее, $n(w_r w) = n(w)+1$ в том и только в том случае, если $r \in w(\Phi^+)$, что доказывает (1) и (2), и $n(ww_r) = n(w)+1$ в том и только в том случае, когда $w(r) \in \Phi^+$, что доказывает (3) и (4). □

Покажем теперь, что $l(w) = n(w)$.

Теорема 2.2.2. *Минимальная длина разложения элемента w в виде произведения фундаментальных отражений равна количеству положительных корней, которые элемент w переводит в отрицательные.*

Доказательство. Пусть w — какой-нибудь элемент из W и $l(w) = k$. Тогда w представим в виде $w_{r_1} \cdot w_{r_2} \cdot \ldots \cdot w_{r_k}$, $r_i \in \Pi$. По лемме 2.2.1 мы имеем $n(w) \leqslant n(w_{r_1} w) + 1 \leqslant n(w_{r_2} w_{r_1} w) + 2 \leqslant \ldots \leqslant k$. Таким образом, $n(w) \leqslant l(w)$.

Предположим теперь, что $n(w) < k$. Тогда, по лемме 2.2.1(3) существует $j \leqslant k-1$ такое, что

$$w_{r_1} w_{r_2} \ldots w_{r_j}(r_{j+1}) \in \Phi^-.$$

Следовательно, существует некоторое $i < j$ такое, что $w_{r_{i+1}} \ldots w_{r_j}(r_{j+1}) \in \Phi^+$ и $w_{r_i} w_{r_{i+1}} \ldots w_{r_j}(r_{j+1}) \in \Phi^-$. Поскольку w_{r_i} меняет знак лишь у r_i и $-r_i$, отсюда следует $w_{r_{i+1}} \ldots w_{r_j}(r_{j+1}) = r_i$. При доказательстве леммы 2.1.9 была получена формула $w_s = w w_r w^{-1}$ если $w(r) = s$. Поэтому $w_{r_i} = w_{r_{i+1}} \ldots w_{r_j} w_{r_{j+1}} w_{r_j} \ldots w_{r_{i+1}}$ и, значит, $w_{r_{i+1}} \ldots w_{r_{j+1}} = w_{r_i} \ldots w_{r_j}$. Используя данное соотношение мы можем теперь сократить разложение элемента w:

$$w = w_{r_1} \ldots w_{r_k} = w_{r_1} \ldots w_{r_i} w_{r_i} \ldots w_{r_j} w_{r_{j+2}} \ldots w_{r_k} = w_{r_1} \ldots w_{r_{i-1}} w_{r_{i+1}} \ldots w_{r_j} w_{r_{j+2}} \ldots w_{r_k}.$$

Таким образом, мы сумели найти разложение элемента w в виде произведения $k-2$ фундаментальных отражений. Полученное противоречие завершает доказательство. □

Следствие 2.2.3. *Если некоторый элемент $w \in W$ удовлетворяет условию $w(\Pi) = \Pi$, то $w = 1$.*

Доказательство. Если $w(\Pi) = \Pi$, то $w(\Phi^+) = \Phi^+$ и, значит, $n(w) = l(w) = 0$, т. е. $w = 1$. □

Теперь мы обсудим связь между различными фундаментальными системами в Φ.

Теорема 2.2.4. *Если Π — это фундаментальная система в Φ, то $w(\Pi)$ — также является фундаментальной системой для любого $w \in W$. Более того, для данных двух фундаментальных систем Π_1 и Π_2 существует в точности один элемент $w \in W$ такой, что $w(\Pi_1) = w(\Pi_2)$.*

Доказательство. Пусть Φ^+ — это положительная система, содержащая Π. Тогда $\Phi^+ = \Phi \cap V^+$ для некоторого полного порядка на V. Очевидно, что $w(V^+)$ также определяет полный порядок на V и положительными корнями относительно этого порядка являются корни $w(\Phi^+) = \Phi \cap w(V^+)$. Так как w линейно, $w(\Pi)$, очевидно, является фундаментальной системой в $w(\Phi^+)$.

Покажем теперь, что для любых двух фундаментальных систем Π_1 и Π_2 существует некоторый элемент $w \in W$ для которого $w(\Pi_1) = \Pi_2$. Пусть Φ_1^+ и Φ_2^+ — положительные системы, содержащие Π_1 и Π_2 соответственно. Будем использовать индукцию по $n = |\Phi_1^+ \cap \Phi_2^-|$. Если $n = 0$, то $\Phi_1^+ = \Phi_2^+$ и, значит, $\Pi_1 = \Pi_2$. Таким образом, мы можем предполагать, что $n > 0$. Тогда $\Pi_1 \cap \Phi_2^-$ непусто. Пусть $r \in \Pi_1 \cap \Phi_2^-$. Тогда $(\Phi_1^+)w_r$ — это множество корней, полученных из Φ^+ заменой корня r на корень $-r$. Следовательно, $|(\Phi_1^+)w_r \cap \Phi_2^-| = n-1$. Далее, по уже доказанному, $w_r(\Pi_1)$ — это фундаментальная система для $w_r(\Phi_1^+)$, следовательно, по индукции существует $w' \in W$ такой, что $w' w_r(\Pi_1) = \Pi_2$. Таким образом, $w(\Pi_1) = \Pi_2$, где $w = w' w_r$.

Докажем теперь единственность элемента w. Предположим, что $w_1(\Pi_1) = \Pi_2$ и $w_2(\Pi_1) = \Pi_2$. Тогда $w_2^{-1} w_1(\Pi_1) = \Pi_1$, следовательно, $w_2^{-1} w_1(\Phi_1^+) = \Phi_1^+$ и, в силу следствия 2.2.3, $w_2^{-1} w_1 = e$. □

Следствие 2.2.5. *Количество фундаментальных систем в Φ равно порядку группы W.*

Лемма 2.2.6. *Пусть Φ^+ — положительная система в Φ и Φ^- — соответствующая отрицательная система. Тогда существует единственный элемент $w_0 \in W$ такой, что $w_0(\Phi^+) = \Phi^-$. Более того, $|w_0| = 2$.*

Доказательство. Пусть Φ^+ — положительная система в Φ, соответствующая некоторому полному порядку на V и Φ^- — положительная система, соответствующая обратному порядку. Ввиду лемм 2.1.4 и 2.2.4 существует единственный элемент $w_0 \in W$ такой, что $w_0(\Phi^+) = \Phi^-$. Поскольку $w_0^2(\Phi^+) = \Phi^+$, мы имеем $w_0^2 = e$. □

Определение 2.2.7. Элемент w_0, определенный в лемме 2.2.6, является *элементом наибольшей длины* в группе W. Он единственный и, ввиду теоремы 2.2.2, его длина $l(w) = |\Phi^+|$.

§3 Параболические подгруппы в группе Вейля

В данном параграфе мы обсудим некоторые подгруппы группы Вейля, которые сами являются группами Вейля для некоторых подсистем корневой системы Φ. Пусть Π — фундаментальная система в Φ и Φ^+ — соответствующая ей положительная система. Пусть J — подмножество в Π. Определим V_J как подпространство пространства V, натянутое на J; $\Phi_J = V_J \cap \Phi$ и W_J — подгруппа группы W, порождённая отражениями в корнях $r \in J$.

Лемма 2.3.1. *Подмножество Φ_J является корневой системой в V_J. Множество J является фундаментальной системой в Φ_J. Группа W_J является группой Вейля для Φ_J.*

Доказательство. По построению Φ_J порождает V_J. Если $r, s \in \Phi_J$, то элемент $w_r(s) = s - \frac{2(r,s)}{(r,r)}r$ также лежит в Φ_J. Таким образом, Φ_J является корневой системой в V_J.

Далее, J линейно независимое множество и любой корень из Φ_J является линейной комбинацией элементов из J. Поскольку J является подмножеством множества Π, коэффициенты в такой линейной комбинации должны быть либо все неотрицательные, либо все неположительные. Таким образом, J является фундаментальной системой в Φ_J. Группа Вейля для корневой системы Φ_J порождена фундаментальными отражениями (см. лемму 2.1.9), следовательно, совпадает с W_J. □

Определение 2.3.2. Подгруппы W_J и сопряженные с ними называются *параболическими подгруппами* группы W.

Лемма 2.3.3. *Подгруппы W_J различны для различных подмножеств J множества* Π.

Доказательство. Пусть J, K — различные подмножества из Π и предположим, что $W_J = W_K$. Без ограничения общности можно предположить, что существует корень $r \in K \setminus J$. Тогда мы имеем $w_r(x) - x = -\frac{2(r,x)}{(r,r)}r$. Далее $w_r \in W_J$ и, значит, $w_r(x) - x \in V_J$ для всех $x \in V$. Выбирая x таким образом, что $(r, x) \neq 0$ мы получаем $r \in V_J$. Ясно, что такой x может быть выбран, поскольку $w_r \in W_J$ и существует вектор, который элемент w_r не стабилизирует. Но свойство $r \in V_J$ противоречит линейной независимости фундаментальной системы. □

Лемма 2.3.4. *Пусть $v \in V$ и $w \in W$ выбраны так, что $w(v) = v$ и $(r, v) \geqslant 0$ для всех корней из* Π. *Тогда $w \in W_J$, где J — множество корней из* Π *ортогональных вектору v.*

Доказательство. Используем индукцию по $l(w)$. Если $l(w) = 0$ результат очевиден. Если $l(w) > 0$, то существует корень $r \in \Pi$ такой, что $w(r) \in \Phi^-$. Тогда $0 \leqslant (r, v) = (w(r), w(v)) = (w(r), v) \leqslant 0$, поскольку $(s, v) \geqslant 0$ для любого $s \in \Pi$. Следовательно, $(r, v) = 0$ и $w_r(v) = v$. Теперь $ww_r(v) = v$ и $l(ww_r) = l(w) - 1$ (см. лемму 2.2.1). Таким образом по индукции, $ww_r \in W_J$ и $w \in W_J$. □

Следствие 2.3.5. *Пусть v — произвольный вектор из V и w — элемент из W такой, что $w(v) = v$. Тогда w является произведением отражений, соответствующих корням ортогональным вектору v.*

Доказательство. Пусть $v \in V$ — некоторый вектор. Рассмотрим множество $\{w(v) | w \in W\}$ и пусть v' — максимальный элемент этого множества относительно порядка $\prec$ (порядок, используемый, для построения Φ^+ и Π). Тогда для любого $r \in \Pi$ справедливо $w_r(v') \preceq v'$, т. е. $w_r(v') = v' - \frac{2(r,v')}{(r,r)}r \prec v'$ и $(r, v') \geqslant 0$. Поэтому для вектора v выполнены условия леммы 2.3.4 если в качестве фундаментальной системы корней взять систему $(\Pi)w^{-1}$ (по теореме 2.2.4, $(\Pi)w^{-1}$ вновь является фундаментальной системой). □

Теорема 2.3.6. *Пусть $w \in W$ и U — подпространство пространства V состоящее из всех векторов, неподвижных относительно w. Тогда w является произведением отражений, соответствующих корням, лежащим в ортогональном дополнении $U^\perp$ к подпространству U.*

Доказательство. Пусть $v_1, \ldots, v_k$ — базис подпространства U. Нам нужно показать, что w является произведением отражений, соответствующих корням, ортогональным к $v_1, \ldots, v_k$. Докажем это индукцией по k. Для $k = 1$ утверждение справедливо ввиду следствия 2.3.5.

Выберем фундаментальную систему Π таким образом, чтобы $(r, v_k) \geqslant 0$ для любого $r \in \Pi$ (как выбрать такую систему мы обсуждали в доказательстве следствия 2.3.5) и пусть J — это множество фундаментальных корней, ортогональных вектору v_k. Рассмотрим разложение $V = V_J \oplus V_J^\perp$ и пусть $v_i = v_i' + v_i''$, где

$v_i' \in V_J$ и $v_i'' \in V_J^{\perp}$. Далее по лемме 2.3.4, $w \in W_J$ и, следовательно, $w(v_i'') = v_i''$. Поскольку $w(v_i) = v_i$, отсюда следует, что $w(v_i') = v_i'$. Теперь W_J — это группа Вейля, действующая на V_J и элемент $w \in W_J$ оставляет неподвижными векторы $v_1', v_2', \ldots, v_{k-1}'$. По индукции, w является произведением отражений, соответствующих корням из V_J, ортогональным $v_1', \ldots, v_{k-1}'$. Эти корни ортогональны также векторам $v_1, \ldots, v_k$, что завершает доказательство теоремы. □

Теорема 2.3.7. *Пусть J, K — подмножества фундаментальной системы* Π. *Тогда* $\langle W_J, W_K \rangle = W_{J\cup K}$ *и* $W_J \cap W_K = W_{J\cap K}$.

Доказательство. РРавенство $\langle W_J, W_K \rangle = W_{J\cup K}$ очевидно следует из определения параболических подгрупп. Докажем теперь, что $W_J \cap W_K = W_{J\cap K}$.

Включение $W_J \cap W_K \supseteq W_{J\cap K}$ очевидно. Докажем теперь обратное включение. Пусть $w \in W_J \cap W_K$. Тогда $w(v) = v$ для всех $v \in V_J^{\perp}$ и для всех $v \in V_K^{\perp}$. Таким образом, w оставляет неподвижным любой вектор из $V_J^{\perp} + V_K^{\perp}$. Далее $V_J^{\perp} + V_K^{\perp} \subseteq V_{J\cap K}^{\perp}$. Кроме того,

$$\dim(V_J^{\perp} + V_K^{\perp}) = \dim V_J^{\perp} + \dim V_K^{\perp} - \dim(V_J^{\perp} \cap V_K^{\perp}) = \dim V_J^{\perp} + \dim V_K^{\perp} - \dim(V_J + V_K)^{\perp} =$$
$$\ell - \dim V_J + \ell - \dim V_K - \ell + \dim(V_J + V_K) = \ell - \dim(V_J \cap V_K) = \ell - \dim V_{J\cap K} = \dim V_{J\cap K}^{\perp}.$$

(Напомним, что $\ell = \dim V$.) Следовательно, $V_j^{\perp} + V_K^{\perp} = V_{J\cap K}^{\perp}$. Таким образом, w оставляет неподвижным любой вектор из $V_{J\cap K}^{\perp}$, значит, является произведением отражений, сооответствующим корням из $V_{J\cap K}$ ввиду теоремы 2.3.6. Следовательно, $w \in W_{J\cap K}$. □

Следствие 2.3.8. *Подгруппы W_J группы W образуют решётку из 2^{ℓ} подгрупп.*

Далее мы обсудим некоторый естественный способ выбора системы представителей левых смежных классов wW_J подгруппы W_J в группе W. Пусть D_J — это множество элементов $w \in W$ таких, что $w(r) \in \Phi^+$ для всех $r \in J$. Тогда D_J — это подмножество, хотя и необязательно подгруппа в W.

Теорема 2.3.9. *Пусть J — подмножество фундаментальной системы* Π. *Тогда любой элемент из W представим единственным образом в виде $w = d_J w_J$, где $d_J \in D_J$ и $w_J \in W_J$. Более того, $l(w) = l(d_J) + l(w_J)$.*

Доказательство. Покажем сначал, что любой элемент $w \in W$ представим в виде $w = d_J w_J$, где $d_J \in D_J$, $w_J \in W_J$ и $l(w) = l(d_J) + l(w_J)$. Если $l(w) = 0$, т. е. $w = e$, то $e = e \cdot e$ — требуемая факторизация. Таким образом, можно предполагать, что $l(w) > 0$ и использовать индукцию по $l(w)$. Если $w \in D_J$, то $w = w \cdot e$ — требуемая факторизация. Если $w \notin D_J$, то существует фундаментальный корень $r \in J$ такой, что $w(r) \in \Phi^-$. Тогда $l(ww_r) = l(w) - 1$ (см. лемму 2.2.1). По индукции $ww_r = d_J \cdot w_J$ и $l(d_J) + l(w_J) = l(ww_r)$. Таким образом, $w = d_J w_J w_r$, где $d_J \in D_J$, $w_J w_r \in W_J$ и $l(d_J) + l(w_J) + 1 = l(w)$. Теперь $l(w_J w_r) \leqslant l(w_J) + 1$, однако, если бы $l(w_J w_r) \lneq l(w_J) + 1$, то тогда мы бы получили разложение элемента w в виде произведения менее чем $l(w)$ фундаментальных отражений. Следовательно, $l(w_J w_r) = l(w_J) + 1$ и $l(w) = l(d_J) + l(w_J w_r)$.

Докажем теперь единственность разложения $w = d_J w_J$. Предположим, что мы имеем $d_J w_J = d_J' w_J'$, где $d_J, d_J' \in D_J$ и $w_J, w_J' \in W_J$. Тогда $d_J' = d_J w_J (w_J')^{-1}$. Предположим, что $w_J (w_J')^{-1} \neq 1$. Ввиду леммы 2.3.1, W_J является группой Вейля для корневой системы Φ_J с фундаментальной системой J. Таким образом, существует $r \in J$ такой, что $w_J (w_J')^{-1}(r) \in \Phi_J^-$, следовательно, $d_J w_J (w_J')^{-1}(r) \in \Phi^-$. Однако $d_J'(r) \in \Phi^+$. Полученное противоречие завершает доказательство теоремы. □

Следствие 2.3.10. *В каждом смежном классе wW_J лежит в точности один элемент из D_J. Его длина меньше длины любого другого элемента из wW_J.*

§4 Матрица Картана и диаграмма Дынкина

Напомним, что ввиду свойства (4) из определения корневой системы, для любых двух $r, s \in \Phi$ число $\frac{2(r,s)}{(r,r)}$, которое мы будем в дальнейшем обозначать $< r, s >$ целое. Сейчас мы дадим геометрическую интерпретацию этого числа.

Пусть p_i, p_j — два различных фундаментальных корня и θ_{ij} — угол между ними. Поскольку $(p_i, p_j) \leqslant 0$ для любых двух фундаментальных корней (см. следствие 2.1.5), мы получаем, что $< p_i, p_j >= -q \leqslant 0$ для любых двух фундаментальных корней. В частности, угол θ_{ij} всегда тупой. Существует весьма ограниченное

количество возможных значений для угла θ_{ij}. Действительно, так как $< p_i, p_j >$ и $< p_j, p_i >$ — целые числа, то число

$$\frac{4(p_i, p_j)}{(p_i, p_i)(p_j, p_j)} = 4\cos^2\theta_{ij}$$

также целое. Поскольку $0 \leqslant \cos^2\theta_{ij} \leqslant 1$, мы получаем, что $4\cos^2\theta_{ij} \in \{0, 1, 2, 3, 4\}$. В силу линейной независимости корней p_i, p_j, выполнено неравенство $\cos^2\theta_{ij} \neq 1$, таким образом $4\cos^2\theta_{ij} \in \{0, 1, 2, 3\}$. Обозначим $n_{ij} = 4\cos^2\theta_{ij}$. Получаем, что n_{ij} допускает разложение в виде произведения двух целых неположительных чисел $< p_i, p_j >$ и $< p_j, p_i >$. Рассмотрим теперь возможные значения числа n_{ij}.

1. $n_{ij} = 1$. Тогда $< p_i, p_j > = < p_j, p_i > = -1$. Таким образом, $(p_i, p_i) = (p_j, p_j)$ и корни p_i, p_j имеют одинаковую длину, а угол $\theta_{ij} = \frac{2\pi}{3}$.

2. $n_{ij} = 2$. Тогда одно из $< p_i, p_j >$, $< p_j, p_i >$ равно -1, а второе равно -2, т. е. один из корней в $\sqrt{2}$ раз длиннее другого, а угол $\theta_{ij} = \frac{3\pi}{4}$.

3. $n_{ij} = 3$. Тогда одно из $< p_i, p_j >$, $< p_j, p_i >$ равно -1, а второе равно -3, т. е. один из корней в $\sqrt{3}$ раз длиннее другого, а угол $\theta_{ij} = \frac{5\pi}{6}$.

4. $n_{ij} = 0$ и никакой информации об относительной длине корней получить нельзя.

Обозначим числа $< p_i, p_j > = A_{ij}$, полагая $A_{ii} = 2$ для всех i. Матрица A, составленная из чисел A_{ij} называется *матрицей Картана* для корневой системы Φ. По фундаментальной системе Π мы можем построить граф, называемый *диаграммой Дынкина* следующим образом: вершины этого графа - это фундаментальные корни $\{p_1, \ldots, p_\ell\}$ и вершины p_i, p_j соединены n_{ij} ребрами. Кроме того, в случае существования корней различной длины, указано, какой из корней длиннее.

Определение 2.4.1. Система корней называется *неразложимой*, если её нельзя представить в виде объединения собственных взаимноортогональных подмножеств. Очевидно, что система является неразложимой в том и только в том случае, когда её диаграмма Дынкина связна.

Определение 2.4.2. Две системы корней Φ_1 и Φ_2 называются *эквивалентными*, если существует биекция $\alpha : \Phi_1 \to \Phi_2$ такая, что $(\alpha(r), \alpha(s)) = \lambda(r, s)$ для некоторого ненулевого скаляра λ, независящего от r, s.

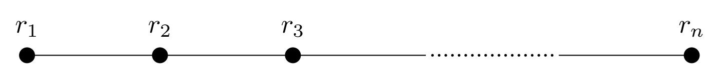
Заметим, что по связной диаграмме Дынкина (или по матрице Картана) можно полностью восстановить неразложимую систему корней с точностью до эквивалентности. Действительно, взяв один из фундаментальных корней произвольным образом, остальные мы восстанавливаем однозначно (количество ребер и указание, какой из корней длиннее в диаграмме Дынкина единственным образом определяет фундаментальную систему кореней). Далее, фундаментальными отражениями мы порождаем всю группу Вейля корневой системы Φ. Наконец, ввиду леммы 2.1.9, любой корень из Φ является образом некоторого фундаментального корня относительно некоторого элемента группы Вейля. Таким образом, для того, чтобы классифицировать неразложимые корневые системы достаточно классифицировать диаграммы Дынкина.

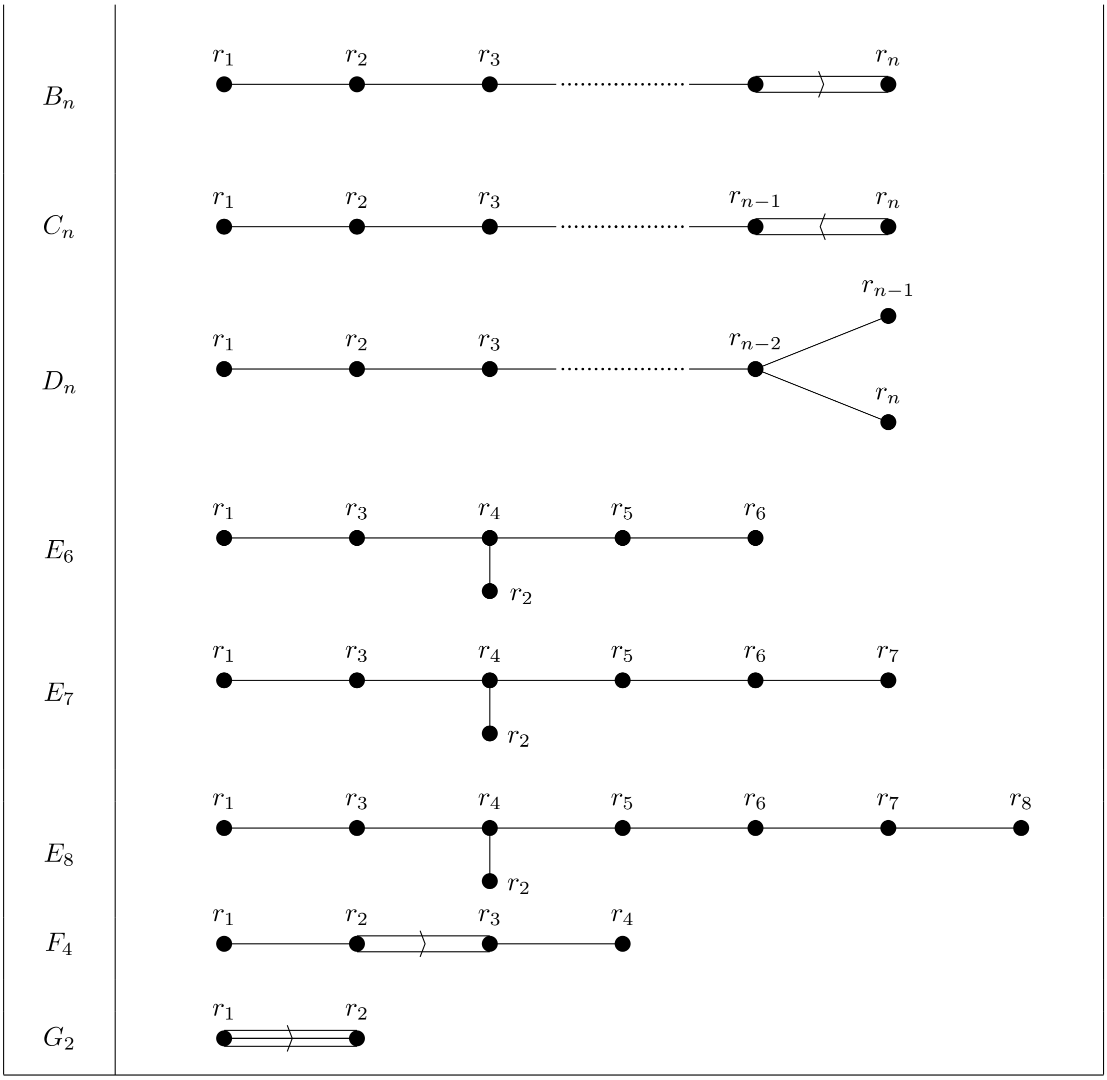
§5 Классификация неразложимых корневых систем

Как мы заметили в конце прошлого параграфа, для классификации неразложимых корневых систем достаточно классифицировать диаграммы Дынкина. Идея доказательства теоремы 2.5.1 взята из [12].

Теорема 2.5.1. *Пусть Φ — неразложимая корневая система. Тогда её диаграмма Дынкина совпадает с одной из диаграмм таблицы 2.5.2.*

Таблица 2.5.2. Корневые системы и диаграммы Дынкина

Тип Φ	Диаграмма Дынкина
A_n	



Теорему 2.5.1 мы докажем следующим образом. Сначала для каждой из указанных в таблице 2.5.2 диаграмм Дынкина мы построим корневую систему, а затем докажем, что других диаграмм Дынкина не существует.

Тип A_n. Рассмотрим евклидово векторное пространство размерности $n+1$, пусть $e_1, \dots, e_{n+1}$ — некоторый его ортонормированный базис. Рассмотрим подпространство V, состоящее из векторов, сумма координат которых равна 0. Тогда корневая система типа A_n будет порождать это подпространство V и её фундаментальные корни — это $\{e_1 - e_2, e_2 - e_3, \dots, e_n - e_{n+1}\}$. Отражение w_r в корне $r = e_i - e_j$ переводит e_i в e_j, e_j в e_i, а остальные векторы базиса оставляет неподвижными. Таким образом, корневая система A_n состоит из векторов вида $e_i - e_j$, её группа Вейля изоморфна Sym_{n+1} и действует на корнях, переставляя индексы.

Тип B_n. В евклидовом пространстве размерности n фундаментальная система корней имеет вид $e_1 - e_2, \dots, e_{n-1} - e_n, e_n$. Группа Вейля состоит из линейных отображений, переводящих e_i в $\pm e_j$ и изоморфна $2 \wr \mathrm{Sym}_n$ ($2^n \leftthreetimes \mathrm{Sym}_n$), а корневая система B_n состоит из векторов вида $e_i - e_j, \pm e_i$.

Тип C_n. В евклидовом пространстве размерности n фундаментальная система корней имеет вид $e_1 - e_2, \dots, e_{n-1} - e_n, 2e_n$. Группа Вейля состоит из линейных отображений, переводящих e_i в $\pm e_j$ и изоморфна $2 \wr \mathrm{Sym}_n$, а корневая система C_n состоит из векторов вида $e_i - e_j, \pm 2e_i$.

Тип D_n. В евклидовом пространстве размерности n фундаментальная система корней имеет вид $e_1 - e_2, \dots, e_{n-1} - e_n, e_{n-1} + e_n$. Группа Вейля состоит из линейных отображений, переводящих e_i в $\pm e_j$, причем количество плюсов четно и изоморфна подгруппе индекса 2 в $2 \wr \mathrm{Sym}_n$, а корневая система D_n состоит из векторов вида $\pm e_i \pm e_j$.

Тип E_n, $n = 6, 7, 8$. Мы опишем как получается корневая система E_8, а системы E_7 и E_6 получим как подсистемы. В качестве фундаментальной системы мы возьмем векторы $r_1 = -\frac{1}{2}\sum_{i=1}^{8} e_i$, $r_2 = e_6 - e_7$, $r_3 = e_6 + e_7$, $r_4 = e_5 - e_6$, $r_5 = e_4 - e_5$, $r_6 = e_3 - e_4$, $r_7 = e_2 - e_3$, $r_8 = e_1 - e_2$ (нумерация выбрана также, как

в таблице 2.5.2). Корневая система E_8 состоит из векторов $\pm e_i \pm e_j, \frac{1}{2}\sum_{i=1}^{8}\epsilon_i e_i$, $\prod_{i=1}^{8}\epsilon_i = 1$. Группа Вейля имеет порядок $2^{14}\cdot 3^5\cdot 5^2\cdot 7$ и изоморфна группе $2.O_8^+(2):2$ (в обозначениях [6]).

Фундаментальная система корневой системы E_7 получается выбрасыванием корня r_8, корневая система типа E_7 состоит из векторов $\pm e_i \pm e_j, i,j \neq 1$, $\pm(e_1+e_8)$, $\frac{1}{2}\sum_{i=1}^{8}\epsilon_i e_i; \epsilon_i = \pm 1, \epsilon_1 = \epsilon_8 = 1, \prod_{i=1}^{8}\epsilon_i = 1$, $-\frac{1}{2}\sum_{i=1}^{8}\epsilon_i e_i; \epsilon_i = \pm 1, \epsilon_1 = \epsilon_8 = 1, \prod_{i=1}^{8}\epsilon_i = 1$. Группа Вейля имеет порядок $2^{10}\cdot 3^4\cdot 5\cdot 7$ и изоморфна группе $2.O_7(2)$ (в обозначениях [6]).

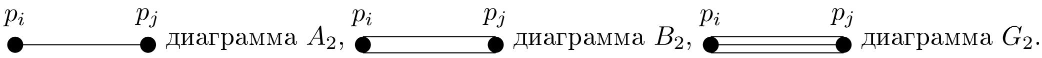
Фундаментальная система корневой системы E_6 получается выбрасыванием корней r_7, r_8 из фундаментальной системы в E_8. Корневая система E_6 состоит из векторов $\pm e_i \pm e_j, i,j \neq 1,2$, $\frac{1}{2}\sum_{i=1}^{8}\epsilon_i e_i; \epsilon_i = \pm 1, \epsilon_1 = \epsilon_2 = \epsilon_8 = 1, \prod_{i=1}^{8}\epsilon_i = 1$, $-\frac{1}{2}\sum_{i=1}^{8}\epsilon_i e_i; \epsilon_i = \pm 1, \epsilon_1 = \epsilon_2 = \epsilon_8 = 1, \prod_{i=1}^{8}\epsilon_i = 1$. Группа Вейля имеет порядок $2^7\cdot 3^4\cdot 5$ и изоморфна группе $PSp_4(3):2$ (в обозначениях [6]).

Тип F_4. Фундаментальная система состоит из векторов e_1-e_2, e_2-e_3, e_3, $\frac{1}{2}(-e_1-e_2-e_3+e_4)$. Вся корневая система состоит из векторов $\pm e_i \pm e_j$, $\pm e_i$, $\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)$, группа Вейля разрешима и её порядок равен $2^7\cdot 3^2$.

Тип G_2. Корневая система состоит из векторов $\pm r_1$, $\pm r_2$, $\pm(r_1+r_2)$, $\pm(r_1+2r_2)$, $\pm(r_1+3r_2)$, $\pm(2r_1+3r_2)$. Ее группа Вейля разрешима и имеет порядок 12.

Корневые системы типов A_n, B_n, C_n и D_n обычно называют корневыми системами классического типа, а остальные корневые системы называют системами исключительного типа.

Покажем теперь, что других фундаментальных систем не существует. Рассмотрим два фундаментальных корня p_i, p_j таких, что $n_{ij} \neq 0$. Тогда в диаграмме Дынкина они связаны n_{ij} ребрами. Поскольку $n_{ij} \in \{0,1,2,3\}$, получаем, что подграф, порождённый этими двумя корнями совпадает с одним из следующих графов:



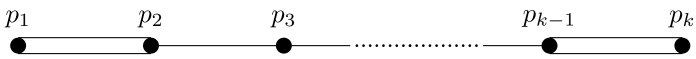
Таким образом, любая диаграмма Дынкина «собрана» из этих трех графов. Поддиаграммой диаграммы Дынкина мы будем называть любой её подграф. Теперь мы последовательно отбросим все невозможные конфигурации для диаграмм. Поскольку длина корней в диаграмме Дынкина однозначно определяется заданием длины одного из корней, будем считать, что самый короткий из корней p_i, p_j, без ограничения общности можно считать, что это корень p_j, имеет длину 1.

Шаг 1. Диаграмма G_2 не является собственной поддиаграммой ни в какой диаграмме Дынкина. Действительно, предположим противное. Тогда существует поддиаграмма вида

(между r и одним из корней p_i, p_j не менее одного ребра). Рассмотрим первый случай (второй разбирается аналогично). Имеем $2(p_i,p_j) = -3$, $(p_i,r) \leqslant 0$ (напомним, что скалярное произведение любых двух фундаментальных корней не превосходит 0, как было показано в предыдущем параграфе). Далее, $< p_j, r >$ либо равно -1, либо равно -2, либо равно -3. В первом случае мы получаем, что $(r,r) = 1$ и $2(p_j,r) = -1$, во втором случае мы получаем, что $(r,r) \leqslant 2$ и $2(p_j,r) = -2$, в третьем случае мы получаем, что $(r,r) \leqslant 3$ и $2(p_j,r) = -3$. Рассмотрим вектор $v = p_i + 2p_j + r$. Тогда $(v,v) \leqslant 0$, т. е. $v = 0$ и фундаментальные корни p_i, p_j, r оказываются линейно зависимыми. В случае смежности p_i и r в качестве вектора v надо взять вектор $2p_i + 3p_j + r$.

Далее можно считать, что диаграмма Дынкина «собрана» лишь из поддиаграмм вида A_2 или B_2.

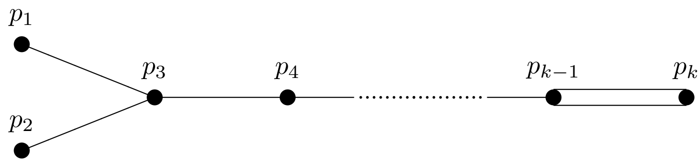
Шаг 2. Диаграмма Дынкина может содержать B_2 в качестве поддиаграммы лишь один раз. В противном случае существовала бы поддиаграмма вида



Рассмотрим теперь вектор $v = p_1 + p_k + 2(p_2 + \ldots + p_{k-1})$. Используя соотношения $(p_i,p_j) \leqslant 0$, $2(p_i,p_{i+1}) \leqslant -1$, $2(p_1,p_2) = 2(p_{k-1},p_k) = -2$, получаем, что $(v,v) \leqslant 0$, т. е. фундаментальные корни $p_1,\ldots,p_k$ линейно зависимы.

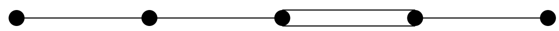
Шаг 3. В диаграмме Дынкина, содержащей поддиаграмму типа B_2 не существует циклов. В противном случае, пройдя по этому циклу мы бы получили, что все корни в нем имеют одинаковую длину, что невозможно.

Шаг 4. В диаграмме Дынкина, содержащей поддиаграмму типа B_2 не существует точек ветвления. В противном случае, такая диаграммы Дынкина содержит поддиаграмму



Рассмотрим вектор $v = p_1 + p_2 + 2(p_3 + \ldots + p_k)$. Вновь $(v, v) \leqslant 0$, что противоречит линейной независимости фундаментальных корней.

Шаг 5. Диаграмма

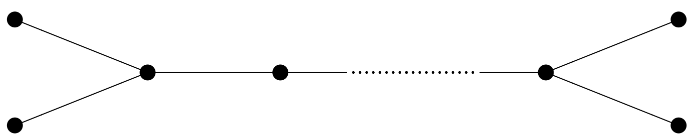


не может возникнуть как поддиаграмма. Действительно, рассмотрим вектор $v = p_1 + 2p_2 + 3p_3 + 4p_4 + 2p_5$, тогда $(v, v) \leqslant 0$.

Шаги 2–5 показывают, что если диаграмма Дынкина содержит ребро «типа B_2», то она совпадает с диаграммой корневой системы B_n, C_n или F_4 из таблицы 2.5.2. Таким образом мы можем считать, что наша диаграмма «собрана» только из ребер «типа A_2», т. е. все фундаментальные корни имеют одинаковую длину.

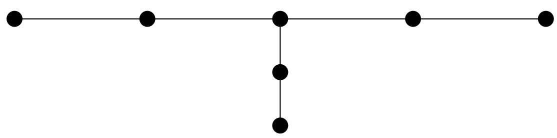
Шаг 6. В диаграмме Дынкина не существует циклов. В противном случае рассмотрим $v = p_1 + \ldots + p_k$ — вектор, полученный из фундаментальных векторов, образующих цикл. Вновь получаем, что $(v, v) \leqslant 0$.

Шаг 7. Существует не более трех конечных точек в диаграмме Дынкина (следовательно, существует не более одной точки ветвления). В противном случае существует поддиаграмма вида



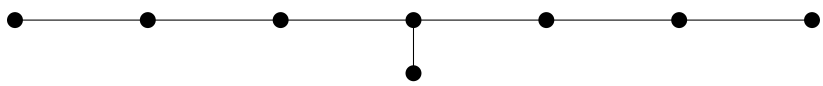
Пусть $p_1, \ldots, p_k$ — соответствующие векторы, причем p_1, p_2 — окончания слева, а p_{k-1}, p_k — окончания справа. Тогда для вектора $v = p_1 + p_2 + 2p_3 + \ldots + 2p_{k-2} + p_{k-1} + p_k$ получаем $(v, v) \leqslant 0$.

Шаг 8. Если существует точка ветвления, то одна из ветвей имеет длину 1. В противном случае существовала бы поддиаграмма вида



Пусть p_1 — центральная точка, p_2, p_3, p_4 — смежные с ней вершины и p_5, p_6, p_7 — конечные вершины. Тогда для $v = 3p_2 + 2(p_2 + p_3 + p_4) + p_5 + p_6 + p_7$ получаем $(v, v) \leqslant 0$.

Шаг 9. Диаграмма



не может возникнуть как поддиаграмма. В противном случае занумеруем векторы в верхней линии $p_1, \ldots, p_7$ и нижний p_8. Получим что для вектора $v = p_1 + 2(p_2 + p_6 + p_8) + 3(p_3 + p_5) + 4p_4 + p_7$ справедливо $(v, v) \leqslant 0$.

Шаг 10. Диаграмма

не может возникнуть в качестве поддиаграммы. В противном случае, занумеровав вновь векторы верхней строки $p_1, \ldots, p_8$ и нижний p_9, получим, что для вектора $v = 2(p_1 + p_7) + 3(p_9 + p_6) + 4(p_2 + p_5) + 6p_3 + 5p_4 + p_8$ выполнено $(v, v) \leqslant 0$.

Таким образом, шаги 6–10 показывают, что диаграммы, в которых все ребра имеют «тип A_2» совпадают с A_n, D_n, E_6, E_7 или E_8.

В качестве следствий мы сформулируем следующие полезные леммы.

Лемма 2.5.3. *Пусть Φ — неразложимая корневая система. Тогда группа Вейля действует транзитивно на множестве корней одинаковой длины.*

Доказательство. Ввиду леммы 2.1.9, любой корень в корневой системе является образом некоторого фундаментального корня относительно некоторого элемента группы Вейля. Таким образом, достаточно доказать, что группа Вейля действует транзитивно на фундаментальных корнях одинаковой длины. Пусть r, s — два фундаментальных корня одинаковой длины. Ввиду теоремы 2.5.1, получаем, что корни r, s связаны цепочкой ребер «типа A_2». Но любые два соседних корня этой цепочки p_1, p_2 переходят друг в друга под действием элемента $w_{p_1+p_2}w_{p_2} \in W$. □

Лемма 2.5.4. Лемма Титса. *Пусть $r, s \in \Pi$ и предположим, что $\alpha^w = \beta$, где $w \in W$. Тогда существуют корни $p_0 = r$, $p_1, \dots, p_k = s \in \Pi$ и элементы $w_0, w_1, \dots, w_{k-1} \in W$, удовлетворяющие следующим условиям:*

(а) $w = w_0 \cdot \ldots \cdot w_{k-1}$;

(б) $p_i^{w_i} = p_{i+1}$;

(в) *для любого $0 \leqslant i \leqslant k-1$, если $p_i \neq p_{i+1}$, то $w_i \in \langle w_{p_i}, w_{p_{i+1}} \rangle$, и если $p_i = p_{i+1}$, то существует $\delta_i \in \Delta$, для которого $w_i \in \langle w_{\gamma_i}, w_{\delta_i} \rangle$.*

Доказательство. Будем вести доказательство индукцией по $l(w)$. В силу следствия 2.2.3, мы получаем, что если $l(w) = 0$, то $w = e$ и доказывать нечего.

Если $l(w) > 0$, то существует $p \in \Pi$, для которого p^w — отрицательный корень. Положим $p_0 = \alpha$ и рассмотрим подсистему Ψ, порождённую корнями p_0, p. Выберем в ней множество $(\Phi^+)w^{-1} \cap \Psi = \Theta$ в качестве множества положительных корней. Ввиду леммы 2.1.4 и теоремы 2.2.4 мы получаем, что существует такой $w_0 \in \langle w_{p_0}, w_p \rangle$, что $(\Theta)w_0 = \Psi \cap \Phi^+$. Положим $w' = w_0^{-1}w$. Поскольку w_{p_0} и w_p стабилизируют $\Theta' = \Phi^+ \setminus \Psi$, мы получаем, что и элемент w_0 стабилизирует множество Θ'. Следовательно, для любого $q \in \Theta'$ корень $q^{w'}$ является положительным тогда и только тогда, когда корень q^w является положительным. С другой стороны, для любого корня q из $\Psi \cap \Phi^+$ мы имеем $q^{w'} > 0$, в то время, как $p^w < 0$ по построению. Таким образом, количество положительных корней, которые элемент w' переводит в отрицательные, строго меньше, чем количество положительных корней, которые элемент w переводит в отрицательные. Ввиду теоремы 2.2.2 мы получаем, что $l(w') < l(w)$.

Определим $p_1 = p_0^{w_0} (= r^{w_0})$. По условию, $p_0 \in (\Pi)w^{-1}$, значит, p_0 принадлежит фундаментальной системе $(\Pi)w^{-1} \cap \Psi$ подсистемы Ψ, которая лежит в $\Theta = (\Phi^+ \cap \Psi)w_0^{-1}$. Следовательно, $p_0 \in (\Pi \cap \Psi)w_0^{-1} \subseteq (\Pi)w_0^{-1}$. Значит, p_1 является фундаменатлльным корнем и лежит в $\Psi \cap \Phi^+$. Если $p_1 \neq p_0$, то это означает, что $p_1 = p$, значит, $s = p^{w'}$. Индукция по длине элемента завершает доказательство. □

§6 Диаграммы Дынкина подсистем

В данном параграфе мы приведем алгоритм описания корневых подсистем в различных неразложимых корневых системах. Данные результаты были получены независимо в [1] и в [9]. Мы в нашем изложении будем в основном придерживаться [9].

Сначала мы установим некоторые дополнительные свойства корневых систем. Пусть r, s — произвольные корни из Φ. Рассмотрим множество всевозможных целочисленных комбинаций корней r, s и пересечем его с Φ. Полученное множество Φ_1 является подсистемой корневой системы Φ ранга 2. В силу классификационной теоремы 2.5.1, отсюда следует, что либо Φ_1 неразложима и имеет тип A_2, B_2 или G_2, либо $\Phi_1 = A_1 \cup A_1$. Непосредственный перебор всех возможных случаев дает нам следующую лемму.

Лемма 2.6.1. *Существуют такие целые неотрицательные числа p, q, что $s + ir \in \Phi$ для любого $-p \leqslant i \leqslant q$, но $s + ir \notin \Phi$ если $i \leqslant -(p+1)$ или $i \geqslant q+1$. Более того $-p+q =< r, s >$, отражение w_r переставляет корни вида $s + ir$ и $w_r(s - pr) = s + qr$.*

Определение 2.6.2. Последовательность корней $s + ir$, определенная в лемме 2.6.1, называется *r-серией корней, содержащей s.*

Следствие 2.6.3. *Если r — положительный нефундаментальный корень, то существует такой фундаментальный корень s, что $r - s \in \Phi$.*

Доказательство. В доказательстве леммы 2.1.7 мы показали, что для любого положительного нефундаментального корня r существует фундаментальный корень s такой, что $(s,r)>0$. Тогда $w_s(r)=r-<s,r>s$ вновь является корнем. По лемме 2.6.1, отсюда следует, что $r-s$ также является корнем. □

Лемма 2.6.4. *В любой неразложимой корневой системе Φ существует единственный корень r_0 максимальной высоты. Для любого положительного корня $r\neq r_0$ существует некоторый фундаментальный корень p_i такой, что $r+p_i\in\Phi$.*

Доказательство. Достаточно доказать, что не существует двух различных корней r,s, удовлетворяющих условию $r+p_i\notin\Phi$ для любого фундаментального корня p_i и $s+p_j\notin\Phi$ для любого фундаментального корня p_j. Предположим, что такие корни r,s существуют и их высота минимальна. Заметим, что если выполнено неравенство $(p_i,r)<0$, то $w_{p_i}(r)=r-<p_i,r>p_i=r+kp_i\in\Phi$ и $k>0$. Ввиду леммы 2.6.3 получаем, что $r+p_i\in\Phi$, что противоречит нашему предположению. Таким образом, $(p_i,r)\geqslant 0$ для любого фундаментального корня p_i и аналогично $(p_j,s)\geqslant 0$ для любого фундаментального корня p_j. Далее, ввиду леммы 2.1.7, существуют такие целые $\alpha_1,\dots,\alpha_\ell$ и $\beta_1,\dots,\beta_\ell$, что $r=\alpha_1p_1+\ldots+\alpha_\ell p_\ell$ и $s=\beta_1p_1+\ldots+\beta_\ell p_\ell$. Покажем сначала, что все α_i и β_j отличны от 0.

Действительно, в силу неразложимости системы Φ мы получаем, что если какие-то из α_i равны 0, то существует фундаментальный корень p_i такой, что $\alpha_i=0$, но $(p_i,p_j)<0$ для некоторого p_j, для которого $\alpha_j>0$. Следовательно, $(p_j,r)<0$, что противоречит доказанному ранее неравенству $(p_j,r)\geqslant 0$ для всех фундаментальных корней p_j. Аналогичными рассуждениями получаем, что все $\beta_j>0$.

Рассмотрим теперь (r,s). Имеем $(r,s)=\sum_i\alpha_i(p_i,s)>0$. Следовательно, $w_r(s)=s-<r,s>r=s-kr\in\Phi$, где k — некоторое положительное число. Ввиду леммы 2.6.3 получаем, что $s-r\in\Phi$. Аналогичные рассуждения показывают, что $r-s\in\Phi$. Таким образом, либо $s-r$, либо $r-s$ является положительным корнем. Без ограничения общности можно считать, что $r-s$ — положительный корень. Если $r-s$ — фундаментальный корень, то мы получаем, что $(r-s)+s\in\Phi$, что противоречит выбору s. В противном случае, как и при доказательстве леммы 2.1.7, мы получаем, что существует некоторый фундаментальный корень p_i такой, что $(r-s,p_i)>0$, следовательно, $(r,p_i)>0$. Как и при доказательстве следствия 2.6.3, отсюда следует, что $r-p_i\in\Phi$ и $(r-s)-p_i\in\Phi$. Заменяя корень r на корень $r'=r-p_i$ и повторяя указанную процедуру, мы получим некоторый корень $\bar r$ такой, что $\bar r-s$ уже фундаментальный корень, что противоречит выбору s. □

Определение 2.6.5. Подмножество Φ_1 корневой системы Φ называется *подсистемой*, если Φ_1 само является корневой системой в своей линейной оболочке.

Лемма 2.6.6. *Подмножество Φ_1 является подсистемой корневой системы Φ в том и только в том случае, когда $r+s\in\Phi\Rightarrow r+s\in\Phi_1$ и $r\in\Phi_1\Rightarrow -r\in\Phi_1$ для любых двух корней $r,s\in\Phi_1$.*

Доказательство. Поскольку r-серия корней, содержащая s однозначно восстанавливается по корням r,s лемма сразу следует из леммы 2.6.1. □

Определение 2.6.7. Подмножество Ξ корневой системы Φ называется Π-*множеством*, если для любых двух корней $r,s\in\Xi$ выполнено $r-s\notin\Phi$.

Ясно, что фундаментальная система является П-множеством. Более того, фундаментальная система любой подсистемы также является П-множеством. С другой стороны, если Ξ — некоторое линейно независимое П-множество, рассмотрим $\mathbb{Z}\Xi\cap\Phi=\Phi_1$. Ввиду леммы 2.6.6 множество Φ_1 является подсистемой корневой системы Φ. Кроме того, Ξ является фундаментальной системой для Φ_1. Действительно, надо проверить лишь, что любой корень из Φ_1 представим в виде целочисленной линейной комбинации элементов из Ξ, все коэффициенты которой либо неположительны, либо неотрицательны. Ясно, что подсистему Φ_1 можно считать неразложимой. Предположим противное, тогда существует корень r такой, что $r=\lambda_1p_1+\ldots+\lambda_kp_k$, где все $\lambda_i>0$ и $p_i\in\Xi$, но $r-p_j\in\Phi_1$ для некоторого $p_j\in\Xi\setminus\{p_1,\dots,p_k\}$ (этот корень r — контрпример минимальной высоты). Предположим сначала, что $\Phi_1\neq G_2$. Тогда p_j-цепь, содержащая r состоит не более, чем из трех корней и, значит, $(p_j,r)\geqslant 0$. С другой стороны $(p_j,p_i)\leqslant 0$ для всех $p_i\in\Xi$. Кроме того, можно считать, что $(p_j,p_i)<0$ для некоторого $p_i\in\{p_1,\dots,p_k\}$. В противном случае мы бы получили, что корни $p_1,\dots,p_k,p_j$ порождают разложимую корневую подсистему $\Phi_2=\Phi_3\cup A_1$, где Φ_3 — подсистема, порождённая корнями $p_1,\dots,p_k$, а A_1 — подсистема, порождённая корнем p_j. Но тогда $r\notin\Phi_2$, вопреки предположению. Следовательно, $(p_j,r)=\lambda_1(p_j,p_1)+\ldots+\lambda_k(p_j,p_k)<0$, что противоречит полученному раньше неравенству $(p_j,r)\geqslant 0$. Если теперь $\Phi_1=G_2$, то легко проверить непосредственными вычислениями, что разность любых двух коротких корней является корнем, а сумма любых двух длинных корней является длинным корнем.

Таким образом, Ξ содержит по крайней мере один короткий и один длинный корень p_1 и p_2. Кроме того, $< p_1, p_2 >= -1$, $< p_2, p_1 >= -3$ и корни p_1, p_2, очевидно, образуют фундаментальную систему в Φ_1. Таким образом, нами получена следующая

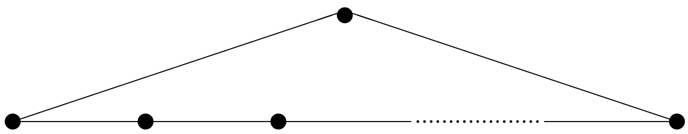
Лемма 2.6.8. *Пусть Ξ — линейно независимое* Π-*подмножество корневой системы Φ и пусть $\Phi_1 = \mathbb{Z}\Xi \cap \Phi$. Тогда Φ_1 является подсистемой системы Φ, Ξ — её фундаментальная система корней и любая подсистема системы Φ порождается некоторым линейно независимым* Π-*подмножеством.*

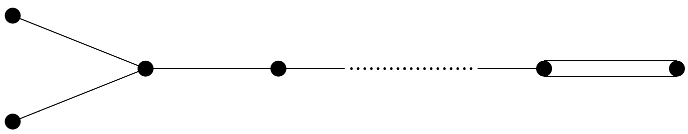
Значит, для классификации подсистем корневой системы Φ достаточно классифицировать линейно независимые Π-подмножества этой системы. Каждому Π-подмножеству мы сопоставим диаграмму, аналогичную диаграмме Дынкина. Т. е. любые два корня p_i, p_j из Π-подмножества соединены $< p_i, p_j > \cdot < p_j, p_i >$ ребрами и указано, какой из корней длиннее. Такую диаграмму мы будем называть *расширенной диаграммой* Π-*множества* Ξ .

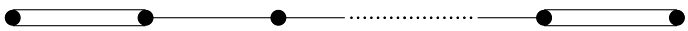
Лемма 2.6.9. *Пусть Ξ — некоторое* Π-*подмножество корневой системы Φ и Φ_1 — корневая подсистема, порождённая этим подмножеством. Тогда существует линейно независимое подмножество Ξ_1 множества Ξ, порождающее Φ_1.*

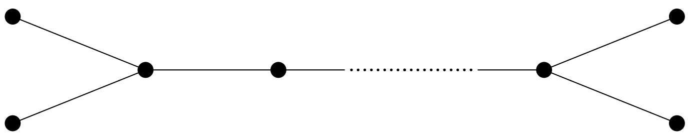
Доказательство. Ясно, что подсистему Φ_1 можно считать неразложимой. Рассмотрим расширенную диаграмму для Ξ. Если расширенная диаграмма совпадает с диаграммой Дынкина, то тогда корни из Ξ линейно независимы и доказывать нечего.

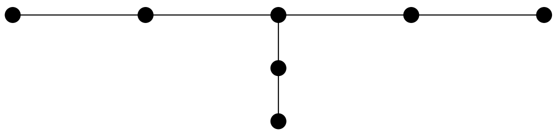
В противном случае расширенная диаграмма содержит поддиаграмму одного из следующих видов:

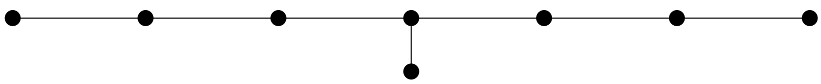
1. 

2. 

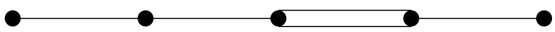
3. 

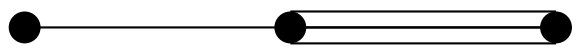
4. 

5. 

6. 

7. 

8. 

9. 

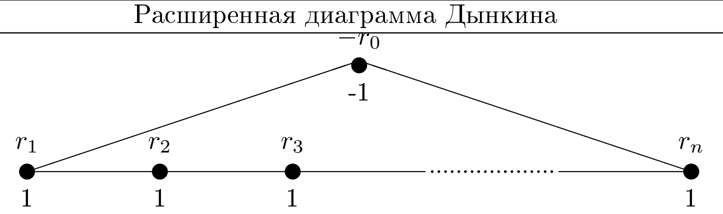
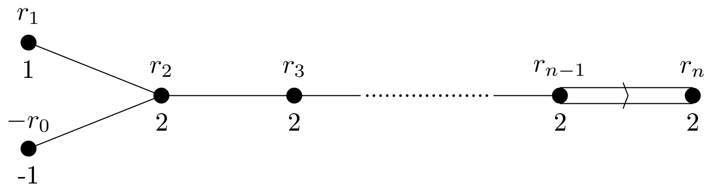
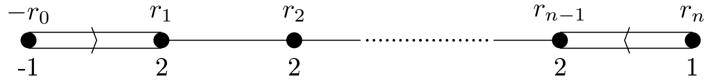
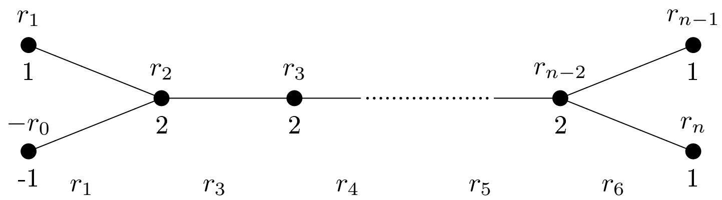
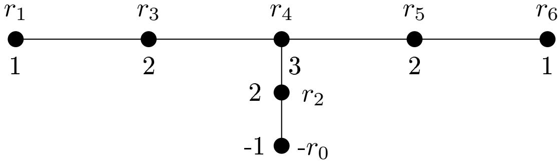
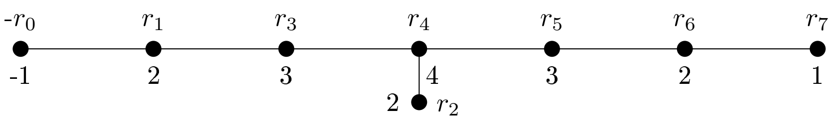
Пусть $p_1, \ldots, p_k$ — корни, являющиеся вершинами одной из приведенных выше диаграмм. Как показано при доказательстве теоремы 2.5.1, для каждой из указанных выше диаграмм существует целочисленная линейная комбинация корней $\lambda_1 p_1 + \ldots + \lambda_k p_k = 0$, причем по меньшей мере один из λ_i равен 1. Следовательно, корень p_i, соответствующий такому $\lambda_i = 1$ лежит в корневой системе, порождённой остальными корнями и мы можем рассмотреть $\Xi_1 = \Xi \setminus \{p_i\}$. Повторяя эту процедуру, мы получим линейно независимое множество Ξ', порождающее подсистему Φ_1. □

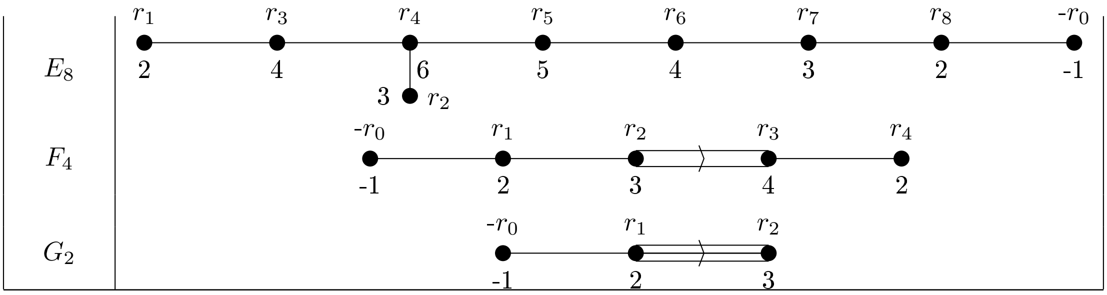
Лемма 2.6.10. *Пусть Ξ — линейно независимая Π-система, порождающая подсистему Φ_1 корневой системы Φ, причем $\Phi \neq \Phi_1$. Тогда существует $r \in \Phi \setminus \Phi_1$ такой, что $\Xi \cup \{r\}$ вновь является Π-системой.*

Доказательство. Дополним Ξ до базиса пространства V, содержащего корневую систему Φ и выберем V^+ таким образом, что $\Xi \subset V^+$. Пусть r — минимальный корень в $\Phi \setminus \Phi_1$. Тогда $r - s \prec r$ для любого $s \in \Xi$, следовательно, $r - s \notin \Phi$ и, значит, $s - r \notin \Phi$. Таким образом, $\Xi \cup \{r\}$ является Π-системой. □

Определение 2.6.11. Диаграмму, полученную из диаграммы Дынкина корневой системы Φ присоединением корня $-r_0$ и соединением его с остальными корнями по обычному правилу назовем *расширенной диаграммой Дынкина.* В таблице 2.6.12 приведены расширенные диаграммы Дынкина для всех неразложимых корневых систем, кроме того, указаны коэффициенты, с которыми фундаментальные корни входят в разложение корня r_0.

Таблица 2.6.12. Расширенные диаграммы Дынкина

Тип Φ	Расширенная диаграмма Дынкина
A_n	
B_n	
C_n	
D_n	
E_6	
E_7	



Теперь мы можем получить алгоритм описания диаграмм Дынкина подсистем корневой системы Φ. Пусть Φ — неразложимая корневая система и Ξ — некоторая П-система, порождающая Φ. Ввиду леммы 2.6.9 она содержит фундаментальную систему Π корневой системы Φ. Ввиду следствия 2.6.3 и леммы 2.6.4 единственным корнем r, удовлетворяющим условию $r-p_i\notin\Phi$ для любого $p_i\in\Pi$ является корень $-r_0$. Следовательно, либо $\Xi=\Pi$, либо $\Xi=\Pi\cup\{-r_0\}$.

Пусть теперь Φ_1 — максимальная собственная подсистема корневой системы Φ и Π_1 — её фундаментальная система. Ввиду леммы 2.6.10 существует корень $r\in\Phi\setminus\Phi_1$ такой, что $\Pi_1\cup\{r\}=\Xi$ является П-множеством. Более того, корневая система, порождённая П-множеством Ξ совпадает с корневой системой, порождённой множеством $\Phi_1\cup\{r\}$ и равна Φ ввиду максимальности подсистемы Φ_1. Как мы заметили выше, это означает, что либо $\Xi=\Pi$, либо $\Xi=\Pi\cup\{-r_0\}$.

Таким образом, алгоритм заключается в следующем. Мы рассматриваем расширенную диаграмму Дынкина корневой системы Φ и выбрасываем из нее одну или несколько вершин. Потом для каждой из оставшихся компонент связности мы повторяем процедуру. Диаграммы, которые можно получить таким образом, дают нам диаграммы Дынкина всех подсистем системы Φ.

***Упражнение* 2.6.13.** Найти максимальные подсистемы во всех неразложимых корневых системах.

§7 Классы сопряженных элементов в группах Вейля

Материал данного параграфа взят в основном из [2, G] и [5]. Там же можно найти более подробное изложение и необходимые технические следствия о характеристических многочленах и допустимых диаграммах.

Напомним, что группа Вейля порождается отражениями w_r в корнях $r\in\Phi$. Таким образом, для любого элемента $w\in W$ существуют корни $r_1,\dots,r_k$, для которых справедливо $w=w_{r_1}\cdot w_{r_2}\cdot\ldots\cdot w_{r_k}$. Обозначим через $\bar{l}(w)$ минимальное такое k, что w представим в виде произведения отражений в корнях $r_1,\dots,r_k$.

Лемма 2.7.1. *$\bar{l}(w)$ равно количеству собственных значений элемента $w\in W$, отличных от 1. В частности, $\bar{l}(w)\leqslant\ell$ (напомним, что ℓ — это размерность векторного пространства V).*

Доказательство. Предположим, что $\bar{l}(w)=k$ и $w=w_{r_1}\cdot\ldots\cdot w_{r_k}$ — соответствующее разложение элемента w в виде произведения отражений. Пусть H_{r_i} — гиперплоскость, ортогональная вектору r_i и положим $U=H_{r_1}\cap\ldots\cap H_{r_k}$. Тогда w оставляет неподвижным любой вектор из U и $\dim U\geqslant l-k$. Таким образом, w имеет по меньшей мере $\ell-k$ собственных значений, равных 1, значит, существует не более k собственных значений, отличных от 1.

Обратно, предположим, что w имеет k собственных значений, отличных от 1. Пусть V_1 — подпространство векторов, неподвижных относительно w и пусть $V_1^\perp$ — его ортогональное дополнение. Тогда $\dim V_1=\ell-k$ и $\dim V_1^\perp=k$. Поскольку w оставляет неподвижным любой вектор из V_1, из теоремы 2.3.6 следует, что w порождён отражениями в корнях из $V_1^\perp\cap\Phi$. Если $k\lneq\ell$, т. е. $\dim V_1^\perp\lneq\dim V$, то мы можем использовать индукцию по размерности пространства и получить, что w является произведением в точности k отражений.

Таким образом, достаточно доказать, что если элемент w не имеет неподвижных векторов на V, то он является произведением не более, чем ℓ отражений. Пусть $r\in\Phi$. Поскольку w не оставляет неподвижным никакой вектор, $w-1$ — невырожденное преобразование. Следовательно, существует вектор v такой, что $(w-1)v=r$, значит, $w(v)=v+r$. Далее, $(w(v),w(v))=(v,v)$. Таким образом, $(v+r,v+r)=(v,v)$ и, значит, $\frac{2(v,r)}{(r,r)}=-1$. Следовательно, $w_r(v)=v+r$ и $w(v)=w_r(v)$. Поэтому $w_rw(v)=v$. Ввиду следствия 2.3.5, элемент w_rw является произведением отражений в корнях, ортогональных вектору v и мы можем применить индукцию. □

Определение 2.7.2. Выражение $w_{r_1}\cdot w_{r_2}\cdot\ldots\cdot w_{r_k}$ называется *приведённым*, если $\bar{l}(w_{r_1}\cdot w_{r_2}\cdot\ldots\cdot w_{r_k})=k$.

Лемма 2.7.3. *Пусть $r_1, r_2, \ldots, r_k \in \Phi$. Тогда выражение $w_{r_1} \cdot w_{r_2} \cdot \ldots \cdot w_{r_k}$ является приведённым в том и только в том случае, когда векторы $r_1, r_2, \ldots, r_k$ линейно независимы.*

Доказательство. Пусть $w = w_{r_1} \cdot w_{r_2} \cdot \ldots \cdot w_{r_k}$ и предположим, что выражение приведенное. Тогда w имеет k собственных значений, отличных от 1 и, значит, $\dim(H_{r_1} \cap \ldots \cap H_{r_k}) = \ell - k$. Размерность не может быть больше, поскольку w фиксирует любой элемент пространства $H_{r_1} \cap \ldots \cap H_{r_k}$ и потому размерность этого пространства не может быть больше, чем размерность пространства неподвижных векторов. Следовательно, векторы $r_1, \ldots, r_k$ линейно независимы.

Обратно, предположим, что векторы $r_1, \ldots, r_k$ линейно независимы. Тогда рассмотрим подпространство $(w-1)V$. Выберем вектор x так, что $x \in H_{r_2} \cap \ldots \cap H_{r_k}$, но $x \notin H_{r_1}$. Тогда вектор $w(x) - x$ кратен r_1 (в силу нашего выбора, $w_{r_2} \cdot \ldots \cdot w_{r_k}(x) = x$), таким образом, $r_1 \in (w-1)V$. Далее выберем $x \in H_{r_3} \cap \ldots \cap H_{r_k}$, но $x \notin H_{r_2}$. Мы имеем, что $w(x) - x = \lambda r_2 + \mu r_1$ и $\lambda \neq 0$. Значит, $r_2 \in (w-1)V$. Продолжая рассуждения таким же образом, мы получаем, что $r_1, \ldots, r_k \in (w-1)V$. Следовательно, элемент w имеет не более $\ell - k$ собственных значений, равных 1 и по лемме 2.7.1, $\bar{l}(w) \geqslant k$. □

Лемма 2.7.4. *Любая инволюция $w \in W$ может быть записана в виде произведения $\bar{l}(w)$ отражений, соответствующий попарно ортогональным корням.*

Доказательство. Пусть V_1 — это подпространство векторов, неподвижных относительно w, и V_{-1} — это подпространство векторов, для которых $w(x) = -x$. Поскольку w — инволюция, пространство V является прямой суммой $V = V_1 \oplus V_{-1}$. Если $\dim V_1 > 0$, мы можем использовать индукцию. В противном случае $V_{-1} = V$, т. е. $w = -1$. Пусть $w = w_{r_1} \cdot w_{r_2} \cdot \ldots \cdot w_{r_\ell}$ — приведенное выражение. Рассмотрим вектор v, ортогональный корню r_1. Мы имеем $w(v) = -v$ и, значит, $w_2 \cdot \ldots \cdot w_{r_\ell}(v) = -w_{r_1}(v) = -v$. Таким образом, мы получили, что $2v = v - w_{r_2} \cdot \ldots \cdot w_{r_\ell}(v)$ является линейной комбинацией векторов $r_2, \ldots, r_\ell$. Поэтому $r_2, \ldots, r_\ell$ образуют базис гиперплоскости H_{r_1}. Повторяя данные рассуждения, мы получаем, что векторы $r_1, r_2, \ldots, r_\ell$ попарно ортогональны. □

Обозначим через W_0 подмножество группы W, состоящее из элементов w, представимых в виде $w = w_1 \cdot w_2$, причем $w_1^2 = w_2^2 = 1$ и $V_{-1}(w_1) \cap V_{-1}(w_2) = \{0\}$. Ясно, что W_0 инвариантно относительно сопряжений и потому является объединением сопряженных классов группы W.

Лемма 2.7.5. *Пусть $w \in W_0$ представлен в виде $w = w_1 \cdot w_2$, где $w_1^2 = w_2^2 = 1$ и $V_{-1}(w_1) \cap V_{-1}(w_2) = \{0\}$. Тогда $\bar{l}(w) = \bar{l}(w_1) + \bar{l}(w_2)$.*

Доказательство. Пусть $x \in V$ выбран так, что $w(x) = x$. Тогда $w_1 w_2(x) = x$ и, значит, $w_1(x) = w_2(x)$. Таким образом, $w_1(x) - x = w_2(x) - x$. Далее, $w_1(x) - x \in V_{-1}(w_1)$ и $w_2(x) - x \in V_{-1}(w_2)$. Поэтому оба из этих векторов равны 0, т. е. $V_1(w) = V_1(w_1) \cap V_1(w_2)$. Далее, $V_{-1}(w_1)^\perp = V_1(w_1)$ и $V_{-1}(w_2)^\perp = V_1(w_2)$. Поскольку $V_{-1}(w_1) \cap V_{-1}(w_2) = \{0\}$, мы имеем $V_1(w_1) + V_1(w_2) = V$. Таким образом,

$$\bar{l}(w) = \ell - \dim V_1(w) = 2\ell - \dim V_1(w_1) - \dim V_1(w_2) = \bar{l}(w_1) + \bar{l}(w_2),$$

где мы воспользовались тем, что $\dim V_1(w) = \dim(V_1(w_1) \cap V_1(w_2)) = \dim V_1(w_1) + \dim V_1(w_2) - \dim(V_1(w_1) + V_1(w_2)) = \dim V_1(w_1) + \dim V_1(w_2) - \ell$. □

Пусть $w \in W_0$ и $w = w_1 \cdot w_2$. Ввиду леммы 2.7.4 элемент w_1 можно записать в виде $w_1 = w_{r_1} \cdot \ldots \cdot w_{r_k}$, а элемент w_2 можно записать в виде $w_2 = w_{r_{k+1}} \cdot \ldots \cdot w_{r_m}$, где $m = \bar{l}(w)$ и множества $\{r_1, \ldots, r_k\}$, $\{r_{k+1}, \ldots, r_m\}$ состоят из попарно ортогональных корней. Таким образом, элементу w мы можем сопоставить диаграмму Γ, вершинами которой являются корни $\{r_1, \ldots, r_m\}$ и корни r_i, r_j соединены $< r_i, r_j > \cdot < r_j, r_i >$ ребрами. Очевидно, что любой сопряженный с w элемент из W имеет ту же диаграмму Γ. Таким образом, мы можем говорить о классе сопряженных элементов, соответствующем диаграмме Γ. Отметим, что одному классу может соответствовать, вообще говоря, несколько диаграмм.

Каждая диаграмма, получаемая таким образом, удовлетворяет следующим двум очевидным условиям:

1. Вершины диаграммы Γ соответствуют множеству линейно независимых корней.

2. Любой цикл в диаграмме Γ имеет четное количество вершин.

Любой граф, удовлетворяющий условиям 1 и 2 мы будем называть *допустимой диаграммой.* В [5] подробно изучены допустимые диаграммы для каждой неприводимой корневой системы. В частности, если допустимая диаграмма не имеет циклов, то она является диаграммой Дынкина некоторой подсистемы. Кроме того, изучен вопрос о том, когда одному классу соответствуют разные допустимые диаграммы и о том, когда разным классам соответствует одна допустимая диаграмма. Последовательным перебором различных типов неразложимых корневых систем доказано, что $W_0 = W$. Мы не будем здесь приводить все эти результаты ввиду громоздкости их изложения.

Глава 3. Введение в алгебраическую геометрию

В данной главе мы введем алгебраическую геометрию, определим линейные алгебраические группы и получим их основные свойства. Наше изложение в основном следует [17]. Заметим, что для понимания дальнейшего изложения достаточно знания понятий аффинного и проективного многообразия, размерности, касательного пространства и полных многообразий, т. е. прочтения параграфов §2, §3, §5 и §6. Остальные параграфы, в основном, приведены для полноты изложения.

§1 Вспомогательные результаты из общей алгебры

Большинство результатов данного параграфа изучаются в общем курсе алгебры и теории Галуа, и могут быть найдены в любом учебнике, например в [10]. Если R — некоторое кольцо и x — переменная или элемент из некоторого кольца R_1, содержащего R, то через $R[x]$ обозначается множество многочленов с коэффициентами из R и переменной x. По индукции, $R[x_1, \ldots, x_k] = R[x_1, \ldots, x_{k-1}][x_k]$. Все кольца в данном параграфе предполагаются коммутативными.

Определение 3.1.1. Говорят, что кольцо R удовлетворяет *условию обрыва возрастающих цепей* или *условию максимальности* (является *нётеровым*), если любая цепочка вложенных идеалов $I_1 \leq I_2 \leq \ldots$ на некотором шаге стабилизируется.

Лемма 3.1.2. *Следующие условия для кольца R эквивалентны:*

1. *Кольцо R является нётеровым.*
2. *Любой идеал кольца R конечнопорождён.*
3. *Всякое непустое множество S идеалов кольца R содержит максимальный элемент.*

Доказательство. 1⇒2. Пусть I — некоторый идеал кольца R. Рассмотрим $a_1 \in I \setminus \{0\}$ и пусть A_1 — идеал кольца R, порождённый элементом a_1. Далее рассмотрим $a_2 \in I \setminus A_1$ и пусть A_2 — это идеал кольца R, порождённый элементами a_1, a_2. Повторяя данную процедуру, получим цепь вложенных идеалов $A_1 < A_2 < \ldots$. Ввиду нётеровости кольца R, данная цепь на некотором шаге стабилизируется, т. е. для некоторого m справедливо $A_m = I$. Но идеал A_m конечнопорождён по построению.

2⇒3. Пусть S — непустое множество идеалов и рассмотрим в нём идеал I_1. Если он немаксимален, то в S существует $I_2 > I_1$. Если I_2 немаксимален, то в S существует $I_3 > I_2$ и т. д. Таким образом, если в S не существует максимального элемента, то мы получим строго возрастающую бесконечную цепь идеалов $I_1 < I_2 < \ldots$. Рассмотрим идеал I, равный объединению всех I_j. Идеал I конечнопорождён, т. е. существуют элементы $x_1, \ldots, x_k$, которые порождают весь I. По построению, все x_i лежат в некотором I_m. Но тогда $I_m < I \geqslant I_m$, что противоречит выбору строго возрастающей цепочки.

3⇒1. Очевидно. □

Теорема 3.1.3. (Теорема Гильберта о базисе) *Пусть R — коммутативное нётерово кольцо. Тогда кольцо $R[X]$ многочленов над R от одной переменной тоже нётерово.*

Доказательство. Пусть I — идеал в $R[X]$. Обозначим через A_i множество элементов $a \in R$, служащих старшими коэффициентами в многочленах $a_0 + a_1X + \ldots + a_iX^i$, лежащих в I (включая 0). Ясно, что A_i — это идеал в R. Кроме того, $A_i \leq A_{i+1}$, т. е. последовательность идеалов $A_0 \leq A_1 \leq \ldots$ возрастающая.

Действительно, если $f(X) \in I$ и его старший коэффициент равен $a_i \in A_i$, то $XF(X)$ вновь лежит в I и его старший коэффициент равен $a_i \in A_{i+1}$.

Так как кольцо R нётерово, последовательность идеалов $\{A_i\}$ стабилизируется? т. е. существует k такой, что $A_0 \leq A_1 \leq \ldots \leq A_k = A_{k+1} = \ldots$. Ввиду нётеровости кольца R, каждый из A_i конечнопорождён. Пусть $a_{i,1}, \ldots, a_{i,m_i}$ — множество порождающих для идеала A_i. Тогда $\{a_{i,j}X^i\}$ — множество порождающих для идеала I, т. е. идеал I конечнопорождён. □

Определение 3.1.4. Пусть $L/\mathbb{F}$ — расширение поля $\mathbb{F}$. Элементы $x_1, \ldots, x_m \in L$ называются *алгебраически независимыми* над $\mathbb{F}$, если для любого ненулевого многочлена $f(t_1, \ldots, t_m)$ с коэффициентами из $\mathbb{F}$ справедливо $f(x_1, \ldots, x_m) \neq 0$. Максимальное множество алгебраически независимых элементов поля L над полем $\mathbb{F}$ называется *базисом трансцендентности.* Количество элементов в базисе трансцендентности не зависит от выбора базиса и называется *степенью трансцендентности.* Обозначать мы её будем $tr.deg_{\mathbb{F}}L$. Если $L = \mathbb{F}(x_1, \ldots, x_m)$ и $x_1, \ldots, x_d$ — базис трансцендентности, то $\mathbb{F}(x_1, \ldots, x_d)$ — *чисто трансцендентное расширение* над $\mathbb{F}$ и L есть конечное алгебраическое расширение над $\mathbb{F}(x_1, \ldots, x_d)$

Определение 3.1.5. Пусть $R > S$ — расширение колец. Элемент $x \in R$ является *целым* над S, если x является корнем полинома с коэффициентами из S и со старшим коэффициентом 1. Кольцо R называется *целым* над S, если каждый элемент из R является целым над S. Подкольцо, состоящее из всех целых над S элементов называется *целым замыканием* кольца S в R.

Если R — область целостности с полем частных F и R совпадает со своим целым замыканием в F, то кольцо R называется *целозамкнутым.*

Лемма 3.1.6. *Пусть $R > S$ — расширение колец и $x \in R$. Тогда следующие утверждения эквивалентны:*

1. *Элемент x является целым над S.*
2. *Подкольцо $S[x]$ — это конечнопорождённый S-модуль.*
3. *Кольцо $S[x]$ действует точно на некотором конечнопорождённом S-модуле V.*

Доказательство. 1⇒2. Пусть $f(t)$ — многочлен с коэффициентом 1 при старшей степени и $f(x) = 0$. Пусть n — степень многочлена $f(t)$. Тогда элементы $x^0 = 1, x, x^2, \ldots, x^{n-1}$ порождают кольцо $S[x]$ как S-модуль.

2⇒3. Кольцо $S[x]$ является конечнопорождённым S-модулем и действует на себе точно левыми (или правыми) сдвигами.

3⇒1. Пусть M — конечнопорождённый S-модуль и $v_1 \in M \setminus \{0\}$. Тогда подмодуль $v_1, v_1x, v_1x^2, \ldots$ также конечно порождён (как S-модуль) и $S[x]$ действует на нем точно. Следовательно, существует такое n, что $v_1x^n = v_1(a_o + a_1x + \ldots + a_{n-1}x^{n-1})$, т. е. элемент $x^n - a_{n-1}x^{n-1} - \ldots - a_1x - a_0$ отправляет v_1 в 0. В силу коммутативности кольца S и поскольку мы рассматриваем модуль, порождённый v_1 (как $S[x]$-модуль) отсюда следует, что $x^n - a_{n-1}x^{n-1} - \ldots - a_1x - a_0 = 0$. □

Теорема 3.1.7. (Теорема Нётер о нормализации.) *Пусть $\mathbb{F}$ — поле, $R = \mathbb{F}[x_1, \ldots, x_n]$ — конечнопорождённая область целостности над $\mathbb{F}$ с полем частных K и $d = tr.deg_{\mathbb{F}}K$. Тогда существуют $y_1, \ldots, y_d \in R$ такие, что кольцо R цело над $\mathbb{F}[y_1, \ldots, y_d]$ и элементы $y_1, \ldots, y_d$ алгебраически независимы над $\mathbb{F}$.*

Доказательство. Если $x_1, \ldots, x_n$ алгебраически независимы над $\mathbb{F}$, то доказывать нечего. В противном случае существует такой многочлен $f(T) \in \mathbb{F}[T_1, \ldots, T_n]$, что $f(x_1, \ldots, x_n) = 0$. Пусть $m_2, \ldots, m_n \in \mathbb{N}$, положим $y_2 = x_2 - x_1^{m_2}, \ldots, y_n = x_n - x_1^{m_n}$ и подставим $x_i = y_i + x_1^{m_i}, 2 \leqslant i \leqslant n$ в равенство $f(x_1, \ldots, x_n) = 0$. Тогда многочлен $f(x_1, \ldots, x_n)$ можно записать в виде $f(x_1, \ldots, x_n) = g(x_1) + h(x_1, y_2, \ldots, y_n)$ и у многочлена $h(x_1, y_2, \ldots, y_n)$ уже нет одночленов, являющихся степенью x_1. Пусть теперь d на 1 больше, чем максимальная степень переменной T_1 многочлена $f(T_1, \ldots, T_n)$ и выберем $m_2 = d, m_3 = d^2, \ldots, m_n = d^{n-1}$. Тогда не все коэффициенты многочлена $g(x_1)$ будут равны 0, следовательно, мы получаем целое уравнение для x_1 над $\mathbb{F}[y_2, \ldots, y_n]$. Индукция по числу порождающих завершает доказательство. □

Рассмотрим кольцо R с единицей. Подмножество S кольца R называется *мультипликативным подмножеством,* если S содержит единицу и для любых двух $x, y \in S$ элемент xy также лежит в S. Определим *кольцо частных кольца R по мультипликативному множеству S* следующим образом. Рассмотрим пары $(r, s), r \in R, s \in S$ и введём на них отношение эквивалентности $(a, s) \sim (a', s')$, если существет такой $t \in S$, что $t(s'a - sa') = 0$. Множество классов эквивалентности обозначается через $S^{-1}R$ и элементы этого множества удобно записывать в виде «дробей» $\frac{r}{s}$. Сложение и умножение дробей вводится обычным образом. Заметим, что если $0 \in S$, то $S^{-1}R$ состоит из одного элемента $\frac{0}{1}$, т. е., для того, чтобы избежать тривиального случая,

можно считать, что $0 \notin S$. Очевидно, что относительно таким образом определённых операций множество $S^{-1}R$ является кольцом. Кроме того, если R — *область целостности*(т. е. не содержит делителей нуля), то вложение $\varphi : R \to S^{-1}R$, заданное правилом $\varphi : a \mapsto \frac{a}{1}$, является инъективным.

Напомним, что идеал I кольца R называется *простым*, если R/I — область целостности. Пусть I — идеал кольца R и $S = R \setminus I$. Очевидно, что S является мультипликативным подмножеством кольца R. Тогда кольцо частных $S^{-1}R$ обозначается R_I и называется *локальным кольцом по идеалу* I. Напомним, что кольцо называется *локальным*, если оно содержит единственный максимальный идеал. Легко проверить, что если I — простой идеал, то R_I — локальное кольцо.

***Упражнение* 3.1.8.** Если I — простой идеал кольца R, то R_I — локальное кольцо с максимальным идеалом $(R \setminus I)^{-1}I$.

***Упражнение* 3.1.9.** Пусть кольцо R является целым над S. Предположим, что P — простой идеал кольца S. Тогда R_P является целым над S_P.

Лемма 3.1.10. (Лемма Накаямы.) *Пусть R — кольцо, M — пересечение всех его максимальных идеалов и V — конечнопорождённый R-модуль, для которого $V = MV$. Тогда $V = 0$. В частности, если R локально, то M является единственным максимальным идеалом.*

Доказательство. Пусть $v_1, \ldots, v_n$ порождают R-модуль V. Ввиду равенства $V = MV$, существует представление $v_1 = m_1v_1 + \ldots + m_nv_n$ для некоторых $m_1, \ldots, m_n \in M$, откуда $(1 - m_1)v_1 = m_2v_2 + \ldots + m_nv_n$. Предположим, что элемент $1 - m_1$ необратим. Тогда он содержится в некотором максимальном идеале I кольца R. Поскольку $m_1 \in M \le I$, мы получаем, что $1 \in I$, противоречие. Значит, элемент $1 - m_1$ обратим и мы можем считать, что он равен 1. В частности, модуль V может быть порождён $n-1$ элементом. Индукция по числу порождающих завершает доказательство. □

***Упражнение* 3.1.11.** Доказать, что если R — локальное кольцо с единицей и M — его единственный максимальный идеал, то любой элемент $x \in R \setminus M$ обратим.

Теорема 3.1.12. (Теорема о подъеме.) *Если P — простой (максимальный) идеал кольца S и R целое над S, то существует простой (максимальный) идеал Q кольца R, для которого $Q \cap S = P$.*

Доказательство. Ввиду упражнений 3.1.8 и 3.1.9, кольцо R_P является целым над S_P и S_P — локальное кольцо с максимальным идеалом $M_P = (S \setminus P)^{-1}P$. Покажем сначала, что $PR \ne R$. Очевидно, что $PR_P = PS_PR_P = (S \setminus P)PR_P$, то для доказательства неравенства можно считать, что S — локальное кольцо. Если $PR = R$, то выполнено $1 = p_1r_1 + \ldots + p_nr_n$, где $p_i \in P$, $r_i \in R$. Пусть R_0 — S-подалгебра кольца R, порождённая элементами $r_1, \ldots, r_n$. Тогда R_0 является целым над S и, по лемме 3.1.6, $PR_0 = R_0$ является конечнопорождённым S-модулем. По лемме Накаямы 3.1.10, $B_0 = 0$, противоречие.

Рассмотрим следующую коммутативную диаграмму

$$\begin{array}{ccc} S & \to & S_P \\ \downarrow & & \downarrow \\ R & \to & R_P \end{array}$$

Поскольку $(S \setminus P)PR_P \ne R_P$, то $(S \setminus P)PR_P$ содержится в некотором максимальном идеале N кольца R_P. Переходя к прообразам, мы получаем, что прообраз N в S_P есть идеал, содержащий $(S \setminus P)P$. Так как $(S \setminus P)P$ — максимальный идеал в S_P, то $N \cap S_P = (S \setminus P)P$. Пусть Q — прообраз идеала N в B. Тогда Q — простой идеал в B и $Q \cap S = P$.

Для доказательства теоремы для максимального идеала, покажем, что идеал Q максимален в том и только в том случае, если P максимален. Часть "только в том"очевидна. Предположим, что P максимален в S. Тогда S/P — поле и R/Q — кольцо, целое над S/P. Если $a \in R/Q$, то элемент a алгебраичен над S/P и, следовательно, S/P -алгебра, порождённая элементом a является полем. Поэтому всякий ненулевой элемент из B/Q обратим в B/Q, т. е. B/Q — поле. □

Теорема 3.1.13. (Теорема о спуске.) *Пусть кольцо S целозамкнуто, если $P_1 > P_2$ — простые идеалы кольца S и Q_1 — простой идеал кольца R, для которого $Q_1 \cap S = P_1$, то существует простой идеал $Q_2 < Q_1$ кольца R, для которого $Q_2 \cap S = P_2$.*

Доказательство. Очевидно, что Q_2 совпадает с пересечением всех идеалов, лежащих над P_2, существование которых гарантирует теорема о подъёме 3.1.12. □

Теорема 3.1.14. (Теорема о продолжении гомоморфизмов.) *Пусть $R > S$ — целое расширение и $\mathbb{F}$ — алгебраически замкнутое поле. Тогда любой гомоморфизм $\varphi : S \to \mathbb{F}$ продолжается до гомоморфизма $\varphi : R \to \mathbb{F}$.*

Доказательство. Пусть P — ядро гомоморфизма φ и $S = S \setminus P$. Мы имеем следующую коммутативную диаграмму:

$$\begin{array}{ccccc} R & \to & (S \setminus P)^{-1}R & & \\ \uparrow & & \uparrow & & \\ S & \to & (S \setminus P)^{-1}S & = & S_P \end{array}$$

и φ может быть пропущен через канонический гомоморфизм $S \to (S \setminus P)^{-1}S$. Действительно, на S_P гомоморфизм φ задан правилом $(x/y)^\varphi = (x\varphi)/(y\varphi)$. Кроме того, кольцо $(S \setminus P)^{-1}R$ — целое над $(s \setminus P)^{-1}S$ (см. упражнение 3.1.9). Таким образом, кольца R, S можно считать локальными, более того, ядро гомоморфизма φ совпадает с единственным максимальным идеалом P_1 кольца S_P. В силу теоремы о подъёме 3.1.12, существует максимальный идеал Q кольца R_P лежащий над P_1. Тогда R_P/Q — поле, являющееся алгебраическим расширением поля S_P/P_1, которое, в свою очередь, является подполем поля $\mathbb{F}$. В силу алгебраической замкнутости поля $\mathbb{F}$, мы получаем гомоморфизм из R_P/Q в $\mathbb{F}$, композиция которого с каноническим гомоморфизмом $R_P \to R_P/Q$ даёт нам требуемый гомоморфизм $R_P \to \mathbb{F}$. □

Определение 3.1.15. Расширение E поля $\mathbb{F}$ называется *сепарабельным*, если либо характеристика поля $\mathbb{F}$ равна 0, либо она равна $p > 0$ и p-е степени линейно независимых элементов над $\mathbb{F}$ вновь являются линейно независимыми.

§2 Аффинные многообразия, топология Зарисского

В данном параграфе мы определим важнейший класс многообразий — аффинные многообразия, топологию Зарисского, а также установим ряд основных свойств аффинных многообразий.

Определение 3.2.1. Пусть $\mathbb{F}$ — алгебраически замкнутое поле. Множество $\mathbb{F}^n = \mathbb{F} \times \mathbb{F} \times \ldots \times \mathbb{F}$ называется *аффинным пространством* и обозначать A^n. Если I — идеал в кольце многочленов $\mathbb{F}[t_1, \ldots, t_n]$ от n переменных над $\mathbb{F}$, то через $\mathcal{V}(I)$ мы будем обозначать множество нулей идеала I в A^n. Множество $\mathcal{V}(I)$ называется *аффинным многообразием*. Обратно, если $X \subset A^n$, то через $\mathcal{I}(X)$ будет обозначаться множество многочленов, обращающихся в 0 на любом элементе из X. *Радикалом* идеала I называется множество $\sqrt{I} = \{f | f^k \in I\}$ для некоторого $k > 0$.

Теорема 3.2.2. (Гильберта о нулях.) *Если I — некоторый идеал из $\mathbb{F}[t_1, \ldots, t_n]$, то $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$.*

Доказательство. Ввиду конечной порождённости идеала I (по теореме Гильберта о базисе 3.1.3, кольцо $\mathbb{F}[t_1, \ldots, t_n]$ нётерово), теорема эквивалентна следующему утверждению:

для любых полиномов $f(T), f_1(T), \ldots, f_s(T) \in \mathbb{F}[T]$, таких что $f([T])$ обращается в 0 в каждой точке $x \in A^n$, в которой обращаются в ноль все полиномы $f_1(T), \ldots, f_s(T)$, существуют $k > 0$ и полиномы $g_1(T), \ldots, g_s(T)$, удовлетворяющие соотношению $f(T)^k = \sum_{i=1}^s g_i(T) f_i(T)$. Здесь и далее T используется для замены набора переменных $t_1, \ldots, t_n$.

Покажем сначала, что достаточно доказать следующее:

если $\mathcal{V}(I) = \varnothing$, то $I = \mathbb{F}[T]$ $\quad(*)$.

Действительно, введем новую переменную t_0 и рассмотрим совокупность полиномов от $(n+1)$-й переменной: $f_1(T), \ldots, f_s(T), 1 - t_0 f(T)$. Они не имеют общих нулей в A^{n+1}, поскольку $f(T)$ обращается в 0 во всех точках, в которых Действительно, введем новую переменную t_0 и рассмотрим совокупность полиномов от $(n+1)$-й переменной: $f_1(T), \ldots, f_s(T), 1 - t_0 f(T)$. Они не имеют общих нулей в A^{n+1}, поскольку $f(T)$ обращается в 0 во всех точках, в которых в 0 обращаются многочлены $f_1(T), \ldots, f_s(T)$. Из $(*)$ следует, что они порождают кольцо $\mathbb{F}[T, t_0]$. Найдем полиномы $h_1(t_0, T), \ldots, h_s(t_0, T), h(t_0, T)$, для которых $1 = h_1(t_0, T) f_1(T) + \ldots + h_s(t_0, T) f_s(T) + (1 - t_0 f(T)) h(t_0, T)$. Теперь подставим вместо t_0 выражение $1/f(T)$ и затем умножим на достаточно большую степень $f(T)^k$, чтобы избавиться от знаменателей. Таким образом получим требуемое соотношение.

Остается доказать утверждение $(*)$ или, что эквивалентно, что любой в 0 обращаются многочлены $f_1(T), \ldots, f_s(T)$. Из $(*)$ следует, что они порождают кольцо $\mathbb{F}[T, t_0]$. Найдем полиномы $h_1(t_0, T), \ldots, h_s(t_0, T)$, $h(t_0, T)$, для которых $1 = h_1(t_0, T) f_1(T) + \ldots + h_s(t_0, T) f_s(T) + (1 - t_0 f(T)) h(t_0, T)$. Теперь подставим вместо t_0 выражение $1/f(T)$ и затем умножим на достаточно большую степень $f(T)^k$, чтобы избавиться от знаменателей. Таким образом получим требуемое соотношение.

Остается доказать утверждение (∗) или, что эквивалентно, что любой собственный идеала I в $\mathbb{F}[T]$ имеет по меньшей мере один общий 0. По лемме Цорна и в силу нётеровости кольца $\mathbb{F}[T]$, любой идеал I лежит в некотором максимальном идеале J кольца $\mathbb{F}[T]$. Таким образом, можно считать идеал I максимальным. Тогда $L = \mathbb{F}[T]/I$ — это поле; более того, если $x_1, \ldots, x_n$ — классы вычетов переменных $t_1, \ldots, t_n$, то $L = \mathbb{F}[x_1, \ldots, x_n]$ — конечное расширение поля $\mathbb{F}$. Ввиду алгебраической замкнутости поля $\mathbb{F}$, мы получаем, что $L = \mathbb{F}$, т. е. $x_1, \ldots, x_n \in \mathbb{F}$. Кроме того, для любого $f \in I$ справедливо $f = f(t_1, \ldots, t_n) \in I$, т. е. $f(x_1, \ldots, x_n) = 0$. □

Определение 3.2.3. Рассмотрим теперь множество всех аффинных многообразий в A^n и определим топологию, в которой замкнутыми множествами являются аффинные многообразия. Очевидно, что пустое множество и все A^n являются замкнутыми, кроме того, объединение любого конечного числа замкнутых множеств вновь замкнуто и пересечение любого числа замкнутых множеств тоже замкнуто. Таким образом, мы действительно получаем топологию, называемую *топологией Зарисского.*

Пусть X — топологическое пространство. Пространство X называется *неприводимым*, если X нельзя представить в виде объединения двух собственных замкнутых подмножеств. Подпространство Y пространства X называется *неприводимым*, если оно неприводимо как топологическое пространство с индуцированной топологией. Заметим, что непосредственно из определения вытекает следующая

Лемма 3.2.4. *Пусть X — топологическое пространство. Тогда следующие утверждения эквивалентны:*

1. *Пространство X неприводимо.*
2. *Любые два непустые открытые подмножества из X имеют непустое пересечение*
3. *Любое непустое открытое множество плотно в X.*

Лемма 3.2.5. *Пусть X — топологическое пространство. Тогда*

1. *Подпространство Y пространства X неприводимо тогда и только тогда, когда его замыкание в X неприводимо.*
2. *Если $\varphi : X \to X'$ — непрерывное отображение и пространство X неприводимо, то и пространство $\varphi(X)$ неприводимо.*

Определение 3.2.6. Топологическое пространство называется *нётеровым* если выполнено одно из следующих эквивалентных условий:

1. Открытые множества удовлетворяют условию обрыва возрастающих цепей.
2. Любая совокупность открытых множеств имеет максимальный элемент.
3. Замкнутые множества удовлетворяют условию обрыва убывающих цепей.
4. Любая совокупность замкнутых множеств имеет минимальный элемент.

Лемма 3.2.7. *Пусть X — нётерово топологическое пространство. Тогда X обладает лишь конечным числом неприводимых максимальных подпространств (в силу леммы* 3.2.5 *обязательно замкнутых). Более того, их объединение совпадает с X.*

Доказательство. Рассмотрим совокупность $\mathcal{A}$ всех конечных объединений замкнутых неприводимых подмножеств пространства X. Тогда $\mathcal{A}$ непусто (например, $\varnothing \in \mathcal{A}$). Если $X \notin \mathcal{A}$, то в силу нётеровости пространства X существует замкнутое подпространство Y, являющееся минимальным среди замкнутых подпространств непринадлежащих $\mathcal{A}$. Тогда Y не является пустым и не является неприводимым множеством, следовательно, $Y = Y_1 \cup Y_2$, где $Y_1, Y_2 \in \mathcal{A}$. Но тогда, по построению, $Y \in \mathcal{A}$.

Запишем теперь $X = X_1 \cup \ldots \cup X_n$, где все X_i — неприводимые замкнутные подмножества. Если теперь Y — некоторое максимальное неприводимое замкнутое подмножество, то $Y \subseteq \cup_{i=1}^{n}(X_i \cap Y)$, все $Y \cap X_i$ неприводимы, следовательно, $Y \cap X_i = Y$, т. е. $Y = X_i$. □

Максимальные неприводимые замкнутые подмножества нётерова пространства X называются *неприводимыми компонентами* пространства X.

Лемма 3.2.8. *Замкнутое множество X пространства A^n неприводимо тогда и только тогда, когда $\mathcal{I}(X)$ — простой идеал. В частности, A^n неприводимо.*

Доказательство. Пусть $I = \mathcal{I}(X)$ и X неприводимо. Предположим, что $f_1(T) \cdot f_2(T) \in I$ (т. е. образ их произведение равен нулю в $R[T]/I$). Тогда каждая точка $x \in X$ является либо нулем для $f_1(T)$, либо нулем для $f_2(T)$. Пусть I_1 — идеал, порождённый полиномом $f_1(T)$ и I_2 — идеал, порождённый полиномом $f_2(T)$. Тогда $X \subseteq \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$. В силу неприводимости множества X получаем, что либо $X \subseteq \mathcal{V}(I_1)$, либо $X \subseteq \mathcal{V}(I_2)$, т. е. либо $f_1(T)$, либо $f_2(T)$ лежит в I.

Обратно, пусть I — простой идеал и предположим, что $\mathcal{V}(I) = X = X_1 \cup X_2$, где каждое из X_i замкнуто. Если $X \neq X_1$ и $X \neq X_2$, то существуют $f_1(T) \in \mathcal{I}(X_1)$ и $f_2(T) \in \mathcal{I}(X_2)$ такие, что $f_1(T), f_2(T) \notin I$, но $f_1(T) \cdot f_2(T) \in I$, что противоречит простоте идеала I. □

Пусть $X \subseteq A^n$, $Y \subseteq A^m$ — замкнутые неприводимые множества. Определим топологию Зарисского на $X \times Y$ следующим образом: мы вкладываем множество $X \times Y$ в A^{n+m} и снабжаем его индуцированной топологией пространства A^{n+m}. Тогда $X \times Y$ будет замкнуто как множество нулей полиномов вида $f(T_1, \ldots, T_n) \cdot g(U_1, \ldots, U_m)$, где $f(T) \in \mathcal{I}(X)$ и $g(U) \in \mathcal{I}(Y)$. Таким образом определенная топология называется *топологией Зарисского произведения.*

Лемма 3.2.9. *Пусть $X \subseteq A^n$, $Y \subseteq A^m$ — замкнутые неприводимые подмножества. Тогда множество $X \times Y$ замкнуто и неприводимо в A^{m+n}.*

Доказательство. Выше мы уже отмечали замкнутость множества $X \times Y$, таким образом, нам осталось доказать его неприводимость. Предположим, что $X \times Y = Z_1 \cup Z_2$, где Z_1, Z_2 — замкнутые подмножества в A^{n+m}. Если $x \in X$, то множество $\{x\} \times Y$ замкнуто. Оно также неприводимо, так как если $\{x\} \times Y = U_1 \cup U_2$, то U_1 и U_2 имеют вид $\{x\} \times V_i$, где V_i — замкнутое подмножество в Y, что противоречит неприводимости пространства Y. Таким образом, для любого $x \in X$ имеем $\{x\} \times Y \subseteq Z_i$ для подходящего Z_i. Тогда $X = X_1 \cup X_2$, где $X_i = \{x | \{x\} \times Y \subseteq Z_i\}$. Заметим, что каждое множество X_i замкнуто в X. Действительно, множество $(X \times \{y\})$ замкнуто для любого y, поэтому множество $(X \times \{y\}) \cap Z_i$ замкнуто. Наконец, $X_i = \cap_{y \in Y} ((X \times \{y\}) \cap Z_i)$. □

Пусть $X \subseteq A^n$ — замкнутое подмножество. Тогда каждый многочлен $f(T) \in \mathbb{F}[T]$ определяет функцию на X со значениями в $\mathbb{F}$ по правилу $x \mapsto f(x)$. Очевидно, что кольцо таких функций изоморфно $\mathbb{F}[T]/\mathcal{I}(X)$. Обозначим это кольцо через $\mathbb{F}[X]$ и будем называть его *аффинной алгеброй* множества X (или *алгеброй полиномиальных функций* на X). Поскольку $\mathbb{F}[T]$ нётерово, кольцо $\mathbb{F}[X]$ также нётерово и конечно порождено. Если множество X неприводимо, то по лемме 3.2.8 идеал $\mathcal{I}(X)$ является простым, т. е. $\mathbb{F}[X]$ — это область целостности и у него существует поле частных $\mathbb{F}(X)$, которое называется *полем рациональных функций* на X.

Рассмотрим множества $X_f = \{x \in X | f(x) \neq 0\}$, где $f \in \mathbb{F}[X]$. Ясно, что X_f — открытые множества в X. Более того, они образуют базис топологии Зарисского на X и называются *главными открытыми множествами.* По теореме Гильберта о нулях 3.2.2 замкнутые подмножества множества X находятся во взаимно однозначном соответствии с радикальными идеалами кольца $\mathbb{F}[X]$, неприводимые подмножества соответствуют простым идеалам кольца $\mathbb{F}[X]$, а точки пространства X соответствуют максимальным идеалам кольца $\mathbb{F}[X]$ или гомоморфизмам $\mathbb{F}$-алгебр $\mathbb{F}[X] \to \mathbb{F}$. Таким образом, пространство X восстанавливается по $\mathbb{F}[X]$.

Определение 3.2.10. Кольцо R называется *приведённым*, если оно не содержит нетривиальных нильпотентных элементов. Заметим, что фактор кольцо $\mathbb{F}[T]/I$ алгебры многочленов $\mathbb{F}[T]$ является приведённым тогда и только тогда, когда идеал I радикальный. В частности, аффинная алгебра $\mathbb{F}[X]$ любого аффинного многообразия X является приведённой.

Пусть теперь R — произвольная приведённая коммутативная конечно порождённая алгебра над полем $\mathbb{F}$, скажем, $R = \mathbb{F}[t_1, \ldots, t_n]$ (число n и выбор образующих неединственны). Тогда R — гомоморфный образ алгебры $\mathbb{F}[T_1, \ldots, T_n]$ с ядром I и, в силу сказанного выше, I — радикальный идеал. Таким образом, $R \simeq \mathbb{F}[X]$, где $\mathcal{V}(I) = X \subseteq \mathbb{F}^n$.

Пусть теперь $X \subseteq A^n$, $Y \subseteq A^m$ — произвольные аффинные многообразия. *Морфизмом* многообразий называется отображение $\varphi : X \to Y$, заданное правилом $(x_1, \ldots, x_n)^\varphi \mapsto (\psi_1(x), \ldots, \psi_m(x))$, где $\psi_i \in \mathbb{F}[X]$ для всех i. Очевидно, что морфизм $X \to Y$ всегда индуцирован некоторым морфизмом $A^n \to A^m$, морфизм $X \to A^1$ — это полиномиальная функция на X. Кроме того, морфизм является непрерывным отображением в топологии Зарисского, т. е. прообразы открытых множеств открыты.

Морфизму $\varphi : X \to Y$ соответствует *коморфизм* аффинных алгебр $\varphi^* : \mathbb{F}[Y] \to \mathbb{F}[X]$, определяемый соотношением $f^{\varphi^*} = \varphi \circ f$, т. е. композиция морфизма φ и функции f.

§3 Проективные многообразия, произведение проективных многообразий

Определение 3.3.1. Рассмотрим множество $\mathbb{F}^{n+1} \setminus \{(0,0,\ldots,0)\}$ и введём на нем следующее отношение эквивалентности: $(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n)$ если существует $a \in \mathbb{F} \setminus \{0\} = \mathbb{F}^*$ такой, что $ax_i = y_i$ для всех i. Множество классов эквивалентности обозначается P^n и называется *проективным пространством* размерности n. Если V — это векторное пространство размерности $n+1$, то P^n — это множество прямых, проходящих через начало координат и обозначается обычно $P(V)$.

Каждая точка проективного пространства P^n задается *однородными координатами* $(x_0, x_1, \ldots, x_n)$, которые определяются с точностью до ненулевого множителя из $\mathbb{F}$. Полином $f(T_0, T_1, \ldots, T_n)$ называется *однородным* степени d, если он есть линейная комбинация одночленов вида $T_0^{i_0} \cdot T_1^{i_1} \cdot \ldots \cdot T_n^{i_n}$, у которых $\sum_{j=0}^n i_j = d$ (или если $f(aT_0, aT_1, \ldots, aT_n) = a^d f(T_0, T_1, \ldots, T_n)$).

Введём на P^n топологию Зарисского, выбирая в качестве замкнутых множеств нули системы однородных полиномов (или идеала, порождённого этими полиномами). Как и в аффинном случае определим $\mathcal{V}(I)$ и $\mathcal{I}(X)$ для идеала I и замкнутого множества X соответственно. Замкнутые множества называются *проективными многообразиями*. Как и в аффинном случае идеал $\mathcal{I}(X)$ является *радикальным*. Кроме того, имеет место аналог теоремы Гильберта о нулях.

Лемма 3.3.2. *Операторы $\mathcal{V}$ и $\mathcal{I}$ устанавливают взаимно однозначное соответствие (с изменением включения) между замкнутыми подмножествами пространства P^n и однородными радикальными идеалами кольца $\mathbb{F}[T_0, T_1, \ldots, T_n]$, отличными от $I_0 = \langle T_0, T_1, \ldots, T_n \rangle$.*

Пусть U_i — множество точек пространства P^n с ненулевой i-ой координатой. Тогда точки множества U_i взаимно однозначно соответствуют точкам аффинного пространства A^n при отображении

$$(x_0, x_1, \ldots, x_n) \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, 1, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}).$$

Координаты $(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, 1, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$ называются *аффинными координатами* множества U_i. Заметим, что множества U_i накрывают все P^n. Более того, при таком соответствии согласуются также и топологии Зарисского. Действительно, каждому полиному $f(X_1, \ldots, X_n)$ можно сопоставить однородный полином $T_i^{deg(f)} f(T_0/T_i, \ldots, T_{i-1}/T_i, T_{i+1}/T_i, \ldots, T_n/T_i)$, где $deg(f)$ — наибольшая степень одночленов, входящих в $f(X)$. Тогда если $X \subseteq A^n$ — множество нулей некоторых полиномов $f(X)$. то образ множества X в U_i есть пересечение множества U_i с множеством нулей в P^n соответствующих однородных полиномов. Обратно, пусть $X \subseteq P^n$ — множество нулей некоторой совокупности однородных полиномов $f(T_0, \ldots, T_n)$. Для каждого i рассмотрим полином $f(T_0/T_i, \ldots, T_{i-1}/T_i, 1, T_{i+1}/T_i, \ldots, T_n/T_i) = f(X_1, \ldots, X_n)$. Ясно, что множество $X \cap U_i$ соответствует множеству нулей в A^n полиномов $f(X)$.

Определение 3.3.3. Подмножества U_i пространства P^n называются *аффинными открытыми подмножествами.* Подмножество X пространства P^n замкнуто тогда и только тогда, когда его пересечение с любым аффинным открытым подмножеством замкнуто.

Пусть теперь $X \subseteq P^n$, $Y \subseteq P^m$ — два проективных многообразия. Рассмотрим вложение $\varphi : P^n \times P^m \to P^q$, где $q = (n+1)(m+1) - 1$, задаваемое соотношением

$$((x_0, x_1, \ldots, x_n), (y_0, y_1, \ldots, y_m)) \mapsto (x_0y_0, \ldots, x_ny_0, \ldots, x_ny_m).$$

Заметим, что $(P^n \times P^m)^\varphi$ замкнуто в P^q. Действительно, пусть однородные координаты в P^n обозначены через X_i, однородные координаты в P^m — через Y_j, в P^q — через $Z_{i,j}$. Пусть P_i^n, P_j^m, $P_{i,j}^q$ — аффинные открытые множества, соответствующие координатам i, j, i,j и пусть S_i, T_j, $U_{i,j}$ — их аффинные координаты. Ясно, что φ отображает $P_i^n \times P_j^m$ в $P_{i,j}^q$. Разберём случай $i = j = 0$. В аффинных координатах φ отображает $((s_1, \ldots, s_n), (t_1, \ldots, t_m))$ в $(\ldots, u_{k,l}, \ldots)$, где $u_{k,l} = s_k \cdot t_l$. Следовательно, образ $P_0^n \times P_0^m$ в $P_{0,0}^q$ является множеством решений уравнений $U_{k,l} = U_{k,0} \cdot U_{0,l}$ и, значит, является замкнутым множеством. Как мы заметили выше, отсюда следует, что образ множества $P^n \times P^m$ замкнут в P^q. Кроме того, для любого $P_{i,j}^q$ можно построить обратное отображение, следовательно, φ является изоморфизмом. Таким образом, $X \times Y$ — это замкнутое подмножество в P^q и на нём задана индуцированная топология Зарисского. Мы получили следующую лемму.

Лемма 3.3.4. *Отображение $\varphi : P^n \times P^m \to P^{nm+n+m}$, заданное выше, является биекцией на замкнутое множество. Если множество X замкнуто в P^n, а Y замкнуто в P^m, то множество $(X \times Y)^\varphi$ замкнуто в P^{nm+n+m}.*

§4 Предмногообразия и многообразия

Напомним, что содержание данного параграфа не является необходимым для понимания дальнейшего изложения, однако здесь приводится ряд вспомогательных утверждений, которые будут использоваться для доказательства важных результатов в дальнейшем.

Рассмотрим неприводимое аффинное многообразие X и его поле функций $\mathbb{F}(X)$ (в силу леммы 3.2.8 алгебра $\mathbb{F}[X]$ является областью целостности и потому мы можем построить поле частных $\mathbb{F}(X)$). Пусть $x \in X$ и рассмотрим рациональные функции вида $f = \{\frac{g}{h} | h(x) \neq 0\}$. Эти функции образуют кольцо $\mathcal{Q}_x$, называемое *локальным кольцом в точке* x. Заметим, что $\mathcal{Q}_x$ является локальным кольцом алгебры $\mathbb{F}[X]$ по простому идеалу $\mathcal{I}(x)$ и единственный его максимальный идеал $m_x = \{\frac{g}{h} | g(x) = h(x) = 0\}$ (см. упражнение 3.1.8).

***Упражнение* 3.4.1.** Пусть X — неприводимое аффинное многообразие и $\mathbb{F}(X)$ — поле частных алгебры $\mathbb{F}[X]$. Пусть $f \in \mathbb{F}(X)$ — произвольная функция из $\mathbb{F}(X)$.

Тогда $\{y | f(y)$ определена$\}$ — открытое подмножество в X.

Лемма 3.4.2. *Пусть X — неприводимое аффинное многообразие. Тогда $\mathbb{F}[X] = \bigcap_{x\in X} \mathcal{Q}_x$ (т. е. локальные кольца определяют алгебру $\mathbb{F}[X]$).*

Доказательство. Очевидно, что $\mathbb{F}[X] \subseteq \bigcap_{x\in X} \mathcal{Q}_x$. Обратно, предположим, что некоторая функция f из $\mathbb{F}(X)$ лежит в $\bigcap_{x\in X} \mathcal{Q}_x$, т. е., для любого $x \in X$, функция f представима в виде $f = \frac{g}{h}$ для некоторых функций $g, h \in \mathbb{F}[X]$, причём $h(x) \neq 0$ (очевидно, что данное представление неединственно). Рассмотрим идеал I, порождённый всеми возможными знаменателями. Если I — собственный идеал алгебры $\mathbb{F}[X]$, то, по теореме Гильберта о нулях 3.2.2, мы получаем, что существует $x \in \mathcal{V}(I)$, что противоречит построению идеала I. Следовательно, $I = \mathbb{F}[X]$ и существуют такие $g_i, h_i, t_i \in \mathbb{F}[X]$, что $f = \frac{g_i}{h_i}$ и $\sum_i h_i t_i = 1$. Умножая второе равенство на f, мы получаем, что $f = \sum_i g_i t_i \in \mathbb{F}[X]$. □

Пусть X — неприводимое аффинное многообразие, сопоставим каждому непустому открытому подмножеству U множества X подкольцо поля $\mathbb{F}(X)$, состоящее из всех *регулярных* (т. е. всюду определённых) функций на U следующим образом: $\mathcal{Q}_X(U) = \bigcap_{x\in U} \mathcal{Q}_x$. Ввиду леммы 3.4.2 мы получаем, что $\mathcal{Q}_X(X) = \mathbb{F}[X]$.

***Упражнение* 3.4.3.** Доказать равенства $\mathcal{Q}_X(X_f) = \mathbb{F}[X_f] = \mathbb{F}[X]_f$, где $\mathbb{F}[X]_f$ — локальное кольцо по идеалу, порождённом элементом f.

Отображение $\mathcal{Q}_X$, переводящее открытые подмножества многообразия X в подкольца поля $\mathbb{F}(X)$ служит примером *пучка функций* на X. Определим пучок функций на топологическом пространстве как отображение $\mathcal{J}$, переводящее каждое открытое подмножество U пространства в некоторую $\mathbb{F}$-алгебру $\mathcal{J}(U)$, состоящую из функций на U со значениями в $\mathbb{F}$, причём выполнены следующие два требования.

(ПФ1) Если $U \subseteq V$ — два открытых множества и $f \in \mathcal{J}(V)$, то ограничение функции f на U лежит в $\mathcal{J}(U)$.

(ПФ2) Пусть U — открытое подмножество, покрытое открытыми подмножествами U_i, $i \in I$. Для данного $f_i \in \mathcal{J}(U_i)$ предположим, что f_i согласуется с f_j на $U_i \cap U_j$ для всех $i, j \in I$. Тогда существует $f \in \mathcal{J}(U)$, ограничение которой на U_i совпадает с f_i для всех $i \in I$

Очевидно, что отображение $\mathcal{Q}_X$, определённое выше, является пучком функций. Если теперь X — произвольное аффинное многообразие и $X = X_1 \cup \ldots \cup X_n$ — его единственное представление в виде объединения неприводимых компонент, то определим $\mathcal{Q}_X$ как расширение пучков $\mathcal{Q}_{X_i}$. Заметим, что, как и в неприводимом случае, $\mathcal{Q}_X(X) = \mathbb{F}[X]$.

Определим *неприводимое предмногообразие* X как неприводимое нётерово топологическое пространство, снабжённое пучком функций $\mathcal{Q}_X$ со значениями в $\mathbb{F}$ и такое, что X является объединением конечного числа открытых подмножеств U_i, каждое из которых изоморфно аффинному многообразию относительно ограничения пучка функций $\mathcal{Q}_X|_{U_i}$. *Предмногообразием* называется нётерово топологическое пространство X, неприводимые компоненты которого X_i являются неприводимыми предмногообразии и $\mathcal{Q}_{X_i}$, $\mathcal{Q}_{X_j}$ образуют один и тот же пучок функций на $X_i \cap X_j$ для всех i, j. Как и в аффинном случае, можно построить пучок функций $\mathcal{Q}_X$, являющийся расширением пучков $\mathcal{Q}_{X_i}$. Элементы пучка $\mathcal{Q}_U$ называются *регулярными функциями* на U, открытые подмножества U_{i_j} каждой из неприводимых компонент X_i называются *аффинными открытыми подмножествами* предмногообразия X.

***Упражнение* 3.4.4.** Доказать, что проективное многообразие P^n является предмногообразием.

Пусть X, Y — два предмногообразия.

Лемма 3.4.5. *Пусть Y — многообразие, X — произвольное предмногообразие. Тогда справедливы следующие утверждения.*

1. *Если $\varphi : X \to Y$ — морфизм, то график $\Gamma_\varphi = \{(x, x^\varphi) | X \in X\}$ замкнут в $X \times Y$.*

2. *Если $\varphi, \psi : X \to Y$ — морфизмы, совпадающие на некотором плотном подмножестве предмногообразия X, то $\varphi = \psi$.*

§5 Размерность многообразий, касательное пространство

Мы в дальнейшем будем рассматривать лишь аффинные и проективные многообразия, поэтому под термином *многообразие* понимается либо аффинное, либо проективное многообразие, либо их декартовы произведения. Если X — неприводимое проективное многообразие, то X можно представить в виде конечного объединения открытых аффинных изоморфных, как аффинные пространства, подмножеств U_i. Определим $\mathbb{F}[X] = \mathbb{F}[U_i]$. Ясно, что данное определение не зависит от выбора U_i. Более того, многообразие U_i неприводимо, следовательно, $\mathbb{F}[U_i]$ — простое кольцо и существует поле частных $\mathbb{F}(U_i) = \mathbb{F}(X)$.

Определение 3.5.1. Пусть X — неприводимое аффинное многообразие. Ввиду леммы 3.2.8 кольцо $\mathbb{F}[X]$ является простым и мы можем рассмотреть поле частных $\mathbb{F}(X)$. Тогда $\mathbb{F}(X)$ конечно порождено над $\mathbb{F}$, следовательно, $tr.deg_{\mathbb{F}}\mathbb{F}(X) = m$ конечна и называется *размерностью* многообразия X (обозначается $\dim X$). Если аффинное многообразие X не является неприводимым, то под размерностью многообразия X понимается максимум размерностей его неприводимых компонент. Если X — проективное многообразие, то X можно представить в виде конечного объединения открытых аффинных подмногообразий U_i и размерностью многообразия X в этом случае называется максимум размерностей многообразий U_i.

Заметим, что если X — неприводимое аффинное многообразие и X_f — главное открытое множество для некоторого $f \in \mathbb{F}[X]$, то $\mathbb{F}(X_f) = \mathbb{F}(X)$ и потому $\dim X_f = \dim X$. Так как любое открытое множество получается как пересечение конечного количества главных открытых множеств, мы получаем, что для любого открытого подмножества U в X справедливо $\dim U = \dim X$. Поскольку размерность для проективных многообразий определяется через размерность открытых аффинных подмножеств, мы получаем, что то же свойство справедливо и для проективных многообразий.

Лемма 3.5.2. *Пусть X, Y — неприводимые многообразия размерностей m и n соответственно. Тогда* $\dim X \times Y = m + n$.

Доказательство. Можно считать, что X, Y — аффинные многообразия, так как размерность и декартово произведение проективных многообразий вводится через их аффинные открытые подмножества. Пусть $X \subseteq A^p$ и $Y \subseteq A^q$. Пусть $S_1, \ldots, S_p$ и $T_1, \ldots, T_q$ — переменные аффинных колец $\mathbb{F}[A^p]$ и $\mathbb{F}[A^q]$ соответственно. Тогда их ограничения s_i, t_j на кольцах $\mathbb{F}[X], \mathbb{F}[Y]$ порождают поля $\mathbb{F}(X)$, $\mathbb{F}(Y)$ соответственно. С точностью до перенумерации мы можем выбрать базисы трансцендентности $s_1, \ldots, s_m$ и $t_1, \ldots, t_n$. Очевидно, что $\mathbb{F}(X \times Y) = \mathbb{F}(s_1, \ldots, s_p, t_1, \ldots, y_q)$ и что поле $\mathbb{F}(X \times Y)$ алгебраично над $\mathbb{F}(s_1, \ldots, s_m, t_1, \ldots, t_n)$. Таким образом, достаточно доказать, что поле $\mathbb{F}(s_1, \ldots, s_m, t_1, \ldots, t_n)$ трансцендентно над $\mathbb{F}$.

Предположим, что существует полиномиальное соотношение $f(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0$. Тогда для любого фиксированного набора $x_1, \ldots, x_m \in X$ мы имеем $f(x_1, \ldots, x_m, t_1, \ldots, t_n) = 0$. Но $t_1, \ldots, t_n$ алгебраически независимы, следовательно, все коэффициенты многочлена $f(x_1, \ldots, x_m, t_1, \ldots, t_n)$ равны 0. Кроме того, коэффициенты этого многочлена — это полиномы от $s_1, \ldots, s_m$, следовательно, они тоже все равны 0. Таким образом, $f(x_1, \ldots, x_m, t_1, \ldots, t_n)$ — нулевой многочлен. □

Лемма 3.5.3. *Пусть X — неприводимое многообразие и Y — собственное замкнутое неприводимое подмножество. Тогда* $\dim Y < \dim X$.

Доказательство. Можно считать, что X — аффинное многообразие размерности d. Пусть $R = \mathbb{F}[X]$ и $\overline{R} = \mathbb{F}[Y] = R/P$, где P — ненулевой простой идеал кольца R. В силу теоремы Нётер о нормализации 3.1.7, мы можем выбрать базисы трансцендентности полей $\mathbb{F}(X)$ и $\mathbb{F}(Y)$ в кольцах $\mathbb{F}[X]$ и $\mathbb{F}[Y]$ соответственно. Предположим, что $\dim Y \geqslant d$ и выберем $\overline{x}_1, \ldots, \overline{x}_d$ — алгебраически независимые элементы поля $\mathbb{F}(Y)$, лежащие в $\mathbb{F}[Y]$. Пусть $x_1, \ldots, x_d$ — их прообразы в кольце $\mathbb{F}[x]$. Рассмотрим $f \in P$ — произвольный ненулевой элемент. Так как $d = tr.deg_{\mathbb{F}}(\mathbb{F}(X))$, существует такой многочлен $g(T_0, T_1, \ldots, T_d)$, что $g(f, x_1, \ldots, x_d) = 0$. Поскольку $f \neq 0$ можно предположить, что $g(T_0, T_1, \ldots, T_d) \neq T_0 g'(T_0, T_1, \ldots, T_d)$, т. е. $h(x_1, \ldots, x_d) = g(0, x_1, \ldots, x_d) \neq 0$. Но тогда $h(\overline{x}_1, \ldots, \overline{x}_d) = 0$, противоречие. □

Предположим, что $X \subseteq A^n$ и $X = \mathcal{V}(I)$, где идеал I порождён полиномами $f(T_1, \ldots, T_n)$. Определим

$$\mathrm{d}_x f = \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x)(T_i - x_i),$$

дифференциал многочлена f в точке x. Пусть J — это идеал, порождённый многочленами $\mathrm{d}_x f$ по всем $f \in I$ для некоторой фиксированной точки x и рассмотрим $\mathrm{Tan}(X)_x = \mathcal{V}(J)$. Многообразие $\mathrm{Tan}(X)_x$ называется *касательным многообразием* в точке x.

Данное нами определение зависит от способа вложения множества X в A^n, поэтому мы приведём эквивалентное определение касательного пространства. Пусть X — неприводимое аффинное многообразие с полем функций $\mathbb{F}(X)$, $x \in X$ и рассмотрим рациональные функции вида $f = \{\frac{g}{h} | h(x) \neq 0\}$. Эти функции образуют кольцо $\mathcal{Q}_x$,, называемое *локальным кольцом в точке* x. Это кольцо действительно является локальным, т. е. содержит единственный максимальный идеал $m_x = \{\frac{g}{h} | g(x) = 0\}$. Тогда $\mathcal{Q}_x/m_x \simeq \mathbb{F}$ — поле и m_x/m_x^2 — векторное пространство над $\mathbb{F}$. Рассмотрим дуальное векторное пространство $(m_x/m_x^2)^*$ и обозначим его через $\mathcal{T}(X)_x$. Тогда $\mathcal{T}(X)_x \simeq \mathrm{Tan}(X)_x$ и $\mathcal{T}(X)_x$ называется *касательным пространством*. Данное определение уже не зависит от способа вложения и может быть перенесено и на проективное многообразие.

Линейное отображение $\delta : \mathcal{Q}_x \to \mathbb{F}$ называется *дифференцированием*, если $(fg)^\delta = f^\delta \cdot g(x) + f(x) \cdot g^\delta$. Обозначим через $\mathcal{D}_x$ множество дифференцирований кольца $\mathcal{Q}_x$ в точке x. Тогда $\mathcal{D}_x \simeq \mathcal{T}(X)_x$ и мы получаем ещё одно эквивалентное определение касательного пространства.

Если многообразие X не является неприводимым и его можно представить в виде объединения $X_1 \cup \ldots \cup X_k$ непересекающихся неприводимых компонент, то любой $x \in X$ лежит лишь в одной компоненте X_i и мы определяем $\mathcal{T}(X)_x = \mathcal{T}(X_i)_x$.

Касательные пространства «хорошо» связаны с произведением многообразий.

Лемма 3.5.4. *Пусть X, Y — неприводимые многообразия, $x \in X$, $y \in Y$. Тогда $\mathcal{T}(X \times Y)_{(x,y)} \simeq \mathcal{T}(X)_x \oplus \mathcal{T}(Y)_y$.*

Доказательство. Достаточно заметить, что $\mathcal{Q}_{(x,y)} \simeq \mathcal{Q}_x \otimes \mathcal{Q}_y$ с максимальным идеалом $m_x \otimes \mathcal{Q}_y + \mathcal{Q}_x \otimes m_y$ и использовать второе определение касательного пространства. □

Теорема 3.5.5. *Пусть X — неприводимое многообразие. Тогда $\dim \mathcal{T}(X)_x \geqslant \dim X$, причём равенство достигается на некотором открытом подмножестве из X.*

Доказательство. Мы докажем эту теорему лишь для аффинных многообразий, так как она нам потребуется лишь в этом случае. Воспользуемся первым определением касательного пространства как $\mathrm{Tan}(X)_x$ и предположим, что X вложено в A^n, а размерность многообразия X равна d. Тогда $\mathcal{I}(X)$ порождён не более, чем $n-d = k$ полиномами $f_1, \ldots, f_k$, так как в противном случае размерность Крулля кольца $\mathbb{F}[T_1, \ldots, T_n] = \mathbb{F}[A^n]$ была бы больше n. Следовательно, функции $g_j = \sum_{i=1}^n \frac{\partial f_j}{\partial T_i}(x)(T_i - x_i)$ порождают идеал I и $\mathcal{V}(I) = \mathrm{Tan}(X)_x$ имеет размерность не меньше, чем $n - k = d$ — число порождающих идеала I. Кроме того, равенство достигается на множестве точек U таких, что $g_j(x) \neq 0$. Таким образом, U — это открытое подмножество в X. □

Пусть $\varphi : X \to Y$ — морфизм неприводимых многообразий. Если $x \in X$ и $y = x^\varphi \in Y$, то φ^* отображает $(\mathcal{Q}_y, m_y)$ в $(\mathcal{Q}_x, m_x)$. Таким образом, если t — линейная функция на m_x/m_x^2, то $\varphi^* \circ t = \mathrm{d}\varphi_x(t)$ является линейной функцией на m_y/m_y^2 и мы получаем отображение $\mathrm{d}\varphi_x : \mathcal{T}(X)_x \to \mathcal{T}(Y)_y$, называемое *дифференциалом морфизма* φ в точке x. Заметим, что если Y является подмногообразием многообразия X, $y \in Y$, то морфизм включения $i : Y \to X$ индуцирует включение $\mathrm{d}i_y : \mathcal{T}(Y)_y \to \mathcal{T}(X)_y$.

Пусть X — некоторое многообразие. Подмножество $Y \subseteq X$ называется *локально замкнутым*, если оно является пересечением открытого и замкнутого подмножеств множества X. Конечное объединение локально замкнутых множеств называется *конструктивным множеством*. Подмножество Y многообразия X называется *плотным*, если оно пересекается с любым открытым подмножеством многообразия X. Заметим, что конструктивное множество всегда содержит плотное открытое подмножество своего замыкания.

Теорема 3.5.6. *Пусть $\varphi : X \to Y$ — морфизм многообразий. Тогда φ переводит конструктивные множества в конструктивные. В частности, образ X^φ является конструктивным множеством.*

Доказательство. См. [17, Теорема 4.4]. □

§6 Полные многообразия

Определение 3.6.1. Многообразие X называется *полным*, если для любого многообразия Y проекция $\pi : X \times Y \to Y$ является *замкнутым* отображением, т. е. замкнутые множества переводит в замкнутые.

Отметим простые свойства полных многообразий.

Лемма 3.6.2. *Пусть X, Y — многообразия.*

1. *Если X полно и Y замкнуто в X, то Y полно.*
2. *Если $\varphi : X \to Y$ — морфизм и X — полное многообразие, то X^{φ} замкнуто и полно.*
3. *Если X, Y полны, то $X \times Y$ полно.*
4. *Если Y — полное подмногообразие многообразия X, то Y замкнуто.*
5. *Если X — полное аффинное многообразие, то $\dim X = 0$.*
6. *Если X — открытое подмножество проективного многообразия и X полно, то X является проективным многообразием.*

Доказательство. Упражнение. Смотри также [17, Предложение 6.1]. □

Теорема 3.6.3. *Любое проективное многообразие полно.*

Доказательство. Смотри [17, Теорема 6.2]. □

Глава 4. Линейные алгебраические группы

§1 Алгебраические группы. Простейшие свойства

Определение 4.1.1. Пусть G — многообразие, на котором задана групповая операция и предположим, что отображения $\mu : G \times G \to G$ и $\iota : G \to G$, заданные правилом $(x, y)\mu = xy$ и $x^{\iota} = x^{-1}$ — это морфизмы. Тогда группа G называется *алгебраической группой*. Заметим, что $f^{\mu^*} = \sum_i f_i \otimes g_i$, причём $f(xy) = \sum_i f_i(x) \cdot g_i(y)$. В частности, $f = \sum_i g_i(e) f_i = \sum_i f_i(e) g_i$.

Пусть G — алгебраическая группа. Тогда e (единичный элемент группы G) содержится лишь в одной из неприводимых компонент. Действительно, пусть $X_1, \ldots, X_m$ — все неприводимые компоненты группы G, содержащие e. Тогда многообразие $X_1 \times \ldots \times X_m$ неприводимо (см. лемму 3.2.9) и его образ $X_1 \cdot \ldots \cdot X_m$ при морфизме произведения является неприводимым (хотя может и не быть замкнутым). Тогда $X_1 \cdot \ldots \cdot X_m$ содержится в одном из X_i. Очевидно также, что любое из X_i лежит в $X_1 \cdot \ldots \cdot X_m$. Следовательно, $m = 1$. Единственную неприводимую компоненту группы G, содержащую e мы будем обозначать G^0 и называть *компонентой единицы* группы G.

Лемма 4.1.2. *Пусть G — алгебраическая группа. Тогда*

(а) *G^0 — нормальная подгруппа группы G конечного индекса, смежные классы по которой являются неприводимыми компонентами группы G;*

(б) *каждая замкнутая подгруппа конечного индекса группы G содержит G^0.*

Доказательство. (а) Для любого $x \in G^0$ множество $x^{-1}G^0$ — это неприводимая компонента группы G, содержащая e, так что $x^{-1}G^0 = G^0$ и $(G^0)^{-1} = G^0$. Аналогично $G^0 \cdot G^0 = G^0$, следовательно, G^0 — подгруппа группы G. Более того $x^{-1}G^0x$ — неприводимая компонента группы G, содержащая e, так что G^0 — это нормальная подгруппа группы G. Левые (или правые) смежные классы подгруппы G^0 в G также являются неприводимыми компонентами. Ввиду леммы 3.2.7 их конечное число, так что индекс $|G : G_0|$ конечен.

(б) Пусть H — замкнутая подгруппа группы G конечного индекса. Тогда каждый из конечного числа левых смежных классов группы G по H является замкнутым множеством и все они не пересекаются. Тогда $G^0 = \cup(G^0 \cap gH)$ представимо в виде конечного объединения замкнутых подмножеств. Следовательно, G^0 содержится в одном из gH и, так как $G^0 \cap H \neq \varnothing$, мы получаем, что $G^0 \leq H$. □

Определение 4.1.3. Далее мы увидим, что любая аффинная алгебраическая группа является линейной. Для линейных групп термин «неприводимая» уже занят для других целей. Поэтому алгебраическую группу, неприводимую как топологическое пространство (т. е. группу, в которой $G = G^0$) мы будем называть *связной*.

Лемма 4.1.4. *Пусть U, V — два плотных открытых подмножества алгебраической группы G. Тогда $G = U \cdot V$.*

Доказательство. Так как взятие обратного элемента и умножение на любой элемент — это гомеоморфизмы группы G как многообразия, мы получаем, что для любого $x \in G$ множества V^{-1} и xV^{-1} — плотные открытые множества. Следовательно, $U \cap xV^{-1} \neq \varnothing$, откуда $x \in U \cdot V$. □

Лемма 4.1.5. *Пусть H — подгруппа алгебраической группы G и $\overline{H}$ — её замыкание. Тогда*

(а) *$\overline{H}$ является подгруппой группы G;*

(б) *если множество H конструктивно, то $H = \overline{H}$.*

Доказательство. (а) Поскольку взятие обратного элемента — гомеоморфизм группы G, мы получаем, что $\overline{H}^{-1} = \overline{H^{-1}} = \overline{H}$. Аналогично для любого $x \in H$ мы имеем $x\overline{H} = \overline{xH} = \overline{H}$. Следовательно, для любого $x \in \overline{H}$ справедливо $Hx \subseteq \overline{H}$ и, значит, $\overline{H}x = \overline{Hx} = \overline{H}$.

(б) Поскольку H — конструктивное множество, оно содержит плотное открытое подмножество U своего замыкания $\overline{H}$. Ввиду леммы 4.1.4 мы получаем $\overline{H} = U \cdot U \subseteq H$. □

Следствие 4.1.6. *Пусть A, B — замкнутые подгруппы алгебраической группы G. Если B нормализует A, то AB — замкнутая подгруппа группы G.*

Доказательство. Очевидно, что AB — подгруппа группы G. Кроме того, она является конструктивной как образ конструктивного множества $A \times B$ относительно морфизма произведения $\mu : G \times G \to G$ (см. теорему 3.5.6). Ввиду леммы 4.1.5(б) подгруппа AB замкнута. □

Лемма 4.1.7. *Пусть $\varphi : G \to H$ — морфизм алгебраических групп. Тогда*

(а) $\mathrm{Ker}(\varphi) = \{x \in G | x^\varphi = e\}$ *— замкнутая подгруппа группы G;*

(б) $\mathrm{Im}(\varphi) = \{x^\varphi | x \in G\}$ *— замкнутая подгруппа группы H;*

(в) $G^0\varphi = (G\varphi)^0$*;*

(г) $\dim G = \dim \mathrm{Ker}\varphi + \dim \mathrm{Im}(\varphi)$.

Доказательство. Множество $\mathrm{Ker}(\varphi)$ замкнуто как прообраз замкнутого множества $\{e\}$. Далее, $\mathrm{Im}(\varphi)$ является конструктивным множеством и подгруппой в H, следовательно, по лемме 4.1.5(б), замкнуто. Таким образом, (а) и (б) доказаны.

(в) Группа $G^0\varphi$ замкнута и связна, следовательно, лежит в $(G\varphi)^0$. Кроме того, индекс $|(G\varphi)^0 : G^0\varphi|$ конечен, в силу леммы 4.1.2(б), получаем, что $G^0\varphi = (G\varphi)^0$.

(г) См. [17, Предложение 7.5Б]. □

Пусть M — произвольное подмножество группы G. Обозначим через $\mathcal{A}(M)$ пересечение всех замкнутых подгрупп группы G, содержащих множество M. Тогда $\mathcal{A}(M)$ является замкнутой подгруппой, порождённой множеством M или *групповым замыканием* множества M.

Теорема 4.1.8. *Пусть G — алгебраическая группа, I — множество индексов и $f_i : X_i \to G$ $(i \in I)$ — семейство морфизмов неприводимых многообразий X_i в G таких, что $e \in Y_i = (X_i)f_i$ для всех $i \in I$. Пусть $M = \cup_{i \in I} Y_i$. Тогда*

(а) $\mathcal{A}(M)$ *— связная подгруппа группы G;*

(б) *для некоторой конечной последовательности индексов $(a(1), \ldots, a(n))$ индексов из I мы имеем $\mathcal{A}(M) = Y_{a(1)}^{\varepsilon_1} \cdot \ldots \cdot Y_{a(n)}^{\varepsilon_n}$, где $\varepsilon_i = \pm 1$.*

Доказательство. Расширим множество индексов и семейство морфизмов таким образом, чтобы оно содержало все морфизмы вида $x \mapsto (xf_i)^{-1}$. Для каждой конечной последовательности $a = (a(1), \ldots, a(n))$ положим $Y_a = Y_{a(1)} \cdot \ldots \cdot Y_{a(n)}$. Множество Y_a конструктивно и неприводимо как образ неприводимого многообразия $X_{a(1)} \times \ldots \times X_{a(n)}$ относительно композиции морфизма $f_{a(1)} \times \ldots \times f_{a(n)}$ с морфизмом умножения в группе G. Следовательно, $\overline{Y_a}$ — замкнутое неприводимое подмножество в G, содержащее e, поэтому каждое из $\overline{Y_a}$ содержится в G^0. Ввиду нётеровости G^0 как топологического пространства, существует такая последовательность a, что множество $\overline{Y_a}$ максимально.

Пусть b, c — две произвольные последовательности индексов из I, покажем, что $\overline{Y_b} \cdot \overline{Y_c} = \overline{Y_{(b,c)}}$. Действительно, если $x \in Y_c$, то гомеоморфизм $y \mapsto yx$ переводит Y_b в $Y_{(b,c)}$, следовательно, он переводит $\overline{Y_b}$ в $\overline{Y_{(b,c)}}$. Таким образом, элемент $x \in \overline{Y_b}$ переводит Y_c в $\overline{Y_{(b,c)}}$, следовательно, переводит $\overline{Y_c}$ в $\overline{Y_{(b,c)}}$, откуда $\overline{Y_b} \cdot \overline{Y_c} = \overline{Y_{(b,c)}}$.

Ввиду максимальности множества $\overline{Y_a}$ мы получаем, что $\overline{Y_a} \cdot \overline{Y_a} = \overline{Y_a}$. Кроме того, мы можем взять множество индексов b таким образом, чтобы $\overline{Y_b} = \overline{Y_a}^{-1}$. Следовательно, $\overline{Y_a}$ — замкнутая связная подгруппа группы G. Более того, множество Y_a конструктивно, поэтому содержит открытое подмножество U группы $\overline{Y_a}$. По лемме 4.1.4 мы имеем

$$\overline{Y_a} = U \cdot U \subseteq Y_a \cdot Y_a = Y_{(a,a)},$$

т. е. $\overline{Y_a} = Y_{(a,a)}$. □

Следствие 4.1.9. *Пусть G — алгебраическая группа, Y_i — семейство замкнутых связных подгрупп группы G, которые порождают G как абстрактную группу. Тогда группа G связна.*

§2 Линейные алгебраические группы

Пусть G — аффинная алгебраическая группа, рассмотрим её аффинную алгебру $\mathbb{F}[G]$. Для каждого элемента $x \in G$ определим ρ_x и λ_x, соответственно *правый и левый сдвиги*, действующие на алгебре $\mathbb{F}[G]$, следующим образом: $(f\rho_x)(y) = f(yx)$ и $(f\lambda_x)(y) = f(x^{-1}y)$. Таким образом мы получаем правое или левое *регулярное представление* группы G.

Лемма 4.2.1. *Пусть H — замкнутая подгруппа аффинной алгебраической группы G и пусть $I = \mathcal{I}(H)$. Тогда $H = \{x | I\rho_x \subseteq I\}$.*

Доказательство. Пусть $x \in H$, рассмотрим $f \in I$. Тогда для любого $y \in H$ справедливо $(f\rho_x)(y) = f(yx) = 0$, т. е. $f\rho_x \in I$. Обратно, пусть $I\rho_x \subseteq I$. Тогда $0 = (f\rho_x)(e) = f(x)$, значит, $x \in H$. □

Определение 4.2.2. Гомоморфизм $\varphi : G \to \mathrm{GL}_n(\mathbb{F})$, являющийся морфизмом, называется *рациональным представлением* алгебраической группы G. Если $\mathrm{Ker}(\varphi) = \{e\}$, то представление называется *точным.*

Лемма 4.2.3. *Пусть G — аффинная алгебраическая группа, R — конечномерное подпространство алгебры $\mathbb{F}[G]$ и рассмотрим правое регулярное представление $G \to \mathrm{GL}(\mathbb{F}[G])$. Тогда существует конечно мерное G-инвариантное подпространство E алгебры $\mathbb{F}[G]$, содержащее R.*

Пусть $\mu : G \times G \to G$ — морфизм произведения, тогда $\mu^* : \mathbb{F}[G] \to \mathbb{F}[G] \otimes \mathbb{F}[G]$. Подпространство R является G-инвариантным тогда и только тогда, когда $R\mu^* \subseteq R \otimes_{\mathbb{F}} \mathbb{F}[G]$.

Доказательство. Можно считать, что подпространство R порождено одним элементом (в конце сложить все полученные пространства E). Запишем (вообще говоря, неоднозначно) $f\mu^* = \sum f_i \otimes g_j$. Тогда для любых двух $x, y \in G$ справедливо $f\rho_x(y) = f(yx) = \sum_i f_i(y)g_i(x)$, откуда $f\rho_x = \sum f_i g_i(x)$. Следовательно, функции f_i порождают над $\mathbb{F}$ конечномерное пространство, которое содержит все сдвиги функции f. Таким образом, в качестве E нужно взять подпространство, порождённое функциями $\{f\rho_x | x \in G\}$.

Предположим теперь, что пространство R является G-инвариантным и рассмотрим базис $\{f_i\}$ пространства R. Дополним его до базиса $\{f_i\} \cup \{g_i\}$ пространства $\mathbb{F}[G]$. Если $f\mu^* = \sum f_i \otimes r_l + \sum g_i \otimes s_m$ для некоторого $f \in R$, то мы имеем $f\rho_x = \sum f_i r_l(x) + \sum g_i s_m(x)$. Левая часть последнего равенства лежит в R, поэтому функции s_i должны обращаться в 0 на всей группе G, откуда $R\mu^* \subseteq R \otimes_{\mathbb{F}} \mathbb{F}[G]$.

Обратно, если $R\mu^* \subseteq R \otimes_{\mathbb{F}} \mathbb{F}[G]$, то, как показывает доказательство первой части леммы, все функции f_i можно взять из R. □

Теорема 4.2.4. *Пусть G — аффинная алгебраическая группа. Тогда G изоморфна некоторой замкнутой подгруппе группы $\mathrm{GL}_n(\mathbb{F})$ для некоторого n.*

Доказательство. Выберем в аффинной алгебре $\mathbb{F}[G]$ порождающие $f_1, \ldots, f_n$. Ввиду леммы 4.2.3, применённой к линейной оболочке R элементов $f_1, \ldots, f_n$, мы можем считать, что R является G-инвариантным подпространством алгебры $\mathbb{F}[G]$. С точностью до переобозначения можно считать, что $f_1, \ldots, f_n$ — базис пространства R (и, по-прежнему, $\mathbb{F}[G]$ порождается элементами $f_1, \ldots, f_n$ как $\mathbb{F}$-алгебра). Вновь в силу предыдущей леммы мы имеем $f_i\mu^* = \sum f_j \otimes m_{i,j}$, где $m_{i,j} \in \mathbb{F}[G]$. Тогда $(f_i\rho_x)(y) = f_i(yx) = \sum f_j(y)m_{i,j}(x)$, откуда $f_i\rho_x = \sum m_{i,j}(x)f_j$. Другими словами, матрица ограничения оператора ρ_x на R в базисе $f_1, \ldots, f_n$ равна $(m_{i,j}(x))$. Таким образом, отображение $\psi : G \to \mathrm{GL}_n(\mathbb{F})$, заданное правилом $\psi : x \mapsto (m_{i,j}(x))$, является морфизмом алгебраических групп.

Заметим, что $f_i(x) = f_i(ex) = \sum m_{i,j}(x)f_j(e)$, значит, $f_i = \sum f_j(e)m_{i,j}$, т. е. функции $m_{i,j}$ также порождают алгебру $\mathbb{F}[G]$. В частности, морфизм ψ инъективен, так как в противном случае мы бы получили, что функция $g_i = f_i - f_i(e)$ зануляется на любом элементе x из ядра. Ввиду леммы 4.1.7(б) образ $H = G^{\psi}$ — замкнутая подгруппа в $\mathrm{GL}_n(\mathbb{F})$. Осталось убедиться, что ψ — изоморфизм многообразий. Действительно, ограничения на H координатных функций $T_{i,j}$ отображается коморфизмом ψ^* в функции $m_{i,j}$, которые, как мы только что показали, порождают $\mathbb{F}[G]$. Следовательно, коморфизм ψ^* сюръективен и потому является изоморфизмом $\mathbb{F}$-алгебр $\mathbb{F}[H]$ и $\mathbb{F}[G]$. □

§3 Действие алгебраической группы на многообразиях

Напомним, что если G — группа и X — некоторое множество, то отображение $\varphi X \times G \to X$, обозначаемое для краткости $(x, g)\varphi = xg = x^g$, называется *действием группы* G если для любых $g_1, g_2 \in G$ и $x \in X$ справедливо

1. $(xg_1)g_2 = x(g_1g_2)$.
2. $xe = x$.

Отображение φ является гомоморфизмом из G в $\mathrm{Sym}(X)$. В дальнейшем через X_G будет обозначаться множество точек, неподвижных относительно действия группы G. Если Y, Z — подмножества множества X, то $\mathrm{Tran}_G(Y,Z) = \{g \in G | Yg \subseteq Z\}$ называется *транспортёром.*

Если теперь G, X — многообразия и существует морфизм $\varphi : X \times G \to X$, который является действием, то будем говорить, что группа G действует *регулярно* на X. Отметим некоторые простые свойства регулярного действия.

Лемма 4.3.1. *Пусть алгебраическая группа G регулярно действует на многообразии X. Пусть Y, Z — подмножества множества X, причем Z замкнуто. Тогда*

(а) $\mathrm{Tran}_G(Y,Z)$ *— замкнутое подмножество группы G;*

(б) *для каждого $x \in X$ группа $St_G(x)$ замкнута в G, в частности, группа $St_G(Y)$ замкнута;*

(в) *множество неподвижных точек любого элемента $g \in G$ замкнуто в X, поэтому X_G замкнуто;*

(г) *если группа G связна, то любая неприводимая компонента множества X является G-инвариантной, в частности, группа G действует на X тривиально, если X конечно.*

Доказательство. Заметим, что для любого $x \in X$ отображение $\varphi_x : G \to X$, заданное правилом $\varphi_x : g \mapsto yg$, есть композиция отображения $g \mapsto (x,g)$ и φ, следовательно, является морфизмом. Если y пробегает множество Y, то прообразы $\varphi_y^{-1}(Z)$ замкнуты в G (так как Z замкнуто), поэтому пересечение этих прообразов $\mathrm{Tran}_G(Y,Z)$ замкнуто в G. Кроме того, $St_G(x) = \mathrm{Tran}_G(\{x\},\{x\})$, следовательно, группа $St_G(x)$ замкнута в G.

Для доказательства пункта (в) выберем $g \in G$ и рассмотрим морфизм $\psi : X \to X \times X$, заданный правилом $\psi : x \mapsto (x, xg)$. Множество неподвижных точек элемента g — это в точности прообраз диагонали относительно отображения ψ и это множество замкнуто, поскольку замкнута диагональ.

Пусть G — связная группа, $X = X_1 \cup \ldots \cup X_k$ — объединение неприводимых компонент. Тогда $H = St_G(X_1)$ — замкнутая подгруппа в G. Так как группа G перемещает между собой лишь конечное количество компонент, мы получаем, что индекс $|G : H|$ конечен. Ввиду леммы 4.1.2, $G = H$. □

Лемма 4.3.2. *Пусть алгебраическая группа G регулярно действует на непустом многообразии X. Тогда каждая G-орбита есть локально замкнутое подмножество многообразия X, граница которого является объединением орбит строго меньшей размерности. В частности, орбиты минимальной размерности замкнуты и всегда существуют.*

Доказательство. Пусть $Y = y \cdot G$ — орбита элемента $y \in X$. Как образ группы G относительно орбитного отражения, построенного в доказательстве леммы 4.3.1, орбита Y является конструктивным множеством (ввиду теоремы 3.5.6 образ конструктивного множества конструктивен) и, следовательно, $\overline{Y}$ содержит открытое плотное подмножество $U \subseteq Y$. Но группа G действует транзитивно на Y, оставляя множество $\overline{Y}$ инвариантным, так что множество Y содержит открытую окрестность (в $\overline{Y}$) каждой своей точки. Поэтому множество Y открыто в $\overline{Y}$, а множество $\overline{Y} \setminus Y$ замкнуто и его размерность строго меньше размерности множества Y. Поскольку $\overline{Y} \setminus Y$ является G-инвариантным, оно является объединением G-орбит. □

Предположим теперь, что алгебраическая группа G регулярно действует на алгебраической группе N. Тогда мы можем рассмотреть полупрямое произведение $N \rtimes G$ со стандартным определением умножения элементов. Нетрудно проверить, что построенная таким образом группа вновь является алгебраической группой, она наследует топологию Зарисского произведения многообразий $(N \times G)$.

§4 Алгебра Ли аффинной алгебраической группы

С этого момента мы будем рассматривать лишь аффинные алгебраические группы, поэтому слово «аффинные» для краткости мы будем опускать.

Определение 4.4.1. Пусть A — некоторая ассоциативная $\mathbb{F}$-алгебра. Определим *алгебру Ли* как подпространство, порождённое всевозможными *скобочными умножениями* $[x,y] = xy - yx$, где $x, y \in A$ и замкнутое относительно скобочного умножения.

Пусть теперь G — алгебраическая группа и $A = \mathbb{F}[G]$. Как мы уже доказывали выше, группа G действует на A правыми и левыми сдвигами. Пусть δ, σ — два произвольных дифференцирования алгебры A (напомним, что дифференцирование δ — это $\mathbb{F}$-линейное отображение, удовлетворяющее равенству $(fg)\delta = f \cdot g^\delta + f^\delta \cdot g$). Тогда $[\delta, \sigma]$ — это вновь дифференцирование алгебры A. Следовательно, множество дифференцирований алгебры A, обозначаемое $\mathrm{Der}\ A$, является алгеброй Ли. *Алгеброй Ли* группы G будем называть подпространство $\mathfrak{L}(G)$ алгебры Ли $\mathrm{Der}\ A$, состоящее из всех правоинвариантных дифференцирований, т. е.

$$\mathfrak{L}(G) = \{\delta \in \mathrm{Der}\ A | \forall x \in X, \delta\rho_x = \rho_x\delta\}.$$

Легко понять, что $\mathfrak{L}(G)$ действительно является алгеброй Ли.

Рассмотрим пространство $\mathcal{T}(G^0)_e$ и обозначим его за $\mathfrak{g}$. Определим отображение $\theta : \mathfrak{L}(G) \to \mathfrak{g}$ по правилу $\theta : f^\delta \mapsto (f^\delta)(e)$, где $f \in \mathbb{F}[G]$, $\delta \in \mathfrak{L}(G)$. Далее мы покажем, что отображение θ является изоморфизмом векторных пространств и, следовательно, позволяет определить на $\mathfrak{g}$ структуру алгебры Ли.

Пусть $\varphi : G \to H$ — морфизм алгебраических групп. Тогда $\mathrm{d}\varphi_e : \mathfrak{g} \to \mathfrak{h}$ является линейным отображением векторных пространств. Более того, отображение $\mathrm{d}\varphi_e$ является гомоморфизмом алгебр Ли. Далее мы будем писать $\mathrm{d}\varphi$ вместо $\mathrm{d}\varphi_e$.

Теорема 4.4.2. *Пусть G, H — алгебраические группы, $\mathfrak{g} = \mathcal{T}(G^0)_e$, $\mathfrak{h} = \mathcal{T}(H^0)_e$ и $\varphi : G \to H$ — морфизм алгебраических групп. Тогда*

(а) $\theta : \mathfrak{L}(G) \to \mathfrak{g}$ *является изоморфизмом векторных пространств;*

(б) $\mathrm{d}\varphi$ *является гомоморфизмом алгебр Ли.*

Доказательство. Для доказательства (а) мы построим обратное отображение $\eta : \mathfrak{g} \to \mathfrak{L}(G)$, отображающее касательный вектор x в дифференцирование $*\mathsf{x}$, задаваемое правилом $(f * \mathsf{x})(x) = (f\rho_x)\mathsf{x}$, где $x \in G, f \in A$. Дифференцирование $*\mathsf{x}$ называется *конволюцией*. Покажем, что $*\mathsf{x}$ — правоинвариантное дифференцирование алгебры A. Пусть $x, y \in G$, $f, g \in A$, тогда мы имеем:

$$(f \cdot g * \mathsf{x})(x) = ((f \cdot g)\rho_x)\mathsf{x} = ((f\rho_x) \cdot (g\rho_x))\mathsf{x} = (f\rho_x \cdot g(x))\mathsf{x} + f(x) \cdot (g\rho_x)\mathsf{x} = ((f * \mathsf{x})g + f(g * \mathsf{x}))(x),$$

т. е. $*\mathsf{x}$ является дифференцированием,

$$((f * \mathsf{x})\rho_y)(x) = (f * \mathsf{x})(xy) = (f\rho_{xy})\mathsf{x} = ((f\rho_y)\rho_x)\mathsf{x} = ((f\rho_y) * \mathsf{x})(x),$$

т. е. дифференцирование $*\mathsf{x}$ правоинвариантно.

Ясно, что $\eta : \mathfrak{g} \to \mathfrak{L}(G)$ является линейным отображением. Чтобы доказать биективность, найдем $\eta \circ \theta$ и $\theta \circ \eta$.

$$(f * \delta^\theta)(x) = (f\rho_x)\delta^\theta = ((f\rho_x)\delta)(e) = ((f\delta)\rho_x)(e) = (f\delta)(x),$$

т. е. $\delta^{\eta\circ\theta} = \delta$ для всех $\delta \in \mathfrak{L}(G)$. Обратно,

$$f(*\mathsf{x})^\theta = (f * \mathsf{x})(e) = (f\rho_e)\mathsf{x} = f\mathsf{x},$$

т. е. $\mathsf{x}^{\theta\circ\eta} = \mathsf{x}$ для всех $\mathsf{x} \in \mathfrak{g}$.

Для доказательства (б) осталось показать, что если $\varphi : G \to H$ — морфизм алгебраических групп, то $\mathrm{d}\varphi : \mathfrak{g} \to \mathfrak{h}$ сохраняет скобочное умножение. Для $\mathsf{x}, \mathsf{y} \in \mathfrak{g}$ положим $\mathsf{x}' = \mathsf{x}^{\mathrm{d}\varphi}$, $\mathsf{y}' = \mathsf{y}^{\mathrm{d}\varphi}$. Пусть $f' \in \mathbb{F}[H]$, положим $f = (f')\varphi^*$. По определению,

$$(f')[\mathsf{x}', \mathsf{y}'] = (f' * \mathsf{y}' * \mathsf{x}')(e) - (f' * \mathsf{x}' * \mathsf{y}')(e) = (f' * \mathsf{y}')\mathsf{x}' - (f' * \mathsf{x}')\mathsf{y}' = ((f' * \mathsf{y}')^{\varphi^*})\mathsf{x} - ((f' * \mathsf{x}')^{\varphi^*})\mathsf{y}.$$

С другой стороны, $[\mathsf{x}, \mathsf{y}]^{\mathrm{d}\varphi}$ отображает f' в

$$(f * \mathsf{y} * \mathsf{x})(e) - (f * \mathsf{x} * \mathsf{y})(e) = (f * \mathsf{y})\mathsf{x} - (f * \mathsf{x})\mathsf{y}.$$

Покажем, что $f * \mathsf{y} = (f' * \mathsf{y}')^{\varphi^*}$, а $f * \mathsf{x} = (f' * \mathsf{x}')^{\varphi^*}$ или, эквивалентно, $(f')^{\varphi^*} * \mathsf{x} = (f' * \mathsf{x}^{\mathrm{d}\varphi})^{\varphi^*}$. Обе части последнего равенства являются функциями на G, так что достаточно сравнить их значения на элементах $x \in G$. Получаем $((f')^{\varphi^*} * \mathsf{x})(x) = ((f')^{\varphi^*}\rho_x)\mathsf{x}$. Остается показать, что $(f')^{\varphi^*}\rho_x = (f'\rho_{x^\varphi})^{\varphi^*}$. Для этого вычислим значения правой и левой частей последнего равенства в точке $y \in G$. С одной стороны мы имеем

$$((f')^{\varphi^*}\rho_x)(y) = (f')^{\varphi^*}(yx) = f'((yx)^\varphi).$$

С другой стороны,
$$(f'\rho_{x^\varphi})^{\varphi^*}(y) = (f'\rho_{x^\varphi})(y^\varphi) = f'(y^\varphi x^\varphi) = f'((yx)^\varphi),$$
что даёт нам требуемое утверждение. □

Пусть G — алгебраическая группа. Рассмотрим внутренний автоморфизм $\mathrm{Int}_x(y) = x^{-1}yx$. Его дифференциал обозначается $\mathrm{Ad}\ x$. Поскольку $(\mathrm{Ad}\ x)\cdot(\mathrm{Ad}\ x^{-1})$ — тождественное отображение алгебры Ли $\mathfrak{g}$, мы получаем, что $\mathrm{Ad}\ x$ — автоморфизм алгебры Ли $\mathfrak{g}$. Более того, нетрудно проверить, что $\mathrm{Ad}\ x\cdot\mathrm{Ad}\ y = \mathrm{Ad}\ xy$, так что $\mathrm{Ad} : G \to \mathrm{Aut}\mathfrak{g} \le \mathrm{GL}(\mathfrak{g})$ — гомоморфизм абстрактных групп, называемый *присоединённым представлением* группы G.

Введем ассоциативное умножение элементов касательного пространства $\mathfrak{g} = \mathcal{T}(G^0)_e$ внутренним образом и покажем, что оно согласуется с умножением, индуцированным изоморфизмом θ. Пусть $\mathsf{x},\mathsf{y}\in\mathfrak{g}$, определим $\mathsf{x}\otimes\mathsf{y} : A\otimes A \to \mathbb{F}$ правилом $(f\otimes g)(\mathsf{x}\otimes\mathsf{y}) = (f\mathsf{x})\cdot(g\mathsf{y})$. Тогда $\mathsf{x}\cdot\mathsf{y} = (\mathsf{x}\otimes\mathsf{y})\circ\mu^* : A \to \mathbb{F}$. Покажем, что при таком определении $((*\mathsf{x})(*\mathsf{y}))^\theta = \mathsf{x}\cdot\mathsf{y}$.

Для этого заметим сначала, что если $f^{\mu^*} = \sum_i f_i\otimes g_i$, то $f*\mathsf{x} = \sum_i (f_i\mathsf{x})g_i$. Действительно, $(f*\mathsf{x})(x) = (f\rho_x)\mathsf{x}$. Далее
$$(f\rho_x)(y) = f(yx) = \sum_i f_i(y)g_i(x),$$
следовательно, $f\rho_x = \sum_i f_i g_i(x)$ и, кроме того, $f\rho_e = \sum_i f_i(e)g_i$. Таким образом $(f\rho_x)\mathsf{x} = \left(\sum_i f_i g_i(x)\right)\mathsf{x}$. С другой стороны,
$$\left(\sum_i (f_i\mathsf{x})g_i\right)(x) = \sum_i (f_i\mathsf{x})g_i(x) = \left(\sum_i f_i g_i(x)\right)\mathsf{x}.$$

Теперь, по определению, мы имеем $f(\mathsf{x}\cdot\mathsf{y}) = \sum_i (f_i\mathsf{x})\cdot(g_i\mathsf{y})$. С другой стороны,
$$((f*\mathsf{x}*\mathsf{y})(e) = \left(\left(\sum_i f_i(g_i\mathsf{y})\right)*\mathsf{x}\right)(e) = \sum_i (f_i*\mathsf{x})(e)\cdot(g_i\mathsf{y}) = \sum_i (f_i\mathsf{x})\cdot(g_i\mathsf{y}).$$

Рассмотрим группу $G = \mathrm{GL}_n(\mathbb{F})$. Тогда функции T_i образуют базис алгебры $\mathbb{F}[G]$, запишем произвольный $\mathsf{x}\in\mathfrak{g} = \mathfrak{L}(G)$ вектором $x_{i,j} = \mathsf{x}(T_{i,j})$. Тогда, используя наше правило, получаем
$$\mathsf{x}\cdot\mathsf{y} = \left(\left(\sum_h T_{i,h}\otimes T_{h,j}\right)(\mathsf{x}\otimes\mathsf{y})\right)_{i,j} = \sum_h x_{i,h}y_{h,j}.$$
Иными словами, отображение $\mathsf{x}\mapsto(x_{i,j})$ является изоморфизмом алгебр $\mathfrak{g}$ и $\mathrm{M}_n(\mathbb{F})$.

Пусть H — замкнутая подгруппа алгебраической группы G. Включение $\eta : H \to G$ является изоморфизмом на замкнутую подгруппу и $\mathrm{d}\eta : \mathfrak{h}\to\mathfrak{g}$ является вложением алгебры Ли подгруппы H в алгебру Ли группы G. Если $I = \mathcal{I}(H)$ — идеал в $\mathbb{F}[G]$, то $\mathcal{T}(H^0)_e$ можно отождествить с подпространством пространства $\mathcal{T}(G^0)_e$, состоящим из тех x, для которых $I\mathsf{x} = 0$. Таким образом, мы получаем следующую лемму.

Лемма 4.4.3. *Пусть H — замкнутая подгруппа группы G и пусть I — идеал алгебры $\mathbb{F}[G]$, состоящий из функций, обращающихся в 0 на H. Тогда $\mathfrak{h} = \{\mathsf{x}|I*\mathsf{x}\subseteq I\}$.*

Доказательство. Пусть $\mathsf{x}\in\mathfrak{h}$. Если $f\in I$и $x\in H$, то $f*\mathsf{x}(x) = (f\rho_x)\mathsf{x} = 0$, поскольку $f\rho_x\in I$ (см. лемму 4.2.1) и, как мы заметили ранее, можно считать, что $I\mathsf{x} = 0$. Таким образом, $f*\mathsf{x}\in I$. Обратно, пусть элемент $\mathsf{x}\in\mathfrak{g}$ удовлетворяет условию $I*\mathsf{x}\subseteq I$. Если $f\in I$, то $(f*\mathsf{x})(e) = f\mathsf{x} = 0$, т. е. $\mathsf{x}\in\mathfrak{h}$. □

§5 Присоединённое представление

В данном параграфе мы докажем, что присоединённое представление, определённое выше, является рациональным представлением и найдем некоторые его свойства. Как обычно, G — алгебраическая группа. Вычислим сначала дифференциал морфизма умножения $\mu : G\times G\to G$ в точке (e,e). Напомним, что $f^{\mu^*} = \sum_i f_i\otimes g_i$, причём $f(xy) = \sum_i f_i(x)\cdot g_i(y)$. В частности,
$$f = \sum_i g_i(e)f_i = \sum_i f_i(e)g_i. \tag{4.1}$$
Кроме того, $\mathcal{T}(G^0\times G^0)_{(e,e)} \simeq \mathcal{T}(G^0)_e\otimes\mathcal{T}(G^0)_e$ (см. лемму 3.5.4) и $\mathcal{T}(G^0)_e\otimes\mathcal{T}(G^0)_e \simeq \mathfrak{g}\oplus\mathfrak{g}$, где $\mathfrak{g} = \mathfrak{L}(G)$.

Пусть $(\mathsf{x},\mathsf{y}) \in \mathcal{T}(G^0 \times G^0)_{(e,e)}$, обозначим через $\mathsf{z} = (\mathsf{x},\mathsf{y})\mathrm{d}\mu_{(e,e)}$. Тогда, по определению дифференциала, мы получаем, что для любого $f \in \mathbb{F}[G]$ выполнено

$$f\mathsf{z} = \left(\sum_i f_i \otimes g_i\right)(\mathsf{x},\mathsf{y}) = \sum_i (f_i\mathsf{x})g_i(e) + \sum_i f_i(e)(g_i\mathsf{y}).$$

Используя равенство (4.1), мы получаем тот же результат, для $f(\mathsf{x}+\mathsf{y})$. Следовательно, $(\mathsf{x},\mathsf{y})\mathrm{d}\mu_{(e,e)} = \mathsf{x}+\mathsf{y}$.

Вычислим теперь $\mathrm{d}\iota_e : \mathfrak{g} \to \mathfrak{g}$. Рассмотрим отображение

$$G \xrightarrow{(1,\iota)} G \times G \xrightarrow{\mu} G.$$

Композиция этих отображений преобразует каждый элемент x в e, следовательно, дифференциал отображает каждый элемент $\mathsf{x} \in \mathfrak{g}$ в 0. Далее, $\mathrm{d}1 = 1$ и $\mathrm{d}(1,\iota) = (\mathrm{d}1, \mathrm{d}\iota)$, таким образом, справедлива следующая цепочка равенств

$$0 = \mathrm{d}\mu \circ (1,\iota)(\mathsf{x}) = \mathrm{d}\mu((\mathrm{d}(1,\iota)(\mathsf{x}))) = \mathrm{d}\mu(\mathsf{x}, \mathrm{d}\iota(\mathsf{x})) = \mathsf{x} + \mathrm{d}\iota(\mathsf{x}).$$

Следовательно, $\mathrm{d}\iota(\mathsf{x}) = -\mathsf{x}$.

Рассмотрим теперь *коммутаторный морфизм относительно* x, $\gamma_x : y \mapsto x^{-1}y^{-1}xy$. Чтобы найти дифференциал этого морфизма, рассмотрим цепочку

$$G \xrightarrow{(\iota\circ \mathrm{Int}_x, 1)} G \times G \xrightarrow{\mu} G.$$

Очевидно, что $\gamma_x = (\iota \circ \mathrm{Int}_x, 1) \circ \mu$, поэтому мы получаем, что $\mathrm{d}\gamma_x = 1 - \mathrm{Ad}\ x$. Таким образом, мы получили следующую лемму.

Лемма 4.5.1. *Пусть G — алгебраическая группа. Тогда для любых $\mathsf{x},\mathsf{y} \in \mathfrak{g}$ справедливо*

(а) $(\mathsf{x},\mathsf{y})\mathrm{d}\mu_{(e,e)} = \mathsf{x}+\mathsf{y}$.

(б) $\mathsf{x}\mathrm{d}\iota_e = -\mathsf{x}$.

(в) $(\mathsf{x})(\mathrm{d}\gamma_x)_e = \mathsf{x} - \mathsf{x}\mathrm{Ad}\ x$.

Следующая лемма устанавливает связь между действием алгебраической группы и её алгебры Ли на аффинной алгебре $\mathbb{F}[G]$. Заметим, что произвольный элемент $\mathsf{x} \in \mathfrak{g}$ можно рассматривать как отображение аффинной алгебры $\mathbb{F}[G]$, заданное правилом $\mathsf{x} : f \mapsto f * \mathsf{x}$.

Лемма 4.5.2. *Любое G-инвариантное подпространство алгебры $\mathbb{F}[G]$ (относительно действия левыми сдвигами) является $\mathfrak{g}$-инвариантным. Более того, если E — G-инвариантное конечномерное подпространство и $\varphi : G \to \mathrm{GL}(E)$ — рациональное представление, то дифференциал левого сдвига есть конволюция.*

Доказательство. Пусть E — G-инвариантное подпространство алгебры $\mathbb{F}[G]$, с базисом $\{f_i\}$, $x \in G$. Поскольку по лемме 4.2.3 любое конечномерное пространство содержится в некотором G-инвариантном конечномерном подпространстве, мы можем считать, что E конечномерно. По той же лемме мы получаем, что $E\mu^* \subseteq \mathbb{F}[G] \otimes_{\mathbb{F}} E$. В частности, $f_i\mu^* = \sum_j m_{i,j} \otimes f_j$. Тогда $f_i\lambda_{x^{-1}} = \sum_j m_{i,j}(x)f_j$ и отображение $\varphi : x \mapsto m_{i,j}(x)$ является морфизмом $\varphi : G \to \mathrm{GL}(E) = \mathrm{GL}_n(\mathbb{F})$.

Вычислим дифференциал морфизма $\mathrm{d}\varphi : \mathfrak{g} \to \mathfrak{gl}_n(\mathbb{F})$, где $\mathfrak{gl}_n(\mathbb{F}) = \mathfrak{L}(\mathrm{GL}_n(\mathbb{F}))$. Если $\mathsf{x} \in \mathfrak{g}$, то, по определению, матрица $(\mathsf{x})\mathrm{d}\varphi$ на месте (i,j) имеет результат применения x к координатной функции $T_{i,j}$. Но мы заметили выше, что $T_{i,j}^{\varphi} = m_{i,j}$, поэтому $(\mathsf{x})\mathrm{d}\varphi = (m_{i,j})\mathsf{x}$. С другой стороны, элемент x на базисе $\{f_i\}$ пространства E действует как $(f_i * \mathsf{x})(x) = (f_i\rho_x)\mathsf{x} = \sum_j (m_{i,j}) * \mathsf{x}f_j(x)$, т. е. x оставляет пространство E инвариантным и его матрица равна $(m_{i,j})\mathsf{x}$ в базисе $\{f_i\}$. □

Пусть G — алгебраическая группа и $\mathfrak{g}$ — её касательное пространство. Если мы будем рассматривать $\mathfrak{g}$ как алгебру Ли $\mathfrak{L}(G)$ правоинвариантных дифференцирований, то тогда $\mathrm{Ad}\ x$ действует по правилу $\delta \mapsto \lambda_x\delta^{\lambda_x^{-1}}$. Рассмотрим сначала частный случай $G = \mathrm{GL}_n(\mathbb{F})$ и $\mathfrak{g} = \mathfrak{gl}_n(\mathbb{F})$. Мы точно вычислим действие группы G и алгебры $\mathfrak{g}$ на $\mathbb{F}[G]$ сдвигами и конволюциями соответственно. Для этого достаточно рассмотреть действие на координатных функциях $T_{i,j}$. Обозначим через T матрицу, чья (i,j)-ая координата равна $T_{i,j}$.

Лемма 4.5.3. *Пусть $x \in \mathrm{GL}_n(\mathbb{F})$, $\mathsf{x} \in \mathfrak{gl}_n(\mathbb{F})$. Тогда $T_{i,j}\rho_x$ (соответственно, $T_{i,j}\lambda_x$ и $T_{i,j}*\mathsf{x}$) равна (i,j)-ому элементу матрицы $T\mathsf{x}$ (соответственно, $x^{-1}T$ и $\mathsf{x}T$).*

Доказательство. Если $y \in \mathrm{GL}_n(\mathbb{F})$, то

$$(T_{i,j}\rho_x)(y) = T_{i,j}(yx) = \sum_k y_{i,k}x_{k,j} = (Tx)_{ij}(y).$$

Аналогичное равенство мы получаем для левого сдвига. Из полученных тождеств вытекает, что

$$(T_{i,j} * \mathsf{x})(y) = (T_{i,j}\rho_y)\mathsf{x} = \left(\sum_k T_{i,k}y_{k,j}\right)\mathsf{x} = \sum_k (T_{i,k}\mathsf{x}y_{k,j} = \sum_k \mathsf{x}_{i,j}y_{k,j} = \sum_k \mathsf{x}_{i,k}T_{k,j}(y) = (\mathsf{x}T)_{i,j}(y),$$

что завершает доказательство леммы. □

Лемма 4.5.4. *Пусть $x \in \mathrm{GL}_n(\mathbb{F})$, $\mathsf{x} \in \mathfrak{gl}_n(\mathbb{F})$. Тогда $\mathsf{x}\mathrm{Ad}\ x = x^{-1}\mathsf{x}x$ (как произведение матриц).*

Доказательство. Достаточно проверить, используя лемму 4.5.3, как каждая из частей нашего равенства действует на $T_{i,j}$.

$$T_{i,j}^{\mathsf{x}\mathrm{Ad}\ x} = T_{i,j}^{\lambda_x(*\mathsf{x})\lambda_x^{-1}} = \left(\sum_k x^{-1}i,kT_{k,j}\right)^{(*\mathsf{x})\lambda_x^{-1}} = \left(\sum_k x^{-1}_{i,k}(\mathsf{x}T)_{k,j}\right)^{\lambda_x^{-1}} = \left(\sum_k\sum_l x_{i,k}\mathsf{x}_{k,l}T_{l,j}\right)^{\lambda_x^{-1}}$$
$$= \sum_k\sum_l\sum_m \left(x^{-1}_{i,k}\mathsf{x}_{k,l}x_{l,m}T_{m,j}\right) = \left(x^{-1}\mathsf{x}xT\right)_{i,j} = T_{i,j}^{x^{-1}\mathsf{x}x},$$

что и требовалось. □

Из точной формулы, полученной в лемме 4.5.4 немедленно вытекает

Следствие 4.5.5. *Отображение $\mathrm{Ad}\ : \mathrm{GL}_n(\mathbb{F}) \to \mathrm{GL}_{n^2}(\mathbb{F})$ является морфизмом алгебраических групп независимо от выбора базиса в $\mathfrak{gl}_n(\mathbb{F})$.*

Теорема 4.5.6. *Пусть G — алгебраическая группа. Тогда отображение $\mathrm{Ad}\ : G \to \mathrm{GL}(\mathfrak{g})$ является морфизмом алгебраических групп. Если G является замкнутой подгруппой группы $\mathrm{GL}_n(\mathbb{F})$, то $\mathrm{Ad}\ x$ есть сопряжение элементом x.*

Доказательство. По теореме 4.2.4 группа G изморфна замкнутой подгруппе группы $\mathrm{GL}_n(\mathbb{F})$ для подходящего n. Этот изоморфизм задает изоморфное вложение алгебры Ли $\mathfrak{g}$ в $\mathfrak{gl}_n(\mathbb{F})$. Тогда отображение $\mathrm{Ad}\ x$ алгебры $\mathfrak{g}$ есть ограничение отображения $\mathrm{Ad}\ x$ алгебры $\mathfrak{gl}_n(\mathbb{F})$, откуда следует лемма. □

§6 Дифференциал морфизма Ad . Некоторые следствия

Как мы доказали в теореме 4.5.6, отображение $\mathrm{Ad}\ : G \to \mathrm{GL}(\mathfrak{g})$ является морфизмом алгебраических групп. Обозначим через ad дифференциал морфизма Ad . Таким образом, $\mathrm{ad}\ : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ является гомоморфизмом алгебры Ли $\mathfrak{g}$.

Теорема 4.6.1. *Для любых $\mathsf{x}, \mathsf{y} \in \mathfrak{g}$ справедлива следующая формула*

$$\mathsf{y}^{(\mathsf{x})\mathrm{ad}} = [\mathsf{y}, \mathsf{x}] = \mathsf{y}\mathsf{x} - \mathsf{x}\mathsf{y}.$$

Доказательство. Как и в предыдущем параграфе рассмотрим сначала частный случай $G = \mathrm{GL}_n(\mathbb{F})$, $\mathfrak{g} = \mathfrak{gl}_n(\mathbb{F})$. Если $x \in G$, то $\mathrm{Ad}\ x$ есть образ элемента x относительно композиции отображений

$$G \xrightarrow{(\iota,1)} G \times G \xrightarrow{\sigma\times tau} \mathrm{GL}(\mathfrak{g}) \times \mathrm{GL}(\mathfrak{g}) \xrightarrow{\mu} \mathrm{GL}(\mathfrak{g}),$$

где σ и τ — морфизмы умножения слева и справа соответственно. Покажем, что σ и τ действительно морфизмы и вычислим их дифференциалы. Рассмотрим стандартный базис $e_{i,j}$ алгебры $\mathfrak{gl}_n(\mathbb{F})(= \mathrm{M}_n(\mathbb{F}))$ из матриц, содержащих 1 на месте (i, j) и 0 на всех остальных местах. На месте (i, j) матрицы $xe_{l,m}$ стоит элемент $x_{i,l}$, если $m = j$ и 0 в противном случае. Следовательно, матрицу x^σ в $\mathrm{GL}_{n^2}(\mathbb{F})$ можно разбить на блоки размера $n \times n$, каждый из которых содержит некоторый столбец матрицы x в качестве одного из столбцов и 0 на остальных местах. Таким образом, σ действительно является морфизмом и, более того, полиномы, задающие

x^σ имеют очень простой вид и могут быть явно вычислены. Отсюда следует, что $\mathsf{y}^{\mathsf{x}\mathrm{d}\sigma_e} = \mathsf{xy}$. Аналогичные рассуждения справедливы и для морфизма τ.

Тогда $\mathrm{ad} = \mathrm{dAd}$ можно получить как последовательность отображений $\mathsf{x} \mapsto (-\mathsf{x}, \mathsf{x}) \mapsto$ левое умножение на $-\mathsf{x}$ плюс правое умножение на x, т. е. $\mathsf{y}^{(\mathsf{x})\mathrm{ad}} = -\mathsf{xy} + \mathsf{yx} = [\mathsf{y}, \mathsf{x}]$.

В общем случае, применяя теорему 4.2.4, мы вкладываем группу G в $\mathrm{GL}_n(\mathbb{F})$ и применяем полученную формулу, для ограничения морфизма. □

Нетрудно заметить, что $\mathrm{Ker}(\mathrm{ad})$ — это в точности центр $\mathfrak{z}(\mathfrak{g}) = \{\mathsf{x} \in \mathfrak{g} | \forall \mathsf{y} \in \mathfrak{g}, [\mathsf{x}, \mathsf{y}] = 0\}$ алгебры $\mathfrak{g}$. С другой стороны, если $x \in Z(G)$, то $\mathrm{Int}\, z = 1$, следовательно, $\mathrm{Ad}\, x = 1$, т. е. $Z(G) \le \mathrm{Ker}(\mathrm{Ad})$. В характеристике 0 на самом деле справедливо равенство, но равенства нет в общем случае.

Следствие 4.6.2. *Пусть H — замкнутая нормальная подгруппа алгебраической группы G и $\mathfrak{h}$ — алгебра Ли группы H. Тогда $\mathfrak{h}$ является идеалом в $\mathfrak{g}$, т. е. для всех $\mathsf{x} \in \mathfrak{g}$, $\mathsf{y} \in \mathfrak{h}$ выполнено $[\mathsf{x}, \mathsf{y}] \in \mathfrak{h}$.*

Доказательство. Поскольку подгруппа H нормальна, мы получаем, что для любого $x \in G$ морфизм $\mathrm{Int} x$ стабилизирует H, следовательно, $\mathrm{Ad}\, x$ стабилизирует $\mathfrak{h}$. Дополним базис алгебры $\mathfrak{h}$ до базиса в $\mathfrak{g}$, тогда матрица элемента $\mathrm{Ad}\, x$ будет иметь вид

$$\begin{pmatrix} * & 0 \\ * & * \end{pmatrix},$$

и матрица $(\mathsf{x})\mathrm{ad}$ будет иметь тот же вид. □

Следствие 4.6.3. *Пусть H — замкнутая подгруппа алгебраической группы G, $N = N_G(H)$ — её нормализатор, $\mathfrak{h}$ и $\mathfrak{n}$ — алгебры Ли групп H и N соответственно. Тогда $\mathfrak{n} \le \mathfrak{n}_{\mathfrak{g}}(\mathfrak{h}) = \{\mathsf{x} \in \mathfrak{g} | [\mathsf{x}, \mathfrak{h}] \le \mathfrak{h}\}$.*

Вновь если характеристика поля $\mathbb{F}$ равна 0, то включение превращается в равенство, но равенства нет в общем случае.

Лемма 4.6.4. *Пусть A, B — замкнутые подгруппы алгебраической группы G и пусть C — замыкание взаимного коммутанта $[A, B]$, обозначим через $\mathfrak{a}$, $\mathfrak{b}$ и $\mathfrak{c}$ алгебры Ли групп A, B и C соответственно.*

Тогда для любых $\mathsf{x} \in \mathfrak{a}$, $\mathsf{y} \in \mathfrak{b}$, $x \in A$, $y \in B$ алгебра $\mathfrak{c}$ содержит элементы $\mathsf{y} - \mathsf{y}\mathrm{Ad}\, x$, $\mathsf{x} - \mathsf{x}\mathrm{Ad}\, y$, $[\mathsf{x}, \mathsf{y}]$.

Доказательство. Если $x \in A$, то отображение γ_x переводит B в C, следовательно, его дифференциал $1 - \mathrm{Ad}\, x$ переводит $\mathfrak{b}$ в $\mathfrak{c}$, откуда следует, что $\mathsf{y} - \mathsf{y}\mathrm{Ad}\, x \in \mathfrak{c}$. Аналогичные рассуждения показывают, что $\mathsf{x} - \mathsf{x}\mathrm{Ad}\, y \in \mathfrak{c}$. Далее, для $\mathsf{x} \in \mathfrak{a}$ рассмотрим морфизм $\varphi : B \to \mathfrak{c}$ ($\mathfrak{c}$ можно рассматривать как аффинное многообразие), заданный правилом $y^\varphi = \mathsf{x} - \mathsf{x}\mathrm{Ad}\, y$. Поскольку φ переводит e в 0, мы можем найти $\mathrm{d}\varphi_e : \mathfrak{b} \to \mathfrak{c}$ ($\mathfrak{c}$ является собственным касательным пространством в точке 0). Поскольку $\mathrm{dAd} = \mathrm{ad}$, мы получаем, что $\mathsf{y}^{\mathrm{d}\varphi_e} = -\mathsf{y}^{(\mathsf{x})\mathrm{ad}} = [\mathsf{x}, \mathsf{y}]$ лежит в $\mathfrak{c}$. □

Следствие 4.6.5. *Пусть G — алгебраическая группа, H — замыкание коммутанта $[G, G]$ и $\mathfrak{h}$ — алгебра Ли группы H. Тогда $\mathfrak{h} \ge [\mathfrak{g}, \mathfrak{g}] = \langle [\mathsf{x}, \mathsf{y}] | \mathsf{x}, \mathsf{y} \in \mathfrak{g} \rangle$.*

Лемма 4.6.6. *Пусть G — алгебраическая группа, $x \in G$. Тогда $\mathfrak{L}(C_G(x)) \le \mathfrak{c}_{\mathfrak{g}}(x) = \{\mathsf{x} \in \mathfrak{g} | \mathsf{x} = \mathsf{x}\mathrm{Ad}\, x\}$. Если $G = \mathrm{GL}_n(\mathbb{F})$, то справедливо равенство.*

Доказательство. Очевидно, поскольку $C_G(x)$ является ядром морфизма $\gamma_x : G \to G$. □

§7 Разложение Жордана-Шевалле

Рассмотрим сначала произвольное векторное пространство V размерности n над полем $\mathbb{F}$ и пусть $x \in \mathrm{M}_n(\mathbb{F}) = \mathrm{M}(V)$. Элемент x называется *полупростым*, если его минимальный многочлен не имеет кратных корней. Это эквивалентно тому, что матрица элемента x подобна диагональной. Напомним, что элемент x является нильпотентным, если $x^k = 0$ для некоторого k. Из курса линейной алгебры хорошо известно, что справедливо следующее *аддитивное разложение Жордана*.

Лемма 4.7.1. *Пусть $x \in \mathrm{M}_n(\mathbb{F})$. Тогда:*

(a) *существуют единственные элементы $x_s, x_n \in \mathrm{M}_n(\mathbb{F})$, удовлетворяющие $x = x_s + x_n$, x_s полупрост, а x_n нильпотентен и $x_s x_n = x_n x_s$;*

(б) *существуют полиномы $p(T), q(T)$ от одной переменной без постоянного члена, для которых $x_s = p(x)$, $x_n = q(x)$. В частности, x_s, x_n перестановочны с любым элементом из $\mathrm{M}_n(\mathbb{F})$, с которым перестановочен x;*

(в) *если $U, W \leq V$ — подпространства и $Ux \leq W$, то $Ux_s \leq W$ и $Ux_n \leq W$;*

(г) *если $xy = yx$ для некоторого $y \in \mathrm{M}_n(\mathbb{F})$, то $(x+y)_s = x_s + y_s$ и $(x+y)_n = x_n + y_n$.*

Если $x \in \mathrm{GL}_n(\mathbb{F})$, то все его собственные значения отличны от 0, поэтому элемент x_s невырожден и мы можем рассмотреть элемент $x_u = 1 + x_s^{-1}x_n$, представимый в виде суммы единичного и нильпотентного преобразования. Тогда $x = x_s x_u$ называется *мультипликативным разложением Жордана*. В общем случае элемент $x \in \mathrm{GL}_n(\mathbb{F})$ называется *унипотентным*, если $x - 1 \in \mathrm{M}_n(\mathbb{F})$ — нильпотентный элемент. Из леммы 4.7.1 сразу следует аналогичная лемма для мультипликативного разложения Жордана.

Лемма 4.7.2. *Пусть $x \in \mathrm{GL}_n(\mathbb{F})$. Тогда:*

(а) *существуют единственные элементы $x_s, x_u \in \mathrm{GL}_n(\mathbb{F})$, удовлетворяющие условиям $x = x_s x_u$, x_s полупрост, x_u унипотентен и $x_s x_u = x_u x_s$;*

(б) *элементы x_s, x_u перестановочны с любым элементом из $\mathrm{M}_n(\mathbb{F})$, перестановочным с x;*

(в) *если U — x-инвариантное подпространство пространства V, то U является x_s- и x_u-инвариантным;*

(г) *если $xy = yx$ для некоторого $y \in \mathrm{GL}_n(\mathbb{F})$, то $(xy)_s = x_s y_s$ и $(xy)_u = x_u y_u$.*

Данные нами определения справедливы лишь для конечномерных пространств. Если же мы рассматриваем бесконечномерное пространство V, то элемент x является *полупростым* (соответственно, *нильпотентным, унипотентным*), если ограничение элемента x на каждое конечномерное x-инвариантное подпространство является полупростым (соответственно, нильпотентным, унипотентным) элементом.

Определение 4.7.3. Пусть теперь G — алгебраическая группа. Мы будем говорить, что элемент x группы G является полупростым (соответственно, унипотентным), если преобразование ρ_x аффинной алгебры $\mathbb{F}[G]$ является полупростым (соответственно, унипотентным). Аналогично элемент x алгебры Ли $\mathfrak{g}$ называется полупростым (соответственно, нильпотентным), если $*x$ является полупростым (соответственно, нильпотентным) преобразованием аффинной алгебры $\mathbb{F}[G]$.

Лемма 4.7.4. *Пусть $G = \mathrm{GL}_n(\mathbb{F})$, $\mathfrak{g} = \mathfrak{gl}_n(\mathbb{F})$. Тогда для элементов $x \in G$, $\mathsf{x} \in \mathfrak{g}$ разложения $\rho_{x_s}\rho_{x_u}$ и $(*\mathsf{x}_s)(*\mathsf{x}_n)$ являются разложениями Жордана элементов ρ_x и $*\mathsf{x}$ соответственно.*

Доказательство. Достаточно показать, что элементы $\rho_{x_s}, (*\mathsf{x}_s)$ полупросты, элемент ρ_{x_u} унипотентен, а элемент $(*\mathsf{x}_n)$ нильпотентен, так как проверка справедливость остальных свойств разложения Жордана очевидна.

Рассмотрим G-инвариантное подпространство E и представления $\varphi : G \to \mathrm{GL}(E)$ и $\mathrm{d}\varphi\mathfrak{g} \to \mathfrak{gl}(E)$. Очевидно, что образ нильпотентного элемента при любом гомоморфизме нильпотентен, откуда следует, что элемент $*\mathsf{x}_n$ нильпотентен. Кроме того, элемент $x_u - e$ нильпотентен, следовательно, элемент $x_u^{\varphi} - e^{\varphi}$ нильпотентен и потому элемент ρ_{x_u} является унипотентным.

Далее полупростой элемент x_s переходит в ограничение правого сдвига ρ_{x_s} на E. Пусть $p(T)$ — минимальный многочлен элемента x_s и $q(T)$ — минимальный многочлен элемента ρ_{x_s}. Очевидно, что $q(T)$ делит $p(T)$ и, поскольку $p(T)$ без кратных корней, то $q(T)$ тоже без кратных корней. Аналогичное рассуждение показывает, что элемент $(*\mathsf{x}_s)$ полупрост. □

Теорема 4.7.5. *Пусть G — алгебраическая группа, $\mathfrak{g}$ — её алгебра Ли, $x \in G$, $\mathsf{x} \in \mathfrak{g}$. Тогда:*

(а) *существуют единственные элементы $s, u \in G$ такие, что $x = su = us$, причем s полупрост, а u унипотентен; элементы s, u называются полупростой и унипотентной частью элемента x соответственно и обозначаются x_s, x_u;*

(б) *существую единственные элементы $\mathsf{s}, \mathsf{n} \in \mathfrak{g}$ такие, что $\mathsf{x} = \mathsf{s} + \mathsf{n}$, $[\mathsf{s}, \mathsf{n}] = 0$, причем s полупрост, а n нильпотентен; элементы s, n называются полупростой и нильпотентной частью элемента x соответственно и обозначаются $\mathsf{x}_s, \mathsf{x}_n$;*

(в) *если $\varphi : G \to H$ — морфизм алгебраических групп, то $(x^{\varphi})_s = x_s^{\varphi}$, $(x^{\varphi})_u = x_u^{\varphi}$, $(\mathsf{x}^{\mathrm{d}\varphi_e})_s = \mathsf{x}_s^{\mathrm{d}\varphi_e}$, $(\mathsf{x}^{\mathrm{d}\varphi_e})_n = \mathsf{x}_n$.*

Доказательство. Рассмотрим группу G как замкнутую подгруппу группы $\mathrm{GL}_n(\mathbb{F})$ для подходящего n, тогда все утверждения теоремы легко следуют из лемм 4.7.1, 4.7.2 и 4.7.4. □

§8 Теорема Шевалле

Введем сначала одно специальное многообразие, которое будет играть важную роль в данном параграфе. Пусть V — векторное пространство размерности n над $\mathbb{F}$ и рассмотрим

$$V^d = \underbrace{V \otimes_{\mathbb{F}} \ldots \otimes_{\mathbb{F}} V}_{d \text{ раз}},$$

тензорную степень пространства V. Пусть W — подпространство в V^d, порождённое элементами, содержащими выражение вида $v \otimes v$ для некоторого $v \in V$. Тогда пространство $\wedge^d V = V^d/W$ называется *внешней d-ой степенью* пространства V. Легко видеть, что $\wedge^0 V \simeq \mathbb{F}$, $\wedge^1 V \simeq V$. В общем случае, если $v_1, \ldots, v_n$ — упорядоченный базис пространства V, то $\binom{n}{d}$ внешних произведений вида $v_{i_1} \wedge v_{i_2} \wedge \ldots \wedge v_{i_d}$ $(i_1 < i_2 < \ldots < i_d)$ являются базисом пространства $\wedge^d V$. В частности, размерность пространства $\wedge^n V$ равна 1.

Пусть W — подпространство размерности d пространства V. Тогда $\wedge^d W$ является одномерным подпространством пространства $\wedge^d V$. Следовательно, существует биекция из множества всех d-мерных подпространств пространства V (обозначаемое $\mathcal{D}_d(V)$) в проективное пространство $P(\wedge^d V)$. Более того, фиксируя базис $v_1, \ldots, v_n$ пространства V, мы получаем, что $P(\wedge^d V)$ — проективное многообразие и, следовательно, $\mathcal{D}_d(V)$ также является проективным многообразием. Ввиду леммы 3.6.2 мы получаем, что $\mathcal{D}_0(V) \times \mathcal{D}_1(V) \times \ldots \times \mathcal{D}_n(V)$ также является проективным многообразием.

Последовательность строго вложенных подпространств $0 < V_1 < \ldots < V_k = V$ пространства V называется ***флагом*** пространства V. Флаг называется ***полным***, если $k = n = \dim V$, т. е. если $\dim V_{i+1}/V_i = 1$ для всех i. Множество всех полных флагов пространства V будем обозначать $\mathcal{F}(V)$ и называть ***многообразием флагов***. Ясно, что $\mathcal{F}(V)$ вкладывается в проективное многообразие $\mathcal{D}_0(V) \times \mathcal{D}_1(V) \times \ldots \times \mathcal{D}_n(V)$. Более того, нетрудно заметить, что его образ при этом вложении является замкнутым множеством, поэтому ввиду леммы 3.6.2 является проективным многообразием.

Рассмотрим теперь алгебраическую группу $\mathrm{GL}_n(\mathbb{F})$, её алгебру Ли $\mathfrak{gl}_n(\mathbb{F})$ и их действие на пространстве V и на его d-мерном подпространстве W. Мы получаем индуцированное действие на $\wedge^d V$ следующим образом, если $v_1, \ldots, v_n$ — фиксированный упорядоченный базис пространства V и $x \in \mathrm{GL}_n(V)$, то

$$(v_{i_1} \wedge \ldots \wedge v_{i_d})^x = \sum_{j=1}^{d} v_{i_1} \wedge \ldots \wedge v_{i_j}^x \wedge \ldots \wedge v_{i_d}.$$

Лемма 4.8.1. *В ведённых выше обозначениях пусть $x \in \mathrm{GL}_n(\mathbb{F})$ и $\mathsf{x} \in \mathfrak{gl}_n(\mathbb{F})$. Тогда*

(а) $(\wedge^d W)^x \leq \wedge^d W$ *в том и только в том случае, когда* $W^x \leq W$;

(б) $(\wedge^d W)^{\mathsf{x}} \leq \wedge^d W$ *в том и только в том случае, когда* $W^{\mathsf{x}} \leq W$;

Доказательство. Достаточность очевидна, так что мы докажем лишь необходимость. Для доказательства (а) выберем базис $v_1, \ldots, v_n$ пространства V таким образом, чтобы $v_1, \ldots, v_d$ порождали подпространство W и существовало l, для которого $v_{l+1}, \ldots, v_{l+d}$ порождают подпространство W^x. Достаточно доказать, что $l = 0$. Действительно, $\wedge^d W$ порождено вектором $v_1 \wedge \ldots \wedge v_d$ и, по предположению, элемент x переводит $v_1 \wedge \ldots \wedge v_d$ в $\alpha v_1 \wedge \ldots \wedge v_d$. С другой стороны, по построению, $(v_1 \wedge \ldots \wedge v_d)^x = \beta v_{l+1} \wedge \ldots \wedge v_{l+d}$, откуда следует, что $l = 0$.

Для доказательства (б) выберем базис $v_1, \ldots, v_d$ таким образом, чтобы для первых k векторов выполнялось $v_i^{\mathsf{x}} \in W$, а начиная с $k+1$-ого номера $v_j^{\mathsf{x}} \notin W$; и дополним его до базиса всего пространства. Теперь рассмотрим $\mathsf{y} \in \mathfrak{gl}_n(\mathbb{F})$ такой, что $v_i^{\mathsf{x}} = v_i^{\mathsf{y}}$ при $i \leqslant k$ и $v_i^{\mathsf{y}} = 0$ при $i > k$. Ясно, что $W^{\mathsf{y}} \leq W$, поэтому $(\wedge^d W)^{\mathsf{y}} \leq \wedge^d W$. Следовательно, после замены элемента x на элемент $\mathsf{x} - \mathsf{y}$, мы можем считать, что $W \cap W^{\mathsf{x}} = \{0\}$. Рассмотрим теперь базис $w_1, \ldots, w_d$ пространства W такой, что векторы $w_1^{\mathsf{x}}, \ldots, w_c^{\mathsf{x}}$ образуют базис в W^{x}, а $w_{c+1}^{\mathsf{x}} = \ldots = w_d^{\mathsf{x}} = 0$. По определению,

$$(w_1 \wedge \ldots \wedge w_d)^{\mathsf{x}} = \sum_{i=1}^{d} w_1 \wedge \ldots \wedge w_i^{\mathsf{x}} \wedge \ldots \wedge w_d.$$

По предположению, $(w_1 \wedge \ldots \wedge w_d)^{\mathsf{x}}$ равен $\alpha w_1 \wedge \ldots \wedge w_d$. Но векторы $w_1 \wedge \ldots \wedge w_i^{\mathsf{x}} \wedge \ldots \wedge w_d$ линейно независимы, либо равны нулю и ни один из них не равен $w_1 \wedge \ldots \wedge w_d$. Поэтому $w_i^{\mathsf{x}} = 0$ и $W^{\mathsf{x}} \leq W$. □

Теорема 4.8.2. (Теорема Шевалле) *Пусть G — алгебраическая группа, H — её замкнутая подгруппа. Тогда существует рациональное представление $\varphi : G \to \mathrm{GL}(V)$ и одномерное подпространство $L \leq V$ такие, что $H = \{x \in G | L^{x^{\varphi}} = L\}$ и $\mathfrak{h} = \{\mathsf{x} \in \mathfrak{g} | L^{\mathsf{x}^{\mathrm{d}\varphi}} \leq L\}$.*

Доказательство. Пусть $I = \mathcal{I}(H)$ — идеал алгебры $\mathbb{F}[G]$. Тогда идеал I конечно порождён и линейная оболочка порождающего множества содержится в конечномерном G-инвариантном подпространстве V алгебры $\mathbb{F}[G]$ (см. лемму 4.2.3). Пусть $W = I \cap V$ (значит, W порождает I как алгебру). Ввиду лемм 4.2.1 и 4.4.3 мы получаем, что $H = \{x \in G | W^x = W\}$ и $\mathfrak{h} = \{\mathsf{x} \in \mathfrak{g} | W * \mathsf{x} \leq W\}$. Если теперь $\dim W = d$, то рассмотрим представления $\varphi : G \to \mathrm{GL}(\wedge^d V)$ и $\mathrm{d}\varphi : \mathfrak{g} \to \mathfrak{gl}(\wedge^d V)$. По лемме 4.8.1 мы получаем, что $H = \{x \in G | (\wedge^d W)^{x^{\varphi}} = \wedge^d W\}$, $\mathfrak{h} = \{\mathsf{x} \in \mathfrak{g} | (\wedge^d W)^{\mathsf{x}^{\mathrm{d}\varphi}} \leq \wedge^d W\}$ и $\wedge^d W$ — одномерное подпространство в $\wedge^d V$. $\square$

Глава 5. Строение алгебраических групп

В настоящей главе будут получены структурные результаты о линейных алгебраических группах, мы докажем сопряженность максимальных торов, максимальных унипотентных подгрупп и подгрупп Бореля, введем параболические подгруппы, корневые подгруппы и систему корней полупростой линейной алгебраической группы, а также дадим классификацию простых алгебраических групп. Как и раньше, под термином «алгебраическая группа» всегда понимается линейная алгебраическая группа.

§1 Сопряженность подгрупп Бореля

Нам понадобится следующая лемма, которую мы приведем без доказательства. (см. [17, Лемма 21.1]).

Лемма 5.1.1. *Пусть алгебраическая группа G действует транзитивно на каждом из двух неприводимых многообразий X, Y и предположим, что существует биективный морфизм $\varphi : X \to Y$, перестановочный с действием группы G. Тогда если многообразие Y полно, то и X полно.*

Отметим также еще одну простую лемму.

Лемма 5.1.2. *Пусть A, B — замкнутые подгруппы алгебраической группы G и группа A связна. Тогда коммутант $[A, B]$ замкнут и связен.*

Доказательство. Очевидно, что $[A, B]$ порождается множествами $\{A^{\gamma_b} | b \in B\}$. Так как группа A связна, то и её образ A^{γ_b} связен для любого $b \in B$, кроме того, он содержит единицу. По теореме 4.1.8 группа $[A, B]$ замкнута и связна. □

Следствие 5.1.3. *Пусть G — связная нильпотентная алгебраическая группа. Тогда* $\dim Z(N) > 0$.

Доказательство. Действительно, нижний центральный ряд состоит из связных подгрупп (по лемме 5.1.2) и последний неединичный член этого ряда содержится в центре. □

Следствие 5.1.4. *Пусть G — связная нильпотентная алгебраическая группа и H — её подгруппа. Тогда* $\dim N_G(H) > \dim H$. *В частности, если H — подгруппа коразмерности 1 группы G, то H нормальна в G*

Доказательство. Если $Z = Z(G)^0 \leq H$, то мы можем рассмотреть факторгруппы G/Z и H/Z и наше утверждение получается индукцией по размерности группы. Если $Z \not\leq H$, то группа ZH является связной (как порождённая связными подгруппами), кроме того, очевидно, что $ZH \leq N_G(H)$. Поскольку $ZH \neq H$ и ZH связна, мы получаем, что $\dim N_G(H) \geq \dim ZH > \dim H$. □

Теорема 5.1.5. (Теорема о неподвижной точке) *Пусть G — связная разрешимая алгебраическая группа и пусть X — непустое полное многообразие, на котором действует группа G. Тогда группа G имеет на X неподвижную точку.*

Доказательство. Доказательство будем вести индукцией по размерности группы G. Если $\dim G = 0$, то $G = \{e\}$ и доказывать нечего. Рассмотрим коммутант $H = [G, G]$. Ввиду леммы 5.1.2 мы получаем, что H является связной замкнутой подгруппой группы G. Так как группа G разрешима, подгруппа H является собственной, следовательно, по лемме 3.5.3, $\dim H < \dim G$. По предположению индукции, множество Y неподвижных точек относительно действия группы H непусто и, по лемме 4.3.1, замкнуто. Ввиду леммы 3.6.2 множество Y является проективным многообразием. Кроме того, H нормальна в G, следовательно, множество Y является G-инвариантным. Поэтому мы можем заменить X на Y и считать, что H действует тривиально на X.

Таким образом, группа H содержится в $St_G(x)$ для любой точки $x \in X$. Так как G/H абелева, мы получаем, что $St_G(x)$ — нормальная подгруппа группы G, следовательно, $G/St_G(x)$ — аффинное многообразие. Ввиду леммы 4.3.2 существует такая точка x, что её орбита $x \cdot G$ замкнута, следовательно, является полным многообразием. Далее, канонический морфизм $G/St_G(x) \to x \cdot G$ биективен, перестановочен с действием группы G и $x \cdot G$ полно. Ввиду леммы 5.1.1 множество $G/St_G(x)$ также полно. Но по лемме 3.6.2 аффинное полное многообразие имеет размерность 0, т. е. $G = St_G(x)$. □

В качестве следствия из теоремы мы докажем теорему Ли-Колчина-Мальцева 1.8.11 для алгебраических разрешимых групп (чуть позже мы дадим её доказательство в общем случае).

Следствие 5.1.6. *Пусть G — связная замкнутая разрешимая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$. Тогда группа G сопряжена с подгруппой группы верхнетреугольных матриц.*

Доказательство. Рассмотрим действие группы G на многообразии флагов $\mathcal{F}(V)$. Это многообразие проективно, следовательно, существует неподвижная точка относительно действия группы G. Эта неподвижная точка является полным флагом, т. е. G стабилизирует цепочку вложенных подпространств $0 < V_1 < \ldots < V_n = V$, и в соответствующей базе любой элемент из G является верхнетреугольной матрицей. □

Определение 5.1.7. Пусть G — линейная алгебраическая группа. Максимальная (по включению) связная замкнутая разрешимая подгруппа B группы G называется её *подгруппой Бореля.*

Теорема 5.1.8. *Пусть B — подгруппа Бореля группы G. Тогда G/B — проективное многообразие и все подгруппы Бореля группы G сопряжены.*

Доказательство. Поскольку подгруппа, порождённая связными группами, связна (см. следствие 4.1.9), мы получаем, что любая подгруппа Бореля группы G лежит в G^0. Таким образом, можно считать, что группа G связна. Пусть S — подгруппа Бореля группы G наибольшей размерности. В силу теоремы Шевалле 4.8.2 существует рациональное представление $\varphi : G \to \mathrm{GL}_n(\mathbb{F})$, при котором S^φ является стабилизатором некоторого одномерного подпространства V_1. По теореме Ли-Колчина-Мальцева (следствие 5.1.6) индуцированное действие группы S на фактор пространстве V/V_1 является триангулируемым, следовательно, подгруппа S оставляет неподвижным некоторый полный флаг $f = 0 < V_1 < \ldots < V_n = V$. Из построения представления φ следует, что $S = St_G(f)$. Следовательно, морфизм многообразия G/S на орбиту флага f в многообразии $\mathcal{F}(V)$ является биекцией. С другой стороны, стабилизатор любого флага разрешим (так как он сопряжен с подгруппой группы верхнетреугольных матриц) и, следовательно, его размерность не превышает размерности подгруппы S. Значит, орбита флага f имеет наименьшую возможную размерносить, следовательно, она замкнута (см. лемму 4.3.2). Как замкнутое подмножества проективного многообразия $\mathcal{F}(V)$ эта орбита является проективным многообразием.

Далее, произвольная подгруппа Бореля B группы G действует правыми умножениями на проективном многообразии G/S и по теореме о неподвижной точке 5.1.5 она имеет неподвижную точку Sx, т. е. $SxB = Sx$ или $xBx^{-1} \leq S$. Но xBx^{-1} является подгруппой Бореля, откуда $xBx^{-1} = S$. □

§2 Диагонализируемые группы

За основу изложения данного параграфа взят [17, § 16].

Напомним, что произвольный элемент замкнутой алгебраической группы представим в виде произведения коммутирующих полупростого и унипотентного элементов (см. теорему 4.7.5). Алгебраическая группа G называется *диагонализируемой*, если она изоморфна (как алгебраическая группа) подгруппе группы $D_n(\mathbb{F})$. Ясно, что подгруппы и гомоморфные образы диагонализируемых групп вновь являются диагонализируемыми группами. Для того, чтобы определить строение алгебраических групп введем понятие *характера алгебраической группы* или просто *характера.* Характером алгебраической группы G называется морфизм $G \to \mathbb{F}^*$ группы G в мультипликативную группу поля $\mathbb{F}$. Если χ, ψ — два характера группы G, то мы можем ввести умножение, полагая $x^{\chi \cdot \psi} = x^\chi \cdot x^\psi$ для произвольного $x \in G$. Относительно определенного таким образом умножения характеры алгебраической группы G образуют *группу характеров*, обозначаемую $X(G)$. Ясно, что $X(G)$ можно рассматривать как подмножество алгебры $\mathbb{F}[G]$.

Лемма 5.2.1. *Пусть G — (абстрактная) группа, X — множество всех гомоморфизмов $G \to \mathbb{F}^*$. Тогда X — линейно независимое подмножество пространства всех функций на G со значениями в $\mathbb{F}$.*

Доказательство. Предположим противное, пусть $\chi_1, \ldots, \chi_n \in X$ — линейно зависимые функции, причем $n > 1$ выбрано наименьшим возможным. Запишем $\sum_{i=1}^{n-1} a_i\chi_i + \chi_n = 0$ ($a_i \in \mathbb{F}$). Так как $\chi_1 \neq \chi_n$, существует такой элемент $y \in G$, что $\chi_1(y) \neq \chi_n(y)$. Для произвольного элемента $x \in G$ мы получаем два уравнения:

$$\sum_{i=1}^{n-1} a_i\chi_i(x)\chi_i(y) + \chi_n(x)\chi_n(y) = 0,$$

$$\sum_{i=1}^{n-1} a_i\chi_i(x)\chi_n(y) + \chi_n(x)\chi_n(y) = 0.$$

Вычитая второе уравнение из первого и пользуясь произвольностью x, мы получаем:

$$\sum_{i=1}^{n-1} a_i(\chi_i(y) - \chi_n(y))\chi_i = 0.$$

Но, ввиду выбора n, все χ_i при $1 \leqslant i \leqslant n-1$ линейно независимы, значит, (так как $\chi_1(y) \neq \chi_n(y)$) $a_1 = 0$, т. е. характеры $\chi_2, \ldots, \chi_n$ линейно зависимы, что противоречит минимальности n. □

***Упражнение* 5.2.2.** Если $G = [G, G]$, то $X(G) = 0$.

Будем говорить, что алгебраическая группа G является *d-группой* , если в алгебре $\mathbb{F}[G]$ существует базис, состоящий из характеров, т. е., ввиду леммы 5.2.1, если $X(G)$ — базис алгебры $\mathbb{F}[G]$.

***Пример* 5.2.3.** Рассмотрим подгруппу диагональных матриц $\mathrm{D}_n(\mathbb{F})$ группы $\mathrm{GL}_n(F)$ и покажем, что $\mathrm{D}_n(\mathbb{F})$ является d-группой. Действительно, $\mathbb{F}[G] = \mathbb{F}[T_1, \ldots, T_n, \frac{1}{T_1}, \ldots, \frac{1}{T_n}]$, где T_i — выбор $i^{\text{ого}}$ диагонального элемента. Поэтому любой одночлен вида $T_1^{m_1} \cdot \ldots \cdot T_n^{m_n}$, где $m_i \in \mathbb{Z}$, является характером группы $\mathrm{D}_n(\mathbb{F})$. Заметим также, что $X(\mathrm{D}_n(\mathbb{F})) \simeq \mathbb{Z}^n$.

Если G_1, G_2 — d-группы, то морфизм $\varphi : G_1 \to G_2$ алгебраических групп индуцирует групповой гомоморфизм $\varphi^0 : X(G_2) \to X(G_1)$, который является сужением коморфизма $\varphi^* : \mathbb{F}[G_2] \to \mathbb{F}[G_1]$. Обратно, гомоморфизм групп $X(G_2) \to X(G_1)$ продолжается до гомоморфизма $\mathbb{F}$-алгебр $\mathbb{F}[G_2] \to \mathbb{F}[G_1]$ и, в свою очередь, определяет гомоморфизм $G_1 \to G_2$.

Лемма 5.2.4. (а) *Если H — замкнутая подгруппа d-группы G, то H также является d-группой, совпадающей с пересечением ядер некоторых характеров группы G. В частности, диагонализируемые группы являются d-группами.*

(б) *Любая d-группа диагонализируема.*

Доказательство. (а) Канонический гомоморфизм $\mathbb{F}[G] \to \mathbb{F}[H]$, индуцированный ограничением функций, сюръективен. Очевидно, ограничение на H характера группы G есть характер группы H, так что пространство $\mathbb{F}[H]$ порождается группой $X(H)$, т. е. H является d-группой. Пусть, далее, $f \in \mathcal{I}(H)$. Так как G — d-группа, имеем $f = \sum a_i\chi_i$, где $a_i \in \mathbb{F}$ и $\chi_i \in X(G)$. Ввиду леммы 5.2.1 (применённой к H), сумма коэффициентов при характерах с одинаковыми ограничениями на H равна 0, так что пространство $\mathcal{I}(H)$ натянуто на различные элементы вида $\sum b_i\chi_i$, где $\sum b_i = 0$ и все χ_i имеют одинаковые ограничения на H (совпадают как характеры группы H). С другой стороны,

$$\sum_{i=1}^{m} b_i\chi_i = \chi_1\left(\sum_{i=2}^{m} b_i(\chi_1^{-1}\chi_i - 1)\right).$$

Отсюда следует, что $\mathcal{I}(H)$ порождается как идеал всевозможными элементами $\theta - 1$, где $\theta = \chi_1^{-1}\chi_i \in X(G)$. Наконец, так как $\mathrm{D}_n(\mathbb{F})$ является d-группой (см. пример 5.2.3), то мы приходим к выводу, что диагонализируемые группы являются d-группами.

(б) Пусть G — d-группа. Так как $\mathbb{F}[G]$ — конечно порождённая $\mathbb{F}$-алгебра, натянутая на $X(G)$, то она порождается как $\mathbb{F}$-алгебра некоторым конечным множеством характеров $\chi_1, \ldots, \chi_n$. Определим отображение $\varphi : G \to \underbrace{\mathbb{F}^* \times \ldots \times \mathbb{F}^*}_{n \text{ экземпляров}} \simeq \mathrm{D}_n(\mathbb{F})$, полагая $x^\varphi = (x^{\chi_1}, \ldots, x^{\chi_n})$. Очевидно, φ — морфизм алгебраических групп с тривиальным ядром (так как $\chi_1, \ldots, \chi_n$ порождают $\mathbb{F}[G]$). В частности, группа G должна быть коммутативной и состоять из полупростых элементов, т. е. группа G диагонализируема. □

Замечание. Заметим, что построенный выше морфизм является изоморфизмом абстрактных групп, но может не являться изоморфизмом алгебраических групп, так как коморфизм может иметь нетривиальное ядро. Смотри упражнение 5.2.10.

Лемма 5.2.5. *Пусть G — d-группа. Тогда $X(G)$ — конечно порождённая абелева группа.*

Доказательство. Ввиду леммы 5.2.4 мы можем считать, что G является замкнутой подгруппой группы $D_n(\mathbb{F})$. Ввиду примера 5.2.3 мы получаем, что $X(\mathrm{D}_n(\mathbb{F})) \simeq \mathbb{Z}^n$. Таким образом, $X(G)$ есть гомоморфный образ группы $X(\mathrm{D}_n(\mathbb{F}))$. □

***Упражнение* 5.2.6.** [17, Упражнение 16.12] Пусть G — алгебраическая группа, $H = \bigcap_{\chi\in X(G)} \mathrm{Ker}(\chi)$. Доказать, что

(а) H — замкнутая подгруппа группы G;

(б) группа G/H диагонализируема;

(в) $X(G) \simeq X(G/H)$.

В частности, группа $X(G)$ конечно порождена. Описать группу $X(\mathrm{GL}_n(\mathbb{F}))$.

Лемма 5.2.7. *Если G — связная алгебраическая группа, то группа $X(G)$ не имеет элементов конечного порядка.*

Доказательство. Для $\chi \in X(G)$ образ G^χ группы G в $\mathbb{F}^*$ связен. Единственные связные подгруппы группы $\mathbb{F}^*$ — это она сама и единичная подгруппа. Отсюда следует, что $\chi^n \neq 1$, если $\chi \neq 1$. □

Алгебраическая группа, изоморфная $\mathrm{D}_n(\mathbb{F})$, называется *тором.*

Лемма 5.2.8. *Пусть T — тор. Если характеры $\chi_1, \ldots, \chi_n \in X(T)$ линейно независимы и $c_1, \ldots, c_r \in \mathbb{F}^*$, то существует элемент $t \in T$, для которого $t^{\chi_i} = c_i$ для $1 \leqslant i \leqslant r$.*

Доказательство. Заметим, что понятие линейной независимости для характеров имеет смысл, поскольку $X(T)$ — свободная абелева группа конечного ранга. Определим морфизм $\varphi : T \to \underbrace{\mathbb{F}\times\ldots\times\mathbb{F}}_{r \text{ экземпляров}}$ формулой $t^\varphi = (t^{\chi_1}, \ldots, t^{\chi_r})$. Так как характеры $\chi_1, \ldots, \chi_n$ линейно независимы, то функции $\prod_{i=1}^n \chi_i^{m_i}$ линейно независимы над $\mathbb{F}$ в $\mathbb{F}[T]$ для всех $m_i \in \mathbb{Z}$ (см. лемму 5.2.1). Следовательно, характеры $\chi_1, \ldots, \chi_n$ алгебраически независимы в $\mathbb{F}(T)$, так что коморфизм φ^* инъективен, значит, φ сюръективен. □

Теорема 5.2.9. *Пусть G — произвольная d-группа. Тогда $G = G^0 \times H$ (прямое произведение алгебраических групп), где G^0 — тор и H — конечная группа, порядок которой взаимно прост с p ($= \mathrm{char}\ \mathbb{F}$). В частности, связная d-группа есть тор.*

Доказательство. Можно считать, что G —замкнутая подгруппа некоторой группы $D = \mathrm{D}_n(\mathbb{F})$. Пусть ранг без кручения группы $X(G)$ равен r ($= \dim G$ ввиду леммы 5.2.7). Если $r = 0$, то группа G конечная и доказывать нечего. В общем случае вложение $G^0 \hookrightarrow D$ индуцирует сюръективный гомоморфизм ограничения $\varphi : \mathbb{Z}^n = X(D) \to X(G^0) = \mathbb{Z}^r$. Из теории свободных абелевых групп следует, что существует расщепление $X(D) = \mathrm{Ker}(\varphi) \oplus \mathbb{Z}^r$. Как подгруппа свободной абелевой группы $X(D)$ ядро $\mathrm{Ker}(\varphi)$ имеет базис $\chi_1, \ldots \chi_{n-r}$, который можно дополнить базисом $\chi_{n-r+1}, \ldots, \chi_n$ модуля $\mathbb{Z}^r$ (отображение φ переводит этот базис в базис модуля $X(G^0)$). Ясно, что отображение $x \mapsto \mathrm{diag}(x^{\chi_1}, \ldots, x^{\chi_n})$ определяет автоморфизм группы D (см. лемму 5.2.7), преобразующий группу G^0 в подгруппу диагональных матриц, у которых первые $n-r$ координат равны 1 (в частности, G^0 — тор). Если D' — подгруппа диагональных матриц, у которых последние r координат равны 1, то $D = D' \times G^0$ (прямое произведение алгебраических групп). Следовательно, $G = H \times G^0$, где $H = D' \cap G \simeq G/G^0$. Наконец, порядок группы H взаимно прост с p, поскольку в группе $\mathbb{F}^*$ нет элементов порядка p. □

***Упражнение* 5.2.10.** [17, Упражнение 16.8] Дифференциалом характера $\chi : G \to \mathbb{F}^*$ является линейная функция $\mathrm{d}\chi : \mathfrak{g} \to \mathbb{F}$. Доказать, что если G — тор и $\chi_1, \ldots, \chi_n$ — базис группы характеров $X(G)$, то $\mathrm{d}\chi = 0$ тогда и только тогда, когда $\chi = p\sum_{i=1}^n a_i\chi_i$, где $a_i \in \mathbb{Z}$ и $p = \mathrm{char}\ \mathbb{F}$.

Основной нашей задачей до конца этого параграфа будет доказательство, так называемой, жесткости d-групп (см. лемму 5.2.12 ниже). Для доказательства этого факта нам потребуются следующие факты об элементах конечного порядка в d-группах:

(а) элементы конечного порядка образуют плотное множество;

(б) имеется лишь конечное число элементов данного конечного порядка.

Чтобы доказать эти факты заметим, что достаточно рассмотреть лишь случай $G = \mathbb{F}^*$. Элементы группы $\mathbb{F}^*$, имеющие порядок m — это в точности $m^{\text{ые}}$ корни из 1 в поле $\mathbb{F}$. Поэтому для каждого $m \in \mathbb{N}$ существует лишь конечное число таких корней и для всех m взаимно простых с характеристикой существует в точности m таких корней (ввиду алгебраической замкнутости поля $\mathbb{F}$). Следовательно, в $\mathbb{F}^*$ существует бесконечно много элементов конечного порядка, которые образуют плотное подмножество, ввиду связности группы $\mathbb{F}^*$.

Теорема 5.2.11. *Пусть $\varphi : V \times G \to H$ — морфизм многообразий, причем выполнены следующие условия:*

(а) *G — алгебраическая группа, элементы конечного порядка которой образуют плотное подмножество;*

(б) *H — алгебраическая группа, содержащая лишь конечное число элементов данного порядка m для каждого $m > 0$;*

(в) *V — связное многообразие;*

(г) *для каждого элемента $x \in V$ морфизм $\varphi_x : G \to H$, заданный правилом $\varphi_x : y \mapsto (x, y)^\varphi$, есть гомоморфизм групп.*

Тогда отображение $x \mapsto \varphi_x$ является постоянным отображением (т. е. для всех $x, z \in V$ выполнено $\varphi_x = \varphi_z$).

Доказательство. Пусть $y \in G$ положим $\psi_y : x \mapsto (x, y)^\varphi$, так что $\psi_y : V \to H$ — морфизм. Если порядок элемента y конечен, то образ морфизма ψ_y также конечен ввиду (б) и (г). Но многообразие V связно ввиду (в), поэтому его образ должен быть точкой. Другими словами, для каждого элемента y конечного порядка в группе G мы имеем $(x, y)^\varphi = (z, y)^\varphi$ для всех $x, z \in V$, т. е. $y^{\varphi_x} = y^{\varphi_z}$. Следовательно $\varphi_z \cdot \varphi_x^{-1}$ ($y^{\varphi_z \cdot \varphi_x^{-1}} = y^{\varphi_z} \cdot (y^{-1})^{\varphi_x}$)) отображает плотное подмножество элементов конечного порядка группы G в e. Значит, $\varphi_x = \varphi_z$ для всех $x, z \in V$. □

Лемма 5.2.12. (лемма о жесткости d-групп) *Пусть D — диагонализируемая замкнутая подгруппа алгебраической группы G. Тогда $N_G(D)^0 = C_G(D)^0$.*

Доказательство. Возьмём G, H из теоремы 5.2.11 равными T, так что условия (а) и (б) выполняются. Тогда положим $V = N_G(D)^0$ и зададим морфизм $\varphi : V \times D \to D$ соотношением $\varphi : (x, y) \mapsto x^{-1}yx$. Очевидно, предположеня (в) и (г) выполняются. Из того, что отображение φ_x постоянно, следует, что $\varphi_x = \varphi_e$, т. е., что все элементы группы $N_G(D)^0$ на самом деле централизуют D. Обратное включение $C_G(D)^0 \subseteq N_G(D)^0$ очевидно. □

В конце данного параграфа мы приведём одну конструкцию, основное применение которой будет позже, а сейчас мы получим одно важное следствие.

Пусть D — некоторая диагонализируемая подгруппа алгебраической группы G. Тогда для любого $x \in D$ отображение $\mathrm{Int}x$ является автоморфизмом группы G и его дифференциал $\mathrm{Ad}\, x$ — есть автоморфизм алгебры ли $\mathfrak{g}$. Так как ввиду теоремы 4.5.6 отображение Ad является морфизмом алгебраических групп, мы получаем, что D^{Ad} является диагонализируемой подгруппой группы $\mathrm{Aut}\mathfrak{g} \le \mathrm{GL}(\mathfrak{g})$. Для любой диагонализируемой подгруппы H группы $\mathrm{GL}(V)$ пространство V удобно записать в виде прямой суммы подпространств V_α, где $\alpha \in X(H)$ и $V_\alpha = \{v \in V | v^x = x^\alpha v$ для всех $x \in H\}$ (подпространство V_α называется *весовым пространством*). Те функции α, для которых $V_\alpha \neq \{0\}$ называются *весами* группы H в пространстве V. В частности, возвращаясь к ситуации $D \le G$, $D^{\mathrm{Ad}} \le \mathrm{GL}(\mathfrak{g})$, мы получаем веса группы D (точнее, её образа D^{Ad}) в $\mathfrak{g}$. Нетривиальные веса называются *корнями группы G относительно D*. Множество корней группы G относительно d-подгруппы D обозначается через $\Phi(G, D)$ или просто через Φ, если не возникает путаницы. Если $\mathfrak{d}$ — алгебра Ли группы D, то весу 0 (в аддитивной терминологии) соответствует некоторая подалгебра $\mathfrak{g}_0$ алгебры $\mathfrak{g}$, содержащая (но, возможно, бóльшая, чем) $\mathfrak{d}$. В этих обозначениях мы можем записать

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \sum_{\alpha \in \Phi(G,D)} \mathfrak{g}_\alpha.$$

Позднее мы покажем, что если группа G полупроста (определение будет дано позднее), то данное сейчас определение согласуется с определением корневой системы, данным во второй главе.

Лемма 5.2.13. *Пусть D — тор алгебраической группы G, H — замкнутая D-инвариантная подгруппа группы G (т. е. $D \leq N_G(H)$). Тогда существует элемент $x \in D$ такой, что $C_H(x) = C_H(D)$ и $\mathfrak{c}_\mathfrak{h}(x) = \mathfrak{c}_\mathfrak{h}(D)$. В частности, $C_G(D)$ совпадает с централизатором некоторого элемента группы D.*

Доказательство. Можно предполагать, что $G = \mathrm{GL}(V)$. Запишем $V = V_1 \oplus \ldots \oplus V_r$, где пространство V_i соответствует весу $\alpha_i \in X(D)$. Так как группа D связна. то подгруппа $\mathrm{Ker}(\alpha_i\alpha_j^{-1})$ (по всем $i \neq j$ имеет коразмерность не менее 1 в D; следовательно, найдётся элемент $x \in D$, не принадлежащий ни одной из этих подгрупп (число которых конечно). Рассмотрим группу $M = \mathrm{GL}(V_1) \times \ldots \times \mathrm{GL}(V_r)$ как замкнутую подгруппу группы $\mathrm{GL}(V)$. Тогда легко видеть, что $C_H(x) = M \cap H = C_H(D)$, $\mathfrak{c}_\mathfrak{h}(x) = \mathfrak{L}(M) \cap \mathfrak{h} = \mathfrak{c}_\mathfrak{h}(d)$. □

***Упражнение* 5.2.14.** Пусть D — произвольный тор алгебраической группы G. Доказать, что множество $X = \{x \in D | C_G(x) = C_G(D)\}$ содержит открытое подмножество тора D и потому плотно в D.

§3 Полупростые элементы

Пусть $s \in G$ — произвольный полупростой элемент группы G. Тогда его образ $\mathrm{Ad}\ s$ является полупростым автоморфизмом алгебры Ли $\mathfrak{g}$, следовательно, мы можем записать разложение $\mathfrak{g} = \mathfrak{c}_\mathfrak{g}(s) \oplus \mathfrak{n}$, где $\mathfrak{n}$ — сумма собственных подпространств автоморфизма $\mathrm{Ad}\ s$, отвечающих собственным значениям отличным от 1.

Пусть H — замкнутая подгруппа группы $G = \mathrm{GL}_n(\mathbb{F})$, которая нормализуется некоторым полупростым элементом $s \in G$. Очевидно, $C_H(s) = H \cap C_G(s)$, откуда следует, что $\mathfrak{L}(C_H(s)) \leq \mathfrak{h} \cap \mathfrak{L}(C_G(s)) = \mathfrak{h} \cap \mathfrak{c}_\mathfrak{g}(s) = \mathfrak{c}_\mathfrak{h}(s)$ (равенство $\mathfrak{L}(C_G(s)) = \mathfrak{c}_\mathfrak{g}(s)$ в том случае, когда $G = \mathrm{GL}_n(\mathbb{F})$ доказано в лемме 4.6.6). Мы хотим доказать обратное включение и, тем самым, доказать равенство. Для доказательства обратного включения надо доказать, что $\dim \mathfrak{c}_\mathfrak{h}(s) \leqslant \dim \mathfrak{L}(C_H(s))$. Поскольку элемент $\mathrm{Ad}\ s$ полупрост, мы имеем разложение $\mathfrak{h} = \mathfrak{c}_\mathfrak{h}(s) \oplus \mathfrak{n}'$, где $\mathfrak{n}'$ — сумма нетривиальный собственных подпространств.

Ввиду леммы 4.3.2 класс сопряженности $Cl_G(s)$ — локально замкнутое множество размерности, дополнительной к размерности централизатора $C_G(s)$ (см. [17, Теорема 4.3], где $X = G$, $Y = Cl_G(s)$, $\varphi : X \to Y$, $g \overset{\varphi}{\mapsto} s^g$). Его сдвиг $M = s^{-1}Cl_G(s)$ содержит e, так что мы можем рассматривать его касательное пространство $\mathcal{T}(M)_e = \mathfrak{m}$ как подпространство в $\mathcal{T}(G)_e = \mathfrak{g}$. Мы увидим ниже, что $\mathfrak{m}$ совпадает с пространством $\mathfrak{n}$, определенным ранее. Далее, $M \cap H \supseteq M' = s^{-1}Cl_H(s)$, коразмерность многообразия M' в H равна $\dim C_H(s)$ и его касательное пространство $\mathfrak{m}'$ лежит в $\mathfrak{m} \cap \mathfrak{h} = \mathfrak{n} \cap \mathfrak{h} = \mathfrak{n}'$. Таким образом, если мы покажем, что $\mathfrak{m} = \mathfrak{n}$, то из включения $\mathfrak{m}' \leq \mathfrak{n}'$ следует, что коразмерность $C_H(s)$ в H равна $\dim M' \leqslant \dim \mathfrak{n}'$ равна коразмерности $\mathfrak{c}_\mathfrak{h}(s)$ в $\mathfrak{h}$, откуда $\dim \mathfrak{c}_\mathfrak{h}(s) \leqslant \dim C_H(s) = \dim \mathcal{L}(C_H(s))$.

Остается показать, что $\mathfrak{m} = \mathfrak{n}$. Напомним, что морфизм $\gamma_s : G \to G$, определенный правилом $x^{\gamma_s} = s^{-1}x^{-1}sx$ имеет своим дифференциалом линейное отображение $1 - \mathrm{Ad}\ s : \mathfrak{g} \to \mathfrak{g}$ (см. лемму 4.5.1). Очевидно, $M = G^{\gamma_s}$, так что $\mathfrak{g}(1 - \mathrm{Ad}\ s) \leq \mathfrak{m}$. С другой стороны ясно, что $\mathrm{Ker}(\mathrm{d}\gamma_s) = \mathfrak{c}_\mathfrak{g}(s)$ и $\mathrm{Im}(\mathrm{d}\gamma_s) = \mathfrak{n}$, так что, в частности, $\mathfrak{n} \leq \mathfrak{m}$. Поскольку $\mathfrak{c}_\mathfrak{g}(s) = \mathfrak{L}(C_G(s))$, то $\dim \mathfrak{m} = \dim M = \dim G - \dim C_G(s) = \dim \mathfrak{g} - \dim \mathfrak{c}_\mathfrak{g}(s) = \dim \mathfrak{n}$. Следовательно, $\mathfrak{n} = \mathfrak{m}$. Таким образом, мы получили следующую лемму.

Лемма 5.3.1. *Пусть H — замкнутая подгруппа группы $\mathrm{GL}_n(\mathbb{F})$, которая нормализуется полупростым элементом $s \in \mathrm{GL}_n(\mathbb{F})$. Тогда $\mathfrak{c}_\mathfrak{h}(s) = \mathfrak{L}(C_H(s))$ и сумма всех нетривиальных собственных подпространств оператора $\mathrm{Ad}\ s$ в $\mathfrak{h}$ есть касательное пространство многообразия $s^{-1}Cl_H(s)$.*

***Упражнение* 5.3.2.** Показать, что лемма 5.3.1 неверна в общем случае.

Лемма 5.3.3. *Пусть H — замкнутая подгруппа группы $G = \mathrm{GL}_n(\mathbb{F})$, нормализуемая полупростым элементом $s \in G$. Тогда класс сопряженности $Cl_H(s)$ замкнут.*

Доказательство. Если x — эндоморфизм конечномерного векторного пространства и T — переменная, обозначим через $m(x, T)$ минимальный многочлен элемента x, а через $\chi(x, T)$ — характеристический многочлен элемента x. Напомним, что x полупрост тогда и только тогда, когда $m(x, T)$ не имеет кратных корней.

Положим теперь $W = \{x \in N_G(H) | m(s, x) = 0 \text{ и } \chi(\mathrm{Ad}\ x\ |_\mathfrak{h}, T) = \chi(\mathrm{Ad}\ s\ |_\mathfrak{h}, T)\}$. Очевидно, что W — замкнутое подмножество в $N_G(H)$ (и, следовательно, в G), инвариантное относительно сопряжения элементами из H. Первое условие в определении множества W требует, чтобы каждый элемент $x \in W$ аннулировал минимальный многочлен элемента s, который, по предположению, не имеет кратных корней. Следовательно, элемент x также полупрост. Применим теперь к действию элемента x на H лемму 5.3.1, получим

$\dim Cl_H(x) = \dim H - \dim C_H(x) = \dim \mathfrak{h} - \dim \mathfrak{c}_{\mathfrak{h}}(x) = \dim \mathfrak{h} - m_1(x)$, где $m_1(x)$ — кратность собственного значения 1 для оператора $\mathrm{Ad}\, x\mid_{\mathfrak{h}}$. Но второе условие в определении W дает $m_1(x) = m_1(s)$, откуда следует, что все H-орбиты в W имеют равные размерности. Ввиду леммы 4.3.2 все орбиты $Cl_H(x)$ замкнуты в W и, следовательно, в G. В частности, орбита $Cl_H(s)$ замкнута. □

***Упражнение* 5.3.4.** Построить элементы группы $\mathrm{GL}_n(\mathbb{F})$, класс сопряженности которых незамкнут.

Теорема 5.3.5. *Пусть U — связная замкнутая унипотентная подгруппа алгебраической группы G, и пусть $s \in G$ — полупростой элемент, нормализующий U. Положим $x^{\gamma_s} = s^{-1}x^{-1}sx$, где $x \in G$; $M = U^{\gamma_s}$, $C = C_U(s)$. Тогда:*

(а) *C — замкнутая подгруппа и M — замкнутое связное подмногообразие многообразия U;*

(б) *морфизм произведения $\tau : C \times M \to U$ биективен и, следовательно, группа C связна;*

(в) *$\gamma = \gamma_s\mid_M$ — биекция многообразия M на себя.*

Доказательство. (а) Замкнутость подгруппы C очевидна, замкнутость многообразия M следует из леммы 5.3.3. Многообразие M связно как образ связного многообразия U относительно морфизма γ_s.

(б) Разобьем рассуждение на несколько шагов, из которых первый тривиален.

1. Если $x \in U$, $y \in C$, то $(xy)^{\gamma_s} = x^{\gamma_s} = x^{\gamma_s}y^{\gamma_s}$.

2. Если $x \in Z(U)$, $y \in U$, то $(xy)^{\gamma_s} = x^{\gamma_s}y^{\gamma_s}$, откуда $(y^{-1})^{\gamma_s} = (y^{\gamma_s})^{-1}$. Действительно, запишем
$$(xy)^{\gamma_s} = s^{-1}y^{-1}x^{-1}sxy = s^{-1}x^{-1}y^{-1}syx = (s^{-1}x^{-1}s)(s^{-1}y^{-1}sy)x = (s^{-1}x^{-1}sx)(s^{-1}y^{-1}sy) = x^{\gamma_s}y^{\gamma_s}.$$

3. Если группа U абелева, то морфизм τ биективен. Так как $U = Z(U)$, то шаг 2 показывает, что $\gamma_s : U \to U$ — гомоморфизм групп. Его образ по определению совпадает с M, а ядро, очевидно, совпадает с C. Так как в этом случае M является группой, то если мы докажем, что $M \cap C = \{e\}$, отсюда будет следовать и инъективность, и сюръективность. Предположим $z \in C \cap M$, тогда, записывая $z = u^{\gamma_s}$ для некоторого $u \in U$, мы имеем $zs = u^{-1}su$. Но элементы z и s коммутируют, так что левая часть равенства есть разложение Жордана полупростого элемента $u^{-1}su$, откуда $z = e$. Следовательно, морфизм τ инъективен и сюръективен.

4. Морфизм τ всегда биективен. Докажем этот шаг индукцией по $\dim U$. Поскольку группа U нильпотентна (по теореме 1.5.8), $\dim Z(U) \geqslant 1$. В частности, $V = Z(U)^0$ — связная s-инвариантная нормальная подгруппа группы U. Если $V = U$, то τ биективен ввиду шага 3. В противном случае, $U' = U/V$ является связной унипотентной группой размерности меньшей, чем $\dim U$. Заметим, что как s, так и U принадлежат замкнутой подгруппе $N_G(V)$ группы G, в которой группа V нормальна. Если $\pi : N_G(V) \to N_G(V)/V$ — канонический гомоморфизм, то мы можем положить $s' = s^\pi$, $G' = (N_G(V))^\pi$. Тогда тройка (G', U', s') удовлетворяет исходным предположениям относительно (G, U, s), так что, по индукции, морфизм произведения $\tau' : C_{U'}(s') \times M' \to U'$ биективен. Заметим, что $M' = (U')^{\gamma_{s'}} = M^\pi$. Кроме того, ввиду шага 3 $\tau_0 : C_V(s) \times V^{\gamma_s} \to V$ — биективный морфизм.

   Теперь мы можем доказать, что морфизм τ инъективен. Пусть $z_1x = z_2y$ ($z_1, z_2 \in C$, $x, y \in M$) или, равносильно, $z \cdot x = y$ ($z = z_2^{-1}z_2 \in C$). Применим к последнему равенству морфизм π; так как $z^\pi \in C_{U'}(s')$ и $x^\pi, y^\pi \in M'$, то инъективность морфизма τ' дает $z^\pi = e$, т. е. $z \in V$. Запишем $x = u^{\gamma_s}, y = v^{\gamma_s}$, так что $(u^{-1}su)z = v^{-1}s^{-1}v$. Поскольку $z \in C$, левая часть есть разложение Жордана полупростого элемента $v^{-1}s^{-1}v$, откуда $z = e$ и $x = y$.

   Остается показать, что морфизм τ сюръективен. Заметим сначала, что $V^{\gamma_s} \leq M \cap V$ (поскольку V является s-инвариантной). Обратно, любой элемент $v \in V$ имеет вид zy, где $z \in C_V(s)$ и $y \in V^{\gamma_s}$ (поскольку морфизм τ_0 сюръективен). Кроме того, если $v \in M$, то $v = y \in V^{\gamma_s}$, так как морфизм τ_0 инъективен. Таким образом, верно равенство $V^{\gamma_s} = V \cap M$. Пусть элемент $x' = x^\pi$ для некоторого $x \in U$ перестановочен с элементом $s' = s^\pi$. Тогда $(x')^{\gamma_{s'}} = e$ или $x^{\gamma_s} \in V \cap M = V^{\gamma_s}$. В частности, существует такой $v \in V$, что $x^{\gamma_s} = v^{\gamma_s}$. Но $V \leq Z(U)$, так что из шага 2 следует, что $v^{-1}x \in C$ и $(v^{-1}x)^\pi = x^\pi$. Значит, $C_{U'}(s') = C^\pi$.

   Теперь легко показать, что морфизм τ сюръективен: $U = CMV = CVM = CC_V(s)V^{\gamma_s}M = CM$. Первое равенство в цепочке следует из того, что морфизм τ' сюръективен и $C^\pi = C_{U'}(s')$, а равенство $V^{\gamma_s}M = M$ следует из шага 2.

(в) Морфизм γ биективен. Ввиду шага 1 и сюръективность морфизма τ мы имеем $M = U^{\gamma_s} = (CM)^{\gamma_s} = M^{\gamma_s}$, так что морфизм γ сюръективен. Если $x^{\gamma_s} = y^{\gamma_s}$ при $x, y \in M$, то $xy^{-1} \in C$ и $\tau(e, x) = \tau(xy^{-1}, y)$, откуда $xy^{-1} = e$ и $x = y$, поскольку морфизм τ инъективен. □

В заключение этого параграфа мы приведем три леммы для d-групп, которые являются прямыми следствиями соответствующих результатов для полупростых элементов.

Лемма 5.3.6. *Пусть H — замкнутая подгруппа группы G, нормализуемая d-группой D. Тогда $\mathfrak{L}(C_H(D)) = \mathfrak{c}_{\mathfrak{h}}(D)$.*

Доказательство. Если $H^0 \leq C_H(D)$, то $\mathfrak{L}(H) \geq \mathfrak{L}(C_H(D)) \geq \mathfrak{L}(H^0) = \mathfrak{L}(H)$ и доказывать нечего. В противном случае воспользуемся индукцией по $\dim H$, начиная с размерности 0. Пусть $s \in D$ — такой элемент, для которого размерность группы $H' \simeq C_H(s)$ меньше, чем размерность группы H (такой элемент существует, так как в противном случае мы получаем $H^0 \leq C_H(D)$). Ясно, что $C_H(D) \leq C_H(s)$. Согласно лемме 5.3.1 мы имеем $\mathfrak{c}_{\mathfrak{h}}(s) = \mathfrak{h}'$; следовательно, $\mathfrak{c}_{\mathfrak{h}}(D) \leq \mathfrak{h}$. Используя эти факты и индукцию, получаем $\mathfrak{L}(C_H(D)) = \mathfrak{L}(C_{H'}(D)) = \mathfrak{c}_{\mathfrak{h}'}(D) = \mathfrak{c}_{\mathfrak{h}}(D) \cap \mathfrak{h}' = \mathfrak{c}_{\mathfrak{h}}(D)$. □

Лемма 5.3.7. *Пусть U — связная замкнутая унипотентная подгруппа группы G, нормализуемая d-группой D. Тогда $C_U(D)$ связна.*

Доказательство. Если группа D централизует U, то доказывать нечего. В противном случае, существует $s \in D$ такой, что $C_U(s) \lneq U$. По лемме 5.3.5 мы получаем, что $C_U(s)$ — связная подгруппа группы U. Ясно, что $C_U(D) \leq C_U(s)$. Индукция по размерности группы завершает доказательство. □

Следующее упражнение показывает, что если связная группа не является унипотентной, то централизатор полупростого элемента не обязательно связен.

***Упражнение* 5.3.8.** Есть $G = \mathrm{PGL}_2(\mathbb{C})$, $s = \mathrm{diag}(i, -i)$, где $i^2 = -1$. Показать, что $C_G(i)$ состоит из двух связных компонент.

Лемма 5.3.9. *Пусть d-группа D действует на алгебраических группах H, H' и пусть $\varphi : H \to H'$ — эпиморфизм, эквивариантный относительно этого действия группы D. Тогда φ отображает компоненту единицы группы $C_H(D)$ на компоненту единицы группы $C_{H'}(D)$.*

Доказательство. Морфизм φ можно представить в виде композиции D-эквивариантных морфизмов $H \to H/K \to H'$, где $K = \mathrm{Ker}(\varphi)$. Так как вторая стрелка — биективный морфизм, то мы можем предполагать, что $H' = H/K$. Пусть $\mathrm{Ker}(\mathrm{d}\varphi) = \mathfrak{t}$. Так как D действует на $\mathfrak{h}$ диагонально, то мы можем найти D-инвариантное подпространство $\mathfrak{n}$, дополнительное к $\mathfrak{t}$, тогда $\mathrm{d}\varphi$ отображает $\mathfrak{n}$ изоморфно на $\mathfrak{h}'$, так что неподвижные точки группы D на $\mathfrak{n}$ соответствуют неподвижным точкам группы D на $\mathfrak{h}'$. Ввиду леммы 5.3.6 мы имеем, что $\dim C_K(D) = \dim \mathfrak{c}_{\mathfrak{t}}(D)$, в то время как $\dim C_{H'}(D) = \dim \mathfrak{c}_{h'}(D) = \dim \mathfrak{c}_{\mathfrak{n}}(D)$. Комбинируя эти соотношения, получаем $\dim C_{H'}(D) = \dim \mathfrak{c}_{\mathfrak{c}}(D) - \dim \mathfrak{c}_{\mathfrak{t}}(D) = \dim C_H(D) - \dim C_K(D) = \dim(C_H(D))^{\varphi}$. Поскольку φ отображает компоненту единицы группы $C_H(D)$ в компоненту единицы группы $C_{H'}(D)$, то данная цепочка равенств означает, что φ сюръективен. □

§4 Связные разрешимые группы

В данном параграфе мы рассмотрим строение связных разрешимых групп и докажем, что максимальные торы в этих группах сопряжены. Напомним, что ввиду теоремы 5.1.6 связная замкнутая разрешимая подгруппа G группы $\mathrm{GL}_n(\mathbb{F})$ сопряжена с подгруппой группы верхнетреугольных матриц $\mathrm{T}_n(\mathbb{F})$. Для группы верхнетреугольных матриц существует точная последовательность

$$1 \to \mathrm{UT}_n(\mathbb{F}) \to \mathrm{T}_n(\mathbb{F}) \xrightarrow{\pi} \mathrm{D}_n(\mathbb{F}) \to 1.$$

Ограничение данной точной последовательности на группу G дает нам следующую точную последовательность для группы G:

$$1 \to G_u \to G \xrightarrow{\pi} T' \to 1. \tag{5.1}$$

Здесь $G_u = G \cap \mathrm{UT}_n(\mathbb{F})$ и $T = G^{\pi}$. Заметим, что группа G_u является нормальной подгруппой группы G, состоящей из всех унипотентных элементов, а группа $T = G^{\pi}$ является связной подгруппой группы $\mathrm{D}_n(\mathbb{F})$ и потому является тором. Поскольку фактор группа G/G_u абелева, мы получаем, что группа G_u содержит коммутант группы G.

Лемма 5.4.1. *Подгруппа G_u группы G, определенная выше, является связной.*

Доказательство. Предположим сначала, что группа G абелева. Поскольку произведение двух перестановочных полупростых элементов вновь является полупростым элементом (в силу перестановочности они лежат в $\mathrm{D}_n(\mathbb{F})$ с точностью до сопряжения в $\mathrm{GL}_n(\mathbb{F})$), мы получаем, что множество полупростых элементов G_s группы G также является замкнутой нормальной подгруппой группы G. Тогда $G_u \simeq G/G_s$ связна как гомоморфный образ связной группы.

Пусть $\varphi : G \to G/[G,G] = H$ — канонический гомоморфизм (который является морфизмом алгебраических групп). Так как группа H абелева, то, как мы заметили выше, $H = H_s \times H_u$ является прямым произведением своей полупростой и унипотентной частей. Очевидно, что $G_u \leq H_u^{\varphi^{-1}}$. Обратно, поскольку $[G,G] \leq G_u$ и $G_u^{\varphi} = H_u$, мы получаем, что $H_u^{\varphi^{-1}} \leq G_u$. Следовательно, $G_u = H_u^{\varphi^{-1}}$. Далее, по лемме 5.1.2, коммутант $[G,G]$ связен. Следовательно, в G_u нет нормальных подгрупп конечного индекса, т. е. группа G_u связна. □

Далее мы докажем, что группа G содержит тор T, размерность которого совпадает с размерностью тора T'. Поскольку $T \cap G_u = \{e\}$, отсюда сразу будет следовать, что последовательность (5.1) для группы G расщепляема.

Лемма 5.4.2. *Пусть G — связная разрешимая алгебраическая группа. Тогда группа G нильпотентна в том и только в том случае, когда множество её полупростых элементов G_s является подгруппой. Если G_s является подгруппой, то она замкнута, связна и $G = G_s \times G_u$.*

Доказательство. Пусть G_s — подгруппа группы G. Тогда $G_s^{\pi} = T'$ и $G_s \cap \mathrm{Ker}(\pi) = \{e\}$. Следовательно, $G_s \simeq T'$ и потому последовательность (5.1) расщепляема, т. е. $G = G_s \leftthreetimes G_u$. С другой стороны, G_s нормальна в G, поэтому $G = G_s \times G_u$. Поскольку группа $\mathrm{UT}_n(\mathbb{F})$ нильпотентна (теорема 1.5.8) и группа G_s абелева, мы получаем, что G_u и G также нильпотентные группы.

Обратно, предположим, что группа G нильпотентна. Требуется доказать, что G_s — подгруппа. Для этого, очевидно, достаточно показать, что любая пара полупростых элементов $x, y \in G$ коммутирует. Мы имеем $x^{-1}y^{-1}xy = z \in [G,G] \leq G_u$, т. е. $x^{-1}y^{-1}x = zy^{-1}$. Поскольку G_u связная группа, по лемме 5.3.5 мы имеем, что для $M = G_u^{\gamma_y}$ морфизм $\gamma_y : M \to M$ биективен. Следовательно, $M \leq G^{\infty} = \{e\}$ в силу нильпотентности группы G (здесь G^n — $n^{\text{ый}}$ член нижнего центрального ряда и $G^{\infty} = \cap_{n=1}^{\infty} G^n$). Таким образом, zy^{-1} есть разложение Жордана полупростого элемента $x^{-1}y^{-1}x$, откуда $z = e$. □

Теорема 5.4.3. *Пусть G — связная разрешимая алгебраическая группа. Тогда:*

(а) *G_u — замкнутая связная нормальная подгруппа группы G, содержащая коммутант $[G,G]$, и обладающая рядом связных замкнутых подгрупп, каждая из которых нормальна в G и имеет коразмерность 1 в предыдущей;*

(б) *максимальные торы группы G сопряжены относительно G^{∞} и, если T — один из этих торов, то $G = T \leftthreetimes U$.*

Доказательство. Утверждение (а) следует из леммы 5.4.1 и замечаний перед ней. Таким образом, нам достаточно доказать лишь (б). Для этого воспользуемся индукцией по $\dim G$ (начиная с размерности 0, когда G тривиальна). Прежде всего нам следует найти тор в группе G, который проектируется на T' в точной последовательности (5.1), откуда будет следовать, что $G = T \leftthreetimes G_u$. Если группа G нильпотентна, то существование такого тора следует из леммы 5.4.2. Если G ненильпотентна, то по лемме 5.4.2 мы можем найти нецентральный полупростой элемент $s \in G$. Тогда размерность группы $H = C_G(s)^0$ будет меньше размерности группы G. Если D — замыкание в G подгруппы, порождённой элементом s, то морфизм $\pi : G \to G/G_u = T'$ эквивариантен относительно D, и действие группы D^{π} на T' тривиально, поскольку группа T' коммутативна. Применяя лемму 5.3.9 мы получаем, что $H^{\pi} = T'$. Это показывает, что коразмерность группы H_u в H равна $\dim T'$. По предположению индукции группа H содержит тор размерности $\dim T'$, который, очевидно, будет максимальным тором группы G.

Зафиксируем некоторый максимальный тор T группы G. Прежде чем доказывать, что все остальные максимальные торы сопряжены с T относительно G^{∞}, мы покажем, что любой полупростой элемент $s \in G$ сопряжён относительно G^{∞} с некоторым элементом из T. Если группа G нильпотентна, то по лемме 5.4.2 имеем $T = G_s$ и доказывать нечего. Если группа G ненильпотентна, то группа $G^{\infty} \leq G_u$ нетривиальна, а также связна и унипотентна (и, в частности, нильпотентна). Поэтому $N = Z(G^{\infty})^0$ — нетривиальная нормальная подгруппа группы G. При каноническом отображении $\varphi : G \to G/N = G'$ группа G^{∞} отображается

на $(G')^\infty$. Запишем $G' = S \leftthreetimes G'_u$, $s = T^\varphi$. По индукции, $(x^{-1})^\varphi s^\varphi x^\varphi \in S$ для некоторого элемента $x^\varphi \in (G')^\infty$ (т. е. $x \in G^\infty$). Это означает, что элемент s относительно G^∞ сопряжён с $x^{-1}sx \in TN$. Поэтому, изменяя, если необходимо, обозначения, достаточно доказать, что любой полупростой элемент $s \in TN$ сопряжен при помощи некоторого элемента из N с элементом группы T. Запишем $s = tn$ ($t \in T$, $n \in N$) и применим теорему 5.3.5(б) к действию элемента t^{-1} на N. Мы имеем $n = u^{\gamma_t}z$ для некоторого $z \in C_N(t)$ и $u \in N$, откуда $s = u^{-1}tuz$. Поскольку группа N абелева и $z \in C_N(t)$, мы получаем, что $usu^{-1} = tz$ и tz является разложением Жордана полупростого элемента usu^{-1}. Следовательно, $z = e$ и $usu^{-1} = t$.

Наконец, пусть S — произвольный максимальный тор группы G. Так как $S \not\leq Z(G)$, существует элемент $s \in S \setminus Z(G)$. Ввиду предыдущего абзаца мы можем считать, что $s \in T$. Но тогда $T, S \leq C_G(s)^0$. Индукция по размерности группы G завершает доказательство. □

Следствие 5.4.4. *Пусть G — связная разрешимая группа. Тогда каждый полупростой элемент группы G лежит в некотором максимальном торе, а каждый унипотентный элемент лежит в максимальной связной унипотентной подгруппе.*

Доказательство. Это прямое следствие доказательства теоремы 5.4.3. □

Следствие 5.4.5. *Пусть G — связная разрешимая алгебраическая группа и S — некоторый её тор. Тогда $N_G(S) = C_G(S)$.*

Доказательство. Пусть T — максимальный тор группы G, содержащий S. Тогда $G = T \leftthreetimes U$. Далее $N_G(S) = \langle T, N_U(S)\rangle$, поэтому достаточно доказать, что $N_U(S) = C_U(S)$. Но $N_U(S) = U \cap N_G(S)$ — нормальная подгруппа группы $N_G(S)$ и $S \cap N_U(S) = \{e\}$. Поскольку S также нормальна в $N_G(S)$, мы получаем, что $S \leftthreetimes U = S \times U$, т. е. $N_G(S) = C_G(S)$. □

Теорема 5.4.6. *Пусть G — связная алгебраическая группа. Тогда все максимальные торы и все максимальные связные унипотентные подгруппы группы G сопряжены.*

Доказательство. Очевидно, любой максимальный тор и любая связная унипотентая подгруппа лежат в некоторой подгруппе Бореля B группы G. Ввиду сопряженности подгрупп Бореля (см. теорему 5.1.8), все утверждения теоремы теперь следуют из теоремы 5.4.3 и следствия 5.4.4. □

Назовём общую размерность максимальных торов группы G *рангом* группы G (обозначается $\mathrm{rank}(G)$). Пусть T — некоторый максимальный тор связной алгебраической группы G. Группа $C_G(T)^0$ называется *подгруппой Картана* алгебраической группы G.

Подгруппа P связной алгебраической группы G называется *параболической*, если фактор многообразие G/P проективно.

Лемма 5.4.7. *Замкнутая подгруппа связной алгебраической группы G является параболической тогда и только тогда, когда она содержит подгруппу Бореля. В частности, связная подгруппа H группы G является подгруппой Бореля тогда и только тогда, когда H разрешима и многообразие G/H полно.*

Доказательство. Действительно, пусть P — замкнутая подгруппа связной алгебраической группы G, для которой многообразие G/P проективно и пусть B — некоторая подгруппа Бореля группы G. Тогда B действует на G/P сдвигами и по теореме о неподвижной точке 5.1.5 имеет на G/P неподвижную точку. Отсюда следует, что B сопряжена с подгруппой группы P и что $\dim G/P \leqslant \dim G/B$.

Обратно, пусть замкнутая подгруппа P группы G содержит подгруппу Бореля B. Тогда естественный морфизм $G/B \to G/P$ является сюръективным морфизмом полного многообразия G/B и потому по лемме 3.6.2(2) многообразие G/P полно. □

***Упражнение* 5.4.8.** Описать параболические подгруппы в $\mathrm{GL}_n(\mathbb{F})$.

Лемма 5.4.9. *Пусть $\varphi : G \to H$ — морфизм алгебраических групп и G связна. Пусть B — подгруппа Бореля (соответственно, подгруппа Картана, максимальный тор, максимальная связная унипотентная подгруппа, параболическая подгруппа) группы G. Тогда B^φ — подгруппа Бореля (соответственно, подгруппа Картана, максимальный тор, максимальная связная унипотентная подгруппа, параболическая подгруппа) группы G^φ.*

Доказательство. Ввиду теоремы 5.4.6 и леммы 5.4.7 достаточно доказать лемму лишь для подгрупп Бореля. Так как группа G связна, её образ G^φ также связен. Кроме того, группа B^φ связна и разрешима. Далее, φ индуцирует сюръективный морфизм $G/B \to G^\varphi/B^\varphi$. Так как многообразие G/B полно, то, вновь по лемме 3.6.2(2), многообразие G^φ/B^φ полно. Ввиду леммы 5.4.7, подгруппа B^φ является подгруппой Бореля группы G^φ. $\square$

Лемма 5.4.10. *Пусть σ — некоторый автоморфизм связной алгебраической группы G, централизующий некоторую подгруппу Бореля B. Тогда автоморфизм σ должен быть тождественным.*

Доказательство. Рассмотрим морфизм $\varphi : G \to G$, действующий по правилу $\varphi : x \mapsto x^\sigma x^{-1}$. Тогда $B^\varphi = \{e\}$, следовательно, φ является морфизмом из G в G/B. Ввиду леммы 4.1.7(б) образ G^φ замкнут в G/B, следовательно, является полным многообразием по лемме 3.6.2(1). С другой стороны, G^φ является алгебраической группой, поэтому многообразие G^φ аффинно. Следовательно, по лемме 3.6.2(5), имеем $G^\varphi = \{e\}$. $\square$

Следствие 5.4.11. $Z(G)^0 \le Z(B) \le C_G(B) = Z(G)$.

Доказательство. Группа $Z(G)^0$ связна и разрешима, поэтому лежит в некоторой борелевской подгруппе B группы G. Отсюда следует, что $Z(G)^0 \le Z(B)$. Кроме того, очевидно, $Z(G) \le C_G(B)$. Обратно, если $x \in C_G(B)$, то автоморфизм $\mathrm{Int}x$ действует тривиально на группе B. По лемме 5.4.9 получаем, что $\mathrm{Int}x$ действует тривиально на группе G, следовательно, $x \in Z(G)$. $\square$

Лемма 5.4.12. (а) *Если подгруппа Бореля B связной алгебраической группы G нильпотентна, то $G = B$.*

(б) *Связная алгебраическая группа G нильпотентна тогда и только тогда, когда G имеет в точности один максимальный тор.*

Доказательство. (а) Если B нильпотентна, то её центр $Z(B)$ имеет положительную размерность. Ввиду следствия 5.4.11 мы получаем, что $Z(G)$ имеет положительную размерность и мы можем рассмотреть группу $G/Z(G)$. Индукция по размерности группы завершает доказательство утверждения (а).

(б) Если G нильпотентна, то $G = B$ и в G существует единственный максимальный тор ввиду леммы 5.4.2. Обратно, если в группе G существует единственный максимальный тор T, то T является нормальной подгруппой группы G и содержится в некоторой борелевской подгруппе B. Ввиду теоремы 5.4.3 мы получаем, что $T \le Z(B) \le Z(G)$, т. е. группа B нильпотентна. Ввиду утверждения (а) отсюда следует нильпотентность группы G. $\square$

Следствие 5.4.13. *Пусть T — максимальный тор связной алгебраической группы G и $C = C_G(T)^0$ — подгруппа Картана группы G. Тогда группа C нильпотентна.*

§5 Нормализатор подгруппы Бореля

Везде в данном параграфе под G понимается связная алгебраическая группа. В данном параграфе мы докажем, что любой элемент связной алгебраической группы содержится в некоторой подгруппе Бореля и что централизатор любого тора связен. Используя эти результаты, мы рассмотрим подгруппы Бореля в централизаторах торов и затем докажем, что подгруппа Бореля совпадает со своим нормализатором. Сначала мы докажем следующую лемму.

Лемма 5.5.1. *Пусть H — замкнутая связная подгруппа связной алгебраической группы G, и пусть $X = \bigcup_{x \in G} H^x$. Тогда*

(а) *если многообразие G/H полно, то множество X замкнуто;*

(б) *если некоторый элемент группы H оставляет неподвижными лишь конечное число точек многообразия G/H, то X содержит открытое подмножество группы G (в частности, множество X плотно).*

Доказательство. Рассмотрим вспомогательные морфизмы

$$G \times G \xrightarrow{\varphi} G \times G \xrightarrow{\psi} (G/H) \times G$$

и проекции $(G/H) \times G \xrightarrow{\pi_1} G/H$, $(G/H) \times G \xrightarrow{\pi_2} G$. Здесь $(x, y)\varphi = (x, y^x)$, так что, очевидно, φ — морфизм многообразий, а $(x, y)\psi = (xH, y)$. Пусть $M = (G \times H)(\varphi \circ \psi)$; тогда $X = M^{\pi_2}$.

Для доказательства (а) достаточно доказать, что множество M замкнуто (поскольку многообразие G/H полно). Поскольку ψ можно рассматривать как канонический морфизм $(G\times G)/(H\times\{e\})$, мы получаем, что ψ переводит открытые множества в открытые (НАПИСАТЬ ПОЗДНЕЕ, см. [17, 12.2]). Но $(G\times H)\varphi \subseteq (M)\psi^{-1}$ и множество $(G\times H)\varphi$ замкнуто. Поэтому нам достаточно доказать равенство.

ДОКАЗАТЕЛЬСТВО НАПИСАТЬ ПОЗДНЕЕ. ПОСЛЕ ДОБАВЛЕНИЯ ТЕОРЕМ О ДОМИНАНТНЫХ МОРФИЗМАХ И СЛОЯХ. □

Пусть G_s — множество полупростых элементов группы G и G_u — множество унипотентных элементов группы G. Тогда верна следующая

Теорема 5.5.2. *Пусть B — подгруппа Бореля связной алгебраической группы G, T — максимальный тор группы G, U — максимальная связная унипотентная подгруппа группы B и $C = C_G(T)^0$ — подгруппа Картана группы G. Тогда объединение всех подгрупп, сопряжённых с B (соответственно с T и с U) совпадает с G (соответственно с G_s и G_u). Кроме того, объединение всех подгрупп, сопряжённых с C, содержит открытое (и потому плотное) подмножество группы G.*

Доказательство. По лемме 5.2.13 существует такой элемент $t\in T$, что $C = C_G(t)^0$. Кроме того, по следствию 5.4.13 мы имеем, что C нильпотентна, следовательно, $C = C_s\times C_u$. Мы утверждаем, что $H = C$ и t удовлетворяют условиям леммы 5.5.1(б). Действительно, t оставляет неподвижной точку $xC\in G/C$ тогда и только тогда, когда $t^x\in C$. Далее, $t^x\in C_s = T$, так что $T\le C_G(t^x)^0 = x^{-1}C_G(t)^0x = C^x$ или $T^x\le T$. Отсюда следует, что $T^x = T$, $C^x = C$, но ввиду жёсткости d-групп (лемма 5.2.12) выполняется $C = N_G(C)^0$, так что для xC есть лишь конечное число возможностей. Таким образом, мы получаем, утверждение теоремы для группы C.

Далее, группа C содержится в некоторой подгруппе Бореля, можно считать, что $C\le B$, откуда следует, что объединение всех подгрупп Бореля плотно в G. Ввиду леммы 5.5.1(а) мы получаем, что это объединение также замкнуто в G, откуда мы получаем, что оно совпадает с G. Остальные утверждения теоремы немедленно следуют из следствия 5.4.4. □

***Упражнение* 5.5.3.** Доказать, что $Z(B) = Z(G)$.

Следующая теорема играет важную роль в различных индуктивных построениях, связанных с торами.

Теорема 5.5.4. *Пусть S — тор связной алгебраической группы G. Тогда группа $C_G(S)$ связна.*

Доказательство. Если группа G разрешима, то $C_G(S) = \langle T, C_{G_u}(S)\rangle$, где T пробегает все максимальные торы группы G, содержащие S. По лемме 5.3.7 группа $C_{G_u}(S)$ связна, поэтому группа $C_G(S)$ также связна (см. теорему 4.1.8).

Пусть теперь $x\in C_G(S)$ и группа G произвольна. Пусть B — подгруппа Бореля группы G, содержащая S и пусть X — множество неподвижных относительно x точек в G/B. Это множество замкнуто (множество неподвижных точек всегда замкнуто) и непусто (по теореме 5.5.2). Следовательно, X полно как замкнутое подмножество полного многообразия (лемма 3.6.2). Так как S коммутирует с x, то S оставляет множество X инвариантным. По теореме 5.1.5 S имеет на X неподвижную точку sB, поэтому x, S лежат в подгруппе Бореля $B^{s^{-1}}$. Следовательно $x\in C_{B^{s^{-1}}}(S)$ и $C_G(S)$ порождается связными подгруппами, а потому связен. □

Следствие 5.5.5. *Подгруппа Картана связной алгебраической группы G есть в точности централизатор максимального тора.*

***Упражнение* 5.5.6.** Пусть x — произвольный элемент из связной алгебраической группы G и $x_s\cdot x_u$ — его разложение Жордана. Доказать, что $x\in C_G(x_s)^0$. Верно ли, что $x\in C_G(x_u)^0$?

Далее мы покажем, что если B — некоторая подгруппа Бореля, содержащая некоторый тор S группы G, то $B\cap C_G(S)$ является подгруппой Бореля группы $C_G(S)$ и любая подгруппа Бореля группы $C_G(S)$ может быть получена таким образом. Заметим, что если мы рассмотрим произвольную связную подгруппу H группы G, то пересечение $B\cap H$ может не быть даже связным.

Теорема 5.5.7. *Пусть S — некоторый тор в связной алгебраической группе G и $C = C_G(S)$. Пусть B — подгруппа Бореля группы G, содержащая S, X — множество неподвижных точек в G/B относительно S и Y — неприводимая компонента множества X. Тогда группа C действует на Y транзитивно.*

Доказательство. Ввиду леммы 4.3.1(б), множество X замкнуто в G/B, поэтому X проективно как замкнутое подмножество проективного многообразия. Ясно, что X инвариантно относительно C. Поскольку группа C связна (см. теорему 5.5.4), то ввиду леммы 4.3.1(г), она оставляет неподвижной каждую неприводимую компоненту множества X. Заметим также, что все эти компоненты полны, как замкнутые подмножества полного многообразия X. Не теряя общности можно считать, что B стабилизирует некоторый элемент $y \in Y$. Для доказательства теоремы достаточно доказать, что $C \cdot y = Y$. Мы докажем равносильное утверждение, что если Z — прообраз множества Y при каноническом отображении $G \to G/B$, то $CB = Z$.

Заметим, что многообразие Z неприводимо, так как Y неприводимо и слои канонического отображения $G \to G/B$ неприводимы. Кроме того, $S^z \leq B$ при $z \in Z$ по построению. Поэтому морфизм $Z \times S \to B$, определяемый соотношением $(z,s) \mapsto s^z$ имеет смысл. Пустьφ — композиция этого морфизма и канонического отображения $B \to B/B_u$. При фиксированном $z \in Z$ полученный морфизм $S \to B/B_u$ является гомоморфизмом торов. Ввиду связности группы Z и из жёсткости торов (лемма 5.2.12) следует, что это отображение не зависит от z. Но $e \in Z$, так что мы имеем $s^z \equiv s(\mod B_u)$ для всех $z \in Z$, $s \in S$. В частности, S^z содержится в связной разрешимой группе SB_u, в которой группы S и S^z являются максимальными торами. Ввиду теоремы 5.4.3, существует элемент $u \in B_u$ такой, что $S^{zu} = S$, т. е. $zu \in N = N_G(S)$. Следовательно, $CB \subseteq Z \subseteq NB$. С другой стороны, индекс $|N : C|$ конечен (вновь лемма 5.2.12), поэтому $\dim CB = \dim Z = \dim NB$. Наконец, $CB = Z$, ввиду связности многообразия Z. □

Следствие 5.5.8. *$C_B(S) = C \cap B$ — подгруппа Бореля группы $C = C_G(S)$ и любая подгруппа Бореля группы C может быть получена таким же образом.*

Доказательство. Пусть множества X и Y выбраны также, как в теореме 5.5.7 и B — стабилизатор точки $y \in Y$. Многообразие Y полно и, в соответствии с теоремой 5.5.7, является орбитой точки y относительно C. Стабилизатор точки y в C есть $C \cap B = C_B(S)$. Следовательно, многообразие $C/(C \cap B) = Y$ полно. По лемме 5.4.7, группа $C \cap B$ является подгруппой Бореля группы C. □

***Упражнение* 5.5.9.** Пусть G — связная алгебраическая группа и B — её подгруппа Бореля. Доказать, что $N_G(B_u)^0 = B$. В частности, $N_G(B) = B^0$.

Теорема 5.5.10. *Пусть B — подгруппа Бореля связной алгебраической группы G. Тогда $N = N_G(B) = B$.*

Доказательство. Ввиду упражнения 5.5.9 мы имеем, что $B = N^0$. Для доказательства того, что $N = B$ воспользуемся индукцией по $\dim G$. Ясно, что *радикал* $R(G)$ группы G (максимальная связная нормальная разрешимая подгруппа) содержится в B. Таким образом, можно считать, что $R(G)$ тривиален, т. е. что группа G *полупроста*.

Пусть $x \in N$ и пусть T — произвольный максимальный тор группы G, содержащийся в B. Тогда T^x — тоже тор, содержащийся в B; поэтому существует элемент $y \in B$ такой, что $T^{xy} = T$ (теорема 5.4.3). Очевидно, элемент x принадлежит группе B тогда и только тогда, когда $xy \in B$, так что мы можем предполагать, что $x \in N_G(T)$. Пусть $S = C_T(x)^0$ — подтор тора T. Возможны следующие два случая.

Случай 1. $S \neq e$. Тогда группа $C = C_G(S)$ обладает нетривиальным радикалом и, таким образом, C — собственная связная подгруппа группы G (см. теорему 5.5.4). Согласно следствию 5.5.8, $B' = B \cap C$ — подгруппа Бореля группы C. По предположению индукции, $B' = N_C(B')$. Но $x \in N_C(B) \leq N_C(B') = B' \leq B$.

Случай 2. $S = e$. Так как $x \in N_G(T)$ и T — коммутативная группа, то коммутаторный морфизм $\gamma_x : T \to T$ является гомоморфизмом групп с ядром $C_T(x)$. Ввиду условия $S = e$ это ядро конечно, так что морфизм γ_x является сюръективным (см. лемму 4.1.7). Следовательно, тор T содержится в группе $[M, M]$, где $M = \langle x, B \rangle \leq N$. По теореме Шевалле 4.8.2, существует такое рациональное представление $\rho : G \to \mathrm{GL}(V)$, что V содержит прямую D, стабилизатор которой в G совпадает с M. Пусть $\chi : M \to \mathbb{F}^*$ — соответствующий характер (если $g \in M$ и $v \in D$, то $v^g = \lambda_g v$ и $g^\chi = \lambda_g$ является характером группы M). Тогда χ тривиален на $[M, M]$, а также на B_u, поэтому χ тривиален на B. Если $0 \neq v \in D$, то представление ρ индуцирует морфизм $G/B \to Y$, где Y — орбита вектора v относительно G^ρ. Так как G/B — полное многообразие, то его образ Y замкнут в V (лемма 3.6.2) и, следовательно, является аффинным многообразием. С другой стороны, Y — полное многообразие (ввиду той же леммы 3.6.2). Кроме того, многообразие Y связно, как образ связного многообразия. Следовательно, многообразие Y — точка и $G = M$. Так как группа G связна и $|M : B|$ конечен, мы получаем, что $G = B$. □

Ниже мы сформулируем ряд следствий, доказательство которых мы оставим в качестве упражнения.

Следствие 5.5.11. *Подгруппа Бореля B является максимальной разрешимой подгруппой связной алгебраической группы G.*

***Упражнение* 5.5.12.** Пусть S — максимальная разрешимая подгруппа группы G, причём S не является подгруппой Бореля. Доказать, что группа S замкнута, несвязна и имеет меньшую размерность, чем любая подгруппа Бореля группы G.

Следствие 5.5.13. *Пусть P — параболическая подгруппа группы G. Тогда $P = N_G(P)$. В частности, группа P связна.*

Следствие 5.5.14. *Пусть P, Q — параболические подгруппы группы G, содержащие подгруппу Бореля B. Если группы P, Q сопряжены в G, то $P = Q$.*

Следствие 5.5.15. *Пусть B — подгруппа Бореля группы G. Тогда $B = N_G(B_u)$.*

§6 Группы Вейля и действие торов на G/B

По прежнему предполагается, что G — связная алгебраическая группа и B — некоторая её фиксированная подгруппа Бореля. Ввиду теоремы 5.5.10 совокупность $\mathfrak{B}$ борелевских подгрупп группы G можно отождествить с многообразием G/B. Действие группы G на $\mathfrak{B}$, индуцированное сопряжением, соответствует правому умножению на G/B. Если теперь S — произвольный тор группы G, то множество неподвижных относительно S точек в $\mathfrak{B}$, обозначаемое $\mathfrak{B}^S$ совпадает борелевским подгруппам, содержащим S. Если множество $\mathfrak{B}^S$ конечно, то тор S называется *регулярным.* В противном случае тор S называется *сингулярным.*

Пусть S — произвольный тор группы G. В силу жёсткости торов (лемма 5.2.12) группа $N_G(S)/C_G(S)$ конечна; она называется *группой Вейля группы G относительно S* и обозначается через $W(G, S)$. Так как все максимальные торы сопряжены, то их группы Вейля изоморфны. Поэтому группа Вейля максимального тора называется просто *группой Вейля группы G* и обозначается $W(G)$.

Лемма 5.6.1. *Пусть T — максимальный тор группы G и $C = C_G(T)$. Тогда C содержится в каждой борелевской подгруппе, содержащей T.*

Доказательство. Так как C связна (теорема 5.5.4) и нильпотентна (следствие 5.4.13), то она содержится по меньшей мере в одной подгруппе Бореля B. Если $B_1 = B^x \in \mathfrak{B}^T$, то T, T^x — максимальные торы группы B_1 и, следовательно, сопряжены посредством некоторого элемента $y \in B_1$. Поэтому $C^{xy} = C \leq B_1$. □

Таким образом, группа C действует тривиально на $\mathfrak{B}^T$. С другой стороны, очевидно, что $N = N_G(T)$ переставляет элементы множества $\mathfrak{B}^T$, в результате чего мы получаем действие $W(G) = N_G(T)/C_G(T)$ на $\mathfrak{B}^T$.

Лемма 5.6.2. *Пусть T — максимальный тор группы G и $W = W(G, T)$. Тогда W действует транзитивно и регулярно на множестве $\mathfrak{B}^T$. В частности, $|\mathfrak{B}^T| = |W|$ — конечное число, т. е. тор T регулярен.*

Доказательство. Пусть $B_1, B_2 \in \mathfrak{B}^T$. По теореме 5.1.8 существует $x \in G$ такой, что $B_1^x = B_2$. Тогда T, T^x — два максимальных тора группы B_1, следовательно, существует $y \in B_1$, для которого $T^{yx} = T$. Значит, $B_1^{yx} = B_2$ и $yx \in N_G(T)$, что доказывает транзитивность действия группы W. Пусть теперь $x \in N_G(T)$ и предположим, что для некоторой $B \in \mathfrak{B}^T$ выполнено $B^x = B$. Тогда $x \in N_B(T)$ и ввиду следствия 5.4.5 $N_B(T) = C_B(T)$. Следовательно, $x \in C_G(T)$, т. е. стабилизатор любой точки в $\mathfrak{B}^T$ относительно действия группы W тривиален. □

Лемма 5.6.3. *Пусть $\varphi : G \to G'$ — эпиморфизм алгебраических групп и $T, T' = T^\varphi$ — соответствующие максимальные торы. Тогда φ индуцирует сюръективные отображения $\mathfrak{B}^T \to {\mathfrak{B}'}^{T'}$ и $W = W(G, T) \to W(G', T') = W'$, которые оказываются и инъективными, если $\mathrm{Ker}(\varphi)$ содержится в каждой борелевской подгруппе группы G.*

Доказательство. Если B — борелевская подгруппа группы G, содержащая тор T, то $B' = B^\varphi$ — борелевская подгруппа группы G', содержащая тор T' (лемма 5.4.9); поэтому отображение $\mathfrak{B}^T \to {\mathfrak{B}'}^{T'}$ корректно определено. Ввиду леммы 5.3.9 и теоремы 5.5.4 справедливо $(C_G(T))^\varphi = C_{G'}(T')$, кроме того, очевидно, что $(N_G(T))^\varphi \leq N_{G'}(T')$, поэтому отображение $W(G, T) \to W(G', T')$ определено.

По лемме 5.3.9, эпиморфизм φ индуцирует сюръективныое отображение $\mathfrak{B} \to \mathfrak{B}'$. Если $B' \in {\mathfrak{B}'}^{T'}$, то каждая борелевская подгруппа группы $H = (B'^{\varphi})^0$ есть борелевская подгруппа группы G, которую φ отображает на B'. Кроме того, T — максимальный тор группы H и, следовательно, лежит в одной из этих подгрупп. Это

показывает, что отображение $\mathfrak{B}^T \to \mathfrak{B}'^{T'}$ сюръективно. Очевидно, что если $\mathrm{Ker}(\varphi)$ содержится в каждой борелевской подгруппе, то тогда $(B'^{\varphi})^0$ является борелевской подгруппой группы G, и отображение $\mathfrak{B}^T \to \mathfrak{B}'^{T'}$ инъективно.

Переходя к группам Вейля мы воспользуемся их регулярностью (лемма 5.6.3). Выберем $B \in \mathfrak{B}^T$ и положим $B^{\varphi} = B'$. Поскольку отображения $W \to \mathfrak{B}^T$ и $W' \to \mathfrak{B}'^{T'}$ биективны, а отображение $\mathfrak{B}^T \to \mathfrak{B}'^{T'}$ сюръективно, мы получаем, что отображение $W \to W'$ также сюръективно. Его инъективность в случае, когда $\mathrm{Ker}(\varphi)$ содержится во всех подгруппах Бореля, также следует из инъективности отображения $\mathfrak{B}^T \to \mathfrak{B}'^{T'}$. □

Ранее мы доказали, что максимальные торы являются регулярными. Следующая лемма даёт нам критерий для проверки регулярности торов.

Лемма 5.6.4. *Пусть S — тор в группе G и $C = C_G(S)$. Тогда тор S регулярен в том и только в том случае, если группа C разрешима. В этом случае группа C содержится в каждой борелевской подгруппе группы G, содержащей S, и для каждого максимального тора T, содержащего S мы имеем $\mathfrak{B}^T = \mathfrak{B}^S$.*

Доказательство. Как и в доказательстве леммы 5.6.2, отождествим $\mathfrak{B}^S$ с замкнутым подмножеством X некоторого многообразия G/B, где $B \geq S$. Размерности всех неприводимых компонент Y многообразия X равны коразмерности в C борелевской подгруппы группы C (вновь смотри доказательство леммы 5.6.2). Поэтому тор S регулярен (т. е. множество $\mathfrak{B}^S$ конечно) в том и только в том случае, когда группа C есть борелевская в себе самой (т. е. группа C разрешима). Это рассуждение показывает также, что для регулярного тора S группа C содержится в каждой борелевской подгруппе группы G, содержащей тор S. В частности, так как любой максимальный тор T, содержащий S, принадлежит C, то $\mathfrak{B}^T = \mathfrak{B}^S$. □

Ввиду леммы 5.6.4, тор S группы G является сингулярным тогда и только тогда, когда группа $C_G(S)$ неразрешима. Некоторые наибольшие торы с неразрешимым централизатором возникают следующим образом. Напомним, что если T — максимальный тор группы G, то корни группы G относительно тора T есть нетривиальные веса T^{Ad} в алгебре $\mathfrak{g} = \mathfrak{c}_{\mathfrak{g}}(T) \oplus \bigoplus_{\alpha\in\Phi} \mathfrak{g}_\alpha$, где $\mathfrak{g}_\alpha = \{\mathsf{x} \in \mathfrak{g} | \mathsf{x}^{\mathrm{Ad}\ t} = x^{t^\alpha}, t \in T, \alpha \in X(T)\}$. Так как группа T^{Ad} диагонализируема, то для любой замкнутой подгруппы H группы G, нормализуемой тором T, существует дополнение к $\mathfrak{h} = \mathfrak{L}(H)$ в алгебре $\mathfrak{g}$, инвариантное относительно T^{Ad} . В частности, пусть $H = \mathfrak{I}(T)$ — компонента единицы пересечения всех борелевских подгрупп группы G, содержащих тор T. Запишем $\mathfrak{g} = \mathfrak{L}(\mathfrak{I}(T)) \oplus \bigoplus_{\alpha\in\Psi} \mathfrak{g}'_\alpha$. В силу следствия 5.5.8 справедливо $C_G(T) \leq \mathfrak{I}(T)$, так что $\Psi \subseteq \Phi$. Ясно также, что Ψ не зависит от выбора дополнения. Определим $T_\alpha = \mathrm{Ker}(\alpha)^0 \leq T$ для всех $\alpha \in \Psi$. Следующая лемма показывает, что тор T_α сингулярен и даёт критерий сингулярности торов.

Лемма 5.6.5. *Пусть S — тор группы G и T — некоторый максимальный тор, содержащий S. Тор S сингулярен тогда и только тогда, когда $S \leq T_\alpha$ для некоторого корня $\alpha \in \Psi$.*

Доказательство. Пусть S — сингулярный тор. Тогда группа $C = C_G(S)$ неразрешима, в частности, группа C имеет бо́льшую размерность, чем разрешимая группа $C \cap H$. Следовательно, пространство неподвижных точек тора S в алгебре $\mathfrak{g}$ не содержится целиком в $\mathfrak{L}(\mathfrak{I}(T))$. Значит, тор S оставляет неподвижной подалгебру $\mathfrak{g}'_\alpha$ для некоторого корня $\alpha \in \Psi$ и $S \leq T_\alpha$.

Обратно, пусть $S \leq T_\alpha$ для некоторого корня $\alpha \in \Psi$. Если тор S несингулярен, то группа C должна быть разрешимой и содержаться в каждой борелевской подгруппе группы G, содержащей S, в частности, $C \leq \mathfrak{I}(T)$. По лемме 5.3.6 мы получаем, что все неподвижные точки тора S в $\mathfrak{g}$ должны принадлежать $\mathfrak{L}(\mathcal{I}(T))$, что противоречит определению T_α. □

Максимальная связная нормальная (унипотентная) подгруппа $R(G)$ $(R_u(G))$ алгебраической группы G называется *(унипотентным) радикалом.* Группа G называется *редуктивной*, если её унипотентный радикал тривиален.

Следствие 5.6.6. *Пусть $\alpha \in \Psi$ и положим $Z_\alpha = C_G(T_\alpha)$. Тогда $G_\alpha = Z_\alpha/R(Z_\alpha)$ — полупростая группа ранга* 1.

Доказательство. Так как тор T_α сингулярен, то связная группа Z_α неразрешима. Следовательно, группа G_α полупроста. Действительно прообраз $R(G_\alpha)$ в Z_α является нормальной связной разрешимой группой, т. е. содержится в $R(Z_\alpha)$. Кроме того, $T_\alpha \leq Z(Z_\alpha)^0 \leq R(Z_\alpha)$, так что ранг группы G_α равен 1. □

***Упражнение* 5.6.7.** Пусть T — максимальный тор группы G и S — подтор тора T. Тогда S регулярен в том и только в том случае, когда $C_G(S) \leq \mathcal{I}(T)$, т. е. когда $\mathfrak{B}^S = \mathfrak{B}^T$.

Зафиксируем некоторый максимальный тор T группы G. Пусть $Y(T)$ — множество морфизмов из $\mathbb{F}^*$ в T. Множество $Y(T)$ становится группой, если на нем ввести умножение правилом $a^{\lambda\mu} = a^\lambda \cdot a^\mu$. Заметим, что композиция $\lambda \in Y(T)$ с $\chi \in X(T)$ приводит к морфизму алгебраических групп $\mathbb{F}^* \to \mathbb{F}^*$, т. е. к элементу группы $X(\mathbb{F}^*) \simeq \mathbb{Z}$. Это позволяет определить спаривание $< \chi, \lambda > \in \mathbb{Z}$, относительно которого $X(T)$ и $Y(T)$ становятся двойственными $\mathbb{Z}$-модулями.

***Упражнение* 5.6.8.** Проверить, что $X(\mathbb{F}^*) \simeq \mathbb{Z}$ и доказать, что $X(T)$ и $Y(T)$ являются двойственными модулями для любого тора T.

Каждый элемент $\lambda \in Y(T)$ можно рассматривать как однопараметрическую подгруппу тора T (поскольку $(\mathbb{F}^*)\lambda \leq T$ имеет размерность 1). Однопараметрическая подгруппа $\lambda \in Y(T)$ называется *регулярной* если тор $(\mathbb{F}^*)\lambda$ регулярен. Обозначим через $Y(T)_{reg}$ множество всех однопараметрических регулярных подгрупп.

Лемма 5.6.9. *Однопараметрическая подгруппа $\lambda \in Y(T)$ является регулярной тогда и только тогда, когда $< \alpha, \lambda > \neq 0$ для всех $\alpha \in \Psi$ (определение множества Ψ дано перед леммой 5.6.5). Множество регулярных однопараметрических подгрупп обозначается через $Y(T)_{reg}$.*

Доказательство. Лемма непосредственно следует из леммы 5.6.5. □

***Упражнение* 5.6.10.** Пусть T — максимальный тор связной алгебраической группы G и $W = W(G,T) = N_G(T)/T$ — группа Вейля. Пусть $\sigma \in W$ и $n \in N_G(T)$ — любой его прообраз относительно естественного гомоморфизма. Тогда W действует на группах $X(T)$ и $Y(T)$ следующим образом:

$$\forall \chi \in X(T), \forall t \in T, t^{\chi^\sigma} = (t^{n^{-1}})^\chi; \tag{5.2}$$

$$\forall \lambda \in Y(T), \forall x \in \mathbb{F}^*, x^{\lambda^\sigma} = (x^\lambda)^n. \tag{5.3}$$

Доказать, что для таким образом определённого действия выполнено равенство $< \chi^\sigma, \lambda^\sigma > = < \chi, \lambda >$.

Поскольку $\Phi \subseteq X(T)$, мы получаем действие группы W на Φ, а именно, для любого $t \in T$, $\alpha \in \Phi$ справедливо $t^{\alpha^\sigma} = (t^{\mathrm{n}^{-1}})^\alpha$. В частности, $\mathfrak{g}_\alpha^{\mathrm{Ad}\ n} = \mathfrak{g}_{\alpha^\sigma}$.

Дальнейшая наша задача до конца этого параграфа — показать, что подгруппы Бореля из $\mathfrak{B}^T$ порождают всю группу G. Мы начнём с того, что покажем, что произвольная однопараметрическая подгруппа $\lambda \in Y(T)$, где T — некоторый тор группы $\mathrm{GL}(V)$ имеет по меньшей мере две неподвижных точки на многообразии $P(V) = P^{n-1}$. Пусть $v_1, \ldots, v_n$ — базис из собственных векторов тора T, тогда веса тора T являются ограничениями $\gamma_1, \ldots, \gamma_n$ соответствующих координатных функций, порождающих $X(T)$. Пусть $m_i = < \gamma_i, \lambda >$, тогда для любого $v = \sum_i \alpha_i v_i$ и для любого $t \in \mathbb{F}^a st$, по определению выполнено $vt^\lambda = \sum_i \alpha_i t^{m_i} v_i$. Таким образом, прямая, порождённая вектором v (обозначим её через $[v]$) переходит в прямую, порождённую вектором vt^λ, следовательно, однопараметрическая группа λ действует на $P(V)$.

Постараемся теперь продолжить отображение $\varphi : t \mapsto [v]t^\lambda$ до морфизма $P^1 \to P(V)$. Ввиду определения аффинных открытых подмножеств, мы получаем, что P^1 покрывается двумя аффинными открытыми подмножествами $\mathbb{F}^* \cap \{0\}$ и $F^* \cap \infty$, пересекающимися по F^*. Пусть как и выше $m_i = < \gamma_i, \lambda >$ и обозначим за m_0 (соответственно за m^0) минимальное (соответственно максимальное) значение m_i при $i \in I = \{i | \alpha_i \neq 0\}$ (напомним, что $v = \sum_i \alpha_i v_i$). Очевидно, что $[v] = [t^{-m_0} v] = [t^{-m^0} v]$ для любого $t \in \mathbb{F}^*$. Таким образом, отображение φ можно записать двумя способами: $t\varphi_0 = [\sum_i \alpha_i t^{m_i - m_0} v_i]$, и $t\varphi^0 = [\sum_i \alpha_i t^{m_i - m^0} v_i]$. Полагая $0^0 = x^0 = \infty^0 = 1$, мы получаем, что φ_0 имеет смысл даже при $t = 0$, а φ^0 имеем смысл даже при $t = \infty$, кроме того $\varphi_0|_{F^*} = \varphi^0|_{\mathbb{F}^*}$, что даёт нам искомый морфизм $P^1 \to P(V)$. Заметим, что $[v]0^\lambda = [\sum_{\{i | m_i = m_0\}} \alpha_i v_i]$ и $[v]\infty^\lambda = [\sum_{\{i | m_i = m^0\}} \alpha_i v_i]$ являются неподвижными точками группы $(F^*)\lambda$. Ясно, что они совпадают в том и только в том случае, когда $m_0 = m^0$, т. е. когда $(F^*)\lambda$ состоит только из скалярных матриц. Следовательно, и в этом случае группа $(F^*)\lambda$ имеет не меньше двух неподвижных точек на $P(V)$. Заметим также, что если подгруппа λ выбрана таким образом, что числа $m_i = < \gamma_i, \lambda >$ при различных γ_i различны, то собственные векторы тора T и группы λ совпадают. В этом случае мы получаем, что тор T также оставляет неподвижными точки $[v]0^\lambda$ и $[v]\infty^\lambda$. Поскольку $X(T) \times Y(T) = \mathbb{Z}$, мы всегда можем выбрать λ удовлетворяющим условию, что все m_i-ые различны. Легко понять также, что если $[v]t^\lambda$ — неподвижная точка для λ при $t \neq 0$, то вектор v является собственным для t^λ, и, значит, является собственным для тора T. Поэтому любая неподвижная точка группы λ является неподвижной точкой тора T. Обратное включение очевидно, так что множества неподвижных точек группы λ и тора T совпадают.

Лемма 5.6.11. *Пусть W — подпространство коразмерности 1 векторного пространства V, и пусть X — неприводимое замкнутое подмногообразие многообразия $P(V)$, которое не содержится целиком в $P(W)$. Если $\dim X > 0$, то $X \cap P(W) \neq \varnothing$ и каждая неприводимая компонента пересечения имеет коразмерность 1 в X.*

Доказательство. Будет написано позже. □

Теорема 5.6.12. *Пусть $T \leq \mathrm{GL}(V)$ — тор, естественным образом действующий на $P(V)$. Пусть X — неприводимое замкнутое T-инвариантное подмножество ненулевой размерности в $P(V)$. Тогда тор T оставляет неподвижными по меньшей мере две точки множества X. Более того, если $\dim X \geqslant 2$, то тор T оставляет неподвижными не менее трёх точек множества X.*

Доказательство. Пусть $v_1, \ldots, v_n$ — базис пространства V, состоящий из собственных векторов тора T с весами $\gamma_i \in X(T)$. Выберем $\lambda \in Y(T)$ так, чтобы числа $m_i =< \gamma_i, \lambda >$ были различны для различных γ_i (как мы заметили выше, такую однопараметрическую подгруппу λ всегда можно выбрать). Ввиду рассуждений, приведённых перед теоремой, множества неподвижных точек тора T и группы λ совпадают, поэтому мы можем заменить тор T на однопараметрическую подгруппу $(F^*)\lambda$.

Так как $\dim X \geqslant 1$, то множество X бесконечно. Если тор T оставляет неподвижными все точки множества X, то доказывать нечего. В противном случае пусть $[v] \in X$ — точка, не являющаяся неподвижной относительно T. В силу рассуждений об однопараметрических подгруппах, приведённых до теоремы, мы получаем, что $[v]0^\lambda$ и $[v]\infty^\lambda$ — две различные неподвижные точки в $P(V)$. Поскольку X является T-инвариантным, мы получаем, что эти две точки должны лежать в X.

Предположим теперь, что $\dim X \geqslant 2$. Мы вновь можем предполагать, что некоторая точка множества X не является неподвижной относительно T. Пусть $v_1, \ldots, v_n$ — базис из собственных векторов тора T, которому соответствуют элементы $\gamma_1, \ldots, \gamma_n \in X(T)$; можно считать, что порядок векторов выбран таким образом, что $< \gamma_1, \lambda >= m^0$. Тогда $W = \langle v_2, \ldots, v_n \rangle$ — T-инвариантное подпространство пространства V коразмерности 1. Более того, можно считать, что $X \not\subseteq P(W)$, в противном случае мы можем заменить пространство V на W и повторить рассуждения. По лемме 5.6.11, мы получаем, что каждая неприводимая компонента $X \cap P(W)$ является замкнутым неприводимым T-инвариантным подмножеством многообразия $P(V)$ (она является T-инвариантной, так как группа T связна, значит, по лемме 4.3.1, оставляет неподвижной каждую неприводимую компоненту множества $X \cap P(W)$). Ввиду уже доказанного мы получаем, что $X \cap P(W)$ содержит по меньшей мере две T-неподвижные точки. По построению множества $X \cap P(W)$, мы получаем, что прямая $[v]$ содержится в X для некоторого $v = \sum_i \alpha_i v_i$, причём $\alpha_1 \neq 0$. Следовательно, $[v]\infty^\lambda$ является T-неподвижной точкой и не лежит в $X \cap P(W)$. □

Следствие 5.6.13. *Пусть P — собственная параболическая подгруппа группы G, T — любой тор в G. Тогда T оставляет неподвижными по меньшей мере две точки многообразия G/P. Более того, тор T оставляет неподвижными по меньшей мере три точки многообразия G/P, если $\dim G/P > 1$. В частности, максимальный тор содержится по меньшей мере в двух борелевских подгруппах (и он содержится по меньшей мере в трёх борелевских подгруппах, если $\dim G/B > 1$.*

Доказательство. Рассмотрим такое представление $G \to \mathrm{GL}(V)$, что P является стабилизатором некоторой прямой (существование такого представления следует из теоремы Шевалле 4.8.2). Тогда многообразие G/P изоморфно орбите X некоторой точки из $P(V)$. Так как G/P замкнуто и неприводимо, то, по лемме 4.3.1, множество X также замкнуто и неприводимо. Ясно также, что X является T-инвариантным. Заметим также, что X не содержится ни в какой проективной гиперплоскости $P(W)$. В противном случае можно рассмотреть представление $G \to \mathrm{GL}(W)$, где W — гиперплоскость, для которой $P(W)$ содержит X. По прежнему P будет являться стабилизатором прямой. По теореме 5.6.12, тор T оставляет неподвижными по меньшей мере 2 точки из X, следовательно, из G/P. □

Следствие 5.6.14. *Пусть T — максимальный тор группы G. Тогда G порождается множеством $\mathfrak{B}^T$ подгрупп Бореля, содержащих тор T.*

Доказательство. Пусть утверждение теоремы неверно и G — контрпример минимальной размерности. Рассмотрим $P = \langle \mathfrak{B}^T \rangle$. Очевидно, что P является параболической подгруппой группы G. Предположим, что $P \neq G$. Тогда тор T имеет не меньше двух неподвижных точек на многообразии G/P, одна из которых соответствует подгруппе P, а вторая — некоторой, отличной от P, подгруппе P'. Далее T является максимальным тором группы P' и борелевские подгруппы группы P', содержащие тор T, лежат в P. По индукции, все такие борелевские подгруппы порождают P', значит, $P' \leq P$, что невозможно. □

§7 Унипотентный радикал

В данном параграфе мы докажем, что унипотентный радикал группы G совпадает с $\mathfrak{I}(G)_u$ и получим ряд следствий о строении редуктивных групп. В частности, мы докажем, что централизатор любого тора в редуктивной группе вновь является редуктивной группой. Для этого мы сначала выясним строение групп полупростого ранга 1, затем введём для каждого $\alpha \in \Psi$ камеры Вейля и затем с их помощью докажем основную теорему об унипотентном радикале.

Ранг факторгруппы $G/R(G)$ (соответственно $G/R_u(G)$) называется *полупростым рангом* $\mathrm{rank}_{ss}(G)$ (соответственно *редуктивным рангом* $\mathrm{rank}_{red}(G)$).

Теорема 5.7.1. *Пусть T — максимальный тор группы G и $W = W(G,T)$. Следующие утверждения эквивалентны:*

(а) $\mathrm{rank}_{ss}(G) = 1$*;*

(б) $|W| = 2$*;*

(в) $|\mathfrak{B}^T| = 2$*;*

(г) $\dim G/B = 1$*;*

(д) $G/B \simeq P^1$*;*

(е) *существует эпиморфизм* $\varphi : G \to \mathrm{PGL}_2(\mathbb{F})$ *такой, что* $\mathrm{Ker}(\varphi)^0 = R(G)$.

Доказательство. (а)⇒(б) Поскольку $R(G)$ содержится во всех подгруппах Бореля группы G и $C_B(T) = N_B(T)$ (см. следствие 5.4.5), мы получаем, что $W(G,T) \simeq W(G/R(G), TR(G)/R(G))$. Далее, $TR(G)/R(G)$ — тор размерности 1 (так как ранг группы $G/R(G) = 1$), следовательно он изморфен группе $\mathbb{F}^*$. Группа W индуцирует автоморфизмы группы $X(T) \simeq \mathbb{Z}$ (см. упражнение 5.6.8). Но $|\mathrm{Aut}(\mathbb{Z})| = 2$, откуда $|W| \leqslant 2$. По следствию 5.6.13 мы получаем, что $|W| \geqslant 2$, значит, $|W| = 2$.

(б)⇒(в). Следует из того, что $|W| = |\mathfrak{B}^T|$ (лемма 5.6.2).

(в)⇒(г). Поскольку $G \neq B$ (в противном случае $\mathrm{rank}_{ss}(G) = 0$), мы получаем, что $\dim G/B \geqslant 1$. Если $\dim G/B > 1$, то ввиду следствия 5.6.13 мы получаем, что $|\mathfrak{B}^T| \geqslant 3$, что противоречит условию $|\mathfrak{B}^T| = 2$.

(г)⇒(д). Так как группа G связна, её образ G/B также связен. Таким образом, G/B — связное проективное многообразие размерности 1. Значит, $G/B \simeq P^1$.

(д)⇒(е). Поскольку $G/B \simeq P^1$ и G действует на G/B сдвигами, мы получаем гомоморфизм группы G в $\mathrm{Aut}(P^1) = \mathrm{PGL}_2(\mathbb{F})$. Очевидно, что ядро этого гомоморфизма есть пересечение всех борелевских подгрупп группы G, следовательно, содержит $R(G)$. Далее, размерность образа группы G нетривиальна, поскольку $\dim G/R(G) > 0$ и образ группы G неразрешим. Поскольку размерность группы $\mathrm{PGL}_2(\mathbb{F})$ равна 3, а размерность её подгруппы Бореля равна 2, мы получаем, что любая подгруппа группы $\mathrm{PGL}_2(\mathbb{F})$ размерности меньшей, чем 3, либо конечна, либо разрешима. Значит, образ группы G совпадает со всей группой $\mathrm{PGL}_2(\mathbb{F})$.

(е)⇒(а). Очевидно по определению. □

Сформулируем теперь следствие о строении редуктивных групп полупростого ранга 1, оставив доказательство читателю.

Следствие 5.7.2. *Пусть G — редуктивная группа полупростого ранга 1, T — её максимальный тор и $Z = Z(G)^0$. Тогда*

(а) *коммутант $[G,G]$ является полупростой группой и имеет размерность 3;*

(б) *$G = [G,G] \cdot Z$, причём $|[G,G] \cap Z| < \infty$;*

(в) *$C_G(T) = T$ и, в частности, $Z(G) < T$;*

(г) *если $\varphi : G \to \mathrm{PGL}_2(\mathbb{F})$ — эпиморфизм, то $\mathrm{Ker}(\varphi) = Z(G)$.*

***Упражнение* 5.7.3.** Пусть $\alpha \in \Psi$, $Z_\alpha = C_G(T_\alpha)$ и T — максимальный тор группы G, содержащий T_α. Ввиду теоремы 5.7.2(б), справедливо $|W(Z_\alpha, T)| = 2$. Пусть σ_α — (единственный) неединичный элемент группы $W(Z_\alpha, T)$. Доказать, что $\alpha^{\sigma_\alpha} = -\alpha$ (напомним, что $\alpha \in X(T)$). *Указание. Рассмотреть гомоморфный образ $Z_\alpha/R(Z_\alpha)/Z(Z_\alpha/R(Z_\alpha)) \simeq \mathrm{PGL}_2(\mathbb{F})$. Тогда образ тора T совпадает с диагональной подгруппой и любой элемент из нормализатора диагональной подгруппы инвертирует любую диагональную матрицу.*

***Упражнение* 5.7.4.** Доказать, что если $\alpha \in \Psi$, то единственный кратный α корень, отличный от α и лежащий в Ψ, есть корень $-\alpha$. *Указание. В противном случае, корни* $\alpha, -\alpha, n\alpha$ *лежали бы в* $\Phi(\mathrm{PGL}_2(\mathbb{F}), T)$, *где* T *— диагональная подгруппа. Следовательно,* $\dim \mathrm{PGL}_2(\mathbb{F}) > 3$.

Далее мы каждой регулярной однопараметрической подгруппе $\lambda \in Y(T)$ сопоставим по некоторому правилу подгруппу Бореля $B(\lambda) \in \mathfrak{B}^T$. Поскольку $|\mathfrak{B}^T| < \infty$, это соответствие, очевидно, не может быть взаимно однозначным. При этом данное соответствие будет сюръективным и обладать некоторыми важными для дальнейших рассуждений свойствами.

Выберем представление $G \to \mathrm{GL}(V)$ так, чтобы подгруппа бореля B являясь стабилизатором прямой (это всегда можно сделать ввиду теоремы Шевалле 4.8.2). Тогда многообразие G/B можно отождествить с орбитой X некоторой точки многообразия $P(V)$. Также, как и при доказательстве следствия 5.6.13, можно считать, что X не содержится в $P(W)$ для любой гиперплоскости $W \leq V$. Пусть $v_1, \ldots, v_n$ — базис из собственных векторов тора T и $\gamma_1, \ldots, \gamma_n \in X(T)$ — соответствующие характеры тора T. Тогда положим $m_i =< \gamma_i, \lambda >$. Упорядочим базис $v_1, \ldots, v_n$ таким образом, что $m^0 = m_1 = m_2 = \ldots = m_r > m_{r+1} \geqslant \ldots \geqslant m_n = m_0$. Пусть W — гиперплоскость, натянутая на $v_2, \ldots, v_n$. Поскольку X не содержится в $P(W)$, мы получаем, что существует точка $[v] = [\sum_i \alpha_i v_i] \in X$, для которой $\alpha_1 \neq 0$. Рассуждения перед леммой 5.6.11 показывают, что $[v]\infty^\lambda = [\alpha_1 v_1 + \ldots + \alpha_r v_r]$ является неподвижной точкой группы $(F^*)\lambda$. Поскольку $T^{\gamma_2} = \mathbb{F}^*$, и $\gamma_1, \ldots \gamma_n$ линейно независимы, мы получаем, что существует бесконечно много точек вида $[\alpha_1 v_1 + \beta v_2 + \alpha_3 v_3 + \ldots + \alpha_r v_r]$ и все они неподвижны относительно $(\mathbb{F}^*)\lambda$, что противоречит регулярности λ. Следовательно, $r = 1$ и $[v]\infty^\lambda = [v_1]$. Рассмотрим окрестность $U = X \setminus P(W)$ точки $[v_1]$. Предыдущие рассуждения показывают, что для любого $[v'] \in U$ справедливо $[v']\infty^\lambda = [v_1]$. Обозначим подгруппу Бореля, соответствующую точке $[v_1]$ через $B(\lambda)$. Заметим, что ввиду упражнения 5.6.7, тор T оставляет неподвижной точку $[v_1]$, т. е. $B(\lambda) \in \mathfrak{B}^T$.

Как мы уже отмечали, группа Вейля W действует на $Y(T)$ (см. (5.3)) и, ввиду упражнения 5.6.10, для любых $\sigma \in W$, $\chi \in X(T)$ и $\lambda \in Y(T)$ справедливо равенство $< \chi^\sigma, \lambda^\sigma >=< \chi, \lambda >$. Ввиду критерия регулярности однопараметрической подгруппы (лемма 5.6.9) мы получаем, что $Y(T)_{reg}$ — W-инвариантное подмножество группы $Y(T)$. Кроме того, ввиду леммы 5.6.2, группа W действует регулярно на $\mathfrak{B}^T$. Покажем, что эти два действия согласованы относительно отображения $\lambda \to B(\lambda)$. Пусть $\sigma \in W$ и $n \in N_G(T)$ — некоторый его прообраз. Тогда элемент n переставляет собственные подпространства тора T и, следовательно, переставляет веса γ_i и целые числа $m_i =< \gamma_i, \lambda >$. Ввиду равенства $< \gamma_i^\sigma, \lambda^\sigma >=< \gamma_i, \lambda >$, мы получаем, что $[v_1^n]$ — неподвижная точка относительно группы $(\mathbb{F}^*)\lambda^\sigma$, получаемая таким же образом, как и точка $[v_1]$ для группы $(\mathbb{F}^*)\lambda$. Следовательно, подгруппа Бореля B^n совпадает с $B(\lambda^\sigma)$, т. е. действие группы Вейля на $Y(T)_{reg}$ и $\mathfrak{B}^T$ согласовано. В частности, соответствие $\lambda \mapsto B(\lambda)$ является сюръективным. Обозначим за $\mathfrak{C}(B) = \{\lambda \in Y(T)_{reg} | B = B(\lambda)\}$ для каждой подгруппы Бореля $B \in \mathfrak{B}^T$. Это множество называется *камерой Вейля* группы B (относительно тора T). Следовательно, непустые множества $\mathfrak{C}(B)$ образуют непересекающееся разбиение множества $Y(T)_{reg}$.

Рассмотрим теперь $\alpha \in \Psi$, пусть σ_α — (единственный) неединичный элемент группы $W(Z_\alpha, T)$, $n_\alpha \in N_{Z_\alpha}(T)$ — некоторый его прообраз. Рассмотрим такой $\lambda_0 \in Y(T)$, что $< \alpha, \lambda_0 >> 0$. Пусть $B = B(\lambda_0)$ и $B_\alpha = B \cap Z_\alpha$. Тогда Z_α содержит в точности две T-инвариантных подгруппы Бореля: B_α и B'_α, причём $B_\alpha^n = B'_\alpha$. Ввиду упражнения 5.7.3 выполнено равенство $\alpha^\sigma = -\alpha$. Следовательно, $B(\lambda) \cap Z_\alpha = B_\alpha$ в том и только в том случае, когда $< \alpha, \lambda >> 0$. Заметим также, что для любой группы Бореля $B \in \mathfrak{B}^T$ справедливо в точности одно из равенств: либо $B \cap Z_\alpha = B_\alpha$, либо $B \cap Z_\alpha = B'_\alpha$, причём если $B \cap Z_\alpha = B_\alpha$, то $B^n \cap Z_\alpha = B'_\alpha$. В частности, мы получаем разбиение множества $\mathfrak{B}^T$ на два равномощных подмножества, т. е. порядок группы Вейля всегда делится на 2. Приведённые выше рассуждения можно сформулировать в следующую лемму.

Лемма 5.7.5. *Зафиксируем максимальный тор T группы G и сопоставим каждому элементу $\lambda \in Y(T)$ подгруппу Бореля $B(\lambda)$ по правилу, определённому выше. Пусть $\alpha \in \Psi$, $Z_\alpha = C_G(T_\alpha)$ и B_α, B'_α — T-инвариантные подгруппы Бореля группы Z_α.*

Тогда для всех $\lambda \in Y(T)_{reg}$, $< \alpha, \lambda >> 0$ в том и только в том случае, когда $B(\lambda) \cap Z_\alpha = B_\alpha$.

Далее мы докажем вспомогательную лемму, которая обеспечивает существование достаточно большого числа регулярных однопараметрических подгрупп.

Лемма 5.7.6. *Пусть $\alpha, \beta \in \Psi$ — непропорциональные корни. Тогда существует однопараметрическая подгруппа $\lambda \in Y(T)_{reg}$, для которой $< \alpha, \lambda >> 0$ и $< \beta, \lambda >< 0$.*

Доказательство. Ввиду леммы 5.2.7, группа $X(T) \simeq \mathbb{Z}^n$. Поскольку $Y(T)$ — двойственное над $\mathbb{Z}$ пространство для $X(T)$, то и $Y(T) \simeq \mathbb{Z}^n$. Таким образом, мы можем рассмотреть векторные пространства над $\mathbb{Q}$, получаемые как $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$ и $Y(T) \otimes_{\mathbb{Z}} \mathbb{Q}$, и продолжить спаривание $< \chi, \gamma >$ на эти пространства. Тогда α, β становятся линейно независимыми векторами, условие регулярности λ $(\forall \chi \in \Psi, < \chi, \lambda > \neq 0)$ означает,

что λ не принадлежит конечному набору гиперплоскостей, ортогональный корням из Ψ. Очевидно, что в пространстве $Y(T)\otimes_{\mathbb{Z}}\mathbb{Q}$ существует вектор λ_0, для которого $<\alpha,\lambda_0>>0$ и $<\beta,\lambda_0><0$, и который не принадлежит объединению гиперплоскостей, ортогональных корням из Ψ. Кроме того, $\lambda_0=\frac{m_1}{k_1}\lambda_1+\ldots+\frac{m_n}{k_n}\lambda_n$, где $\lambda_i\in Y(T)$ и $m_i\in\mathbb{Z}$, $k_i\in\mathbb{N}$. Умножая на наименьшее общее кратное чисел $k_1,\ldots,k_n$, мы получаем элемент $\lambda\in Y(T)$, удовлетворяющий всем условиям леммы. $\square$

Теорема 5.7.7. *Пусть G — связная алгебраическая группа и T — её максимальный тор. Пусть $\mathfrak{I}(T)=\left(\bigcup_{B\in\mathfrak{B}^T}B\right)^0$. Тогда $R_u(G)=\mathfrak{I}(T)_u$.*

Доказательство. Обозначим для краткости $\mathfrak{I}(T)_u$ за U. Поскольку $R_u(G)$ совпадает с унипотентным радикалом пересечения всех подгрупп Бореля группы G, включение $R_u(G)\le U$ очевидно. Для того, чтобы доказать обратное включение, достаточно доказать, что U нормальна в G. Ввиду следствия 5.6.14, мы получаем, что множество подгрупп Бореля, содержащих тор T, порождает всю группу G. Заметим, что если $B\in\mathfrak{B}^T$, то B порождается группами $C_B(S)$, где S пробегает все подторы тора T коразмерности 1. Действительно, пусть A — подгруппа, порождённая группами $C_B(S)$. Поскольку $C_B(T)\le C_B(S)$, то всякий элемент веса 0 алгебры $\mathfrak{L}(B)=\mathfrak{b}$ содержится в $\mathfrak{L}(A)=\mathfrak{a}$ (см. лемму 5.3.6). Если α — нетривиальный вес, то $\mathrm{Ker}(\alpha)^0=S$ — тор коразмерности 1 в T. Таким образом, все нетривиальные веса α алгебры $\mathfrak{b}$ содержатся в $\mathfrak{a}$. Значит, $\mathfrak{a}=\mathfrak{b}$, следовательно, $\dim B=\dim A$. Так как группа B связна, это влечёт равенство $B=A$.

Таким образом, достаточно доказать, что группа U нормализуется всеми $C_B(S)$, где S — подтор коразмерности 1 в T. Если тор S регулярен, то, ввиду упражнения 5.6.7, $C_B(S)\le\mathfrak{I}(T)$ и доказывать нечего. Поэтому можно считать, что тор S сингулярен, т. е. совпадает с T_α для некоторого $\alpha\in\Psi$. Тогда $C_B(T_\alpha)=Z_\alpha\cap B$ совпадает с одной из двух подгрупп Бореля группы Z_α: либо B_α, либо B'_α. В частности, для любого $\beta\in\Psi$ и любой $B\in\mathfrak{B}^T$, в точности один из корней $\beta,-\beta$ может лежать в $\mathfrak{L}(B)$. Более того, если $B=B(\lambda)$ для некоторого $\lambda\in Y(T)_{reg}$, то мы можем считать, что $B\cap Z_\alpha=B_\alpha$ тогда и только тогда, когда $<\alpha,\lambda>>0$. Ввиду упражнения 5.7.3, мы получаем, что $\alpha,-\alpha\in\mathfrak{L}(Z_\alpha)$. Более того, ввиду леммы 5.7.5, для любого $\beta\in\Psi$ и для любой подгруппы Бореля $B\in\mathfrak{B}^T$, в точности один из корней $\beta,-\beta$ лежит в $\Phi(B,T)$.

Пусть H — унипотентный радикал пересечения всех $B\in\mathfrak{B}^T$, для которых $B\cap Z_\alpha=B_\alpha$. Очевидно, что достаточно доказать $U\trianglelefteq H$. Ввиду леммы 5.7.5 он совпадает с унипотентным радикалом пересечения тех $B(\lambda)$, для которых $<\alpha,\lambda>>0$. Очевидно, что $R_u(Z_\alpha)\le U\le H$. Поскольку группа H является T-инвариантной, то $\mathfrak{L}(H)=\mathfrak{h}$ является суммой подпространства $\mathfrak{L}(U)=\mathfrak{u}$ и некоторых ненулевых пространств $\mathfrak{g}_\beta$, где $\beta\in\Psi$ (все веса из $\mathfrak{L}(\mathfrak{I}(T))$, очевидно, лежат в $\mathfrak{u}$). Обозначим множество корней таких корней за Θ. По построению, $\alpha\in\Theta$ и $-\alpha\notin\Theta$. Ввиду упражнения 5.7.4, мы получаем, что если $\beta\in\Psi$ и $\beta\notin\{\alpha,-\alpha\}$, то β непропорционален α. По лемме 5.7.6, существует $\lambda\in Y(T)_{reg}$, для которого $<\alpha,\lambda>>0$ и $<\beta,\lambda><0$. Ввиду леммы 5.7.5 мы получаем, что $B(\lambda)\cap Z_\beta=B'_\beta$ и $-\beta\in\Phi(B,T)$. С другой стороны, по построению, $\beta\in\Theta$ и $H\le B(\lambda)$, значит, $\beta\in\Phi(B(\lambda),T)$, что невозможно. Следовательно, только корень α лежит в Θ, т. е. коразмерность группы U в H равна 1. Поскольку группа H нильпотентна и связна, мы получаем, что её центр нетривиален. Индукцией по размерности группы H легко доказать, что любая связная подгруппа коразмерности 1 нормальна в H. Действительно, V — связная подгруппа коразмерности 1 и $Z(H)\le V$, то переходим к факторгруппе $H/Z(H)$ и применяем индукцию по размерности. В противном случае, $\dim Z(H)V>\dim V$, значит, $Z(H)V=H$. Таким образом, $U\trianglelefteq H$, что заканчивает доказательство теоремы. $\square$

Далее мы получим ряд следствий из теоремы.

Следствие 5.7.8. *Пусть G — связная редуктивная группа, T — её максимальный тор и S — некоторый подтор тора T. Тогда*

(а) *группа $C_G(S)$ редуктивна (и связна);*

(б) *если тор S регулярен, то $C_G(S)=T$. В частности, картановские подгруппы группы G — это в точности максимальные торы и $Z(G)\le T$.*

Доказательство. Пусть $C=C_G(S)$. По теореме 5.7.7, применённой к C, мы получаем, что $R_u(C)$ совпадает с унипотентным радикалом пересечения всех борелевских подгрупп группы C, содержащих T. Она в свою очередь совпадает с $\mathfrak{I}(T)_u=\{e\}$, что доказывает (а). Если тор S регулярен, то $C_G(S)$ разрешима (лемма 5.6.4) и редуктивна (пункт (а)), следовательно, является тором. $\square$

Следствие 5.7.9. *Пусть G — связная редуктивная группа T — её максимальный тор и $\Phi=\Phi(G,T)$ — её система корней. Тогда*

(а) $\Phi = \Psi$ *и* $\Phi = -\Phi$;

(б) $\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha\in\Phi} \mathfrak{g}_\alpha$, *где* $\mathfrak{t} = \mathfrak{L}(T)$ *и* $\dim \mathfrak{g}_\alpha = 1$;

(в) *сингулярные торы коразмерности* 1 *в* T *имеют вид* $T_\alpha = \mathrm{Ker}(\alpha)^0$, $\alpha \in \Phi$;

(г) *если* $Z_\alpha = C_G(T_\alpha)$, *то* Z_α *— редуктивная группа полупростого ранга* 1 *и* $\mathfrak{L}(Z_\alpha) = \mathfrak{z}_\alpha = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$, *кроме того группы* Z_α *порождают* G;

(д) $Z(G)^0 = (\cap_{\alpha\in\Phi} T_\alpha)^0$;

(е) *ранг подгруппы* $R = \langle\Phi\rangle \leq X(T)$ *равен* $\mathrm{rank}_{ss} G$.

Доказательство. Утверждения (а)–(г) очевидным образом следуют из классификации редуктивных подгрупп ранга 1 (следствие 5.7.2), замечаний вначале доказательства теоремы 5.7.7 и следствия 5.7.9. Утверждения (д) и (е) оставляются читателю в качестве упражнения. □

Следствие 5.7.10. *Пусть* G *— редуктивная групп. Для каждой борелевской подгруппы* B, *содержащей максимальный тор* T, *существует такая группа* $B^- \in \mathfrak{B}^T$, *что* $B \cap B^- = T$. *Тогда* $\mathfrak{g} = \mathfrak{L}(B) + \mathfrak{L}(B^-) = \mathfrak{b} + \mathfrak{b}^- = \mathfrak{u}^- \oplus \mathfrak{t} \oplus \mathfrak{u}$, *где* $\mathfrak{t} = \mathfrak{L}(T)$, $\mathfrak{u} = \mathfrak{L}(R_u(B))$, $\mathfrak{u}^- = \mathfrak{L}(R_u(B^-))$.

Доказательство. По лемме 5.7.5 существует такой $\lambda \in Y(T)$, что $B = B(\lambda)$. Положим $B^- = B(-\lambda)$. Для каждого $\alpha \in \Phi$ группы $Z_\alpha \cap B$ и $Z_\alpha \cap B^-$ являются различными борелевскими подгруппами группы Z_α, содержащими тор T. Ввиду следствия 5.7.9 мы получаем, что $B \cap B^- = T$ и алгебра Ли $\mathfrak{g}$ имеет требуемое разложение. □

***Упражнение* 5.7.11.** Группа B^-, определённая в следствии 5.7.10, единственная. Она называется подгруппой Бореля, *противоположной* группе B.

§8 Одномерные T-инвариантные подгруппы

В данном параграфе мы заметим, что корневую систему связной редуктивной алгебраической группы можно ввести и внутренним образом, не переходя к алгебре Ли и изучим строение одномерных T-инвариантных унипотентных подгрупп.

Лемма 5.8.1. *Для любого поля* $\mathbb{F}$ *мультипликативная и аддитивная группы поля* $\mathbb{F}$ *являются единственными связными алгебраическими группами размерности* 1.

Доказательство. *Мы приведём здесь лишь краткую схему, оставив подробное доказательство читателю.* По лемме 5.3.3 мы получаем, что класс сопряжённости любого полупростого элемента замкнут. Кроме того, он связен, как образ связной группы, потому тривиален. Значит, все полупростые элементы произвольной одномерной группы G лежат в центре, и подгруппа Бореля группы G нильпотентна. Следовательно, группа G нильпотентна, связна и имеет размерность 1. Как мы заметили в доказательстве теоремы 5.7.7, $Z(G)$ имеет положительную размерность, следовательно, группа G абелева. Далее, множество полупростых элементов G_s группы G образует замкнутую подгруппу. Следовательно, она либо конечна, либо совпадает с G. В первом случае мы получаем, что $|G : G_u| = |G_s|$, т. е. $G = G_u$ и G состоит из унипотентных элементов. Тогда алгебра $L = \langle e - g | g \in G\rangle$ — нильпотентная ассоциативная алгебра матриц размерности 1, следовательно, она изоморфна аддитивной группе поля $\mathbb{F}$. Но тогда группа G, очевидно, тоже изоморфна аддитивной группе поля $\mathbb{F}$. Во втором случае G_s — тор размерности 1, изоморфный мультипликативной группе поля $\mathbb{F}$. □

Для любого $\alpha \in \Phi$ подалгебра $\mathfrak{g}_\alpha$ является алгеброй Ли унипотентной части U_α борелевской подгруппы B_α группы $Z_\alpha = C_G(T_\alpha)$ (см. следствие 5.7.9(г)). Более того, группа U_α — единственная связная T-инвариантная подгруппа группы G, алгебра Ли которой совпадает с $\mathfrak{g}_\alpha$. Предположим, что некоторая подгруппа V_α является связной T-инвариантной подгруппой группы G, алгебра Ли которой совпадает с $\mathfrak{g}_\alpha$. Тогда её алгебра Ли одномерна и состоит из нильпотентных элементов (нильпотентных в ассоциативной алгебре). Также, как и при доказательстве леммы 5.8.1, это сразу влечёт, что V_α унипотентна. Кроме того, $H = TV_\alpha$ — связная разрешимая подгруппа группы G и, следовательно, содержится в некоторой подгруппе Бореля $B \in \mathfrak{B}^T$. Так как T_α централизует $\mathfrak{L}(H) = \mathfrak{L}(T) + \mathfrak{g}_\alpha$, то T_α централизует H. Следовательно, $V_\alpha \in B \cap Z_\alpha$, откуда $V_\alpha = U_\alpha$.

Теорема 5.8.2. *Пусть* G *— связная редуктивная алгебраическая группа,* T *— её максимальный тор и* $\alpha \in \Phi(G, T) = \Phi$. *Тогда*

(а) *существует единственная связная T-инвариантная подгруппа U_α группы G, алгебра Ли которой совпадает с $\mathfrak{g}_\alpha$;*

(б) *если элемент $n \in N$ является некоторым представителем элемента $\sigma \in W$, то $U_\alpha^n = U_{\alpha^\sigma}$;*

(в) *существует такой изоморфизм $\varepsilon_\alpha : \mathbb{F} \to U_\alpha$, что для всех $t \in T$, $x \in \mathbb{F}$ выполнено $(x^{\varepsilon_\alpha})^t = (x^{t^\alpha})^{\varepsilon_\alpha}$ (здесь $\mathbb{F}$ — аддитивная группа поля $\mathbb{F}$);*

(г) *группа G порождается подгруппами U_α $(\alpha \in \Phi)$ и T.*

Доказательство. Пункт (а) следует из рассуждений, приведённых выше. Так как

$$\mathfrak{L}(n^{-1}U_\alpha n) = (\mathfrak{L}(U_\alpha))^{\mathrm{Ad}\ n} = \mathfrak{g}_\alpha^{\mathrm{Ad}\ n} = \mathfrak{g}_{\alpha^\sigma}$$

и группа U_α^n связна и T-инвариантна, то (б) следует из (а). Поскольку каждая из Z_α порождается подгруппами $T, U_\alpha, U_{-\alpha}$, то утверждение (г) вытекает из следствия 5.7.9(г). Таким образом, осталось доказать (в).

Поскольку U_α — связная одномерная унипотентная группа, упражнение 5.8.1 влечёт существование некоторого изоморфизма $\varepsilon : \mathbb{F} \to U_\alpha$. Следовательно, действие тора T сопряжениями на группе U_α задает действие тора T на $\mathbb{F}$ (согласованное с изоморфизмом ε) и мы получаем морфизм алгебраических групп $T \to \mathrm{Aut}(\mathbb{F}) = \mathrm{GL}_1(\mathbb{F}) = \mathbb{F}^*$, где $\mathbb{F}^*$ — мультипликативная группа поля $\mathbb{F}$, т. е. характер γ тора T. Таким образом, $t^{-1}x^\varepsilon t = (x^{t^\gamma})^\varepsilon$, т. е. для каждого элемента $t \in T$ следующая диаграмма коммутативнапростая

$$\begin{array}{ccc} \mathbb{F} & \xrightarrow{\varepsilon} & U_\alpha \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Int}_t} \\ \mathbb{F} & \xrightarrow{\varepsilon} & U_\alpha \end{array}$$

где отображение $\mathbb{F} \to \mathbb{F}$ есть умножение на t^γ. Далее, $\mathfrak{L}(\mathbb{F}) = \mathbb{F}$, поэтому дифференциал умножения на t^γ вновь является умножением на t^γ, а $\mathrm{d}(\mathrm{Int}t) = \mathrm{Ad}\ t$. Следовательно, $\mathsf{x}^{\mathrm{Ad}\ t} = \mathsf{x}^{t^\gamma}$ для любого $\mathsf{x} \in \mathfrak{g}_\alpha$ и $\gamma = \alpha$. Таким образом мы можем положить $\varepsilon_\alpha = \varepsilon$. □

Ввиду теоремы 5.8.2(в), существует изоморфизм $\varepsilon : \mathbb{F} \to U_\alpha$, для которого выполнено равенство $(x^{\varepsilon_\alpha})^t = (x^{t^\alpha})^{\varepsilon_\alpha}$. Далее элементы группы U_α мы будем обозначать через $u_\alpha(x)$, предполагая, что $x \in F$ выбран таким образом, что для любого $t \in T$ справедливо $u_\alpha(x)^t = u_\alpha(t^\alpha \cdot s)$. Подгруппы U_α далее будут называться *корневыми подгруппами*, а элементы $u_\alpha(x)$ — *корневыми элементами*.

Далее мы докажем лемму о связи представления редуктивной алгебраической группы и её весов. Рассмотрим случай, когда G является замкнутой подгруппой группы $\mathrm{GL}(V)$ и пусть χ — некоторый вес максимального тора T. Напомним (см. §2 настоящей главы), что весовое пространство $V_\chi = \{v \in V | \forall x \in T, v^x = x^\chi v\}$.

Лемма 5.8.3. *Пусть $\rho : G \to \mathrm{GL}(V)$ — рациональное представление и $\mathrm{Ker}(\rho) \leq Z(G)$. Пусть V_χ — весовое пространство относительно T^ρ. Если $\alpha \in \Phi$, то $(V_\chi)U_\alpha^\rho \subseteq \sum_{k \in \mathbb{N} \cup \{0\}} V_{\chi + k\alpha}$.*

Доказательство. Ввиду следствия 5.7.8(б), выполнено $Z(G) \leq T$, значит, $G^\rho \leq Z(G) \leq T$. Таким образом, без ограничения общности, группу G можно заменить на её образ G^ρ и считать, что $U_\alpha^\rho = U_\alpha$. Так как группа TU_α связна и разрешима, по теореме Ли-Колчина (следствие 5.1.6) можно считать, что она состоит из нижнетреугольных матриц, группа U_α состоит из нижнеунитреугольных матриц и тор T состоит из диагональных матриц вида $\mathrm{diag}(t_1, \ldots, t_n)$. Заметим, что если $u \in U_\alpha$, то элемент на месте (i,j) в матрице u^t равен $t_i^{-1}t_j u_{i,j}$.

Рассмотрим изоморфизм $\varepsilon_\alpha : \mathbb{F} \to U_\alpha$, определённый в теореме 5.8.2(в). Тогда $(x^{\varepsilon_\alpha})_{i,j}$ является многочленом от x, т. е. $(x^{\varepsilon_\alpha})_{i,j} = c_0 + c_1 x + \ldots + c_m x^m$ для некоторых $c_0, \ldots, c_m \in \mathbb{F}$. Значит, $((t^\alpha x)^{\varepsilon_\alpha})_{i,j} = c_0 + c_1(t^\alpha x) + \ldots + c_m(t^\alpha x)^m$. По теореме 5.8.2(в) справедливо также $(x^{\varepsilon_\alpha})^t = (x^{t^\alpha})^{\varepsilon_\alpha}$, поэтому $((t^\alpha x)^{\varepsilon_\alpha})_{i,j} = t_i^{-1}t_j$. Таким образом, мы получили следующее тождество $c_0(1 - t_i^{-1}t_j) + c_1(t^\alpha - t_i^{-1}t_j)x + \ldots + c_m((t^\alpha)^m - t_i^{-1}t_j)x^m = 0$. Поскольку поле $\mathbb{F}$ бесконечно, это значит, что каждый из коэффициентов равен 0. Если за γ обозначить характер $\gamma : t \mapsto t_i^{-1}t_j$, то равенство нулю коэффициентов означает, что $l\alpha = \gamma$ каждый раз, когда $c_l \neq 0$. Поскольку характер α нетривиален, это означает, что в точности одно из c_l отлично от 0, можно считать, что $c_m \neq 0$ и $(x^{\varepsilon_\alpha})_{i,j} = c_m x^m$.

Пусть теперь χ задан правилом $\chi : T \mapsto t_i$ (характеры такого вида порождают группу $X(T)$, поэтому можно рассматривать лишь их). Мы имеем, что $v_i^u = \sum_{j \leqslant i} \lambda_j v_j$, т. е. вектор v^u является линейной комбинацией векторов с весами η_j, для которых $\eta_j : t \mapsto t_j$. Тогда предыдущие рассуждения показывают, что $\eta_j - \chi = m\alpha$ для некоторого $0 \leqslant m \in \mathbb{N} \cup \{0\}$. □

§9 Абстрактные корневые системы

Напомним, см. определение 2.1.1 подмножество Φ евклидового пространства E называется корневой системой если выполнены следующие аксиомы:

1. Φ является конечным множеством ненулевых векторов.

2. Φ порождает пространство E.

3. Если $r, s \in \Phi$, то $s^{w_r} \in \Phi$.

4. Если $r, s \in \Phi$, то $2(r,s)/(r,r)$ целое.

5. Если $r, \lambda r \in \Phi$, где $\lambda \in \mathbb{R}$, то $\lambda = \pm 1$.

В случае абстрактной корневой системы $s^{w_r} = s - \frac{2(r,s)}{(r,r)}r$, то условие 4 можно заменить следующим утверждением: $s^{w_r} - s$ целочисленно кратен r. Кроме того, в алгебраических группах для записи корней удобнее использовать греческие буквы (и это согласуется с обозначениями корней, использованными ранее), поэтому множество аксиом системы корней можно записать в следующем виде:

A1 Φ является конечным множеством ненулевых векторов.

A2 Φ порождает пространство E.

A3 Если $\alpha, \beta \in \Phi$, то $\beta^{w_\alpha} \in \Phi$.

A4 Если $\alpha, \lambda\alpha \in \Phi$, где $\lambda \in \mathbb{R}$, то $\lambda = \pm 1$.

A5 Если $\alpha, \beta \in \Phi$, то $\beta^{w_\alpha} - \beta$ целочисленно кратен α.

Напомним также, что группой Вейля корневой системы Φ называется группа, порождённая отражениями $w_\alpha, \alpha \in \Phi$. В качестве w_α мы рассмотрим σ_α — единственный неединичный элемент из факторгруппы $N_{Z_\alpha}(T)/T$. Для того, чтобы проверить, что σ_α можно взять в качестве отражения в корне α достаточно показать, что $\alpha^{\sigma_\alpha} = -\alpha$, и что σ_α оставляет неподвижной некоторую гиперплоскость в E. Выберем однопараметрическую подгруппу λ, для которой $\lambda^{\sigma_\alpha} = -\lambda$. Очевидно, что такая подгруппа существует, в качестве λ можно взять тот, для которого выполнено $< \alpha, \lambda > \neq 0$. Тогда подгруппа $X = \{\chi \in X(T) | < \chi, \lambda >= 0\}$ имеет ранг $n-1$ и потому порождает требуемую гиперплоскость. Наша задача в данном параграфе доказать, что корневая система связной редуктивной группы G относительно максимального тора T, определённая в § 2 настоящей главы. Ясно, что достаточно доказать следующую теорему.

Теорема 5.9.1. *Пусть G — полупростая группа и $E = \mathbb{R} \otimes_{\mathbb{Z}} X(T)$. Тогда Φ — абстрактная система корней в пространстве E, ранг которой совпадает с рангом группы G и абстрактная группа Вейля совпадает с $W = W(G,T) = N_G(T)/T$.*

Доказательство. Аксиомы A1 и A2 очевидны. Аксиома A3 следует из действия группы Вейля на корневой системе Φ, определённом в упражнении 5.6.10 и после него. Аксиома A4 следует из упражнения 5.7.4. Заметим, что в силу леммы 5.3.6 ядро присоединённого представления редуктивной группы совпадает с её центром. Поскольку корни являются весами относительно присоединённого представления, лемма 5.8.3 влечёт, что $\mathfrak{g}_\beta^{U_\alpha} \leq \sum_{k \in \mathbb{N} \cup \{0\}} \mathfrak{g}_{\beta+k\alpha}$ и $\mathfrak{g}_\beta^{U_{-\alpha}} \leq \sum_{k \in \mathbb{N} \cup \{0\}} \mathfrak{g}_{\beta-k\alpha}$. Поскольку Z_α порождается тором T и группами $U_\alpha, U_{-\alpha}$, причём T нормализует $\mathfrak{g}_\beta$, мы получаем, что для любого $x \in Z_\alpha$ справедливо $\mathfrak{g}_\beta^x \leq \sum_{k \in \mathbb{Z}} \mathfrak{g}_{\beta+k\alpha}$. Поскольку представитель n_α элемента $\sigma_\alpha \in W$ лежит в группе Z_α, мы получаем, что $\mathfrak{g}_\alpha^{n_\alpha} = \mathfrak{g}_{(\beta)\sigma} = \mathfrak{g}_{\beta+k\alpha}$ для некоторого $k \in \mathbb{Z}$, откуда следует аксиома A5. □

Напомним, что любая корневая система Φ содержит набор фундаментальных корней Π, причём любой корень из Φ является целочисленной комбинацией корней из Π, все коэффициенты которой либо неположительны, либо неотрицательны. Более того (см. лемму 2.1.9) любой корень из $r \in \Phi$ является образом некоторого фундаментального корня $p \in \Pi$ относительно некоторого $w \in W$, т. е. $p^w = r$. В частности, справедлива следующая

Лемма 5.9.2. *Пусть G — связная редуктивная группа, тогда G порождается группами Z_α, $\alpha \in \Pi$ или, что равносильно, тором T и всеми группами $U_{\pm\alpha}$, $\alpha \in \Pi$.*

Поскольку любой корень корневой системы Φ представим в виде целочисленной комбинации фундаментальных корней, все коэффициенты которой либо неотрицательны, либо неположительны, мы получаем разбиение корневой системы Φ на множество положительных и множество отрицательных корней. Обратно, если мы зададим какое-нибудь разбиение корневой системы Φ на множество положительных и отрицательных корней, согласованное со сложением, то мы получим фундаментальную систему корней, соответствующую этому разбиению (см. лемму 2.1.3). Таким образом, взяв произвольный $\lambda \in Y(T)_{reg}$, мы получаем множество положительных корней Φ^+ как $\{\alpha | <\alpha, \lambda >> 0\}$, т. е. если $B = B(\lambda)$, то $\Phi^+ = \{\alpha | \mathfrak{g}_\alpha \leq \mathfrak{L}(B)\} = \{\alpha | \alpha \in \Phi(B, T)\}$. Следовательно, зафиксировав некоторую подгруппу Бореля $B \in \mathfrak{B}^T$, мы таким образом однозначно задаём связанный с ней набор фундаментальных корней.

Далее мы рассмотрим группу автоморфизмов полупростой алгебраической группы и покажем, что полупростая алгебраическая группа является центральным произведением своих простых компонент. Пусть $\mathrm{Aut}G$ — группа автоморфизмов полупростой группы G, $\mathrm{Inn}G$ — группа её внутренних автоморфизмов. Обозначим за D подгруппу группы $\mathrm{Aut}G$, состоящую из автоморфизмов, оставляющих инвариантными некоторый фиксированный максимальный тор T и некоторую фиксированную, содержащую его подгруппу Бореля B. Пусть, кроме того, Γ обозначает группу симметрий диаграммы Дынкина корневой системы Φ.

Как отмечалось выше, фиксируя подгруппу Бореля B, мы получаем некоторый набор фундаментальных корней Π корневой системы Φ. Поскольку для любого $\sigma \in \mathrm{D}$ выполнено $T\sigma = T$, мы получаем, что σ индуцирует автоморфизм $\hat{\sigma}$ корневой системы Φ. Кроме того, поскольку $B^\sigma = B$, то и $\Pi^\sigma = \Pi$, т. е. $\hat{\sigma} \in \Gamma$. Отображение $\sigma \mapsto \hat{\sigma}$, очевидно, является гомоморфизмом групп $\mathrm{D} \to \Gamma$. В ведённых выше обозначениях справедлива следующая теорема.

Теорема 5.9.3. *Пусть G — полупростая группа. Тогда*

(а) $\mathrm{Aut}G = (\mathrm{Inn}G)D$*;*

(б) *естественное отображение* $\mathrm{D} \to \Gamma$ *индуцирует мономорфизм (на самом деле изоморфизм, мы докажем это позже)* $\mathrm{Aut}G/\mathrm{Inn}G \to \Gamma$*, в частности, группа* $\mathrm{Inn}G$ *имеет конечный индекс в* $\mathrm{Aut}G$*.*

Доказательство. (а) Пусть $\sigma \in \mathrm{Aut}G$. Ввиду сопряжённости борелевских подгрупп, существует такой $x \in G$, что $B^{x^{-1}} = B^\sigma$, т. е. $B^{\sigma \mathrm{Int}x} = B$. Кроме того, в силу сопряжённости максимальных торов, существует такой $y \in B$, что $T^{y^{-1}} = T^{\sigma \mathrm{Int}x}$, т. е. $B^{\sigma \cdot \mathrm{Int}x \cdot \mathrm{Int}y} = B$ и $T^{\sigma \cdot \mathrm{Int}x \cdot \mathrm{Int}y} = T$.

(б) Ввиду утверждения (а) достаточно доказать, что $\mathrm{Inn}G \cap \mathrm{D}$ совпадает с ядром гомоморфизма $\mathrm{D} \to \Gamma$. Действительно, если $\mathrm{Int}x \in \mathrm{D}$, то $x \in N_G(B) = B$ (см. теорему 5.5.10) и $x \in N_B(T) = C_B(T) = T$ (см. следствия 5.4.5 и 5.7.8). В частности, $\mathrm{Int}x$ индуцирует тождественный автоморфизм корневой системы Φ.

Обратно, пусть $\sigma \in \mathrm{D}$ индуцирует на Φ тождественное отображение. Нам нужно доказать, что σ — внутренний автоморфизм. Для каждого $\alpha \in \Pi$ выберем автоморфизм $\varepsilon_\alpha : \mathbb{F} \to U_\alpha$ (как в теореме 5.8.2(в)). Тогда $U_\alpha^\sigma = U_\alpha$, следовательно, существует такой $c_\alpha \in \mathbb{F}^*$, что $(x^{\varepsilon_\alpha})^\sigma = (c_\alpha x)^{\varepsilon_\alpha}$ для всех $x \in K$ (напомним, что $\mathrm{Aut}\mathbb{F} = \mathrm{GL}_1(\mathbb{F}) = \mathbb{F}^*$). В силу линейной независимости множества Π лемма 5.2.8 влечёт существование $t \in T$, для которого $t^\alpha = c_\alpha$ для всех $\alpha \in \Pi$. Заменяя σ на $\sigma \mathrm{Int}t^{-1}$ мы можем считать, что $c_\alpha = 1$ для всех $\alpha \in \Pi$, т. е. σ централизует каждую из U_α, $\alpha \in \Pi$. Кроме того, очевидно, что $(t^\sigma)^\alpha = t^\alpha$ для любого $t \in T$. Ввиду следствия 5.7.9(е), множество Π порождает подгруппу конечного индекса в $X(T)$, поэтому гомоморфизм $t \mapsto t^\sigma t^{-1}$ имеет конечный и связный образ, т. е. $t^\sigma = t$ для всех $t \in T$. В частности, элемент σ оставляет неподвижной любую подгруппу Z_α, $\alpha \in \Pi$. Кроме того, он централизует её подгруппу Бореля TU_α, следовательно, по лемме 5.4.10, автоморфизм σ централизует Z_α при $\alpha \in \Pi$. Так как $G = \langle Z_\alpha | \alpha \in \Pi \rangle$, то мы получаем, что σ — тривиальный автоморфизм. □

Пусть, по прежнему, G — полупростая группа. Любая замкнутая связная нормальная подгруппа группы G также является полупростой. Действительно, её радикал является характеристической подгруппой, следовательно, нормальной подгруппой группы G.

Теорема 5.9.4. *Пусть G — полупростая группа, и пусть $\{G_i | i \in I\}$ — минимальные замкнутые связные нормальные подгруппы положительной размерности. Тогда*

(а) *если $i \neq j$, то $[G_i, G_j] = \{e\}$;*

(б) *множество I конечно (скажем, $I = \{1, \ldots, n\}$) и морфизм произведения $G_1 \times \ldots \times G_n \to G$ сюръективен и имеет конечное ядро;*

(в) *произвольная замкнутая связная нормальная подгруппа группы G является произведением содержащихся в ней подгрупп G_i и централизует остальные G_j;*

(г) $G = [G, G]$;

(д) *G порождается группами $U_{\pm\alpha}$, $\alpha \in \Pi$.*

Доказательство. (а) По лемме 5.1.2 мы получаем, что $[G_i, G_j]$ — связная нормальная подгруппа группы G, содержащаяся как в G_i, так и в G_j. Ввиду минимальности групп G_i, G_j, она равна $\{e\}$.

(б) Пусть $J = \{i_1, \dots, i_r\} \subseteq I$. Поскольку $[G_i, G_j] = \{e\}$ при $i \neq j$, мы получаем, что морфизм произведения $\pi : G_{i_1} \times \ldots \times G_{i_r} \to G$ является морфизмом алгебраических групп. В частности, $G_{i_1} \cdot \ldots \cdot G_{i_r}$ — замкнутая связная нормальная подгруппа группы G. Как мы заметили выше, она является полупростой. Из (а) следует, что любая G_i, $i \notin J$ централизует $G_{i_1} \cdot \ldots \cdot G_{i_r}$, значит, $G_i \cap G_{i_1} \cdot \ldots \cdot G_{i_r} \leq Z(G_{i_1} \cdot \ldots \cdot G_{i_r})$, а $Z(G_{i_1} \cdot \ldots \cdot G_{i_r})$ конечен. Следовательно, ядро $\mathrm{Ker}(\pi)$ конечно. Поскольку размерность группы G конечна, мы получаем, что I конечно и равно $\{1, \dots, n\}$. Пусть $H = G_1 \cdot \ldots \cdot G_n$, покажем, что $G = H$.

Действительно, H — нормальная подгруппа группы G, потому действие группы G на H сопряжениями задаёт гомоморфизм $\psi : G \to \mathrm{Aut} H$, причём $H^\psi = \mathrm{Inn} H$. Поскольку группа H полупроста, теорема 5.9.3 влечёт, что $|\mathrm{Aut} H : \mathrm{Inn} H| < \infty$. Ввиду связности группы G мы получаем, что $G^\psi = \mathrm{Inn} H = H^\psi$. Пусть $C = \mathrm{Ker}(\psi)^0$. Тогда CH — подгруппа группы G конечного индекса, т. е. $CH = G$. Кроме того, $C \trianglelefteq G$, следовательно, C — полупростая группа. Её минимальные замкнутые связные нетривиальные подгруппы централизуют H и, значит, нормальны в G. По построению, они лежат в множестве $\{G_1, \dots, G_n\}$, т. е. $C = \{e\}$.

(в) Пусть H — произвольная замкнутая связная нормальная подгруппа группы G и $H \neq \{e\}$. Как показывают предыдущие рассуждения, любая из подгрупп $G_1, \dots, G_n$ либо централизует H, либо лежит в H, откуда следует, что минимальные нормальные связные подгруппы группы H совпадают с некоторыми из G_i.

(г) Коммутант группы G является нормальной подгруппой в G. Поскольку каждая из G_i некоммутативна (так как её центр конечен), то $[G_i, G_i] = G_i$, откуда $[G, G] = G$.

(д) Так как группа G порождена группами T и $U_{\pm\alpha}$, $\alpha \in \Pi$ (см. лемму 5.9.2), то группа H, порождённая только группами U_α, замкнута, связна и нормальна в G, причём $G/H \simeq T/(T \cap H)$, т. е. абелева. Поскольку $[G, G] = G$, отсюда следует, что $G = H$. □

***Упражнение* 5.9.5.** Пусть G — связная редуктивная группа, H — её замкнутая нормальная подгруппа, T — максимальный тор группы G. Тогда $T \cap H$ — максимальный тор группы H.

Рассмотрим теперь $\Phi_1, \dots \Phi_k$ — неразложимые подсистемы корневой системы Φ. Тогда $\Phi = \Phi_1 \cup \ldots \cup \Phi_k$ и если α, β — корни из разных неразложимых подсистем, то $\alpha + k\beta \notin \Phi$ для любого $k \in \mathbb{Z}$. Ввиду леммы 5.8.3 мы получаем, что $\mathfrak{g}_\beta^{\mathrm{Int} U_{\pm\alpha}} = \mathfrak{g}_\beta$, т. е. $U_{\pm\alpha}$ оставляет инвариантным одномерное пространство $\mathfrak{g}_\beta$. Поскольку группа $U_{\pm\alpha}$ унипотентна, это значит, что $U_{\pm\alpha}$ централизует $\mathfrak{g}_\beta$, следовательно, централизует U_β. С другой стороны, если α, β — неортогональные корни, то $\beta^{w_\alpha} \neq \beta$, следовательно, группа Z_α не нормализует U_β, значит, либо U_α, либо $U_{-\alpha}$ не нормализует β. Рассмотрим $H_i = \langle U_\alpha | \alpha \in \Phi_i \rangle$. В силу сказанного выше, $[H_i, H_j] = \{e\}$ при $i \neq j$, следовательно, H_i — замкнутая связная нормальная подгруппа группы G. Ввиду утверждения (в) теоремы 5.9.4, мы получаем, что она является произведением некоторых из G_i. Как мы заметили выше, корни $\Phi(G_l)$ ортогональны корням из $\Phi(G_j)$, поэтому, из неразложимости $\Phi(H_i) = \Phi_i$ следует, что $H_i = G_l$ для подходящего l. Таким образом, доказана следующая

Лемма 5.9.6. *Разложение полупростой группы $G = G_1 \cdot \ldots \cdot G_n$ соответствует разложению корневой системы $\Phi = \Phi_1 \cup \ldots \cup \Phi_n$ в объединение неразложимых подсистем.*

Как следует из теоремы 5.9.4, каждая из G_i некоммутативна, имеет конечный центр и не имеет собственных нормальных подгрупп ненулевой размерности. Такие группы мы будем называть *простыми алгебраическими группами.* Из леммы 4.3.1(г) следует, что каждая конечная нормальная подгруппа связной алгебраической группы центральна, поэтому, если G — простая связная алгебраическая группа, то $G/Z(G)$ является простой уже как абстрактная группа. Группы, удовлетворяющие условиям $G = [G, G]$ и $G/Z(G)$ простая называют *квазипростыми группами*, таким образом, простая алгебраическая группа всегда является квазипростой.

Глава 6. BN-пары и изоморфизм

В настоящей главе мы продолжим изучение свойств связных редуктивных линейных алгебраических групп, используя свойства их корневых систем. В частности, мы докажем, что корневая система определяет связную полупростую линейную алгебраическую группу с точностью до конечного центра. Далее везде в главе, если не оговорено противное, алгебраическая группа предполагается связной. Кроме того, мы изучим группы с BN-парами (или с системой Титса), получим критерий простоты таких групп и докажем, что линейные редуктивные алгебраические группы обладают BN-парой. Далее мы построим разложение Брюа произвольного элемента и докажем его единственность. Используя это разложение, мы изучим автоморфизмы полупростых линейных алгебраических групп и строение централизаторов полупростых элементов.

§1 Группы с BN-парой

Наше изложение в основном следует [3, Глава 8] и [11, 1.6]. Доказательство критерия простоты группы с BN-парой взято из [3, Теорема 11.1.1].

Определение 6.1.1. Пусть G — группа. Говорят, что G является *группой с BN-парой* или *группой с системой Титса*, если в группе G существуют такие подгруппы B и N, что выполнены следующие условия:

(BN1) группа G порождается подгруппами B и N;

(BN2) $B \cap N = H \trianglelefteq N$ и факторгруппа $W = N/H$ является конечной группой, порождённой множеством S инволюций (т. е. элементов порядка 2);

(BN3) если $s \in S$ и n_s — представитель смежного класса s в N, то $n_s B n_s \neq B$;

(BN4) $n_s B n \subseteq B n_s n B \cup B n B$ для любых $s \in S, n \in N$;

Если кроме этого ещё выполнена *аксиома полноты*:

(BN5) $\bigcap_{n \in N} B^n = H$,

то BN-пара называется *полной* или *насыщенной*. Группа W называется *группой Вейля* группы G.

Далее для любого $w \in W$ через n_w обозначен представитель смежного класса элемента w в N. Поскольку $H = B \cap N$, то многие свойства и, в частности, аксиомы BN3 и BN4 не зависят от выбора представителя. Определим функцию длины на W следующим образом: $l(e) = 0$ и если $w \neq e$, то $l(w)$ — минимальная возможная длина выражения элемента w в виде произведение порождающих элементов из S. Позже мы докажем, что W для линейной алгебраической группы совпадает с группой Вейля, определённной ранее, а множество порождающих элементов S совпадает с отражениями в фундаментальных корнях. Поэтому для обозначения длины элемента из группы Вейля мы используем то же обозначение, что и в главе 2. Если $l(w) = k$, то выражение $w = s_1 \cdot \ldots \cdot s_k$, где все $s_i \in S$ называется *приведённым*. Заметим, что данное определение отличается от определения приведённого выражения в §7 главы 2 тем, что здесь в качестве порождающего множества используются отображения в фундаментальных корнях (а не во всех корнях). Ясно также, что приведённое выражение определено, вообще говоря, не единственным образом.

Лемма 6.1.2. *Пусть $J \subseteq S$ и определим $W_J = \langle s | s \in J \rangle \leq W$. Пусть $N_J \leq N$ — прообраз группы W_J в N относительно естественного гомоморфизма $N \to W$.*

Тогда $P_J = BN_JB$ является подгруппой группы G. В частности, $G = BNB$.

Доказательство. Поскольку множество P_J замкнуто относительно взятия обратного элемента, достаточно проверить лишь замкнутость по умножению. Очевидно, что $BP_J \subseteq P_J$, так что надо показать, что $N_J P_J \subseteq P_J$. Далее $N_J = \langle H, \{n_s | s \in J\} \rangle$, так что достаточно показать лишь, что $n_s P_J \subseteq P_J$ для всех $s \in J$. Но это очевидно из аксиомы BN4. $\square$

Теорема 6.1.3. (разложение Брюа) *Пусть G — группа с BN-парой. Тогда справедливо следующее разложение в непересекающееся объединение двойных смежных классов:*

$$G = \bigcup_{w \in W} B n_w B.$$

Более того, для данных $s \in S$, $w \in W$ выполнено $l(sw) = l(w) \pm 1$ и

$$Bn_sB \cdot Bn_wB = \begin{cases} Bn_s n_w B, & \text{если } l(sw) = l(w) + 1, \\ Bn_s n_w B \cup Bn_w B, & \text{если } l(sw) = l(w) - 1. \end{cases}$$

Доказательство. Ввиду леммы 6.1.2 мы получаем, что $G = BNB$, откуда $G = \bigcup_{w \in W} Bn_wB$. Пусть теперь $v, w \in W$, надо показать, что $Bn_vB = Bn_wB$ влечёт $v = w$. Докажем утверждение индукцией по $\min\{l(v), l(w)\}$. Без ограничения общности можно считать, что $l(v) \leqslant l(w)$. Далее, если $l(v) = 0$, то $y = e$ и, значит, $B = Bn_vB = Bn_wB$, откуда $n_w \in B \cap N = H$. Предположим теперь, что $l(v) > 0$. Тогда мы можем записать $v = sx$, где $s \in S$ и $l(v) = l(x) + 1$. Тогда мы имеем $n_s n_x B \subseteq Bn_vB = Bn_wB$, значит, используя аксиому BN4,

$$n_x B \subseteq n_s B n_w B \subseteq B n_s n_w B \cup B n_w B.$$

Поскольку $n_s^2 \in B$, мы получаем, что $Bn_xB = Bn_sn_wB$ или $Bn_xB = Bn_wB$. По индукции мы имеем $x = sw$ или $x = w$. Второй случай невозможен, поскольку $l(x) < l(v) \leqslant l(w)$. Таким образом, $v = sx = w$.

Рассмотрим теперь правило умножения. Пусть $s \in S$ и $w \in W$. Заметим сначала, что, очевидно, $l(w) - 1 \leqslant l(sw) \leqslant l(w) + 1$. Индукцией по $l(w)$ легко показать, что если $l(sw) \neq l(w)$ для всех $s \in S$. Поэтому либо $l(w) = l(sw) + 1$, либо $l(w) = l(sw) - 1$.

Предположим, что $l(sw) \geqslant l(w)$. Покажем индукцией по $l(w)$, что $Bn_sBn_wB = Bn_sn_wB$. Если $l(w) = 0$, то $w = e$ и доказывать нечего. Предположим, что $l(w) > 0$ и запишем $w = yt$, где $t \in S$ и $y \in W$ таковы, что $l(w) = l(y) + 1$. По аксиоме BN4 мы имеем, что либо $Bn_sB \cdot Bn_wB = Bn_sn_wB$, либо $n_sBn_w \cap Bn_wB \neq \varnothing$. Предположим, что выполнен второй случай. Тогда $n_sBn_y \cap Bn_wBn_t \neq \varnothing$. Далее $l(sy) \geqslant l(y)$ и, значит, по индукции, справедливо $n_sBn_y \subseteq Bn_sn_yB$, откуда $Bn_sn_yB \cap Bn_wBn_t \neq \varnothing$. Переходя к обратным элементам в аксиоме BN4, мы получаем, что справедлив её «правосторонний» аналог:

$$nBn_s \subseteq Bnn_sB \cup BnB \text{ для любых } s \in S, n \in N.$$

Это означает, что $Bn_sn_yB \cap Bn_wn_tB \neq \varnothing$ или $Bn_sn_yB \cap Bn_wB \neq \varnothing$. Ввиду первой части доказательства, $sy = wt$, либо $sy = w$. Первое равенство даёт $sy = yt^2 = y$, и, значит, $s = 1$, что противоречит аксиоме BN3. Второе равенство даёт $sw = y$ и, значит, $l(sw) = l(y) < l(w)$, противоречие. Таким образом, наше предположение неверно и $Bn_sB \cdot Bn_wB = Bn_sn_wB$, как и требовалось.

Предположим теперь, что $l(sw) \leqslant l(w)$. Ввиду аксиомы BN4, выполнено $n_sBn_s \subseteq B \cup Bn_sB$. Используя аксиому BN3, это влечёт, что $n_sBn_s \cap Bn_sB \neq \varnothing$. Следовательно, также и $n_sB \cap Bn_sBn_s \neq \varnothing$ и $n_sBn_w \cap Bn_sBn_sn_w \neq \varnothing$. Теперь мы имеем, что $l(ssw) = l(w) \geqslant l(sw)$ и значит, $Bn_sBn_sn_w = Bn_wB$, по предыдущему случаю. Это означает, что $n_sBn_w \cap Bn_wB \neq \varnothing$. С другой стороны, очевидно, что $n_sn_w \in Bn_sn_wB$, что даёт требуемое равенство. $\square$

Точная формула умножения, полученная в теореме 6.1.3 имеет ряд важных следствий. Подгруппа P группы G, содержащую B^g для некоторого $g \in G$, называется *параболической*. Например, подгруппы P_J, определённые в лемме 6.1.2, являются параболическими. Мы покажем, что любая параболическая подгруппа группы G сопряжена с некоторой P_J и, более того, P_I и P_J сопряжены в том и только в том случае, когда $I = J$.

Лемма 6.1.4. *Пусть G — группа с BN-парой и $n \in N$. Пусть w — образ элемента n относительно естественного гомоморфизма $N \to W$ и $w = s_1 \cdot \ldots \cdot s_k$ — приведённое разложение элемента w. Обозначим за $J = \{s_1, \ldots, s_k\} \subseteq S$.*

Тогда группы $\langle B, n \rangle$, $\langle B, B^n \rangle$, P_J совпадают.

Доказательство. Поскольку $n = n_{s_1} \cdot \ldots \cdot n_{s_k}$, то $n \in W_J$ и, значит, справедливы включения $\langle B, B^n \rangle \leq \langle B, n \rangle \leq P_J$. Теперь $P_J = \langle B, n_{s_1}, \ldots, n_{s_k} \rangle$. Поскольку $l(s_1 w) < l(w)$, теорема 6.1.3 влечёт, что $n_{s_1}Bn \cap BnB \neq \varnothing$, откуда $n_{s_1} \in \langle B, B^n \rangle$. Аналогично $n_{s_2} \in \langle B, B^{n_s n} \rangle = \langle B, B^n \rangle$, откуда $n_{s_1}, \ldots, n_{s_k} \in \langle B, B^n \rangle$ и $P_J \leq \langle B, B^n \rangle$. $\square$

Следствие 6.1.5. *Множество S — это множество таких элементов w из W, что $B \cup BwB$ является подгруппой группы G. В частности, множество S определено однозначно.*

Лемма 6.1.6. *Пусть G — группа с BN-парой. Тогда подгруппы P_J — единственные подгруппы группы G, содержащие B.*

Доказательство. Пусть M — подгруппа группы G, содержащая B. Тогда подгруппа M является объединением двойных смежных классов по B группы G и по теореме 6.1.3, каждый такой двойной смежный класс содержит элемент из N. Таким образом, M порождается подгруппой B и некоторым множеством элементов из N. Пусть $n_\alpha \in N \cap M$. По лемме 6.1.4, $\langle B, n_\alpha \rangle = P_{J_\alpha}$ для подходящего подмножества J_α множества S. Значит, $M = P_J$, где $J = \cup J_\alpha$. □

Лемма 6.1.7. *Пусть G — группа с BN-парой. Тогда $N_G(P_J) = P_J$ для любого $J \subseteq S$. Более того, различные подгруппы P_J, P_K не могут быть сопряжены в G.*

Доказательство. Поскольку $N_G(P_J)$ содержит B, лемма 6.1.6 влечёт, что $N_G(P_J)$ порождается подгруппой B и некоторыми из элементов из N. Пусть $n \in N \cap N_G(P_J)$. Тогда по лемме 6.1.4 выполнено $P_J \geq \langle B, B^n \rangle = \langle B, n \rangle$, т. е. $n \in P_J$ и $P_J = N_G(P_J)$.

Предположим, что P_J и P_K сопряжены в G. Пусть $P_J^g = P_K$, где $g = b_1 n b_2$ и $b_1, b_2 \in B$, $n \in N$. Тогда $P_J^n = P_K$, значит, $P_K \geq \langle B, B^n \rangle = \langle B, n \rangle$ и $P_J = P_K$. □

Лемма 6.1.8. *Множество S является минимальным множеством порождающих группы W.*

Доказательство. Предположим, что можно удалить некоторый элемент $s \in S$ таким образом, что $\overline{S} = S \backslash \{s\}$ по прежнему порождает W. Тогда группа G является группой с BN-парой, в которой вместо множества S взято множество $\overline{S}$. Рассмотрим $s = s_1 \cdot \ldots \cdot s_k$ — приведённое выражение для s, в котором все $s_i \in \overline{S}$. Пусть n — представитель смежного класса s в N и пусть $J = \{s_1, \ldots, s_k\}$. По лемме 6.1.4 мы получаем, что $\langle B, n \rangle = P_J$. Ввиду разложения Брюа, мы получаем, что $\langle B, n \rangle = B \cup BnB$ и, с другой стороны, $P_J \supseteq B \cup Bn_{s_1}B \cup \ldots \cup Bn_{s_k}B$, противоречие. □

Теорема 6.1.9. *Пусть G — группа с BN-парой. Тогда подгруппы P_I, P_J совпадают в том и только в том случае, если $I = J$. Более того, $P_I \cap P_J = P_{I \cap J}$. Поскольку $\langle P_I, P_J \rangle = P_{I \cup J}$, отсюда следует, что подгруппы P_I образуют решётку, изоморфную решётке подмножеств множества I.*

Доказательство. Пусть I, J — подмножества множества S. Поскольку $P_I \cap P_J$ является подгруппой группы G, содержащей B, то лемма 6.1.6 влечёт, что существует такое $K \subseteq S$, что $P_K = P_I \cap P_J$. Очевидно, что $P_{I \cap J} \leq P_K$. Предположим, что $P_{I \cap J} \neq P_K$. Тогда K не содержится либо в I, либо в J, можно считать, что K не содержится в J. Однако, $P_K \leq P_J$ и, значит, разложение Брюа влечёт $N_K \leq N_J$. Следовательно, $W_K \leq W_J$. Пусть $s \in K \backslash L$. Тогда $s \in W_K$ и поэтому $s \in W_J$. Но это значит, что s выражается через элементы из $S \setminus \{s\}$, что противоречит лемме 6.1.8.

Предположим теперь, что $P_J = P_I$. Если $J \neq I$, то $J \setminus I \neq \varnothing$. Поскольку $P_J = P_J \cap P_I = P_{J \cap I}$, мы получаем, что $W_J = W_{J \cap I}$, что опять влечёт противоречие с леммой 6.1.8. □

***Упражнение* 6.1.10.** Пусть G — связная редуктивная алгебраическая группа, H — её максимальный тор, B — подгруппа Бореля группы G, содержащая тор H и $N = N_G(H)$. Доказать, что подгруппы B и N образуют BN-пару группы G.

В заключение параграфа мы сформулируем критерий простоты групп с BN-парой.

Теорема 6.1.11. *Пусть G — группа с BN-парой, удовлетворяющая следующим условиям:*

(а) $G = [G, G]$;

(б) *B разрешима;*

(в) $\bigcap_{g \in G} B^g = \{e\}$;

(г) *множество S нельзя разложить на такие два непустые подмножества I, J, что каждый элемент из I коммутирует с любым элементом из J.*

Тогда G проста.

Доказательство. Пусть G_1 — нормальная подгруппа группы G. Тогда G_1B — подгруппа группы G, содержащая B и, по лемме 6.1.6, совпадает с P_J для некоторого $J \subseteq S$. Пусть $I = S \setminus J$ и $s \in J$, $t \in I$. Тогда $l(st) > l(s)$, поэтому теорема 6.1.3 влечёт, что $Bn_sB \cdot Bn_tB = Bn_sn_tB$. Далее, поскольку $G_1B = P_J = BN_JB$, значит, $Bn_sB \cap G_1 \neq \varnothing$. Поскольку G_1 нормальна в G, то $n_tBn_sBn_t \cap G_1 \neq \varnothing$. Однако, по аксиоме BN4, мы имеем $n_tBn_sBn_t \subseteq n_tBn_sn_tB \subseteq Bn_sn_tB \cup Bn_tn_sn_tB$. Таким образом, либо $Bn_sn_tB \cap G_1 \neq \varnothing$, либо $Bn_tn_sn_tB \cap G_1 \neq \varnothing$.

Первое неравенство влечёт, что $n_sn_t \in N_J$, значит, $n_t \in N_J$ и $t \in W_J$, что противоречит лемме 6.1.8. Следовательно, мы имеем $Bn_tn_sn_tB \cap G_1 \neq \varnothing$. Это значит, что $n_tn_sn_t \in N_J$. Поскольку $n_tn_sn_t \in N_{\{s,t\}}$, теорема 6.1.9 влечёт, что $n_tn_sn_t \in P_J \cap P_{\{s,t\}} = P_{\{s\}} = B \cup Bn_sB$. Значит, либо $tst = e$, либо $tst = s$. Первый случай невозможен, так как $s \neq e$ и $t^{-1} = t$. Во втором случае мы получаем, что для любого $s \in J$, $t \in I$ выполнено $st = ts$. В силу условия (г), это значит, что либо $J = \varnothing$, либо $I = \varnothing$.

Предположим, что $I = \varnothing$. Тогда $J = S$ и $G_1B = G$. Таким образом, $G/G_1 \simeq B/G_1 \cap B$ разрешима. По свойству (а), выполнено $G = [G, G]$, значит, $G = G_1$.

Предположим, что $J = \varnothing$. Тогда $G_1B = B$, поэтому $G_1 \leq B$. Поскольку G_1 нормальна в G, мы имеем $G_1 \leq \cap_{g\in G} B^g = \{e\}$. □

***Упражнение* 6.1.12.** Проверить, что условия (а), (в), (г) теоремы являются необходимыми.

§2 Расщепляемые BN-пары

В данном параграфе мы рассмотрим группы с расщепляемыми BN-парами и получим точную форму разложения Брюа. Наше изложение следует [11, 1.6]. Как и в предыдущем параграфе для $w \in W$ через n_w мы обозначаем некоторого представителя смежного класса w в N.

Лемма 6.2.1. *Пусть G — группа с BN-парой и W — её группа Вейля. Рассмотрим $w \in W$ и запишем $w = s_1 \cdot \ldots \cdot s_k$, где $s_i \in S$ и $k = l(w)$. Пусть $s \in S$ и предположим, что $l(sw) < l(w)$.*

Тогда $sw = s_1 \cdot \ldots \cdot s_{i-1} \cdot s_{i+1} \cdot \ldots \cdot s_k$ для некоторого $1 \leqslant i \leqslant k$.

Доказательство. По лемме 6.1.4 мы получаем, что $n_s \in Bn_wBn_w^{-1}B$. В силу точной формулы умножения, найденной в теореме 6.1.3, индукцией по $l(w)$ мы получаем, что

$$Bn_wBn_w^{-1}B = \bigcup_{1\leqslant i_1<\ldots<i_m\leqslant k, (0\leqslant m\leqslant k)} Bn_{s_{i_1}} \cdot \ldots \cdot n_{s_{i_m}} \cdot n_w^{-1}B.$$

Следовательно, $s = xw^{-1} = s_{i_1} \cdot \ldots \cdot s_{i_m} w^{-1}$ для некоторых $1 \leqslant i_1 < \ldots < i_m \leqslant k$. Вычислим xw^{-1}, умножая множители в этом выражении для x. Тогда на каждом шаге длина либо уменьшается, либо увеличивается на 1. В конце мы получаем, что $1 = l(s) = l(xw^{-1}) \geqslant k - m \geqslant 0$, откуда либо $m = k$, либо $m = k - 1$. В первом случае мы получаем, что $x = w$ и $s = e$, противоречие. Во втором случае мы получаем, что $x = s_1 \cdot \ldots \cdot s_{i-1}s_{i+1} \cdot \ldots \cdot s_k$, что и утверждалось. □

Лемма 6.2.2. *Пусть G — группа с BN-парой. Существует единственный элемент $w_0 \in W$ максимальной длины. Кроме того, w_0 единственным образом определяется свойством, что $l(sw) < l(w)$ для всех $s \in S$.*

Доказательство. Поскольку W конечна, существует такой элемент $w_0 \in W$, что $l(w)] \leqslant l(w_0)$ для всех $w \in W$. Докажем индукцией по $l(w)$, что для любого $w \in W$ справедливо

$$l(ww_0) = l(w_0) - l(w). \tag{6.1}$$

Если $l(w) = 0$, то $w = 1$ и доказывать нечего. Предположим теперь, что $l(w) = k + 1$, где $k \geqslant 0$ и запишем $w = s_1 \cdot \ldots \cdot s_k \cdot s$, где $s, s_i \in S$. Тогда, по индукции, $m = l(s_1 \cdot \ldots \cdot s_kw_0) = l(w_0) - k$. Рассмотрим теперь приведённое выражение $s_1 \cdot \ldots \cdot s_k \cdot w_0 = t_1 \cdot \ldots \cdot t_m$, где $t_j \in S$. Тогда $w_0 = s_1 \cdot \ldots \cdot s_k \cdot t_1 \cdot \ldots \cdot t_m$ — приведённое выражение для w_0. Поскольку $l(sw_0) < l(w_0)$, лемма 6.2.1 влечёт, что либо $sw_0 = s_k \cdot \ldots \cdot s_{i+1} \cdot s_{i-1} \cdot \ldots \cdot s_1 \cdot t_1 \cdot \ldots \cdot t_m$ для некоторого $1 \leqslant i \leqslant k$, либо $sw_0 = s_k \cdot \ldots \cdot s_1 \cdot t_1 \cdot \ldots \cdot t_{j-1} \cdot t_{j+1} \cdot \ldots \cdot t_m$ для некоторого $1 \leqslant j \leqslant m$.

В первом случае мы получаем, что $ss_k \cdot \ldots \cdot s_1 = s_k \cdot \ldots \cdot s_{i+1} \cdot s_{i-1} \cdot \ldots \cdot s_1$, откуда $l(w) = l(w^{-1}) \leqslant k - 1$, противоречие. Следовательно, выполнен второй случай и это значит, что $ww_0 = t_1 \cdot \ldots \cdot t_{j-1} \cdot t_{j+1} \cdot \ldots \cdot t_m$. Поэтому $l(ww_0) = m - 1 = l(w_0) - k - 1 = l(w_0) - l(w)$, что и утверждалось.

Далее, полагая $w = w_0$ мы получаем, что $l(w_0^2) = 0$ и, значит, $w_0^2 = e$. Пусть теперь $w \in W$ — другой элемент, для которого $l(w) = l(w_0)$. Вновь $l(ww_0) = 0$, откуда $w = w_0^{-1} = w_0$. Наконец предположим, что

$w \in W$ выбран так, чтобы $l(sw) < l(w)$ для всех $s \in S$. Предположим, что $l(w) < l(w_0)$. Тогда, в силу (6.1), выполнено $l(ww_0) = l(w_0) - l(w) > 0$ и, значит, $l(sww_0) < l(ww_0)$ для некоторого $s \in S$. Вновь применяя (6.1) мы получаем, что $l(sw) > l(w)$. $\square$

Лемма 6.2.3. *Пусть $s \in S$ и $w \in W$ выбраны так, что $l(sw) = l(w) + 1$. Тогда $n_sBn_s \cap Bn_wBn_w^{-1} \subseteq B$.*

Доказательство. Предположим, что утверждение леммы неверно. Тогда, поскольку $n_sBn_s \subseteq B \cup Bn_sB$, мы получаем, что $Bn_sB \cap Bn_wBn_w^{-1} \neq \varnothing$ и, значит, $Bn_sBn_w \cap Bn_wB \neq \varnothing$. Кроме того, аксиома BN4 влечёт, что $Bn_sBn_w \subseteq Bn_sn_wB \cup Bn_wB$, значит, $Bn_sBn_w \not\subseteq Bn_sn_wB$, что противоречит точной форме умножения, полученной в теореме 6.1.3. $\square$

Для удобства, далее мы будем использовать следующие обозначения: $B^w = B^{n_w}$ и $B_w = B \cap B^{n_{w_0w}}$, где $w \in W$.

Лемма 6.2.4. *Пусть $y, w \in W$ таковы, что $l(yw) = l(y) + l(w)$.*
Тогда $B \cap B^{yw} \subseteq B \cap B^w$. Более того, если BN-пара является насыщенной, то $B \cap B^{w_0} = H$.

Доказательство. Докажем индукцией по $l(y)$. При $l(y) = 0$ доказывать нечего. Предположим теперь, что $l(y) = 1$, тогда $y = s \in S$. По лемме 6.2.3 мы имеем

$$n_w(B \cap B^{sw})n_w^{-1} = n_w(B \cap n_w^{-1}n_s^{-1}Bn_sn_w)n_w^{-1} = n_wBn_w^{-1} \cap n_sBn_s \subseteq B$$

и, значит, $B \cap B^{sw} \subseteq B \cap B^w$. Предположим теперь, что $l(y) > 1$ и выберем такой $s \in S$, что $l(ys) < l(y)$. Положим $y' = ys$ и $w' = sw$. Тогда $yw = y'w'$ и $l(y'w') = l(y') + l(w')$. По индукции мы имеем, что $B \cap B^{yw} \subseteq B \cap B^{w'} = B \cap B^{sw}$. По уже доказанному, мы получаем $B \cap B^{sw} \subseteq B \cap B^w$, что и требовалось.

Рассмотрим теперь $B \cap B^{w_0}$. Пусть $y \in W$. В силу равенства (6.1) мы можем записать $w_0 = xy$, где $x \in W$ и $l(w_0) = l(x) + l(y)$. Тогда $B \cap B^{w_0} = B \cap B^{xy} \subseteq B^y$ выполнено для всех $y \in W$ и, значит, $B \cap B^{w_0} \subseteq \bigcap_{y \in W} B^y \subseteq \bigcap_{n \in N} B^n = H$ по аксиоме BN5. $\square$

Лемма 6.2.5. *Пусть $s \in S$ и $w \in W$ таковы, что $l(ws) = l(w) + 1$. Тогда справедливы следующие утверждения:*

(а) $B = B_s \cdot B_{w_0s} = B_{w_0s} \cdot B_s$ *и* $H \subsetneqq B_s$;

(б) $B_s \subseteq B_{w_0w}$;

(в) $B_{ws} = B_s \cdot B_w^s = B_w^s \cdot B_s$.

Доказательство. (а) Пусть $y = w_0s$, тогда по (6.1) мы имеем $l(ys) = l(y) + 1$ и, значит, $l(sy^{-1}) = l(y^{-1}) + 1$. Ввиду точной формулы умножения, полученной в разложении Брюа (теорема 6.1.3), справедливо $n_sBn_y^{-1} \subseteq Bn_sn_y^{-1}B$ и, значит, $B \subseteq n_s^{-1}Bn_sn_y^{-1}Bn_y = B^s \cdot B^y$.

Пусть $b \in B$. Тогда $b = b' \cdot b''$, где $b' \in B^s$ и $b'' \in B^y$. Далее $b' \in n_sBn_s \cap Bn_y^{-1}Bn_y \subseteq B$ (последнее включение следует из леммы 6.2.3) и, значит, b', b'' оба лежат в B. Следовательно, $B = (B \cap B^s) \cdot (B \cap B^y) = B_{w_0s} \cdot B_s$. Переходя в этом равенстве к обратным элементам, мы получаем, что $B = B_s \cdot B_{w_0s}$. Более того, очевидно, что $H \subseteq B_s$. Если $B_s = H$, то $B = B_{w_0s} = B \cap B^s$ и, значит, $n_sBn_s = B$, что противоречит аксиоме BN3.

(б) В силу равенства (6.1), мы можем записать $w_0 = yws$, где $y \in W$ выбран так, что $l(w_0) = l(y) + l(ws) = l(y) + l(w) + 1$. Тогда $w_0s = yw$, где $l(w_0s) = l(w_0) - 1 = l(y) + l(w)$, поэтому лемма 6.2.4 влечёт

$$B_s = B \cap B^{w_0s} = B \cap B^{yw} \subseteq B \cap B^w = B_{w_0w}.$$

(в) В силу (а) справедливо равенство $B = B_s \cdot B_{w_0s}$. Заметим, что $l(w_0wss) = l(w_0) - l(w) = l(w_0) - l(ws) + 1 = l(w_0ws) + 1$ и, значит, $B_s \subseteq B_{ws}$ (в силу (б)). Таким образом,

$$B_{ws} = B_{ws} \cap B = B_{ws} \cap B_s \cdot B_{w_0s} = B_sB_{ws} \cap B_sB_{w_0s} = B_s(B_{ws} \cap B_{w_0s}).$$

Осталось показать, что $B_{ws} \cap B_{w_0s} = B_w^s$. Заметим сначала, что

$$B_{ws} \cap B_{w_0s} = B \cap B^{w_0ws} \cap B^s = n_s^{-1}(B^s \cap B^{w_0w} \cap B)n_s = n_s^{-1}(B^s \cap B_w)n_s.$$

Далее $l(w_0ws) = l(w_0) - l(w) - 1 = l(w_0w) - 1$ и, значит, можно записать $w_0w = xs$, где $x \in W$ таков, что $l(xs) = l(x) + 1$. По лемме 6.2.4 отсюда следует, что $B_w = B \cap B^{w_0w} \subseteq B^s$. Следовательно, $B_{ws} \cap B_{w_0s} = n_s^{-1}B_wn_s$. $\square$

Лемма 6.2.6. *Пусть G — группа с насыщенной BN-парой. Тогда для любого $w \in W$ справедливо $B = B_w \cdot B_{w_0 w} = B_{w_0 w} \cdot B_w$.*

Доказательство. Покажем сначала, что выполнено следующее утверждение:

$$\text{Для любых } s \in S \text{ и } w \in W, \text{ для которых выполнено } l(sw) = l(w)+1, \text{ справедливо } B_{sw} = B_w \cdot B_s^w. \tag{6.2}$$

При $l(w) = 0$ мы имеем $w = e$ и, значит, по лемме 6.2.4 справедливо $B_e = B \cap B^{w_0} = H$. Таким образом, $B_s = B_e \cdot B_s$. Пусть теперь $l(w) > 0$ и выберем такой $t \in S$, что $l(wt) < l(w)$. Мы полагаем $y = wt$, тогда $sw = syt$ и $l(sy) = l(y) + 1$. Значит, $B_{sw} = B_{syt} = B_{sy}^t \cdot B_t$ (по лемме 6.2.5(в)), что, в свою очередь равно $n_t^{-1}(B_y \cdot B_s^y)n_t B_t = (B_s^y \cdot B_y)^t B_t$ по индукции. Отсюда, вновь применяя лемму 6.2.5(в), мы получаем $B_{sw} = B_s^{yt} \cdot B_y^t \cdot B_t = B_s^{yt} \cdot B_{yt} = B_s^w \cdot B_w$.

Докажем теперь разложение $B = B_w \cdot B_{w_0 w}$ индукцией по $l(w)$. Если $l(w) = 0$, то доказывать нечего. Предположим, что $l(w) > 0$ и запишем $w = sy$, где $s \in S$ и $y \in W$ таковы, что $l(sy) = l(y) + 1$. Используя (6.2), мы получаем $B_w \cdot B_{w_0 w} = B_{sy} \cdot B_{w_0 sy} = B_y \cdot B_s^y \cdot B_{w_0 sy}$. Заметим, что $B_{w_0 sy} = B \cap B^{sy} = B^{sy}_{w_0 (sy)^{-1}}$. Тогда, используя лемму 6.2.5(в) и индукцию мы получаем следующие равенства

$$B_w \cdot B_{w_0 w} = B_y \cdot B_s^y \cdot B^{sy}_{w_0(sy)^{-1}} = B_y \cdot n_y^{-1}(B_s \cdot B^s_{w_0(sy)^{-1}})n_y = B_y \cdot n_y^{-1} B_{w_0(sy)^{-1}s} n_y = B_y \cdot B^y_{w_0 y^{-1}}.$$

Теперь мы замечаем, что $B^y_{w_0 y^{-1}} = B_{w_0 y}$, т. е. $B_w \cdot B_{w_0 w} = B_y \cdot B_{w_0 y} = B$ □

***Упражнение* 6.2.7.** Показать, что лемма 6.2.6 справедлива для любой BN-пары (а не только для насыщенной BN-пары).

Определение 6.2.8. Пусть G — группа с BN-парой. Говорят, что BN-пара *расщепляема*, если существует такая нормальная подгруппа $U \trianglelefteq B$, что выполнены следующие условия.

(BNS1) Пусть $H = B \cap N$. Тогда $B = H \leftthreetimes U$.

(BNS2) Для любого $n \in N$ справедливо $U^n \leq U$.

Теорема 6.2.9. (точная форма разложение Брюа) *Пусть G — группа с насыщенной расщепляемой BN-парой. Положим $U_w = U \cap n_{w_0 w}^{-1} U n_{w_0 w} = U \cap B^{w_0 w}$ для всех $w \in W$ (очевидно, что w не зависит от выбора w, поскольку U нормальна в B).*

Тогда любой элемент $g \in Bn_wB$ записывается единственным образом в виде $g = bn_w u$, где $b \in B$, $u \in U_w$. Более того, $U_w \neq \{1\}$ для всех нееденичных $w \in W$.

Доказательство. Мы будем обозначать $U^w = U^{n_w}$ для всех $w \in W$. Покажем сначала, что $B_w = U_w H$ для всех $w \in W$. Действительно, поскольку $H \trianglelefteq N$ и $B = UH$, мы имеем $B \cap B^w = UH \cap U^w H \supseteq (U \cap U^w)H$. Осталось показать, что верно и обратное включение. Пусть $g \in B \cap B^w$. Тогда $g = n_w^{-1} u n_w h = u'h'$, где $u, u' \in U$ и $h, h' \in H$. Поскольку $g \in B$, то $u^{n_w} \in U^{n_w} \cap B \subseteq U$, по аксиоме 2 для расщепляемой BN-пары. Таким образом, по аксиоме 1 расщепляемой BN-пары, мы заключаем, что $u^{n_w} = u'$ и $h = h'$, значит, $g \in (U \cap U^w)H$. Заменяя теперь w на $w_0 w$, мы получаем, что $B_w = U_w H$.

Далее лемма 6.2.6 влечёт равенства $U = U_w \cdot U_{w_0 w} = U_{w_0 w} \cdot U_w$ для всех $w \in W$. Заметим также, что $n_w U_{w_0 w} n_w^{-1} = n_w (U \cap U^{n_w}) n_w^{-1} = n_w U n_w^{-1} \cap U \subseteq U$, следовательно, $Bn_wB = Bn_wHU = Bn_wU = Bn_wU_{w_0 w}U_w = Bn_wU_w$. Таким образом, разложение Брюа (теорема 6.1.3) влечёт, что G представима в виде непересекающегося объединения $G = \bigcup_{w \in W} Bn_wU_w$ и осталось доказать единственность разложения.

Пусть $g \in Bn_wU_w$ и запишем $g = bn_w u = b'n_w u'$, где $b, b' \in B$ и $u, u' \in U$. Тогда $n_w u(u')^{-1} n_w^{-1} = b^{-1}b' \in n_w(U \cap U^{w_0 w})n_w^{-1} \cap B \subseteq B \cap U^{w_0}$, поэтому достаточно показать, что $B \cap U^{w_0} = \{e\}$. По лемме 6.2.3 мы имеем $B \cap U^{w_0} \subseteq B \cap B^{w_0} = H$. В силу аксиомы 2 расщепляемой BN-пары, мы также имеем $B \cap U^{w_0} \subseteq U$ и, значит, это пересечение должно быть тривиальным.

Предположим, что $U_w = \{e\}$. Тогда мы имеем $B_w = H$. Если $w \neq e$, то существует такой $s \in S$, что $l(ws) = l(w) - 1$. По лемме 6.2.5 мы имеем $B_w = B_s \cdot B_{ws}^s \supseteq B_s \supsetneqq H$, противоречие. □

***Упражнение* 6.2.10.** Доказать, что отображение умножения $\mu : U_w \times U_{w_0 w} \to U$ является биекцией.

***Упражнение* 6.2.11.** Пусть $GF(q)$ — конечное поле из q элементов и $\mathrm{GL}_n(q)$ — группа всех невырожденных матриц степени n над этим полем. Доказать, что подгруппа треугольных матриц $B = \mathrm{T}_n(q)$ и подгруппа мономиальных матриц N группы $\mathrm{GL}_n(q)$ образуют расщепляемую насыщенную BN-пару и найти порядок группы $\mathrm{GL}_n(q)$, используя точную форму разложения Брюа.

§3 Группы Кокстера

Иногда группы Вейля параболических подгрупп удобно рассматривать как абстрактные группы Кокстера. В данном параграфе мы определим группы Кокстера и докажем теорему об их изоморфизме. Наше изложение следует [17, 29.4].

Пусть $\widehat{W}$ — абстрактная группа, порождённая элементами $\hat{s}_1, \ldots, \hat{s}_n$ и соотношениями $(\hat{s}_i\hat{s}_j)^{m_{ij}} = e$, причём $m_{ii} = 1$ для всех i и все m_{ij} конечны. Тогда группа $\widehat{W}$ назывется *группой Кокстера*. Пусть G — произвольная группа с BN-парой и пусть W — её группа Вейля, с множеством порождающих инволюций $s_1, \ldots, s_n$. Определим $m_{ij} = |s_is_j|$. В ведённых обозначениях справедлива следующая теорема.

Теорема 6.3.1. *Пусть m_{ij} — порядок элемента s_is_j в группе Вейля W и $\widehat{W}$ — группа Кокстера, порождённая элементами $\hat{s}_1, \ldots, \hat{s}_n$ и соотношениями $(\hat{s}_i\hat{s}_j)^{m_{ij}} = e$.*

Тогда гомоморфизм $\pi : \widehat{W} \to W$ является изоморфизмом.

Доказательство. Сюръективность гомоморфизма π очевидно, так что достаточно доказать инъективность.

Покажем сначала, что если $s_{i_1} \cdot \ldots \cdot s_{i_k}$, $s_{j_1} \cdot \ldots \cdot s_{j_k}$ — два приведённых разложения одного и того же элемента $s \in W$, то в группе $\widehat{W}$ выполнено равенство $\hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_k} = \hat{s}_{j_1} \cdot \ldots \cdot \hat{s}_{j_k}$. Доказательство будем вести индукцией по k. Для $k = 1$ утверждение тривиально. Поскольку $l(s_{j_1}s) = l(s) - 1 < l(s)$, то лемма 6.2.1 влечёт, что существует такое $m \leqslant k$, для которого $s_{j_1}s = s_{i_1} \cdot \ldots \cdot s_{i_{m-1}} \cdot s_{i_{m+1}} \cdot \ldots \cdot s_{i_k}$. По индукции мы имеем равенство $\hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_{m-1}} \cdot \hat{s}_{i_{m+1}} \cdot \ldots \cdot \hat{s}_{i_k} = \hat{s}_{j_2} \cdot \ldots \cdot \hat{s}_{j_k}$. Отсюда мы получаем равенство $\hat{s}_{j_1} \cdot \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_{m-1}} \cdot \hat{s}_{i_{m+1}} \cdot \ldots \cdot \hat{s}_{i_k} = \hat{s}_{j_1} \cdot \hat{s}_{j_2} \cdot \ldots \cdot \hat{s}_{j_k}$. Если при этом $m < k$, то применение индукции к элементу $s_{j_1} \cdot s_{i_1} \cdot \ldots \cdot s_{i_{m-1}} = s_{i_1} \cdot \ldots \cdot s_{i_m}$ даёт нам равенство $\hat{s}_{j_1} \cdot \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_{m-1}} = \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_m}$, откуда следует утверждение.

Таким образом, нам осталось доказать равенство $\hat{s}_{j_1} \cdot \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_{k-1}} = \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_k}$ (при условии, что верно равенство $s_{j_1} \cdot s_{i_1} \cdot \ldots \cdot s_{i_{k-1}} = s_{i_1} \cdot \ldots \cdot s_{i_k}$). Умножив обе части этого равенства на $\hat{s}_{i_1}$ слева и повторив те же рассуждения, что и выше, мы получаем, что либо равенство выполняется по индукции, либо достаточно доказать равенство $\hat{s}_{i_1} \cdot \hat{s}_{j_1} \cdot \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_{k-2}} = \hat{s}_{j_1} \cdot \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_{k-1}}$ (при условии, что верно равенство $s_{i_1} \cdot s_{j_1} \cdot s_{i_1} \cdot \ldots \cdot s_{i_{k-2}} = s_{j_1} \cdot s_{i_1} \cdot \ldots \cdot s_{i_{k-1}}$). Последовательно повторяя рассуждения мы получаем, что достаточно доказать равенства $\underbrace{\hat{s}_{i_1} \cdot \hat{s}_{j_1} \cdot \hat{s}_{i_1} \cdot \ldots}_{t\ \text{раз}} = \underbrace{\hat{s}_{j_1} \cdot \hat{s}_{i_1} \cdot \hat{s}_{j_1} \cdot \ldots}_{t\ \text{раз}}$ при условии выполнения аналогичных равенств в группе W. Но это последнее равенство, очевидно, эквивалентно утверждению $|\hat{s}_{i_1}\hat{s}_{j_1}| = |s_{i_1}s_{j_1}|$.

В силу доказанного утверждения, мы можем определить гомоморфизм $\varphi : W \to \widehat{W}$, правилом $\varphi : s_{i_1} \cdot \ldots \cdot s_{i_k} \mapsto \hat{s}_{i_1} \cdot \ldots \cdot \hat{s}_{i_k}$, где выражение $s_{i_1} \cdot \ldots \cdot s_{i_k}$ является приведённым. Очевидно, что композиция $\varphi\pi$ является тождественным отображением на W, откуда следует инъективность. □

§4 BN-пары в алгебраических группах

Основной задачей настоящего параграфа является проверка аксиом BN-пары в линейных алгебраических группах. Везде в данном параграфе предполагается, что G — связная редуктивная алгебраическая группа, B — её подгруппа Бореля, T — максимальный тор группы G, содержащийся в B, и $U = R_u(B)$ — унипотентный радикал группы G. По следствию 5.7.8 мы получаем, что $C_G(T) = T$, так что $C_U(T) = \{e\}$.

Мы будем говорить, что подмножество H группы G *прямо порождено* подмножествами $H_1, \ldots, H_k$ (в заданном порядке), если морфизм произведения $H_1 \times \ldots \times H_k \to H$ является биекцией.

Лемма 6.4.1. *Пусть H — замкнутая T-инвариантная подгруппа группы U. Тогда группа H связна и прямо порождена теми подгруппами U_α, для которых $\mathcal{L}(U_\alpha) = \mathfrak{g}_\alpha$ содержится в $\mathcal{L}(H) = \mathfrak{h}$ (при этом группы U_α можно взять в произвольном порядке).*

Доказательство. Пусть $\Psi = \Phi(H, T)$, т. е. $\mathfrak{h} = \bigoplus_{\alpha \in \Psi} \mathfrak{g}_\alpha$. Упорядочим Ψ произвольным образом, пусть $\Psi = \{\alpha_1, \ldots, \alpha_n\}$ и пусть $\pi : U_{\alpha_1} \times \ldots \times U_{\alpha_n} \to H$ — морфизм произведения. Заметим, что определение морфизма ψ корректно, поскольку при $\alpha \in \Psi$ группа U_α лежит в H (см. теорему 5.8.2). Покажем, что морфизм π биективен.

Предположим сначала, что группа H связна. Если, кроме того H коммутативна, то π является гомоморфизмом групп, причём $\mathrm{Ker}(\pi)$ конечно (поскольку π отображает U_{α_i} на U_{α_i}) и T-инвариантно (поскольку морфизм π является T-эквивариантным). Ввиду леммы 4.3.1(г), отсюда следует, что T централизует $\mathrm{Ker}(\pi)$. Как мы заметили выше, $\{e\} = C_U(T) \geqslant C_H(T)$, следовательно, $\mathrm{Ker}(\pi) = \{e\}$. С другой стороны, $\dim H = \dim \mathfrak{h} = n = \dim U_{\alpha_1} + \ldots + \dim U_{\alpha_n}$, следовательно, группа $(U_{\alpha_1} \times \ldots \times U_{\alpha_n})\pi$ является замкнутой

связной подгруппой группы H, размерность которой совпадает с H. Ввиду связности группы H мы получаем, что $(U_{\alpha_1} \times \ldots \times U_{\alpha_n})\pi = H$, т. е. морфизм π является сюръективным.

Если группа H не является коммутативной, то она является нильпотентной и обладает центром положительной размерности $Z = Z(H)^0$ (следствие 5.1.3), который, очевидно, является T-инвариантным. Из рассмотренного коммутативного случая следует, что группа Z прямо порождена содержащимися в ней подгруппами U_α (взятыми в любом порядке). Очевидно, можно считать, что центральные подгруппы U_α находятся в конце и совпадают с $U_{\alpha_{k+1}}, \ldots, U_{\alpha_n}$. Если $\varphi : H \to H/Z$ — канонический гомоморфизм, то группа T действует естественным образом на H/Z. Кроме того, поскольку $\mathcal{L}(H/Z) = \bigoplus_{i=1}^k \mathfrak{g}_{\alpha_i} \leq \mathfrak{h}$ и $C_\mathfrak{h}(T) = \{0\}$, лемма 5.3.6 влечёт, что $C_{H/Z}(T) = \{e\}$. Используя индукцию по размерности, мы заключаем, что H^φ прямо порождается группами $U_{\alpha_1}^\varphi, \ldots, U_{\alpha_k}^\varphi$ (в любом порядке). Отсюда следует, что группа H прямо порождена группами $U_{\alpha_1}, \ldots, U_{\alpha_n}$ (в любом порядке).

Предположим теперь, что группа H не является связной. Пусть V — подмножество группы U, прямо порождённое теми из U_α, которые не входят в H^0. Приведённое выше доказательство для связного случая позволяет утверждать, что $U = H^0V$, следовательно, H прямо порождена множествами H^0 и $H \cap V$. Но множество $H \cap V$ конечно (так как $V \cap H^0 = \{e\}$ и $|H : H^0|$ конечен) и T-инвариантно. Следовательно, T централизует $H \cap V$ и поэтому $H \cap V \leq C_U(T) = \{e\}$. □

Заметим, что, вообще говоря, не для любого подмножества $\{r_1, \ldots, r_k\} = \Psi$ множества положительных корней Φ^+ следующее множество $U_{r_1} \ldots X_{r_k}$ является подгруппой группы U. Рассмотрим один важный случай. Пусть $n \in N$ и $\sigma \in W$ — его образ относительно естественного гомоморфизма. Поскольку $T = N_N(U)$, мы будем использовать обозначение $U^\sigma = U^n$. Ввиду теоремы 5.8.2(б), для любой корневой подгруппы U_α справедливо $U_\alpha^n = U_{\alpha^\sigma}$. Пусть $B^- = TU^-$ — борелевская подгруппа, содержащая T и противоположная $B = TU$. Тогда мы можем построить две T-инвариантные подгруппы группы U: $U_\sigma = U \cap (U^-)^\sigma$ и $U'_\sigma = U \cap U^\sigma$ (мы хотим особо подчеркнуть, что через U_σ обозначена группа $U \cap (U^-)^\sigma$; это сделано для того, чтобы обозначения для разложения Брюа в алгебраических группах совпадали с обозначениями для разложения Брюа из предыдущего параграфа). Этим подгруппам соответствуют разбиения $\Phi_\sigma^- = \{\alpha \in \Phi^+ | \alpha^\sigma < 0\}$ и $\Phi^+\sigma = \{\alpha \in \Phi^+ | \alpha^\sigma > 0\}$. Лемма 6.4.1 показывает, что верно равенство $U = U_\sigma U'_\sigma = U'_\sigma U_\sigma$, но, вообще говоря, группа U не является полупрямым произведением подгрупп U_σ и U'_σ.

Предположим теперь, что $\alpha \in \Pi$ — фундаментальный корень и рассмотрим $\sigma = \sigma_\alpha$. По лемме 2.1.6, отображение σ_α переставляет положительные корни, отличные от α, поэтому $\Phi_{\sigma_\alpha}^+ = \Phi^+ \setminus \{\alpha\}$ и U'_{σ_α} имеет коразмерность 1 в U. По следствию 5.1.4 мы получаем, что U'_{σ_α} нормальна в U и, следовательно, в B. Так как $\sigma_\alpha^2 = e$, то и σ_α нормализует U'_{σ_α}. Значит, вся группа Z_α нормализует U'_{σ_α}.

Лемма 6.4.2. *Пусть G — связная алгебраическая группа полупростого ранга 1 (в частности, $|W| = 2$ и σ — единственный неединичный элемент группы W).*

Тогда $G = B \cup B\sigma B$. В частности, группы B, N образуют BN-пару группы G.

Доказательство. Очевидно, утверждение леммы достаточно доказать лишь для группы $G/R(G)$, поэтому можно считать, что G — полупростая группа. Более того, если $Z(G) \neq \{e\}$, то мы можем заменить группу G на $G/Z(G)$ и, таким образом, считать, что $Z(G)$ тривиален. В виду теоремы 5.7.2(е), мы получаем, что $G \simeq \mathrm{PGL}_2(\mathbb{F})$, B — подгруппа треугольных матриц и σ — образ матрицы $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ относительно естественного гомоморфизма $\mathrm{GL}_2(\mathbb{F}) \to \mathrm{PGL}_2(\mathbb{F})$. Таким образом, утверждение теоремы следует из того, что любая матрица из $\mathrm{GL}_n(\mathbb{F})$ раскладывается в произведение диагональной и трансвекций. □

Теорема 6.4.3. *Пусть G — связная алгебраическая группа, B — её подгруппа Бореля с максимальным тором T и унипотентным радикалом U, $N = N_G(T)$ — мономиальная подгруппа группы G.*

Тогда подгруппы B, N образуют расщепляемую насыщенную BN-пару группы G.

Доказательство. Выполнение аксиом (BN1)–(BN3), (BN5), а также аксиом (BNS1) и (BNS2) легко следует из результатов предыдущей главы и их проверку мы оставляем читателю. Здесь мы проверим лишь аксиому (BN4). Заметим, что в качестве множества S необходимо взять множество $\{\sigma_\alpha | \alpha \in \Pi\}$. Таким образом, обозначая за n_α некоторый прообраз элемента σ_α в группе N, нам необходимо проверить включение $n_\alpha B n \subseteq B n_\alpha n B \cup B n B$. Как мы заметили выше, элемент n_α нормализует U'_{σ_α}, следовательно, $\langle n_\alpha, B \rangle = Z_\alpha \leftthreetimes U'_{\sigma_\alpha}$ — группа полупростого ранга 1 (унипотентный радикал которой совпадает с U'_{σ_α}).

Рассмотрим точку $nB \in \mathfrak{B}$. Её стабилизатор в Z_α есть одна из борелевских подгрупп B_α или B'_α группы Z_α, содержащих тор T (см. лемму 5.7.5). Следовательно, многообразие Z_α/B_α биективно отображается на

орбиту точки nB относительно Z_α. Ввиду леммы 6.4.2, мы получаем, что эта орбита $Z_\alpha(nB)$ совпадает с $B(nB) \cup B\sigma_\alpha(nB)$. Таким образом, справедлива следующая цепочка равенств

$$Z_\alpha BnB = Z_\alpha U'_{\sigma_\alpha} U_\alpha nB = U'_{\sigma_\alpha} Z_\alpha nB = U'_{\sigma_\alpha} BnB \cup U'_{\sigma_\alpha} Bn_\alpha nB = BnB \cup Bn_\alpha nB,$$

откуда следует аксиома (BN4). □

***Упражнение* 6.4.4.** Пусть группа G редуктивна и B_1, B_2 — её подгруппы Бореля. Тогда $B_1 \cap B_2$ содержит максимальный тор группы G.

§5 Фундаментальная группа

Пусть G — связная алгебраическая группа и $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ — её рациональное представление. *Весами представления* ρ называются образы в группе $X(T)$ весов группы T^ρ на пространстве V относительно гомоморфизма $X(T^\rho) \to X(T)$. Для удобства, мы будем опускать ρ и считать, что V является G-модулем. Пусть λ — некоторый вес представления ρ, обозначим через $V_\lambda = \{v \in V | vt = t^\lambda v\}$ весовое пространство для λ. Тогда $\dim V_\lambda$ называется *кратностью* веса λ. Заметим, что действие группы W на $X(T)$, определённое в упражнении 5.6.10, даёт нам действие группы W на весах представления ρ. Более точно, если $n \in N_G(T)$ является представителем элемента $\sigma \in W$, то $V_\lambda^n = V_{\lambda^\sigma}$, значит, все веса в одной W-орбите имеют одинаковую кратность.

Ввиду теоремы 4.2.4, для любой алгебраической группы существует изоморфизм на подгруппу некоторой группы $\mathrm{GL}_n(\mathbb{F})$. Веса этого изоморфного представления порождают группу $X(T)$. Если G — простая группа, то для произвольного представления ρ мы имеем, что $\mathrm{Ker}(\rho)$ — конечная группа и потому существует лишь конечное число возможностей для выбора $\mathrm{Ker}(\rho)$. При этом веса представления ρ порождают подгруппу конечного индекса в $X(T)$. Если $\rho = \mathrm{Ad}$, то весами присоединённого представления являются корни (каждый кратности 1) с добавлением тривиального веса 0 (кратности $n = \mathrm{rank}(G)$).

Пусть теперь ρ — произвольное представление простой группы G. Тогда, по лемме 5.8.3, для любого $\alpha \in \Phi$ подгруппа $(U_\alpha)\rho$ отображает произвольное весовое пространство V_λ в $V_{\lambda+k\alpha}$, где $k \in \mathbb{N}, k \geqslant 0$. Следовательно, группа $(Z_\alpha)\rho$ оставляет инвариантным пространство $\sum V_{\lambda+k\alpha}$, $k \in \mathbb{Z}$; в частности, $\lambda^{\sigma_\alpha} = \lambda + k\alpha$ для некоторого $k \in \mathbb{Z}$. С другой стороны, в евклидовом пространстве $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ элемет σ_α действует как отражение $\lambda^{\sigma_\alpha} = \lambda - 2\frac{(\lambda,\alpha)}{(\alpha,\alpha)}\alpha$. Таким образом, число $2\frac{(\lambda,\alpha)}{(\alpha,\alpha)}$ является целым.

Определение 6.5.1. Пусть Φ — корневая система, порождающая евклидово пространство E^n. Вектор λ из E^n называется *весом* корневой системы Φ, если для любого корня $\alpha \in \Phi$ число $\frac{(\lambda,\alpha)}{(\alpha,\alpha)} =< \alpha, \lambda >$ является целым. Множество весов корневой системы Φ будем обозначать за $\Lambda(\Phi)$ или просто за Λ. Заметим, что для любого представления ρ и для любого веса λ представления ρ, вес λ является весом корневой системы Φ.

Для любого корня α элемент $\check{\alpha} = \frac{2\alpha}{(\alpha,\alpha)}$ называется *кокорнем* корня α. Таким образом, для любого веса λ и корня α справедливо $< \lambda, \alpha >= (\lambda, \check{\alpha})$, т. е. пространство, порождённое весами является дуальным пространству, порождённому кокорнями. В пространстве, порождённом весами из Λ существует дуальный базис к базису, пространства, порождённого кокорнями. Пусть $\alpha_1, \dots, \alpha_n$ — фундаментальный набор корней корневой системы Φ. Тогда $\check{\alpha}_1, \dots, \check{\alpha}_n$ — базис пространства, порождённого кокорнями. Обозначим за $\lambda_1, \dots, \lambda_n$ двойственный базис пространства, порождённого кокорнями. Тогда $(\lambda_i, \check{\alpha}_j) = 1$ при $i = j$ и 0 при $i \neq j$, т. е. $\lambda_1, \dots, \lambda_n$ лежат в Λ. Нетрудно проверить, что любой вес из Λ является целочисленной комбинацией весов $\lambda_1, \dots, \lambda_n$. Веса $\lambda_1, \dots, \lambda_n$ называются *фундаментальными весами* корневой системы Φ.

***Упражнение* 6.5.2.** Проверить, что любой вес из Λ является целочисленной линейной комбинацией весов $\lambda_1, \dots, \lambda_n$.

***Упражнение* 6.5.3.** Пусть $P = \mathbb{Z}\Phi$ — свободная абелева группа, порождённая корнями и $Q = \mathbb{Z}\Lambda$ — свободная абелева группа, порождённая всеми весами корневой системы Φ. Доказать, что P является подгруппой группы Q и найди факторгруппу Q/P для всех неразложимых корневых систем.

***Упражнение* 6.5.4.** Доказать, что множество кокорней образует корневую систему, называемую *двойственной* или *дуальной* для Φ. Найти дуальные корневые системы для всех неразложимых корневых систем.

Заметим, что любой корень также можно насматривать как вес корневой системы, поскольку для любых $\alpha, \beta \in \Phi$ число $< \alpha, \beta >$ является целым. Таким образом, мы получаем следующие включения $\mathbb{Z}\Phi \leq X(T) \leq$

$\mathbb{Z}\Lambda$. Ввиду упражнения 6.5.3, группа $\mathbb{Z}\Lambda/\mathbb{Z}\Phi$ конечна и почти всегда циклическая, за исключением случая $\Phi = D_{2n}$, когда группа $\mathbb{Z}\Lambda/\mathbb{Z}\Phi$ является элементарной абелевой группой порядка 4. Факторгруппу $\mathbb{Z}\Lambda/\mathbb{Z}\Phi$ в дальнейшем мы будем обозначать через $\Delta(\Phi)$. Факторгруппа $\mathbb{Z}\Lambda/X(T)$ будет обозначаться через $\pi(G)$ и называться *фундаментальной группой* алгебраической группы G. Полупростая алгебраическая группа называется *односвязной*, если $\pi(G) = \{e\}$. В другом крайнем случае, когда $\pi(G) = \Delta(\Phi)$, группа G называется *группой присоединённого типа*.

§6 Теорема об изоморфизме

В данном параграфе мы сформулируем теорему об изоморфизме простых алгебраических групп и сведём её доказательство к изучению редуктивных подгрупп ранга 2. Везде в этом и следующем параграфе, если не оговорено противное, группа G является связной и простой. Введём ряд обозначений, которые будут использоваться в этом и следующем параграфе. Напомним, что для любого $\alpha \in \Phi$ через T_α обозначена подгруппа $(\mathrm{Ker}(\alpha))^0$ максимального тора T и через Z_α — её (связный) централизатор $C_G(T_\alpha)$. Обозначим $Z_{\alpha\beta} = C_G((T_\alpha \cap T_\beta)^0)$. Обозначим через $\Phi_{\alpha\beta}$ подсистему системы Φ, порождённую корнями α и β. Заметим, что $Z_{\alpha,\beta}$ связна и редуктивна. Более того, она порождена группами $Z_\alpha, Z_\beta = \langle T, U_{\pm\alpha}, U_{\pm\beta}\rangle$, следовательно, $\Phi(Z_{\alpha\beta}) = \Phi_{\alpha\beta}$. Действительно, включение $\Phi_{\alpha\beta} \subseteq \Phi(Z_{\alpha\beta})$ очевидно. Обратно, для любого $\gamma \in \Phi \setminus \Phi_{\alpha\beta}$ группа U_γ не централизует тор $(T_\alpha \cap T_\beta)^0$ (см. теорему 5.8.2(в)). Следовательно, $\mathfrak{g}_\gamma \not\leq \mathcal{L}(Z_{\alpha\beta})$ и $\gamma \notin \Phi(Z_{\alpha\beta})$. Положим также, для удобства $Z_{\alpha\alpha} = Z_\alpha$.

Сформулируем теорему об изоморфизме, которую мы будем доказывать в этом и в следующем параграфах.

Теорема 6.6.1. *Пусть G, H — простые алгебраические группы, для которых $\Phi(G) \simeq \Phi(H)$ и $\Delta(G) \simeq \Delta(H)$. Тогда группы G и H изоморфны.*

Обозначим через T_1, B_1, Φ максимальный тор, подгруппу Бореля и корневую систему группы G, а через T_2, B_2, Φ — максимальный тор, подгруппу Бореля и корневую систему группы H (по условию теоремы, корневые системы изоморфны и мы будем использовать для них один и тот же символ). Рассмотрим евклидовы пространства $E_1 = X(T_1) \otimes_{\mathbb{Z}} \mathbb{R}$ и $E_2 = X(T_2) \otimes_{\mathbb{Z}} \mathbb{R}$. Поскольку Φ порождает пространства E_1 и E_2, существует изоморфизм $f : E_1 \to E_2$, сохраняющий произведение корней $< \alpha, \beta >$. Таким образом, мы получаем изоморфизм решёток весов $\mathbb{Z}\Lambda_1$ и $\mathbb{Z}\Lambda_2$.

Далее, $\mathbb{Z}\Phi \leq X(T_1) \leq \mathbb{Z}\Lambda$ и $\mathbb{Z}\Phi \leq X(T_2) \leq \mathbb{Z}\Lambda$. В силу упражнения 6.5.3, для всех корневых систем, кроме D_{2n} группа $\mathbb{Z}\Lambda/\mathbb{Z}\Phi$ является циклической, поэтому мы получаем, что группы $X(T_1)$ и $X(T_2)$ изоморфны.

***Упражнение* 6.6.2.** Доказать, что и в случае корневой системы D_{2n} группы $X(T_1)$ и $X(T_2)$ изоморфны.

Далее, каждому изоморфизму $f^{-1} : X(T_2) \to X(T_1)$ соответствует единственный изоморфизм $\varphi_T : T_1 \to T_2$. Таким образом, нам необходимо продолжить его до изоморфизма $\varphi : G \to H$ алгебраических групп. Таким образом, мы можем переформулировать теорему об изоморфизме.

Теорема 6.6.3. *Пусть G, H — полупростые алгебраические группы с максимальными торами T_1, T_2 и корневыми системами Φ_1, Φ_2 соответственно. Если $\varphi_T : T_1 \to T_2$ — изоморфизм торов, чьё ассоциированное отображение $X(T_2) \to X(T_1)$ индуцирует изоморфизм корневых систем Φ_1, Φ_2, то отображение φ_T можно продолжить до изоморфизма $\varphi : G \to H$.*

Прежде, чем продолжать доказательство, мы кратко опишем его схему. Сначала мы построим соласованные расширения отображения φ_T до вложений $\varphi_N : N \to H$ и $\varphi_B : B \to H$. Тогда образы групп B, N образуют BN-пару группы H и, используя точную форму разложения Брюа (теорема 6.2.9) мы построим биекцию $\varphi : G \to H$. Далее мы покажем, что эта биекция сохраняет операцию, т. е. является гомоморфизмом. Кроме того, ограничение φ на B является морфизмом. Тогда и φ будет являться морфизмом. Действительно, поскольку $U^- = R_u(B^-) = U^{\sigma_0}$, то ограничение φ на U^- также будет морфизмом. Обозначим через $\Omega = B\sigma_0 B = U^- B$ *большую клетку*. Тогда следующая диаграмма коммутативна:

$$\begin{array}{ccc} U^- \times B & \longrightarrow & (U^-)\varphi \times B\varphi \\ \downarrow & & \downarrow \\ \Omega & \longrightarrow & \Omega\varphi \end{array}$$

Заметим, что морфизм произведения $\mu : U^- \times B \to \Omega$ сюръективен, так как $U^- \cap B = \{e\}$, значит, $\dim \Omega = \dim U^- + \dim B = \dim G$. Таким образом, Ω содержит открытое подмножество группы G (на самом деле,

само Ω является открытым подмножеством, но нам здесь это не требуется). Следовательно, φ является морфизмом на некотором открытом подмножестве группы G и потому задаётся рациональной функцией, всюду определённой на G. По лемме 3.4.2 мы получаем, что φ является морфизмом.

Перейдём теперь к последовательному выполнению всех шагов доказательства.

Шаг 1. Продолжение отображения φ_T на $N = N_G(T)$. Заметим, что ввиду теоремы 6.3.1, группа W порождается элементами σ_α, $\alpha \in \Pi$ и соотношениями $(\sigma_\alpha, \sigma_\beta)^{m_{\alpha\beta}} = e$. Мы хотим продолжить это представление группы W на группу N, используя отображение φ_T. Для этого мы выберем произвольных представителей n_α для $\sigma_\alpha, \alpha \in \Pi$ (ясно что этих представителей, вместе с тором T, достаточно, чтобы породить всю группу N). Далее положим $t_{\alpha\beta} = (n_\alpha \cdot n_\beta)^{m_{\alpha\beta}} \in T$. Мы утверждаем, что этих соотношений вместе с тором T достаточно, чтобы породить единственным образом группу N.

Лемма 6.6.4. *Пусть $\psi : T \to H$ — гомоморфизм абстрактных групп и пусть $h_\alpha \in H, \alpha \in \Pi$. Тогда ψ можно продолжить до гомоморфизма $N \to H$, переводящего n_α в h_α в том и только в том случае, если $(h_\alpha h\beta)^{m_{\alpha\beta}} = (t_{\alpha\beta})\psi$ для всех $\alpha, \beta \in \Pi$.*

Доказательство. Необходимость условия $(h_\alpha h_\beta)^{m_{\alpha\beta}} = (t_{\alpha\beta})\psi$ очевидна, докажем его достаточность. Рассмотрим свободную группу W^* с множеством порождающих n_α, $\alpha \in \Pi$. Каждому из n_α сопоставим автоморфизм $t \mapsto n_\alpha^{-1} t n_\alpha$ тора T, получая таким образом канонический гомоморфизм $W^* \to \mathrm{Aut}T$. Пусть $N^* = W^* \leftthreetimes T$ — полупрямое произведение групп W^* и T. Профакторизуем N^* по наименьшей нормальной подгруппе, содержащей элементы $t_{\alpha\beta}^{-1}(n_\alpha^* n_\beta^*)^{m_{\alpha\beta}}$, $\alpha, \beta \in \Pi$ и обозначим полученную факторгруппу за $\widetilde{N}$. Очевидно, группа N является гомоморфным образом группы $\widetilde{N}$, причём подгруппа T группы N^* изоморфно отображается на подгруппу группы $\widetilde{N}$ (также называемую T) и затем на T. Очевидно также, что $\psi : T \to H$ единственным образом продолжается до гомоморфизма $\widetilde{N} \to H$, переводящего $\tilde{n}_\alpha$ в h_α, где $\tilde{n}_\alpha$ — образ элемента n_α^*.

Осталось доказать, что канонический гомоморфизм $\widetilde{N} \to N$ является изоморфизмом. Для этого достаточно доказать, что эпиморфизм $\widetilde{N}/T \to N/T = W$ является изоморфизмом. Но $\widetilde{N}/T$ порождается образами элементов $\tilde{n}_\alpha$, удовлетворяющими соотношениям для группы W. Ввиду теоремы 6.3.1, она не может быть больше, чем W. □

Вернёмся теперь к продолжению отображения $\varphi_T : T \to H$ до $\varphi_N : N \to H$. Мы должны выбрать элементы $n_\alpha \in N$, $\alpha \in \Pi$, определив таким образом элементы $t_{\alpha\beta}$, $\alpha, \beta \in \Pi$. Затем выбрать такие образы h_α, для которых $(h_\alpha h_\beta)^{m_{\alpha\beta}} = (t_{\alpha\beta})\varphi_T$. Все эти вычисления зависят лишь от групп $Z_{\alpha\beta}$ полупростого ранга 1 или 2. Заметим, что поскольку группы Вейля групп G, H изоморфны и конечны, построенный нами изоморфизм φ_N автоматически является морфизмом алгебраических групп.

Шаг 2. Продолжение φ_T на Z_α. Прежде, чем строить продолжение отображения φ_T на подгруппу Бореля B, нам нужно построить его продолжение на корневые подгруппы. Мы сделаем это, построив продолжение морфизма φ_T на группы Z_α. Напомним, что $Z_\alpha / Z(Z_\alpha) \simeq \mathrm{PGL}_2(\mathbb{F})$ (см. теорему 5.7.1(e)). Здесь и далее образ матрицы $A = (a_{i,j}) \in \mathrm{GL}_n(\mathbb{F})$, $1 \leqslant i, j \leqslant n$ в группе $\mathrm{PGL}_n(\mathbb{F})$ относительно естественного гомоморфизма будем обозначать через $[A] = [a_{i,j}]$. Пусть $\pi : Z_\alpha \to \mathrm{PGL}_2(\mathbb{F})$ — упоминавшийся выше гомоморфизм. Тогда U_α^π является максимальной унипотентной подгруппой группы $\mathrm{PGL}_2(\mathbb{F})$ и потому, с точностью до сопряжения, состоит из матриц вида $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$, где $x \in \mathbb{F}$. Кроме того, T^π — максимальный тор группы $\mathrm{PGL}_n(\mathbb{F})$, нормализующий U_α^π, поэтому $T^\pi = \{\begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix} | t_1, t_2 \in F^*\}$. Ввиду теоремы 5.8.2(в) можно считать, что $(u_\alpha(x))^\pi = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$. В силу симметрии мы получаем, что $(u_{-\alpha}(x))^\pi = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$. Далее мы можем выбрать $n_\alpha = u_\alpha(1) u_{-\alpha}(-1) u_\alpha(1) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Тогда $t_\alpha = n_\alpha^2$ переходит в $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Пусть теперь $Z'_{\alpha'}$ — другая редуктивная группа полупростого ранга 1, будем обозначать её элементы также, как элементы группы Z_α, добавляя штрих. Тогда для неё тоже существует гомоморфизм $\pi' : Z'_{\alpha'} \to \mathrm{PGL}_2(\mathbb{F})$, для которого образы элементов $u'_{\pm\alpha'}(x)$, $n'_{\alpha'}$, $t'_{\alpha'}$ можно выбрать такими же, как и образы соответствующих элементов группы Z_α. Тогда справедлива следующая лемма.

Лемма 6.6.5. *В ведённых выше обозначениях пусть $\varphi_T : T \to T'$ — изоморфизм торов, для которого изоморфизм групп характеров $X(T') \to X(T)$ переводит α' в α. Тогда φ_T можно продолжить единствен-*

ным образом до изоморфизма алгебраических групп $\varphi : Z_\alpha \to Z'_{\alpha'}$ так, что $(u_\alpha(x))\varphi = u'_{\alpha'}(x)$, где $x \in \mathbb{F}$ и $n_\alpha \varphi = n'_{\alpha'}$.

Доказательство. Единственность изоморфизма φ очевидна, поскольку T, n_α, U_α порождают Z_α. Также очевидно, как определить измоморфизм многообразий между соответствующими большими клетками $\Omega_\alpha, \Omega'_{\alpha'}$, а именно: $(u_{-\alpha}(x)tu_\alpha(y))\,\varphi = u'_{-\alpha'}(x)t^{\varphi_T}u'_{\alpha'}(y)$. Далее мы используем эпиморфизмы π, π' на $\mathrm{PGL}_2(\mathbb{F})$, чтобы построить общую «накрывающую» группу S, удовлетворяющую условию: существуют такие гомоморфизмы $\rho : S \to Z_\alpha$ и $\rho' : S \to Z'_{\alpha'}$, что следующая диаграмма коммутативна.

$$\begin{tikzcd} & S \arrow[dl, "\rho"'] \arrow[dr, "\rho'"] & \\ Z_\alpha \arrow[rr, dashed, "\varphi"] \arrow[dr, "\pi"'] & & Z'_{\alpha'} \arrow[dl, "\pi'"] \\ & \mathrm{PGL}_2(\mathbb{F}) & \end{tikzcd}$$

Рассмотрим замкнутую подгруппу $R = \{(z, z') \in Z_\alpha \times Z'_{\alpha'} | (z)\pi = (z')\pi'\}$ (она замкнута, как прообраз замкнутого множества — диагонали в $\mathrm{PGL}_2(\mathbb{F}) \times \mathrm{PGL}_2(\mathbb{F})$), положим $S = R^0$ и пусть ρ, ρ' — соответствующие проекции. Очевидно, $\rho\pi = \rho'\pi'$. Поскольку π, π' сюръективны, то и проекции группы R на $Z_\alpha, Z'_{\alpha'}$ также сюръективны. Но S имеет конечный индекс в R, так что проекции ρ, ρ' сюръективны.

На данный момент мы определили φ на плотном открытом подмножестве Ω_α и потому φ является рациональной функцией. Кроме того, $\rho\varphi = \rho'$. Покажем, что φ всюду определена, откуда будет следовать, что φ — гомоморфизм групп. Пусть $x \in S$, $z = (x)\rho$, $z' = (x)\rho'$. Обозначим через $\lambda_0, \lambda, \lambda'$ соответствующие левые сдвиги групп $S, Z_\alpha, Z'_{\alpha'}$, индуцированные этими элементами. Мы имеем, что $\rho\varphi\lambda' = \rho'\lambda' = \lambda_0\rho$ на всех элементах, для которых определено отображение $\rho\varphi$. Кроме того, $\lambda_0\rho' = \lambda_0\rho\varphi = \rho\lambda\varphi$. Из сюръективности φ следует, что $\varphi\lambda' = \lambda\varphi$ (вновь для тех элементов, для которых соответствующие отображения определены). Таким образом, если φ определено в точке $y \in Z_\alpha$, то оно определено и в точке $(y)\lambda = zy$ правилом $(zy)\varphi = (y)\varphi\lambda' = z'(y)\varphi$. В силу произвольности выбора элемента z, мы получаем, что φ всюду определено и $\rho\varphi = \rho'$. Следовательно, φ является гомоморфизмом.

По построению, $(n_\alpha)\varphi = n'_{\alpha'}$. В силу симметрии и используя точную форму разложению Брюа (теорема 6.2.9) мы получаем, что существует и обратное отображение $\varphi' : Z'_{\alpha'} \to Z_\alpha$, следовательно, φ является изоморфизмом. □

***Упражнение* 6.6.6.** Доказать, что полупростая группа ранга 1 изоморфна либо $\mathrm{SL}_2(\mathbb{F})$, либо $\mathrm{PGL}_2(\mathbb{F})$.

Продолжение φ_T на TU_α. На предыдущем шаге мы показали, каким образом продолжить отображение φ_T до изомоморфизма группы Z_α в соответствующую подгруппу группы H для любого корня $\alpha \in \Phi^+$. Однако, корни не являются «независимыми» (значение этого понятия будет ясно из последующих рассуждений). Построим сначала расширения φ_{Z_α} только для фундаментальных корней $\alpha \in \Pi$. Обозначим через φ_α сужение изоморфизма φ_{Z_α} на U_α и через n_α элемент $u_\alpha(1)u_{-\alpha}(-1)u_\alpha(1)$, определённый на предыдущем шаге и через t_α элемент $n_\alpha^2 (= t_{\alpha\alpha})$. Положим $h_\alpha = (n_\alpha)\varphi_{Z_\alpha}$.

Ввиду шага 1, изоморфизм φ_T можно продолжить до изоморфизма $\varphi_N : N \to H$, переводящего $n_\alpha \mapsto h_\alpha$, $\alpha \in \Pi$, если выполнено следующее условие.

(А) *Если $t_{\alpha\beta} = (n_\alpha n_\beta)^{m_{\alpha\beta}}$ для всех $\alpha, \beta \in \Pi$, то $(t_{\alpha\beta})\varphi_T = (h_\alpha h_\beta)^{m_{\alpha\beta}}$, где $m_{\alpha\beta} = |\sigma_\alpha\sigma_\beta|$.*

Мы проверим выполнение этого условия в следующем параграфе, пока же предположим, что условие **(А)** выполнено и будем использовать изоморфизм φ_N. По построению, φ_N и φ_{Z_α} согласуются на Z_α. Далее наша задача — построить продолжение изоморфизма φ_T до изоморфизма $\varphi_B : B \to H$, которое должно совпадать с φ_α на U_α. В частности, если $U_{\alpha\beta} = U \cap Z_{\alpha\beta}$, то необходимо потребовать выполнения следующего условия.

(Б) *Для любой пары фундаментальных корней $\alpha, \beta \in \Pi$ существует такой изоморфизм алгебраических групп $\varphi_{\alpha\beta}$ из $U_{\alpha\beta}$ на соответствующую подгруппу группы H, что он является расширением и φ_α, и φ_β.*

Как и условие **(А)**, второе условие необходимо проверить лишь для групп ранга 2 и его проверкой мы займёмся в следующем параграфе. Сейчас же мы предположим, что это условие выполнено.

Далее, если мы хотим продолжить φ_T не только на B, но и на всю группу G, необходимо наложить дополнительные ограничения. Предположим, что β — некоторый положительный корень и $\sigma \in W$ выбран так, что $\beta^\sigma = \alpha \in \Pi$. Выберем представителя n элемента σ в группе N (для краткости мы будем использовать обозначение $\bar{n} = \sigma$). Тогда $U_\alpha = n^{-1}U_\beta n$ или $U_\beta = nU_\alpha n^{-1}$. Если существует гомоморфизм $\varphi : G \to H$, продолжающий как φ_N, так и φ_α, то полученное равенство показывает, как φ должен быть определён на U_β. Но при этом β может переходить в α под действием другого элемента из W и β может переходить в какой-то другой фундаментальный корень. Нам необходимо убедиться, что все такие варианты по прежнему являются согласованными, для этого, оказывается, вновь достаточно проверки следующего условия для групп ранга 2.

(В) *Пусть* $\alpha, \beta \in \Pi$. *Если* $\gamma \in \Phi^+_{\alpha\beta}$ *и* $\gamma \neq \alpha$, *то* $\varphi_{\alpha\beta} \circ \mathrm{Int}_{h_\alpha}$ *согласуется на* U_γ *с* $\mathrm{Int}_{n_\alpha} \circ \varphi_{\alpha\beta}$.

Как и условия **(А)** и **(Б)**, условие **(В)** будет проверено в следующем параграфе. Пока же предположим, что и это условие выполнено и докажем, что φ_α можно определить на всех корнях α (как положительных, так и отрицательных).

Лемма 6.6.7. *Предположим, что выполнены условия* **(А)**, **(Б)**, **(В)**, *так что определены отображения* φ_N *и* $\varphi_\alpha, \varphi_{\alpha\beta}$, $\alpha, \beta \in \Pi$. *Тогда для любого* $\alpha \in \Phi$ *существует изоморфизм* φ_α *группы* U_α *на соответствующую подгруппу группы* H, *удовлетворяющий условиям:*

(а) *если* $\alpha \in \Pi$, *то* φ_α *согласуется с морфизмом* $\varphi_{-\alpha} = \varphi_{Z_\alpha}|_{U_{-\alpha}}$;

(б) *если* $\alpha, \beta \in \Pi$ *и* $\gamma \in \Phi^+_{\alpha\beta}$, *то* $\varphi_\gamma = \varphi_{\alpha\beta}|_{U_\gamma}$;

(в) *если* $n \in N$ *и* $(\alpha)\bar{n} = \beta$, $\alpha, \beta \in \Phi$, *то* $\varphi_\alpha \circ \mathrm{Int}_{(n)\varphi_N}$ *согласуется с* $\mathrm{Int}_n \circ \varphi_\beta$ *на* U_α.

Доказательство. Положим $N_{\alpha\beta} = N_{Z_{\alpha\beta}}(T)$. Доказательство этой леммы мы проведём в четыре этапа.

(1) Пусть $\alpha, \beta \in \Pi$, $\alpha \neq \beta$. Если $n \in N_{\alpha\beta}$ и $(\alpha)\bar{n} = \alpha$ (соотв. $(\alpha)\bar{n} = \beta$), то $\varphi_\alpha \circ \mathrm{Int}_{(n)\varphi_N}$ согласуется с $\mathrm{Int}_n \circ \varphi_\alpha$ (соотв. с $\mathrm{Int}_n \circ \varphi_\beta$) на U_α.

Запишем $n = n_{\gamma_1} \cdot \ldots \cdot n_{\gamma_k} t$ для некоторого $t \in T$ и некоторых $\gamma_i \in \{\alpha, \beta\}$. В случае $n = t$ (значит $(\alpha)\bar{n} = \alpha$) наше утверждение следует из построения отображения φ_{Z_α}. Поэтому мы можем предполагать, что $n = n_{\gamma_1} \cdot \ldots \cdot n_{\gamma_k}$ и использовать индукцию по k. Напомним (см. лемму 2.1.6), что $\alpha^{\sigma_\alpha} = -\alpha$ и σ_α переставляет остальные положительные корни (то же самое справедливо для β и σ_β).

Для выполнения индукционного шага рассмотрим последовательность корней $\alpha_i = (\alpha)\varphi_{\gamma_1} \cdot \ldots \cdot \varphi_{\gamma_{i-1}} \in \Phi_{\alpha\beta}$. Если все α_i положительны, то мы получаем требуемое утверждение последовательным применением условия **(В)**. Поэтому предположим, что существует такое i, что $\alpha_i \in \Phi^+_{\alpha\beta}$, а $(\alpha_i)\sigma_{\gamma_i} \in \Phi^-_{\alpha\beta}$. Как мы заметили выше, это означает, что либо $\alpha_i = \alpha$ и $\sigma_{\gamma_i} = \sigma_\alpha$, либо $\alpha_i = \beta$ и $\sigma_{\gamma_i} = \sigma_\beta$. Тогда можно записать элемент n в виде $n' \cdot n''$, где $n' = n_{\gamma_1} \cdot \ldots \cdot n_{\gamma_{i-1}}$ и $n'' = n_{\gamma_i} \cdot \ldots \cdot n_{\gamma_k}$. Кроме того, заметим что и n', и n'' удовлетворяют условиям для n (для n'', возможно, необходимо поменять ролями корни α и β), откуда по индукции получаем требуемое утверждение.

(2) Пусть $\alpha, \beta \in \Pi$ и предположим, что $(\alpha)\bar{n} = \beta$, $n \in N$. Тогда $\varphi_\alpha \circ \mathrm{Int}_{(n)\varphi_N}$ согласуется с $\mathrm{Int}_n \circ \varphi_\beta$ на U_α.

Заметим, что этап (2) сразу следует из этапа (1), если $\alpha \neq \beta$ и $n \in N_{\alpha\beta}$ либо если $\alpha = \beta$ и $n \in N_{\alpha,\gamma}$ для некоторого $\gamma \in \Pi$. Применяя лемму Титса 2.5.4, мы получаем этап (2).

(3) Пусть $\alpha \in \Phi$, $n, n' \in N$. Предположим, что $(\alpha)\bar{n} = \beta \in \Pi$ и $(\alpha)\bar{n}' = \beta' \in \Pi$. Тогда $\mathrm{Int}_n \circ \varphi_\beta \circ \mathrm{Int}^{-1}_{(n)\varphi_N}$ согласуется с $\mathrm{Int}_{n'} \circ \varphi_{\beta'} \circ \mathrm{Int}^{-1}_{(n')\varphi_N}$ на U_α.

Достаточно доказать, что $\varphi_\beta \circ \mathrm{Int}_{(n^{-1}n')\varphi_N}$ согласуется с $\mathrm{Int}_{n^{-1}n'} \circ \varphi_{\beta'}$ на U_α, а это следует из этапа (2).

(4) Теперь мы можем определить φ_α так, чтобы он согласовывался со всеми случаями, упомянутыми в **(Б)**. По лемме 2.1.9, существует такой фундаментальный корень β и $n \in N$, что $(\alpha)\bar{n} = \beta$. Для $x \in U_\alpha$ определим $(x)\varphi_\alpha$ равным $(x)\mathrm{Int}_n \circ \varphi_\beta \circ \mathrm{Int}^{-1}_{(n)\varphi_N}$. Ввиду этапа (3), это определение не зависит от выбора β и n, что даёт нам утверждение леммы. □

Шаг 4. Продолжение φ_T на B. Мы по прежнему предполагаем, что выполнены условия **(А)**, **(Б)**, **(В)**, сформулированные на предыдущем шаге. На предыдущем шаге мы построили согласованные морфизмы φ_α для всех $\alpha \in \Phi$, что даёт нам морфизм (как многообразий) φ_B подгруппы Бореля B группы G на подгруппу Бореля группы H. Действительно, группа B как многообразие изоморфна прямому произведению $T \times \prod_{\alpha \in \Phi^+} U_\alpha$. Мы хотим показать, что φ_B является гомоморфизмом групп. Для этого нам потребуется изучать коммутаторы в группе U. Заметим, что для любых $\alpha, \beta \in \Phi^+$ коммутант $[U_\alpha, U_\beta]$ является

T-инвариантной подгруппой и потому, по лемме 6.4.1, прямо порождается теми U_γ, которые в ней содержатся. Далее лемма 5.8.3 показывает, какие корни γ могут встретиться.

Лемма 6.6.8. Коммутаторная формула Шевалле. *Пусть $\alpha, \beta \in \Phi^+$ и Ψ — множество корней вида $r\alpha+s\beta$, где r, s — натуральные числа. Тогда $[u_\alpha(x), u_\beta(y)] = \prod_{r,s>0} u_{r\alpha+s\beta}(C_{\alpha,\beta,r,s}x^r y^s)$, произведение берётся по всем $r\alpha+s\beta \in \Psi$ и константы $C_{\alpha,\beta,r,s}$ не зависят от выбора x, y. В частности, $[U_\alpha, U_\beta] = e$, если $\alpha+\beta \notin \Phi$.*

Доказательство. Упорядочим положительные корни каким-нибудь образом $\alpha_1, \ldots, \alpha_m$, чтобы порядок согласовывался со сложением корней (одно из возможных упорядочений приведено в главе про корневые системы). Тогда отображение произведения $\mu : U_{\alpha_1} \times \ldots \times U_{\alpha_m} \to U$ является изоморфизмом многообразий. Далее определим морфизм $\psi : \mathbb{F} \times \mathbb{F} \to U$ правилом $(x, y)\psi = [u_\alpha(x), u_\beta(y)]$. Его образ имеет вид $u_{\alpha_1}(p_1(x, y)) \cdot \ldots \cdot u_{\alpha_m}(p_m(x, y))$, где $p_i(X, Y) \in \mathbb{F}[X, Y]$ — многочлены от двух переменных: $p_i(X, Y) = \sum_{r,s\geqslant 0} a_{i,r,s}X^r Y^s$. По определению морфизма ψ, мы имеем $(x, 0)\psi = e = (0, y)\psi$, так что XY делит $p_i(X, Y)$.

Далее сопряжем $(x, y)\psi$ элементом $t \in T$ и запишем результат двумя способами. С одной сторноны, $[u_\alpha(t^\alpha x), u_\beta(t^\beta y)] = \prod_i u_{\alpha_i}(p_i(t^\alpha x, t^\beta y))$. С другой стороны, правая часть равна $\prod_i u_{\alpha_i}(t^{\alpha_i} p_i(x, y))$. Сравнивая оба выражения, получаем, что $a_{i,r,s} = 0$ во всех случаях, кроме $\alpha_i = r\alpha + s\beta$, откуда следует лемма. □

Покажем, каким образом из данной леммы получается вложение φ_B. В том случае, когда α, β — простые корни, лемма вместе с условием **(Б)** влечёт, что $\varphi_{\alpha\beta} = \varphi_B|_{U_{\alpha\beta}}$ является изоморфизмом. Если теперь α, β — произвольные корни, то существует такой $n \in N$, что $\alpha^{\bar{n}}$ — фундаментальный корень и существует такой фундаментальный корень γ, что $\beta^{\bar{n}} \in \Phi^+_{\alpha^{\bar{n}}\gamma}$ (см. лемму 2.1.9). По лемме 6.6.7 и из того, что $\varphi_{\alpha^{\bar{n}}\gamma} : U_{\alpha^{\bar{n}}\gamma} \to H$ — гомоморфизм групп, мы получаем, что φ_B сохраняет коммутаторную формулу. В частности, отсюда следует, что $\varphi_B|_U : U \to H$ является изоморфизмом. Поскольку φ_B сохраняет действие тора T на U и его ограничение на T является изоморфизмом, мы получаем, что $\varphi_B : B \to H$ является изоморфизмом.

Шаг 5. φ сохраняет операцию. На данном шаге мы покажем, что $\varphi : G \to H$ сохраняет операцию и, тем самым, по модулю проверки свойств **(А)**, **(Б)**, **(В)**, завершим доказательство теоремы об изоморфизме. Доказательство того, что φ сохраняет операцию, следует из следующих двух лемм. В первой мы докажем, что если φ сохраняет операцию на некотором открытом подмножестве связной алгебраической группы, то тогда φ сохраняет операцию на всей группе. А во второй мы проверим, что φ сохраняет операцию на большой клетке Ω.

Лемма 6.6.9. *Пусть G_1, G_2 — связные алгебраические группы, U — непустое открытое подмножество группы G_1, $\psi : G_1 \to G_2$ — такой морфизм, что $(xy)^\psi = x^\psi y^\psi$ если только $x, y, xy \in U$.*

Тогда ψ продолжается (единственным образом) до морфизма алгебраических групп $\psi' : G_1 \to G_2$.

Доказательство. Ввиду леммы 4.1.4, выполнено равенство $G_1 = U \cdot U$, которое диктует продолжение для ψ'. Если $x \in G_1$ записан в виде $x = yz$, где $y, z \in U$, то мы обязаны положить $x^{\psi'} = y^\psi z^\psi$. Для того, чтобы определить таким образом отображение, нам нужно проверить, что выполнено условие $(*)$: $y^\psi y^\psi = (y')^\psi (z')^\psi$ если только $y, z, y', z' \in U$ и $yz = y'z'$. Если мы сумеем доказать условие $(*)$, то тогда ψ' автоматически будет морфизмом, поскольку его ограничение на любом сдвиге xU будет морфизмом. Кроме того, ψ' также автоматически будет сохранять операцию. Действительно, заметим, что подмножество V множества $U \times U$, состоящее из пар (x, y), для которых $xy \in U$ является плотным в $G_1 \times G_1$, поскольку V является пересечением открытых множеств $U \times U$ и $U^{\mu^{-1}}$, где $\mu : G_1 \times G_1 \to G_1$ — морфизм произведения. Далее, морфизм $G_1 \times G_1 \to G_2$, определённый правилом $(x, y) \mapsto (xy)^{\psi'}(y^{\psi'})^{-1}(x^{\psi'})^{-1}$ на V совпадает с тождественным морфизмом $(x, y) \mapsto e$, значит, по лемме 3.4.5, совпадает с тождественным морфизмом на всём многообразии $G_1 \times G_1$.

Таким образом, достаточно доказать выполнение условия $(*)$. Обозначим через D_1 (соотв. D_2) диагональ в $G_1 \times G_1$ (соотв. $G_2 \times G_2$), значит, диагонали являются замкнутыми множествами (так как для многообразия выполнена аксиома Хаусдорфа). Пусть X — прообраз диагонали D_1 относительно морфизма

$$(U \times U) \times (U \times U) \xrightarrow{\mu\times\mu} G_1 \times G_1$$

и Y — прообраз диагонали D_2 относительно композиции морфизмов

$$(U \times U) \times (U \times U) \xrightarrow{\psi\times\psi\times\psi\times\psi} (G_2 \times G_2) \times (G_2 \times G_2) \xrightarrow{\mu\times\mu} G_2 \times G_2 .$$

Таким образом, X, Y — замкнутые подмножества, как прообразы замкнутых подмножеств. Заметим также, что X является неприводимым, поскольку отображение $(w, x, y, z) \mapsto (w, x, y)$ индуцирует изоморфизм многообразий из прообраза диагонали D_1 в $(G_1 \times G_1) \times (G_1 \times G_1)$ на $G_1 \times G_1 \times G_1$ и X — открытое подмножество в первом из этих многообразий.

Если теперь подмножество V в $U \times U$ определно также, как и раньше, то предположение, что $(xy)^\psi = x^\psi y^\psi$ при $x, y, xy \in U$ влечёт, что $X' = (V \times V) \cap X$ содержится в Y. Но X' — открытое (и, в силу неприводимости X, плотное) подмножество множества X, значит, замкнутось множества Y влечёт $X \subseteq Y$. □

Лемма 6.6.10. *Предположим, что выполнены условия* **(А)**, **(Б)**, **(В)** *и определим $\varphi : G \to H$ из разложения Брюа. Тогда $(xy)^\varphi = x^\varphi y^\varphi$ как только $x, y, xy \in \Omega$.*

Доказательство. Мы проведём доказательство в несколько этапов, активно используя уже доказанные изоморфизмы ограничений φ на Z_α, N, U, U^-.

(1) *Пусть $n_0 \in N$ — представитель самого длинного элемента $\sigma_0 \in W$, переводящего все положительные корни в отрицательные, так что $U^n = U^-$, $(U^-)^n = U$. Тогда для всех $u \in U$ (соотв. $u \in U^-$) выполнено $(u^{n_0})^\varphi = (n_0^{-1})^\varphi \cdot u^\varphi \cdot n_0^\varphi$.* Действительно, поскольку ограничения $\varphi|_U$ и $\varphi|_{U^-}$ — изоморфизмы, наше утверждение следует из леммы 6.6.7(в).

(2) *Пусть $u \in B$, $v \in B^-$, $x \in \Omega$. Тогда $(vxu)^\varphi = v^\varphi \cdot x^\varphi \cdot u^\varphi$.*

Запишем $v = v_1t_1$, $x = v_2t_2u_2$, $u = t_3u_3$, где $v_i \in U^-$, $t_i \in T$, $u_i \in U$. Тогда по определению, $v^\varphi \cdot x^\varphi \cdot u^\varphi = v_1^\varphi \cdot t_1^\varphi \cdot v_2^\varphi \cdot t_2^\varphi \cdot u_2^\varphi \cdot t_3^\varphi \cdot u_3^\varphi$. Аналогично, $(vxu)^\varphi = (v_1t_1v_2t_1^{-1}t_1t_2t_3t_3^{-1}u_2t_3u_3)^\varphi = (v_1t_1v_2t_1^{-1})^\varphi \cdot (t_1t_2t_3)^\varphi \cdot (t_3^{-1}u_2t_3u_3)^\varphi$. Ввиду леммы 6.6.7(c), мы получаем, что $(v_1t_1v_2t_1^{-1})^\varphi = v_1^\varphi \cdot t_1^\varphi \cdot v_2^\varphi \cdot (t_1^{-1})^\varphi$ и $(t_3^{-1}u_2t_3u_3)^\varphi = (t_3^{-1})^\varphi \cdot u_2^\varphi \cdot t_3^\varphi \cdot u_3^\varphi$, откуда следует требуемое утверждение.

(3) *Пусть $\alpha \in \Pi$, $x \in \Omega$. Если $(x)\mathrm{Int}_{n_\alpha}$ лежит в Ω, то $(n_\alpha^{-1}xn_\alpha)^\varphi = (n_\alpha^{-1})^\varphi \cdot x^\varphi \cdot n_\alpha^\varphi$.*

Запишем $x = vx_{-\alpha}tx_\alpha u$, где $t \in T, x_{-\alpha} \in U_{-\alpha}, x_\alpha \in U_\alpha$, v лежит в произведении $U_{-\beta}$, u лежит в произведении U_β, где $\beta \in \Phi^+ \setminus \{\alpha\}$ (существование такой записи следует из леммы 6.4.1 и замечания после неё). Последние два произведения нормализуются элементом n_α, поскольку $\bar{n}_\alpha$ переставляет положительные корни, отличные от α (см. лемму 2.1.6). Значит, если $x_{-\alpha} = x_\alpha = e$, то требуемое утверждение следует из леммы 6.6.7(в). Ввиду (2), утверждение достаточно проверить для $x = x_{-\alpha}tx_\alpha \in Z_\alpha$. Но $\varphi|_{Z_\alpha}$ является изоморфизмом ввиду леммы 6.6.5 и $n_\alpha \in Z_\alpha$, откуда следует требуемое утверждение.

(4) *Пусть $n \in N$, $x \in \Omega$. Если $x^{\mathrm{Int}_n} \in \Omega$, то $(n^{-1}xn)^\varphi = (n^{-1})^\varphi \cdot x^\varphi \cdot n^\varphi$.*

Утверждение справедливо для $n \in T$ и для $n = n_\alpha$, $\alpha \in \Pi$. Хотя любой элемент из n можно получить как произведение некоторого элемента из t и элементов n_α, наше утверждение нельзя доказать по индукции, поскольку мы не можем утверждать, что x^{n_α} лежит в Ω на каждом промежуточном шаге.

Заметим, что правая и левая части формулы, которую нужно доказать, задают морфизмы из $\Omega \cap \Omega^{\mathrm{Int}_{n^{-1}}}$ в H. Для совпадения этих морфизмов, по лемме 3.4.5, достаточно проверить, что $(*)$ существует такое открытое подмножество V_n множества Ω (зависящее от n), что $V_n^{\mathrm{Int}_n} \subseteq \Omega$ и что $\mathrm{Int}_n \circ \varphi$ совпадает с $\varphi \circ \mathrm{Int}_{n^\varphi}$ на V_n. Запишем $n = n'n_\alpha$ и будем доказывать утверждение $(*)$ индукцией по длине $l(\bar{n})$. По индукции, $V_{n'}$ задано, определим $V_n = \Omega \cap V_{n'}^{(\mathrm{Int}_{n_\alpha})^{-1}}$, так что $V_n^{\mathrm{Int}_n} \subseteq V_{n'}^{\mathrm{Int}_{n'}} \subseteq \Omega$. Тогда для любого $x \in \Omega$ справедливо $x^{\mathrm{Int}_n} = x^{\mathrm{Int}_{n'} \circ \mathrm{Int}_{n_\alpha}}$ и требуемая формула следует по индукции и из (3).

(5) Окончание доказательства леммы. Если $x, x' \in \Omega$, то запишем $x = vtu$, $x' = v't'u'$, где $v, v' \in U^-$, $t, t' \in T$, $u, u' \in U$, так что $xx' = vtuv't'u'$. Так как $U^-\Omega U = \Omega$ и в силу этапа (2) достаточно доказать, что если $uv' \in \Omega$, то $(uv')^\varphi = u^\varphi \cdot (v')^\varphi$. Ввиду (1) мы имеем $u^\varphi = n_0^\varphi \cdot (n_0^{-1}un_0)^\varphi \cdot (n_0^{-1})^\varphi$ и $v^\varphi = n_0^\varphi \cdot (n_0^{-1}vn_0)^\varphi \cdot (n_0^{-1})^\varphi$, откуда $u^\varphi \cdot (v')^\varphi = n_0^\varphi \cdot (n_0^{-1}un_0)^\varphi \cdot (n_0^{-1}v'n_0)^\varphi \cdot (n_0^{-1})^\varphi$. Поскольку $n_0^{-1}un_0 \in U^-$ и $n_0^{-1}v'n_0 \in U$, из определения морфизма φ на Ω следует, что $(n_0^{-1}un_0)^\varphi \cdot (n_0^{-1}v'n_0)^\varphi = (n_0^{-1}uv'n_0)^\varphi$. Предположение $uv' \in \Omega$ вместе с (4) завершает доказательство леммы. □

§7 Изоморфизм полупростых групп ранга 2

В предыдущем параграфе мы доказали теорему об изоморфизме простых алгебраических групп 6.6.1 при условии выполнения следующих трёх условий:

(А) Если $t_{\alpha\beta} = (n_\alpha n_\beta)^{m_{\alpha\beta}}$ для всех $\alpha, \beta \in \Pi$, то $(t_{\alpha\beta})\varphi_T = (h_\alpha h_\beta)^{m_{\alpha\beta}}$, где $m_{\alpha\beta} = |\sigma_\alpha \sigma_\beta|$.

(Б) Для любой пары фундаментальных корней $\alpha, \beta \in \Pi$ существует такой изоморфизм алгебраических групп $\varphi_{\alpha\beta}$ из $U_{\alpha\beta}$ на соответствующую подгруппу группы H, что он является расширением и φ_α, и φ_β.

(В) Пусть $\alpha, \beta \in \Pi$. Если $\gamma \in \Phi^+_{\alpha\beta}$ и $\gamma \neq \alpha$, то $\varphi_{\alpha\beta} \circ \mathrm{Int}_{h_\alpha}$ согласуется на U_γ с $\mathrm{Int}_{n_\alpha} \circ \varphi_{\alpha\beta}$.

Заметим, что при $\alpha = \beta$ условия **(Б)**,**(В)** вырождаются, а условие **(А)** проверено в лемме 6.6.5. Хотя условия **(А)**, **(Б)**, **(В)** включают в себя проверку в обеих группах G, H, мы покажем, что они допускают такую переформулировку, которая позволяет работать внутри группы G. Для доказательства **(А)** достаточно

выразить $t_{\alpha\beta}$ через t_α, t_β, используя информацию о системе ранга 2, порождённой корнями α, β (поскольку t_α, t_β и их образы уже определены по лемме 6.6.5).

Для доказательства **(Б)** мы должны выбрать $\varepsilon_\gamma \mathbb{F} \to U_\gamma$ для любого $\gamma \in \Phi^+_{\alpha\beta}$ так, чтобы этот выбор зависел лишь от корневой системы и затем показать, что константы, появляющиеся в коммутаторных формулах Шевалле (лемма 6.6.8), полностью определяются данным выбором. Таким образом, теоретико-групповое строение группы $U_{\alpha\beta}$ зависит лишь от корневой системы. С другой стороны, легко построить морфизм многообразия $U_{\alpha\beta}$ на соответствующую подгруппу группы H, используя известные вложения групп U_α, U_β. Тогда, используя ε_γ и соответствующий ему $\varepsilon'_{\gamma'}$, мы получим групповой изоморфизм. Например, в корневой системе A_2 множество положительных корней имеет вид $\alpha, \beta, \alpha+\beta$. У нас уже есть ε_α, n_β, тогда $u_{\alpha+\beta}(x) = (u_\alpha(x))^{\mathrm{Int}_{n_\beta}}$ (конечно, надо проверить, что результат не изменится, если поменять ролями корни α и β). В данной корневой системе мы закончим доказательство группового закона для $U_{\alpha\beta}$ проверкой, что $[u_\alpha(x), u_\beta(y)] = u_{\alpha+\beta}(x+y)$, в то время как $U_{\alpha+\beta} \le Z(U_{\alpha\beta})$.

Далее рассмотрим **(В)**. Требование $\gamma \neq \alpha$ эквивалентно тому, что $\delta = \gamma^{\sigma_\alpha}$ вновь является положительным корнем, значит, ε_γ и ε_δ заданы, ввиду условия **(В)**. Композиция ε_γ с Int_{n_α} влечёт ещё один допустимый изоморфизм $\mathbb{F} \to U_\delta$, который мы свяжем с ε_δ способом, зависящим лишь от корневой системы. Это гарантирует такое же соотношение в H, следовательно, доказывая **(В)**. Например, в случае корневой системы A_2, мы оставили открытым вопрос о том, как $\varepsilon_\beta \circ \mathrm{Int}_{n_\alpha}$ связаны с $\varepsilon_{\alpha+\beta}$; будет показано, что $n_\alpha^{-1} u_\beta(x) n_\alpha = u_{\alpha+\beta}(-x)$. Более точно, выбор допустимого изоморфизма ε_γ зависит лишь от умножения на ненулевой скаляр, т. е. от автоморфизма аддитивной группы поля $\mathbb{F}$. Следовательно, если $\mathsf{x}_{\alpha+\beta}$ — базисный вектор в $\mathfrak{g}_{\alpha+\beta}$, то соотношение, выписанное выше для A_2, эквивалентно равенству $\mathsf{x}_\beta^{\mathrm{Ad}\ n_\alpha} = -\mathsf{x}_{\alpha+\beta}$.

Как только мы определяем x_γ для нефундаментального положительного корня γ посредством $\mathsf{x}_\gamma = \mathsf{x}_\alpha^{\mathrm{Ad}\ n_\beta}$, где $\alpha, \beta \in \Pi$, мы также получаем $\mathsf{x}_{-\gamma} = \mathsf{x}_{-\alpha}^{\mathrm{Ad}\ n_\beta}$. Определив таким образом $\varepsilon_\gamma, \varepsilon_{-\gamma}$, мы можем положить $n_\gamma = u_\gamma(1) u_{-\gamma}(-1) u_\gamma(1)$. В этом случае, Int_{n_β} переносит канонический выбор, сделанный в Z_α на Z_γ. В частности, мы можем вычислить

$$n_\beta^{-1} n_\alpha n_\beta = (n_\beta^{-1} u_\alpha(1) n_\beta)(n_\beta^{-1} u_{-\alpha}(-1) n_\beta)(n_\beta^{-1} u_\alpha(1) n_\beta) = n_\gamma. \tag{6.3}$$

Заметим, что ввиду теоремы 2.5.1, существует лишь 4 корневых системы ранга 2: $A_1 \times A_1$, A_2, B_2, G_2. Только в системе G_2 нам потребуются длительные вычисления. Поскольку G_2 не может возникнуть в качестве подсистемы, данные вычисления не влияют на классификацию алгебраических групп с корневыми системами типов A–F. Также уместно заметить, что фундаментальная группа группы G влияет лишь на выбор элементов t_α, тогда как условия **(А), (Б), (В)** зависят лишь от корневой системы. Далее мы последовательно разберём все типы корневых систем ранга 2.

Прежде, чем переходить к изучению корневых систем, проверим, чему равны элементы t_α^β и $t_\alpha^{n_\beta}$. Для любого $\alpha \in \Pi$ коммутант $[Z_\alpha, Z_\alpha]$ изоморфен либо $\mathrm{SL}_2(\mathbb{F})$, либо $\mathrm{PGL}_2(\mathbb{F})$ (см. упражнение 6.6.6). В любом случае, соответствие $x \mapsto \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ даёт вложение $\gamma : \mathbb{F}^* \to T \cap [Z_\alpha, Z_\alpha]$, для которого $t_\alpha = (-1)^\gamma$ и для которого $< \alpha, \gamma >= 2$. Таким образом, $\gamma \in Y(T)$ можно считать равным кокорню $\check{\alpha}$. Тогда при естественном спаривании $X(T) \times Y(T) \to \mathbb{Z}$ мы имеем $< \check{\alpha}, \beta >=< \alpha, \beta >= \frac{2(\alpha,\beta)}{(\alpha,\alpha)}$. Кроме того, ввиду упражнения 5.6.10, это спаривание согласовано с действием группы W. Отсюда вытекают следующие основные формулы:

$$t_\alpha^\beta = ((-1)^{\check{\alpha}})^\beta = (-1)^{<\alpha,\beta>}; \tag{6.4}$$

$$t_\alpha^{n_\beta} = (-1)^{\check{\alpha}\sigma\beta} = (-1)^{\check{\alpha} - <\beta,\alpha>\check{\beta}} = (-1)^{\check{\alpha}}((-1)^{-<\alpha,\beta>})^{\check{\beta}} = t_\alpha t_\beta^{-<\alpha,\beta>}. \tag{6.5}$$

Корневая система типа $A_1 \times A_1$. Отметим, что коммутаторная формула Шевалле 6.6.8 показывает, что $[U_\alpha, U_\beta] = \{e\}$, если $\alpha + \beta \notin \Phi$. В частности, если α, β таковы, что ни $\alpha+\beta$, ни $\alpha-\beta$ не являются корнями, то $\mathsf{x}_\beta^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_\beta$ и $\mathsf{x}_\alpha^{\mathrm{Ad}\ n_\beta} = \mathsf{x}_\alpha$; кроме того $n_\alpha n_\beta = n_\beta n_\alpha$. Отсюда сразу следуют требуемые утверждения для корневой системы $A_1 \times A_1$.

Лемма 6.7.1. *Пусть $\Phi_{\alpha\beta}$ имеет тип $A_1 \times A_1$ с положительными фундаментальными корнями α, β. Тогда:*

(а) $t_{\alpha\beta} = (n_\alpha n_\beta)^2 = t_\alpha t_\beta = (n_\beta n_\alpha)^2 = t_{\beta\alpha}$;

(б) $[U_\alpha, U_\beta] = \{e\}$;

(в) $\mathsf{x}_\beta^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_\beta$ *и* $\mathsf{x}_\alpha^{\mathrm{Ad}\ n_\beta} = \mathsf{x}_\alpha$.

Корневая система типа A_2.

Лемма 6.7.2. *Предположим, что $\Phi_{\alpha\beta}$ имеет тип A_2 и её положительные корни равны $\alpha, \beta, \alpha+\beta$. Положим $\mathsf{x}_{\alpha+\beta} = \mathsf{x}_{\alpha}^{\mathrm{Ad}\ n_\beta}$. Тогда:*

(а) $t_{\alpha\beta} = (n_\alpha n_\beta)^3 = e = (n_\beta n_\alpha)^3 = t_{\beta\alpha}$;

(б) *для всех* $x, y \in \mathbb{F}$, $u_\beta(y)u_\alpha(x) = u_\alpha(x)u_\beta(y)u_{\alpha+\beta}(-xy)$;

(в) $\mathsf{x}_{\beta}^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_{\alpha+\beta}$, $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = -\mathsf{x}_\beta$, $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = -\mathsf{x}_\alpha$.

Доказательство. Поскольку $<\alpha,\beta>=<\beta,\alpha>= -1$, форумула (6.4) влечёт $t_\alpha^\beta = t_\beta^\alpha = -1$. Из определения $\mathsf{x}_{\alpha+\beta}$ вытекает, что $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = t_\beta^\alpha \mathsf{x}_\alpha = -\mathsf{x}_\alpha$, как и утверждается в (в). С другой стороны, $\mathsf{x}_{\beta}^{\mathrm{Ad}\ n_\alpha} = b\mathsf{x}_{\alpha+\beta}$ для некоторого $b \in \mathbb{F}$, следовательно, $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = t_\alpha^\beta b^{-1}\mathsf{x}_\beta = -b^{-1}\mathsf{x}_\beta$. Значит, для доказательства остальных утверждений пункта (в) достаточно показать, что $b = 1$.

По лемме 6.6.8, существует такой элемент $a \in \mathbb{F}$, независящий от x, y, что выполнено следующее тождество:

$$u_\beta(y)u_\alpha(x) = u_\alpha(x)u_\beta(y)u_{\alpha+\beta}(axy). \tag{6.6}$$

Чтобы доказать (б) нужно показать, что $a = -1$. Применив Int_{n_β} к обеим частям (6.6), получим:

$$u_{-\beta}(-y)u_{\alpha+\beta}(x) = u_{\alpha+\beta}(x)u_{-\beta}(-y)u_\alpha(-axy). \tag{6.7}$$

По определению, $n_\beta^{-1}u_\alpha(x)n_\beta = u_{\alpha+\beta}(x)$, поэтому, записав $n_\beta = u_\beta(1)u_{-\beta}(-1)u_\beta(1)$, получаем:

$$u_\beta(-1)u_{-\beta}(1)u_\beta(-1)u_\alpha(x)u_\beta(1)u_{-\beta}(-1)u_\beta(1) = u_{\alpha+\beta}(x). \tag{6.8}$$

Поскольку $\alpha + 2\beta \notin \Phi$, элементы $x_{\alpha+\beta}(x)$ и $x_\beta(y)$ коммутируют для любых $x, y \in \mathbb{F}$, поэтому 6.8 можно переписать как:

$$u_\beta(-1)u_\alpha(x)u_\beta(1) = u_{-\beta}(-1)u_{\alpha+\beta}(x)u_{-\beta}(1). \tag{6.9}$$

После применения (6.6) к левой части (при $y = -1$) и (6.7) к правой части (при $y = 1$), равенство (6.9) принимает вид:

$$u_\alpha(x)u_\beta(-1)u_{\alpha+\beta}(-ax)u_\beta(1) = u_{\alpha+\beta}(x)u_{-\beta}(-1)u_\alpha(-ax)u_{-\beta}(1). \tag{6.10}$$

Поскольку $\alpha + 2\beta, \alpha - \beta, 2\alpha + \beta \notin \Phi$, мы вновь используем факт, что элементы из подгрупп $U_{\alpha+\beta}$ и U_β, U_α и $U_{-\beta}$, U_α и $U_{\alpha+\beta}$ соответственно попарно коммутируют. Поэтому 6.10 можно записать как:

$$u_\alpha(x)u_{\alpha+\beta}(-ax) = u_\alpha(-ax)u_{\alpha+\beta}(x). \tag{6.11}$$

Поскольку U прямо порождается подгруппами U_α (см. лемму 6.4.1 отсюда следует, что $a = -1$, что доказывает (б). Далее применим Int_{n_α} к обеим частям равенства (6.6):

$$u_{\alpha+\beta}(by)u_{-\alpha}(-x) = u_{-\alpha}(-x)u_{\alpha+\beta}(by)u_\beta(b^{-1}xy). \tag{6.12}$$

Аналогично тому, как из $n_\beta^{-1}u_\alpha(x)n_\beta = u_{\alpha+\beta}(x)$ было получено равенство 6.9, из $n_\alpha^{-1}u_\beta(y)n_\alpha = u_{\alpha+\beta}(by)$ получается:

$$u_\alpha(-1)u_\beta(y)u_\alpha(1) = u_{-\alpha}(-1)u_{\alpha+\beta}(by)u_{-\alpha}(-1). \tag{6.13}$$

Теперь применяя (6.6) к левой части равенства (6.13) и (6.12) к правой части равенства (6.13), получаем:

$$u_\beta(y)u_{\alpha+\beta}(y) = u_\beta(-b^{-1}y)u_{\alpha+\beta}(by). \tag{6.14}$$

Вновь используя лемму 6.4.1, получаем, что $\beta = 1$. Осталось доказать пункт (а) леммы. Рассмотрим равенство

$$n_\alpha n_\beta n_\alpha = n_\alpha^2 n_\alpha^{-1} n_\beta n_\alpha = t_\alpha n_{\alpha+\beta}^{-1}, \tag{6.15}$$

где $n_\alpha^{-1}n_\beta n_\alpha$ вычислено по форумуле (6.3). Из (6.3) (6.5) и (6.15) мы получаем:

$$n_\beta n_\alpha n_\beta n_\alpha n_\beta = n_\beta^2 n_\beta^{-1} t_\alpha n_{\alpha+\beta}^{-1} n_\beta = t_\beta t_\alpha t_\beta^{-<\alpha,\beta>} n_\beta^{-1} n_{\alpha+\beta}^{-1} n_\beta = t_\beta t_\alpha t_\beta^{-<\alpha,\beta>} = t_\alpha n_\alpha = n_\alpha^{-1}, \tag{6.16}$$

где мы используем тот факт, что $t_\alpha^2 = t_\beta^2 = e$. Отсюда следует (а). □

Корневая система типа B_2.

Лемма 6.7.3. *Пусть $\Phi_{\alpha\beta}$ имеет тип B_2 и её положительные корни $\alpha, \beta, \alpha+\beta, 2\alpha+\beta$. Положим $\mathsf{x}_{\alpha+\beta} = \mathsf{x}_\alpha^{\mathrm{Ad}\ n_\beta}$, $\mathsf{x}_{2\alpha+\beta} = \mathsf{x}_\beta^{\mathrm{Ad}\ n_\alpha}$. Тогда:*

(а) $t_{\alpha\beta} = (n_\alpha n_\beta)^4 = t_\alpha = (n_\beta n_\alpha)^4 = t_{\beta\alpha}$;

(б) $u_\beta(y)u_\alpha(x) = u_\alpha(x)u_\beta(y)u_{\alpha+\beta}(-xy)u_{2\alpha+\beta}(x^2y)$ *и* $u_{\alpha+\beta}(y)u_\alpha(x) = u_\alpha(x)u_{\alpha+\beta}(y)u_{2\alpha+\beta}(-2xy)$;

(в) $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_{\alpha+\beta}$, $\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_\beta$, $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = -\mathsf{x}_\alpha$, $\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = \mathsf{x}_{2\alpha+\beta}$.

Доказательство. Поскольку $<\beta,\alpha>= -1$, $<\alpha,\beta>= -2$, формула (6.4) даёт $t_\beta^\alpha = -1$, $t_\alpha^\beta = 1$. Из определения $\mathsf{x}_{\alpha+\beta}$ и $\mathsf{x}_{2\alpha+\beta}$ вытекает, что $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = t_\beta^\alpha \mathsf{x}_\alpha = -\mathsf{x}_\alpha$ и что $\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = t_\alpha^\beta \mathsf{x}_\beta = \mathsf{x}_\beta$, как и утверждается в (в). Более того, поскольку $2\alpha+2\beta, 2\alpha \notin \Phi$, подгруппы $U_{\pm\beta}$ централизуют $U_{2\alpha+\beta}$, следовательно, $\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = \mathsf{x}_{2\alpha+\beta}$. Чтобы закончить доказательство (в) нам необходимо показать, что $d = 1$, где $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = d\mathsf{x}_{\alpha+\beta}$.

Коммутаторная форумула Шевалле (лемма 6.6.8) даёт существование таких скаляров $a, b, c \in \mathbb{F}$ (независящих от $x, y \in \mathbb{F}$), что выполнены следующие равенства:

$$u_\beta(y)u_\alpha(x) = u_\alpha(x)u_\beta(y)u_{\alpha+\beta}(axy)u_{2\alpha+\beta}(bx^2y), \tag{6.17}$$

$$u_{\alpha+\beta}(y)u_\alpha(x) = u_\alpha(x)u_{\alpha+\beta}(y)u_{2\alpha+\beta}(cxy). \tag{6.18}$$

Для доказательства (б) нужно показать, что $a = -1$, $b = 1$ и $c = -2$. Применяя Int_{n_α} к обеим частям равенства (6.17) (соотв. (6.18)), получим:

$$u_{2\alpha+\beta}(y)u_{-\alpha}(-x) = u_{-\alpha}(-x)u_{2\alpha+\beta}(y)u_{\alpha+\beta}(adxy)u_\beta(bx^2y), \tag{6.19}$$

$$u_{\alpha+\beta}(dy)u_{-\alpha}(-x) = u_{-\alpha}(-x)u_{\alpha+\beta}(dy)u_\beta(cxy). \tag{6.20}$$

Аналогично, применяя Int_{n_β} к обеим частям равенства (6.17):

$$u_{-\beta}(-y)u_{\alpha+\beta}(x) = u_{\alpha+\beta}(x)u_{-\beta}(-y)u_\alpha(-axy)u_{2\alpha+\beta}(bx^2y). \tag{6.21}$$

Поскольку $n_\beta^{-1}u_\alpha(x)n_\beta = u_{\alpha+\beta}(x)$ и из того факта, что $\alpha+2\beta \notin \Phi$ (поэтому элементы из U_β и $U_{\alpha+\beta}$ попарно коммутируют), мы получаем:

$$u_\beta(-1)u_\alpha(x)u_\beta(1) = u_{-\beta}(-1)u_{\alpha+\beta}(x)u_{-\beta}(1). \tag{6.22}$$

Применяя (6.17) к левой части и (6.21) к правой части, равенство (6.22) принимает вид:

$$u_\alpha(x)u_\beta(-1)u_{\alpha+\beta}(-ax)u_{2\alpha+\beta}(-bx^2)u_\beta(1) = u_{\alpha+\beta}(x)u_{-\beta}(-1)u_\alpha(-ax)u_{2\alpha+\beta}(bx^2)u_{-beta}(1). \tag{6.23}$$

Вновь используя тот факт, что $\alpha+2\beta, 2\alpha+2\beta, \alpha-\beta, 2\alpha \notin \Phi$, мы получаем что элементы из $U_{\alpha+\beta}$ и U_β, $U_{2\alpha+\beta}$ и U_β, U_α и $U_{-\beta}$, $U_{2\alpha+\beta}$ и $U_{-\beta}$ попарно коммутируют. Поэтому равенство (6.23) принимает вид:

$$u_\alpha(x)u_{\alpha+\beta}(-ax)u_{2\alpha+\beta}(-bx^2) = u_{\alpha+\beta}(x)u_\alpha(-ax)u_{2\alpha+\beta}(bx^2). \tag{6.24}$$

В свою очередь (6.18) можно применить к правой части, чтобы получить:

$$u_\alpha(x)u_{\alpha+\beta}(-ax)u_{2\alpha+\beta}(-bx^2) = u_\alpha(-ax)u_{\alpha+\beta}(x)u_{2\alpha+\beta}((b-ca)x^2). \tag{6.25}$$

Как и раньше лемме 6.4.1 влечёт, что $a = -1$ и $c = -2b$. Из равенства $n_\alpha^{-1}u_\beta(y)n_\alpha = u_{2\alpha+\beta}(y)$ и того факта, что $3\alpha+\beta \notin \Phi$ (значит, элементы групп U_α и $U_{2\alpha+\beta}$ попарно перестановочны), мы далее получаем:

$$u_\alpha(-1)u_\beta(y)u_\alpha(1) = u_{-\alpha}(-1)u_{2\alpha+\beta}(y)u_{-\alpha}(1). \tag{6.26}$$

После применения (6.17) к левой части и (6.19) к правой части, равенство (6.26) принимает вид:

$$u_\beta(y)u_{\alpha+\beta}(-y)u_{2\alpha+\beta}(by) = u_{2\alpha+\beta}(y)u_{\alpha+\beta}(-dy)u_\beta(by). \tag{6.27}$$

Поскольку элементы из U_β, $U_{\alpha+\beta}$ и $U_{2\alpha+\beta}$ попарно коммутируют, мы делаем вывод, что $b = 1$, $d = 1$, $c = -2$. Осталось доказать (а). Начнём с:

$$n_\alpha n_\beta n_\alpha = t)\alpha n_\alpha^{-1}n_\beta n_\alpha = t_\alpha n_{2\alpha+\beta}, \tag{6.28}$$

где мы вновь используем форумулу (6.3). Следующий шаг:

$$n_\beta n_\alpha n_\beta n_\alpha n_\beta = t_\beta n_\beta^{-1} t_\alpha n_{2\alpha+\beta} n_\beta = t_\beta t_\alpha t_\beta^{-<\alpha,\beta>} n_\beta^{-1} n_{2\alpha+\beta} n_\beta = t_\alpha t_\beta n_{2\alpha+\beta}, \tag{6.29}$$

поскольку $<\alpha,\beta>=-2$, $t_\beta^2=e$ и $n_\beta, n_{2\alpha+\beta}$ перестановочны. Тогда:

$$n_\alpha (n_\beta n_\alpha)^3 = t_\alpha (n_\alpha^{-1} t_\alpha t_\beta n_\alpha)(n_\alpha^{-1} n_{2\alpha+\beta} n_\alpha) = t_\alpha t_\alpha t_\beta t_\alpha^{-<\beta,\alpha>} n_\beta = t_\alpha t_\beta n_\beta. \tag{6.30}$$

Наконец, (6.30) влечёт, что $(n_\alpha n_\beta)^4 = t_\alpha = (n_\beta n_\alpha)^4$. □

Корневая система типа G_2.

Лемма 6.7.4. *Предположим, что $\Phi_{\alpha\beta}$ имеет тип G_2 и её положительные корни равны $\alpha, \beta, 2\alpha+\beta, 3\alpha+\beta, 3\alpha+2\beta$. Положим $\mathsf{x}_{\alpha+\beta} = \mathsf{x}_\beta^{\mathrm{Ad}\ n_\beta}$, $\mathsf{x}_{2\alpha+\beta} = \mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} \mathsf{x}_{3\alpha+\beta} = (-\mathsf{x}_\beta)^{\mathrm{Ad}\ n_\alpha}, \mathsf{x}_{3\alpha+2\beta} = \mathsf{x}_{3\alpha+\beta}^{\mathrm{Ad}\ n_\beta}$. Тогда:*

(а) $t_{\alpha\beta} = (n_\alpha n_\beta)^6 = e = (n_\beta n_\alpha)^6 = t_{\beta\alpha}$;

(б) *для всех $x, y \in \mathbb{F}$,*

$$\begin{aligned}
u_\beta(y)u_\alpha(x) &= u_\alpha(x)u_\beta(y)u_{\alpha+\beta}(-xy)u_{2\alpha+\beta}(x^2y)u_{3\alpha+\beta}(-x^3y)u_{3\alpha+2\beta}(x^3y^2),\\
u_{\alpha+\beta}(y)u_\alpha(x) &= u_\alpha(x)u_{\alpha+\beta}(y)u_{2\alpha+\beta}(2xy)u_{3\alpha+\beta}(3x^2y)u_{3\alpha+2\beta}(3xy^2),\\
u_{2\alpha+\beta}(y)u_\alpha(x) &= u_\alpha(x)u_{2\alpha+\beta}(y)u_{3\alpha+\beta}(-3xy),\\
u_{3\alpha+\beta}(y)u_\beta(x) &= u_\beta(x)u_{3\alpha+\beta}(y)u_{3\alpha+2\beta}(xy),\\
u_{2\alpha+\beta}(y)u_{\alpha+\beta}(x) &= u_{\alpha+\beta}(x)u_{2\alpha+\beta}(y)u_{3\alpha+2\beta}(-3xy);
\end{aligned}$$

(в) $\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = -\mathsf{x}_{\alpha+\beta}$, $\mathsf{x}_{3\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_\beta$, $\mathsf{x}_{3\alpha+2\beta}^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_{3\alpha+2\beta}$, $\mathsf{x}_{\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = -\mathsf{x}_\alpha$, $\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = \mathsf{x}_{2\alpha+\beta}$, $\mathsf{x}_{3\alpha+2\beta}^{\mathrm{Ad}\ n_\beta} = -\mathsf{x}_{3\alpha+\beta}$.

Доказательство. Поскольку $<\alpha,\beta>=-3$ и $<\beta,\alpha>=-1$, мы имеем $t_\alpha^\beta = t_\beta^\alpha = -1$ (напомним, что $t_\alpha^2 = t_\beta^2 = e$). Из определения следует, что:

$$\mathsf{x}_{\alpha+\beta}^{n_\beta} = t_\beta^\alpha \mathsf{x}_\alpha = -\mathsf{x}_\alpha, \tag{6.31}$$

$$\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = t_\alpha^\alpha t_\alpha^\beta \mathsf{x}_{\alpha+\beta} = -\mathsf{x}_{\alpha+\beta}, \tag{6.32}$$

$$\mathsf{x}_{3\alpha+\beta}^{\mathrm{Ad}\ n_\alpha} = -t_\alpha^\beta \mathsf{x}_\beta = \mathsf{x}_\beta, \tag{6.33}$$

$$\mathsf{x}_{3\alpha+2\beta}^{\mathrm{Ad}\ n_\beta} = (t_\beta^\alpha)^3 t_\beta^\beta \mathsf{x}_{3\alpha+\beta} = -\mathsf{x}_{3\alpha+\beta}. \tag{6.34}$$

Поскольку $(3\alpha+2\beta)\pm\alpha \notin \Phi$ и $(2\alpha+\beta)\pm\beta \notin \Phi$, мы также получаем:

$$\mathsf{x}_{3\alpha+2\beta}^{\mathrm{Ad}\ n_\alpha} = \mathsf{x}_{3\alpha+2\beta}, \tag{6.35}$$

$$\mathsf{x}_{2\alpha+\beta}^{\mathrm{Ad}\ n_\beta} = \mathsf{x}_{2\alpha+\beta}. \tag{6.36}$$

Равенства (6.31)–(6.36) дают (в). Обратимся теперь к (б). Вновь, используя коммутаторную формулу Шевалле (лемма 6.6.8), получаем существование таких констант $a, b, c, d, e, f, g, h, i$ (независящих от x, y), что справедливы следующие формулы:

$$u_\beta(y)u_\alpha(x) = u_\alpha(x)u_\beta(y)u_{\alpha+\beta}(axy)u_{2\alpha+\beta}(bx^2y)u_{3\alpha+\beta}(cx^3y)u_{3\alpha+2\beta}(dx^3y^2), \tag{6.37}$$

$$u_{\alpha+\beta}(y)u_\alpha(x) = u_\alpha(x)u_{\alpha+\beta}(y)u_{2\alpha+\beta}(exy)u_{3\alpha+\beta}(fx^2y)u_{3\alpha+2\beta}(gxy^2), \tag{6.38}$$

$$u_{2\alpha+\beta}(y)u_\alpha(x) = u_\alpha(x)u_{2\alpha+\beta}(y)u_{3\alpha+\beta}(hxy), \tag{6.39}$$

$$u_{3\alpha+\beta}(y)u_\beta(x) = u_\beta(x)u_{3\alpha+\beta}(y)u_{3\alpha+2\beta}(ixy). \tag{6.40}$$

Действуя Int_{n_β} на обеих частях равенств (6.37), (6.39) и (6.40), мы получаем соответственно:

$$u_{-\beta}(-y)u_{\alpha+\beta}(x) = u_{\alpha+\beta}(x)u_{-\beta}(-y)u_\alpha(-axy)u_{2\alpha+\beta}(bx^2y)u_{3\alpha+2\beta}(cx^3y)u_{3\alpha+\beta}(-dx^3y^2), \tag{6.41}$$

$$u_{2\alpha+\beta}(y)u_{\alpha+\beta}(x) = u_{\alpha+\beta}(x)u_{2\alpha+\beta}(y)u_{3\alpha+2\beta}(hxy), \tag{6.42}$$

$$u_{3\alpha+2\beta}(y)u_{-\beta}(-x) = u_{-\beta}(-x)u_{3\alpha+2\beta}(y)u_{3\alpha+\beta}(-ixy). \tag{6.43}$$

Аналогично подействуем Int_{n_α} на обе части равенства (6.37):

$$u_{3\alpha+\beta}(-y)u_{-\alpha}(-x) = u_{-\alpha}(-x)u_{3\alpha+\beta}(-y)u_{2\alpha+\beta}(axy)u_{\alpha+\beta}(-bx^2y)u_\beta(cx^3y)u_{3\alpha+2\beta}(dx^3y^2). \tag{6.44}$$

Из-за того, что $\alpha \pm 2\beta \notin \Phi$, равенство $n_\beta^{-1}u_\alpha(x)n_\beta = u_{\alpha+\beta}(x)$ упрощается до:

$$u_\beta(-1)u_\alpha(x)u_\beta(1) = u_{-\beta}(-1)u_{\alpha+\beta}(x)u_{-\beta}(1). \tag{6.45}$$

Последовательным применением (6.37) и (6.40) левая часть равенства (6.45) может быть записана:

$$\begin{aligned} &u_\beta(-1)u_\alpha(x)u_\beta(1) = \\ &\qquad u_\alpha(x)u_\beta(-1)u_{\alpha+\beta}(-ax)u_{2\alpha+\beta}(-bx^2)u_{3\alpha+\beta}(-cx^3)u_{3\alpha+2\beta}(dx^3)u_\beta(1) = \\ &\qquad u_\alpha(x)u_\beta(-1)u_{\alpha+\beta}(-ax)u_{2\alpha+\beta}(-bx^2)u_\beta(1)u_{3\alpha+\beta}(-cx^3)u_{3\alpha+2\beta}((d-ci)x^3) = \\ &\qquad u_\alpha(x)u_{\alpha+\beta}(-ax)u_{2\alpha+\beta}(-bx^2)u_{3\alpha+\beta}(-cx^3)u_{3\alpha+2\beta}((d-ci)x^3). \end{aligned} \tag{6.46}$$

Последовательным применением (6.41) и затем (6.43), правая часть равенства (6.45) может быть записана:

$$\begin{aligned} &u_{-\beta}(-1)u_{\alpha+\beta}(x)u_{-\beta}(1) = \\ &\qquad u_{\alpha+\beta}(x)u_{-\beta}(-1)u_\alpha(-ax)u_{2\alpha+\beta}(bx^2)u_{3\alpha+2\beta}(cx^3)u_{3\alpha+\beta}(-dx^3)u_{-\beta}(1) = \\ &\qquad u_{\alpha+\beta}(x)u_\alpha(-ax)u_{2\alpha+\beta}(bx^2)u_{3\alpha+2\beta}(cx^3)u_{3\alpha+\beta}((ci-d)x^3). \end{aligned} \tag{6.47}$$

Следующим шагом (6.38) преобразует правую часть равенства (6.47) в:

$$\begin{aligned} &u_\alpha(-ax)u_{\alpha+\beta}(x)u_{2\alpha+\beta}(-aex^2)u_{3\alpha+\beta}(a^2fx^3)u_{3\alpha+2\beta}(-agx^3)u_{2\alpha+\beta}(bx^2)u_{3\alpha+2\beta}(cx^3)u_{3\alpha+\beta}((ci-d)x^3) = \\ &\qquad u_\alpha(-ax)u_{\alpha+\beta}(x)u_{2\alpha+\beta}((b-ae)x^2)u_{3\alpha+\beta}((a^2f+ci-d)x^3)u_{3\alpha+2\beta}((c-ag)x^3). \end{aligned} \tag{6.48}$$

Сравнение выражений (6.46) и (6.48) влечёт:

$$a=-1,\ e=2b,\ d-c=f+ci,\ f=g. \tag{6.49}$$

Так как $4\alpha+\beta \notin \Phi$, равенство $n_\alpha^{-1}u_\beta(y)n_\alpha = u_{3\alpha+\beta}(-y)$ можно упростить до:

$$u_\alpha(-1)u_\beta(y)u_\alpha(1) = u_{-\alpha}(-1)u_{3\alpha+\beta}(-y)u_{-\alpha}(1). \tag{6.50}$$

Применяем (6.37) к левой части, чтобы получить:

$$u_\alpha(-1)u_\beta(y)u_\alpha(1) = u_\beta(y)u_{\alpha+\beta}(-y)u_{2\alpha+\beta}(by)u_{3\alpha+\beta}(cy)u_{3\alpha+2\beta}(dy^2). \tag{6.51}$$

Применяем последовательно (6.44), (6.42), (6.40) к правой части равенства (6.50), чтобы получить:

$$\begin{aligned} &u_{-\alpha}(-1)u_{3\alpha+\beta}(-y)u_{-\alpha}(1) = \\ &\qquad u_{3\alpha+\beta}(-y)u_{2\alpha+\beta}(y)u_{\alpha+\beta}(-by)u_\beta(-cy)u_{3\alpha+2\beta}(-dy^2) = \\ &\qquad u_{3\alpha+\beta}(-y)u_{\alpha+\beta}(-by)u_{2\alpha+\beta}(y)u_{3\alpha+2\beta}(-hby^2)u_\beta(-cy)u_{3\alpha+2\beta}(-dy^2) = \\ &\qquad u_\beta(-cy)u_{\alpha+\beta}(-by)u_{2\alpha+\beta}(y)u_{3\alpha+\beta}(-y)u_{3\alpha+2\beta}((ci-d-bh)y^2). \end{aligned} \tag{6.52}$$

Сравнение (6.51) и (6.52) даёт:

$$c=-1,\ b=1,\ 2d+i-h=0. \tag{6.53}$$

Вместе с формулами (6.46) равенства (6.53) дают нам:

$$a=c=-1,\ b=1,\ e=2,\ f=g,\ 2d=-h-i,\ d+1=f-i. \tag{6.54}$$

Далее мы используем равенство $n_\beta^{-1}u_{3\alpha+\beta}(x)n_\beta = u_{3\alpha+2\beta}(x)$, которое переписывается:

$$u_\beta(-1)u_{3\alpha+\beta}(x)u_\beta(1) = u_{-\beta}(-1)u_{3\alpha+2\beta}(x)u_{-\beta}(1). \tag{6.55}$$

Преобразуем левую часть, используя (6.40), и правую часть, используя (6.43), чтобы получить:

$$u_{3\alpha+\beta}(x)u_{3\alpha+2\beta}(ix) = u_{3\alpha+2\beta}(x)u_{3\alpha+\beta}(ix), \tag{6.56}$$

откуда $i = 1$. Наконец, используем равенство $n_\alpha^{-1}u_{\alpha+\beta}(y)n_\alpha = u_{2\alpha+\beta}(y)$, записанное в виде:

$$u_\alpha(-1)u_{\alpha+\beta}(y)u_\alpha(1) = u_{-\alpha}(-1)u_\alpha(1)u_{2\alpha+\beta}(y)u_\alpha(-1)u_{-\alpha}(1). \tag{6.57}$$

Преобразуем левую часть с помощью (6.38), а правую часть с помощью (6.39), чтобы получить

$$u_{\alpha+\beta}(y)u_{2\alpha+\beta}(2y)u_{3\alpha+\beta}(fy)u_{3\alpha+2\beta}(gy^2) = u_{-\alpha}(-1)u_{2\alpha+\beta}(y)u_{3\alpha+\beta}(-hy)u_{-\alpha}(1). \tag{6.58}$$

Передвижение $u_{-\alpha}(1)$ влево требует перестановки с $u_{3\alpha+\beta}$ и затем перестановки с $u_{2\alpha+\beta}(y)$, которые не дают новых символов вида $u_{3\alpha+\beta}$ в правой части равенства (6.58). Следовательно, $f = -h$ и, используя форумулы (6.54), получаем:

$$a = c = -1,\ b = d = i = 1,\ e = 2, f = g = 3, h = -3, \tag{6.59}$$

таким образом доказывая первые четыре формулы из (б). Пятая формула из (б) следует из (6.42).

Осталось доказать (а). Мы действуем также, как и в предыдущих леммах:

$$n_\alpha n_\beta n_\alpha = t_\alpha n_{3\alpha+\beta}^{-1}. \tag{6.60}$$

$$n_\beta(n_\alpha n_\beta)^2 = t_\beta(n_\beta^{-1}t_\alpha n_\beta)(n_\beta^{-1}n_{3\alpha+\beta}^{-1}n_\beta) = t_\alpha n_{3\alpha+2\beta}^{-1}. \tag{6.61}$$

$$n_\alpha(n_\beta n_\alpha)^3 = n_\alpha^{-1}n_{3\alpha+2\beta}^{-1}n_\alpha = n_{3\alpha+2\beta}^{-1}. \tag{6.62}$$

$$n_\beta(n_\alpha n_\beta)^4 = t_\beta n_\beta^{-1}n_{3\alpha+2\beta}^{-1}n_\beta = t_\beta n_{3\alpha+\beta}. \tag{6.63}$$

$$n_\alpha(n_\beta n_\alpha)^5 = t_\alpha(n_\alpha^{-1}t_\beta n_\alpha)(n_\alpha^{-1}n_{3\alpha+\beta}n_\alpha) = t_\alpha t_\alpha t_\beta n_\beta = n_\beta^{-1}. \tag{6.64}$$

Наконец, $(n_\alpha n_\beta)^6 = (n_\beta n_\alpha)^6 = e$. □

§8 Существование простых групп

При доказательстве теоремы об изоморфизме мы не рассматривали вопросы существования. Типы A–D называются классическими, в то время как типы E–F называются исключительными.

Односвязные группы типа A_n и C_n изоморфны матричным группам $\mathrm{SL}_{n+1}(\mathbb{F})$ и $\mathrm{Sp}_{2n}(\mathbb{F})$ и все остальные группы этих типов получаются как факторгруппы по подгруппе из центра. Для типа B_n группа $\mathrm{SO}_{2n+1}(\mathbb{F}) = \mathrm{PSO}_{2n+1}(\mathbb{F})$ имеет присоединённый тип, и для типа D_n группа $\mathrm{PSO}_{2n}(\mathbb{F})$ имеет присоединённый тип, в то время как факторгруппа $\mathrm{SO}_{2n}(\mathbb{F})/\mathrm{PSO}_{2n}(\mathbb{F})$ имее порядок 2. Для построения соответствующих односвязных групп необходимо рассматривать более сложные спинорные группы, которые реализуются как группы автоморфизмов некоторых алгебр Клиффорда.

Заметим, что все алгебраические группы являются примерами, так называемых, групп Шевалле. Присоединённые группы Шевалле над произвольными полями для всех типов корневых систем построены, например, в [3]. Там же приведены формулы для подсчета структурных констант в коммутаторной формуле Шевалле для произвольных корней.

Глава 7. Подгруппы и автоморфизмы алгебраических групп

§1 Разложение Леви

Напомним, что подгруппа P связной редуктивной алгебраической группы G называется параболической, если она содержит некоторую подгруппу Бореля B. Ввиду следствия 5.5.13 мы получаем, что для любой параболической подгруппы P выполнено $P = N_G(P)$. Зафиксируем подгруппу Бореля B и рассмотрим множество параболических подгрупп, содержащих подгруппу B. По следствию 5.5.14 мы получаем, что две параболические подгруппы, содержащие B, сопряжены тогда и только тогда, когда они совпадают. Кроме того, поскольку G является группой с BN-парой, параболические подгруппы группы G, содержащие B находятся в биективном соответствии с подмножествами множества фундаментальных корней Π корневой системы Φ (см. леммы 6.1.4 и 6.1.7). Таким образом, любую параболическую подгруппу можно записать в виде $P = P_I$, где $I \subseteq \Pi$.

Рассмотрим унипотентный радикал $R_u(P_I)$. В том случае, когда $I = \Pi$ или $I = \varnothing$ мы получаем, что $P_i = G$ или $P_i = B$ соответственно и строение унипотентного радикала очевидно. Обозначим за Ψ подсистему системы Φ, порождённую множеством I. В ведённых обозначениях справедлива следующая лемма.

Лемма 7.1.1. $R_u(P_I)$ *прямо порождается множеством* $\{U_\alpha | \alpha \in \Phi^+ \setminus \Psi\}$.

Доказательство. Поскольку P содержит максимальный тор T, радикал $R_u(P)$ является T-инвариантной замкнутой подгруппой. По лемме 6.4.1 он прямо порождается теми U_α, которые в него в ходят. Поскольку для любого $\alpha \in \Psi$ его противоположный корень $-\alpha$ также лежит в Ψ, а $U_{-\alpha}$ не нормализует U_α, мы получаем, что никакая группа U_α, $\alpha \in \Psi$ не лежит в $R_u(P_I)$. С другой стороны, любой σ_α, где $\alpha \in I$ оставляет инвариантным множество $\Phi^+ \setminus \Psi$, откуда следует лемма. □

Таким образом, алгебра Ли $\mathcal{L}(P) = \mathfrak{p}$ раскладывается в прямую сумму $\mathfrak{l} \oplus \mathfrak{u}$, где $\mathfrak{l} = \mathfrak{t} \oplus \bigoplus_{\alpha\in\Psi} \mathfrak{g}_\alpha$ и $\mathfrak{u} = \mathcal{L}(R_u(P_I)) = \bigoplus_{\alpha\in\Phi^+\setminus\Psi} \mathfrak{g}_\alpha$. Поскольку $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subseteq \mathfrak{g}_{\alpha+\beta}$ (данное свойство следует из полученной классификации простых алгебраических групп и известных свойств алгебр Ли), то $\mathfrak{l}$ является подалгеброй, а $\mathfrak{u}$ — идеалом алгебры $\mathfrak{p}$. Наша задача в данном параграфе получить аналогичное разложение для параболической подгруппы P_I в виде $P_I = l \leftthreetimes V$, где $V = R_u(P_I)$ и L должна быть редуктивной подгруппой максимального ранга с корневой системой Ψ. Такое разложение (если оно существует) называется *разложением Леви*, а подгруппа L — *фактором Леви.*

Подгруппу L можно построить тремя способами. Рассмотрим следующую подгруппу группы P_I:

$$L = \langle T, U_\alpha | \alpha \in \Psi \rangle.$$

Поскольку для любого $\alpha \in \Psi$ его противоположный $-\alpha$ также лежит в Ψ, мы получаем, что L редуктивна. Кроме того, в силу коммутаторной формулы Шевалле (лемма 6.6.8), мы получаем, что корневая система подгруппы L совпадает с Ψ, следовательно, $\mathcal{L}(L) = \mathfrak{t} \oplus \bigoplus_{\alpha\in\Psi} \mathfrak{g}_\alpha$ и $L \cap U = \{e\}$.

Другой способ — рассмотреть подгруппу $B^- \cap P = B_1$ и положить $L = B_1 W_I B_1$ (группа W_I определена в § 3 главы 2). Здесь, однако, есть некоторые трудности с доказательством того, что L редуктивна и не пересекается с V.

Третий способ является для нас наиболее предпочтительным. Рассмотрим тор $Z = (\cap_{\alpha\in I} \mathrm{Ker}(\alpha))$ и определить $L = C_G(Z)$. По следствию 5.7.8 мы получаем, что L — редуктивная подгруппа группы G. Корни, которые тривиальны на Z — это в точности корни, лежащие в Ψ по построению. В частности, $\mathcal{L}(L) = \mathfrak{l} = \mathfrak{t} \oplus \bigoplus_{\alpha\in\Psi} \mathfrak{g}_\alpha \leq \mathfrak{p}$. В силу равенства централизаторов диагонализируемых подгрупп в алгебраических группах и в алгебрах Ли (лемма 5.3.6), мы получаем, что $L \leq P_I$ и что $L \cap V$ конечна и T-инвариантна, значит, $L\mathcal{V} = \{\rceil\}$.

Заметим, что Z — это не что иное, как компонента единицы центра группы L, так что $ZV = R(P_I)$ и Z — максимальный тор радикала $R(P_I)$.. Если теперь L_1 — другой фактор Леви группы P_I, то тогда $L_1 = C_G(Z(L_1)^0)$ и $Z(L_1)^0 = Z_1 \leq ZV$, то Z_1 — другой максимальный тор радикала $R(P_I)$. В силу сопряжённости максимальных торов (теорема 5.4.3), мы получаем, что существует такой $x \in V$, что $Z_1^x = Z$. Отсюда $L_1^x = L$ и мы получаем следующую теорему.

Теорема 7.1.2. *Любая параболическая подгруппа P группы G имеет разложение Леви $P = L \leftthreetimes V$, где $V = R_u(P)$ и L —- связная редуктивная подгруппа максимального ранга группы G, удовлетворяющая $L = C_G(Z(L)^0)$. Более того, любые два фактора Леви сопряжены некоторым элементом из V.*

Заметим, что если $P \neq G$, то $V \neq \{e\}$. Поэтому редуктивная подгруппа L имеет меньший полупростой ранг, чем группа G, что даёт исключительно важный индукционный инструмент изучения редуктивных групп.

§2 Теорема Бореля-Титса

Пусть U — замкнутая, но необязательно связная унипотентная подгруппа группы G. Определим $N_1 = N_G(U)$, $U_1 = U \cdot R_u(N_1)$ и затем индуктивно $N_i = N_G(U_{i-1})$, $U_i = U_{i-1} \cdot R_u(N_i)$. Поскольку унипотентные радикалы связны, ясно, что либо $\dim U_{i+1} > \dim U_i$, либо $U_{i+1} = U_i$. В частности, данная последовательность замкнутых подгрупп группы G должна стабилизироваться на некотором k, т. е. $U_k = U_{k+1} = \ldots$ и $N_k = N_{k+1} = \ldots$. Определим $\mathcal{P}(U) = N_k$, $V = U_k$. Заметим сначала, что любой автоморфизм группы U вида Int_x, $x \in G$ стабилизирует N_1, значит, стабилизирует $R_u(N_1)$, значит, стабилизирует $U_1, \ldots$, значит, стабилизирует $\mathcal{P}(U)$.

Предположим, что U лежит в некоторой подгруппе Бореля группы G (этого нельзя утверждать, если U не является связной). Следующая лемма показывает, что тогда это условие выполнено и для любой U_i.

Лемма 7.2.1. *Пусть H — алгебраическая группа, B — подгруппа Бореля и A — подмножество группы B. Если S — связная разрешимая подгруппа группы H, нормализуемая множеством A, то $S \cdot A$ лежит в некоторой подгруппе Бореля группы H.*

Доказательство. По предположению, замкнутое множество X неподвижных точек множества A в H/B непусто и S стабилизирует X. Поскольку S связна и разрешима, она фиксирует некоторую точку проективного многообразия X (см. теорему 5.1.5), т. е. S лежит в подгруппе Бореля, содержащей A. □

Возвращаясь к нашей подгруппе $V = U_k$, мы получаем, что V содержит унипотентный радикал группы $N_G(V)$ (и, следовательно, совпадает с ним), а также U. Предполагая, что U (следовательно, V) лежит в некоторой подгруппе Бореля, мы докажем, что $\mathcal{P}(U)$ параболическая и что V связна. Из этого будет следовать, что $N_G(U) \leq \mathcal{P}(U)$, поскольку параболические подгруппы совпадают со своими нормализаторами, и также, что $U \leq R_u(\mathcal{P}(U)) = V$.

Лемма 7.2.2. *Пусть V — замкнутая унипотентная подгруппа группы G, $N = N_G(V)$. Предположим, что V лежит в некоторой подгруппе Бореля группы G, и что $V \geq R_u(N)$ (эквивалентно $V^0 = R_u(N)$). Тогда N является параболической подгруппой группы G и $V = R_u(N)$.*

Доказательство. Пусть B — подгруппа Бореля группы G, содержащая V и положим $S = (B \cap N)^0$. Тогда S лежит в подгруппе Бореля B_1 группы N, и мы можем выбрать «противоположную» подгруппу Бореля $n^{-1}B_1n$, где $n \in N$, т. е. $R_u(B_1 \cap n^{-1}B_1n) = R_u(N)$ (применим следствие 5.7.10 к $N^0/R_u(N)$). Тогда наш выбор влечёт $R_i(N \cap B \cap n^{-1}Bn) \leq R_u(N) \leq V$. С другой стороны, n нормализует V, значит, V лежит в унипотентной части разрешимой группы $N \cap B \cap n^{-1}Bn$. Это влечёт равенство, в частности, $V = R_u(N)$ связна. Более того, V лежит в пересечении $B \cap B'$, где $B' = n^{-1}Bn$. Если бы V была меньше, чем $R_u(B \cap B'$, её нормализатор в этой группе имел бы размерность бо́льшую, чем V (см. следствие 5.1.4), что противоречит равенству $R_u(N \cap B \cap B') = V$. Следовательно, $V = R_u(B \cap B')$, значит, $B \cap B' \leq N$. Но $B \cap B'$ содержит максимальный тор T группы G (упражнение 6.4.4), значит N имеет максимальный ранг в G.

Далее мы будем использовать корневую систему группы G, чтобы показать, что N является параболической. Пусть Π — фундаментальная система корневой системы Φ, определённая подгруппой Бореля B (напомним, что задание подгруппы Бореля определяет множество положительных корней, а задание множества положительных корней однозначно определяет фундаментальную систему по лемме 2.1.4). Пусть Ψ — корневая система группы N относительно T. Если $U_\alpha \leq V$ ($\alpha \in \Pi$), то $\alpha \in \Psi$. В противном случае $U_\alpha \leq B$, но $U_\alpha \not\leq V$ влечёт $U_\alpha \not\leq B'$ и, в свою очередь, $U_{-\alpha} \in B'$. Пусть $B'' = \sigma_\alpha B \sigma_\alpha$, её корни совпадают с корнями

группы B, за исключением корня α, который меняется на $-\alpha$ (см. лемму 2.1.9). Далее, $U_{-\alpha}$ нормализует и B' и $R_u(B\cap B'')$, значит, нормализует также $R_u(B\cap B''\cap B')=R_u(B\cap B')=V$. Поэтому $-\alpha\in\Psi$. Поскольку $U_{-\alpha}$ лежит в B' и не лежит в B, аналогичные рассуждения показывают, что U_α нормализует V, т. е. $\alpha\in\Psi$. Отсюда следует, что $\Pi\subseteq\Psi$, и, значит, $B\leq N$. Следовательно, подгруппа N является параболической. □

Таким образом, мы получаем следующую теорему, называемую также теоремой Бореля-Титса.

Теорема 7.2.3. *Пусть G — редуктивная алгебраическая группа, U — унипотентная подгруппа группы G, содержащаяся в некоторой подгруппе Бореля группы G. Тогда существует такая параболическая подгруппа P группы G, что $N_G(U)\leq P$ и $U\leq R_u(P)$.*

§3 Централизаторы полупростых элементов

Теорема 7.3.1. *Пусть G — редуктивная алгебраическая группа, $s\in G$ — полупростой элемент группы G и T — максимальный тор группы G, содержащий s (существование такого тора следует из теоремы 5.5.2).*

Тогда $C_G(s)$ порождается, теми корневыми подгруппами U_α, для которых $s^\alpha=e$ и $C_{N_G(T)}(s)$. Кроме того, $C_G(s)^0$ порождается тором T и теми корневыми подгруппами U_α, для которых $s^\alpha=e$ и $C_G(s)/C_G(s)^0$ изоморфна секции группы Вейля W группы G. В частности, любой унипотентный элемент, централизующий s, лежит в $C_G(s)^0$.

Доказательство. Пусть B — подгруппа Бореля, содержащая тор T, U_α — корневые подгруппы группы G относительно тора T и $U=R_u(B)$. Для любого $n\in N_G(T)$ обозначим через $\bar{n}$ его образ относительно естественного гомоморфизма $N_G(T)\rangle N_G(T)/T=W$. Очевидно (см. теорему 5.8.2(в)), что все группы U_α, удовлетворяющие условию $s^\alpha=e$ и $C_{N_G(T)}(s)$ лежат в $C_G(s)$. Покажем, что эти подгруппы порождают $C_G(s)$. Пусть $x\in C_G(s)$. В силу точной формы разложения Брюа (теорема 6.2.9) элемент x единственным образом записывается в виде $x=unv$, где $u\in U$, $n\in N_G(T)$, $v\in U_{\bar{n}}$. Поскольку $x\in C_G(s)$, то $x^s=x$, откуда $u^s=u$, $n^s=n$, $v^s=v$. Ввиду действия элемента s на корневых подгруппах, определённого в теореме 5.8.2(в), а также из того факта, что U прямо порождается группами U_α (лемма 6.4.1) следует, что $u,v\in\langle U_\alpha|s^\alpha=e\rangle$, откуда следует утверждение для $C_G(s)$.

Далее, рассмотрим подгруппу R группы $C_G(s)$, порождённую тором T и группой $\langle U_\alpha|s^\alpha=e\rangle$. По теореме 4.1.8 она замнута и связна. Кроме того $C_G(s)/R\simeq C_{N_G(T)}(s)/(C_{N_G(T)}\cap R)$ изоморфна секции группы Вейля и потому конечна. Значит, $R=C_G(s)^0$, откуда следует теорема. □

Доказательство следующей леммы требует длительных вычислений и изучения двойственных групп к алгебраическим группам, поэтому мы не будем здесь его приводить, ограничившись лишь ссылкой.

Лемма 7.3.2. [18, Предложение 2.10] *Пусть G — полупростая алгебраическая группа, s — её полупростой элемент конечного порядка Тогда $C_G(s)/C_G(s)^0$ изоморфна подгруппе фундаментальной группы $\Delta(G)$ группы G.*

Теорема 7.3.3. *Пусть G — полупростая алгебраическая группа, s — её полупростой элемент конечного порядка Тогда $C_G(s)/C_G(s)^0$ изоморфна подгруппе фундаментальной группы $\Delta(G)$ группы G.*

Доказательство. Если порядок элемента s конечен, то теорема сразу следует из леммы 7.3.2. Если порядок бесконечен, рассмотрим замыкание S циклической группы, порождённой элементом s. В силу леммы 3.4.5, если морфизм Int_x действует тождественно на плотном подмножестве $\langle\, s\,\rangle$ группы S, то он действует тожественно и на S. Поэтому $C_G(s)=C_G(S)$. Далее группа S является диагонализируемой (как замыкание диагонализируемой группы), поэтому теорема 5.2.9 влечёт, что $S=S^0\times H$, где S^0 — тор и H — конечная группа. Если $H=\{e\}$, то по теореме 5.5.4 централизатор $C_G(S)=C_G(S^0)$ связен и доказывать нечего. В противном случае запишем $s=s_0h$, где $s_0\in S^0$ и $h\in H$. Рассмотрим естественный гомоморфизм $S\to S/S^0\simeq H$, который действует как изоморфизм на H, поэтому можно считать, что h переходит сам в себя под действием этого гомоморфизма. Прообраз элемента h в S замкнут и содержит s, следовательно, совпадает с S. Значит, $\langle\, h\,\rangle=H$ и $C_G(H)=C_G(h)$. По лемме 7.3.2 мы получаем, что $C_G(h)/C_G(h)^0$ изоморфна подгруппе группы $\Delta(G)$. Поскольку $C_G(S)=C_{C_G(h)}(S^0)$ и $C_{C_G(h)^0}(S^0)$ связна, отсюда следует утверждение теоремы. □

Данная теорема имеет важное следствие, которое, ввиду его важности, сформулируем отдельно.

Следствие 7.3.4. *Пусть G — односвязная полупростая алгебраическая группа (т. е. $\Delta(G)=\{e\}$). Тогда для любого полупростого элемента s группы G его централизатор $C_G(s)$ связен.*

§4 Автоморфизмы линейных алгебраических групп

В данном параграфе мы рассмотрим автоморфизмы линейных алгебраических групп, как абстрактных групп (дело в том, что не любой автоморфизм алгебраической группы является морфизмом).

Построим сначала специальные типы изоморфизмов линейной алгебраической группы. Пусть f — некоторый автоморфизм поля $\mathbb{F}$. Поскольку любая корневая подгруппа U_α изоморфна аддитивной группе поля $\mathbb{F}$, мы можем рассматривать f как автоморфизм каждой из корневых подгрупп U_α. Поскольку константы в коммутаторной формуле Шевалле по модулю не превосходят 3, мы получаем, что если на данных константах, рассматриваемых как элементы поля $\mathbb{F}$ автоморфизм f действует тривиально. Таким образом, в силу коммутаторной формулы Шевалле, f можно продолжить на максимальную унипотентную подгруппу U группы G.

Пусть $\alpha_1, \ldots, \alpha_n$ — $\mathbb{Z}$-базис решётки $X(T)$. Для каждого α_i определим элемент $h_i(t) \in T$ (где T — максимальный тор группы G, относительно которого определены группы U_α) следующим правилом: $(h_i(t))^{\alpha_i} = t$ и $(h_i(t))^{\alpha_j} = e$ при $i \neq j$ (существование такого элемента гарантирует нам лемма 5.2.8). Поскольку $\alpha_1, \ldots, \alpha_n$ является $\mathbb{Z}$-базисом решётки $X(T)$, мы получаем, что каждый $h_i(t)$ определён единственным образом. Пусть $H_i = \langle h_i(t) | t \in \mathbb{F}^* \rangle$. Тогда f продолжается до автоморфизма каждого из H_i. Кроме того, любой элемент из T единственным образом записывается в виде произведения элементов из H_i, $i = 1, \ldots, n$ (порядок неважен, в силу коммутативности группы T). Таким образом, f продолжается до автоморфизма группы T. По лемме 5.8.2(в) автоморфизм f согласуется с действием тора T на U, следовательно, f продолжается до автоморфизма группы B. Так как $n_\alpha = u_\alpha(1)u_{-\alpha}(-1)u_\alpha(1)$, мы получаем, что $n_\alpha^f = n_\alpha$, откуда f действует тривиально на $N_G(T)/T$ и мы получаем продолжение f на $N_G(T)$. В силу разложения Брюа, мы получаем продолжение автоморфизма f на всю группу G.

***Упражнение* 7.4.1.** Доказать, что таким образом определённый f сохраняет операцию.

Автоморфизм f группы G, определённый выше, называется *полевым автоморфизмом* группы G. Заметим, что нетривиальный полевой автоморфизм никогда не является морфизмом. Действительно, полевой автоморфизм индуцирует автоморфизм аддитивной группы поля $\mathbb{F}$. Но группа автоморфизмов, являющихся морфизмами, аддитивной группы поля $\mathbb{F}$ изоморфна $\mathbb{F}^*$ и умножение ни на какой из неединичных элементов из $\mathbb{F}^*$ не является автоморфизмом поля $\mathbb{F}$.

Пусть вновь $G = G_1 * G_2 * \ldots * G_k$ — полупростая алгебраическая группа, где $G_1, \ldots, G_k$ — простые алгебраические группы.

Указатель терминов

Предметный указатель

Литература

[1] *A.Borel and J.de Siebental*, Les-sous-groupes fermés de rang maximum des groupes de Lie clos, *Comment. Math. Helv.*, **23** (1949), 200-221.

[2] *А.Борель, Р.Картер, К.В.Кэртис, Н.Ивахори, Т.А.Спрингер, Р.Стейнберг*, *Семинар по алгебраическим группам*, Москва, «Мир», 1973.

[3] *R.W.Carter*, *Simple groups of Lie type.* Wiley and sons, 1972.

[4] *R.W.Carter*, *Finite groups of Lie type. Conjugacy classes and complex characters.* Wiley and sons, 1985.

[5] *R.W.Carter*, Conjugacy classes in the Weyl group, *Compositio Mathematica*, **25** N 1 (1972), 1-59.

[6] *J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson*, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[7] *Ч.Кэртис, И.Райнер*, *Теория представлений конечных групп и ассоциативных алгебр.* Москва, «Наука», 1969.

[8] *Н.Джекобсон*, *Алгебры Ли.* Москва, «Мир», 1964.

[9] *Е.Б.Дынкин*, Полупростые подалгебры полупростых алгбер Ли, *Математический сборник*, **30** N 2 (1952), 349–462.

[10] *С.Ленг*, *Алгебра*, Москва, «Мир», 1968.

[11] *M.Geck*, *An Introduction to Algebraic Geometry and Algebraic Groups*, Oxford Univ.Press, 2003.

[12] *H.Samelson*, *Notes on Lie algebras (2nd ed.)*, Springer-Verlag, 1990.

[13] *R.Steinberg*, *Endomorphisms of linear algebraic groups.* Mem. of AMS, N 80, 1968.

[14] *Д.А.Супруненко*, *Группы матриц.* Москва, «Наука», 1972.

[15] *Д.А.Супруненко*, *Разрешимые и нильпотентные линейные группы.* Минск, 1958.

[16] *Д.Супруненко и Р.Апатёнок*, О нильпотентных неприводимых подргуппах линейных групп над конечными полями. *ДАН БССР.* **3** (1959), 475–478.

[17] *Дж.Хамфри*, *Линейные алгебраические группы.* Москва, «Наука», 1980.

[18] *J. E. Humphreys*, *Conjugacy classes in semisimple algebraic groups*, American Mathematical Society, Providence, Rhode Island, Mathematical Survey and Monographs, **43**, 1995.