ведение $z = x \cdot y$ определено. Положим $x' = \mu x$, $y' = \mu y$ и $z' = \mu z$. Тогда

$$z' = x' + y' + \sum \frac{c_{\alpha, \beta}}{\mu^{|\alpha|+|\beta|-1}} x'^{\alpha} y'^{\beta}.$$

Следовательно, новый групповой закон F_μ имеет коэффициенты $\frac{c_{\alpha, \beta}}{\mu^{|\alpha|+|\beta|-1}}$. Выбирая элемент μ с достаточно большим значением $|\mu|$, мы можем считать, что все коэффициенты группового закона F_μ лежат в A^n и $|\mu|\varepsilon \geqslant 1$, так что все новые ряды сходятся в шаре радиуса 1. Таким образом, в новой координатной системе шар $P_0(1, \ldots, 1)$ является стандартной подгруппой группы G.

Следствие 1. *Всякая локальная аналитическая группа эквивалентна аналитической группе.*

Следствие 2. *Во всякой локальной аналитической группе единица группы обладает фундаментальной системой окрестностей, состоящей из открытых подгрупп.*

§ 9. Фильтрация в стандартных группах

Сохраним обозначения предыдущего параграфа.

Обозначим через $w : k \to \mathbf{R} \cup \{\infty\}$ нормирование поля k, т. е. такую функцию w, что

$$|x| = \rho^{w(x)},$$

где ρ — фиксированное вещественное число, $0 < \rho < 1$.

На элементах $x = (x_1, \ldots, x_n) \in k^n$ мы определим функцию $w(x) = \inf(w(x_i))$. Для каждого действительного числа $\lambda \geqslant 0$ положим

$$G_\lambda = \{x \in G \mid w(x) \geqslant \lambda\},$$

$$G_\lambda^+ = \{x \in G \mid w(x) > \lambda\}.$$

Более общим образом, пусть $\mathfrak{a}$ — идеал кольца A. Положим

$$G_{\mathfrak{a}} = \{x \in G \mid x_i \in \mathfrak{a},\ 1 \leqslant i \leqslant n\},$$

$$G_{\mathfrak{a}}^+ = \{x \in G \mid x_i \in \mathfrak{a} \cdot \mathfrak{m},\ 1 \leqslant i \leqslant n\}.$$

Таким образом, если $\mathfrak{a}_\lambda = \{x \in A \mid w(x) \geqslant \lambda\}$, то $G_\lambda = G_{\mathfrak{a}_\lambda}$ и $G_\lambda^+ = G_{\mathfrak{a}_\lambda}^+ = G_{\mathfrak{a}_\lambda \cdot \mathfrak{m}}$.

Теорема 1. *Для любого идеала*[1] $\mathfrak{a} \subset A$ *множества вида* $G_\mathfrak{a}$ *и* $G_\mathfrak{a}^+$ *являются нормальными подгруппами группы* G. *Сравнение* $x \equiv y \pmod{G_\mathfrak{a}}$ $(x, y \in G)$ *равносильно системе сравнений* $x_i \equiv y_i \pmod{\mathfrak{a}}$, $1 \leqslant i \leqslant n$.

Доказательство. Рассмотрим группу $G(A/\mathfrak{a})$, индуцированную групповым законом F на множестве $(\mathfrak{m}/\mathfrak{a})^n$. Сопоставляя каждому элементу $x = (x_1, \ldots, x_n) \in \mathfrak{m}^n$ элемент $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n) \in (\mathfrak{m}/\mathfrak{a})^n$, мы получаем сюръективный гомоморфизм $\varphi_\mathfrak{a}$: $G \to G(A/\mathfrak{a})$. Его ядром является, очевидно, множество $G_\mathfrak{a}$, что доказывает наше утверждение относительно $G_\mathfrak{a}$. Что касается множества $G_\mathfrak{a}^+$, то оно также является нормальной подгруппой, поскольку $G_\mathfrak{a}^+ = G_{\mathfrak{a} \cdot \mathfrak{m}}$.

(Другое доказательство можно получить, используя формулу (1) из § 6 и формулы (2) и (3) из § 7.)

Следствие. *Подмножества* $\{G_\lambda\}$ *определяют фильтрацию группы* G.

Доказательство. Проверим все аксиомы фильтрации (см. часть I, гл. II, § 2):

(1) $w(0) = \infty$;

(2) $w(x) > 0$ для всех $x \in G$;

(3) $w(xy^{-1}) \geqslant \inf\{w(x), w(y)\}$;

(4) $w((x, y)) \geqslant w(x) + w(y)$.

Аксиомы (1) и (2) очевидны в силу определения группы G. Аксиома (3) эквивалентна утверждению, что G_λ — подгруппа группы G для любого числа λ. Аксиома (4) эквивалентна включению $(G_\lambda, G_\mu) \subset G_{\lambda+\mu}$. Действительно, пусть $x \in G_\lambda$ и $y \in G_\mu$. Тогда

---

[1]) Здесь, по-видимому, имеются в виду *замкнутые* идеалы $\mathfrak{a}$. Если кольцо A нётерово (что верно, например, для локально компактного поля k), то любой идеал кольца A замкнут (см. Самюэль и Зарисский, Коммутативная алгебра, т. II, гл. VIII, § 4). — *Прим. перев.*

(а) $[x, y] \in G_{\lambda+\mu}$,

(б) $(x, y) \equiv [x, y] \pmod{G^+_{\lambda+\mu}}$.

Свойство (а) очевидно, а свойство (б) является следствием теоремы 1 и формулы (5) из § 7.

Теорема 2. *Пусть* $\mathfrak{a}$ *и* $\mathfrak{b}$ — *идеалы кольца* A, *такие, что* $\mathfrak{a} \supset \mathfrak{b} \supset \mathfrak{a}^2$. *Отображение редукции* $\varphi_{\mathfrak{b}}$: $G \to G(A/\mathfrak{b})$ *индуцирует изоморфизм группы* $G_{\mathfrak{a}}/G_{\mathfrak{b}}$ *на аддитивную группу* $(\mathfrak{a}/\mathfrak{b})^n$.

Доказательство. Как видно из формулы (1) § 6, для любой пары $x, y \in G_{\mathfrak{a}}$ имеем

$$F(x, y) \equiv x + y \pmod{\mathfrak{a}^2}.$$

Наша теорема очевидным образом вытекает теперь из теоремы 1.

Следствие 1. *Пусть* $\lambda \in w(\mathfrak{m})$ $(\lambda \neq \infty)$. *Тогда факторгруппа* G_λ/G^+_λ *изоморфна аддитивной группе* $(A/\mathfrak{m})^n$.

Доказательство. Выберем такой элемент $a \in \mathfrak{m}$, что $w(a) = \lambda$, и положим $\mathfrak{a} = (a)$. По теореме 2 § 9 группа $G_{\mathfrak{a}}/G^+_{\mathfrak{a}}$ изоморфна группе $(\mathfrak{a}/\mathfrak{a} \cdot \mathfrak{m})^n$. Но отображение $\alpha \mapsto \alpha \cdot a$ устанавливает изоморфизм групп $A/\mathfrak{m}$ и $\mathfrak{a}/\mathfrak{a} \cdot \mathfrak{m}$.

Следствие 2. *Пусть поле* k *локально компактно, и пусть* p — *характеристика поля* $A/\mathfrak{m}$. *Тогда*

(1) G_λ/G^+_λ — *коммутативная конечная* p-*группа, если* $\lambda \in w(\mathfrak{m})$ *и* $\lambda \neq \infty$;

(2) G/G^+_λ — (*не обязательно конечная*) p-*группа для всех* $\lambda \in w(\mathfrak{m})$, $\lambda \neq \infty$;

(3) G — *проективный предел* p-*групп* (“*про-*p-*группа*“).

Доказательство. Ввиду локальной компактности поля k имеем:

(а) поле $A/\mathfrak{m}$ компактно и дискретно, а потому конечно;

(б) множество $\mathfrak{m}$ компактно, так что функция $w(x)$ достигает на нем минимума в некоторой точке $a \in \mathfrak{m}$.

Теперь ясно, что $\mathfrak{m}=(a)$ и, следовательно, A является кольцом дискретного нормирования.

Первое утверждение вытекает из следствия 1 и свойства (а). Второе утверждение есть следствие первого и дискретности нашего нормирования. Третье утверждение вытекает из второго.

Применим построенную фильтрацию $\{G_\lambda\}$ к изучению отображения возведения в r-ю степень f_r (см. § 7). Пусть $\bar{k}=A/\mathfrak{m}$ и p — характеристика поля $\bar{k}$.

Теорема 3. *Предположим, что числа r и p взаимно просты. Тогда для каждого числа $\lambda\in w(\mathfrak{m})$ $(\lambda\neq\infty)$ отображение f_r определяет изоморфизм аналитического многообразия G_λ на себя.*

Доказательство. Вычет числа r в $\bar{k}$ отличен от 0, поэтому r — обратимый элемент в кольце A. Отсюда видно, что ряды f_r обратимы в кольце $A[[X]]$. Положим $\theta=f_r^{-1}$. Ряды, входящее в θ, абсолютно сходятся на множестве G, а лемма из § 8 показывает, что $f_r\circ\theta=\theta\circ f_r=\mathrm{id}$. Поскольку f_r и θ отображают группу G_λ в себя, f_r — биекция на G_λ. Наконец, производная отображения f_r в любой точке $x\in G$ сравнима по модулю $\mathfrak{m}$ с отображением $r\cdot\mathrm{id}$ и, следовательно, обратима. Следовательно, f_r — наложение и, значит, является аналитическим изоморфизмом на G_λ.

Теорема 4. *Пусть поле k имеет нулевую характеристику и $p\neq 0$. Тогда для всех $\lambda\in w(\mathfrak{m})$, таких, что $\frac{\mu}{p-1}<\lambda<\infty$, отображение f_p является изоморфизмом аналитического многообразия G_λ на $G_{\lambda+\mu}$.*

Доказательство. В силу следствия теоремы Лазара

$$f_p(X)=p(X+\psi(X))+\psi'(X),$$

причем порядок $\psi(X)$ не меньше двух, а порядок $\psi'(X)$ не меньше p.

Очевидно, $w(x^\alpha)\geqslant\lambda\cdot|\alpha|$, если $x\in G_\lambda$ и $|\alpha|\geqslant 1$. В частности,

(а) $w(\psi(x)) > \lambda$;

(б) $w(\psi'(x)) \geqslant p\lambda = \lambda + (p-1)\lambda > \lambda + \mu$.

Поэтому $f_p(G_\lambda) \subset G_{\lambda+\mu}$. Для доказательства того, что f_p: $G_\lambda \to G_{\lambda+\mu}$ — аналитический изоморфизм, выберем элемент $a \in G$, такой, что $w(a) = \lambda$, и определим отображение F: $A^n \to A^n$ формулой $F(x) = \frac{1}{ap} f_p(ax)$. Тогда

$$F(X) = X + \frac{1}{a}\psi(aX) + \frac{1}{ap}\psi'(aX).$$

Возьмем такое число $r \in \mathbf{R}$, $0 < r < 1$, что $\frac{|a|^{p-1}}{|p|}$, $|a| < r^{p-1}$. Пусть

$$\frac{1}{a}\psi(aX) = \sum_{|\alpha| \geqslant 2} a_\alpha X^\alpha \quad \text{и} \quad \frac{1}{ap}\psi'(aX) = \sum_{|\alpha| \geqslant p} a'_\alpha X^\alpha.$$

Легко видеть, что $|a_\alpha| \leqslant |a|^{|\alpha|-1} \leqslant r^{|\alpha|-1}$ и

$$|a'_\alpha| \leqslant |a|^{|\alpha|-p} \frac{|a|^{p-1}}{|p|} \leqslant r^{|\alpha|-1}.$$

Теорема доказана.

Ниже (см. добавление 2) будет доказано, что следствием этих условий является абсолютная сходимость F и его формального обращения θ на множестве A^n. Таким образом, F: $A^n \to A^n$ — аналитический изоморфизм, откуда непосредственно следует соответствующее утверждение для отображения f_p: $G_\lambda \to G_{\lambda+\mu}$.

Теорема 5. *Пусть G — аналитическая группа над полем k. Существует открытая подгруппа U, не содержащая конечных подгрупп, порядок которых взаимно прост с характеристикой поля.*

Доказательство. Поскольку группа G содержит открытую подгруппу, изоморфную стандартной, наше утверждение сводится к теоремам 3 и 4.

Замечание. Теорема 5 утверждает, в частности, что если характеристика поля k равна нулю, то группа G не содержит „малых“ конечных подгрупп.

В добавлении 3 будут даны некоторые приложения теоремы 5.

УПРАЖНЕНИЯ

1. Пусть k — локально компактное поле, и пусть A — компактная аналитическая группа над k.

а) Пусть G — конечная группа, порядок которой взаимно прост с характеристикой поля k. Допустим, что группа G действует аналитически [1]) на группе A. Определим обычным образом множество одномерных когомологий $H^1(G, A)$. (Если группа A коммутативна, то определены все группы когомологий [2]) $H^q(G, A)$.) Доказать, что множество $H^1(G, A)$ конечно. [*Указание*: использовать структуру многообразия на коциклах.] Доказать аналогичный результат для групп $H^q(G, A)$, $q \geqslant 1$, в случае абелевой группы A.

б) Доказать (используя пункт а)), что имеется лишь конечное число классов сопряженных конечных подгрупп группы A заданного порядка (взаимно простого с характеристикой поля k).

2. Пусть i и j — два положительных целых числа.

а) Доказать, что произведение $\binom{m}{i}\binom{m}{j}$ (как функция от m) является линейной комбинацией биномиальных коэффициентов $\binom{m}{k}$, где $i, j \leqslant k \leqslant i+j$.

б) Доказать тождество

$$\binom{m}{i}\binom{m}{j} = \sum_{i,\, j \leqslant k \leqslant i+j} \frac{k!}{(k-i)!\,(k-j)!\,(i+j-k)} \binom{m}{k}.$$

[*Указание*: двумя способами представить произведение биномов $(1+X)^m(1+Y)^m$, где X и Y — две независимые переменные.]

---

[1]) Группа G *аналитически действует* на A, если задан гомоморфизм группы G в группу всех аналитических автоморфизмов группы A. — *Прим. ред.*

[2]) Определение когомологий см., например, в книге Серра [2*]. — *Прим. ред.*

3. Пусть обозначения те же, что в § 7 (теорема Лазара). Рассмотрим случай, когда $F(X, Y)$ обладает свойством

(а) $F(X, Y) \equiv X + Y + 0$ $(d^0 \geqslant 2)$,

но не обладает свойством

(б) $F(0, Y) = 0$.

Показать, что и в этом случае f_m могут быть представлены в виде $\sum \binom{m}{i} \psi_i$, но уже неверно, что $\operatorname{ord}(\psi_i) \geqslant 1$.

4. Показать, что лемма 4.2 останется справедливой, если условие (1) заменить следующим условием:

(1′) A — отделимая топологическая группа, полная относительно обеих равномерных структур, причем ее топология может быть задана счетным семейством открытых подмножеств. [*Указание*: имитировать доказательство теоремы Банаха о замкнутом графике.]

5. Пусть k — локально компактное неархимедово поле и G — стандартная группа размерности n над k. Обозначим через dx меру Хаара на аддитивной группе k^n. Показать, что ограничение меры dx на G определяет левую и правую меры Хаара на G. [*Указание*: использовать тот факт, что $G = \varprojlim G/G_\lambda$ и что мера Хаара на группе G есть проективный предел мер Хаара на конечных группах G/G_λ.]

6. а) Пусть $F(X, Y) = X + Y + XY$ — „мультипликативный“ формальный групповой закон от одной переменной. Показать, что ряды ψ_i, определенные в теореме Лазара, суть просто одночлены X^i.

б) Предположим дополнительно, что поле k неархимедово и имеет нулевую характеристику; пусть p — характеристика поля вычетов. Показать равносильность следующих условий:

(1) $f_p(x) = 0$;

(2) $1 + x$ — корень p-й степени из единицы (в поле k).

Используя теорему 9.4, доказать, что для таких элементов x имеет место неравенство

$$w(x) \geqslant w(p)/p - 1.$$

Показать далее, что если $x \neq 0$ (т. е. если $1+x$ — примитивный корень p-й степени), то имеет место равенство.

7. Пусть F и F' — два формальных групповых закона над полем k характеристики p, и пусть $\varphi(X)$ — формальный гомоморфизм одного закона в другой (т. е. $\varphi(F(X, Y)) = F'(\varphi(X), \varphi(Y))$). Предположим, что все члены первой степени в $\varphi(X)$ равны нулю. Показать, что $\varphi(X)$ имеет вид $\psi(X^p)$. [*Указание*: рассмотреть дифференциальное уравнение

$$\varphi'(X) \cdot D_2F(X, 0) = D_2F'(\varphi(X), 0) \cdot \varphi'(0)$$

для доказательства равенства $\varphi'(X) = 0$.] Интерпретировать этот результат как разложение гомоморфизма φ при помощи *отображения Фробениуса* $F \to F^{(p)}$ в случае, когда поле k совершенно.

Добавление 1

МАКСИМАЛЬНЫЕ КОМПАКТНЫЕ ПОДГРУППЫ В $GL(n, k)$

Основная цель этого добавления — доказать теорему, сформулированную в § 2, п. 1.

Пусть k — локально компактное неархимедово поле, A — кольцо его нормирования, $\mathfrak{m}$ — максимальный идеал кольца A и G — группа матриц $GL(n, A)$ ($n \in \mathbf{Z}$, $n > 0$).

Лемма 1. *Пусть L — некоторый A-подмодуль модуля k^n. Следующие условия эквивалентны:*

(1) *модуль L конечно порожден над A и множество L порождает пространство k^n над k;*

(2) *L — свободный модуль ранга n над A.*

Доказательство. Поскольку A — кольцо главных идеалов, модуль L свободен. Далее, $rk_A L = n$, так как L порождает k^n над k.

Обратное очевидно.

A-модуль L, удовлетворяющий эквивалентным условиям леммы 1, называется *решеткой* в k^n.

Лемма 2. *Пусть $L_1, L_2, \ldots, L_r$ — решетки в k^n. Подмодуль L (модуля k^n), порожденный модулями $L_1, \ldots, L_r$, является решеткой.*

Доказательство. Покажем, что выполняется условие (1) предыдущей леммы. Ясно, что множество L порождает пространство k^n над k, поскольку этим свойством обладает любая решетка L_i. Далее, так как все модули L_i конечно порождены над A, модуль L также конечно порожден.

Лемма 3. *Пусть L — решетка в пространстве k^n. Обозначим через K_L подгруппу группы $GL(n, k)$, которая переводит в себя решетку L. Существует такой элемент $d \in GL(n, k)$, что $K_L = \alpha G \alpha^{-1}$; в частности, группа K_L компактна и открыта.*

Доказательство. В силу условия (2) леммы 1 найдется такой элемент $\alpha \in GL(n, k)$, что $\alpha(A^n) = L$. Из определения группы $GL(n, A)$ ясно, что $K_L = \alpha G \alpha^{-1}$. Как было отмечено выше, группа G компактна и открыта (в $GL(n, k)$), следовательно, такими же свойствами обладает и группа K_L.

Лемма 4. *Пусть L и L' — две решетки в k^n, причем $K_L \subset K_{L'}$. Тогда $K_L = K_{L'}$ и $L' = \lambda L$ для некоторого $\lambda \in k^*$.*

Доказательство. Очевидно, что у решеток вида L и λL ($\lambda \in k^*$) группа K_L одна и та же. Поэтому мы можем считать, что $L' \subset L$ и $L' \not\subset \mathfrak{m} \cdot L$ (идеал $\mathfrak{m}$ главный!). Пусть $V = L/\mathfrak{m}L$ и $V' = (L' + \mathfrak{m}L)/\mathfrak{m}L$. По предположению V' — ненулевое линейное подпространство пространства V (над полем вычетов $A/\mathfrak{m}$). Далее, поскольку $K_L \subset K_{L'}$, решетка L' инвариантна относительно группы K_L, а следовательно, и ее образ V' в пространстве V инвариантен относительно K_L, т. е. относительно $GL(V)$. Учитывая, что $V' \neq (0)$, мы получаем $V' = V$, т. е. $L' + \mathfrak{m}L = L$. Отсюда, согласно известной лемме Накаямы, вытекает равенство $L = L'$.

Теорема 1. *Пусть H — компактная подгруппа группы $GL(n, k)$. Тогда*

(1) *существует решетка $M \subset k^n$, инвариантная относительно всех элементов группы H;*

(2) *существует матрица* $\alpha \in GL(n, k)$, *такая, что* $H \subset \alpha \cdot G\alpha^{-1}$.

Доказательство. Возьмем для начала любую n-мерную решетку L, например $L = A^n$. Группа $H_L = H \cap K_L$ состоит в точности из тех элементов группы H, которые переводят в себя решетку L. Множество K_L (соответственно H_L) открыто в $GL(n, k)$ (соответственно в H), а значит, факторгруппа H/H_L компактна и дискретна (т. е. конечна). Итак, имеется лишь конечное число множеств вида σL $(\sigma \in H)$. Пусть M — подмодуль A-модуля k^n, порожденный семейством $\{\sigma L\}_{\sigma \in H}$. В силу леммы 2 модуль M является решеткой, которая, разумеется, инвариантна относительно группы H.

Второе утверждение нашей теоремы немедленно вытекает из первого и леммы 3.

Теорема 2. (1) $G = GL(n, A)$ — *максимальная компактная подгруппа группы* $GL(n, k)$.

(2) *Все максимальные компактные подгруппы группы* $GL(n, k)$ *сопряжены группе* G.

(3) *Всякая компактная подгруппа группы* $GL(n, k)$ *содержится в некоторой максимальной компактной подгруппе.*

Доказательство. Допустим, что группа G содержится в компактной подгруппе $H \subset GL(n, k)$. На основании теоремы 1 найдется решетка M, такая, что $H \subset K_M$. Но тогда $G \subset K_M$; более того, $G = K_M$ ввиду леммы 4. Итак, G — максимальная компактная подгруппа.

Утверждения (2) и (3) нашей теоремы являются следствиями этого факта и теоремы 1.

Добавление 2

НЕКОТОРЫЕ ЛЕММЫ О СХОДИМОСТИ

Рассмотрим систему $F(X) = (F_i(X))$ из n формальных степенных рядов от n переменных, такую, что каждый ряд $F_i(X)$ имеет вид

$$F_i(X) = X_i - \sum_{|\alpha| \geqslant 2} a_\alpha^i X^\alpha = X_i - \varphi_i(X).$$

Как мы уже видели при доказательстве теоремы об обратной функции, система F формально обратима, причем обратная формальная система $\theta(X)=(\theta_i(X))$ имеет вид

$$\theta_i(X)=X_i+\sum_{|\beta|\geqslant 2} b_\beta^i X^\beta = X_i+\psi_i(X).$$

Пусть $r\in\mathbf{R}$, $0<r<1$. Рассмотрим два условия

$$(\mathrm{A}_r)\ |a_\alpha^i|\leqslant r^{|\alpha|-1} \text{ для всех } \alpha;$$

$$(\mathrm{B}_r)\ |b_\beta^i|\leqslant r^{|\beta|-1} \text{ для всех } \beta.$$

Лемма 1. $(\mathrm{A}_r)\Rightarrow F$ *абсолютно сходится в шаре* A^n.
$(\mathrm{B}_r)\Rightarrow\theta$ *абсолютно сходится в шаре* A^n.

Доказательство. Достаточно заметить, что

$$\sum_{|\gamma|\geqslant 0} r^{|\gamma|}=\frac{1}{(1-r)^n}<\infty.$$

Лемма 2. $(\mathrm{A}_r)\Leftrightarrow(\mathrm{B}_r)$.

Доказательство. Поскольку условия симметричны, покажем, например, что $(\mathrm{A}_r)\Rightarrow(\mathrm{B}_r)$. Применим индукцию по $|\beta|$. Предположим, что для всех индексов β' с $|\beta'|<|\beta|$ наше утверждение справедливо. Имеем

$$X_i=F_i(\theta(X))=\theta_i(X)-\varphi_i(\theta(X)).$$

Сравнивая коэффициенты при X^β, мы видим, что b_β^i есть суммарный коэффициент при X^β в $\varphi_i(\theta(X))$. В силу неархимедовости основного поля достаточно проверить, что для всех одночленов вида bX^β, встречающихся в $\varphi_i(\theta(X))$, выполняется неравенство $|b|\leqslant r^{|\beta|-1}$. Но

$$\varphi_i(\theta(X))=\sum_{|\alpha|\geqslant 2} a_\alpha^i(\theta(X))^\alpha,$$

где $\theta(X)^\alpha=\theta_1(X)^{\alpha_1}\ldots\theta_n(X)^{\alpha_n}$. Все одночлены, входящие в $\theta(X)^\alpha$, имеют вид

$$\prod_{i=1}^{n}\prod_{j=1}^{\alpha_i}\left(b_{\gamma_{i,j}}^i X^{\gamma_{i,j}}\right).$$

Нас интересуют члены с $\sum \gamma_{i,j} = \beta$. По предположению индукции

$$\left| \prod_{i,j} b^i_{\gamma_{i,j}} \right| \leqslant \prod_{i,j} r^{|\gamma_{i,j}|-1} = r^{|\beta|-|\alpha|}.$$

Требуемая оценка коэффициентов при X^β в $\varphi_i(\theta(X))$ непосредственно вытекает теперь из неравенства $|a^i_\alpha| \leqslant r^{|\alpha|-1}$.

Следствие. $(A_r) \Rightarrow (F$ — *аналитический изоморфизм* A^n *на* $A^n)$.

Доказательство. Ввиду леммы 2 имеют место оба условия (A_r) и $B_r)$. По лемме 1 для всех $x \in A^n$ имеем

$$x = (f \circ \theta)(x) = f(\theta(x)) = (\theta \circ f)(x) = \theta(f(x)).$$

Добавление 3

ПРИМЕНЕНИЯ § 9. ФИЛЬТРАЦИЯ В СТАНДАРТНЫХ ГРУППАХ

Теорема 1. *Для каждого* $n > 0$, $n \in \mathbf{Z}$, *существует такое* $N > 0$, $N \in \mathbf{Z}$, *что порядок любой конечной подгруппы в* $GL(n, \mathbf{Q})$ *не превосходит* N.

Доказательство. 1°. Докажем вначале соответствующее утверждение для группы $GL(n, \mathbf{Z}_p)$, где $\mathbf{Z}_p$ — кольцо целых p-адических чисел, p — любое простое число. По теореме 9.8 § 9 в группе $GL(n, \mathbf{Z}_p)$ имеется открытая подгруппа U, не содержащая конечных подгрупп. Многообразие $GL(n, \mathbf{Z}_p)/U$ компактно и дискретно, т. е. конечно. Обозначим через N его порядок. Для всякой конечной подгруппы $H \subset GL(n, \mathbf{Z}_p)$ имеем $H \subset GL(n, \mathbf{Z}_p)/U$, поэтому ее порядок не превышает N.

2°. Сведем нашу теорему к доказанному выше утверждению. Имеются два существенно различных способа.

Способ 1. Пусть H — конечная подгруппа группы $GL(n, \mathbf{Q})$. Вложим группу $GL(n, \mathbf{Q})$ в группу $GL(n, \mathbf{Q}_p)$, так что $H \subset GL(n, \mathbf{Q}_p)$. Поскольку группа H компактна, мы можем утверждать (см. теорему 1, добавление 1), что некоторая подгруппа, сопряженная H, лежит в $GL(n, \mathbf{Z}_p)$. Следовательно, в силу доказанного выше в пункте 1° порядок группы H ограничен некоторым числом N.

Способ 2. Читатель без труда проверит, что леммы 1 и 2 из добавления 1 справедливы для $k = \mathbf{Q}$ и $A = \mathbf{Z}$. Нам потребуются также следующие утверждения.

(а) Пусть L — решетка в $\mathbf{Q}^n$. Подгруппа

$$\{\alpha \in GL(n, \mathbf{Q}) \mid \alpha(L) = L\} \subset GL(n, \mathbf{Q})$$

сопряжена подгруппе $GL(n, \mathbf{Z})$.

(б) Для каждой конечной подгруппы $H \subset GL(n, \mathbf{Q})$ существует решетка M, инвариантная относительно группы H (т. е. $h(M) \subset M$, $h \in H$).

Утверждение (а) доказывается в точности тем же способом, что и лемма 3 из добавления 1. Докажем утверждение (б). Возьмем для этого произвольную решетку L и построим с ее помощью решетку $M = \{\sigma L\}_{\sigma \in H}$, порожденную решетками вида σL. Из построения ясно, что каждый элемент группы H отображает решетку M на себя.

Комбинируя доказанные утверждения, нетрудно усмотреть, что любая конечная подгруппа $H \subset GL(n, \mathbf{Q})$ сопряжена некоторой подгруппе, лежащей в $GL(n, \mathbf{Z})$.

Таким образом, мы можем считать, что $H \subset GL(n, \mathbf{Z})$. Замечая, что $GL(n, \mathbf{Z}) \subset GL(n, \mathbf{Z}_p)$, мы сводим нашу теорему к разобранному выше случаю.

Из доказательства теоремы 1 мы можем извлечь явную оценку числа N, оценивая порядок группы $GL(n, \mathbf{Z}_p)/U$ для каждого простого p. Рассмотрим два случая.

1) p нечетно. В этом случае $1 > \frac{1}{p-1}$, и в качестве группы U можно взять группу

$$G_1 = \{y \in GL(n, \mathbf{Z}_p) \mid y = 1 + x, \quad x = (x_{ij}), \quad x_{ij} \in m\}.$$

Тогда $GL(n, \mathbf{Z}_p)/U = GL(n, \mathbf{F}_p)$, где $\mathbf{F}_p$ — поле из p элементов. Мы можем явно вычислить порядок группы $\mathrm{GL}(n, \mathbf{F}_p)$. Он равен числу различных *упорядоченных* базисов в $\mathbf{F}_p^n$, т. е.

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

2) $p = 2$. Имеем $2 > \frac{1}{p-1}$, так что можно положить $U = G_2$. Тогда $GL(n, \mathbf{Z}_p)/U = \mathrm{GL}(n, \mathbf{Z}/4\mathbf{Z})$. Имеет место точная последовательность

$$0 \to (2\mathbf{Z}/4\mathbf{Z})^{n^2} \to GL(n, \mathbf{Z}/4\mathbf{Z}) \to GL(n, \mathbf{Z}/2\mathbf{Z}) \to 1,$$

позволяющая вычислить порядок группы $\mathrm{GL}(n, \mathbf{Z}/4\mathbf{Z})$; он равен

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

Рассмотрим подробнее случай $n = 2$.

1) p нечетно. Имеем $(p^2 - 1)(p^2 - p) = (p - 1)^2 p \times \times (p + 1)$. В силу нечетности p имеют место сравнения

а) $p^2 - 1 \equiv 0 \pmod 8$, $(p^2 - 1)(p^2 - p) \equiv \pmod{16}$;

б) $(p - 1)p(p + 1) \equiv 0 \pmod 3$.

Следовательно, $(p - 1)^2 p(p + 1) \equiv 0 \pmod{48}$. При $p = 3$ имеем $(p - 1)^2 p(p + 1) = 48$.

2) $p = 2$. В этом случае $2^{2^2}(2^2 - 1)(2^2 - 1) = 96$. Таким образом, наилучшей оценкой порядка конечных подгрупп группы $GL(2, \mathbf{Z})$, которую дает приведенный выше метод, является число 48. Фактически эту оценку можно несколько улучшить. Заметим прежде всего, что любая конечная подгруппа группы $GL(n, \mathbf{Q})$ содержится в группе G_0 всех матриц с определителем ± 1. Имеет место точная последовательность

$$1 \to SL(2, \mathbf{Q}) \to G_0 \to \mathbf{Z}/2\mathbf{Z} \to 0.$$

Отсюда видно, что оценки для группы G_0 можно получить из соответствующих оценок для группы $SL(n, \mathbf{Q})$, умножая их на 2.

Докажем следующее

Предложение. (1) *Всякая конечная подгруппа группы $SL(2, \mathbf{Q})$ содержится в группе вращений плоскости и потому является циклической.*

(2) *Порядок конечных циклических подгрупп группы* $SL(2, \mathbf{Z})$ *может равняться лишь одному из чисел* 1, 2, 3, 4, 6.

Доказательство. (1) Пусть задана конечная подгруппа $H \subset SL(2, \mathbf{Q})$. Возьмем любую положительно определенную билинейную форму $B(x, y)$ в пространстве $\mathbf{Q}^2$. Положим $\bar{B}(x, y) = \sum_{\sigma \in H} B(\sigma x, \sigma y)$. Очевидно, новая форма $\bar{B}$ положительно определена и инвариантна относительно группы H. Поскольку определитель любого элемента из H равен единице, группа H является подгруппой группы вращений плоскости $\mathbf{R}^2$ относительно скалярного произведения, определенного формой $\bar{B}$.

(2) Пусть $\alpha \in SL(n, \mathbf{Q})$ — некоторый элемент конечного порядка. Расширим основное поле $\mathbf{Q}$ до поля комплексных чисел $\mathbf{C}$ и приведем матрицу α к жордановой форме. Имеются две возможности.

(i) Жорданова форма имеет вид

$$\begin{pmatrix} \mu & 1 \\ 0 & \mu \end{pmatrix}.$$

Простая проверка показывает, что в этом случае элемент α не может иметь конечного порядка.

(ii) Жорданова форма имеет вид

$$\begin{pmatrix} \mu & 0 \\ 0 & \nu \end{pmatrix}.$$

Обозначим через N порядок элемента α. Очевидно, $\mu^N = \nu^N = 1$. Далее, числа μ и ν являются корнями характеристического многочлена матрицы α и, следовательно, лежат в квадратичном расширении поля $\mathbf{Q}$. При этом числа μ и ν либо оба содержатся в поле $\mathbf{Q}$, либо являются комплексно сопряженными. Учитывая, что μ и ν — корни из единицы, мы получаем следующие возможности:

а) $\mu = \nu = 1$ или $\mu = \nu = -1$;

б) λ — примитивный корень N-й степени из единицы, $N > 2$ и $\nu = \bar{\mu}$.

В последнем случае поле $\mathbf{Q}(\mu)$ есть круговое расширение поля $\mathbf{Q}$ степени $\varphi(N)$, где φ — функция Эйлера. Из равенства $\varphi(N)=2$ легко извлечь, что число N может равняться 3, 4 или 6. Это завершает доказательство второго утверждения.

Укажем явно элементы четвертого и шестого порядка в группе $SL(2, \mathbf{Z})$. Для этого мы возьмем соответствующее квадратичное расширение $K=\mathbf{Q}(x)$ поля $\mathbf{Q}$ и посмотрим, какой матрицей в базисе $\{1, x\}$ записывается умножение на элемент x.

1. *Построение элемента четвертого порядка.* Пусть x — примитивный корень четвертой степени из единицы. Умножение на x как линейное преобразование имеет порядок 4 и записывается матрицей

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

2. *Построение элемента шестого порядка.* Пусть x — примитивный корень шестой степени из единицы. Умножение на x имеет порядок 6 и записывается матрицей

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Пусть k — локально компактное неархимедово поле, A — кольцо его нормирования, $\mathfrak{m}$ — максимальный идеал кольца A, p — характеристика поля k и $q=\mathrm{Card}(A/\mathfrak{m})$. Обозначим через w каноническое нормирование поля k (w: $k \to \mathbf{Z} \cup \{\infty\}$ и $w(k^*)=\mathbf{Z}$). Каноническое абсолютное значение в поле k можно определить тремя эквивалентными способами:

1) $\|x\| = \mathrm{Card}(A/xA)^{-1}$;

2) $\|x\| = q^{-w(x)}$;

3) умножение на x изменяет меру Хаара в $\|x\|$ раз.

Допустим, что $r \in \mathbf{Z}$ взаимно просто с p. Рассмотрим возведение в r-ю степень f_r: $A^* \to A^*$. Пусть $s=\mathrm{Card}(\mathrm{Ker}\, f_r)$ — число корней r-й степени из единицы в поле k.

Теорема 2. $\mathrm{Card}(A^*/A^{*r}) = \|r\|^{-1} \cdot s$.

Эту теорему мы получим как следствие более общей теоремы об аналитических группах над k.

Пусть G — *коммутативная компактная аналитическая группа* над полем k. Положим

$$h_r(G) = \operatorname{Card}(\operatorname{Coker} f_r)/\operatorname{Card}(\operatorname{Ker} f_r).$$

Как мы увидим ниже, число $h_r(G)$ определено (т. е. числитель и знаменатель написанной дроби конечны).

Теорема 3. *Число $h_r(G)$ существует и равно $\|r\|^{-n}$, где $n = \dim_k G$.*

Доказательство. Предварительно мы установим три вспомогательных утверждения.

(1) Теорема справедлива, если $G = G'_\lambda$, где G' — стандартная группа и $\lambda \gg 0$.

(2) Теорема справедлива, если G — конечная группа.

(3) Теорема справедлива, если в G существует группа Ли H, такая, что теорема верна для H и для факторгруппы G/H.

Доказательство этих утверждений проведем в обратном порядке.

(3) Рассмотрим коммутативную диаграмму с точными строками

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r] \arrow[d, "\varphi_1"'] & G \arrow[r] \arrow[d, "\varphi_2"] & G/H \arrow[r] \arrow[d, "\varphi_3"] & 1 \\
1 \arrow[r] & H \arrow[r] & G \arrow[r] & G/H \arrow[r] & 1
\end{tikzcd}$$

где $\varphi_1 = f_r$ (на группе H), $\varphi_2 = f_r$ (на группе G), $\varphi_3 = f_r$ (на группе G/H). Следствием этой диаграммы является точность последовательности

$$1 \to \operatorname{Ker}\varphi_1 \to \operatorname{Ker}\varphi_2 \to \operatorname{Ker}\varphi_3 \xrightarrow{\delta} \operatorname{Coker}\varphi_1 \to$$
$$\to \operatorname{Coker}\varphi_2 \to \operatorname{Coker}\varphi_3 \to 1 \qquad (*)$$

(см., например, Бурбаки [2*], гл. I, § 1, п. 4). Все отображения в этой последовательности определены очевидным образом, за исключением разве что δ. Последнее определяется так. Пусть $x'' \in \operatorname{Ker}\varphi_3$; выберем представителя $x \in G$ элемента x'' (т. е. $x'' = xH$). Ввиду точности нижней строки $x^r \in H$. Определим

$\delta(x'')$ как образ элемента x^r в $\operatorname{Coker}\varphi_1$. Читателю предоставляется проверка корректности этого определения и точности последовательности (*).

Мы предположили, что для групп H и G/H теорема 3 справедлива. Поэтому все группы $\operatorname{Ker}\varphi_1$, $\operatorname{Ker}\varphi_3$, $\operatorname{Coker}\varphi_1$, $\operatorname{Coker}\varphi_3$ конечны. В силу точности последовательности (*) отсюда следует, что, во-первых, группы $\operatorname{Ker}\varphi_2$ и $\operatorname{Coker}\varphi_2$ конечны, а во-вторых, справедливо равенство ($\mathrm{c} \equiv \mathrm{Card}$)

$$\mathrm{c}(\operatorname{Ker}\varphi_1)\,\mathrm{c}(\operatorname{Ker}\varphi_2)^{-1}\,\mathrm{c}(\operatorname{Ker}\varphi_3)\,\mathrm{c}(\operatorname{Coker}\varphi_1)^{-1}\times \\ \times\,\mathrm{c}(\operatorname{Coker}\varphi_2)\,\mathrm{c}(\operatorname{Coker}\varphi_3)^{-1}=1.$$

Другими словами,

$$h_r(G)=h_r(H)\cdot h_r(G/H).$$

Пусть $m=\dim_k H$, тогда $n-m=\dim_k G/H$ и

$$\|r\|^{-n}=\|r\|^{-m}\cdot\|r\|^{-(n-m)}.$$

Но по предположению

$$h_r(H)=\|r\|^{-m} \quad \text{и} \quad h_r(G/H)=\|r\|^{-(n-m)},$$

откуда $h_r(G)=\|r\|^{-n}$, как и утверждалось.

(2) Имеет место точная последовательность

$$1\to\operatorname{Ker}f_r\to G\xrightarrow{f_r}G\to\operatorname{Coker}f_r\to 1.$$

Поскольку группа G конечна, конечны также ядро $\operatorname{Ker}f_3$ и коядро $\operatorname{Coker}f_r$; далее,

$$1=\mathrm{c}(\operatorname{Coker}f_r)\,\mathrm{c}(G)^{-1}\,\mathrm{c}(G)\,\mathrm{c}(\operatorname{Ker}f_r)^{-1}=h_r(G)$$

и

$$1=\|r\|^n,$$

так как $n=0$.

(1) Поскольку доказательство достаточно провести для достаточно большого числа $\lambda\in\mathbf{Z}$, мы можем

предполагать (см. теоремы 3 и 4 из § 9), что f_r: $G_\lambda \to G_{\lambda+w(r)}$ — изоморфизм. Но тогда

$$c(\operatorname{Ker} f_r) = 1$$

и

$$c(\operatorname{Coker} f_r) = (q^{w(r)})^n = \| r \|^{-n}.$$

Итак, все три утверждения доказаны, остается применить теорему 8.1.

Упражнение. Пусть φ: $G \to G$ — аналитический эндоморфизм группы Ли G, являющийся наложением. Используя, например, меру Хаара, показать, что

1) группы $\operatorname{Ker} \varphi$ и $\operatorname{Coker} \varphi$ конечны;

2) $h_\varphi = c(\operatorname{Coker} \varphi)/c(\operatorname{Ker} \varphi) = \| \det T_e\varphi \|^{-1}$.

Глава V

ТЕОРИЯ ЛИ

Если не оговорено противное, k обозначает поле, полное относительно нетривиального абсолютного значения.

§ 1. Алгебра Ли локальной аналитической группы

Пусть $F(X, Y)$ — формальный групповой закон (над полем k). Как мы видели (см. гл. IV, § 7, п. 1),

$$F(X, Y) = X + Y + B(X, Y) + o(d^0 \geqslant 3),$$

где $B(X, Y)$ — билинейная форма.

Положим

$$[X, Y]_F = B(X, Y) - B(Y, X).$$

Операция $[X, Y]_F$ определяет на пространстве k^n структуру алгебры Ли (см. гл. IV, § 7, п. 6). Эту алгебру мы назовем *алгеброй Ли, ассоциированной с формальной группой* F.

Пусть G — локальная аналитическая группа над полем k. Положим $L(G) = \mathfrak{g} = T_e G$. Введем в пространстве $\mathfrak{g}$ структуру алгебры Ли. Для этого выберем на группе G некоторую карту $c = (U, \varphi, n)$ в точке e. Закон композиции в локальной группе G определяется (посредством карты φ) некоторым формальным групповым законом F. Пусть $T_e\varphi = \bar{\varphi}$: $\mathfrak{g} \to k^n$ — соответствующий изоморфизм касательных пространств. Для любой пары элементов $x, y \in \mathfrak{g}$ положим

$$[x, y]_c = \bar{\varphi}^{-1}([\bar{\varphi}x, \bar{\varphi}y]_F).$$

Мы утверждаем, что в действительности $[x, y]_c$ не зависит от выбора карты c. Нам понадобится следующая лемма.

Лемма 1. *Пусть G и G' — две локальные аналитические группы, c и c' — их карты в точках e и e' соответственно и $f\colon G \to G'$ — локальный гомоморфизм. Тогда касательное отображение $T_e f\colon \mathfrak{g} \to \mathfrak{g}'$ является гомоморфизмом алгебр Ли относительно операций $[\ ,\ ]_c$ и $[\ ,\ ]_{c'}$.*

Доказательство немедленно сводится к следующей лемме.

Лемма 2. *Пусть $F(X, Y)$ и $F'(X', Y')$ — два формальных групповых закона и f — формальный гомоморфизм первого закона во второй. Обозначим через f_1 линейную часть отображения f. Тогда*

$$[f_1(X), f_1(Y)]_{F'} = f_1([X, Y]_F).$$

Доказательство. Согласно формуле 5° (гл. IV, § 7), имеем

$$f(X)^{-1} f(Y)^{-1} f(X) f(Y) = [f_1(X), f_1(Y)]_{F'} + o(d^0 \geqslant 3),$$
$$f(X^{-1}Y^{-1}XY) = f_1([X, Y]_F) + o(d^0 \geqslant 3).$$

Сравнивая члены второго порядка, получаем искомую формулу.

Определение. В описанной выше ситуации линейное пространство $\mathfrak{g}$, наделенное канонической структурой алгебры Ли, называется *алгеброй Ли группы G*.

Замечание. Лемма 1 показывает, что указанное соотношение алгебр Ли локальным группам функториально.

§ 2. Простейшие примеры и свойства

1. Алгебра Ли полной линейной группы. Пусть R — конечномерная ассоциативная k-алгебра с единицей. Выше доказывалось (см. гл. IV, § 2, п. 1), что

$G_m(R)$ — аналитическая группа и открытое подмножество в R. Следовательно, $T_1G_m(R)=R$. Умножение в $G_m(R)$ имеет вид

$$(1+x)(1+y)=1+x+y+xy.$$

Ему соответствует следующий формальный групповой закон:

$$F(X, Y)=X+Y+XY.$$

Таким образом, структура алгебры Ли в пространстве $T_1G_m(R)$ задается формулой

$$[x, y]=xy-yx.$$

В частности, если R есть кольцо эндоморфизмов $\operatorname{End} V$ конечномерного векторного пространства V, получаем хорошо известную структуру алгебры Ли.

2. Алгебра Ли прямого произведения групп. Пусть G_1 и G_2 — аналитические группы. Естественный изоморфизм линейных пространств $T_e(G_1\times G_2)$ и $T_eG_1\times T_eG_2$ есть изоморфизм соответствующих алгебр Ли, т. е.

$$L(G_1\times G_2)=L(G_1)\times L(G_2).$$

В самом деле, пусть c_1 и c_2 — карты групп G_1 и G_2 в точках e_1 и e_2 соответственно. Тогда $c=c_1\times c_2$ — карта произведения $G_1\times G_2$. Требуемое утверждение легко вытекает из сравнения операций $[\ ,\ ]_{c_i}$ $(i=1, 2)$ и $[\ ,\ ]_c$.

3. Алгебра Ли подгруппы Ли. Пусть заданы две аналитические группы G и H и аналитический *регулярный гомоморфизм* f: $H\to G$. Отображение $L(f)$: $L(H)\to L(G)$, очевидно, инъективно, так что $L(H)$ можно отождествить с подалгеброй алгебры $L(G)$. Это замечание применимо, в частности, тогда, когда H — подгруппа Ли группы G и f — соответствующее вложение.

Рассмотрим подробнее случай, когда характеристика поля k равна нулю.

Теорема 1. *Пусть H_1 и H_2 — подгруппы Ли группы Ли G, и пусть характеристика поля k равна нулю. Тогда пересечение $H_1 \cap H_2$ — тоже подгруппа Ли и $L(H_1 \cap H_2) = L(H_1) \cap L(H_2)$.*

Доказательство. Согласно теореме 4.5.1, множество (левых) смежных классов G/H_1 является многообразием. Обозначим через $\bar{e}$ смежный класс H_1 в G/H_1. Группа H_2 действует (слева) в пространстве G/H_1, причем $H_1 \subset H_2$ — стационарная подгруппа точки $\bar{e}$. Но тогда $H_1 \cap H_2$ — подгруппа Ли группы G (см. гл. IV, § 5, теоремы 2 и 3). Наконец, $L(H_1 \cap H_2)$ отождествляется со своим образом в $L(G)$, который, очевидно, равен ядру отображения $T_e H_2 \to T_e G / T_e H_1$ (см. теорему 4.5.2, (2)), т. е. пересечению $L(H_1) \cap L(H_2)$.

Следствие 1. *Допустим, что $L(H_1) \subset L(H_2)$. Тогда в некоторой окрестности единицы $H_1 \subset H_2$.*

Доказательство. Имеем

$$T_e(H_1 \cap H_2) = L(H_1) \cap L(H_2) = L(H_1) = T_e H_1$$

и

$$H_1 \cap H_2 \subset H_1,$$

откуда ясно, что вложение $H_1 \cap H_2 \to H_2$ есть локальный изоморфизм. Поэтому в некоторой окрестности точки e группы H_1 и $H_1 \cap H_2$ совпадают, т. е. локально $H_1 \subset H_2$.

Следствие 2. *Допустим, что $L(H_1) = L(H_2)$. Тогда в некоторой окрестности единицы $H_1 = H_2$.*

Следствие 3. *Пусть G_1 и G_2 — две группы Ли и φ, ψ: $G_1 \to G_2$ — пара аналитических гомоморфизмов. Условие $L(\varphi) = L(\psi)$ равносильно совпадению отображений φ и ψ в некоторой окрестности точки e_1.*

Доказательство. Пусть графики G_φ и G_ψ гомоморфизмов φ и ψ в $G_1 \times G_2$ являются подгруппами

Ли. Имея в виду указанные выше отождествления, мы можем написать

$$L(G_\varphi)=\{(x,\ y)\in L(G_1\times G_2)\,|\,y=L(\varphi)(x)\},$$
$$L(G_\psi)=\{(x,\ y)\in L(G_1\times G_2)\,|\,y=L(\psi))x)\}.$$

Далее, на основании следствия 2 условия:

а) отображения φ и ψ совпадают в окрестности точки e_1;

б) графики G_φ и G_ψ совпадают в окрестности точки $(e_1,\ e_2)\in G_1\times G_2$;

в) $L(\varphi)=L(\psi)$

эквивалентны. Это завершает доказательство.

4. Алгебра Ли ядра гомоморфизма. Пусть заданы две аналитические группы G и H и аналитический локально линейный гомоморфизм f: $G\to H$. Обозначим через K ядро этого гомоморфизма. В силу следствия теоремы 2 §5 гл. IV K — подгруппа Ли группы G; кроме того,

$$L(K)=\operatorname{Ker}T_e(\varphi)=\{x\in L(G)\,|\,L(\varphi)(x)=0\}.$$

§ 3. Линейные представления

Пусть G — аналитическая группа и V — векторное пространство[1]). *Линейным представлением* группы G в пространстве V называется аналитический гомоморфизм σ: $G\to GL(V)$. Линейное представление определяет *действие* группы G в пространстве V:

$$gv=\sigma(g)(v).$$

Представление σ индуцирует также представление алгебры $L(G)$, т. е. гомоморфизм алгебр Ли $\tilde\sigma$: $L(G)\to$ $\to\operatorname{End}V$.

1. Основные примеры. (i) Тождественное представление:

$$GL(V)\to GL(V).$$

[1]) Все рассматриваемые здесь линейные пространства предполагаются конечномерными. — *Прим. перев.*

(ii) Обозначим через V^* пространство, двойственное к V. Введем отображение *: $GL(V) \to GL(V^*)$, $u \mapsto {}^t u^{-1}$ Легко, проверяется, что * — аналитический групповой изоморфизм. Пусть $1 = \mathrm{id}_V$ и $1^* = \mathrm{id}_{V^*}$. В некоторой окрестности элемента 1 имеем

$$^*(1+x) = (1^* + {}^t x)^{-1} = \sum_{\mu=0}^{\infty} (-1)^\mu ({}^t x)^\mu = 1^* - {}^t x + o(d^0 \geqslant 2).$$

В частности, $L(^*)(x) = -{}^t x$.

(iii) Пусть $V_1, \ldots, V_n$ — векторные пространства и $V = V_1 \otimes \ldots \otimes V_n$. Определим отображение

$$\theta\colon \operatorname{End} V_1 \times \ldots \times \operatorname{End} V_n \to \operatorname{End} V,$$

положив

$$\theta(y_1, \ldots, y_n) = y_1 \otimes \ldots \otimes y_n, \quad y_i \in \operatorname{End} V_i, \quad i = 1, \ldots, n.$$

Это отображение, очевидно, индуцирует аналитический гомоморфизм $\prod_{i=1}^{n} GL(V_i) \to GL(V)$, причем в некоторой окрестности единицы

$$\theta(1+x_1, \ldots, 1+x_n) = 1 + \sum_{i=1}^{n} 1 \otimes \ldots \otimes x_i \otimes \ldots \\ \ldots \otimes 1 + o(d^0 \geqslant 2).$$

В частности,

$$L(\theta)(x_1, \ldots, x_n) = \sum_{i=1}^{n} 1 \otimes \ldots \otimes x_i \otimes \ldots \otimes 1.$$

(iv) Пусть $V_1, \ldots, V_n, W$ — векторные пространства, $V = \operatorname{Hom}_k(V_1 \otimes \ldots \otimes V_n, W)$ — пространство полилинейных отображений и $G = \left(\prod_{i=1}^{n} GL(V_i)\right) \times GL(W)$. Пространство V канонически изоморфно тензорному произведению $V_1^* \otimes \ldots \otimes V_n^* \otimes W$. Используя отображения из примеров (ii) и (iii), получаем гомоморфизм θ: $G \to GL(V)$. Он задается следующей формулой:

$$\theta(y_1, \ldots, y_n, w)(v) = w \circ v \circ (y_1 \otimes \ldots \otimes y_n)^{-1}.$$

Применяя предыдущие результаты, находим

$$L(\theta)(x_1, \ldots, x_n, z)(y) = \\ = z \circ y - \sum_{i=1}^{n} y \circ (1 \otimes \ldots \otimes x_i \otimes \ldots \otimes 1).$$

(v) Возьмем группу $G = GL(V)$ и рассмотрим аналитический гомоморфизм det: $G \to G_m(k)$. Здесь $\det(y)$ означает определитель отображения y, а $G_m(k)$ есть просто группа ненулевых элементов k^*. В некоторой окрестности единицы группы G имеем

$$\det(1 + x) = 1 + \operatorname{Tr}(x) + \ldots + \det(x) = \\ = 1 + \operatorname{Tr}(x) + o(d^0 \geqslant 2),$$

где $\operatorname{Tr}(x)$ — след отображения x. В частности,

$$L(\det)(x) = \operatorname{Tr}(x).$$

2. Ядра представлений. Если линейное представление локально линейно, то можно применить результат п. 4 § 2. Применим его, в частности, к примеру (v) предыдущего пункта. Действительно, отображение det корегулярно (при $V \neq (0)$). Рассмотрим группу

$$SL(V) = \ker(\det).$$

Она является группой Ли. Ее называют *специальной линейной группой*. В частности, с учетом результатов § 1 получаем

$$L(SL(V)) = \{x \in \operatorname{End} V \mid \operatorname{Tr}(x) = 0\}.$$

3. Стационарные подгруппы. Пусть, как и раньше, char $k = 0$. В предыдущей главе (см. § 5, теоремы 2 и 3) было доказано, что стационарная подгруппа $G_x = \{g \in G \mid g \cdot x = x\}$ точки x многообразия X, на котором действует группа Ли G, является подгруппой Ли. Применим этот результат к теории представлений

(i) Пусть σ: $G \to GL(V)$ — линейное представление аналитической группы G в векторном пространстве V. Рассмотрим стационарную подгруппу точки $v \in V$

$$G_v = \{g \in G \mid g \cdot v = v\}.$$

Тогда G_v есть подгруппа Ли в G и

$$L(G_v) = \{x \in L(G) \mid \bar{\sigma}(x)(v) = 0\}.$$

Действительно, пусть φ: $GL(V) \to V$ — отображение, задаваемое правилом $u \to u(v)$. Ясно, что касательное отображение $T_e(\varphi)$: $\operatorname{End} V \to V$ задается формулой $T_e(\varphi)(z) = z(v)$. При этом

$$T_e G_v = \ker(T_e(\varphi \circ \sigma)) = \ker(T_e(\varphi) \circ \bar{\sigma}),$$

что и утверждалось.

(ii) В тех же обозначениях рассмотрим представление $* \circ \sigma$: $G \to GL(V^*)$. Пусть G_f — стационарная подгруппа элемента $f \in V^*$. Тогда

$$G_f = \{g \in G \mid f \circ \sigma(g) = f\},$$
$$L(G_f) = \{x \in L(G) \mid f \circ \bar{\sigma}(x) = 0\}.$$

Для того чтобы установить первое соотношение, достаточно (поскольку G_f — группа) доказать, что включение $g^{-1} \in G_f$ равносильно равенству $f \circ \sigma(g) = f$. Имеем

$$* \circ \sigma(g^{-1})(f) = {}^t\sigma(g^{-1})^{-1}(f) = f \circ \sigma(g),$$

и наш результат вытекает из определения группы G_f. Что касается второго соотношения, то в силу первого достаточно доказать равносильность равенств $L(* \circ \sigma) \cdot (x)(f) = 0$ $(x \in L(G))$ и $f \circ \bar{\sigma}(x) = 0$. Но, согласно п. 1,

$$L(* \circ \sigma)(x)(f) = -{}^t\bar{\sigma}(x)(f) = -f \circ \bar{\sigma}(x),$$

что и доказывает требуемую равносильность.

Важным примером группы типа G_f является группа $A(V)$ аффинных преобразований векторного пространства V. Отождествляя аддитивную группу пространства V с группой сдвигов этого пространства, группу $A(V)$ можно определить как полупрямое произведение групп V и $GL(V)$.

Умножение в этой группе определяется формулой

$$(v_1, g_1)(v_2, g_2) = (v_1 + g_1 v_2, g_1 g_2)$$
$$(v_1, v_2 \in V, g_1, g_2 \in GL(V)).$$

Оказывается, что группу $A(V)$ можно отождествить с подгруппой $G \subset GL(V \times k)$, оставляющей инвариантными гиперплоскости вида $V \times \alpha$ ($\alpha \in k$). Для доказательства этого факта нужно рассмотреть отображение σ: $A(V) \to G$, определенное формулой

$$\sigma(v, g)(w, \alpha) = (\alpha v + gw, \alpha),$$

где $(v, g) \in A(V)$ и $(w, \alpha) \in V \times k$. Группа G имеет вид $GL(V \times k)_f$, где f: $V \times k \to k$ — линейная форма, задаваемая формулой $f(w, \alpha) = \alpha$.

(iii) Пусть σ: $G \to GL(V)$ — линейное представление группы Ли G в векторном пространстве V, и пусть

$$\theta\colon GL(V) \times GL(V) \to GL(V \otimes V)$$

— аналитический гомоморфизм, определенный в п. 1 (здесь $V = V_1 = V_2$). Рассмотрим композицию

$$\tau = \theta \circ (\sigma \times \sigma)\colon G \to GL(V \otimes V).$$

Для всякого элемента $\beta \in (V \otimes V)^*$ определена группа G_β, причем (см. (ii))

$$G_\beta = \{g \in G \mid \beta \circ (\sigma(g) \otimes \sigma(g)) = \beta\}$$

и

$$L(G_\beta) = \{x \in L(G) \mid \beta \circ (\bar{\sigma}(x) \otimes 1 + 1 \otimes \bar{\sigma}(x)) = 0\}.$$

Условие, определяющее алгебру $L(G_\beta)$, означает, что

$$\beta(\bar{\sigma}(x) v \otimes w) + \beta(v \otimes \bar{\sigma}(x) w) = 0$$

для всех v, $w \in V$.

Укажем два применения предыдущих рассмотрений. Пусть $G = GL(V)$ и σ — тождественное представление, причем $V = k^n$, что является наиболее интересным случаем.

А. Ортогональная группа. Определим билинейную форму β в пространстве k^n равенством

$$\beta(x_1, \ldots, x_n; y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i y_i.$$

Соответствующая группа G_β называется *ортогональной группой* пространства k^n. Определим явным образом элементы группы G_β и алгебры Ли $L(G_\beta)$. Пусть $u \in \mathrm{End}(k^n)$. Обозначим через ${}^t u$ сопряженное преобразование (оно задается транспонированной матрицей); легко проверить, что

$$\beta(ux, y) = \beta(x, {}^t u y)$$

для любых $x, y \in k^n$.

Пусть $g \in GL(k^n)$ и $u \in \mathrm{End}(k^n)$. Тогда

а) $\beta(gx, gy) = \beta(x, y) \Leftrightarrow \beta(x, {}^t g \cdot gy) = \beta(x, y)$;

б) $\beta(ux, y) + \beta(x, uy) = 0 \Leftrightarrow \beta(x, ({}^t u + u) y) = 0$.

Ввиду невырожденности формы β это означает, что

$$G_\beta = \{g \in GL(k^n) \mid {}^t g \cdot g = 1\},$$
$$L(G_\beta) = \{u \in \mathrm{End}(k^n) \mid {}^t u + u = 0\}.$$

Б. Симплектическая группа. Пусть $n = 2m$, а билинейная форма β определена равенством

$$\beta(x_1, \ldots, x_{2m}; y_1, \ldots, y_{2m}) = \sum_{i=1}^{m} (x_i y_{m+i} - x_{m+i} y_i).$$

Соответствующая группа G_β называется *симплектической группой* пространства k^{2m}. Покажем, как явно определить группу G_β и алгебру Ли $L(G_\beta)$. Мы можем отождествить пространства $\mathrm{End}(k^m \times k^m)$ и $\mathrm{End}(k^n)$. Иными словами, любое линейное отображение u: $k^n \to k^n$ можно представить в виде

$$u = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

где $A, B, C, D \in \mathrm{End}(k^m)$. Отображению u сопоставим отображение

$$u' = \begin{pmatrix} {}^t D & -{}^t B \\ -{}^t C & {}^t A \end{pmatrix}.$$

Легко проверяется, что

$$\beta(ux, y) = \beta(x, u'y),$$

где $x, y \in k^n$. Используя это тождество, а также невырожденность формы β, нетрудно усмотреть, что

$$G_\beta = \{g \in GL(k^n) \mid g' \cdot g = 1\},$$
$$L(G_\beta) = \{u \in \operatorname{End}(k^n) \mid u' + u = 0\}.$$

Условие, определяющее алгебру $L(G_\beta)$, эквивалентно совокупности трех равенств:

$${}^tA + D = 0, \ {}^tB = B, \ {}^tC = C.$$

(iv) „Метод стационарных подгрупп" можно применять всякий раз, как мы имеем дело с комбинациями стандартных представлений, указанных в п. 1. Формулировку общего утверждения мы предоставляем читателю; приведем здесь еще один пример.

Пусть A — конечномерная k-алгебра, и пусть β: $A \times A \to A$ (или β: $A \otimes_k A \to A$) — закон умножения в алгебре A. Следующие условия эквивалентны ($\beta(x, y) \equiv x \cdot y$):

(а) $g \in GL(A)_\beta$;

(б) $g \in GL(A)$ и $g\beta(g^{-1}x, g^{-1}y) = \beta(x, y)$ для любых $x, y \in A$;

(в) $g \in GL(A)$ и $g(x \cdot y) = (gx) \cdot (gy)$ для любых $x, y \in A$.

Условия (а) и (б) эквивалентны по определению. Эквивалентность условий (б) и (в) доказывается заменой элементов x и y элементами gx и gy соответственно. Таким образом, G_β есть просто группа автоморфизмов алгебры A. Покажем, что $L(G_\beta)$ есть не что иное, как пространство дифференцирований $\operatorname{Der}(A)$ алгебры A в A. В самом деле, включение $d \in L(G_\beta)$ означает, что

$$d\beta(x, y) - \beta(dx, y) - \beta(x, dy) = 0 \text{ для всех } x, y \in A.$$

Но эту формулу можно переписать и так:

$$d(x \cdot y) = (dx) \cdot y + x \cdot (dy),$$

что и требовалось доказать.

4. Присоединенное представление. Пусть G — аналитическая группа. Для каждого элемента $g \in G$ оп-

ределен внутренний автоморфизм φ_g: $G \to G$, $x \mapsto gxg^{-1}$. Пусть $\mathfrak{g} = L(G)$; обозначим через Ad: $G \to GL(\mathfrak{g})$ отображение $g \mapsto T_e\varphi_g$. Очевидно, что отображение Ad является гомоморфизмом. Более того, как мы сейчас увидим, это отображение аналитично, а потому определено отображение $L(\mathrm{Ad})$: $\mathfrak{g} \to \mathrm{End}(\mathfrak{g})$. Будет показано, что $L(\mathrm{Ad})$ совпадает с ad — присоединенным представлением, которое определяется для любых алгебр Ли.

Поскольку Ad — гомоморфизм, достаточно проверить аналитичность этого отображения какой-нибудь окрестности единицы. Вычислим Ad в локальных координатах; для этого воспользуемся формулой 3° гл. IV, § 7. Имеем (в окрестности точки e)

$$\varphi_g(x) = x + [g, x] + \sum d_{\alpha,\beta} g^\alpha x^\beta,$$

где $|\alpha| \geqslant 1$, $|\beta| \geqslant 1$, $|\alpha| + |\beta| \geqslant 3$. Следовательно,

$$\mathrm{Ad}(g) = T_e\varphi_g\colon\ x \mapsto x + [g, x] + \sum d_{\alpha,\beta}\, g^\alpha x^\beta.$$

Мы видим, что отображение Ad аналитично в единице. Далее, в последней сумме $|\alpha| \geqslant 2$, так как $|\beta| = 1$. Поэтому касательное отображение $T_e\mathrm{Ad}(y)$ совпадает с отображением $x \mapsto [y, x]$. Таким образом, $L(\mathrm{Ad})(y) = T_e(\mathrm{Ad})(y) = \mathrm{ad}(y)$, как и утверждалось.

§ 4. Сходимость формулы Кэмпбелла — Хаусдорфа

Теорема 1. *Всякая конечномерная алгебра Ли $\mathfrak{g}$ над полем k нулевой характеристики является алгеброй Ли некоторой локальной аналитической группы.*

Доказательство. Пусть $n = \dim_k \mathfrak{g}$. С помощью формулы Кэмпбелла — Хаусдорфа (см. часть I, § 7, 8) определим формальный групповой закон $F = (F_i)$ от n переменных, такой, что ряды F_i сходятся и алгебра $\mathfrak{g}$ изоморфна алгебре Ли, определенной в пространстве k^n посредством операции $[\,,\,]_F$. Доказательство мы проведем в три приема.

1°. С каждым базисом $x_1, \ldots, x_n$ алгебры $\mathfrak{g}$ связана однозначно определенная система *структурных констант*

$$\gamma_{ij}^h = \gamma_{ij}^h(x_1, \cdots x_n),$$

таких, что

$$[x_i, x_j] = \sum_{h=1}^{n} \gamma_{ij}^h x_h, \quad 1 \leqslant i, j \leqslant n.$$

Положим

$$\gamma = \gamma(x_1, \ldots, x_n) = \max |\gamma_{ij}^h|.$$

Система $\lambda x_1, \ldots, \lambda x_n (\lambda \in k, \lambda \neq 0)$ также является базисом, причем

$$\gamma_{ij}^h(\lambda x_1, \ldots, \lambda x_n) = \lambda \gamma_{ij}^h(x_1, \ldots, x_n),$$
$$\gamma(\lambda x_1, \ldots, \lambda x_n) = |\lambda| \gamma(x_1, \ldots, x_n).$$

2°. Пусть $R = k[[X, Y]] = k[[X_1, \ldots, X_n; Y_1, \ldots \ldots, Y_n]]$, и пусть $E = R^n$. При фиксированном базисе $x_1, \ldots, x_n$ определим на множестве E структуру алгебры Ли формулой

$$[(f_i), (g_j)] = \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \gamma_{ij}^h f_i g_j\right), \quad 1 \leqslant h \leqslant n.$$

В частности, рассмотрим отображения $\mathrm{ad}(X)$ и $\mathrm{ad}(Y)$, где $X = (X_1, \ldots, X_n)$ и $Y = (Y_1, \ldots, Y_n)$.

Будем называть набор $P = (P_1, \ldots, P_n) \in E$ *однородным многочленом* степени r, если каждый ряд P_i является однородным многочленом степени r. Символом $\|P\|$ в этом случае обозначим $\max\limits_{i\alpha} |a_\alpha^i|$, где a_α^i — коэффициенты многочлена P_i.

Лемма 1. *Пусть $P \in E$ — однородный многочлен степени r. Тогда $\mathrm{ad}(X)(P)$ и $\mathrm{ad}(Y)(P)$ — однородные многочлены степени $r+1$, причем $\|\mathrm{ad}(X)(P)\| \leqslant n^2\gamma\|P\|$ и $\|\mathrm{ad}(Y)(P)\| \leqslant n^2\gamma\|P\|$.*

Доказательство леммы. Пусть $\mathrm{ad}(X)(P) = (Q_1, \ldots, Q_n)$, и пусть $P_j = \sum Q_{\alpha,\beta}^j X^\alpha Y^\beta$, $Q_h = \sum b_{\alpha,\beta}^h X^\alpha Y^\beta$. По определению

$$Q_h = \sum_{i,j} \gamma_{ij}^h X_i P_j,$$

а следовательно, Q_h — однородный многочлен степени $r+1$ и

$$b^h_{\alpha,\beta} = \sum_{i=1}^{n} \sum_{j=1}^{n} \gamma^h_{ij} a^j_{\alpha-\delta_i,\beta} (\delta_i = (0, \ldots, 1, \ldots, 0)).$$

Отсюда $|b^h_{\alpha,\beta}| \leqslant n^2\gamma\|P\|$. Аналогично доказывается утверждение для многочлена $\mathrm{ad}(Y)(P)$.

Следствие. *Пусть* $\mathfrak{m}$ — *максимальный идеал* (X, Y) *в кольце* R. *Тогда*

$$\mathrm{ad}(X)(\mathfrak{m}^r E) \subset \mathfrak{m}^{r+1} E$$

и

$$\mathrm{ad}(Y)(\mathfrak{m}^r E) \subset \mathfrak{m}^{r+1} E \ (r > 0).$$

3° Пусть $S = \{\bar{x}, \bar{y}\}$ — множество из двух элементов. Рассмотрим свободную алгебру Ли L_S над S, ее пополнение $\hat{L}_S = \prod_{r=0}^{\infty} L^r_S$ (см. часть I, гл. IV, § 3, 7) и канонический гомоморфизм алгебр Ли θ: $L_S \to E$, такой, что $\theta(\bar{x}) = X$ и $\theta(\bar{y}) = Y$.

Лемма 2. $\theta(L^r_S) \subset \mathfrak{m}^r E \ (r > 0)$.

Доказательство непосредственно вытекает из следствия леммы 1.

В частности, θ единственным образом продолжается до гомоморфизма $\hat{L}_S \to E$.

В алгебре $\hat{L}_S$ существует однозначно определенный элемент $\bar{z}$, для которого $e^{\bar{x}} \cdot e^{\bar{y}} = e^{\bar{z}}$ (теорема 1.4.7.4). Пусть $F = \theta(\bar{z})$. Используя замечание в конце § 7 гл. IV ч. I, получаем следующие утверждения:

1) F — формальный групповой закон от переменных X и Y;

2) $F = X + Y + B(X, Y) + o(d^0 \geqslant 3)$, причем $B(X,Y) = {}^1/_2 [X, Y]$.

В частности, $[X, Y]_F = {}^1/_2 [X, Y] - {}^1/_2 [Y, X] = [X, Y]$.

Прежде чем завершить доказательство теоремы 1, докажем следующую теорему.

Теорема 2. *Ряды* $F = (F_i)$ *сходятся.*

Доказательство. Нам понадобятся две элементарные леммы.

Лемма 3. *При достаточно малых t ряд*

$$\sum_{\substack{p_1, \ldots, p_m \in \mathbf{N} \\ q_1, \ldots, q_m \in \mathbf{N} \\ p_i + q_i \geqslant 1 \\ m \geqslant 1}} t^{\Sigma p_i + \Sigma q_i}$$

сходится.

Доказательство леммы 3. Указанный ряд можно переписать так:

$$\sum_{m=1}^{\infty} \left(\sum_{p+q \geqslant 1} t^{p+q} \right)^m.$$

При $|t| < 1$ член в скобках сходится к α, где

$$\alpha = \frac{1}{(1-t)^2} - 1.$$

Но при достаточно малых $|t|$ имеем $0 < \alpha < 1$, что гарантирует сходимость всего ряда.

Лемма 4. *Существует константа a, $0 < a \leqslant 1$, такая, что*

$$|n!| \geqslant a^n \text{ и } |n| \geqslant a^n \, (n \in \mathbf{Z},\ n > 0).$$

Доказательство леммы 4. Рассмотрим три случая.

А) Поле k архимедово. Берем $a = 1$.

Б) Поле k неархимедово и ограничение его абсолютного значения на подполе $\mathbf{Q}$ тривиально. Берем $a = 1$.

В) Поле k неархимедово и ограничение его абсолютного значения на подполе $\mathbf{Q}$ совпадает с одним из p-адических абсолютных значений.

Заметим сначала, что неравенство $|n| \geqslant a^n$ следует из неравенства $|n!| \geqslant a^n$, так как $|(n-1)!| \leqslant 1$ для всех $n \geqslant 1$. Возьмем в качестве a число $|p|^{1/p-1}$. Неравенство $|n!| \geqslant a^n$ означает, что $v_p(n!) \leqslant n/p - 1$. Однако

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots < \frac{n}{p} + \frac{n}{p^2} + \ldots = \frac{n}{p-1}.$$

Приступим теперь к доказательству теоремы 2. Заметим прежде всего, что если умножить все координаты на некоторый элемент $\lambda \in k^*$, это не повлияет на сходимость. Поэтому можно заменить базис $x_1, \ldots, x_n$ алгебры $\mathfrak{g}$ на базис $\lambda x_1, \ldots, \lambda x_n$ $(\lambda \neq 0)$, где

$$|\lambda|\gamma \leqslant \frac{1}{n^2}.$$

Используя для нового базиса старые обозначения, получаем (в силу леммы 1) следующую лемму.

Лемма 1′. *Пусть $P \in E$ — однородный многочлен степени r. Тогда* $\operatorname{ad}(X)(P)$ *и* $\operatorname{ad}(Y)(P)$ — *однородные многочлены степени* $(r+1)$, *причем* $\|\operatorname{ad}(X)(P)\| \leqslant \|P\|$ *и* $\|\operatorname{ad}(Y)(P)\| \leqslant \|P\|$.

Воспользуемся теперь формулой Дынкина (см. ч. I, гл. IV, § 8):

$$\theta(\bar{z}) = F(X, Y) = \sum_{\nu} f_\nu(X, Y),$$

где

$$f_\nu(X, Y) = \frac{1}{\nu} \sum_{p+q=\nu} (f'_{p,q}(X, Y) + f''_{p,q}(X, Y)).$$

Здесь

$$f'_{p,q} = \sum_{\substack{p_1+\ldots+p_m=p \\ q_1+\ldots+q_{m-1}=q-1 \\ p_i+q_i \geqslant 1 \\ p_m \geqslant 1}} \frac{(-1)^{m+1}}{m} \frac{\operatorname{ad}(X)^{p_1} \operatorname{ad}(Y)^{q_1} \ldots \operatorname{ad}(X)^{p_m}(Y)}{p_1!\, q_1! \ldots p_m!},$$

$$f''_{p,q} = \sum_{\substack{p_1+\ldots+p_{m-1}=p-1 \\ q_1+\ldots+q_{m-1}=q \\ p_i+q_i \geqslant 1}} \frac{(-1)^{m+1}}{m} \frac{\operatorname{ad}(X)^{p_1} \operatorname{ad}(Y)^{q_1} \ldots \operatorname{ad}(Y)^{q_{m-1}}(X)}{p_1!\, q_1! \ldots q_{m-1}!}.$$

Все числители в последних двух суммах представляют собой однородные многочлены степени $\nu = p + q$, причем, согласно лемме 1, значение нашего абсолютного значения на коэффициентах этих многочленов не превосходит единицы. Далее, используя явный вид операции [,], легко подсчитать по индукции, что количество одночленов, входящих в эти

многочлены, не превышает $n^{2\nu}$. Итак, каждый числитель мажорируется вещественным однородным многочленом от переменных X и Y степени ν, все коэффициенты которого равны единице, а число одночленов не превышает $n^{2\nu}$. Значение такого многочлена на векторе $(s, \ldots, s) \in R^{2n}$ $(s > 0)$ оценивается сверху числом

$$n^{2\nu} s^{\nu} = (n^2 s)^{p+q}.$$

С другой стороны, для чисел, входящих в знаменатель, имеют место следующие оценки:

$$|\nu| \geqslant a^{\nu} = a^{p+q},$$

$$|m| \geqslant a^{m} \geqslant a^{p+q},$$

$$\left.\begin{array}{l} |p_1!\, q_1! \ldots p_m!| \\ |p_1!\, q_1! \ldots q_{m-1}!| \end{array}\right\} \geqslant a^{\Sigma p_i + \Sigma q_i} = a^{p+q}.$$

Полагая $t = (n^2 s / a^3)$, мы видим, что ряд $F(X, Y) = \sum\limits_{\nu} f_{\nu}(X, Y)$ мажорируется вещественным рядом из леммы 3. При достаточно малых значениях t последний ряд сходится, что обеспечивает сходимость ряда $F(x, y)$ при достаточно малых s.

Таким образом, все теоремы полностью доказаны.

Замечания. 1. Если $\mathfrak{g}$ — нильпотентная алгебра Ли (см. ч. I, гл. V, § 2), то ряд F вырождается в многочлен, так что его сходимость тривиальна.

2. Для того чтобы в общем случае оценить радиус сходимости ряда F, надо оценить две константы, фигурирующие в доказательстве, а именно:

1) константу a из леммы 4;

2) радиус сходимости ряда из леммы 3.

Что касается последнего ряда, то, как легко видеть, он сходится, если

$$|t| < \frac{\sqrt{2} - 1}{\sqrt{2}}.$$

Следовательно, ряд F сходится в шаре $B(r)$, где

$$r < \frac{a^3}{n^2} \frac{\sqrt{2} - 1}{\sqrt{2}}.$$

Это не слишком хорошая оценка, но для $k = \mathbf{R}$ или $\mathbf{C}$ ничего лучшего неизвестно.

Пусть k — неархимедово поле и ограничение его абсолютного значения на подполе $\mathbf{Q}$ индуцирует p-адическое абсолютное значение. Предположим, что $\mathfrak{g}$ — подалгебра алгебры Ли $L(G_m(R))$, где R — конечномерная ассоциативная k-алгебра с единицей. Другими словами, $\mathfrak{g} \subset R$ и $[x, y] = xy - yx \in \mathfrak{g}$ для любых $x, y \in \mathfrak{g}$. Допустим для простоты, что умножение в алгебре R удовлетворяет неравенству $|x \cdot y| \leqslant \leqslant |x| \cdot |y|$. При этих условиях можно определить экспоненциальный ряд

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots .$$

Экспонента определяет изоморфизм открытой аддитивной подгруппы M на себя, где

$$M = \left\{ x \in R \mid v(x) < \frac{v(p)}{p-1} \right\}.$$

На множестве M можно определить групповой закон, полагая $G(x, y) = z$, где элемент $z \in M$ однозначно определяется соотношением $e^x \cdot e^y = e^z$. Из конструкции формулы Кэмпбелла — Хаусдорфа (см. теорему 1.4.7.4) видно, что наш закон согласуется с формулой Кэмпбелла — Хаусдорфа там, где последняя сходится. Как показал Лазар[1]), фактически она сходится на всем множестве M. В частности, мы получаем, что формула Кэмпбелла — Хаусдорфа сходится на $M \cap \mathfrak{g}$.

3. Если поле k неархимедово, то, как известно (см. гл. IV, § 8), каждая локальная аналитическая группа соответствует некоторой аналитической группе. Поэтому справедливо

Следствие. *Если поле k неархимедово и имеет нулевую характеристику, то каждая конечномерная алгебра Ли является алгеброй Ли некоторой аналитической группы над k.*

---

[1]) См. Лазар [3*]. — *Прим. перев.*

§ 5. Точечные распределения

В этом параграфе мы введем понятие *распределения*[1]), *носитель которого сосредоточен в одной точке.* Это понятие понадобится нам в качестве технического средства в следующем параграфе, где будет доказана эквивалентность категории формальных групп и категории алгебр Ли.

При изучении „формальных вопросов" k будет предполагаться просто коммутативным кольцом с единицей (иногда $\mathbf{Q}$-алгеброй); однако, рассматривая „вопросы сходимости", мы будем, как правило, считать, что k — поле, полное относительно нетривиального абсолютного значения.

1. Пусть X — аналитическое многообразие, и пусть $P \in X$. В гл. III, § 7 было определено локальное кольцо $\mathscr{H}_P$ многообразия X в точке P и его максимальный идеал $\mathfrak{m}_P$. Было показано, что кольцо $\mathscr{H}_P$ изоморфно кольцу сходящихся степенных рядов от n переменных, где $n = \dim_P X$. Наделим это кольцо обычной топологией, принимая степени идеала $\mathfrak{m}_P$ за фундаментальную систему окрестностей нуля. Поле $k \subset \mathscr{H}_P$ при этом автоматически наделяется дискретной топологией.

Точечным распределением на $\mathscr{H}_P$ мы назовем линейную форму $u: \mathscr{H}_P \to k$, удовлетворяющую одному из следующих двух эквивалентных условий:

(1) форма u обращается в нуль на некоторой степени идеала $\mathfrak{m}_P$;

(2) отображение u: $\mathscr{H}_P \to k$ непрерывно (относительно дискретной топологии в k).

Форму u можно продолжить по непрерывности на пополнение $\tilde{\mathscr{H}}_P$ кольца $\mathscr{H}_P$ в этой топологии. Заметим, что $\tilde{\mathscr{H}}_P$ изоморфно кольцу формальных степенных рядов от n переменных над полем k.

2. Пусть k — коммутативное кольцо с единицей и $H = k[[X_1, \ldots, X_n]]$ — кольцо формальных степен-

---

[1]) У нас больше принят термин „обобщенная функция". — *Прим. ред.*

ных рядов от n переменных над кольцом k. Обозначим через $\mathfrak{m}$ идеал, порожденный элементами $X_1, \ldots, X_n$, а через H_r — факторкольцо $H/\mathfrak{m}^{r+1}$ ($r \in \mathbf{Z}$, $r > 0$). Положим, далее, $U_r = H_r^* = L(H_r, k)$. Как и выше, линейную форму u: $H \to k$ мы назовем *точечным распределением*, если выполнены следующие эквивалентные условия:

(1) форма u обращается в нуль на некоторой степени $\mathfrak{m}^{r+1}$ (иными словами, отображение u „пропускается" через проекцию $H \to H_r$);

(2) отображение u непрерывно на H.

Пусть $U \subset H^*$ — подмножество всех точечных распределений. Рассмотрим проекцию $H \to H_r$. Сопряженным к ней отображением будет инъекция $U_r \to H^*$. Мы видим, что U можно отображать с объединением образов множеств $\{U_r\}$.

Рассмотрим подробнее строение k-модулей H и U. По определению H (как k-модуль) есть произведение $\prod kX^\alpha$. Для каждого α определим элемент $\Delta^\alpha \in U$ формулой

$$\Delta^\alpha(X^\beta) = \begin{cases} 1 \text{ при } \alpha = \beta, \\ 0 \text{ при } \alpha \neq \beta. \end{cases}$$

Элементы Δ^α линейно независимы над k. Кроме того, любой элемент $u \in U$ представляется в виде конечной линейной комбинации (над k) этих элементов, поскольку u аннулируется на некоторой степени идеала $\mathfrak{m}$. Итак, справедлива

Лемма 1. $U = \bigoplus_\alpha k \cdot \Delta^\alpha$.

Имеет также место

Лемма 2. $U^* = H$.

Доказательство. Поскольку $U \subset H^*$, имеется отображение $H \to H^{**} \to U^*$. При этом отображении элемент X^α отождествляется с такой линейной формой на U, которая равна 1 на Δ^α и нулю на Δ^β ($\beta \neq \alpha$). Поэтому

$$U^* = L\left(\bigoplus_\alpha k\cdot\Delta^\alpha,\ k\right) = \prod_\alpha L(k\cdot\Delta^\alpha,\ k) = \prod_\alpha k\cdot X^\alpha = H.$$

Замечание. Распределение $\varepsilon = \Delta^0$ называется *распределением Дирака*[1]).

Посмотрим теперь, какую структуру индуцирует на U закон умножения μ: $H\otimes H\to H$. Пусть $\mathfrak{m} = \mathfrak{m}\otimes H + H\otimes\mathfrak{m}$ — идеал кольца $H\otimes H$. Введем в этом кольце топологию, определенную степенями идеала $\mathfrak{m}$. В такой топологии отображение μ непрерывно и потому продолжается на пополнение $H\hat{\otimes}H$ кольца $H\otimes H$. Пусть $\bar{U}$ — множество точечных распределений кольца $H\otimes H$ (или, что то же самое, кольца $H\hat{\otimes}H$). Сопряженное отображение μ^*: $H^*\to(H\hat{\otimes}H)^*$ индуцирует при ограничении так называемое *диагональное отображение* δ: $U\to\bar{U}$. Смысл названия поясняет следующая

Лемма 3. (а) *Каноническое отображение $U\otimes U\to\bar{U}$ есть изоморфизм.*

(б) $\delta(\Delta^\alpha) = \sum_{\beta+\gamma=\alpha}\Delta^\beta\otimes\Delta^\gamma$ (*формула Лейбница*).

Доказательство. Положим $X_i\otimes 1 = Y_i$ и $1\otimes X_i = Z_i$, $1\leqslant i\leqslant n$. Каноническое вложение

$$H\otimes H\to k[[Y_1,\ \ldots,\ Y_n,\ Z_1,\ \ldots,\ Z_n]] = \bar{H}$$

продолжается до изоморфизма колец $H\hat{\otimes}H$ и $\bar{H}$. При этом отождествлении в $\bar{U}$ выделяется канонический базис $\Delta^{\alpha,\beta}$:

$$\Delta^{\alpha,\beta}(Y^{\alpha'}Z^{\beta'}) = \begin{cases} 1, & \text{если } \alpha=\alpha' \text{ и } \beta=\beta', \\ 0 & \text{в противном случае.}\end{cases}$$

Отображение $U\otimes U\to\bar{U}$ переводит базисный элемент $\Delta^\alpha\otimes\Delta^\beta$ модуля $U\otimes U$ в базисный элемент $\Delta^{\alpha,\beta}$ модуля $\bar{U}$. Тем самым первое утверждение доказано.

---

[1]) Или дельта-функцией Дирака. — *Прим. ред.*

Для доказательства второго утверждения достаточно посмотреть, какое значение принимает форма $\delta(\Delta^\alpha)$ на произвольном одночлене $Y^\beta Z^\gamma$. Имеем

$$\delta(\Delta^\alpha)(Y^\beta Z^\gamma) = \Delta^\alpha(\mu(Y^\beta Z^\gamma)) = \Delta^\alpha(X^{\beta+\gamma}).$$

Отсюда

$$\delta(\Delta^\alpha)(Y^\beta Z^\gamma) = \begin{cases} 1, & \text{если } \beta+\gamma=\alpha, \\ 0 & \text{в противном случае,} \end{cases}$$

что и доказывает формулу Лейбница, а с ней и лемму.

Равенство $H = k \oplus \mathfrak{m}$ позволяет обобщить понятие касательного вектора на алгебраическую ситуацию, которую мы изучаем. Именно: мы скажем, что $u \in U$ — *касательный вектор*, если выполняются следующие три эквивалентных условия:

(1) отображение u: $H \to k$ — дифференцирование;

(2) форма u обращается в нуль на k и на $\mathfrak{m}^2$;

(3) элемент u примитивен относительно δ, т. е. $\delta(u) = u \otimes 1 + 1 \otimes u$.

Эквивалентность первых двух условий доказывается так же, как в гл. III, § 8, п. 1. Эквивалентность условий (1) и (3) вытекает из формулы Лейбница.

§ 6. Биалгебра, ассоциированная с формальной группой

Для того чтобы мотивировать изучение „формального случая“, мы рассмотрим сначала вкратце „случай сходимости“.

1. Пусть G — аналитическая группа, $\mathscr{H}$ — локальное кольцо этой группы в точке e, $\mathfrak{m}$ — максимальный идеал этого кольца, $\hat{\mathscr{H}}$ — его пополнение (относительно топологии, определенной степенями идеала $\mathfrak{m}$) и U — множество точечных распределений на $\mathscr{H}$ (или на $\hat{\mathscr{H}}$). В формальной теории (§ 5, п. 2) было определено диагональное отображение δ: $U \to U \otimes U$. Используя групповой закон $\varphi : G \times G \to G$, можно определить умножение θ: $U \otimes U \to U$. Именно: введем отображение σ: $\mathscr{H}_e \to \mathscr{H}_{(e,e)}$ $f \mapsto f \circ \varphi$ (здесь $\mathscr{H}_e = \mathscr{H}$ и $\mathscr{H}_{(e,e)}$ — локальное кольцо группы $G \times G$ в точке

(e, e)). Полученное отображение продолжим до отображения $\hat{\sigma}$: $\mathscr{H} \to \mathscr{H}_{(e,e)} = \mathscr{H} \widehat{\otimes} \mathscr{H}$. Сопряженное к $\hat{\sigma}$ отображение u есть искомое отображение $\theta = (\hat{\sigma})^*$: $U \otimes \otimes U \to U$.

В „формальной ситуации", как мы увидим, U является (относительно θ) ассоциативной $\mathbf{Q}$-алгеброй с единицей (каковою является распределение Дирака).

2. Сохраним все обозначения и предположения § 5, п. 2. Пусть $\overline{H} = k[[Y_1, \ldots, Y_n, Z_1, \ldots, Z_n]]$, и пусть $F \in \overline{H}^n$ — формальный групповой закон над k от n переменных. Положим $\overline{\mathfrak{m}} = \mathfrak{m} \widehat{\otimes} H + H \widehat{\otimes} \mathfrak{m}$ (напомним, что при доказательстве леммы 5.3 кольца $\overline{H}$ и $H \widehat{\otimes} H$ были отождествлены).

Поскольку ряды $F = (F_i)$ не имеют свободных членов, для любого элемента $f \in H$ можно образовать композицию $f \circ F \in \overline{H}$ (см. Бурбаки [3*], гл. IV, § 5, п. 5). Обозначим через σ: $H \to \overline{H}$ отображение $f \mapsto f \circ F$. Тогда $\sigma(\mathfrak{m}^r) \subset \overline{\mathfrak{m}}^r$, так что σ — непрерывное отображение (относительно топологий, определенных идеалами $\mathfrak{m}$ и $\overline{\mathfrak{m}}$). Пусть θ: $U \otimes U \to U$ — сопряженное к σ отображение.

Лемма 1. *Отображение θ наделяет U структурой ассоциативной алгебры с единицей (каковой является распределение Дирака).*

Доказательство. Нам придется иметь дело с двумя кольцами степенных рядов $\overline{H} = k[[Y, Z]]$ и $\overline{\overline{H}} = k[[Y, Z, W]]$, где $W = (W_1, \ldots, W_n)$. Через Δ_Y^α, Δ_Z^β, Δ_W^γ обозначим элементы, двойственные к одночленам Y^α, Z^β, W^γ соответственно. Тогда, например, произведение $\Delta_Y^\alpha \Delta_Z^\beta \Delta_W^\gamma$ двойственно к одночлену $Y^\alpha Z^\beta W^\gamma$.

Покажем вначале ассоциативность операции θ. Пусть $\Delta^\alpha \otimes \Delta^\beta \otimes \Delta^\gamma$ — произвольный базисный элемент модуля $U \otimes U \otimes U$. Тогда для $f \in H$ имеем

$$\theta(\Delta^\alpha, \theta(\Delta^\beta, \Delta^\gamma)) f = \Delta_Y^\alpha \Delta_Z^\beta \Delta_W^\gamma (f \circ F(Y, F(Z, W))),$$

$$\theta(\theta(\Delta^\alpha, \Delta^\beta), \Delta^\gamma) f = \Delta_Y^\alpha \Delta_Z^\beta \Delta_W^\gamma (f \circ (F(Y, Z), W)).$$

Требуемая ассоциативность легко вытекает из ассоциативности закона F.

Осталось показать, что распределение Дирака ε является единицей относительно нашего умножения. Пусть $\Delta^\alpha \in U$ и $f \in H$. Тогда

$$\theta(\varepsilon, \Delta^\alpha) f = \varepsilon_Y \Delta^\alpha_Z (f \circ F(Y, Z)) = \Delta^\alpha_Z (f \circ F(0, Z)) = \Delta^\alpha_Z (f(Z)).$$

Это означает, что $\theta(\varepsilon, \Delta^\alpha) = \Delta^\alpha$. Тем самым доказано, что ε — левая единица. Аналогично доказывается, что ε — правая единица.

Лемма 2. *Диагональное отображение* $\delta\colon U \to U \otimes U$ *является гомоморфизмом алгебр.*

Доказательство. Мы должны доказать коммутативность следующей диаграммы:

$$\begin{tikzcd} U \otimes U \arrow[r, "\delta \otimes \delta"] \arrow[d, "\theta"'] & (U \otimes U) \otimes (U \otimes U) \arrow[d, "\theta \otimes \theta"] \\ U \arrow[r] & U \otimes U \end{tikzcd}$$

Поскольку все модули в этой диаграмме свободны, нам достаточно доказать коммутативность двойственной диаграммы:

$$\begin{tikzcd} H \hat{\otimes} H & (H \hat{\otimes} H) \hat{\otimes} (H \hat{\otimes} H) \arrow[l, "\mu \hat{\otimes} \mu"'] \\ H \arrow[u, "\sigma"] & H \hat{\otimes} H \arrow[l, "\mu"'] \arrow[u, "\sigma \hat{\otimes} \sigma"'] \end{tikzcd}$$

Поскольку все отображения этой диаграммы непрерывны относительно соответствующих топологий, достаточно проверить коммутативность на элементах вида $f \otimes g \in H \hat{\otimes} H$, где $f, g \in H$. Но

$$\sigma(\mu(f \otimes g)) = \sigma(fg) = fg \circ F = (f \circ F)(g \circ F) = \\ = \mu \hat{\otimes} \mu (\sigma \hat{\otimes} \sigma (f \otimes g)),$$

что и требовалось доказать.

Множество U, наделенное законом умножения $\theta\colon U \otimes U \to U$ и диагональным отображением $\delta\colon U \to$

$\to U \otimes U$, называется *биалгеброй, ассоциированной с формальной группой* F.

Примем следующие обозначения:

$$\theta(u, v) = u * v$$

и

$$[u, v]_* = u * v - v * u.$$

Лемма 3. *Для любых* α *и* β *имеем*

$$\Delta^\alpha * \Delta^\beta = \binom{\alpha+\beta}{\alpha} \Delta^{\alpha+\beta} + E_{\alpha,\beta},$$

где остаточный член $E_{\alpha,\beta}$ *есть линейная комбинация элементов* Δ^γ, $0 < |\gamma| < |\alpha+\beta|$.

Доказательство. Требуется показать, что формы $\Delta^\alpha * \Delta^\beta$ и $\binom{\alpha+\beta}{\alpha}\Delta^{\alpha+\beta}$ принимают на элементах X^γ, $|\gamma| \geqslant |\alpha+\beta|$, одинаковые значения и что $E_{\alpha,\beta}$ обращается в нуль на k. Но

$$X^\gamma \circ F(Y, Z) = F(Y, Z)^\gamma = (Y+Z)^\gamma + o(d^0 \geqslant |\gamma|)$$

и

$$(Y+Z)^\gamma = \sum_{\lambda+\mu=\gamma} \binom{\gamma}{\lambda} Y^\lambda Z^\mu.$$

Так как

$$\Delta^\alpha * \Delta^\beta(X^\gamma) = \Delta_Y^\alpha \Delta_Z^\beta (X^\gamma \circ F(Y, Z)),$$

мы получаем

$$\Delta^\alpha * \Delta^\beta(X^\gamma) = \left\{ \begin{matrix} \binom{\alpha+\beta}{\alpha} & \text{при} \quad \alpha+\beta=\gamma \\ 0 & \text{в противном случае} \end{matrix} \right\} = \binom{\alpha+\beta}{\alpha} \Delta^{\alpha+\beta}(X^\gamma).$$

Итак, мы проверили совпадение элементов $\Delta^\alpha * \Delta^\beta$ и $\binom{\alpha+\beta}{\alpha}\Delta^{\alpha+\beta}$ на одночленах X^γ, где $|\gamma| \geqslant |\alpha+\beta|$. Заметим теперь, что оба эти элемента на X^0 равны 1, если $\alpha+\beta=0$, и равны нулю в противном случае, т. е. $E_{\alpha,\beta}$ обращается в нуль на k. Лемма доказана.

Пусть $\mathfrak{g}$ — алгебра Ли, ассоциированная с формальной группой F (см. § 1). Как векторное пространство алгебра $\mathfrak{g}$ совпадает с k^n. Обозначим через $\{D_i\}$, $1 \leqslant i \leqslant n$, стандартный базис пространства k^n. Определим отображение ψ: $\mathfrak{g} \to U$ формулой $\psi(D_i) = \Delta^{\delta_i}$. Из определения ясно, что ψ — линейный изоморфизм пространства $\mathfrak{g}$ на множество тех элементов $u \in U$, которые обращаются в нуль на k^n и $\mathfrak{m}^2$.

Лемма 4. *Пусть $x, y \in \mathfrak{g}$ и $f \in H$ — линейная функция. Тогда*

$$\psi([x, y])f = f(B(x, y) - B(y, x)).$$

Доказательство. Так как по определению $[x, y] = B(x, y) - B(y, x)$, нам нужно показать, что

$$\psi([x, y])f = f([x, y]).$$

Учитывая, что обе части этого равенства трилинейны по x, y и f, достаточно рассмотреть случай $x = D_i$, $y = D_j$, $f = X_k$. Но тогда как правая, так и левая части равны просто структурной константе $\gamma_{ij}^k(D_1, \ldots, D_n)$, что и завершает доказательство леммы.

Теорема 1. *Отображение ψ: $\mathfrak{g} \to U$ является гомоморфизмом алгебр Ли, т. е. $\psi([x, y]) = [\psi(x), \psi(y)]_*$.*

Доказательство. Нам известно, что $\psi([x, y])$ обращается в нуль на k и $\mathfrak{m}^2$. То же самое справедливо и для $[\psi(x), \psi(y)]_*$ (см. лемму 3). Остается, следовательно, показать, что $\psi([x, y])$ и $[\psi(x), \psi(y)]_*$ совпадают на множестве представителей смежных классов фактормодуля $\mathfrak{m}/\mathfrak{m}^2$, например на линейных функциях. Но для $f \in H$ имеем

$$\begin{aligned}[\psi(x), \psi(y)]_* f &= (\psi(x) \otimes \psi(y) - \psi(y) \otimes \psi(x))(f \circ F(X, Y)) = \\ &= (\psi(x) \otimes \psi(y) - \psi(y) \otimes \psi(x))(f \circ X + f \circ Y + \\ &\qquad + f \circ B(X, Y) + \ldots) = \\ &= (\psi(x) \otimes \psi(y) - \psi(y) \otimes \psi(x))(f \circ B(X, Y)) = \\ &= f(B(x, y) - B(y, x)).\end{aligned}$$

и теорема 6.1 вытекает из леммы 4.

Начиная с этого момента мы будем предполагать, что кольцо k является $\mathbf{Q}$-алгеброй.

Отображение ψ: $\mathfrak{g} \to U$ продолжается до гомоморфизма $U\mathfrak{g} \to U$ универсальной обертывающей алгебры (см. ч. I, гл. III, § 1); этот гомоморфизм мы для краткости обозначим той же буквой ψ.

Теорема 2. *Отображение* ψ: $U\mathfrak{g} \to U$ — *изоморфизм биалгебр.*

Доказательство. В алгебрах $U\mathfrak{g}$ (см. ч. I, гл. III, § 4) и U (§ 5, п. 2) определены фильтрации. Непосредственно проверяется, что гомоморфизм ψ согласован с этими фильтрациями и что относительно них алгебры $U\mathfrak{g}$ и U отделимы и полны. Следовательно (см. Бурбаки [2*], Ch. 3. § 2, п. 8), достаточно установить, что отображение $\mathrm{gr}(\psi)$ — изоморфизм.

По теореме Пуанкаре—Биркгофа—Витта (теорема 13.4.3) алгебра $U\mathfrak{g}$ — свободный k-модуль с базой $D^\alpha = D_1^{\alpha_1} \ldots D_n^{\alpha_n}$. Замечая, что k — алгебра над $\mathbf{Q}$, мы видим, что в качестве базиса алгебры U можно взять элементы $\overline{D}^\alpha = \frac{1}{\alpha!}\Delta^\alpha$. По лемме 2 $\psi(D^\alpha)$ и $\overline{D}^\alpha$ совпадают в $\mathrm{gr}(U)$, а потому $\mathrm{gr}(\psi)$ — изоморфизм.

Итак, установлено, что ψ — изоморфизм алгебр. Для того чтобы распространить это утверждение на биалгебры, нам надо проверить коммутативность следующей диаграммы:

$$\begin{tikzcd} U\mathfrak{g} \arrow[r, "\Delta"] \arrow[d, "\psi"'] & U\mathfrak{g} \otimes U\mathfrak{g} \arrow[d, "\psi\otimes\psi"] \\ U \arrow[r, "\delta"] & U \otimes U \end{tikzcd}$$

На основании предложения 1.3.5.2 леммы 5.3 и леммы 2 имеем

а) Δ и δ — гомоморфизмы алгебр;

б) для любого $u \in \mathfrak{g} \subset U\mathfrak{g}$

$$(\psi \otimes \psi)\Delta(u) = \psi(u) \otimes 1 + 1 \otimes \psi(u) = \delta \circ \psi(u).$$

Поскольку элементы из $\mathfrak{g}$ порождают $U\mathfrak{g}$ (предложение 1.3.4.1) равенство $\psi \circ \Delta = \delta \circ \psi$ выполняется для любых элементов алгебры $U\mathfrak{g}$. Теорема доказана.

Теорема 3. *Функтор* T: $(FG) \to (LA)$ *из категории формальных групп над* k *в категорию конечномерных* k*-алгебр Ли, определенный в* § 1, *задает эквивалентность этих категорий, т. е.*

(1) *отображение* $\mathrm{Hom}(F_1, F_2) \to \mathrm{Hom}(TF_1, TF_2)$ *биективно* ($F_1, F_2 \in (FG)$);

(2) *для любой алгебры Ли* $\mathfrak{g} \in (LA)$ *существует формальная группа* $F \in (FG)$, *такая, что алгебры* TF *и* $\mathfrak{g}$ *изоморфны.* (*Напомним, что* k *здесь* — $\mathbf{Q}$*-алгебра.*)

Доказательство. (1) Пусть F_1 и F_2 — формальные групповые законы от n_1 и n_2 переменных (над k) соответственно. Обозначим через H_i ($i = 1, 2$) кольцо формальных степенных рядов $k[[X_1, \ldots, X_{n_i}]]$, через U_i — биалгебру точечных распределений кольца H_i, через $\mathfrak{g}_i$ — алгебру Ли, ассоциированную с F_i, и через $\bar{U}_i$ — универсальную обертывающую алгебру алгебры $\mathfrak{g}_i$. Введем далее следующие обозначения для отображений:

а) μ_i: $H_i \widehat{\otimes} H_i \to H_i$
θ_i: $U_i \otimes U_i \to U_i$ законы умножения;
$\bar{\theta}_i$: $\bar{U}_i \otimes \bar{U}_i \to \bar{U}_i$

б) σ_i: $H_i \to H_i \widehat{\otimes} H_i$
δ_i: $U_i \to U_i \otimes U_i$ диагональные отображения;
$\bar{\delta}_i$: $\bar{U}_i \to \bar{U}_i \otimes \bar{U}_i$

в) ψ_i: $\bar{U}_i \to U_i$ — изоморфизм из теоремы 2.

Итак, для заданного гомоморфизма t: $\mathfrak{g} \to \mathfrak{g}$ мы должны найти соответствующий гомоморфизм формальных групп τ: $F_1 \to F_2$, такой, что $T(\tau) = t$, и доказать его единственность.

Покажем, что отображение

$$\mathrm{Hom}(F_1, F_2) \to \mathrm{Hom}(TF_1, TF_2)$$

разлагается в цепочку отображений, каждое из которых биективно. Мы сделаем это за шесть шагов.

Шаг 0. Начнем с предварительного шага. Пусть $\mathrm{Hom}_{AL}(H_2, H_1)$ — множество всех гомоморфизмов алгебр, переводящих $\mathfrak{m}_2$ в $\mathfrak{m}_1$ (такие гомоморфизмы мы будем называть *допустимыми*; они непрерывны отно-

сительно естественных топологий колец H_2 и H_1). Обозначим через S множество всех элементов $\tau = (\tau_1, \ldots, \tau_{n_2}) \in H_1^{n_2}$, у которых $\tau_i(0) = 0$ для всех i.

Каждый элемент $\tau \in S$ определяет отображение $\varphi_\tau : H_2 \to H_1$, $g \mapsto g \circ \tau$ $(g \in H_2)$. Нетрудно проверить (см. Бурбаки [3*], гл. IV, § 5, п. 5), что φ_τ — допустимый гомоморфизм алгебр.

Лемма 5. *Отображение* $\tau \mapsto \varphi_\tau$ *есть биекция множества* S *на* $\mathrm{Hom}_{AL}(H_2, H_1)$.

Доказательство. Указанное отображение, очевидно, инъективно, так как $\varphi_\tau(X_i) = \tau_i$. Докажем, что оно сюръективно. Рассмотрим элемент $\tau = (\tau_1, \ldots, \tau_n) \in S$, где $\tau_i = \varphi(X_i)$. Поскольку φ и φ_τ — гомоморфизмы алгебр, они совпадают на кольце $k[X_1, \ldots, X_{n_2}]$. Но тогда они совпадают и всюду, так как это кольцо плотно в H_2, а φ и φ_τ непрерывны.

Шаг 1. Пусть $\mathrm{Hom}_{BA}(H_2, H_1)$ — множество допустимых гомоморфизмов биалгебр.

Лемма 6. *Пусть* $\tau \in S$. *Тогда*

$$\tau \in \mathrm{Hom}_{FG}(F_1, F_2) \Leftrightarrow \varphi_\tau \in \mathrm{Hom}_{BA}(H_2, H_1) \quad (\tau \in S).$$

Доказательство. Ввиду леммы 5 включение $\varphi_\tau \in \mathrm{Hom}_{BA}(H_2, H_1)$ означает коммутативность следующей диаграммы:

$$\begin{tikzcd} H_2 \arrow[r, "\delta_2"] \arrow[d, "\varphi_\tau"'] & H_2 \otimes H_1 \arrow[d, "\varphi_\tau \otimes \varphi_\tau"] \\ H_1 \arrow[r, "\delta_1"] & H_1 \otimes H_1 \end{tikzcd}$$

Последняя имеет место тогда и только тогда, когда

$$g \circ \tau \circ F_1(X, Y) = \delta_1 \circ \varphi_\tau(g) = (\varphi_\tau \otimes \varphi_\tau) \circ \delta_2(g) = \\ = g \circ F_2(\tau X, \tau Y)$$

для всех $g \in H_2$. Это равенство в свою очередь равносильно соотношению

$$\tau \circ F_1(X, Y) = F_2(\tau X, \tau Y),$$

которое и выражает тот факт, что τ — гомоморфизм формальных групп.

Шаг 2. Пусть $\mathrm{Hom}_{BA}(U_1, U_2)$ и $\mathrm{Hom}_{BA}(\bar{U}_1, \bar{U}_2)$ — множества гомоморфизмов биалгебр.

Лемма 7. *Двойственность определяет изоморфизм*

$$\mathrm{Hom}_{BA}(H_2, H_1) \simeq \mathrm{Hom}_{BA}(U_1, U_2).$$

Доказательство. Пусть $\varphi: H_2 \to H_1$ — допустимый гомоморфизм биалгебр, и пусть $u \in U_1$. Отображение $u_1 \circ \varphi: H_2 \to k$ непрерывно, и, следовательно, $u_1 \circ \varphi \in U_2$. Итак, определено отображение $\mathrm{Hom}_{BA}(H_2, H_1) \to \mathrm{Hom}_{BA}(U_1, U_2)$.

Обратно, пусть $\psi: U_1 \to U_2$ — гомоморфизм биалгебр, и пусть $g \in H_2$. На основании леммы 5 (§ 5) $g \circ \psi \in H_1$. В силу двойственности отображение $g \mapsto g \circ \psi$ есть гомоморфизм биалгебр, поскольку таков гомоморфизм ψ. Далее, поскольку $\varphi(\varepsilon_1) = \varepsilon_2$, $g \in \mathfrak{m}_2 \Rightarrow g \circ \psi \in \mathfrak{m}_1$. Итак, $g \mapsto g \circ \psi$ — допустимый гомоморфизм биалгебр; тем самым определено отображение

$$\mathrm{Hom}_{BA}(U_1, U_2) \to \mathrm{Hom}_{BA}(H_2, H_1).$$

Построенные отображения, как легко проверить, взаимно обратны. Лемма доказана.

Шаг 3. Из теоремы 6.2 вытекает

Лемма 8. *Отображения* ψ_i $(i = 1, 2)$ *определяют изоморфизм*

$$\mathrm{Hom}_{BA}(U_1, U_2) \simeq \mathrm{Hom}(\bar{U}_1, \bar{U}_2).$$

Шаг 4. Из определения универсальной алгебры и теоремы 1.3.5.4 вытекает

Лемма 9. $\mathrm{Hom}_{BA}(\bar{U}_1, \bar{U}_2) = \mathrm{Hom}_{LA}(\mathfrak{g}_1, \mathfrak{g}_2)$.

Шаг 5. Нам осталось рассмотреть композицию биекций, фигурирующих в леммах 6, 7, 8, 9, и убедиться, что она совпадает с функтором T.

Пусть $\tau \in \mathrm{Hom}_{FG}(F_1, F_2)$. Запишем

$$\tau(X) = \sum_i t_i(X),$$

где $t_i(X)$ — однородная компонента степени i. Ясно, что $T(\tau) = t_1$. Пусть $t \in \mathrm{Hom}_{LA}(\mathfrak{g}_1, \mathfrak{g}_2)$ — элемент, соо-

тветствующий гомоморфизму τ при наших биекциях. Мы должны показать, что $t = t_1$.

Пусть $u \in \mathfrak{g}_1$. Для того чтобы проверить равенство $t(u) = t_1(u)$, достаточно показать, что $g(t(u)) = g(t_1(u))$, где $g \in H_2$ — линейная функция. Но

$$g(t(u)) = u(\varphi_\tau(g)) = u(g \circ \tau) = u\left(\sum_i g t_i\right) = u(g t_1),$$

$$g(t_1(u)) = u(g t_1).$$

Первая строка есть просто расшифровка изоморфизмов, определенных в леммах 6, 7, 8, 9; во второй строке мы воспользовались отождествлением алгебры $\mathfrak{g}_i$ с подмножеством в U_i (указанное отождествление задается отображением ψ_i). Сравнивая оба результата, получаем искомое равенство.

(2) Сопоставим алгебре Ли $\mathfrak{g} \in (LA)$ формальную группу с помощью формулы Кэмпбелла—Хаусдорфа. Все основные детали этого построения по существу приведены в первой части доказательства теоремы 4.1; там же было установлено, что алгебра Ли этой формальной группы совпадает с $\mathfrak{g}$. Хотя в той теореме кольцо k предполагалось полем нулевой характеристики, доказательство было полностью „формальным“ и использовало лишь тот факт, что k есть $\mathbf{Q}$-алгебра.

Теорема полностью доказана.

Замечание. Доказательство части (2) теоремы 3 можно было бы провести иначе, доказав вначале, что k-алгебра, двойственная к $U\mathfrak{g}$, изоморфна кольцу формальных степенных рядов $k[[X_1, \ldots, X_n]]$ ($n = \dim \mathfrak{g}$), а затем заметив, что диагональная структура алгебры $U\mathfrak{g}$ определяет в этом кольце искомый формальный групповой закон $F(X, Y)$.

§ 7. Сходимость формальных гомоморфизмов

Пусть снова k — поле, полное относительно нетривиального абсолютного значения, и $\operatorname{char} k = 0$.

Теорема 1. *Пусть G_1 и G_2 — локальные аналитические группы, F_1 и F_2 — формальные групповые*