БИБЛИОТЕКА СБОРНИКА
МАТЕМАТИКА

Ж.-П. СЕРР

Алгебры Ли и группы Ли

ИЗДАТЕЛЬСТВО
«МИР»

JEAN-PIERRE SERRE

LIE ALGEBRAS
AND
LIE GROUPS

LECTURES GIVEN AT HARVARD UNIVERSITY
NEW YORK – AMSTERDAM BENJAMIN, 1965

JEAN-PIERRE SERRE

ALGÈBRES DE LIE
SEMI-SIMPLES COMPLEXES

NEW YORK – AMSTERDAM, BENJAMIN, 1966

БИБЛИОТЕКА СБОРНИКА «МАТЕМАТИКА»

Ж.-П. СЕРР

Алгебры Ли и группы Ли

Перевод с английского и французского

А. Б. ВОЛЫНСКОГО

Под редакцией

А. Л. ОНИЩИКА

ИЗДАТЕЛЬСТВО «МИР»

МОСКВА 1969

УДК 512; 519.46

Книга известного французского математика, уже знакомого нашему читателю по переводам его книг „Алгебраические группы и поля классов“ и „Когомологии Галуа“ (изд-во „Мир“, 1968), содержит изложение основ теории алгебр Ли и групп Ли, а также теорию комплексных полупростых алгебр Ли. Наряду с классическим случаем вещественных и комплексных групп Ли она охватывает случай p-адических групп Ли и является единственной в мировой литературе книгой, содержащей подробное изложение теории p-групп с точки зрения классических методов теории групп Ли.

Книга рассчитана на студентов старших курсов и аспирантов. Может быть полезна математикам различных специальностей.

Редакция литературы по математическим наукам

Инд. 2-2-3
28-69

ОТ ИЗДАТЕЛЬСТВА

Здесь объединены переводы двух книг Ж.-П. Серра. Части I и II — это перевод (с английского) книги „Алгебры Ли и группы Ли“ (1965), которая представляет собой запись курса лекций, прочитанного Серром в Харвардском университете в 1964 г. Часть III — перевод (с французского) книги „Полупростые комплексные алгебры Ли“ (1966), представляющей собой запись курса лекций, прочитанного им в Алжире в 1965 г.

В связи с объединением двух книг в одну было сочтено целесообразным ввести единую систему ссылок на предыдущие теоремы и определения (например, „теорема 3.1.2.1“ — это теорема 1 из § 2, гл. I, ч. III). При ссылках на теорему той же части (главы, параграфа) номер части (главы, параграфа) опускается.

Часть I

Алгебры Ли

Здесь излагаются основные общие теоремы об алгебрах Ли в объеме примерно первой главы книги Бурбаки.

К этому я присовокупил некоторые результаты о свободных алгебрах Ли, полезные как в самой теории Ли (формула Кэмпбелла — Хаусдорфа), так и в приложениях к про-p-группам.

Недостаток времени не позволил включить сюда более развитую теорию полупростых алгебр Ли (корни, веса и т. д.); все-таки в последней главе разобран типичный случай алгебры $sl\ (n)$.

В работе над этой частью мне оказали помощь Ф. Рэгги и Дж. Тейт. Я хотел бы поблагодарить их, а также Сью Голэн, отпечатавшую обе части рукописи.

Ж.-П. С.

Харвард
осень 1964

Глава I

АЛГЕБРЫ ЛИ. ОПРЕДЕЛЕНИЯ И ПРИМЕРЫ

Пусть k — коммутативное кольцо с единицей и A — некоторый k-модуль. Мы будем называть этот модуль *k-алгеброй*, если задано k-билинейное отображение $A \times A \to A$ (т. е. k-гомоморфизм $A \otimes_k A \to A$).

Как обычно, определяются левые, правые, двусторонние идеалы и факторалгебры.

Определение 1. *Алгеброй Ли* над k называется k-алгебра A, обладающая следующими свойствами:

1) гомоморфизм $A \otimes_k A \to A$ допускает разложение

$$A \otimes_k A \to \overset{2}{\wedge} A \to A.$$

Иными словами, если обозначить образ пары (x, y) при этом гомоморфизме через $[x, y]$, то

$$[x, x] = 0 \text{ для всех } x \in A;$$

2) (тождество Якоби)

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0.$$

Заметим, что из условия 1) вытекает равенство $[x, y] = -[y, x]$.

Примеры. (i) Пусть k — поле, полное относительно некоторого нормирования, G — аналитическая группа над k и $\mathfrak{g}$ — множество касательных векторов к G в единице. Как будет показано ниже, на $\mathfrak{g}$ существует естественная структура алгебры Ли.

(Относительно алгебраического аналога этой ситуации см. пример (vi) ниже.)

(ii) Пусть $\mathfrak{g}$ — произвольный k-модуль, и пусть $[x, y]=0$ для всех $x, y \in \mathfrak{g}$. В этом случае $\mathfrak{g}$ называется *коммутативной* алгеброй Ли.

(iii) Пусть $\mathfrak{g}$ то же, что и в предыдущем примере. Рассмотрим модуль $\mathfrak{g} \oplus \overset{2}{\wedge} \mathfrak{g}$ и положим

$$\begin{gathered}[x, y]=x \wedge y, \\ [x, y \wedge z]=0, \\ [x \wedge y, z]=0, \\ [x \wedge y, z \wedge t]=0\end{gathered}$$

для любых $x, y, z, t \in \mathfrak{g}$. Модуль $\mathfrak{g} \oplus \overset{2}{\wedge} \mathfrak{g}$ с такой операцией есть алгебра Ли.

(iv) Пусть A — ассоциативная алгебра над k. Положим $[x, y]=xy-yx$. Очевидно, что алгебра A с таким умножением удовлетворяет аксиомам 1) и 2).

Определение 2. Пусть A — алгебра над k. *Дифференцированием* $D\colon A \to A$ называется k-линейное отображение, для которого

$$D(x \cdot y)=Dx \cdot y+x \cdot Dy.$$

(v) Множество $\operatorname{Der}(A)$ всех дифференцирований алгебры A является алгеброй Ли с операцией $[D, D']=DD'-D'D$.

Тот факт, что $[D,D']$ есть дифференцирование, доказывается прямым вычислением:

$$\begin{aligned}
&[D,D'](x \cdot y)=DD'(x \cdot y)-D'D(x \cdot y)= \\
&=D(D'x \cdot y+x \cdot D'y)-D'(Dx \cdot y+x \cdot Dy)= \\
&=DD'x \cdot y+D'x \cdot Dy+Dx \cdot D'y+x \cdot DD'y- \\
&-D'Dx \cdot y-Dx \cdot D'y-D'x \cdot Dy-x \cdot D'Dy= \\
&=DD'x \cdot y+x \cdot DD'y-DD'x \cdot y-x \cdot D'Dy= \\
&=[D, D']x \cdot y+x \cdot [D, D']y.
\end{aligned}$$

Теорема 3. *Пусть $\mathfrak{g}$ — алгебра Ли. Для каждого $x \in \mathfrak{g}$ определим отображение* $\operatorname{ad} x\colon \mathfrak{g} \to \mathfrak{g}$ *формулой* $\operatorname{ad} x(y)=[x, y]$. *Тогда*

(1) *отображение* $\operatorname{ad} x$ *есть дифференцирование алгебры* $\mathfrak{g}$;

(2) *отображение* $x \mapsto \operatorname{ad} x$ *есть гомоморфизм алгебры Ли* $\mathfrak{g}$ *в алгебру Ли* $\operatorname{Der}(\mathfrak{g})$.

Доказательство.

$$\operatorname{ad} x([y, z]) = [x, [y, z]] = -[y,[z, x]] - [z, [x, y]] = \\ = [[x, y], z] + [y, [x, z]] = [\operatorname{ad} x(y), z] + [y, \operatorname{ad} x(z)].$$

Таким образом, утверждение (1) эквивалентно тождеству Якоби.

Далее,

$$\operatorname{ad}[x,y](z) = [[x, y], z] = -[[y, z], x] - [[z, x], y] = \\ = [x,[y, z]] - [y, [x, z]] = \operatorname{ad} x \operatorname{ad} y(z) - \operatorname{ad} y \operatorname{ad} x(z) = \\ = [\operatorname{ad} x, \operatorname{ad} y](z).$$

Следовательно, утверждение (2) также эквивалентно тождеству Якоби.

(vi) *Алгебра Ли алгебраической матричной группы.* Пусть k — коммутативное кольцо с единицей и $A = M(n,k)$ — алгебра квадратных матриц порядка n над k. *Нулем* системы многочленов $\{P_\alpha(X_{ij})\}$ (с коэффициентами в k) называется матрица $X = (x_{ij})$, такая, что $x_{ij} \in k$ и $P_\alpha(x_{ij}) = 0$ для всех α. Обозначим через $G(k)$ множество всех нулей данной системы $\{P_\alpha\}$. Аналогичным образом для любой ассоциативной коммутативной k-алгебры k' с единицей рассмотрим множество $G(k') \subset M(n, k')$.

Определение 4. Мы скажем, что система $\{P_\alpha\}$ определяет *алгебраическую группу* над k, если для любой ассоциативной коммутативной k-алгебры k' с единицей $G(k')$ есть подгруппа в $GL(n, k')$[1]).

Примером алгебраической группы может служить *ортонормальная группа* (определяющее уравнение: ${}^tX \cdot X = 1$, где ${}^tX$ — матрица, транспонированная к X).

---

[1]) Через $GL(n, k')$, как обычно, обозначается множество всех матриц из $M(n, k')$, определитель которых есть *обратимый* элемент в k'. — *Прим. перев.*

Пусть, далее, k' — свободная (как k-модуль) алгебра над k с базисом $\{1, \varepsilon\}$, где $\varepsilon^2 = 0$, т. е. $k' = k[\varepsilon]$.

Теорема 5. *Пусть* $\mathfrak{g}$ — *совокупность всех матриц* $X \in M(n, k)$, *таких, что* $1 + \varepsilon X \in G(k[\varepsilon])$. *Тогда* $\mathfrak{g}$ *является подалгеброй Ли алгебры* $M(n, k)$.

Доказательство. Мы должны установить, что включение $X, Y \in \mathfrak{g}$ влечет включение $\lambda X + \mu Y \in \mathfrak{g}$, где $\lambda, \mu \in k$ и $XY - YX \in \mathfrak{g}$. Заметим сначала, что по определению условие $P_\alpha(1 + \varepsilon X) = 0$ для всех α означает, что $X \in \mathfrak{g}$. Так как $\varepsilon^2 = 0$, мы имеем $P_\alpha(1 + \varepsilon X) = P_\alpha(1) + dP_\alpha(1)\varepsilon X$[1]. Но $1 \in G(k)$, так что $P_\alpha(1) = 0$. Следовательно,

$$P_\alpha(1 + \varepsilon X) = dP_\alpha(1)\varepsilon X,$$

что доказывает первое утверждение.

Введем теперь вспомогательную алгебру $k'' = k[\varepsilon, \varepsilon', \varepsilon \cdot \varepsilon']$, где $\varepsilon^2 = \varepsilon'^2 = 0$ и $\varepsilon\varepsilon' = \varepsilon'\varepsilon$; другими словами, $k'' = k[\varepsilon] \otimes_k k[\varepsilon']$. Пусть $X, Y \in \mathfrak{g}$. Тогда

$$\begin{aligned} g &= 1 + \varepsilon X \in G(k[\varepsilon]) \subset G(k''), \\ g' &= 1 + \varepsilon' Y \in G(k[\varepsilon']) \subset G(k''), \\ gg' &= (1 + \varepsilon X)(1 + \varepsilon' Y) = 1 + \varepsilon X + \varepsilon' Y + \varepsilon\varepsilon' XY, \\ g'g &= 1 + \varepsilon X + \varepsilon' Y + \varepsilon\varepsilon' YX. \end{aligned}$$

Если положить $Z = [X, Y]$, то в силу написанных выше формул будет иметь место равенство $gg' = g'g(1 + \varepsilon\varepsilon' Z)$.

Поскольку $gg', g'g \in G(k'')$, отсюда вытекает, что

$$1 + \varepsilon\varepsilon' Z \in G(k'').$$

Но подалгебра $k[\varepsilon\varepsilon']$ алгебры k'' изоморфна $k[\varepsilon]$ [над k], поэтому $1 + \varepsilon Z \in G(k[\varepsilon])$ и, следовательно, $Z \in \mathfrak{g}$, что и требовалось доказать.

---

[1]) Символ $dP_\alpha(1)X$ есть сокращенное обозначение выражения $\sum\limits_{i,j} \frac{\partial P_\alpha}{\partial X_{ij}}(1)\, x_{ij}$. — *Прим. перев.*

Пример. Алгебра Ли ортонормальной группы есть множество всех матриц X, для которых $(1+\varepsilon X)\times\times(1+\varepsilon\,{}^tX)=1$, т. е. $X+{}^tX=0$.

(vii) *Построение новых алгебр Ли, исходя из заданных алгебр.*

а) Пусть $\mathfrak{g}$ — алгебра Ли и $\mathfrak{a}$ — ее идеал. Фактор-алгебра $\mathfrak{g}/\mathfrak{a}$ является алгеброй Ли.

б) Пусть $\{\mathfrak{g}_i\}_{i\in I}$ — семейство алгебр Ли. Прямое произведение $\prod\limits_{i\in I}\mathfrak{g}_i$ есть также алгебра Ли.

в) Предположим, что $\mathfrak{g}$ — алгебра Ли, $\mathfrak{a}$ — ее идеал и $\mathfrak{b}$ — ее подалгебра. Мы будем говорить, что $\mathfrak{g}$ — *полупрямое произведение* $\mathfrak{b}$ и $\mathfrak{a}$, если каноническое отображение $\mathfrak{g}\to\mathfrak{g}/\mathfrak{a}$ индуцирует изоморфизм $\mathfrak{b}\xrightarrow{\sim}\mathfrak{g}/\mathfrak{a}$ [1]). Пусть $\mathfrak{g}$ — полупрямое произведение $\mathfrak{b}$ и $\mathfrak{a}$. Поскольку $\mathfrak{a}$ — идеал, постольку для любого $x\in\mathfrak{b}$ отображение $\operatorname{ad}x$ переводит $\mathfrak{a}$ в себя, т. е. ограничение $\operatorname{ad}x$ на $\mathfrak{a}$ является дифференцированием $\mathfrak{a}$. Таким образом, имеется гомоморфизм алгебр Ли $\theta\colon \mathfrak{b}\to\operatorname{Der}(\mathfrak{a})$.

Теорема 6. *Структура алгебры Ли* $\mathfrak{g}$ *однозначно определяется заданием* $\mathfrak{a}$, $\mathfrak{b}$ *и* θ, *причем их можно задавать произвольно.*

Доказательство. Поскольку $\mathfrak{g}$ есть прямая сумма $\mathfrak{a}$ и $\mathfrak{b}$ (как k-модулей) и поскольку умножение в $\mathfrak{g}$ билинейно и антикоммутативно, достаточно рассмотреть произведение $[x, y]$ для следующих трех случаев:

$$x,\ y\in\mathfrak{a},$$
$$x,\ y\in\mathfrak{b},$$
$$x\in\mathfrak{b},\quad y\in\mathfrak{a}.$$

В первом случае произведение $[x, y]$ есть произведение в $\mathfrak{a}$, во втором — в $\mathfrak{b}$, а в последнем случае

$$[x, y]=\operatorname{ad}x(y)=\theta(x)(y).$$

Обратно, пусть даны алгебры Ли $\mathfrak{a}$ и $\mathfrak{b}$ и гомоморфизм Ли $\theta\colon \mathfrak{b}\to\operatorname{Der}(\mathfrak{a})$. С помощью приведенной

[1]) Иными словами, $\mathfrak{g}$ есть прямая сумма $\mathfrak{a}$ и $\mathfrak{b}$ как k-модулей. — *Прим. перев.*

выше формулы мы можем построить алгебру $\mathfrak{g}$ на прямой сумме модулей $\mathfrak{a}$ и $\mathfrak{b}$ так, чтобы $\theta(x) = \mathrm{ad}_{\mathfrak{a}}\, x$, где $\mathrm{ad}_{\mathfrak{a}}\, x$ — ограничение $\mathrm{ad}_{\mathfrak{g}}\, x$ на $\mathfrak{a}$, для $x \in \mathfrak{b}$. Нам остается только проверить, что относительно введенной операции в $\mathfrak{g}$ имеет место тождество Якоби:

$$J(x, y, z) = [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

Это достаточно сделать в следующих четырех случаях:

а) $x, y, z \in \mathfrak{a}$; тогда $J(x, y, z) = 0$, поскольку $\mathfrak{a}$ — алгебра Ли;

б) $x, y \in \mathfrak{a}$ и $z \in \mathfrak{b}$; в этом случае $J(x, y, z) = 0 \Leftrightarrow \theta(z)$ — дифференцирование в $\mathfrak{a}$;

в) $x \in \mathfrak{a}$, $y, z \in \mathfrak{b}$; в данном случае

$$J(x, y, z) = 0 \Leftrightarrow \theta([y, z]) = \theta(y)\,\theta(z) - \theta(z)\,\theta(y);$$

г) $x, y, z \in \mathfrak{b}$; тогда $J(x, y, z) = 0$, поскольку $\mathfrak{b}$ — алгебра Ли.

Глава II

ФИЛЬТРОВАННЫЕ ГРУППЫ И АЛГЕБРЫ ЛИ

§ 1. Тождества с коммутаторами

Пусть G — группа и x, y, $z \in G$. Мы примем следующие обозначения:

(i) $x^y = y^{-1}xy$; тогда отображение $G \to G$, задаваемое правилом $x \mapsto x^y$, есть автоморфизм группы G, и выполняется соотношение $(x^y)^z = x^{yz}$;

(ii) $(x, y) = x^{-1}y^{-1}xy$; мы будем называть (x, y) *коммутатором* элементов x и y.

Предложение 1. *Имеют место следующие тождества*:

1) $xy = yx^y = yx(x, y)$, $x^y = x(x, y)$, $(x, x) = 1$ $(y, x) = (x \cdot y)^{-1}$;

2) $(x, yz) = (x, z)(x, y)^z$;

2′) $(xy, z) = (x, z)^y (y, z)$;

3) $(x^y, (y, z))(y^z, (z, x))(z^x, (x, y)) = 1$.

Доказательство. 1) Очевидно.

2) В силу (i) и 1) имеем

$$x(x, yz) = x^{yz} = (x^y)^z = [x, (x, y)]^z = \\ = x^z (x, y)^z = x(x, z)(x, y)^z,$$

откуда

$$(x, yz) = (x, z)(x, y)^z.$$

2′) $$xy(xy, z) = (xy)^z = x^z y^z = x(x, z)y(y, z) = \\ = xy(x, z)^y (y, z),$$

откуда

$$(xy, z) = (x, z)^y (y, z).$$

3) $$(x^y, (y, z)) = (y^{-1}x^{-1}yz^{-1}y^{-1}zyy^{-1}xyy^{-1}z^{-1}yz = \\ = y^{-1}x^{-1}yz^{-1}y^{-1}zxz^{-1}yz.$$

Положим $u = zxz^{-1}yz$, $v = xyx^{-1}zx$, $w = yzy^{-1}xy$. Тогда $(x^y, (y, z)) = w^{-1}u$.

Аналогично (циклическая перестановка)

$$(y^z, (z, x)) = u^{-1}v,$$
$$(z^x, (x, y)) = v^{-1}w,$$

и, следовательно,

$$(x^y, (y, z))(y^z, (z, x))(z^x, (x, y)) = 1, \text{ ч. т. д.}$$

В качестве приложения доказанных тождеств получаем следующее утверждение.

Пусть A и B — подгруппы группы G. Обозначим через (A, B) подгруппу в G, порожденную элементами вида (a, b), где $a \in A$ и $b \in B$. Если A, B, C — нормальные подгруппы в G, то (A, B) также является нормальной подгруппой, и имеет место включение

$$(A, (B, C)) \subset (B, (C, A))(C, (A, B)).$$

Это вытекает из тождества 3).

§ 2. Фильтрация на группе

Определение 1. *Фильтрацией* на группе G называется отображение $w\colon G \to \mathbf{R} \cup \{+\infty\}$, удовлетворяющее следующим аксиомам:

(1) $w(1) = +\infty$;
(2) $w(x) > 0$ для всех $x \in G$;
(3) $w(xy^{-1}) \geqslant \inf(w(x), w(y))$;
(4) $w((x, y)) \geqslant w(x) + w(y)$.

Из аксиомы (3) вытекает, что $w(y^{-1}) = w(y)$. Для $\lambda \in \mathbf{R}_+$ положим

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

Очевидно, G_λ и G_λ^+ являются подгруппами группы G. Более того, если $x \in G_\lambda$ и $y \in G$, то $x^y \equiv x \pmod{G_\lambda^+}$. Действительно,

$$w((x, y)) \geqslant \lambda + w(y) > \lambda.$$

Сказанное выше означает, что G_λ — нормальная подгруппа G, а поскольку $G_\lambda^+ = \bigcup\limits_{\mu > \lambda} G_\mu$, группа G_λ^+ — тоже нормальная подгруппа в G.

Семейство $\{G_\lambda\}$ (соответственно $\{G_\lambda^+\}$) является убывающим, т. е. $G_\lambda \supset G_\mu$ (соответственно $G_\lambda^+ \supset G_\mu^+$) при $\lambda < \mu$.

Определение 2. Для каждого $\alpha \geqslant 0$ положим $\mathrm{gr}_\alpha G = G_\alpha / G_\alpha^+$ и $\mathrm{gr}\, G = \sum\limits_\alpha \mathrm{gr}_\alpha G$. Будем называть $\mathrm{gr}\, G$ *присоединенной группой* группы G.

Предложение 3. 1) *Группа* $\mathrm{gr}_\alpha G$ *абелева.*

2) *Если для каждого* $x \in G_\alpha$ *обозначить через* $\bar{x}$ *соответствующий элемент в* $\mathrm{gr}_\alpha G$, *то* $\overline{(x^y)} = \bar{x}$ *для всех* $y \in G$.

3) *Отображение* $c_{\alpha\beta}$: $G_\alpha \times G_\beta \to G_{\alpha+\beta}$, *определенное правилом* $x, y \mapsto (x, y)$, *индуцирует билинейное отображение* $c_{\alpha\beta}'$: $\mathrm{gr}_\alpha G \times \mathrm{gr}_\beta G \to \mathrm{gr}\, G_{\alpha+\beta}$.

4) *Отображения* $c_{\alpha\beta}$ *могут быть продолжены по линейности до отображения* c: $\mathrm{gr}\, G \times \mathrm{gr}\, G \to \mathrm{gr}\, G$, *и это отображение задает структуру алгебры Ли на* $\mathrm{gr}\, G$.

Доказательство. 1) Это утверждение вытекает из определения 1, (4).

2) Это было доказано выше.

3) Пусть $x \in G_\alpha$ и $y \in G_\beta$. Тогда $(x, y) \in G_{\alpha+\beta}$, и мы должны показать, что $(xu, y) \equiv (x, y) \pmod{G_{\alpha+\beta}^+}$ и $(x, yv) \equiv (x, y) \pmod{G_{\alpha+\beta}^+}$ для любых $u \in G_\alpha^+$ и $v \in G_\beta^+$. В силу 1.1, 2′) и в силу (3) имеем

$$\overline{(xu, y)} = \overline{(x, y)^u} + \overline{(u, y)} = \overline{(x, y)},$$
$$\overline{(x, yv)} = \overline{(x, v)} + \overline{(x, y)^v} = \overline{(x, y)}.$$

Пусть $x, x' \in G_\alpha$ и $y, y' \in G_\beta$. Тогда

$$\overline{(xx', y)} = \overline{(x, y)^{x'}} + \overline{(x', y)} = \overline{(x, y)} + \overline{(x', y)},$$
$$\overline{(x, y'y)} = \overline{(x, y)} + \overline{(x, y')^y} = \overline{(x, y)} + \overline{(x, y')}.$$

4) Пусть $\xi \in \mathrm{gr}_\alpha G$ и $\eta \in \mathrm{gr}_\beta G$. Выберем элементы $x \in G_\alpha$ и $y \in G_\beta$, такие, что $\bar{x} = \xi$ и $\bar{y} = \eta$. Тогда по определению $\overline{(x, y)} = \bar{c}_{\alpha, \beta}(\xi, \eta)$; мы будем записывать это выражение также в виде $[\xi, \eta]$. Далее, если $\xi \in \mathrm{gr}\, G$, то $\xi = \sum \xi_\alpha$, где $\xi_\alpha \in \mathrm{gr}_\alpha G$. Доказать равенство $[\xi, \xi] = 0$ — это значит установить, что $[\xi_\alpha, \xi_\alpha] = 0$ и $[\xi_\alpha, \xi_\beta] = -[\xi_\beta, \xi_\alpha]$. Для каждого α выберем $x_\alpha \in G_\alpha$, такое, что $\bar{x}_\alpha = \xi_\alpha$. Имеем

$$[\xi_\alpha, \xi_\alpha] = \overline{(x_\alpha, x_\alpha)} = \bar{1} = 0$$

и

$$[\xi_\alpha, \xi_\beta] = \overline{(x_\alpha, x_\beta)} = \overline{(x_\beta, x_\alpha)^{-1}} = -[\xi_\beta, \xi_\alpha].$$

При доказательстве тождества Якоби $J(x, y, z) = 0$ можно (ввиду линейности J по каждому аргументу) ограничиться случаем $\xi \in \mathrm{gr}_\alpha G$, $\eta \in \mathrm{gr}_\beta G$ и $\zeta \in \mathrm{gr}_\gamma G$. Выберем $x \in G_\alpha$, $y \in G_\beta$ и $z \in G_\gamma$, такие, что $\bar{x} = \xi$, $\bar{y} = \eta$ и $\bar{z} = \xi$. Тогда в силу предложения 1.1, 3),

$$J(\xi, \eta, \zeta) = \overline{(x^y, (y, z))(y^z, (z, x))(z^x, (x, y))} = \bar{1} = 0,$$

поскольку $\overline{x^y} = \xi$, $\overline{y^x} = \eta$ и $\overline{z^x} = \zeta$.

§ 3. Дискретные фильтрации группы

Предложение 1. *Для всякой группы G существует взаимно однозначное соответствие между*

1) *фильтрациями группы w: $G \to \mathbf{R} \cup \{+\infty\}$, такими, что $w(G) \subset \mathbf{N} \cup \{+\infty\}$,*

2) *убывающими последовательностями $\{G_n\}_{n \in \mathbf{N}}$ подгрупп группы G, такими, что*

(i) $G_1 = G$,

(ii) $(G_n, G_m) \subset G_{n+m}$.

Доказательство. По каждой дискретной фильтрации очевидным образом восстанавливается семейство подгрупп $\{G_n\}_{n \in \mathbf{N}}$ со свойствами (i) и (ii).

Обратно, пусть задано такое семейство. Определим фильтрацию w: $G \to \mathbf{R} \cup \{+\infty\}$, полагая для каждого $x \in G$

$$w(x) = \sup_{x \in G_n} \{n\}.$$

Ясно, что $w(1) = +\infty$ и $w(x) > 0$ для всех $x \in G$, а также что $w(x) = w(x^{-1})$. Пусть теперь $w(x) = n$, $w(y) = m$, т. е. $x \in G_n$, $y \in G_m$, но $x \notin G_{n+1}$ и $y \notin G_{m+1}$. Допустим, что $n \leqslant m$. Тогда $G_m \subset G_n$, и, следовательно, $xy^{-1} \in G_n$, т. е.

$$w(x y^{-1}) \geqslant \inf \{w(x), w(y)\}.$$

В случае $n = +\infty$ или $m = +\infty$ это неравенство очевидно.

Наконец, неравенство $w((x, y)) \geqslant w(x) + w(y)$ непосредственно вытекает из (ii), ч. т. д.

Пример. *Убывающий центральный ряд группы G.* Положим $G_1 = G$ и определим по индукции G_{n+1} формулой

$$G_{n+1} = (G, G_n).$$

Полученная последовательность подгрупп $\{G_n\}$ удовлетворяет условиям (i) и (ii) предложения 1. Действительно, (i) имеет место по условию. Чтобы доказать (ii), применим индукцию по n.

При $n = 1$ имеем $(G, G_m) \subset G_{m+1}$ по определению. При $n > 1$

$$\begin{aligned}(G_n, G_m) = ((G, G_{n-1}), G_m) &\subset \\ \subset (G, (G_{n-1}, G_m))(G_{n-1}, (G, G_m)) &\subset \\ \subset (G, G_{n+m-1})(G_{n-1}, G_{m+1}) &\subset G_{n+m}G_{n+m} \subset G_{n+m}.\end{aligned}$$

Обратно, если $\{H_n\}$ — убывающая последовательность подгрупп группы G, удовлетворяющая условиям (i) и (ii), то $H_n \supset G_n$ для каждого n. Доказывается это также по индукции. При $n = 1$ по определению $H_1 \supset G_1$, а при $n > 1$ имеют место включения

$$H_{n+1} \supset (H, H_n) \supset (G, G_n) = G_{n+1}.$$

§ 4. Фильтрации группы $GL(n)$

Пусть k — некоторое поле с неархимедовым абсолютным значением $|x| = \rho^{v(x)}$ [1]. Пусть A_v — кольцо нормирования v, $\mathfrak{m}_v$ — его идеал и $k_v = A_v/\mathfrak{m}_v$.

Для всякого натурального числа n обозначим через G множество всех квадратных матриц g порядка n с коэффициентами в A_v, таких, что $g \equiv 1 \pmod{\mathfrak{m}_v}$ (т. е. $g_{ij} \equiv \delta_{ij} \pmod{\mathfrak{m}_v}$, где $g = (g_{ij})$). Таким образом, если $g \in G$, то $g = 1 + x$, где x — матрица с коэффициентами в $\mathfrak{m}_v$. Ясно, что множество G является группой, поскольку G есть ядро гомоморфизма

$$GL(n, A_v) \to GL(n, k_v).$$

Для каждой матрицы $X \in M(n, k)$, $X = (x_{ij})$, положим $v(X) = \inf\{v(x_{ij})\}$ и определим отображение $w\colon G \to \mathbf{R} \cup \{+\infty\}$ равенством $w(g) = v(x)$, где $g = 1 + x$.

Теорема 1. *Отображение w является фильтрацией группы G.*

Доказательство. Соотношения $w(1) = +\infty$ и $w(g) > 0$ для всех $g \in G$ очевидны.

Пусть $G_\lambda = \{g \in G \mid w(g) \geqslant \lambda\}$. Рассмотрим для каждого $\lambda > 0$ идеал $\mathfrak{a}_\lambda$ в кольце A_v:

$$\mathfrak{a}_\lambda = \{x \in k \mid v(x) \geqslant \lambda\}.$$

Понятно, что G_λ есть ядро канонического гомоморфизма

$$GL(n, A_v) \to GL(n, A_v/\mathfrak{a}_\lambda).$$

Следовательно, G_λ — подгруппа в G, и, значит, условие (3) выполнено.

Для проверки условия (4), т. е. включения $(G_\lambda, G_\mu) \subset G_{\lambda+\mu}$, запишем элементы $g \in G_\lambda$ и $h \in G_\mu$ в следующем виде:

$$g = 1 + x \quad \text{и} \quad h = 1 + y.$$

[1] См. ч. II, гл. I. — *Прим. перев.*

Мы должны показать, что $hg \equiv gh \pmod{G_{\lambda+\mu}}$. Но

$$hg = 1 + x + y + yx,$$
$$gh = 1 + x + y + xy,$$

причем коэффициенты матриц xy и yx лежат в $\mathfrak{a}_{\lambda+\mu}$. Элементы hg и gh имеют поэтому один и тот же образ в группе $GL(n, A_v/\mathfrak{a}_{\lambda+\mu})$, что и означает их сравнимость по модулю $G_{\lambda+\mu}$.

УПРАЖНЕНИЯ

1. Описать алгебру Ли группы $\operatorname{gr} G$.

2. Доказать, что $G = \varprojlim G/G_\lambda$, если k — полное поле[1]).

[1]) То есть k является полным метрическим пространством относительно своей метрики $|x| = \rho^{v(x)}$. — *Прим. перев.*

Глава III

УНИВЕРСАЛЬНАЯ ОБЕРТЫВАЮЩАЯ АЛГЕБРА

§ 1. Определение и построение универсальной обертывающей алгебры

Пусть k — коммутативное кольцо с единицей и $\mathfrak{g}$ — алгебра Ли над кольцом k.

Определение 1. Назовем *универсальной обертывающей алгеброй* алгебры $\mathfrak{g}$ отображение $\varepsilon: \mathfrak{g} \to U\mathfrak{g}$, где $U\mathfrak{g}$ — ассоциативная k-алгебра с единицей, обладающее следующими свойствами:

1) ε есть гомоморфизм алгебр Ли (т. е. ε k-линейно и $\varepsilon([x, y]) = \varepsilon x \cdot \varepsilon y - \varepsilon y \cdot \varepsilon x$);

2) для всякой ассоциативной алгебры A с единицей и для всякого гомоморфизма алгебр Ли $\alpha: \mathfrak{g} \to A$ существует единственный гомоморфизм ассоциативных алгебр $\varphi: U\mathfrak{g} \to A$, такой, что диаграмма

$$\begin{tikzcd} \mathfrak{g} \arrow[r, "\varepsilon"] \arrow[d, "\alpha"'] & U\mathfrak{g} \arrow[dl, "\varphi"] \\ A & \end{tikzcd}$$

коммутативна. (Иными словами, имеет место изоморфизм

$$\mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g}, LA) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Ass}}(U\mathfrak{g}, A),$$

где LA обозначает алгебру Ли, ассоциированную с A, см. гл. I, пример (iv).)

То, что алгебра $U\mathfrak{g}$, если она существует, определяется единственным образом с точностью до изоморфизма, очевидно. Для доказательства ее существования рассмотрим *тензорную алгебру* $T\mathfrak{g}$ над $\mathfrak{g}$. Напомним, что $T\mathfrak{g} = \sum_{n=0}^{\infty} T^n\mathfrak{g}$, где $T^0\mathfrak{g} = k$ и $T^n\mathfrak{g} = \mathfrak{g} \otimes \ldots \otimes \mathfrak{g} = \overset{n}{\otimes}\mathfrak{g}$ при

$n>0$. Для любой ассоциативной алгебры A с единицей имеет место канонический изоморфизм

$$\mathrm{Hom}_{\mathrm{Mod}}(\mathfrak{g}, A) \simeq \mathrm{Hom}_{\mathrm{Ass}}(T\mathfrak{g}, A).$$

Обозначим через I двусторонний идеал в $T\mathfrak{g}$, порожденный элементами вида $[x, y] - x \otimes y + y \otimes x$, $x, y \in \mathfrak{g}$, и положим $U\mathfrak{g} = T\mathfrak{g}/I$.

Теорема 2. *Пусть* ε: $\mathfrak{g} \to U\mathfrak{g}$ — *композиция отображений* $\mathfrak{g} \to T^1\mathfrak{g} \to T\mathfrak{g} \to U\mathfrak{g}$. *Тогда пара* $(U\mathfrak{g}, \varepsilon)$ *является универсальной обертывающей алгеброй для* $\mathfrak{g}$.

Доказательство. В самом деле, пусть задан некоторый гомоморфизм α алгебры $\mathfrak{g}$ в ассоциативную алгебру A. Так как α линейно над k, это отображение продолжается до гомоморфизма ψ: $T\mathfrak{g} \to A$. При этом ясно, что $\psi(I) = 0$, а потому ψ определяет отображение φ: $U\mathfrak{g} \to A$. Тем самым свойство универсальности алгебры $U\mathfrak{g}$ доказано, поскольку φ восстанавливается по α единственным образом.

Замечание. Пусть E — некоторый $\mathfrak{g}$-модуль (т. е. k-модуль, снабженный билинейным отображением $\mathfrak{g} \times E \to E$, таким, что $[x, y]e = x(ye) - y(xe)$, где $x, y \in \mathfrak{g}$ и $e \in E$). Отображение $\mathfrak{g} \to \mathrm{End}(E, E)$, определяющее на E структуру $\mathfrak{g}$-модуля, является гомоморфизмом алгебр Ли, поэтому оно продолжается до гомоморфизма ассоциативных алгебр $U\mathfrak{g} \to \mathrm{End}(E, E)$, так что E становится *левым* $U\mathfrak{g}$-*модулем*. Легко понять, что таким образом мы получаем *изоморфизм* категории $\mathfrak{g}$-модулей на категорию левых $U\mathfrak{g}$-модулей.

Упражнение (Бергман). Доказать, что $U\mathfrak{g} = k$ тогда и только тогда, когда $\mathfrak{g} = 0$. [*Указание*: использовать присоединенное представление.]

§ 2. Функториальные свойства

1) *Если* $\mathfrak{g} = \varinjlim \mathfrak{g}_a$, *то* $U\mathfrak{g} = \varinjlim U\mathfrak{g}_a$.

2) *Пусть* $\mathfrak{g} = \mathfrak{g}_1 \times \mathfrak{g}_2$ — *прямое произведение алгебр Ли* (*т. е.* $\mathfrak{g}_1$ *и* $\mathfrak{g}_2$ *коммутируют в* $\mathfrak{g}$). *Тогда* $U\mathfrak{g} = U\mathfrak{g}_1 \otimes_k U\mathfrak{g}_2$.

3) *Пусть k' — расширение поля k (т. е. k' — коммутативная ассоциативная k-алгебра с единицей), и пусть $\mathfrak{g}' = \mathfrak{g} \otimes_k k'$. Тогда $U\mathfrak{g}' = U\mathfrak{g} \otimes_k k'$.*

Доказательство свойства 2). Нам заданы гомоморфизмы ε_i: $\mathfrak{g}_i \to U\mathfrak{g}_i$, $i = 1, 2$. Рассмотрим отображение f: $\mathfrak{g} \to U\mathfrak{g}_1 \otimes_k U\mathfrak{g}_2$, задаваемое формулой

$$f(x) = \varepsilon_1(x_1) \otimes 1 + 1 \otimes \varepsilon_2(x_2),$$

где $x = x_1 + x_2$ и $x_1 \in \mathfrak{g}_1$, $x_2 \in \mathfrak{g}_2$. Отображение f есть гомоморфизм алгебр Ли, поскольку $\mathfrak{g}_1$ и $\mathfrak{g}_2$ коммутируют в $\mathfrak{g}$. Следовательно, f индуцирует гомоморфизм ассоциативных алгебр ψ: $U\mathfrak{g} \to U\mathfrak{g}_1 \otimes_k U\mathfrak{g}_2$.

С другой стороны, имеют место гомоморфизмы

$$\mathfrak{g}_i \to \mathfrak{g} \to U\mathfrak{g}, \quad i = 1, 2,$$

индуцирующие гомоморфизмы φ_i: $U\mathfrak{g}_i \to U\mathfrak{g}$. Поскольку $\mathfrak{g}_1$ и $\mathfrak{g}_2$ коммутируют, $\varphi_1(x_1)\varphi_2(x_2) = \varphi_2(x_2)\varphi_1(x_1)$ для всех $x_1 \in \mathfrak{g}_1$, $x_2 \in \mathfrak{g}_2$[1]).

Определим, наконец, отображение φ: $U\mathfrak{g}_1 \otimes U\mathfrak{g}_2 \to U\mathfrak{g}$, полагая $\varphi(x_1 \otimes x_2) = \varphi_1(x_1)\varphi_2(x_2)$. В силу сказанного выше φ есть гомоморфизм ассоциативных алгебр, причем по построению $\psi \circ \varphi = \mathrm{id}$ и $\varphi \circ \psi = \mathrm{id}$.

Аналогично, исходя из категорного определения универсальной обертывающей алгебры, доказываются свойства 1) и 3).

§ 3. Симметрическая алгебра модуля

Пусть $\mathfrak{g}$ — произвольный k-модуль. Положим $[x, y] = 0$ для всех $x, y \in \mathfrak{g}$. В этом случае универсальная обертывающая алгебра $U\mathfrak{g}$ называется *симметрической алгеброй* k-модуля $\mathfrak{g}$ и обозначается $S\mathfrak{g}$.

---

[1]) А следовательно, и для всех $x_1 \in U\mathfrak{g}_1$, $x_2 \in U\mathfrak{g}_2$, так как $\mathfrak{g}_i$ порождает $U\mathfrak{g}_i$. — *Прим. перев.*

Алгебру $S\mathfrak{g}$ можно определить также как наибольшую коммутативную факторалгебру алгебры $T\mathfrak{g}$. Иными словами,

$$S\mathfrak{g} = \sum_{n=0}^{\infty} S^n\mathfrak{g},$$

где $S^n\mathfrak{g} = \left(\overset{n}{\otimes}\,\mathfrak{g}\right)\Big/I$. (Здесь I обозначает идеал, порожденный элементами вида $a - \sigma a$, где σ — подстановка порядка n и $a \in \overset{n}{\otimes}\,\mathfrak{g}$.)

Рассмотрим пример свободного k-модуля $\mathfrak{g}$ с базисом $(e_i)_{i \in I}$.

Обозначим через S кольцо многочленов над k от переменных $(X_i)_{i \in I}$. Пусть $\varepsilon\colon \mathfrak{g} \to S$ — гомоморфизм k-модулей, однозначно определяемый равенствами $\varepsilon(e_i) = X_i$, $i \in I$. Легко проверяется, что пара (ε, S) обладает свойством универсальности (определение 1.1), а именно, ε есть k-линейное отображение и $\varepsilon(x)\,\varepsilon(y) = \varepsilon(y)\,\varepsilon(x)$. Далее, всякому k-линейному отображению $f\colon \mathfrak{g} \to A$, для которого $f(x)f(y) = f(y)f(x)$ (здесь A — коммутативная ассоциативная k-алгебра с единицей), отвечает единственный гомоморфизм ассоциативных алгебр $f^*\colon S \to A$, такой, что $f^* \circ \varepsilon = f$. В самом деле, если $P(X_i) \in S$, то $f^*(P) = P(f(e_i))$. Приведенное рассуждение показывает, что $S\mathfrak{g}$ канонически отождествляется с алгеброй многочленов $S = k\left[(X_i)_{i \in I}\right]$.

Если множество I линейно упорядочено, то в $S\mathfrak{g}$ можно выделить базис, состоящий из одночленов $e_{i_1} \ldots e_{i_n}$, $i_1 \leqslant i_2 \leqslant \ldots \leqslant i_n$, $n \geqslant 0$.

§ 4. Фильтрация алгебры $U\mathfrak{g}$

Пусть $\mathfrak{g}$ — алгебра Ли над k и $U\mathfrak{g}$ — ее универсальная обертывающая алгебра.

Обозначим через $U_n\mathfrak{g}$ подмодуль в $U\mathfrak{g}$, порожденный произведениями $\varepsilon(x_1) \ldots \varepsilon(x_m)$, где $m \leqslant n$ и

$x_i \in \mathfrak{g}$. Имеем

$$U_0\mathfrak{g} = k,$$
$$U_1\mathfrak{g} = k + \varepsilon(\mathfrak{g})$$

и

$$U_0\mathfrak{g} \subset U_1\mathfrak{g} \subset \ldots \subset U_n\mathfrak{g} \subset U_{n+1}\mathfrak{g} \subset \ldots .$$

Положим

$$\operatorname{gr} U\mathfrak{g} = \sum_{n=0}^{\infty} \operatorname{gr}_n U\mathfrak{g},$$

где

$$\operatorname{gr}_n U\mathfrak{g} = U_n\mathfrak{g}/U_{n-1}\mathfrak{g}.$$

Отображение $U_p\mathfrak{g} \times U_q\mathfrak{g} \to U_{p+q}\mathfrak{g}$, задаваемое правилом $(a, b) \longmapsto ab$, дает при факторизации билинейное отображение

$$\operatorname{gr}_p U\mathfrak{g} \times \operatorname{gr}_q U\mathfrak{g} \to \operatorname{gr}_{p+q} U\mathfrak{g}.$$

Алгебра $\operatorname{gr} U\mathfrak{g}$ с таким законом композиции называется *градуированной алгеброй*, ассоциированной с $U\mathfrak{g}$. Эта алгебра, очевидно, ассоциативна и обладает единицей.

Предложение 1. *Алгебра* $\operatorname{gr} U\mathfrak{g}$ *порождается образом алгебры* $\mathfrak{g}$ *при отображении, индуцированном отображением* $\varepsilon\colon \mathfrak{g} \to U\mathfrak{g}$[1]).

Доказательство. Пусть $\alpha \in \operatorname{gr}_n U\mathfrak{g}$ и $a \in U_n\mathfrak{g}$ — любой представитель элемента α, т. е. $\bar{a} = \alpha$. Как мы знаем,

$$a = \sum_{m_\mu \leqslant n} \lambda_\mu \varepsilon\left(x_1^{(\mu)}\right) \ldots \varepsilon\left(x_{m_\mu}^{(\mu)}\right).$$

Поэтому $\alpha = \sum_{m_\mu = n} \lambda_\mu \overline{\varepsilon\left(x_1^{(\mu)}\right)} \ldots \overline{\varepsilon\left(x_{m_\mu}^{(\mu)}\right)}$, что и требовалось доказать.

Теорема 2. *Алгебра* $\operatorname{gr} U\mathfrak{g}$ *коммутативна.*

Доказательство. Ввиду предложения 1 достаточно показать, что $\overline{\varepsilon(x)}$ и $\overline{\varepsilon(y)}$ перестановочны

[1]) Иными словами алгебра $\operatorname{gr} U\mathfrak{g}$ порождается $\operatorname{gr}_1 U\mathfrak{g}$ и единицей. — *Прим. перев.*

в $\mathrm{gr}_2 U\mathfrak{g}$ при любых x, $y \in \mathfrak{g}$. Поскольку ε — гомоморфизм алгебр Ли, имеем

$$\varepsilon(x)\varepsilon(y)-\varepsilon(y)\varepsilon(x)=\varepsilon([x, y]).$$

Однако $\varepsilon([x, y]) \in U_1\mathfrak{g}$, так что

$$\varepsilon(x)\varepsilon(y) \equiv \varepsilon(y)\varepsilon(x) \pmod{U_1\mathfrak{g}}$$

и

$$\overline{\varepsilon(x)}\cdot\overline{\varepsilon(y)}=\overline{\varepsilon(y)}\cdot\overline{\varepsilon(x)}.$$

Теорема доказана.

Из теоремы 2 немедленно вытекает, что каноническое отображение $\mathfrak{g} \to \mathrm{gr}\, U\mathfrak{g}$ продолжается до гомоморфизма

$$\tau\colon S\mathfrak{g} \to \mathrm{gr}\, U\mathfrak{g},$$

где $S\mathfrak{g}$ — симметрическая алгебра модуля $\mathfrak{g}$ (см. § 3).

Так как $\mathrm{gr}\, U\mathfrak{g}$ порождается образом $\mathfrak{g}$, гомоморфизм τ сюръективен.

Теорема 3 (Пуанкаре — Биркгоф — Витт). *Если $\mathfrak{g}$ — свободный k-модуль, то τ — изоморфизм*[1]).

Прежде чем доказывать теорему, установим предварительно две леммы.

Пусть $(x_i)_{i \in I}$ — базис модуля $\mathfrak{g}$, причем множество индексов I произвольным образом линейно упорядочено.

Лемма 4. *Семейство одночленов $\varepsilon(x_{i_1})\ldots\varepsilon(x_{i_m})$, $i_1 \leqslant \ldots \leqslant i_m$, $m \leqslant n$, порождает k-модуль $U_n\mathfrak{g}$.*

Доказательство. Воспользуемся индукцией по n. При $n=0$ утверждение очевидно. Предположим, что $n>0$, и рассмотрим элемент $a \in U_n\mathfrak{g}$. Его образ $\bar{a} \in \mathrm{gr}_n U\mathfrak{g}$ есть многочлен степени n от элементов $\overline{\varepsilon(x_i)}$. Отсюда вытекает, что элемент a представляет собой с точностью до элемента $a_1 \in U_{n-1}\mathfrak{g}$ линейную комбинацию произведений $\varepsilon(x_{i_1})\ldots\varepsilon(x_{i_m})$, $i_1 \leqslant \ldots \leqslant i_m$. Однако, согласно предположению индукции, a_1 есть

---

[1]) *Градуированных* алгебр. — *Прим. перев.*

линейная комбинация произведений вида $\varepsilon(x_1)\ldots\ldots\varepsilon(x_{i_m})$, $i_1\leqslant\ldots\leqslant i_m$, $m<n$, что и завершает доказательство.

Лемма 5. *Следующее утверждение эквивалентно теореме* 3: *семейство одночленов* $\varepsilon(x_1)\ldots\varepsilon(x_{i_n})$, $i_1\leqslant\ldots\leqslant i_n$, $n\geqslant 0$, *образует базис модуля* $U\mathfrak{g}$.

Доказательство. Условимся вначале о некоторых обозначениях. Пусть задан набор $M=(i_1,\ldots,i_m)$, $i_1\leqslant\ldots\leqslant i_m$. Назовем число m *длиной* $l(M)$ этого набора и будем для краткости вместо $\varepsilon(x_1)\ldots\varepsilon(x_{i_m})$ писать x_M.

Для каждого $n\geqslant 0$ элементы x_M длины n лежат в $U_n\mathfrak{g}$, а их образы $\bar{x}_M$ в $\mathrm{gr}_n\,U\mathfrak{g}=U_n\mathfrak{g}/U_{n-1}\mathfrak{g}$ совпадают с образами (при отображении $\tau\colon S^n\mathfrak{g}\to\mathrm{gr}_n\,U\mathfrak{g}$) базисных одночленов из $S^n\mathfrak{g}$. Таким образом, инъективность отображения τ равносильна отсутствию нетривиальных сравнений вида

$$\sum_{l(M)=n} c_M x_M = 0 \pmod{U_{n-1}\mathfrak{g}}.$$

По лемме 4 это сравнение эквивалентно равенству

$$\sum_{l(M)=n} c_M x_M = \sum_{l(M)<n} c_M x_M,$$

где по крайней мере один коэффициент c_M отличен от нуля. Но любая нетривиальная линейная зависимость элементов x_M над k может быть приведена к такому виду. Лемма доказана.

Теперь мы можем доказывать теорему 4.3 в ее новой формулировке. В дальнейшем мы можем (и будем) предполагать множество I *вполне упорядоченным*.

Пусть V — свободный k-модуль с базисом $\{Z_M\}$, где M, как и выше, пробегает множество наборов $(i_1,\ldots,i_n)$, таких, что $n\geqslant 0$ и $i_1\leqslant\ldots\leqslant i_n$. Пусть $i\in I$ и $M=(i_1,\ldots,i_n)$. По определению $i\leqslant M\Leftrightarrow i\leqslant i_1$. В случае $i\leqslant M$ введем обозначение $iM=(i,i_1,\ldots,i_n)$.

Основная лемма. *Модуль* V *можно наделить структурой* $\mathfrak{g}$-*модуля так, чтобы* $x_i Z_M = Z_{iM}$ *при* $i\leqslant M$.

Доказательство. Прежде всего мы должны определить k-линейное отображение $\mathfrak{g} \times V \to V$ и доказать, что V является $\mathfrak{g}$-модулем, т. е.

$$xyv - yxv = [x, y]\, v \quad (x, y \in \mathfrak{g},\ v \in V). \tag{1}$$

Чтобы определить xv, достаточно задать $x_i Z_M$ для всех i и M. Мы определим $x_i Z_M$ по индукции. Будем считать (предположение индукции) элемент $x_j Z_N$ определенным для *всех* $j \in I$, если $l(N) < l(M)$, и для $j < i$, если $l(M) = l(N)$; кроме того, мы будем предполагать, что каждый элемент $x_j Z_N$ является линейной комбинацией над k элементов Z_l, где

$$l(L) \leqslant l(N) + 1. \tag{$*$}$$

Положим

$$x_i Z_M = \begin{cases} Z_{iM}, & \text{если} \quad i \leqslant M, \\ x_j(x_i Z_N) + [x_i, x_j]\, Z_N, & \text{если} \quad M = jN,\ i > j. \end{cases} \tag{2}$$

Выражение $x_j(x_i Z_N)$ имеет здесь смысл, так как $j < i$; по предположению индукции $x_i Z_N$ есть линейная комбинация элементов Z_L, где $l(L) \leqslant l(N) + 1 = l(M)$. Выражение $[x_i, x_j]\, Z_N$ также определено, поскольку $[x_i, x_j]$ линейно выражается через x_k. Из равенства (2), между прочим, видно, что условие ($*$) остается справедливым при замене j и N соответственно на i и M.

Для доказательства равенства (1) достаточно в силу линейности установить справедливость формулы

$$x_i x_j Z_N - x_j x_i Z_N = [x_i, x_j]\, Z_N \tag{1'}$$

для всех i, j и N. Так как обе стороны этого равенства совершенно симметричны и обращаются в нуль при $i = j$, мы предположим, что $i > j$. Если $j \leqslant N$, то $x_j Z_N = Z_{jN}$ и равенство (1′) следует из индуктивного определения (2). Остается разобрать случай $N = kL$, где $i > j > k$. Соотношение (1′) переписывается в этом случае так:

$$x_i x_j x_k Z_L - x_j x_i x_k Z_L = [x_i, x_j]\, x_k Z_L. \tag{ijk}$$

В силу сказанного выше нетрудно установить справедливость равенств (jki) и (kij), получаемых из (ijk) циклической перестановкой. Действительно, учитывая, что $i > j > k \geqslant L$, мы получаем, например, для (jki)

$$x_j x_k x_i Z_L - x_k x_j x_i Z_L = x_j x_k Z_{iL} - x_k x_j Z_{iL}.$$

Но

$$x_j x_k Z_{iL} - x_k x_j Z_{iL} = [x_j, x_k] Z_{iL} = [x_j, x_k] x_i Z_L,$$

так как $k < iL$, а в этом случае соотношение (1′) уже установлено. Аналогично доказывается (kij).

Далее, применяя индукцию по $l(N)$, мы можем считать, что

$$xyZ_L = yxZ_L + [x, y] Z_L$$

для *всех* $x, y \in \mathfrak{g}$. Таким образом, мы можем переписать правую часть равенства (ijk) следующим образом:

$$\begin{aligned}[x_i, x_j] x_k Z_L = x_k [x_i, x_j] Z_L + [[x_i, x_j], x_k] Z_L = \\ = x_k x_i x_j Z_L - x_k x_j x_i Z_L + [[x_i, x_j], x_k] Z_L.\end{aligned}$$

Подставим это выражение в правую часть (ijk) и сложим полученное равенство с (уже доказанными) равенствами (jki) и (kij), записанными в такой же форме. В результате мы придем к соотношению вида

$$\sum = \sum + J(x_i, x_j, x_k) Z_L,$$

справедливость которого доказывает (ijk) и тем самым нашу лемму.

Поскольку V является $\mathfrak{g}$-модулем, на нем определена структура левого $U\mathfrak{g}$-модуля (см. замечание в конце § 1).

В частности, в модуле V имеется элемент $Z_\varnothing$[1]), где $\varnothing$ — пустое множество. Для всех M имеем

$$x_M Z_\varnothing = Z_M.$$

[1]) То есть элемент Z_M, где $l(M) = 0$. — *Прим. перев.*

Докажем это равенство индукцией по $l(M)$. Если $l(M)=0$, то по определению $x_M=1$. Если $l(M)>0$, то $M=iN$, где $i\leqslant N$. Тогда $x_M=\varepsilon(x_i)x_N$ и

$$x_M Z_{\mathfrak{Z}}=x_i(x_N Z_{\mathfrak{Z}})=x_i Z_N=Z_{iN}=Z_M.$$

Доказательство теоремы 4.3 в новой формулировке. Предположим, что $\sum c_M x_M=0$. Тогда

$$0=\sum c_M x_M Z_{\mathfrak{Z}}=\sum c_M Z_M,$$

откуда вытекает, что $c_M=0$ для всех M, ч. т. д.

Следствие 1. *Если $\mathfrak{g}$ — свободный k-модуль, то отображение ε: $\mathfrak{g}\to U\mathfrak{g}$ инъективно.*

Доказательство. Утверждение очевидно, если заметить, что ε индуцирует изоморфизм $\mathfrak{g}\simeq \operatorname{gr}_1 U\mathfrak{g}$ (т. е. $S^1\mathfrak{g}\simeq \operatorname{gr}_1 U\mathfrak{g}$).

Следствие 2. *Пусть $\mathfrak{g}=\mathfrak{g}_1\oplus\mathfrak{g}_2$, где $\mathfrak{g}_1$ и $\mathfrak{g}_2$ — подалгебры в $\mathfrak{g}$, свободные как модули над k. Отображение $U\mathfrak{g}_1\otimes U\mathfrak{g}_2\to U\mathfrak{g}$, индуцированное гомоморфизмами $U\mathfrak{g}_i\to U\mathfrak{g}$ и задаваемое правилом $u_1\otimes u_2\mapsto u_1u_2$, есть изоморфизм k-модулей.*

Доказательство. Пусть $(x_i)_{i\in I}$, $(y_j)_{j\in J}$ — свободные образующие алгебр $\mathfrak{g}_1$ и $\mathfrak{g}_2$ соответственно. Элементы $\{(x_i), (y_j)\}$ образуют базис алгебры $\mathfrak{g}$. Упорядочим линейно множество $I\cup J$ так, чтобы каждый элемент из I был строго меньше любого элемента из J. Мы знаем (лемма 4.5), что наборы одночленов $\{\varepsilon(x_{i_1})\ldots\varepsilon(x_{i_m})\}$, $\{\varepsilon(y_{j_1})\ldots\varepsilon(y_{j_m})\}$ и $\{\varepsilon(x_{i_1})\ldots\ldots\varepsilon(x_{i_n})\varepsilon(y_{j_1})\ldots\varepsilon(y_{j_m})\}$, $i_1\leqslant\ldots\leqslant i_n$, $j_1\leqslant\ldots\leqslant j_m$, являются свободными образующими модулей $U\mathfrak{g}_1$, $U\mathfrak{g}_2$ и $U\mathfrak{g}$ соответственно. Остается заметить, что отображение $U\mathfrak{g}_1\otimes_k U\mathfrak{g}_2\to U\mathfrak{g}$ $(u_1\otimes u_2\mapsto u_1u_2)$ взаимно однозначно переводит базис модуля $U\mathfrak{g}_1\otimes_k U\mathfrak{g}_2$ (построенный из базисов $U\mathfrak{g}_1$ и $U\mathfrak{g}_2$) в базис алгебры $U\mathfrak{g}$, ч. т. д.

Отметим, что в данном случае наше отображение $U\mathfrak{g}_1 \otimes_k U\mathfrak{g}_2 \to U\mathfrak{g}$ индуцирует изоморфизм

$$\operatorname{gr} U\mathfrak{g}_1 \otimes_k \operatorname{gr} U\mathfrak{g}_2 \simeq \operatorname{gr} U\mathfrak{g},$$

поскольку $\operatorname{gr} U\mathfrak{g}_i \simeq S\mathfrak{g}_i$ и $\operatorname{gr} U\mathfrak{g} \simeq S\mathfrak{g} \simeq S\mathfrak{g}_1 \otimes S\mathfrak{g}_2$.

§ 5. Диагональное отображение

Пусть $\mathfrak{g}$ — алгебра Ли над k. Предположим, что $\mathfrak{g}$ свободна как k-модуль.

Определение 1. Гомоморфизм алгебр Ли

$$\Delta\colon \mathfrak{g} \to \mathfrak{g} \times \mathfrak{g},$$

задаваемый правилом $x \to (x, x)$, индуцирует гомоморфизм ассоциативных алгебр

$$\Delta\colon U\mathfrak{g} \to U\mathfrak{g} \otimes_k U\mathfrak{g},$$

который мы будем называть *диагональным* отображением.

Предложение 2. *Диагональное отображение Δ однозначно определяется следующими двумя свойствами:*

1) *Δ — гомоморфизм алгебр;*

2) *$\Delta x = x \otimes 1 + 1 \otimes x$ для всех $x \in \mathfrak{g}$*[1]).

(Здесь мы отождествляем элемент $x \in \mathfrak{g}$ с его образом $\varepsilon(x) \in \mathfrak{g}$.)

Определение 3. Элемент $\alpha \in U\mathfrak{g}$ называется *примитивным*, если $\Delta\alpha = \alpha \otimes 1 + 1 \otimes \alpha$.

В частности, каждый элемент из $\mathfrak{g}$ примитивен.

Теорема 4. *Предположим, что k (как $\mathbf{Z}$-модуль) не имеет кручения и что $\mathfrak{g}$ — свободный модуль над k. Тогда множество примитивных элементов алгебры $U\mathfrak{g}$ совпадает с $\mathfrak{g}$.*

Доказательство. 1°. *Случай, когда алгебра $\mathfrak{g}$ абелева.* Универсальная обертывающая алгебра $U\mathfrak{g}$ есть не что иное, как кольцо многочленов $k[(X_i)]$

[1]) Предложение очевидно, так как $U\mathfrak{g}$ порождается элементами из $\mathfrak{g}$. — *Прим. перев.*

(см. § 3) от переменных X_i, соответствующих свободным образующим x_i модуля $\mathfrak{g}$. Диагональное отображение может быть интерпретировано как гомоморфизм

$$\Delta\colon\ k[(X_i)] \to k\left[(X_i'),\ (X_i'')\right]$$

$(X_i'$ соответствует элементу $X_i \otimes 1$, а X_i'' — элементу $1 \otimes X_i)$, где $\Delta f(X_i) = f(X_i' + X_i'')$, поскольку $\Delta(X_i) = X_i' + X_i''$ для каждого i. Таким образом, примитивные элементы $f(X_i) \in k[(X_i)]$ удовлетворяют уравнению

$$f(X_i' + X_i'') = f(X_i') + f(X_i'').$$

Если многочлен f обладает свойством аддитивности, то этим же свойством обладают и его однородные компоненты f_n. Пусть f — однородный многочлен степени n с таким свойством. Тогда

$$2^n f(X_i) = f(2X_i) = f(X_i + X_i) = 2f(X_i),$$

и $(2^n - 2)f = 0$. Поскольку k как $\mathbf{Z}$-модуль не имеет кручения, $f = 0$ при $n \neq 1$. Итак, линейные однородные многочлены и только они обладают свойством аддитивности.

2°. *Общий случай*. Гомоморфизм $\Delta\colon U\mathfrak{g} \to U\mathfrak{g} \otimes_k U\mathfrak{g}$ индуцирует отображения

$$\operatorname{gr}\Delta\colon \operatorname{gr} U\mathfrak{g} \to \operatorname{gr}(U\mathfrak{g} \otimes U\mathfrak{g}) \simeq \operatorname{gr} U\mathfrak{g} \oplus \mathfrak{g} \simeq \operatorname{gr} U\mathfrak{g} \otimes \operatorname{gr} U\mathfrak{g}$$

(см. конец § 4). С другой стороны, как мы знаем, $\operatorname{gr} U\mathfrak{g} \simeq S\mathfrak{g}$, причем соответствующее отображение $S\mathfrak{g} \to S\mathfrak{g} \otimes S\mathfrak{g}$ то самое, какое мы рассматривали в первом случае. Последнее можно усмотреть, прослеживая в цепочке отождествлений путь элементов вида $\bar{x} \in \operatorname{gr}_1 U\mathfrak{g}$, где $x \in \mathfrak{g}$.

Пусть $x \in U_n\mathfrak{g}$ и $\bar{x}$ — его образ в $\operatorname{gr}_n U\mathfrak{g}$. Если x примитивен, то таков же и $\bar{x}$ относительно отображения $\operatorname{gr}\Delta$. Следовательно, как было показано выше, $\bar{x} = 0$, если $n > 1$. Повторяя этот прием нужное число раз, заключаем, что $x \in U_1\mathfrak{g}$, т. е. $x = \lambda + y$, где $\lambda \in k$ и $y \in \mathfrak{g}$. Но тогда

$$\Delta x = \lambda + y \otimes 1 + 1 \otimes y,$$

$$x \otimes 1 + 1 \otimes x = \lambda + y \otimes 1 + \lambda + 1 \otimes y.$$

Таким образом, если x — примитивный элемент, то $2\lambda = \lambda$, т. е. $\lambda = 0$ и $x \in \mathfrak{g}$.

УПРАЖНЕНИЯ

1. Пусть $PU\mathfrak{g}$ — множество примитивных элементов алгебры $U\mathfrak{g}$. Показать, что $PU\mathfrak{g}$ устойчиво относительно коммутирования, т. е. $xy - yx \in PU\mathfrak{g}$, если $x, y \in PU\mathfrak{g}$.

2. Предположим, что $pk = 0$ для некоторого простого числа p и что алгебра Ли $\mathfrak{g}$ является свободным k-модулем с базисом $(x_i)_{i \in I}$. Доказать, что

а) множество $PU\mathfrak{g}$ устойчиво относительно отображения $y \mapsto y^p$;

б) элементы $\left(x_i^{p^\nu}\right)$, $i \in I$, $\nu \geqslant 0$, образуют базис над k для $PU\mathfrak{g}$;

в) $(x + y)^p - x^p - y^p \in \mathfrak{g}$, если x и y лежат в $\mathfrak{g}$.

Глава IV

СВОБОДНЫЕ АЛГЕБРЫ ЛИ

Как и прежде, k — коммутативное (и ассоциативное) кольцо с единицей. Все рассматриваемые алгебры и модули определены над k.

§ 1. Свободные моноиды

Определение 1. *Моноидом*[1]) называется множество M с отображением $M \times M \to M$, которое записывается в виде $(x, y) \mapsto xy$.

Для заданного множества X определим по индукции семейство множеств X_n $(n \geqslant 1)$:

1) $X_1 = X$;

2) $X_n = \coprod_{p+q=n} X_p \times X_q$ $(n \geqslant 2)$ (объединение непересекающихся множеств).

Положим $M_X = \coprod_n X_n$ и определим отображение

$$M_X \times M_X \to M_X$$

посредством отображений $X_p \times X_q \to X_{p+q} \subset M_X$, где стрелка обозначает каноническое включение, вытекающее из 2.

Построенный моноид M_X называется *свободным моноидом* на X. Элемент $w \in M_X$ иногда называют *неассоциативным словом* на X. Длина $l(w)$ этого слова есть по определению (единственное) число n, такое, что $w \in X_n$.

---

[1]) В оригинале „magma". — *Прим. перев.*

Теорема 2. *Пусть N — некоторый моноид и $f\colon X \to N$ — произвольное отображение. Существует единственный гомоморфизм моноидов $F\colon M_X \to N$,* продолжающий f.

Доказательство. Гомоморфизм F определяется индуктивно: $F(u, v) = F(u) \cdot F(v)$, где $(u, v) \in X_p \times X_q$.

В заключение этого параграфа отметим следующие очевидные свойства моноида M_X:

1) M_X порождается множеством X;

2) $m \in M_X \backslash X \Leftrightarrow m = uv$ с $u, v \in M_X$; при этом u, v однозначно определяются по m.

§ 2. Свободная алгебра над X

Обозначим через A_X k-алгебру свободного моноида M_X. Каждый элемент $\alpha \in A_X$ есть конечная сумма вида $\alpha = \sum\limits_{m \in M_X} c_m m$, где $c_m \in k$. Умножение в A_X является продолжением по линейности умножения в M_X.

Определение 1. Алгебра A_X называется *свободной алгеброй* над X.

Введение такого определения оправдывается следующей теоремой.

Теорема 2. *Пусть B — некоторая k-алгебра и $f\colon X \to B$ — произвольное отображение. Существует единственный гомоморфизм k-алгебр $F\colon A_X \to B$, продолжающий f.*

Доказательство. Согласно теореме 1.2, f продолжается до гомоморфизма моноидов $f'\colon M_X \to B$, где B рассматривается как моноид относительно умножения. Отображение f' по линейности продолжается до k-линейного отбражения $F\colon A_X \to B$. Легко видеть, что F—гомоморфизм алгебр. Единственность F очевидна, так как X порождает A_X.

Замечание. В A_X имеется структура *градуированной алгебры*, причем однородные элементы степени n суть линейные комбинации слов длины n.

§ 3. Свободная алгебра Ли над X

Пусть I — двусторонний идеал в A_X, порожденный элементами вида $a \cdot a$ и $J(a, b, c)$, где $a, b, c \in A_X$ и

$$J(a, b, c) = (ab)c + (bc)a + (ca)b.$$

Определение 1. Факторалгебра A_X/I называется *свободной алгеброй Ли над* X.

Эту алгебру мы будем обозначать $L_X(k)$ или просто L_X.

Функториальные свойства. 1) *Пусть* $f\colon X \to X'$ — *произвольное отображение множеств. Тогда существует единственный гомоморфизм* $F\colon L_X \to L_{X'}$, *такой, что* $F \mid X = f$.

1′) *Пусть* $\{X_\alpha, i_\alpha^\beta\}$ — *индуктивная система множеств и* $X = \varinjlim X_\alpha$. *Тогда*

$$\varinjlim L_{X_\alpha} = L_X.$$

2) *Если* k' — *расширение кольца* k (*т. е. ассоциативная коммутативная* k-*алгебра с единицей*), *то*

$$L_X(k') = L_X(k) \otimes_k k'.$$

3) *Идеал* I *является однородным идеалом в градуированной алгебре* A_X, *что позволяет определить на* L_X *естественную структуру градуированной алгебры.*

4) *Однородные компоненты* L_X^1 *и* L_X^2 *имеют в качестве базисов над* k *множества* X *и* $[X, X] = \{[x, y]\colon x < y;\ x, y \in X\}$ *соответственно.* (*Множество* X *предполагается линейно упорядоченным.*)

Доказательство свойства 3). Обозначим через $I^\#$ множество всех $a \in A_X$, таких, что каждая однородная компонента элемента a принадлежит I. Ясно, что $I^\#$ — двусторонний идеал и $I^\# \subset I$.

Пусть $x \in A_X$, $x = \sum x_n$, где элементы x_n однородны. Тогда $x \cdot x = \sum x_n^2 + \sum\limits_{n<m} (x_n x_m + x_m x_n)$. Но $x_n^2 \in I$, $x_n x_m + x_m x_n = (x_n + x_m)^2 - x_n^2 - x_m^2 \in I$, поэтому

$x \cdot x \in I^{\#}$. Аналогично для трех элементов $x = \sum x_n$, $y = \sum y_n$, $z = \sum z_n$ имеем $J(x, y, z) = \sum\limits_{l, m, n} J(x_l, y_m, z_n) \in I^{\#}$. Таким образом, $I^{\#} = I$, ч. т. д.

Доказательство свойства 4). Очевидно, X порождает L_X^1, а $[X, X]$ порождает L_X^2. Рассмотрим модуль $E = k^{(X)}$ [1] и алгебру Ли $E \oplus \bigwedge^2 E = \mathfrak{g}$ (пример (iii) из гл. I). Каноническое отображение $L \to \mathfrak{g}$ индуцирует гомоморфизм алгебр Ли $L_X \to \mathfrak{g}$, и композиция $L_X^1 \oplus L_X^2 \to L_X \to \mathfrak{g}$ является изоморфизмом, ч. т. д.

§ 4. Связь со свободной ассоциативной алгеброй над X

Определение 1. Пусть $E = k^{(X)}$ — свободный k-модуль с базисом X. Будем называть *свободной ассоциативной алгеброй над X* и обозначать через Ass_X тензорную алгебру TE модуля E.

(Элементы алгебры Ass_X можно было бы назвать „ассоциативными, но не коммутативными“ многочленами от элементов множества X.)

Теорема 2. *Пусть φ: $L_X \to \mathrm{Ass}_X$ и Φ: $UL_X \to \mathrm{Ass}_X$ — два отображения, индуцированных вложением $X \to \mathrm{Ass}_X$. Тогда*

(1) *отображение Φ есть изоморфизм;*

(2) *гомоморфизм φ изоморфно отображает L_X на подалгебру Ли алгебры Ass_X, порожденную множеством X;*

(3) *алгебра L_X и ее однородные компоненты L_X^n являются свободными k-модулями;*

(4) *если множество X конечно и* $\mathrm{Card}\, X = d$ [2], *то L_X^n — свободный k-модуль конечного ранга $l_d(n)$, причем*

$$\sum_{m \mid n} m l_d(m) = d^n. \qquad (*)$$

[1]) То есть свободный k-модуль с базисом X. — *Прим. перев.*

[2]) Card X обозначает мощность множества X. — *Прим. перев.*

Замечание. Формула (*) определяет число $l_d(n)$ по индукции. Фактически

$$nl_d(n) = d^n - \sum_{\substack{m \mid n \\ m < n}} ml_d(m).$$

(Точнее, пусть μ — *функция Мёбиуса*, определенная соотношением

$$\sum_{n=1}^{\infty} \mu(n) n^{-s} = 1/\zeta(s) = \prod_p (1 - p^{-s}).$$

Тогда

$$nl_d(n) = \sum_{m \mid n} \mu(m) d^{n/m}.)$$

Доказательство. Утверждение (1) очевидно, так как отображение $X \to UL_X$ определяет гомоморфизм Ψ: $\mathrm{Ass}_X \to UL_X$, причем $\Phi \circ \Psi = \mathrm{id}$ и $\Psi \circ \Phi = \mathrm{id}$.

Отметим также, что φ отображает L_X *на* подалгебру Ли алгебры Ass_X, порожденную множеством X. Поэтому свойство (2) эквивалентно инъективности φ. Наконец, заметим, что (3)$\Rightarrow$(2). В самом деле, если L_X — свободный k-модуль, то (по следствию из теоремы Биркгофа — Витта) отображение $L_X \to UL_X$ инъективно. Но мы можем отождествить алгебры UL_X и Ass_X.

Доказательство остальных утверждений проводится в четыре шага.

Шаг 1. *Предположим, что k — поле и множество X конечно.* Выберем *однородный* базис $(\gamma_i)_{i \in I}$ алгебры L_X и линейно упорядочим множество I. Положим $d_i = \deg(\gamma_i)$. При доказательстве теоремы Биркгофа — Витта было установлено, что семейство элементов вида $\gamma^e = \gamma_{i_1}^{e_{i_1}} \ldots \gamma_{i_s}^{e_{i_s}}$, где $i_1 < \ldots < i_s$, образует базис алгебры $UL_X = \mathrm{Ass}_X$, причем $\deg(\gamma^e) = \sum e_{i_j} d_{i_j}$. Поскольку элементы γ^e, где $\deg(\gamma^e) = n$, составляют базис модуля Ass_X^n, ранг $a(n)$ этого модуля равен числу (конечных) наборов (e_i), таких, что $\sum e_i d_i = n$, $e_i > 0$.

Последнее высказывание можно переформулировать следующим образом: формальный степенной ряд $A(t) = \sum a(n) t^n$ представим в виде

$$A(t) = \prod_{i \in I} \frac{1}{1 - t^{d_i}}.$$

Действительно,

$$\prod_{i \in I} \frac{1}{1 - t^{d_i}} = \prod_{i \in I} (1 + t^{d_i} + t^{2d_i} + \ldots),$$

и коэффициент при t^n есть в точности число (конечных) наборов (e_i), таких, что $\sum e_i d_i = n$.

По определению для каждого натурального m число элементов γ_i степени m равно $l_d(m)$. Поэтому

$$A(t) = \prod_{m=1}^{\infty} \frac{1}{(1 - t^m)^{l_d(m)}}.$$

С другой стороны, по построению алгебры Ass_X семейство одночленов $x_{i_1} \ldots x_{i_n}$, $x_{i_\nu} \in X$, образует базис модуля Ass_X^n. Значит, $a(n) = d^n$ и

$$A(t) = \sum_{n=0}^{\infty} d^n t^n = \frac{1}{1 - dt},$$

откуда

$$\prod_{m=1}^{\infty} \frac{1}{(1 - t^m)^{l_d(m)}} = \frac{1}{1 - dt}.$$

Используя равенство $\operatorname{Log} \frac{1}{1-t} = \sum_{n=1}^{\infty} \frac{1}{n} t^n$, получаем

$$\sum_{m, \nu} \frac{1}{\nu} l_d(m) t^{m\nu} = \sum_{n=1}^{\infty} \frac{1}{n} d^n t^n.$$

Поэтому для каждого n

$$\frac{1}{n} d^n = \sum_{m\nu=n} \frac{1}{\nu} l_d(m),$$

т. е.

$$d^n = \sum_{m \mid n} m l_d(m),$$

что и доказывает утверждение (4) в этом случае.

Шаг 2. *Предположим, что $k = \mathbf{Z}$ и X — конечное множество.* Нам понадобится следующая

Лемма 3. *Пусть E — конечно порожденный $\mathbf{Z}$-модуль. Если размерность пространства $E \otimes_{\mathbf{Z}} \mathbf{F}_p$ над $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ для всех простых p одинакова, то E — свободный $\mathbf{Z}$-модуль, и его ранг равен этой размерности.*

Указанная лемма есть простое следствие основной теоремы о строении абелевых групп с конечным числом образующих.

Остается заметить, что $L_X^n(\mathbf{Z}) \otimes_{\mathbf{Z}} F_p = L_X^n(F_p)$ и размерность $\dim\left(L_X^n(F_p)\right) = l_d(n)$ не зависит от p, так что L_X^n — свободный $\mathbf{Z}$-модуль ранга $l_d(n)$.

Шаг 3. *Предположим, что $k = \mathbf{Z}$, а множество X произвольно.* Пусть $\{Y_\alpha\}$ — семейство всех *конечных* подмножеств в X. Тогда $X = \varinjlim Y_\alpha$.

Докажем вначале свойство (2).

Используя второй шаг, мы видим, что отображение

$$\varphi_\alpha\colon L_{Y_\alpha} \to \mathrm{Ass}_{Y_\alpha}$$

инъективно для всех α. Однако отображение

$$\varphi\colon L_Y \to \mathrm{Ass}_Y$$

есть $\varinjlim \varphi_\alpha$, а индуктивный предел семейства инъективных отображений инъективен. Таким образом, свойство (2) доказано.

Из (2), в частности, вытекает, что L_X и L_X^n — подмодули $\mathbf{Z}$-модуля Ass_X; последний свободен, а потому L_X и L_X^n (для всех n) также являются свободными

Z-модулями. Тем самым теорема в рассматриваемом случае доказана.

Шаг 4. *Общий случай.* Учитывая тот факт, что модуль $L_X^n(\mathbf{Z})$ свободен, а также равенство $L_X^n(k) = L_X^n(\mathbf{Z}) \otimes_{\mathbf{Z}} k$, заключаем, что $L_X^n(k)$ — свободный модуль над k. Значит, справедливо (3) и, следовательно, (2).

С другой стороны, $\mathrm{rk}_k L_X^n(k) = \mathrm{rk}_{\mathbf{Z}} L_X^n(\mathbf{Z})$. Поэтому, если X конечно, то $\mathrm{rk}_k L_X^n(k) = l_d(n)$.

§ 5. Семейства Холла

Определение 1. Пусть задано некоторое множество X. *Семейством Холла* в свободном моноиде M_X называется линейно упорядоченное подмножество $H \subset M_X$ со следующими свойствами:

(1) $X \subset H$;

(2) если $u, v \in H$ и $l(u) < l(v)$, то $u < v$;

(3) пусть $v \in M_X \setminus X$ и $v = uw$ — (единственное) разложение элемента v (с $u, w \in M_X$); тогда элемент v принадлежит H в том и только в том случае, когда выполнены следующие условия:

(a) $u \in H$, $w \in H$ и $u < w$;

(b) либо $w \in X$, либо $w = w' \cdot w''$, где $w', w'' \in H$ и $w' \leqslant v$.

Лемма 2. *Семейство Холла существует для любого множества X.*

Доказательство. Определим по индукции множества $H^n = H \cap X_n$. Положим $H^1 = X$ и линейно упорядочим X. Допустим, что $H^1, \ldots, H^{n-1}$ уже определены и линейно упорядочены таким образом, что условия (1), (2) и (3) выполняются для всех элементов длины $\leqslant n-1$. Тогда множество H^n однозначно определяется условием (3). Выберем в H^n некоторое линейное упорядочение и положим $u < v$, если $u \in H^i$ $(i \leqslant n-1)$, а $v \in H^n$. Очевидно, что $\bigcup_{n=1}^{\infty} H^n$ есть семейство Холла.

Пример. Пусть $X=\{x, y\}$, где $x \neq y$. Тогда

$$H^1=\{x, y\}, \quad x<y,$$
$$H^2=\{x \cdot y\},$$
$$H^3=\{x \cdot (x \cdot y),\ y \cdot (x \cdot y)\},\ x \cdot (x \cdot y)<y \cdot (x \cdot y),$$
$$H^4=\{x(x(xy)),\ y(x(xy)),\ y(y(xy))\},$$
$$H^5=\{x(x(x(xy))),\ y(x(x(xy))),\ y(y(x(xy))),\ y(y(y(xy))),\ (xy)(x(xy)),\ (xy)(y(xy))\}.$$

Теорема 3. *Если H — семейство Холла в M_X, то канонические образы элементов $h \in H$ образуют базис в L_X.*

Обозначим через $\bar{h}$ образ элемента $h \in H$ в L_X. Наша теорема эквивалентна следующим двум утверждениям:

(1) семейство $\{\bar{h}\}$, $h \in H$, порождает L_X;

(2) элементы $\{\bar{h}\}$, $h \in H$, линейно независимы.

Мы докажем здесь лишь первую (более легкую) часть теоремы. Вторую часть доказательства читатель сможет найти в книге Холла [1], гл. 11, или в работе Витта [1]. Доказательство Холла носит чисто вычислительный характер; доказательство Витта лучше, но длиннее.

Доказательство утверждения (1). Символом L'_X обозначим k-подмодуль, порожденный элементами $\bar{h}$. Поскольку L'_X содержит X, нам достаточно показать, что L'_X — алгебра Ли, т. е. $[\bar{h}_1, \bar{h}_2] \in L'_X$, если $h_1, h_2 \in H$.

Доказательство мы проведем при помощи двойной индукции: сначала по числу $l(h_1)+l(h_2)$ (т. е. по длине n элемента h_1h_2), а затем для заданного n, спуском по числу $\inf(h_1, h_2)$. Для того чтобы такой индуктивный процесс можно было осуществить, мы предположим, что X *конечно*. Общий случай получится переходом к индуктивному пределу.

Мы можем считать, что $h_1<h_2$ (в противном случае воспользуемся соотношениями $[\bar{h}_1, \bar{h}_2]=-[\bar{h}_2, \bar{h}_1]$ и $[\bar{h}, \bar{h}]=0$).

Первый случай. Пусть $h_2 \in X$. Тогда $h_1 \in X$ (поскольку $h_1 < h_2$), откуда (по определению семейства Холла) $h_1 h_2 \in H$, так что $\overline{h_1 h_2} = [\bar{h}_1, \bar{h}_2]$.

Второй случай. Пусть $h_2 \notin X$. Положим $h_2 = h_3 h_4$, где $h_3 h_4 \in H$ и $h_3 < h_4$. Имеют место два подслучая:

a) $h_3 \leqslant h_1$; тогда $h_1 (h_3 h_4) \in H$ и

$$[\bar{h}_1, \bar{h}_2] = [\bar{h}_1, [\bar{h}_3, \bar{h}_4]] = \overline{h_1 (h_3 h_4)};$$

b) $h_1 < h_3 < h_4$; в этом случае имеем, согласно тождеству Якоби,

$$[\bar{h}_1, [\bar{h}_3, \bar{h}_4]] = [\bar{h}_3, [\bar{h}_1, \bar{h}_4]] - [\bar{h}_4, [\bar{h}_1, \bar{h}_3]].$$

Поскольку $l(h_1 h_4) < l(h_1 h_2)$, получаем (по предположению индукции) соотношение $[\bar{h}_1, \bar{h}_4] = \sum c_\alpha \bar{h}_\alpha$, где $h_\alpha \in H$. Отсюда вытекает, что $l(h_\alpha) = l(h_1) + l(h_4)$ и, в частности, $l(h_\alpha) > l(h_1)$, так что $h_\alpha > h_1$. Вспоминая, что $h_1 < h_3$, заключаем, что $\inf(h_3, h_\alpha) > h_1 = \inf(h_1, h_2)$. Следовательно, согласно второму предположению индукции, имеет место включение $[\bar{h}_3, \bar{h}_\alpha] \in L'_X$.

Аналогичное рассуждение (с заменой h_3 на h_4) показывает, что элемент $[\bar{h}_4, [\bar{h}_1, \bar{h}_3]]$ также есть линейная комбинация элементов вида $\bar{h}$, где $h \in H$. Доказательство закончено.

§ 6. Свободные группы

В этом параграфе мы предполагаем, что $k = \mathbf{Z}$. Пусть X — некоторое множество и F_X — свободная группа над X, и пусть $\{F_X^n\}$ — *убывающий центральный ряд* этой группы, т. е. (по определению) $F_X^1 = F_X$ и $F_X^n = (F_X, F_X^{n-1})$ при $n > 1$.

Присоединенная градуированная группа

$$\operatorname{gr} F_X = \sum_{n=1}^{\infty} \operatorname{gr}^n F_X, \quad \operatorname{gr}^n F_X = F_X^n / F_X^{n+1}$$

является, как мы знаем, алгеброй Ли. Заметим, кстати, что $\operatorname{gr}^1 F_X = F_X/(F_X, F_X)$, т. е. $\operatorname{gr}^1 F_X$ есть *свободная абелева* группа над X.

Теорема 1. *Каноническое отображение* $X \to \operatorname{gr}^1 F_X$ *индуцирует изоморфизм алгебр Ли*

$$\varphi_1\colon L_X \xrightarrow{\sim} \operatorname{gr} F_X.$$

Следствие 2. *Группы* F_X^n / F_X^{n+1} — *свободные* $\mathbf{Z}$-*модули; если* $\operatorname{Card}(X) = d$ *конечно, то* $\operatorname{rk}(F_X^n / F_X^{n+1}) = l_d(n)$.

Прежде чем доказывать теорему, введем некоторые понятия и обозначения.

Рассмотрим свободную ассоциативную алгебру Ass_X над X и обозначим через Ass_X^n ее однородную компоненту степени n. *Пополнением* $\widehat{\mathrm{Ass}}_X$ алгебры Ass_X назовем бесконечное произведение $\prod\limits_{n=0}^{\infty} \mathrm{Ass}_X^n$. Элемент $f \in \widehat{\mathrm{Ass}}_X$ можно представить в виде формального ряда $f = \sum\limits_{n=0}^{\infty} f_n$, где $f_n \in \mathrm{Ass}_X^n$.

Пусть $\widehat{\mathrm{Ass}}_X^*$ — мультипликативная группа обратимых элементов алгебры $\widehat{\mathrm{Ass}}_X$. Определим гомоморфизм $\theta\colon F_X \to \widehat{\mathrm{Ass}}_X^*$, полагая $\theta(x) = 1 + x$ [1]) (ясно, что элемент $1 + x$ обратим в $\widehat{\mathrm{Ass}}_X$).

Для каждого целого положительного числа n положим

$$\widehat{\mathfrak{m}}^n = \left\{ f \in \widehat{\mathrm{Ass}}_X \mid f = \sum_{m=0}^{\infty} f_m,\ f_0 = f_1 = \ldots = f_{n-1} = 0 \right\}$$

и рассмотрим группу $'F_X^n = \theta^{-1}(1 + \widehat{\mathfrak{m}}^n)$. Легко видеть, что $'F_X^1 = F_X$ и $'F_X^n \subset {}'F_X^{n-1}$.

Теорема 3. $'F_X^n = F_X^n$.

Доказательства теорем 1 и 3.

1°. Очевидно, что отображение $\varphi_1\colon L_X \to \operatorname{gr} F_X$ *сюръективно.*

[1]) На элементах $x \in X$. — *Прим. перев.*

2°. Докажем, что $\{'F_X^n\}$ — фильтрация группы F_X. Фактически для этого нужно лишь проверить, что

$$('F_X^m, 'F_X^p) \subset 'F_X^{m+p}.$$

Возьмем $g \in 'F_X^m$ и $h \in 'F_X^p$. Тогда $\theta(g) = 1 + G$ и $\theta(h) = 1 + H$, где $G \in \hat{\mathfrak{m}}^m$ и $H \in \hat{\mathfrak{m}}^p$. Отсюда

$$\theta(gh) = 1 + G + H + GH,$$
$$\theta(hg) = 1 + G + H + HG.$$

Но $gh = hg(g, h)$ и θ — гомоморфизм, поэтому $\theta(gh) = \theta(hg)\theta((g, h))$; следовательно,

$$\theta((g, h)) = 1 + (GH - HG) + \text{члены высших порядков.} \quad (*)$$

Таким образом, $(g, h) \in 'F_X^{m+p}$.

Далее, имеется естественное отображение η: $\operatorname{gr} F_X \to \operatorname{Ass}_X$, определяемое следующим образом. Пусть $\xi \in '\operatorname{gr} F_X$, и пусть $g \in 'F_X^n$ — представитель класса ξ. Допустим, что

$$\theta(g) = 1 + G_n + G_{n+1} + \ldots, \quad \text{где} \quad G_p \in \operatorname{Ass}_X^p.$$

Положим

$$\eta(\xi) = G_n.$$

Легко видеть, что это определение не зависит от выбора представителя g. Формула $(*)$ показывает, что η: $'\operatorname{gr} F_X \to \operatorname{Ass}_X$ есть *гомоморфизм алгебр Ли*.

Поскольку $\{'F_X^n\}$ — фильтрация, для всех n имеют место включения $F_X^n \subset 'F_X^n$, индуцирующие гомоморфизм

$$\psi\colon \operatorname{gr} F_X \to '\operatorname{gr} F_X.$$

Рассмотрим теперь композицию отображений

$$L_X \xrightarrow{\varphi_1} \operatorname{gr} F_X \xrightarrow{\psi} '\operatorname{gr} F_X \xrightarrow{r} \operatorname{Ass}_X,$$

где φ_1 сюръективно, а η инъективно. Композиция эта есть, очевидно, отображение φ: $L_X \to \operatorname{Ass}_X$, фигурирующее в теореме 4.2, которое, как мы знаем, инъективно. Значит, гомоморфизм φ_1 инъективен и, следовательно, является изоморфизмом. Этим доказана теорема 6.1.

Из сказанного выше вытекает также инъективность отображения ψ. Докажем теперь по индукции равенство $F_X^n = {}'F_X^n$.

При $n=1$ имеем $F_X^1 = {}'F_X^1$ по определению.

При $n>1$ имеем

$$F_X^n \subset {}'F_X^n \subset {}'F_X^{n-1} = F_X^{n-1},$$

причем инъекция $\mathrm{gr}^{n-1} F_X \to \mathrm{gr}^{n-1\prime} F_X$ есть каноническое отображение

$$F_X^{n-1}/F_X^n \to F_X^{n-1}/{}'F_X^n,$$

откуда $F_X^n = {}'F_X^n$, ч. т. д.

§ 7. Формула Кэмпбелла—Хаусдорфа

В §§ 7 и 8 предполагается, что основное кольцо k — алгебра над $\mathbf{Q}$ (например, поле нулевой характеристики).

Теорема 1. *Пусть X — некоторое множество. Тогда свободная алгебра L_X совпадает с множеством примитивных элементов алгебры* Ass_X *(т. е.*

$$L_X = \{w \in \mathrm{Ass}_X \mid \Delta w = w \otimes 1 + 1 \otimes w\},$$

где $\Delta\colon \mathrm{Ass}_X \to \mathrm{Ass}_X \otimes \mathrm{Ass}_X$ *— диагональное отображение).*

Это следует из теоремы 5.4, доказанной в гл. III, поскольку алгебра Ass_X может быть отождествлена с UL_X.

Так же как в § 6, мы определим *пополнение* $\hat{L}_X$ алгебры Ли L_X равенством

$$\hat{L}_X = \prod_{n=0}^{\infty} L_X^n.$$

Определим аналогично *полное тензорное произведение* $\widehat{\mathrm{Ass}}_X \mathbin{\widehat{\otimes}} \widehat{\mathrm{Ass}}_X$ формулой

$$\widehat{\mathrm{Ass}}_X \mathbin{\widehat{\otimes}} \widehat{\mathrm{Ass}}_X = \prod_{p,\,q} \mathrm{Ass}_X^p \otimes \mathrm{Ass}_X^q.$$

Диагональное отображение Δ продолжается до гомоморфизма Δ: $\widehat{\mathrm{Ass}}_X \to \widehat{\mathrm{Ass}}_X \mathbin{\widehat{\otimes}} \widehat{\mathrm{Ass}}_X$, причем ясно, что теорема 7.1 остается справедливой при замене Ass_X, $\mathrm{Ass}_X \otimes \mathrm{Ass}_X$ и L_X их пополнениями.

Теорема 2. *Пусть* $\hat{\mathfrak{m}}$ — *идеал в алгебре* $\widehat{\mathrm{Ass}}_X$, *порожденный множеством* X. *Определим отображения*

$$\exp\colon \hat{\mathfrak{m}} \to 1 + \hat{\mathfrak{m}} \quad \text{и} \quad \log\colon 1 + \hat{\mathfrak{m}} \to \hat{\mathfrak{m}}$$

следующими формулами:

$$\exp(x) = \sum_{n=0}^{\infty} x^n/n!, \quad \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} x^n/n.$$

Тогда $\exp \circ \log = 1$ *и* $\log \circ \exp = 1$ [1]).

Доказательство. Установим, например, равенство $\exp(\log(1+y)) = 1 + y$, $y \in \hat{\mathfrak{m}}$. Хорошо известно, что в кольце $\mathbf{Q}[[T]]$ формальных степенных рядов от переменной T имеет место формула

$$\exp(\log(1+T)) = T.$$

Но поскольку y лежит в $\hat{\mathfrak{m}}$, имеется (корректно определенный) *непрерывный* гомоморфизм $\rho\colon \mathbf{Q}[[T]] \to \widehat{\mathrm{Ass}}_X$, переводящий T в y. Применяя ρ к равенству $\exp(\log(1+T)) = T$, получаем $\exp(\log(1+y)) = 1 + y$, ч. т. д.

Следствие 3. *Отображение* exp *определяет биекцию множества* $\{\alpha \in \hat{\mathfrak{m}} \mid \Delta\alpha = \alpha \otimes 1 + 1 \otimes \alpha\}$ *на множество* $\{\beta \in 1 + \hat{\mathfrak{m}} \mid \Delta\beta = \beta \otimes \beta\}$.

[1]) В дальнейшем потребуется еще одно очевидное свойство отображения exp, доказываемое прямым вычислением. А именно, $\exp(x+y) = \exp(x) \cdot \exp(y)$, $x, y \in \hat{\mathfrak{m}}$, если элементы x и y коммутируют. — *Прим. перев.*

Доказательство. Пусть $\alpha \in \hat{\mathfrak{m}}$, $\beta = e^{\alpha}$ и $\Delta\alpha = \alpha \otimes 1 + 1 \otimes \alpha$. Поскольку Δ коммутирует с экспоненциальным отображением, а элементы $\alpha \otimes 1$ и $1 \otimes \alpha$ перестановочны, получаем цепочку равенств

$$\Delta\beta = \Delta e^{\alpha} = e^{\Delta\alpha} = e^{\alpha \otimes 1 + 1 \otimes \alpha} = e^{\alpha \otimes 1} \cdot e^{1 \otimes \alpha} = (\beta \otimes 1)(1 \otimes \beta) = \beta \otimes \beta\,[1]).$$

Теорема 4 (Кэмпбелл — Хаусдорф). *Пусть* $X = \{x, y\}$, $x \neq y$. *Тогда* $e^x \cdot e^y = e^z$, *где* $z \in \hat{L}_X$.

Доказательство. Поскольку e^x, $e^y \in 1 + \hat{\mathfrak{m}}$, постольку $e^x \cdot e^y \in 1 + \hat{\mathfrak{m}}$. Поскольку экспоненциальное отображение биективно, существует один и только один элемент $z \in \hat{\mathfrak{m}}$, такой, что $e^x \cdot e^y = e^z$.

Далее,

$$\Delta(e^z) = \Delta(e^x \cdot e^y) = \Delta(e^x) \cdot \Delta(e^y) = (e^x \otimes e^x)(e^y \otimes e^y) = e^x \cdot e^y \otimes e^x \cdot e^y = e^z \otimes e^z.$$

В силу следствия 3 z — есть примитивный элемент, и по теореме 1 (для пополнений) $z \in \hat{L}_X$, ч. т. д.

Рассмотрим теперь произвольное множество X. Для любых элементов $x, y \in X$ обозначим через $z(x, y)$ элемент множества $\hat{L}_{\{x, y\}} \subset \hat{L}_X$, такой, что $e^x \cdot e^y = e^{z(x, y)}$.

Мы имеем $z(x, y) = \sum_{n=1}^{\infty} z_n(x, y)$, где $z_n(x, y) \subset L_X^n$. Явные выражения для первых трех однородных компонент элемента $z(x, y)$ таковы:

$$z_1(x, y) = x + y,$$

$$z_2(x, y) = \frac{1}{2}[x, y],$$

$$z_3(x, y) = \frac{1}{12}[x, [x, y]] + \frac{1}{12}[y, [y, x]].$$

---

[1]) Обратно, пусть $\beta \in 1 + \hat{\mathfrak{m}}$, $\Delta\beta = \beta \otimes \beta$ и $\beta = e^{\alpha}$, где $\alpha = \log \beta \in \hat{\mathfrak{m}}$. Очевидно, $\beta \otimes \beta = (\beta \otimes 1)(1 \otimes \beta) = (e^{\alpha} \otimes 1)(1 \otimes e^{\alpha}) = e^{\alpha \otimes 1} \cdot e^{1 \otimes \alpha} = e^{\alpha \otimes 1 + 1 \otimes \alpha}$. Однако $\Delta\beta = e^{\Delta\alpha}$, откуда $\Delta\alpha = \alpha \otimes 1 + 1 \otimes \alpha$. — *Прим. перев.*

Ясно также, что $z(0, y) = y$, $z(x, 0) = x$ и $z(z(w, x), y) = z(w, z(x, y))$.

§ 8. Явная формула

Введем линейные отображения Φ: $\mathfrak{m} \to L_X$ и φ: $\mathfrak{m} \to L_X$ ($\mathfrak{m} \subset \mathrm{Ass}_X$), полагая

$$\Phi(x_1 \dots x_n) = [x_1, [x_2, \dots [x_{n-1}, x_n] \dots]] = \\ = \mathrm{ad}\, x_1 \dots \mathrm{ad}\, x_{n-1}(x_n),$$

$$\varphi(x_1 \dots x_n) = \frac{1}{n} \Phi(x_1 \dots x_n),$$

$x_i \in X$.

Теорема 1. *Отображение φ является ретракцией идеала $\mathfrak{m}$ на L_X, т. е. $\varphi \mid L_X = \mathrm{id}_{L_X}$.*

Доказательство. Наша задача — доказать, что $\Phi(u) = nu$, если $u \in L_X^n$. Рассмотрим гомоморфизм ассоциативных алгебр θ: $\mathrm{Ass}_X \to \mathrm{End}(L_X)$, продолжающий гомоморфизм алгебр Ли ad: $L_X \to \mathrm{End}(L_X)$.

Лемма 2. *Для любых $u \in \mathrm{Ass}_X$ и $v \in m$ справедливо равенство $\Phi(uv) = \theta(u) \cdot \Phi(v)$.*

Доказательство леммы. Так как Φ и θ линейны, достаточно рассмотреть случай $u = x_1 \dots x_n$, $x_i \in X$; проведем индукцию по n. При $n = 1$ утверждение очевидно. Пусть $n > 1$. Тогда

$$\Phi(x_1 \dots x_n \cdot v) = \theta(x_1)\Phi(x_2 \dots x_n \cdot v) = \\ = \theta(x_1)\theta(x_2 \dots x_n)\Phi(v) = \theta(x_1 \dots x_n)\Phi(v).$$

Тем самым лемма доказана.

Вернемся к нашей теореме. Доказательство формулы $\Phi(u) = nu$, $u \in L_X^n$, проведем опять по индукции.

При $n = 1$ формула очевидна.

Пусть $n > 1$. Тогда $u = \sum [v_i, w_i]$. Мы можем поэтому считать, что $u = [v, w]$, где $v \in L_X^p$, $w \in L_X^q$, $p + q = n$, $p, q > 0$.