

Группы и их приложения
Факультет наук о материалах МГУ

В. А. Артамонов

Содержание

Глава 1. Основы теории групп	5
1. Группы, примеры	5
2. Подгруппы	8
3. Порядки элементов группы	9
4. Циклические группы и их подгруппы	9
5. Смежные классы и теорема Лагранжа	10
6. Гомоморфизмы, нормальные подгруппы, факторгруппы	11
7. Классы сопряженных элементов	13
8. Коммутант группы	15
9. Прямые произведения групп	17
Глава 2. Конечно порожденные абелевы группы	19
Глава 3. Кристаллографические группы	25
1. Группы движений	25
2. Двумерный случай	26
3. Трехмерный случай	27
Глава 4. Элементы теории представлений групп	33
1. Основные понятия и примеры	33
2. Теорема Машке и ее приложения	35
3. Лемма Шура и ее следствия	36
4. Характеры представления	38
Глава 5. Алгебры и поля	43
1. Кольца и алгебры	43
2. Теорема Фробениуса	45
3. Алгебры Ли	47
Глава 6. Линейные группы и их алгебры Ли	51
1. Касательные пространства	51
2. Структура алгебры Ли на T_E	54
3. Представления групп Ли	58
Литература	61

ГЛАВА 1

Основы теории групп

В этой главе изучаются основные понятия теории групп.

1. Группы, примеры

Напомним некоторые необходимые определения.

ОПРЕДЕЛЕНИЕ 1.1. Множество G с бинарной операцией умножения xy называется *группой*, если

1. умножение ассоциативно, т. е. $(xy)z = x(yz)$ для всех $x, y, z \in G$;
2. существует такой элемент $1 \in G$, называемый *единицей* G , что $x1 = 1x = x$ для всех $x \in G$;
3. для любого элемента $x \in G$ найдется такой элемент x^{-1} , называемый *обратным* к x , что $xx^{-1} = x^{-1}x = 1$.

ОПРЕДЕЛЕНИЕ 1.2. *Порядком* группы G называется число $|G|$ элементов в G .

УПРАЖНЕНИЕ 1.3. Пусть F – поле из q элементов. Доказать, что

$$|\mathrm{GL}(n, F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

ПРЕДЛОЖЕНИЕ 1.4. *Единичный элемент в группе единственен. Для каждого элемента $x \in G$ обратный элемент x^{-1} определен однозначно. Кроме того, если $x \in G$, то $(x^{-1})^{-1} = x$.*

ОПРЕДЕЛЕНИЕ 1.5. Пусть правильный n -угольник M расположен в $\mathbb{C} = \mathbb{R}^2$, причем его центр находится в нуле, вершины лежат на окружности радиуса 1, и одна из вершин в точке 1. Группой *диэдра* D_n называется множество всех аффинных обратимых преобразований комплексной плоскости, переводящих M в себя. Операцией умножения в D_n является произведение (композиция) преобразований.

ПРЕДЛОЖЕНИЕ 1.6. *Пусть правильный n -угольник расположен в $\mathbb{C} = \mathbb{R}^2$, причем его центр находится в нуле, вершины лежат на окружности радиуса 1, и одна из вершин в точке 1. Пусть*

$$a = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Тогда D_n состоит из элементов $1, a, a^2, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}$ и потому имеет порядок $2n$. Кроме того, $a^n = b^2 = (ba)^2 = 1$.

УПРАЖНЕНИЕ 1.7. Пусть

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in \text{SL}(2, \mathbb{C}).$$

Доказать, что

1. $I^2 = J^2 = K^2 = -E$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, $IK = -J$;
2. 8 матриц $\pm E, \pm I, \pm J \pm K$ образуют подгруппу кватернионов Q_8 в группе $\text{SL}(2, \mathbb{C})$.

УПРАЖНЕНИЕ 1.8. Если $H_i, i \in I$ – подгруппы группы G , то $\bigcap_{i \in I} H_i$ – подгруппа группы G .

Приведем еще одну важную серию примеров групп. Пусть

$$X_n = \{1, 2, \dots, n\}.$$

ОПРЕДЕЛЕНИЕ 1.9. *Перестановкой (подстановкой) степени n* называется биективное отображение X_n в себя. Через S_n обозначается множество всех перестановок степени n .

ПРЕДЛОЖЕНИЕ 1.10. *Произведение перестановок и обратная и тождественная перестановки снова являются перестановками. Умножение перестановок ассоциативно. В частности, S_n является группой.*

ОБОЗНАЧЕНИЕ 1.11. Пусть $\sigma \in S_n$. Тогда если $X_n = \{i_1, \dots, i_n\}$, то σ однозначно задается в виде двустрочной матрицы

$$\sigma = \begin{pmatrix} i_1 & \dots & i_n \\ \sigma(i_1) & \dots & \sigma(i_n) \end{pmatrix} \quad (1)$$

УПРАЖНЕНИЕ 1.12. Пусть σ из (1), и

$$\tau = \begin{pmatrix} j_1 & \dots & j_n \\ i_1 & \dots & i_n \end{pmatrix}.$$

Тогда

$$\sigma\tau = \begin{pmatrix} j_1 & \dots & j_n \\ \sigma(i_1) & \dots & \sigma(i_n) \end{pmatrix}$$

и

$$\sigma^{-1} = \begin{pmatrix} \sigma(i_1) & \dots & \sigma(i_n) \\ i_1 & \dots & i_n \end{pmatrix}$$

ОПРЕДЕЛЕНИЕ 1.13. Пусть σ из (1). Тогда *знаком σ* называется $(-1)^k$ в степени k , где k – сумма числа инверсий в перестановках

$$i_1, \dots, i_n \text{ и } \sigma(i_1), \dots, \sigma(i_n).$$

ПРЕДЛОЖЕНИЕ 1.14. *Определение знака подстановки корректно и не зависит от представления (1). Знак произведения подстановок равен произведению знаков.*

ОПРЕДЕЛЕНИЕ 1.15. Пусть i_1, \dots, i_k – различные числа из X_n . *Циклом $(i_1, \dots, i_k) \in S_n$ длины k* называется такая перестановка σ , что для $m \in X_n$

$$\sigma(m) = \begin{cases} i_{s+1}, & \text{если } m = i_s, s < k; \\ i_1, & \text{если } m = i_k; \\ m, & \text{если } m \in X_n \setminus \{i_1, \dots, i_k\}. \end{cases}$$

Два цикла

$$(i_1, \dots, i_k), (j_1, \dots, j_s) \in S_n$$

независимы, если все элементы $i_1, \dots, i_k, j_1, \dots, j_s$ различны.

ТЕОРЕМА 1.16. *Любая перестановка разлагается в произведение независимых циклов.*

ДОКАЗАТЕЛЬСТВО. Пусть $\sigma \in S_n$. Можно считать, что $\sigma \neq 1$. Возьмем произвольный элемент $k, 1 \leq k \leq n$, и предположим, что элементы $k_0 = k, k_1 = \sigma k, k_2 = \sigma^2 k, \dots, k_l = \sigma^l k$ различны, но $\sigma^{l+1} k = \sigma^s k$, где $0 \leq s \leq l$.

ЛЕММА 1.17. $s = 0$.

ДОКАЗАТЕЛЬСТВО. Если $s > 0$, то $\sigma(k_{s-1}) = \sigma(k_l)$, что невозможно, ибо σ действует инъективно на $X = \{1, \dots, n\}$, но $k_{s-1} \neq k_l$ в силу выбора l . \square

Итак, на множестве $\{k_0, k_1, \dots, k_l\}$ подстановка σ действует как

$$\begin{pmatrix} k_0 & k_1 & \dots & k_{l-1} & k_l \\ k_1 & k_2 & \dots & k_l & k_0 \end{pmatrix}$$

Выберем теперь произвольное число $j, 1 \leq j \leq n$, причем $j \notin \{k_0, k_1, \dots, k_l\}$. Как и выше строим множество $\{j_0, j_1, \dots, j_t\}$, на котором подстановка σ действует как цикл

$$\begin{pmatrix} j_0 & j_1 & \dots & j_{t-1} & j_t \\ j_1 & j_2 & \dots & j_t & j_0 \end{pmatrix}$$

ЛЕММА 1.18. *Все элементы $k_0, k_1, \dots, k_l, j_0, j_1, \dots, j_t$ различны.*

ДОКАЗАТЕЛЬСТВО. Пусть $j_r = k_q$. Тогда

$$j_0 = \sigma^{-r} j_r \in \{k_0, k_1, \dots, k_l\},$$

что невозможно. \square

Продолжая этот процесс, получаем подстановку

$$\tau = \begin{pmatrix} k_0 & k_1 & \dots & k_{l-1} & k_l \\ k_1 & k_2 & \dots & k_l & k_0 \end{pmatrix} \begin{pmatrix} j_0 & j_1 & \dots & j_{t-1} & j_t \\ j_1 & j_2 & \dots & j_t & j_0 \end{pmatrix} \dots$$

Непосредственная проверка показывает, что $\tau = \sigma$. \square

ПРЕДЛОЖЕНИЕ 1.19. *Пусть $\pi \in S_n$ и (i_1, \dots, i_k) — цикл из S_n . Тогда*

$$\pi(i_1, \dots, i_k)\pi^{-1} = (\pi(i_1), \dots, \pi(i_k)).$$

ДОКАЗАТЕЛЬСТВО. Непосредственная проверка. \square

ОПРЕДЕЛЕНИЕ 1.20. *Транспозицией* называется цикл длины 2.

ТЕОРЕМА 1.21. *Каждая перестановка является произведением транспозиций.*

ДОКАЗАТЕЛЬСТВО. $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$. \square

ОПРЕДЕЛЕНИЕ 1.22. Пусть i_1, \dots, i_n — последовательность различных чисел из X_n . *Инверсией* в этой последовательности называется такая пара i_s, i_t , что $s < t$ и $i_s > i_t$. *Знаком* последовательности называется число $(-1)^M$, где M — число инверсий в последовательности. Если подстановка $\sigma \in S_n$ имеет двустрочную запись (1), где $i_1 = 1, \dots, i_n = n$, то *знак* $(-1)^{\text{sigma}}$ перестановки σ равен знаку последовательности из второй строки.

СЛЕДСТВИЕ 1.23. Если подстановка разложена в произведение s транспозиций, то ее знак равен $(-1)^s$. В частности, знак цикла длины k равен $(-1)^{k-1}$.

ДОКАЗАТЕЛЬСТВО. Нужно воспользоваться теоремой 1.21. \square

ОПРЕДЕЛЕНИЕ 1.24. Перестановка *четна*, если она имеет знак 1, в противном случае она *нечетна*. Через A_n обозначается множество всех четных перестановок из S_n .

ТЕОРЕМА 1.25. $|S_n| = n!$, $|A_n| = \frac{n!}{2}$.

ДОКАЗАТЕЛЬСТВО. Отображение $\sigma \mapsto \sigma(1, 2)$ переводит A_n в $S_n \setminus A_n$ и наоборот. \square

2. Подгруппы

ОПРЕДЕЛЕНИЕ 1.26. Непустое подмножество H в группе G называется *подгруппой*, если вместе с любыми двумя его элементами оно содержит их произведение, и с каждым своим элементом H содержит его обратный.

ПРЕДЛОЖЕНИЕ 1.27. Если H – подгруппа в группе G и 1 – единичный элемент G , то $1 \in H$.

УПРАЖНЕНИЕ 1.28. В произвольной группе произведение любого числа элементов не зависит от расстановки скобок.

ПРЕДЛОЖЕНИЕ 1.29. Для непустого подмножества H в группе G следующие условия эквивалентны:

1. H является подгруппой в G ;
2. если $x, y \in H$, то $xy^{-1} \in H$.

ДОКАЗАТЕЛЬСТВО. Пусть выполнено условие (1), и $x, y \in H$. В силу определения 1.26 получаем $x, y^{-1} \in H$, откуда $xy^{-1} \in H$, т. е. выполнено условие (2).

Обратно, пусть выполнено условие (2), и $y \in H$. Тогда $y, y \in H$, откуда $1 = yy^{-1} \in H$ по (2). Далее $1, y \in H$, откуда $y^{-1} = 1y^{-1} \in H$ по (2). Наконец, если $x, y \in H$, то $x, y^{-1} \in H$ по доказанному выше. Отсюда $x(y^{-1})^{-1} = xy \in H$ по предложению 1.4. \square

ПРИМЕРЫ 1.30. Приведем примеры групп и их подгрупп:

1. группа S_n содержит подгруппы A_n, S_{n-1} ;
2. группа $GL(n, \mathbb{C})$ содержит подгруппы

$$\begin{aligned} &GL(n, \mathbb{R}), \quad GL(n, \mathbb{Q}), \quad SL(n, \mathbb{C}), \quad SL(n, \mathbb{R}), \quad O(n, \mathbb{R}), \\ &SO(n, \mathbb{R}) = SL(n, \mathbb{R}) \cap O(n, \mathbb{R}), \quad U(n, \mathbb{C}), \\ &SU(n, \mathbb{C}) = SL(n, \mathbb{C}) \cap U(n, \mathbb{C}); \end{aligned}$$

3. группа $*$ содержит подгруппы $U = U(1, \mathbb{C}), U_n = \{z \in \mathbb{C} | z^n = 1\}$;
4. группа диэдра $D_n, n \geq 3$, состоящая из всех движений \mathbb{R}^2 , переводящих правильный n -угольник в себя.

УПРАЖНЕНИЕ 1.31. Если $H_i, i \in I$ – подгруппы группы G , то $\bigcap_{i \in I} H_i$ – подгруппа группы G .

3. Порядки элементов группы

ОПРЕДЕЛЕНИЕ 1.32. Пусть a – элемент группы G . Для произвольного целого числа n положим

$$a^n = \begin{cases} 1, & \text{если } n = 0; \\ \underbrace{a \cdot \dots \cdot a}_n, & \text{если } n > 0; \\ (a^{-n})^{-1}, & \text{если } n < 0. \end{cases}$$

ПРЕДЛОЖЕНИЕ 1.33. Пусть a – элемент некоторой группы и $n, m \in \mathbb{Z}$. Тогда

$$a^{n+m} = a^n a^m, \quad (a^n)^m = a^{nm}.$$

ОПРЕДЕЛЕНИЕ 1.34. Пусть a – элемент некоторой группы. Порядком $|a|$ (или $o(a)$) элемента a называется такое наименьшее натуральное число n , что $a^n = 1$. Если такого числа n нет, то говорят, что порядок a равен бесконечности.

ПРЕДЛОЖЕНИЕ 1.35. Пусть $|a| = n < \infty$, и $m \in \mathbb{Z}$. Следующие условия эквивалентны:

1. $n|m$ (n делит m);
2. $a^m = 1$.

ОПРЕДЕЛЕНИЕ 1.36. Пусть $a \in G$. Через $\langle a \rangle$ обозначим множество $\{a^n | n \in \mathbb{Z}\}$ всех степеней элемента a .

УПРАЖНЕНИЕ 1.37. $\langle a \rangle$ является подгруппой в G .

4. Циклические группы и их подгруппы

ОПРЕДЕЛЕНИЕ 1.38. Пусть $a \in G$. Подгруппа $\langle a \rangle$ называется *циклической* подгруппой в группе G , порожденной элементом a . Группа G называется *циклической с порождающим (образующим) элементом a* , если $\langle a \rangle = G$.

ПРИМЕРЫ 1.39. Доказать, что

1. группа \mathbb{Z} является циклическая с порождающим элементом 1 (или -1);
2. группа U_n комплексных корней n -ой степени из 1 является циклической группой с порождающим элементом

$$\exp \frac{2\pi i}{n} = \cos \frac{2\pi i}{n} + i \sin \frac{2\pi i}{n}.$$

ПРЕДЛОЖЕНИЕ 1.40. Пусть a – элемент некоторой группы. Тогда $|\langle a \rangle| = |a|$.

ДОКАЗАТЕЛЬСТВО. Если $a^r = a^m$ при некоторых $r < m$, то $a^{m-r} = 1$ и $|a| = n < \infty$. В этом случае $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$. \square

ОБОЗНАЧЕНИЕ 1.41. Если $|a| = n$ в условии предложения 1.40, то циклическую группу, порожденную элементом a , мы будем обозначать $\langle a \rangle_n$.

ТЕОРЕМА 1.42. Подгруппа циклической группы сама является циклической.

ДОКАЗАТЕЛЬСТВО. Пусть H – подгруппа циклической группы $G = \langle a \rangle$. Если $H = 1$, то утверждение очевидно. Пусть H содержит неединичный элемент a^m , $m \neq 0$. Если $m < 0$, то H содержит и элемент a^{-m} , $-m > 0$. Выберем такое наименьшее натуральное число m , что $b = a^m \in H$. Если $a^r \in H$, $r \in \mathbb{Z}$, то, деля r с остатком на m , получаем $r = sm + q$, $0 \leq q < m$. При этом $a^q = a^{r-sm} = a^r(a^m)^{-s} \in H$ по предложению 1.33, что противоречит выбору m , если $q > 0$. \square

СЛЕДСТВИЕ 1.43. Пусть $m_1, \dots, m_n \in \mathbb{Z}$, и d – число m_1, \dots, m_n . Тогда существуют такие целые числа $u_1, \dots, u_n \in \mathbb{Z}$, что $m_1u_1 + \dots + m_nu_n = d$.

ДОКАЗАТЕЛЬСТВО. Пусть $H = \mathbb{Z}m_1 + \dots + \mathbb{Z}m_n$. Тогда H – подгруппа в \mathbb{Z} , и, следовательно, $H = \mathbb{Z}d$. Остается убедиться, что $d = (m_1, \dots, m_n)$. \square

ТЕОРЕМА 1.44. Пусть $G = \langle a \rangle_n$ и H – подгруппа в G . Тогда существует и притом единственное такое число d , делящее n , что $H = \langle a^d \rangle_{\frac{n}{d}}$.

ДОКАЗАТЕЛЬСТВО. По теореме 1.42 получаем $H = \langle a^k \rangle$ для некоторого $0 \leq k < n$. Положим $d = (n, k)$. Остается заметить, что $H = \langle a^d \rangle$. \square

УПРАЖНЕНИЕ 1.45. Описать все подгруппы в $\langle a \rangle_{12}$.

5. Смежные классы и теорема Лагранжа

ОПРЕДЕЛЕНИЕ 1.46. Пусть H – подгруппа в группе G , и $g \in G$. *Левым смежным классом* gH называется подмножество $\{gh | h \in H\}$ в G .

УПРАЖНЕНИЕ 1.47. Найти

1. левые смежные классы $\text{GL}(n, \mathbb{C})$ по $\text{SL}(n, \mathbb{C})$;
2. левые смежные классы \mathbb{Z} по $n\mathbb{Z}$;
3. левые и правые смежные классы S_n по S_{n-1} .

УПРАЖНЕНИЕ 1.48. Пусть H – подгруппа в группе G и $x, y \in G$. Доказать, что следующие условия эквивалентны:

1. $xH = yH$;
2. $x^{-1}y \in H$.

ПРЕДЛОЖЕНИЕ 1.49. Пусть H – подгруппа в группе G и $x \in G$. Тогда $|H| = |xH|$.

ПРЕДЛОЖЕНИЕ 1.50. Пусть H – подгруппа в группе G и $x, y \in G$, причем $y \in xH$. Тогда $xH = yH$.

ДОКАЗАТЕЛЬСТВО. Ясно, что $yH \subseteq xH$. По условию $y = xh$ для некоторого $h \in H$. Следовательно, для любого $u \in H$ получаем $xu = y(h^{-1}u)$, где $h^{-1}u \in H$. Отсюда $xH \subseteq yH$, т. е. $xH = yH$. \square

СЛЕДСТВИЕ 1.51. Пусть H – подгруппа в группе G . Тогда два левых (правых) смежных класса G по H либо совпадают, либо не пересекаются.

ДОКАЗАТЕЛЬСТВО. Воспользоваться предложением 1.50. \square

ТЕОРЕМА 1.52 (Теорема Лагранжа). Пусть H – подгруппа в конечной группе G . Тогда $|G| = |H|j$, где j – число левых (правых) смежных классов G по H .

ДОКАЗАТЕЛЬСТВО. Разобьем G на левые смежные классы по H . Тогда каждый элемент $x \in G$ лежит в некотором классе, именно, в xH . Остается воспользоваться следствием 1.51 и предложением 1.49 \square

СЛЕДСТВИЕ 1.53. *Порядок элемента конечной группы делит порядок группы.*

СЛЕДСТВИЕ 1.54. *Группа простого порядка является циклической.*

6. Гомоморфизмы, нормальные подгруппы, факторгруппы

ОПРЕДЕЛЕНИЕ 1.55. Отображение групп $f : G \rightarrow H$ называется *гомоморфизмом*, если $f(xy) = f(x)f(y)$ для всех $x, y \in G$. Инъективный гомоморфизм называется *мономорфизмом*. Сюръективный гомоморфизм называется *эпиморфизмом*. Биъективный гомоморфизм называется *изоморфизмом*. Изоморфизм группы на себя называется *автоморфизмом*.

ПРИМЕРЫ 1.56. Примеры гомоморфизмов:

1. $\det : \text{GL}(n, \mathbb{C}) \rightarrow \mathbb{C}^*$;
2. знак подстановки $\sigma : S_n \rightarrow \{\pm 1\}$.

УПРАЖНЕНИЕ 1.57. Если g – фиксированный элемент группы G , то отображение $x \mapsto gag^{-1}$ является автоморфизмом группы G .

ОПРЕДЕЛЕНИЕ 1.58. Автоморфизм из упражнения 1.57 называется *внутренним*. Он также называется *сопряжением с помощью g* .

ПРЕДЛОЖЕНИЕ 1.59. Пусть $f : G \rightarrow H$ – гомоморфизмом. Тогда $f(1) = 1$ и $f(x^{-1}) = f(x)^{-1}$ для всех $x \in G$.

УПРАЖНЕНИЕ 1.60. Пусть $f : G \rightarrow H$ – гомоморфизм групп. Доказать, что

1. если G_1 – подгруппа в G , то $f(G_1)$ является подгруппой в H ;
2. если $g : H \rightarrow F$ – гомоморфизм групп, то $gf : G \rightarrow F$ также является гомоморфизмом групп.

ОПРЕДЕЛЕНИЕ 1.61. Подгруппа H в группе G называется *нормальной*, если $xHx^{-1} \subseteq H$ для любого $x \in G$. Если H – нормальная подгруппа в группе G , то пишут $H \triangleleft G$.

ПРЕДЛОЖЕНИЕ 1.62. Пусть H – подгруппа в группе G . Тогда следующие условия эквивалентны:

1. подгруппа H нормальна в G ;
2. $xHx^{-1} = H$ для любого $x \in G$;
3. каждый левый смежный класс G по H является правым смежным классом;
4. каждый правый смежный класс G по H является левым смежным классом.

ДОКАЗАТЕЛЬСТВО. Пусть выполнено условие (1) и $x \in G$. Тогда

$$x^{-1}H(x^{-1})^{-1} = x^{-1}Hx \subseteq H,$$

откуда $H \subseteq xHx^{-1}$ и поэтому $xHx^{-1} = H$ в силу (1).

Пусть теперь выполнено (2). Тогда $xH = xHx^{-1}x = Hx$, т. е. выполнено (3).

Предположим теперь, что выполнено (3), и рассмотрим левый смежный класс xH . По условию он является правым смежным классом, содержащим x , т. е. $xH = Hx$ по предложению 1.50. Отсюда вытекает (2), и, следовательно, (1).

Итак, первые три условия эквивалентны. Аналогично показывается, что четвертое условие эквивалентно второму. \square

ОПРЕДЕЛЕНИЕ 1.63. Пусть $f : G \rightarrow H$ – гомоморфизм групп. *Ядром* $\ker f$ называется множество всех таких $x \in G$, что $f(x) = 1$.

ПРЕДЛОЖЕНИЕ 1.64. $\ker f \triangleleft G$.

ПРИМЕРЫ 1.65. Доказать, что

1. $A_n \triangleleft S_n$;
2. $\mathrm{SL}(n, \mathbb{C}) \triangleleft \mathrm{GL}(n, \mathbb{C})$;
3. $V_4 \triangleleft S_4$, $S_3 \not\triangleleft S_4$.

УПРАЖНЕНИЕ 1.66. Пусть $f : G \rightarrow H$ – гомоморфизм групп. Доказать, что отображение f инъективно $\iff \ker f = 1$.

ПРЕДЛОЖЕНИЕ 1.67. Пусть $f : G \rightarrow H$ – гомоморфизм групп и $x \in G$. Тогда $f^{-1}(f(x)) = x \ker f$.

ДОКАЗАТЕЛЬСТВО. Заметим, что в силу упражнения 1.48

$$\begin{aligned} y \in f^{-1}(f(x)) &\iff f(y) = f(x) \iff f(x^{-1}y) = 1 \\ &\iff x^{-1}y \in \ker f \iff x \ker f = y \ker f. \end{aligned}$$

Отсюда вытекает утверждение \square

ТЕОРЕМА 1.68. Пусть $\mathrm{Symm} T$ – группа симметрий тетраэдра T . Тогда $\mathrm{Symm} T \simeq S_4$.

ДОКАЗАТЕЛЬСТВО. Пусть 1, 2, 3, 4 – номера вершин в T . Если $g \in \mathrm{Symm} T$, то $g(1), g(2), g(3), g(4)$ – все вершины T . Зададим $f : \mathrm{Symm} T \rightarrow S_4$, полагая

$$f(g) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ g(1) & g(2) & g(3) & g(4) \end{pmatrix}.$$

Нетрудно убедиться, что g является эпиморфизмом и $\ker f = 1$. \square

Построение *факторгруппы* G/H , где $H \triangleleft G$. Построение *естественного гомоморфизма* $\pi : G \rightarrow G/N$.

УПРАЖНЕНИЕ 1.69. Если $\pi : G \rightarrow G/N$ – естественный гомоморфизм, то $\ker \pi = N$.

ТЕОРЕМА 1.70 (Теорема о гомоморфизмах). Пусть $f : G \rightarrow H$ – гомоморфизм групп. Тогда $G/\ker f \simeq f(G)$.

ДОКАЗАТЕЛЬСТВО. Пусть $x \in G$. По предложению 1.67 получаем, что $f^{-1}(f(x)) = x \ker f$. Зададим теперь отображение $\zeta : f(G) \rightarrow G/\ker f$ по правилу

$$\zeta(f(x)) = f^{-1}(f(x)) = x \ker f.$$

Проверим, что ζ является гомоморфизмом групп. Пусть $x, y \in G$. Тогда $xy \in f^{-1}(f(xy))$, т. е.

$$\zeta(f(xy)) = xy(\ker f) = (x \ker f)(y \ker f) = \zeta(f(x))\zeta(f(y)).$$

Итак, ζ является гомоморфизмом.

Убедимся, что ζ инъективно. Пусть $g, h \in f(G)$ и $\zeta(g) = \zeta(h)$. По определению $g = f(x), h = f(y)$ для некоторых $x, y \in G$. Отсюда $x \ker f = y \ker f$, и поэтому $g = f(x) = f(y) = h$.

Убедимся, что ζ сюръективно. Если $x \in G$, то $x \ker f = \zeta(f(x))$. Итак, ζ – изоморфизм. \square

ПРИМЕРЫ 1.71. Доказать, что

1. $\text{GL}(n, \mathbb{C}) / \text{SL}(n, \mathbb{C}) \simeq \mathbb{C}^*$;
2. $S_n / A_n \simeq \{\pm 1\}$;
3. $\mathbb{Z} / n\mathbb{Z} \simeq U_n$.

7. Классы сопряженных элементов

ОПРЕДЕЛЕНИЕ 1.72. Два элемента x, y группы G сопряжены, если существует такой элемент $g \in G$, что $x = gyg^{-1}$. Классом сопряженных элементов в G называется множество всех сопряженных между собой элементов из G .

ПРЕДЛОЖЕНИЕ 1.73. *Два класса сопряженных элементов либо совпадают, либо не пересекаются.*

ДОКАЗАТЕЛЬСТВО. Пусть X, Y – два класса сопряженных элементов в G . Предположим, что $x \in X \cap Y$. Если $z \in X$, то $z = gxg^{-1}$ для некоторого элемента $g \in G$. Если $y \in Y$, то $y = h x h^{-1}$ для некоторого $h \in G$. Отсюда $z = (gh^{-1})y(gh^{-1})^{-1}$. Таким образом, $X \subseteq Y$. Аналогично, $Y \subseteq X$. \square

СЛЕДСТВИЕ 1.74. *Разные классы сопряженных элементов не пересекаются.*

ОПРЕДЕЛЕНИЕ 1.75. Пусть $x \in G$. Центризатором $C(x)$ называется множество всех таких элементов $g \in G$, что $gx = xg$.

ПРЕДЛОЖЕНИЕ 1.76. *Существует биекция между классом сопряженных элементов, содержащих x и множеством левых смежных классов G по $C(x)$.*

ДОКАЗАТЕЛЬСТВО. Пусть $g \in G$. Сопоставим элементу gxg^{-1} класс $gC(x)$. \square

СЛЕДСТВИЕ 1.77. *Пусть K – класс сопряженных элементов в группе G , содержащий элемент x . Тогда $|K| = \frac{|G|}{|C(x)|}$.*

По теореме 1.16 каждая подстановка из S_n разлагается в произведение независимых циклов.

УПРАЖНЕНИЕ 1.78. Доказать, что

1. если $\sigma = \sigma_1 \cdots \sigma_m$ – разложение перестановки $\sigma \in S_n$ в произведение независимых циклов, то $|\sigma|$ равен наибольшему общему делителю длин $\sigma_1, \dots, \sigma_m$;
2. два независимых цикла из S_n перестановочны.

ТЕОРЕМА 1.79. *Две перестановки из S_n сопряжены тогда и только тогда, когда они имеют одинаковое цикловое строение.*

ДОКАЗАТЕЛЬСТВО. Для доказательства необходимости нужно воспользоваться предложением 1.19. Обратное, пусть подстановки σ, τ имеют одинаковое цикловое строение, т. е.

$$\begin{aligned}\sigma &= (k_0, k_1, \dots, k_l)(j_0, j_1, \dots, j_t) \cdots, \\ \tau &= (k'_0, k'_1, \dots, k'_l)(j'_0, j'_1, \dots, j'_t) \cdots.\end{aligned}$$

По предложению 1.19 имеем $\pi\sigma\pi^{-1} = \tau$, где

$$\pi = \begin{pmatrix} k_0 & k_1 & \dots & k_l & j_0 & j_1 & \dots & j_t & \dots \\ k'_0 & k'_1 & \dots & k'_l & j'_0 & j'_1 & \dots & j'_t & \dots \end{pmatrix}.$$

□

УПРАЖНЕНИЕ 1.80. Доказать, что две матрицы из $\text{GL}(n, \mathbb{C})$ сопряжены (подобны) тогда и только тогда, когда они имеют одинаковые жордановы формы.

ТЕОРЕМА 1.81. Пусть $U \in \text{U}(n, \mathbb{C})$. Тогда матрица U сопряжена в $\text{U}(n, \mathbb{C})$ диагональной матрице $\text{diag}(\lambda_1, \dots, \lambda_n)$, где $|\lambda_j| = 1$.

ДОКАЗАТЕЛЬСТВО. Нам потребуется

ЛЕММА 1.82. Пусть U – унитарный (ортогональный) линейный оператор в эрмитовом (евклидовом) пространстве L , и W – инвариантное подпространство. Тогда W^\perp инвариантно относительно U .

Воспользуемся этой леммой для доказательства теоремы. Пусть U – унитарный линейный оператор в эрмитовом пространстве L . Достаточно показать, что в U имеется собственный ортонормированный базис. Оператор U имеет собственный вектор e_1 с собственным значением λ_1 , причем можно считать, что $\|e_1\| = 1$. Тогда $\langle e_1 \rangle^\perp$ инвариантно относительно U . По индукции в $\langle e_1 \rangle$ существует искомый базис e_2, \dots, e_n . □

ТЕОРЕМА 1.83. Пусть $U \in \text{O}(n, \mathbb{R})$. Тогда матрица U сопряжена в $\text{O}(n, \mathbb{R})$ блочно-диагональной матрице с блоками размера не больше 2. Блоки размера 1 имеют вид ± 1 . Блоки размера 2 имеют вид

$$\begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix}. \quad (2)$$

ДОКАЗАТЕЛЬСТВО. Нам потребуется

ЛЕММА 1.84. Пусть U линейный оператор в вещественном пространстве L . Тогда он имеет одномерное или двумерное инвариантное подпространство.

ЛЕММА 1.85. Пусть Q – ортогональная (2×2) -матрица, не имеющая вещественного собственного значения. Тогда Q имеет вид (2).

Воспользуемся этими леммами для доказательства теоремы. Пусть U – ортогональный линейный оператор в евклидовом пространстве L . Если оператор U имеет собственный вектор e_1 с собственным значением λ_1 , то $|\lambda_1| = 1$ и дальше нужно повторить доказательство предыдущей теоремы.

Пусть U имеет двумерное инвариантное подпространство W , в котором нет собственного вектора. Тогда в любом ортонормированном базисе W матрица $U|_W$ имеет вид (2). При этом W^\perp инвариантно относительно U . Соображения индукции завершают доказательство. □

СЛЕДСТВИЕ 1.86. Пусть $Q \in O(2, \mathbb{R})$. Если $\det Q = 1$, то Q имеет вид (2). Если $\det Q = -1$, то Q сопряжена в $O(2, \mathbb{R})$ матрице $\text{diag}(1, -1)$.

СЛЕДСТВИЕ 1.87. Пусть $Q \in O(3, \mathbb{R})$. Тогда Q сопряжена в $O(2, \mathbb{R})$ матрице

$$\begin{pmatrix} \det Q & 0 & 0 \\ 0 & \cos \phi & -\sin \phi \\ 0 & \sin \phi & \cos \phi \end{pmatrix}.$$

8. Коммутант группы

ОПРЕДЕЛЕНИЕ 1.88. Пусть x, y — элементы группы G . Коммутатором элементов x, y называется элемент $[x, y] = xyx^{-1}y^{-1}$.

ПРИМЕРЫ 1.89. Доказать, что

1. в группе перестановок S_n $[(i, j), (j, k)] = (i, k, j)$, если индексы i, j, k различны;
2. в группе матриц $\text{GL}(n, k)$, где k — кольцо, $[1 + aE_{ik}, 1 + bE_{kj}] = 1 + abE_{ij}$, если индексы i, j, k различны.

ПРИМЕРЫ 1.90. ОПРЕДЕЛЕНИЕ 1.91. Коммутантом $G' = [G, G]$ называется множество всех произведений коммутаторов в G .

ПРЕДЛОЖЕНИЕ 1.92. $G' \triangleleft G$.

ПРЕДЛОЖЕНИЕ 1.93. Если $N \triangleleft G$, то следующие условия эквивалентны:

1. группа G/N — абелева;
2. $N \supseteq G'$.

ТЕОРЕМА 1.94. $S'_n = A_n$.

ДОКАЗАТЕЛЬСТВО. Нужно воспользоваться примером 1.89. □

ТЕОРЕМА 1.95. Если $n \geq 3$, и k — поле, то $\text{GL}(n, k)' = \text{SL}(n, k)' = \text{SL}(n, k)$.

УПРАЖНЕНИЕ 1.96. Доказать, что

1. если поле k содержит не менее четырех элементов, то

$$\text{GL}(2, k)' = \text{SL}(2, k);$$

именно, если существует такой элемент $q, q - 1 \in k^*$, то

$$\left[\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & (q-1)^{-1}a \\ 0 & 1 \end{pmatrix} \right] = 1 + aE_{12};$$

2. $\text{GL}(2, \mathbb{F}_2) \simeq S_3$, и поэтому $\text{GL}(2, \mathbb{F}_2)' \neq \text{SL}(2, \mathbb{F}_2) = \text{GL}(2, \mathbb{F}_2)$.

УПРАЖНЕНИЕ 1.97. Вычислить $\text{GL}(2, \mathbb{F}_3)'$.

ПРИМЕРЫ 1.98. $A'_4 = V_4$, и $A'_n = A_n$, если $n \geq 5$.

ОПРЕДЕЛЕНИЕ 1.99. Если G — группа, то положим $G^{(1)} = G'$ и $G^{(k+1)} = [G^{(k)}, G^{(k)}]$. Группа G разрешима, если существует такое натуральное число m , что $G^{(m)} = 1$.

ЗАМЕЧАНИЕ 1.100. Для любых $m, n > 0$ верно равенство $(G^{(n)})^{(m)} = G^{(n+m)}$.

ПРЕДЛОЖЕНИЕ 1.101. Пусть $f : G \rightarrow H$ — гомоморфизм групп. Тогда $f(G^{(k)}) \subseteq H^{(k)}$. Если f — сюръективно, то $f(G^{(k)}) = H^{(k)}$.

УПРАЖНЕНИЕ 1.102. Доказать, что

1. если H – подгруппа в группе G , то $H^{(k)} \subseteq G^{(k)}$ для любого натурального числа k ;
2. $G^{(k)} \triangleleft G$ для любого натурального числа k .

ПРЕДЛОЖЕНИЕ 1.103. Пусть $N \triangleleft G$. Следующие условия эквивалентны:

1. группы G разрешима;
2. группы G/N , и N разрешимы.

ДОКАЗАТЕЛЬСТВО. Воспользоваться предложением 1.101 □

ПРЕДЛОЖЕНИЕ 1.104. Для группы G следующие условия эквивалентны:

1. группы G разрешима;
2. существует такой ряд подгруппы

$$G = G_0 \supset G_1 \supset \cdots \supset G_{k-1} \supset G_k = 1,$$

что $G_{i+1} \triangleleft G_i$ и G_i/G_{i+1} – абелево для всех i .

ДОКАЗАТЕЛЬСТВО. Нужно воспользоваться предложением 1.103 и индукцией по k , убедившись, что группа G_1 разрешима. □

ПРЕДЛОЖЕНИЕ 1.105. Пусть

$$A, A' \in \text{Mat}(t, k), \quad B, B' \in \text{Mat}(t \times s, k), \quad C, C' \in \text{Mat}(s, k).$$

Тогда

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \begin{pmatrix} A' & B' \\ 0 & C' \end{pmatrix} = \begin{pmatrix} AA' & AB' + BC' \\ 0 & CC' \end{pmatrix}$$

ОПРЕДЕЛЕНИЕ 1.106. Группа *верхнетреугольных* матриц $T(n, k)$, k – поле. Группа *верхнеунитреугольных* матриц $UT(n, k)$, k – поле.

СЛЕДСТВИЕ 1.107. Рассмотрим отображение $\varphi : T(n, k) \rightarrow T(n-1, k)$ по правилу: если

$$X = \left(\begin{array}{c|c} A & B \\ \hline 0 & c \end{array} \right) \in T(n, k), \quad \text{где } A \in T(n-1, k), B \in \text{Mat}((n-1) \times 1, k), c \in k^*,$$

то $\varphi(X) = A$. Тогда φ является гомоморфизмом групп, причем $\varphi(UT(n, k)) = UT(n-1, k)$.

ПРЕДЛОЖЕНИЕ 1.108. $T(n, k)' \subset UT(n, k)$

ДОКАЗАТЕЛЬСТВО. Воспользоваться предложением 1.93. □

ТЕОРЕМА 1.109. Группа $T(n, k)$ разрешима.

ДОКАЗАТЕЛЬСТВО. По предложениям 1.108 и 1.103 достаточно показать, что группа $UT(n, k)$ разрешима. Будем вести доказательство индукцией по n . Если $n = 1$, то $UT(1, k) = 1$ и потому разрешима.

Пусть для $n-1$ теорема доказана. Рассмотрим гомоморфизм групп $\varphi : UT(n, k) \rightarrow UT(n-1, k)$ из следствия 1.107. Заметим, что

$$\ker \varphi = \left\{ \left(\begin{array}{c|c} E & B \\ \hline 0 & 1 \end{array} \right) \in UT(n, k), \quad \text{где } B \in \text{Mat}((n-1) \times 1, k) \right\}.$$

По предложению 1.105 получаем, что $\ker \varphi$ – абелева группа. Остается воспользоваться индукцией и следствием 1.103 с $N = \ker \varphi$. □

9. Прямые произведения групп

ОПРЕДЕЛЕНИЕ 1.110. Группы G является (внутренним) прямым произведением своих подгрупп G_1, \dots, G_n , (обозначение $G = G_1 \times \dots \times G_n$) если:

- ♡ каждая подгруппа G_i нормальна в G ;
- ♡ каждый элемент $g \in G$ имеет и притом единственное представление в виде произведения $g = g_1 \cdots g_n$, где $g_i \in G_i$.

Если G – группа относительно сложения, то говорят, что G является *прямой суммой* своих подгрупп G_1, \dots, G_n , и пишут $G = G_1 \oplus \dots \oplus G_n$.

УПРАЖНЕНИЕ 1.111. Доказать, что $|G| = |G_1| \cdots |G_n|$.

ПРЕДЛОЖЕНИЕ 1.112. Пусть $G = G_1 \times \dots \times G_n$ и $g_i \in G_i, g_j \in G_j$, где $i \neq j$. Тогда $g_i g_j = g_j g_i$.

СЛЕДСТВИЕ 1.113. Пусть $G = G_1 \times \dots \times G_n$ и $g = g_1 \cdots g_n, h = h_1 \cdots h_n$, где $g_i, h_i \in G_i$ для всех i . Тогда

$$gh = (g_1 h_1) \cdots (g_n h_n), \quad g^{-1} = g_1^{-1} \cdots g_n^{-1}.$$

ПРИМЕРЫ 1.114. Имеются следующие прямые разложения:

1. группа $\mathbb{C}^* \simeq U \times \mathbb{R}_+^*$;
2. $\mathbb{R}^n = \mathbb{R}^k \oplus \mathbb{R}^{n-k}$.

ПРЕДЛОЖЕНИЕ 1.115. Группа \mathbb{Z} неразложима в прямую сумму.

ПРЕДЛОЖЕНИЕ 1.116. Пусть $G = G_1 \times \dots \times G_n$ и $g = g_1 \cdots g_n$. Тогда $|g| = (|g_1|, \dots, |g_n|)$.

ТЕОРЕМА 1.117. Пусть группа $G = G_1 \times \dots \times G_n$ конечна. Следующие условия эквивалентны:

- группа G циклическа;
- каждая группа G_i циклическа и порядки групп $G_i, i = 1, \dots, n$, попарно взаимно просты.

ДОКАЗАТЕЛЬСТВО. Пусть группа G циклическа, и $m_i = |G_i|$. Тогда каждая подгруппа $G_i, i = 1, \dots, n$, циклическа. Если, например, $(m_1, m_2) > 1$, то $(m_1, \dots, m_n) < m_1 \cdots m_n$. Поэтому в силу предложения 1.116 в G нет элемента порядка $m_1 \cdots m_n = |G|$.

Обратно, пусть $G_i = \langle a_i \rangle_{m_i}$, причем все числа m_1, \dots, m_n попарно взаимно просты. Рассмотрим элемент $a = a_1 \cdots a_n \in G$. По предложению 1.116 его порядок равен $m_1 \cdots m_n = |G_1| \cdots |G_n| = |G|$. Следовательно, $G = \langle a \rangle$. \square

СЛЕДСТВИЕ 1.118. Циклическая группа порядка d неразложима в прямое произведение тогда и только тогда, когда ее порядок является степенью простого числа.

ПРИМЕР 1.119. Прямое разложение циклической группа порядка 12.

ТЕОРЕМА 1.120. Пусть $N_i \triangleleft G_i, i = 1, \dots, m$. Тогда

$$(N_1 \times \dots \times N_m) \triangleleft (G_1 \times \dots \times G_m)$$

и $(G_1 \times \dots \times G_m) / (N_1 \times \dots \times N_m) \simeq (G_1 / N_1) \times \dots \times (G_m / N_m)$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим гомоморфизм групп

$$\pi : G \rightarrow (G_1/N_1) \times \cdots \times (G_m/N_m),$$

отображающий элемент

$$g = g_1 \cdots g_m \mapsto (g_1 N_1) \cdots (g_m N_m) \in (G_1/N_1) \times \cdots \times (G_m/N_m),$$

и воспользоваться теоремой о гомоморфизмах. \square

ОПРЕДЕЛЕНИЕ 1.121. Определение *внешнего прямого произведения* $G = G_1 \times \cdots \times G_m$.

ТЕОРЕМА 1.122. *Внешнее и внутреннее прямые произведения изоморфны.*

ГЛАВА 2

Конечно порожденные абелевы группы

В этой главе описывается строение конечно порожденных абелевых групп. Все абелевы группы будут предполагаться аддитивными.

ОПРЕДЕЛЕНИЕ 2.1. Элементы $\mathbf{e} = (e_1, \dots, e_n)$ являются *базисом* в абелевой группе A , если

♣ элементы из \mathbf{e} *независимы*, т. е. из того, что

$$m_1 e_1 + \dots + m_n e_n = 0, \text{ где } m_1, \dots, m_n \in \mathbb{Z},$$

следует, что $m_1 = \dots = m_n = 0$.

♠ элемент из \mathbf{e} *порождают* группу A , т. е. каждый элемент $x \in A$ представим в виде $x = m_1 e_1 + \dots + m_n e_n$.

Другими словами, каждый элемент $x \in A$ имеет и притом единственно представление в виде

$$x = m_1 e_1 + \dots + m_n e_n, \quad m_i \in \mathbb{Z}. \quad (3)$$

Группа A *свободна*, если она обладает базисом. *Рангом* свободной абелевой группы A называется число векторов в базисе A .

ПРЕДЛОЖЕНИЕ 2.2. Для абелевой группы A следующие условия эквивалентны:

1. группа A обладает базисом $\mathbf{e} = (e_1, \dots, e_n)$;
2. группа

$$A \simeq \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n.$$

ДОКАЗАТЕЛЬСТВО. Если \mathbf{e} – базис A , то зададим

$$\psi : A \rightarrow \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n$$

по правилу: если $x \in A$ имеет представление (3), то $\psi(x) = (m_1, \dots, m_n)$.

Обратно, группа

$$A = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n$$

обладает базисом $\mathbf{e} = (e_1, \dots, e_n)$, где

$$e_i = (0, \dots, \overset{i}{1}, 0, \dots, 0), \quad i = 1, \dots, n.$$

□

ПРЕДЛОЖЕНИЕ 2.3. Число векторов в базисе свободной абелевой группы определено однозначно. Другими словами, ранг свободной абелевой группы определен однозначно.

ДОКАЗАТЕЛЬСТВО. Пусть (e_1, \dots, e_n) и (f_1, \dots, f_m) – два базиса в A . Предположим, что $m > n$. Тогда каждое f_j имеет представление

$$f_j = \sum_{i=1}^n a_{ji} e_i, \quad a_{ji} \in \mathbb{Z}.$$

Строки матрицы $(a_{ji}) \in \text{Mat}(m \times n, \mathbb{Z})$ линейно зависимы над \mathbb{Q} . Следовательно, они линейно зависимы над \mathbb{Z} . Поэтому найдется такой ненулевой набор целых чисел $b_1, \dots, b_m \in \mathbb{Z}$, что

$$(b_1, \dots, b_m) \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = 0.$$

Отсюда $b_1 f_1 + \dots + b_m f_m = 0$, что противоречит независимости f_1, \dots, f_m . \square

УПРАЖНЕНИЕ 2.4. Пусть A – свободная абелева группа с базисом $\mathbf{e} = (e_1, \dots, e_n)$. Предположим, что c_1, \dots, c_n – элементы произвольной абелевой группы C . Тогда существует и притом единственный такой гомоморфизм $\psi : A \rightarrow C$, что $\psi(e_i) = c_i$, $1 \leq i \leq n$.

СЛЕДСТВИЕ 2.5. Пусть A – свободная абелева группа с базисом

$$\mathbf{e} = (e_1, \dots, e_n).$$

Тогда $|\text{hom}(A, \mathbb{Z}_2)| = 2^n$. В частности, в ранг A определен однозначно.

ТЕОРЕМА 2.6. Пусть A – свободная абелева группа ранга n . Если B – ненулевая подгруппа в A , то она свободна и ее ранг $\leq n$.

ДОКАЗАТЕЛЬСТВО. Будет вести доказательство индукцией по n . Если $n = 1$, то $A \simeq \mathbb{Z}$. Тогда группа A циклическа и, следовательно, по теореме 1.42 группа $B = \langle b \rangle$ циклическа, причем $b \neq 0$. Тогда элемент b является базисом B .

Пусть для $n - 1$ теорема доказана, и $\mathbf{e} = (e_1, \dots, e_n)$ – базис A . Положим

$$H = \left\{ \sum_{i=1}^{n-1} a_i e_i \mid a_i \in \mathbb{Z} \right\}.$$

Тогда H – свободная абелева группа с базисом (e_1, \dots, e_{n-1}) . По индукции $B \cap H$ – свободная абелева группа с базой (f_1, \dots, f_m) , $m \leq n - 1$. Следовательно, если $B \subseteq H$, то теорема доказана.

Пусть $B \not\subseteq H$. Рассмотрим такое наименьшее натуральное число d , что элемент $f = c_1 e_1 + \dots + c_{n-1} e_{n-1} + d e_n \in H$. Покажем, что элементы f_1, \dots, f_m, f составляют базис H . Действительно, если $b = u_1 e_1 + \dots + u_n e_n \in B$, $u_i \in \mathbb{Z}$, то $u_n = rd$ для некоторого $r \in \mathbb{Z}$. В самом деле, пусть $u_n = rd + l$, где $0 \leq l < d$. Тогда $b - rf = u'_1 e_1 + \dots + u'_{n-1} e_{n-1} + l e_n \in H$, что противоречит выбору d , если $l \neq 0$. Итак, $u_n = rd$ и $b - rf \in B \cap H$. Поэтому $b - rf = a_1 f_1 + \dots + a_m f_m$, $a_i \in \mathbb{Z}$. Таким образом, $b = rf + a_1 f_1 + \dots + a_m f_m$, $r, a_i \in \mathbb{Z}$, т. е. элементы

$$f, f_1, \dots, f_m \tag{4}$$

порождают B .

Покажем, что элементы (4) независимы. Пусть

$$rf + a_1 f_1 + \dots + a_m f_m = 0, \quad r, a_i \in \mathbb{Z}, \tag{5}$$

Коэффициент при e_n у элемента левой части (4) равен $rd = 0$, откуда $r = 0$, ибо $d \neq 0$. Таким образом, в (5) получаем, что $a_1f_1 + \dots + a_mf_m = 0$, откуда $a_1 = \dots = a_m = 0$, ибо элементы f_1, \dots, f_m независимы. \square

ОПРЕДЕЛЕНИЕ 2.7. *Целочисленные элементарные преобразования строк (столбцов) целочисленной матрицы состоят из двух типов преобразований:*

- умножение слева (справа) на элементарные матрицы $E + aE_{ij}$, $a \in \mathbb{Z}$,
- умножение строки (столбца) на -1 .

УПРАЖНЕНИЕ 2.8. Совершая целочисленные элементарные преобразования строк (столбцов) можно переставить любые две строки (столбца).

ТЕОРЕМА 2.9. *Пусть $A \in \text{Mat}(n \times m, \mathbb{Z})$. Целочисленными элементарными преобразованиями строк и столбцов можно A привести к диагональному виду $\text{diag}(d_1, d_2, \dots)$, $d_i \geq 0$.*

ДОКАЗАТЕЛЬСТВО. Можно считать, что $A = (a_{ij}) \neq 0$. Пусть

$$\delta(A) = \min_{ij} \{|a_{ij}| \mid a_{ij} \neq 0\}.$$

Предположим, что матрицу A целочисленными элементарными преобразованиями строк и столбцов привели в такому виду, что далее $\delta(A)$ уменьшить нельзя. Переставляя строки и столбцы и умножая, если необходимо, на -1 , можно считать, что $\delta(A) = a_{11}$.

ЛЕММА 2.10. a_{11} делит a_{1j} , a_{i1} для всех i, j .

ДОКАЗАТЕЛЬСТВО. Пусть, например, a_{11} не делит a_{21} , т. е. $a_{21} = qa_{11} + r$, где $0 < r < a_{11}$. Вычитая из второй строки первую, умноженную на q , получаем на месте (21) элемент r , что противоречит выбору $\delta(A) = a_{11}$. \square

По лемме 2.10 совершая элементарные преобразования строк и столбцов, можно добиться, чтобы $a_{1j} = a_{i1} = 0$ для всех $i, j > 1$. Доказательство теоремы завершается индукцией по размеру матрицы. \square

ТЕОРЕМА 2.11 (Теорема о согласованном базисе). *Пусть B – ненулевая подгруппа в свободной абелевой группе ранга n . Тогда в A существует такой базис $\mathbf{e} = (e_1, \dots, e_n)$ и такие натуральные числа d_1, d_2, \dots, d_k , $k \leq n$, что элементы d_1e_1, \dots, d_ke_k составляют базис B .*

ДОКАЗАТЕЛЬСТВО. Пусть f_1, \dots, f_n и g_1, \dots, g_k , $k \leq n$, – произвольные базисы в A и в B (см. теорему 2.6). Тогда

$$g_i = \sum_{j=1}^n a_{ij}f_j, \quad a_{ij} \in \mathbb{Z}, \quad i = 1, \dots, k.$$

Рассмотрим целочисленную матрицу $A = (a_{ij}) \in \text{Mat}(k \times n, \mathbb{Z})$. Целочисленные элементарные преобразования строк A соответствуют элементарным преобразованиям базиса g_1, \dots, g_k , а целочисленные элементарные преобразования столбцов A соответствуют элементарным преобразованиям базиса f_1, \dots, f_n . По теореме 2.9 изменяя оба базиса, можно считать, что $g_1 = d_1f_1, \dots, g_k = d_kf_k$. \square

ОПРЕДЕЛЕНИЕ 2.12. Абелева группа A *конечно порождена*, если существуют такие элементы $a_1, \dots, a_n \in A$, что каждый элемент $x \in A$ имеет представление $x = c_1 a_1 + \dots + c_n a_n, c_i \in \mathbb{Z}$.

ОПРЕДЕЛЕНИЕ 2.13. Циклическая группа *примарна*, если ее порядок является степенью простого числа.

ТЕОРЕМА 2.14 (Строение конечно порожденных абелевых групп). *Пусть A – конечно порожденная абелева группа. Тогда A разлагается в прямую сумму свободной абелевой группы и примарных циклических групп.*

ДОКАЗАТЕЛЬСТВО. Пусть $a_1, \dots, a_n \in A$ из определения 2.12. Рассмотрим свободную абелеву группу F ранга n , например,

$$F = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n$$

Выберем в F базис e_1, \dots, e_n и зададим гомоморфизм $\xi : F \rightarrow A$, при котором

$$\xi\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i a_i.$$

Нетрудно видеть, что ξ является эпиморфизмом. Пусть $B = \ker \xi$. По теореме 2.11 можно считать, что $d_1 e_1, \dots, d_k e_k$ составляют базис B , где d_1, \dots, d_k – натуральные числа, $k \leq n$. Положим

$$N_i = \begin{cases} \mathbb{Z} d_i e_i, & \text{если } 1 \leq i \leq k; \\ 0, & \text{если } k < i \leq n. \end{cases}$$

По теореме 1.70 о гомоморфизмах и по теореме 1.120 получаем

$$A \simeq F/B \simeq (\mathbb{Z} e_1/N_1) \oplus \dots \oplus (\mathbb{Z} e_n/N_n). \quad (6)$$

Если $1 \leq i \leq k$, то

$$\mathbb{Z} e_i/N_i = \mathbb{Z} e_i/\mathbb{Z} d_i e_i \simeq \mathbb{Z}/\mathbb{Z} d_i. \quad (7)$$

По теореме 1.117 группа (7) разлагается в прямую сумму примарных циклических групп.

Если $k < i \leq n$, то $N_i = 0$, и поэтому $\mathbb{Z} e_i/N_i \simeq \mathbb{Z}$. Итак, по (6) получаем, что $A \simeq (\oplus_i C_i) \oplus H$, где C_i – примарные циклические группы, и

$$H = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n-k}.$$

По предложению 2.2 группа H свободна. □

ОПРЕДЕЛЕНИЕ 2.15. Группа G *не имеет кручения*, если в ней нет нетривиальных, т. е. отличный от 1, элементов конечного порядка.

СЛЕДСТВИЕ 2.16. *Конечно порожденная абелева группа без кручения свободна.*

ОПРЕДЕЛЕНИЕ 2.17. Подгруппа $H \subseteq \mathbb{R}^n$ *дискретна, или решетка*, если существует такая окрестность нуля U , что $U \cap H = 0$.

ТЕОРЕМА 2.18. *Дискретная подгруппа в \mathbb{R}^n свободна.*

ДОКАЗАТЕЛЬСТВО. По следствию 2.16 достаточно показать, что группа H конечно порождена. Выберем в H максимальную линейно независимую систему векторов f_1, \dots, f_k , $k \leq n$. Положим $\Gamma = \{\sum_{i=1}^k \alpha_i f_i \mid 0 \leq \alpha_i \leq 1\}$. Тогда Γ является компактом, и, следовательно, $\Gamma \cap H$ конечно. Остается заметить, что H порождается $\Gamma \cap H, f_1, \dots, f_k$. \square

ТЕОРЕМА 2.19. Пусть G – дискретная подгруппа в \mathbb{R}^n , и $\mathbf{e} = (e_1, \dots, e_k)$ – ее базис. Тогда векторы из \mathbf{e} независимы в \mathbb{R}^n .

ДОКАЗАТЕЛЬСТВО. Пусть, например,

$$e_1 = \lambda_2 e_2 + \dots + \lambda_k e_k, \quad \lambda_i \in \mathbb{R}.$$

Положим

$$S = \{\alpha_2 e_2 + \dots + \alpha_k e_k \mid 0 \leq \alpha_j \leq 1, \quad j = 2, \dots, k\}.$$

Тогда S является компактом, и, следовательно, как и в предыдущей теореме, $S \cap G$ конечно.

Для любого натурального числа d получаем

$$de_1 = [d\alpha_2]e_2 + \dots + [d\alpha_k]e_k + (\beta_2 e_2 + \dots + \beta_k e_k),$$

где $\beta_2 e_2 + \dots + \beta_k e_k \in S \cap G$. Поэтому найдутся такие натуральные числа $d_1 > d_2$, что $d_1 e_1 - d_2 e_1$ лежит в подгруппе, порожденной e_2, \dots, e_k , т. е.

$$(d_1 - d_2)e_1 = m_2 e_2 + \dots + m_k e_k, \quad m_j \in \mathbb{Z}.$$

Это противоречит определению базиса в G . \square

УПРАЖНЕНИЕ 2.20. Пусть G – подгруппа в \mathbb{R} , порожденная $1, \sqrt{2}$. Будет ли она плотна в \mathbb{R} ?

Кристаллографические группы

1. Группы движений

ОПРЕДЕЛЕНИЕ 3.1. Преобразование Φ евклидова пространства E называется *движением*, если существует такой ортогональный линейный оператор ϕ и вектор b , что $\Phi(x) = \phi(x) + b$ для всех $x \in E$.

УПРАЖНЕНИЕ 3.2. Все движений евклидова пространства E образуют - группу $G(E)$ относительно операции композиции отображений.

УПРАЖНЕНИЕ 3.3. Доказать, что если Φ движение евклидова пространства E , то $\|\Phi(x) - \Phi(y)\| = \|x - y\|$ для всех $x, y \in E$.

Примерами движений являются *сдвиги* $\Phi(x) = x + b$ на фиксированный вектор $b \in E$ и ортогональные преобразования.

ТЕОРЕМА 3.4. Множество N всех сдвигов образует нормальную подгруппу в $G(E)$, причем $G(E)/N \simeq O(E)$, где $O(E)$ - группа всех ортогональных преобразований в E . Кроме того, $N \simeq E$.

ДОКАЗАТЕЛЬСТВО. Зададим отображение $\xi : G(E) \rightarrow O(E)$ по следующему правилу. Если $\Phi(x) = \phi(x) + b$ для всех $x \in E$, то положим $\xi(\Phi) = \phi$. Это определение корректно. Действительно, пусть $\Phi(x) = \phi(x) + b = \phi'(x) + b'$ для всех $x \in E$, где $b, b' \in E$ и $\phi, \phi' \in O(E)$. Тогда $\Phi(0) = b = b'$, откуда $\phi(x) = \phi'(x)$ для всех $x \in E$. Покажем теперь, что ξ является гомоморфизмом групп. Пусть Φ как и выше, $\Psi(x) = \psi(x) + d$. Тогда $\Phi[\Psi(x)] = \phi[\psi(x)] + \phi(d) + b$, и поэтому $\xi(\Phi\Psi) = \phi\psi = \xi(\Phi)\xi(\Psi)$. Более того, $\ker \xi = N$. Поэтому $N \triangleleft G(E)$ и $G(E)/N \simeq O(E)$.

Сопоставляя $\psi \in N$ вектор $\psi(0)$ получаем изоморфизм $N \simeq E$. □

ОПРЕДЕЛЕНИЕ 3.5. Кристаллографической или пространственной группой называется подгрупп Γ в группе движений $G(E)$ евклидова пространства E размерности n , причем

1. при отождествлении N с E образ L подгруппы $\Gamma \cap N$ является дискретной подгруппой (или решеткой) в E ранга n ;
2. $\Gamma \cap N$ имеет конечный индекс в Γ .

Конечная группа $\Delta = \Gamma/(\Gamma \cap N)$ называется *точечной группой*.

УПРАЖНЕНИЕ 3.6. $\Gamma \cap N \triangleleft \Gamma$.

ОБОЗНАЧЕНИЕ 3.7. Положим $\Delta = \Gamma/(\Gamma \cap N) \subset O(E)$. Зафиксируем в соответствии с теоремой 2.18 базис f_1, \dots, f_n образа $\Gamma \cap N$ в E . Тогда L состоит из всех векторов $m_1 f_1 + \dots + m_n f_n$, $m_1, \dots, m_n \in \mathbb{Z}$.

ПРЕДЛОЖЕНИЕ 3.8. Пусть $\phi \in \Delta$ и $l \in L$. Тогда $\phi(l) \in L$.

ДОКАЗАТЕЛЬСТВО. Пусть $\Phi(x) = \phi(x) + b$ и $\Psi(x) = x + l$ для всех $x \in E$, где $\Phi, \Psi \in \Gamma$. Тогда $\Phi^{-1}(x) = \phi^{-1}(x) - \phi^{-1}(b)$, откуда

$$(\Phi\Psi\Phi^{-1})(x) = \Phi(\Phi^{-1}(x) + l) = \phi(\phi^{-1}(x) - \phi^{-1}(b) + l) + b = x + \phi(l).$$

□

СЛЕДСТВИЕ 3.9. Существует такая матрица $X \in GL(n, \mathbb{R})$, что

$$X\Delta X^{-1} \subseteq GL(n, \mathbb{Z}).$$

В частности, если $A \in \Delta$, то $\text{tr } A \in \mathbb{Z}$.

ТЕОРЕМА 3.10 (Жордан). Существует такая функция $\tau(n)$, что для любой конечной подгруппы G в $O(n, \mathbb{R})$ порядок G не превосходит $\tau(n)$.

2. Двумерный случай

В этом разделе мы опишем кристаллографические группы в двумерном пространстве. Рассмотрим сначала строение конечных подгрупп Δ в группе $SO(2, \mathbb{R})$. Группа $SO(2, \mathbb{R})$ состоит из всех вращений двумерного евклидова пространства. В любом ортонормированном базисе этого пространства матрица оператора вращения имеет вид

$$g = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}.$$

Если $g \in \Delta$, то по следствию 3.9 $\text{tr } g = 2 \cos \alpha \in \mathbb{Z}$. Таким образом, $2 \cos \alpha = 0, \pm 1, \pm 2$, откуда $\alpha = 0, \pm \frac{\pi}{3}, \pm \frac{\pi}{2}, \pm \frac{2\pi}{3}, \pi$. Итак, доказана

ТЕОРЕМА 3.11. Подгруппа Δ в $SO(2, \mathbb{R})$ является циклической группой порядка 1, 2, 3, 4, 6.

Пусть теперь $\Delta \subset O(2, \mathbb{R})$, но $\Delta \not\subset SO(2, \mathbb{R})$. Тогда Δ содержит симметрию b относительно некоторой оси, причем $b^2 = 1$. Если $x \in \Delta \setminus SO(2, \mathbb{R})$, то $bx \in SO(2, \mathbb{R}) \cap \Delta$, причем bx – снова симметрия относительно некоторой оси, т. е. $(bx)^2 = 1$. По теореме 3.11 получаем $SO(2, \mathbb{R}) \cap \Delta = \langle a \rangle_n$, $n = 1, 2, 3, 4, 6$. Тогда $SO(2, \mathbb{R}) \cap \Delta$ – подгруппа индекса 2 в Δ . Отсюда

$$\Delta = \{1, a, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\},$$

т. е. $\Delta = D_n$ – группа диэдра. Итак, доказана

ТЕОРЕМА 3.12. Δ – одна из следующих групп:

1. циклическая группа вращений порядка 1, 2, 3, 4, 6;
2. группа диэдра D_n , $n = 1, 2, 3, 4, 6$.

По предложению 3.8 группа Δ действует как группа преобразований решетки L .

ТЕОРЕМА 3.13. Возможны следующие варианты для решетки $\Gamma \cap N$ с базисом f_1, f_2 .

1. Длины f_1, f_2 различны и они не перпендикулярны. В этом случае они порождают параллелограм. Тогда Δ – циклическая группа порядка 2, порождаемая центральной симметрией, или поворотом на π .

2. Длины f_1, f_2 различны и они перпендикулярны. В этом случае они порождают прямоугольник. Тогда Δ – группа D_2 порядка 4, порождаемая симметрией относительно прямой, проходящей через f_1 и поворотом на π .
3. Длины f_1, f_2 одинаковы и они перпендикулярны. В этом случае они порождают квадрат. Тогда Δ – группа D_4 .
4. Длины f_1, f_2 одинаковы и они не перпендикулярны. Кроме того, длина $f_1 - f_2$ отлична от длины f_2 . В этом случае они порождают ромб. Тогда Δ – группа D_2 , порождаемая двумя симметриями относительно прямых, параллельных диагоналям ромба.
5. Длины f_1, f_2 одинаковы и они не перпендикулярны. Кроме того, длина $f_1 - f_2$ равна длине f_2 . В этом случае они порождают ромб. Тогда Δ – группа D_6 , порождаемая двумя симметрией относительно прямых, параллельных диагоналям ромба и поворотом на угол $\frac{\pi}{3}$.

Кроме того, для каждой решетки допустимы подгруппы рассмотренных групп симметрий Δ , указанных выше.

3. Трехмерный случай

Рассмотрим теперь трехмерный случай. Как и выше рассмотрим строение конечных подгрупп в $SO(3, \mathbb{R})$, затем в $O(3, \mathbb{R})$ и, наконец, возможные решетки и их группы симметрий. Нам потребуется

ТЕОРЕМА 3.14. Пусть $g \in O(3, \mathbb{R})$, причем $hgh^{-1} \in GL(3, \mathbb{Z})$. Тогда существует такая матрица $u \in SO(3, \mathbb{R})$, что

$$ugu^{-1} = \begin{pmatrix} \det g & 0 & \\ 0 & \cos \alpha & -\sin \alpha \\ 0 & \sin \alpha & \cos \alpha \end{pmatrix}, \quad (8)$$

где $\alpha = 0, \pm \frac{\pi}{3}, \pm \frac{2\pi}{3}, \pm \frac{\pi}{2}, \pi$.

ДОКАЗАТЕЛЬСТВО. Из курса алгебры известно, что матрица ортогонального оператора в некотором ортонормированном базисе имеет вид (8). Поэтому

$$\det g + 2 \cos \alpha = \text{tr}(ugu^{-1}) = \text{tr} g = \text{tr}(hgh^{-1}) \in \mathbb{Z}.$$

Так как $\det g = \pm 1$, то $2 \cos \alpha \in \mathbb{Z}$. Отсюда как и выше получаем требуемое утверждение. \square

ОБОЗНАЧЕНИЕ 3.15. Обозначим через S трехмерную сферу единичного радиуса в трехмерном пространстве с центром в нуле. Предположим, что Δ – конечная подгруппа в $SO(3, \mathbb{R})$. Тогда каждый неединичный элемент из Δ является вращением относительно некоторой оси в перпендикулярной плоскости на угол из теоремы 3.14. Пересечение этой оси с S состоит из двух точек. Обозначим через X – множество всех таких точек из S для всех неединичных элементов из Δ .

ПРЕДЛОЖЕНИЕ 3.16. Пусть $x \in X$ и $g \in \Delta$. Тогда $g(x) \in X$.

ДОКАЗАТЕЛЬСТВО. Пусть l – неподвижная ось для $h \in \Delta \setminus 1$, и $x \in l \cap S$. Тогда $hgh^{-1}(g(l)) = g(l)$, т. е. $g(l)$ – неподвижная ось для $ghg^{-1} \in \Delta \setminus 1$, причем $g(x) \in g(l) \cap S$. \square

ПРЕДЛОЖЕНИЕ 3.17. Пусть $x \in X$ и Δ_x – стабилизатор x в Δ , т. е. множество всех таких $g \in \Delta$, что $g(x) = x$. Тогда H_x – циклическая группа порядка 1, 2, 3, 4, 6. При этом если $\Delta = \Delta_x \cup g_2 \Delta_x \cup \dots \cup g_m \Delta_x$ – разбиение Δ на левые смежные классы по Δ_x , то орбита x при действии Δ имеет порядок m и состоит из $x, g_2(x), \dots, g_m(x)$. В частности, $|\Delta| = m|\Delta_x|$. Стабилизатор $g_i(x)$ равен $g_i \Delta_x g_i^{-1}$.

ДОКАЗАТЕЛЬСТВО. Сопоставим $g_i \Delta_x$ элемент $g_i(x)$. □

ОБОЗНАЧЕНИЕ 3.18. Обозначим через M множество пар (x, g) , где $g \in \Delta_x \setminus 1$.

Так как каждому $g \in \Delta \setminus 1$ соответствуют две точки из X , то $|M| = 2(|\Delta| - 1)$. С другой стороны, X разбивается на орбиты X_1, \dots, X_k действия группы Δ . По предложению 3.17 число пар (x, g) , где x пробегает одну орбиту X_i порядка m_i равно $m_i(|\Delta_i| - 1)$, где $\Delta_i = \Delta_{x_i}$ для некоторого элемента $x_i \in X_i$. Кроме того, $m_i |\Delta_i| = |\Delta|$. Итак,

$$2(|\Delta| - 1) = m_1(|\Delta_1| - 1) + \dots + m_k(|\Delta_k| - 1).$$

Деля на $|\Delta|$, получаем

$$2 - \frac{2}{|\Delta|} = \left(1 - \frac{1}{|\Delta_1|}\right) + \dots + \left(1 - \frac{1}{|\Delta_k|}\right). \quad (9)$$

Так как $|\Delta_i| \geq 2$ для всех i , то $1 - \frac{1}{|\Delta_i|} \geq \frac{1}{2}$. Поэтому из (9) получаем $2\left(1 - \frac{1}{|\Delta|}\right) \geq \frac{k}{2}$, т. е. $k \leq 4 - \frac{4}{|\Delta|} < 4$. Случай $k = 1$ невозможен, поскольку

$$2\left(1 - \frac{1}{|\Delta|}\right) > 1 > 1 - \frac{1}{|\Delta_1|}.$$

Следовательно, $k = 2, 3$.

Пусть $k = 2$ и

$$2\left(1 - \frac{1}{|\Delta|}\right) = 2 - \frac{1}{|\Delta_1|} - \frac{1}{|\Delta_2|}$$

или,

$$\frac{2}{|\Delta|} = \frac{1}{|\Delta_1|} + \frac{1}{|\Delta_2|}$$

При этом $|\Delta_1|, |\Delta_2| \leq |\Delta|$. Отсюда $|\Delta_1| = |\Delta_2| = |\Delta|$. Это означает, что X состоит из двух точек, соответствующих одной оси. Поэтому Δ – циклическая группа вращений вокруг одной оси. Порядок Δ равен 1, 2, 3, 4, 6.

Пусть $k = 3$. Тогда из (9) вытекает

$$1 + \frac{2}{|\Delta|} = \frac{1}{|\Delta_1|} + \frac{1}{|\Delta_2|} + \frac{1}{|\Delta_3|}. \quad (10)$$

Можно считать, что $2 \leq |\Delta_1| \leq |\Delta_2| \leq |\Delta_3|$. Если $|\Delta_1| \geq 3$, то в равенстве (10) правая часть меньше 1, а левая больше. Следовательно, $|\Delta_1| = 2$ и

$$\frac{1}{2} + \frac{2}{|\Delta|} = \frac{1}{|\Delta_2|} + \frac{1}{|\Delta_3|}.$$

Непосредственный перебор показывает, что возможны лишь следующие случаи:

$$1. \quad |\Delta_2| = 2, \quad |\Delta_3| = \frac{|\Delta|}{2};$$

2. $|\Delta_2| = 3, \quad |\Delta_3| = 3 \quad |\Delta| = 12;$
3. $|\Delta_2| = 3, \quad |\Delta_3| = 4 \quad |\Delta| = 24;$
4. $|\Delta_2| = 3, \quad |\Delta_3| = 5 \quad |\Delta| = 60.$

Отсюда вытекает

ТЕОРЕМА 3.19. Пусть Δ – конечная подгруппа в $SO(3, \mathbb{R})$. Тогда Δ одна из следующих групп:

1. циклическая группа порядка 1, 2, 3, 4, 6;
2. группа диэдра D_n , где $n = 1, 2, 3, 4, 6$;
3. группа вращений тетраэдра $T \simeq A_4$, см. Рисунок 1;
4. группа вращений октаэдра $O \simeq S_4$, см. Рисунок 1;
5. группа вращений икосаэдра $I \simeq A_5$, см. Рисунок 1.

Рис. 1

Отметим, что указанные группы действительно реализуются как группы симметрий некоторых молекул, см. Рисунок 2. Так группой симметрий молекулы $H_3C - CCl_3$ является циклическая группа порядка 3, группой симметрий молекулы C_{26} является группа диэдра D_3 , группой симметрий молекулы метана CH_4 является группа тетраэдра T , группой симметрий молекулы гексафторид урана UF_4 является группа октаэдра T .

Рис. 2

Для завершения рассмотрения опишем точечные группы, состоящие не только из вращения.

ОБОЗНАЧЕНИЕ 3.20. Обозначим через j центральную симметрию в трехмерном пространстве, т. е. $j(x) = -x$ для всех векторов x .

УПРАЖНЕНИЕ 3.21. $j^2 = 1$ и $j \in O(3, \mathbb{R}) \setminus SO(3, \mathbb{R})$. Более того,

$$O(3, \mathbb{R}) = SO(3, \mathbb{R}) \times \langle j \rangle_2.$$

Предположим, что Δ – конечная подгруппа в $O(3, \mathbb{R})$, не лежащая в $SO(3, \mathbb{R})$. Тогда $A = \Delta \cap SO(3, \mathbb{R})$ является подгруппой индекса 2 в Δ .

ПРЕДЛОЖЕНИЕ 3.22. Если $j \in \Delta$, то $\Delta = A \times \langle j \rangle_2$.

Предположим, что $j \notin \Delta$ и $\Delta \setminus A = jM$, где $M \subset SO(3, \mathbb{R})$.

ПРЕДЛОЖЕНИЕ 3.23. $AM = MA = M$, $M^2 = A^2 = A$. В частности, $G = A \cup M$ является подгруппой в $SO(3, \mathbb{R})$, причем A – подгруппа индекса 2 в G .

ОБОЗНАЧЕНИЕ 3.24. Группа G из предложения 3.23 обозначается через (G, A) .

В силу теоремы 3.19 и предложения 3.23 справедлива

ТЕОРЕМА 3.25. Пусть Δ – конечная подгруппа в $O(3, \mathbb{R})$, не лежащая в $SO(3, \mathbb{R})$. Тогда Δ – одна из следующих групп:

1. $\langle a \rangle_n \times \langle j \rangle_2$;
2. $D_n \times \langle j \rangle_2$;
3. $T \times \langle j \rangle_2$;
4. $O \times \langle j \rangle_2$;
5. $I \times \langle j \rangle_2$;
6. $(\langle a \rangle_{2n}, \langle a^2 \rangle_n)$;
7. $(D_n, \langle c \rangle_n)$;
8. (D_{2n}, D_n) ;
9. (O, T) .

Возможные многогранники, возникающие на репере f_1, f_2, f_3 указываются в Рисунок 3.

Рис. 3

ГЛАВА 4

Элементы теории представлений групп

1. Основные понятия и примеры

Пусть V – векторное пространство над полем комплексных чисел \mathbb{C} . Через $\text{GL}(V)$ обозначается множество всех обратимых линейных операторов на V , т. е. множество всех линейных операторов \mathcal{A} в V , у которых есть такой (обратный) оператор \mathcal{A}^{-1} , что $\mathcal{A}\mathcal{A}^{-1} = \mathcal{A}^{-1}\mathcal{A} = \mathcal{E}$.

УПРАЖНЕНИЕ 4.1. $\text{GL}(V)$ является группой относительно операции умножения операторов.

ОПРЕДЕЛЕНИЕ 4.2. Пусть G – группа и V – комплексное векторное пространство. *Представлением* группы G в V называется гомоморфизм групп $\xi : G \rightarrow \text{GL}(V)$.

Другими словами, каждому элементу $g \in G$ сопоставлен обратимый линейный оператор $\xi(g)$, причем $\xi(gh) = \xi(g)\xi(h)$ для всех $g, h \in G$. Если представление ξ фиксировано, то обычно действие оператора $\xi(g)$, $g \in G$, на векторе $v \in V$ обозначается через gv . Тогда для всех $v, w \in V$ и $g, h \in G$ выполнены условия

$$g(\alpha v + \beta w) = \alpha(gv) + \beta(gw), \quad (gh)v = g(hv), \quad 1v = v. \quad (11)$$

Последние два равенства из (11) показывают, что группа G действует на множестве V .

ПРИМЕРЫ 4.3. Укажем ряд представлений групп.

1. Пусть $G = S_4$ и T – тетраэдр с вершинами, занумерованными числами 1,2,3,4. Предположим, что тетраэдр вложен в \mathbb{R}^3 , причем его центр расположен в начале координат. Сопоставим каждой перестановке $\sigma \in S_4$ ортогональное преобразование \mathbb{R}^3 , переводящее вершины 1,2,3,4 в $\sigma 1, \dots, \sigma 4$. Такое преобразование существует, так как σ является произведением транспозиций, и для каждой транспозиции такое преобразование существует. Ясно, что возникает представление S_4 .
2. Группа S_n действует в $k[X_1, \dots, X_n]$ с помощью перестановок переменных.
3. Группы диэдра D_n и кватернионов Q_8 имеют естественное представление в \mathbb{R}^2 и в \mathbb{C}^2 .

ОПРЕДЕЛЕНИЕ 4.4. Пусть заданы два представления $\xi : G \rightarrow \text{GL}(V)$, $\phi : G \rightarrow \text{GL}(W)$. Эти представления *эквивалентны (изоморфны)*, если существует такой изоморфизм векторных пространств $\zeta : V \rightarrow W$, что $\zeta[\xi(g)v] = \phi(g)[\zeta(v)]$ для всех $g \in G, v \in V$. Другими словами, для любого $g \in G$ коммутативна

диаграмма

$$\begin{array}{ccc} V & \xrightarrow{\zeta} & W \\ \xi(g) \downarrow & & \downarrow \phi(g) \\ V & \xrightarrow{\zeta} & W. \end{array}$$

Переформулируем понятие представления и изоморфизм в матричных терминах.

Пусть V – комплексное векторное пространство с базисом $\mathbf{e} = (e_1, \dots, e_n)$. Если задано представление $\xi : G \rightarrow \text{GL}(V)$, то каждому элементу $g \in G$ сопоставлена матрица $T_g = (a_{ij}(g)) \in \text{GL}(n, \mathbb{C})$. Если $g, h \in G$, то $T_{gh} = T_g T_h$ и если $x = \sum_{i=1}^n x_i e_i \in V, x_i \in \mathbb{C}$, то столбец из координат вектора $T_g x$ в базисе \mathbf{e} равен

$$T_g \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Предположим, что (f_1, \dots, f_n) – базис пространства W , и $\zeta : V \rightarrow W$ – изоморфизм представления, причем $\zeta(e_i) = \sum_{j=1}^n f_j c_{ji}$, $c_{ji} \in \mathbb{C}$, $i = 1, \dots, n$. Положим $C = (c_{ji}) \in \text{GL}(n, \mathbb{C})$, пусть при представлении $\phi : G \rightarrow \text{GL}(W)$ элементу $g \in G$ соответствует матрица $T'_g \in \text{GL}(n, \mathbb{C})$. Тогда для любого $g \in G$ по определению 4.4 получаем

$$CT_g = T'_g C \text{ или } T'_g = CT_g C^{-1} \quad (12)$$

ТЕОРЕМА 4.5. *Каждое конечномерное представление конечной группы G над полем \mathbb{R} (над \mathbb{C}) эквивалентно ортогональному (унитарному).*

ДОКАЗАТЕЛЬСТВО. Пусть задано представление $\psi : G \rightarrow \text{GL}(V)$, где V – конечномерное комплексное пространство. В V существует структура эрмитова пространства со скалярным произведением $(\ , \)$. Введем в V новое скалярное произведение

$$[x, y] = \frac{1}{|G|} \sum_{g \in G} (gx, gy).$$

Непосредственная проверка показывает, что $[\ , \]$ является скалярным произведением, и $[gx, gy] = [x, y]$ для всех $x, y \in V$. \square

СЛЕДСТВИЕ 4.6. *Пусть $\psi : G \rightarrow \text{GL}(V)$ – из теоремы 4.5. Если подпространство $U \subseteq V$ инвариантно относительно всех операторов $\psi(g), g \in G$, то $V = U \oplus W$, где подпространство W инвариантно относительно всех операторов $\psi(g), g \in G$.*

СЛЕДСТВИЕ 4.7. *Пусть задан гомоморфизм $\psi : G \rightarrow \text{GL}(n, \mathbb{C})$ конечной группы G , причем существует такое $1 < k < n$, что для всех $g \in G$*

$$\psi(g) = \left(\begin{array}{c|c} B_g & C_g \\ \hline 0 & D_g \end{array} \right),$$

$$B_g \in \text{GL}(k, \mathbb{C}), \quad D_g \in \text{GL}(n - k, \mathbb{C}), \quad C_g \in \text{Mat}(k \times (n - k), \mathbb{C}),$$

Тогда существует такая матрица $F \in \text{GL}(n, \mathbb{C})$, что

$$F \left(\begin{array}{c|c} B_g & C_g \\ \hline 0 & D_g \end{array} \right) F^{-1} = \left(\begin{array}{c|c} B'_g & 0 \\ \hline 0 & D'_g \end{array} \right), \quad B'_g \in \text{GL}(k, \mathbb{C}), \quad D'_g \in \text{GL}(n-k, \mathbb{C}),$$

для всех $g \in G$.

ДОКАЗАТЕЛЬСТВО. Можно считать, что ψ ортогонально. Тогда $W = U^\perp$. \square

2. Теорема Машке и ее приложения

ОПРЕДЕЛЕНИЕ 4.8. *Подпредставление, прямая сумма представлений, неприводимое представление, вполне приводимое представление.*

ТЕОРЕМА 4.9. *Любое конечномерное комплексное (вещественное) представление конечной группы вполне приводимо.*

ДОКАЗАТЕЛЬСТВО. Индукция по размерности представления. \square

УПРАЖНЕНИЕ 4.10. Доказать, что

1. естественные двумерные представления D_n, Q_8 неприводимы;
2. представление S_4 из 4.3 неприводимо.

ТЕОРЕМА 4.11. *Все одномерные представления группы G сводятся к одномерным представлениям G/G' .*

ДОКАЗАТЕЛЬСТВО. Нужно воспользоваться предложением 1.93. \square

ТЕОРЕМА 4.12. *Любое неприводимое конечномерное комплексное абелевой группы одномерно.*

ДОКАЗАТЕЛЬСТВО. Пусть задано представление ψ абелевой группы G в пространстве V . Если $g \in G$, то оператор $\psi(g)$ имеет ненулевой собственный вектор с собственным значением λ_g . Следовательно, подпространство U в V , состоящее из нуля и всех собственных векторов для $\psi(g)$ с собственным значением λ_g отлично от нуля, причем в силу абелевости G оно инвариантно. Следовательно, $U = V$. Так как g – любой элемент из G , то для любых $g \in G, v \in V$ имеем $gv = \lambda_g v$. Отсюда вытекает утверждение. \square

СЛЕДСТВИЕ 4.13. *Пусть конечная абелева группа G имеет в силу по теореме 2.14 разложение*

$$G = \langle a_1 \rangle_{p_1}^{k_1} \times \cdots \times \langle a_m \rangle_{p_m}^{k_m},$$

где p_1, \dots, p_m – простые числа. Каждое неприводимое комплексное представление ψ группы G имеет вид $\psi(a_j) = \zeta_j$, где ζ_j – комплексный корень степени $p_j^{k_j}$ из 1. В частности, число неэквивалентных неприводимых комплексных представлений конечной абелевой группы G равно ее порядку.

ПРЕДЛОЖЕНИЕ 4.14. *Пусть V – комплексное пространство размерности n с базисом $\mathbf{e} = (e_1, \dots, e_n)$. Зададим представление S_n в V , полагая $\sigma(e_i) = e_{\sigma i}$, $i = 1, \dots, n$, для $\sigma \in S_n$. Пусть $U = k(e_1 + \cdots + e_n)$ и*

$$W = \{x_1 e_1 + \cdots + x_n e_n \mid x_i \in \mathbb{C}, \quad x_1 + \cdots + x_n = 0\}$$

Тогда U, W неприводимые подпредставления, причем $V = U \oplus W$.

ДОКАЗАТЕЛЬСТВО. Достаточно показать, что W неприводимо. Пусть $h = h_1 e_1 + \dots + h_n e_n$ — ненулевой вектор из W . Переставляя e_i с помощью S_n можно считать, что $h_1 \neq 0$. Заметим, что случай $h_1 = h_2 = \dots = h_n$ невозможен в силу нулевой характеристики поля. Переставляя e_2, \dots, e_n с помощью S_n можно считать, что $h_1 \neq h_2$. Тогда $h - (1, 2)h = (h_1 - h_2)(e_1 - e_2)$. Следовательно, любое ненулевое инвариантное относительно S_n подпространство в W содержит вектор $(h_1 - h_2)^{-1}(h - (1, 2)h) = e_1 - e_2$. Но тогда оно содержит и $(2, i)(e_1 - e_2) = e_1 - e_i$ для любого i . Поэтому это подпространство совпадает с W . \square

3. Лемма Шура и ее следствия

ТЕОРЕМА 4.15 (Лемма Шура). Пусть

$$\phi_1 : G \rightarrow \text{GL}(V_1), \quad \phi_2 : G \rightarrow \text{GL}(V_2)$$

два неприводимых представления группы G . Пусть $f : V_1 \rightarrow V_2$ — линейное отображение, причем для любого $g \in G$ коммутативна диаграмма

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ \phi_1(g) \downarrow & & \downarrow \phi_2(g) \\ V_1 & \xrightarrow{f} & V_2. \end{array}$$

Если ϕ_1, ϕ_2 не эквивалентны, то $f = 0$. Если $V_1 = V_2 = V$ — конечномерно, и $\phi_1 = \phi_2 = \phi$, то существует такое комплексное число λ , что $f(x) = \lambda x$ для всех $x \in V$.

ДОКАЗАТЕЛЬСТВО. Пусть $f \neq 0$, и $W = \ker f$. Тогда $W \neq V_1$, причем W инвариантно относительно ϕ_1 . Следовательно, $W = 0$. Аналогично $\text{Im } f$ — инвариантное подпространство в V_2 . Поэтому $\text{Im } f = V_2$, т. е. f — эквивалентность, что невозможно.

Пусть $V_1 = V_2 = V$ и $\phi_1 = \phi_2 = \phi$. Тогда f имеет собственный вектор x с собственным значением λ . Собственное подпространство в V для оператора f с собственным значением λ инвариантно относительно ϕ . Отсюда V совпадает с этим собственным подпространством. \square

СЛЕДСТВИЕ 4.16. Пусть $\phi_1 : G \rightarrow \text{GL}(V_1)$, $\phi_2 : G \rightarrow \text{GL}(V_2)$ два неприводимых конечномерных представления группы конечной группы G . Пусть $B : V_1 \rightarrow V_2$ — линейное отображение. Положим

$$\Phi = \frac{1}{|G|} \sum_{g \in G} \phi_2(g) B \phi_1(g^{-1}) : V_1 \rightarrow V_2.$$

Если V_1, V_2 не эквивалентны, то $\Phi = 0$. Если $V_1 = V_2 = V$ и $\phi_1 = \phi_2 = \phi$, то

$$\Phi(x) = \frac{\text{tr } B}{\dim V} x$$

для любого $x \in V$.

ДОКАЗАТЕЛЬСТВО. Для любого $h \in G$ имеем

$$\begin{aligned}\phi_2(g)\Phi &= \frac{1}{|G|} \sum_{g \in G} \phi_2(h)\phi_2(g)B\phi_1(g^{-1}) = \\ &= \frac{1}{|G|} \sum_{g \in G} \phi_2(hg)B\phi_1(g^{-1}) = \frac{1}{|G|} \sum_{u \in G} \phi_2(u)B\phi_1(u^{-1}h) = \\ &= \left[\frac{1}{|G|} \sum_{u \in G} \phi_2(u)B\phi_1(u^{-1}) \right] \phi_1(h) = \Phi\phi_1(h).\end{aligned}$$

Поэтому если ϕ_1, ϕ_2 не эквивалентны, то по теореме 4.15 $\Phi = 0$.

Во втором случае существует такое $\lambda \in \mathbb{C}$, что

$$\Phi(x) = \frac{1}{|G|} \sum_{g \in G} \phi_2(g)B\phi_1(g^{-1})(x) = \lambda x$$

для любого $x \in V$. В частности, $\text{tr } \Phi = \lambda \dim V$, т. е. $\lambda = \frac{\text{tr } \Phi}{\dim V}$. Но

$$\text{tr } \Phi = \frac{1}{|G|} \sum_{g \in G} \text{tr}[\phi(g)B\phi(g)^{-1}] = \text{tr } B.$$

□

СЛЕДСТВИЕ 4.17. Пусть в условии следствия 4.16 \mathbf{e} – базис в пространстве V_1 и \mathbf{f} – базис в пространстве V_2 , причем если $V_1 = V_2 = V$ и $\phi_1 = \phi_2 = \phi$, то $\mathbf{e} = \mathbf{f}$. Пусть

$$\phi_1(g) = (T^1(g)_{ij}), \phi_2(g) = (T^2(g)_{ij})$$

– матрицы $\phi_1(g), \phi_2(g)$ в этой паре базисов. Если $\phi_1, \phi_2(g)$ не эквивалентны, то для любой тройки индексов i, j, s имеем

$$\sum_{g \in G} T^2(g)_{ij} \overline{T^1(g)_{is}} = 0. \quad (13)$$

Если $V_1 = V_2 = V$ и $\phi_1 = \phi_2 = \phi$, то для любого набора индексов i, j, r, s

$$\sum_{g \in G} T^2(g)_{ij} \overline{T^1(g)_{rs}} = \frac{\delta_{is}\delta_{jr}}{\dim V}. \quad (14)$$

ДОКАЗАТЕЛЬСТВО. Пусть $B : V_1 \rightarrow V_2$ – произвольный оператор, имеющий в этой паре базисов матрицу $B = (b_{ij})$. Тогда матрица Φ имеет в этой паре базисов матрицу, в которой на месте i, r стоит

$$\frac{1}{|G|} \sum_{g \in G} \sum_{j, s} T^2(g)_{ij} b_{js} \overline{T^1(g)_{rs}}.$$

Если ϕ_1, ϕ_2 не эквивалентны, то $\Phi = 0$ для любой матрицы B . В частности, если $b_{j,s} = 1$ и все остальные элементы B нулевые, то получаем равенство (13).

Во втором случае по следствию 4.16

$$\frac{1}{|G|} \sum_{g \in G} \sum_{j, s} T^2(g)_{ij} b_{js} \overline{T^1(g)_{rs}} = \frac{\text{tr } B \delta_{is}}{\dim V}$$

Беря $b_{js} = \delta_{j,j_0} \delta_{s,s_0}$ получаем (14). □

Пусть \mathcal{L} – пространство всех комплексных функций $\tau : G \rightarrow \mathbb{C}$. Если $\tau, \psi \in \mathcal{L}$, то положим

$$(\tau, \psi) = \frac{1}{|G|} \sum_{g \in G} \tau(g) \overline{\psi(g)}.$$

Таким образом, если ϕ_1, ϕ_2 – неприводимые представления с матрицами $T^1(g), T^2(g)$, и эти представления не эквивалентны, то по (13)

$$(T^2(g)_{ij}, T^1(g)_{is}) = 0. \quad (15)$$

Если же эти представления равны, то

$$(T^2(g)_{ij}, T^1(g)_{is}) = \frac{\delta_{is} \delta_{jr}}{\dim V}. \quad (16)$$

4. Характеры представления

Пусть $\phi : G \rightarrow \text{GL}(V)$ – конечномерное комплексное представление конечной группы G .

ОПРЕДЕЛЕНИЕ 4.18. *Характером* представления ϕ называется функция $\chi_\phi \in \mathcal{L}$, для которой $\chi_\phi(g) = \text{tr } \phi(g) \in \mathbb{C}$.

ПРЕДЛОЖЕНИЕ 4.19. *Пусть $\phi : G \rightarrow \text{GL}(V)$ – представление. Справедливы следующие равенства:*

1. $\chi_\phi(hgh^{-1}) = \chi_\phi(g)$;
2. $\chi_\phi(1) = \dim V$;
3. $\chi_\phi(g^{-1}) = \overline{\chi_\phi(g)}$;
4. $|\chi_\phi(g)| \leq \dim V$, причем если $|\chi_\phi(g)| = \dim V$, то $\phi(g) = \lambda E$, где $\lambda \in \mathbb{C}$ – корень из 1 степени $|G|$.

ДОКАЗАТЕЛЬСТВО. Имеем $\chi_\phi(hgh^{-1}) = \text{tr}(\phi(h)\phi(g)\phi(h)^{-1}) = \text{tr}(\phi(g)) = \chi_\phi(g)$. Кроме того, $\chi_\phi(1) = \text{tr } 1 = \dim V$. Так как $\phi(g)$ унитарно по теореме 4.5, то по теореме 1.81 матрица $\phi(g)$ в некотором ортонормированном базисе имеет диагональный вид $\text{diag}(\lambda_1, \dots, \lambda_n)$, причем $\lambda_j^m = 1$, если $m = |g|$. Отсюда вытекают остальные утверждения. \square

ПРЕДЛОЖЕНИЕ 4.20. *Если $\phi = \phi_1 \oplus \phi_2$, то $\chi_\phi = \chi_{\phi_1} + \chi_{\phi_2}$.*

Итак, ϕ – функция на G и на классах сопряженных элементов.

ОПРЕДЕЛЕНИЕ 4.21. *Функция $\xi \in \mathcal{L}$ центральна, если $\xi(hgh^{-1}) = \xi(g)$, т. е. ξ является функцией на классах сопряженных элементов в G .*

Нетрудно видеть, что центральные функции образуют подпространство в \mathcal{H} , размерность которого равна числу классов сопряженных элементов в G .

ТЕОРЕМА 4.22. *Пусть χ – характер неприводимого представления конечной группы G . Тогда $(\chi, \chi) = 1$. Если ϕ_1, ϕ_2 – два неприводимых неэквивалентных представления G , то $(\chi_{\phi_1}, \chi_{\phi_2}) = 0$.*

ДОКАЗАТЕЛЬСТВО. Пусть $\chi(g)$ задается некоторой матрицей $T(g) = (T(g)_{ij}) \in \text{GL}(n, \mathbb{C})$. По следствию 4.17

$$\begin{aligned} (\chi, \chi) &= \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_s T(g)_{ss} \right) \left(\sum_j \overline{T(g)_{jj}} \right) = \sum_{s,j} \frac{1}{|G|} \sum_{g \in G} T(g)_{ss} \overline{T(g)_{jj}} = \\ &= \sum_{s,j} (T(g)_{ss}, T(g)_{jj}) = \sum_{s,j} \frac{\delta_{sj} \delta_{sj}}{\dim V} = 1. \quad (17) \end{aligned}$$

Аналогично проверяется второе равенство. \square

ТЕОРЕМА 4.23. Пусть конечномерное представление ϕ конечной группы G разложено в прямую сумму неприводимых представлений $\phi = \phi_1 + \dots + \phi_k$. Если χ_j — характер представления ϕ_j и r_j — его кратность, то $(\chi, \chi_j) = r_j$.

ТЕОРЕМА 4.24. Пусть n_1, \dots, n_s — размерности неприводимых комплексных представлений конечной группы G . Тогда $|G| = n_1^2 + \dots + n_s^2$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим пространство V с базисом $e_g, g \in G$. Имеется регулярное представление $\tau : G \rightarrow V, \rho(g)e_h = e_{gh}$. Отсюда $\chi_\rho(1) = |G|, \chi_\rho(g) = 0$, если $g \neq 1$. При этом

$$(\chi_\rho, \chi_j) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_j(g)} = \frac{1}{|G|} |G| \overline{\chi_j(1)} = \dim V_j = n_j.$$

Итак, $\chi_\rho = n_1 \chi_1 + \dots + n_s \chi_s$. Следовательно, $|G| = \chi_\rho(1) = n_1^2 + \dots + n_s^2$. \square

Пусть как и выше, \mathcal{H} — пространство всех центральных функций на G .

ТЕОРЕМА 4.25. Пусть $\phi : G \rightarrow \text{GL}(V)$ — конечномерное комплексное представление группы G и $f \in \mathcal{H}$. Положим $\phi_f = \sum_{g \in G} f(g) \phi(g)$. Если ϕ неприводимо и имеет размерность n , то $\phi_f = \frac{|G|}{n} (f, \overline{\chi_\phi})$.

ДОКАЗАТЕЛЬСТВО. Имеем

$$\begin{aligned} \phi(h) \phi_f \phi(h^{-1}) &= \sum_{g \in G} \phi(h) f(g) \phi(g) \phi(h^{-1}) = \\ &= \sum_{g \in G} f(g) \phi(hgh^{-1}) = \sum_{g \in G} f(g) \phi(g) = \phi_f. \end{aligned}$$

Следовательно, по следствию 4.16 $\phi_f(x) = \lambda x$ для некоторого комплексного числа λ . Отсюда

$$\text{tr}(\phi_f) = \lambda \dim V = \sum_{g \in G} f(g) \chi_\phi(g) = |G| (f, \overline{\chi_\phi}).$$

\square

ТЕОРЕМА 4.26. Функции χ_1, \dots, χ_s составляют базис пространства \mathcal{H} .

ДОКАЗАТЕЛЬСТВО. Пусть $f \in \mathcal{H}$ и $f \perp \chi_j$ для всех j . Тогда $\phi_f = 0$ по предыдущей теореме для любого представления ϕ . В частности, при регулярном представлении ρ имеем

$$\rho_f(e_1) = \sum_{g \in G} \overline{f(g)} \rho(g) e_1 = \sum_{g \in G} \overline{f(g)} e_g = 0.$$

Следовательно, $f(g) = 0$. \square

СЛЕДСТВИЕ 4.27. Число классов сопряженных элементов группы G равно числу неэквивалентных неприводимых представлений группы G .

ТЕОРЕМА 4.28. Любое неприводимое конечномерное комплексное абелевой группы одномерно.

ДОКАЗАТЕЛЬСТВО. Пусть задано представление ψ абелевой группы G в пространстве V . Если $g \in G$, то оператор $\psi(g)$ имеет ненулевой собственный вектор с собственным значением λ_g . Следовательно, подпространство U в V , состоящее из нуля и всех собственных векторов для $\psi(g)$ с собственным значением λ_g отлично от нуля, причем в силу абелевости G оно инвариантно. Следовательно, $U = V$. Так как g — любой элемент из G , то для любых $g \in G, v \in V$ имеем $gv = \lambda_g v$. Отсюда вытекает утверждение. \square

Неприводимые представления циклической группы $G = \langle a \rangle_n$ одномерны и имеют вид

$$\phi_k(a) = \exp\left(\frac{2\pi i k}{n}\right), \quad k = 0, \dots, n-1.$$

При этом

$$\chi_{\phi_k} = \exp\left(\frac{2\pi i k}{n}\right), \quad k = 0, \dots, n-1.$$

Отсюда при $k \neq k'$

$$\begin{aligned} (\chi_{\phi_k}, \chi_{\phi_{k'}}) &= \\ \frac{1}{n} \sum_{j=0}^{n-1} \exp\left(\frac{2\pi i k j}{n}\right) \exp\left(-\frac{2\pi i k' j}{n}\right) &= \frac{1}{n} \sum_{j=0}^{n-1} \exp\left(\frac{2\pi i (k - k') j}{n}\right) = \\ \frac{1}{n} \frac{\exp\left(\frac{2\pi i (k - k') n}{n}\right) - 1}{\exp\left(\frac{2\pi i (k - k')}{n}\right) - 1} &= 0. \end{aligned}$$

При $k = k'$

$$(\chi_{\phi_k}, \chi_{\phi_k}) = \frac{1}{n} \sum_{j=0}^{n-1} \exp\left(\frac{2\pi i k j}{n}\right) \exp\left(-\frac{2\pi i k j}{n}\right) = \frac{1}{n} \sum_{j=0}^{n-1} 1 = 1.$$

Отсюда в силу теоремы о строении конечных абелевых групп получается общее описание конечномерных представления конечных абелевых групп.

Перейдем к описанию неприводимых представлений некоторых неабелевых групп.

ТЕОРЕМА 4.29. Все одномерные представления группы G сводятся к одномерным представлениям G/G' .

ДОКАЗАТЕЛЬСТВО. Нужно воспользоваться предложением 1.93. \square

Укажем ряд примеров одномерных представлений симметрических групп S_n , групп диэдра $D_n, n \geq 3$, и группы кватернионов Q_8 . Во всех случаях воспользуемся теоремой 4.29. Напомним, что $S'_n = A_n$, $D'_n = \langle a^2 \rangle$, $Q'_8 = \{\pm 1\}$. При этом S_n/A_n — циклическая группа порядка 2. Поэтому имеется два одномерных представления S_n — тождественное и представление $\sigma \mapsto (-1)^\sigma$.

Если n нечетно, то $D'_n = \langle a \rangle$ и поэтому D_n/D'_n имеет порядок два. Таким образом, имеется два одномерных представления группы диэдра D_n ,

$$a \mapsto 1, \quad b \mapsto 1, \quad \text{и} \quad a \mapsto 1, \quad b \mapsto -1.$$

Если n четно, то $D_n/D'_n \simeq \langle aD'_n \rangle_2 \times \langle bD'_n \rangle_2$. Отсюда имеется четыре одномерных представления группы D_n , именно,

$$\begin{aligned} a \mapsto 1, \quad b \mapsto 1; \\ a \mapsto 1, \quad b \mapsto -1; \\ a \mapsto -1, \quad b \mapsto 1; \\ a \mapsto -1, \quad b \mapsto -1. \end{aligned}$$

Для группы кватернионов Q_8 имеем $Q_8/Q'_8 \simeq \langle iQ'_8 \rangle_2 \times \langle jQ'_8 \rangle_2$. Поэтому имеется четыре одномерных представления группы Q_8 , именно,

$$\begin{aligned} i \mapsto 1, \quad j \mapsto 1; \\ i \mapsto 1, \quad j \mapsto -1; \\ i \mapsto -1, \quad j \mapsto 1; \\ i \mapsto -1, \quad j \mapsto -1. \end{aligned}$$

Опишем все неприводимые представления группы S_3 и S_4 . Их число совпадает с числом классов сопряженных элементов. Напомним, что в S_3 имеется 3 класса сопряженных элементов, $\{1\}, \{(12)\}, \{(123)\}$. Поэтому имеется три неприводимых представления. Два из них одномерны. Следовательно, имеется еще одно размерности n , причем $|S_3| = g = 1 + 1 + n^2$. Отсюда $n = 2$. Это представление совпадает с естественным представлением $S_3 = D_3$.

Опишем все неприводимые представления группы S_4 . Напомним, что в S_4 имеется 5 класса сопряженных элементов,

$$\{1\}, \{(12)\}, \{(123)\}, \{(1234)\}, \{(12)(34)\}.$$

Поэтому имеется 5 неприводимых представлений. Два из них одномерны. Одно двумерно и связано с изоморфизмом $S_4/V_4 \simeq S_3$. Два трехмерных связаны с тетраэдром и кубом.

Опишем все неприводимые представления группы D_n . Их число совпадает с числом классов сопряженных элементов. Напомним, что в группе D_n имеются следующие классы $\{a^k, a^{-k}\}, \{b, ba^2, ba^4, \dots\}, \{ba, ba^3, \dots\}$. Поэтому кроме двух (четырех) одномерных представлений имеются двумерные представления

$$a \mapsto \begin{pmatrix} \exp\left(\frac{2\pi k}{n}\right) & 0 \\ 0 & \exp\left(-\frac{2\pi k}{n}\right) \end{pmatrix}, \quad k = 1, \dots, [n/2]; \quad b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

В заключение приведем следующие результаты.

ТЕОРЕМА 4.30. *Конечные подгруппы в $SO(3, \mathbb{R})$, отличные от циклических групп и групп диэдра, имеют порядки 12, 24, 60. Это группы симметрий тетраэдра, куба, октаэдра, додекаэдра, икосаэдра. Они имеют порядки 12, 24, 24, 60, 60 и изоморфны группам A_4, S_4, A_5 .*

ГЛАВА 5

Алгебры и поля

1. Кольца и алгебры

ОПРЕДЕЛЕНИЕ 5.1. *Кольцо* (не обязательно ассоциативное). *Ассоциативные, коммутативные, антикоммутативные кольца, кольца Ли.*

ПРЕДЛОЖЕНИЕ 5.2. *В любом кольце имеем $0x = x0 = 0$.*

ОПРЕДЕЛЕНИЕ 5.3. Поля, тела.

ОПРЕДЕЛЕНИЕ 5.4. *Алгебра над полем* (не обязательно ассоциативная). *Ассоциативные, коммутативные, антикоммутативные алгебры, алгебры Ли.*

ПРИМЕРЫ 5.5. Укажем ряд алгебр.

♡ Ассоциативные алгебры – алгебры матриц $\text{Mat}(n, k)$.

♡ Ассоциативно-коммутативные алгебры – алгебры многочленов

$$k[X_1, \dots, X_n],$$

алгебры рядов $k[[X]]$, алгебры непрерывных функций на топологическом пространстве.

♡ Если R – ассоциативная алгебра с 1, то алгебра матриц $\text{Mat}(n, R)$ снова является ассоциативной алгеброй с 1.

♡ Алгебры Ли $A^{(-)}$ для ассоциативной алгебры A .

ОПРЕДЕЛЕНИЕ 5.6. *Единичный элемент, делители нуля, обратимые элементы алгебры. Области, тела.*

ПРЕДЛОЖЕНИЕ 5.7. *Единичный элемент алгебры определен однозначно. Обратимые элементы ассоциативной алгебры образуют группу по умножению. Обратимый элемент ассоциативной алгебры не может быть делителем нуля.*

СЛЕДСТВИЕ 5.8. *В теле и в поле нет делителей нуля.*

ПРИМЕРЫ 5.9. Группы обратимых элементов в

1. $k[X_1, \dots, X_n]$ – это ненулевые константы;
2. $k[[X]]$ – это ряды с ненулевым свободным членом;
3. $\text{Mat}(n, k)$ – это $\text{GL}(n, k)$; делители нуля в $\text{Mat}(n, k)$ – это вырожденные матрицы и только они.

ОПРЕДЕЛЕНИЕ 5.10. Подалгебры, подалгебры с 1.

ПРЕДЛОЖЕНИЕ 5.11. *Пусть A – ассоциативная алгебры и $z \in A$. Положим $k[z] = \{\sum a_i z^i \mid a_i \in k, i \geq 0\}$. Тогда $k[z]$ – наименьшая подалгебра с 1 в A , содержащая z .*

ОПРЕДЕЛЕНИЕ 5.12. *Идеал* в кольце и в алгебре. Обозначение $I \triangleleft R$. Алгебра A *проста*, если в ней только два идеала A и 0 .

ПРЕДЛОЖЕНИЕ 5.13. Пусть A – коммутативно-ассоциативная алгебра, и $z_1, \dots, z_n \in A$. Тогда $(z_1, \dots, z_n) = \{\sum_{i=1}^n a_i z_i \mid a_i \in A\}$ является идеалом в A .

УПРАЖНЕНИЕ 5.14. Если идеал I кольца R с единицей содержит обратимый элемент, то $I = R$.

СЛЕДСТВИЕ 5.15. *Любое тело просто.*

ОПРЕДЕЛЕНИЕ 5.16. Идеал (z_1, \dots, z_n) называется идеалом, порожденным множеством z_1, \dots, z_n . Идеал вида (z) в A называется *главным*.

ТЕОРЕМА 5.17. *Любой идеал в алгебра многочленов $k[X]$ является главным.*

УПРАЖНЕНИЕ 5.18. Любой идеал в \mathbb{Z} и в $\mathbb{Z}[i]$ является главным.

ТЕОРЕМА 5.19. Пусть R – ассоциативная алгебра, и $A = \text{Mat}(n, R)$. Предположим, что $I \triangleleft A$. Тогда существует и притом единственный такой идеал $J \triangleleft R$, что $I = \text{Mat}(n, J)$.

ДОКАЗАТЕЛЬСТВО. Положим $J = \{a \in R \mid aE_{11} \in I\}$. Пусть $X = (x_{ij}) \in I$, где $x_{ij} \in R$. Для любых $i, j = 1, \dots, n$ имеем $x_{ij}E_{11} = E_{1i}XE_{j1} \in I$. Следовательно, $x_{ij} \in J$, т. е. $I \subseteq \text{Mat}(n, J)$.

Обратно, пусть $X = (x_{ij}) \in \text{Mat}(n, J)$, т. е. $x_{ij} \in J$ для всех $i, j = 1, \dots, n$. В этом случае $x_{ij}E_{11} \in I$, откуда

$$X = \sum_{ij} x_{ij}E_{ij} = \sum_{ij} E_{i1}(x_{ij}E_{11})E_{1j} \in I.$$

□

СЛЕДСТВИЕ 5.20. Пусть D – тело. Тогда $\text{Mat}(n, D)$ – простая алгебра.

ОПРЕДЕЛЕНИЕ 5.21. *Гомоморфизмы* колец и алгебр. *Изоморфизмы, автоморфизмы. Ядро* гомоморфизма $\ker \phi$.

ПРЕДЛОЖЕНИЕ 5.22. $\ker \phi$ является идеалом кольца (алгебры).

СЛЕДСТВИЕ 5.23. Пусть $\phi : k \rightarrow A$ – ненулевой гомоморфизм поля k в алгебре A . Тогда ϕ является мономорфизмом.

ДОКАЗАТЕЛЬСТВО. Рассмотрим идеал $\ker \phi$. По следствию 5.15 либо $\ker \phi = k$, либо $\ker \phi = 0$. В первом случае $\phi = 0$, что противоречит предположению. Следовательно, $\ker \phi = 0$, и ϕ – мономорфизм по следствию 1.66. □

ОПРЕДЕЛЕНИЕ 5.24. Пусть $I \triangleleft R$. Рассмотрим факторгруппу (относительно сложения) R/I . Для $a + I, b + I \in R/I$ и $\alpha \in k$ положим

$$(a + I)(b + I) = ab + I \in R/I, \quad \alpha(a + I) = \alpha a + I.$$

Получающаяся алгебра (кольцо) называется *факторалгеброй (факторкольцом)*

ПРЕДЛОЖЕНИЕ 5.25. *Определение факторалгебры (факторкольца) R/I корректно. Если R ассоциативно (коммутативно, кольцо или алгебра Ли), то этим же свойством обладает R/I .*

ДОКАЗАТЕЛЬСТВО. Пусть $a + I = a' + I, b + I = b' + I$. Тогда $a' = a + x, b' = b + y$, где $x, y \in I$. Поэтому $a'b' = ab + xb + ay + xy \in ab + I$, поскольку $xb + ay + xy \in I$ в силу определения идеала. Аналогично, если $\alpha \in k$, то $\alpha a' = \alpha a + \alpha x \in \alpha a + I$. Несложно проверяется и последнее утверждение. \square

ОПРЕДЕЛЕНИЕ 5.26. Рассмотрим гомоморфизм $\pi : R \rightarrow R/I, a \mapsto a + I$. Тогда π является гомоморфизмом колец (алгебр). Он называется *естественным* гомоморфизмом колец (алгебр).

ПРЕДЛОЖЕНИЕ 5.27. Гомоморфизм $\pi : R \rightarrow R/I$ из определения 5.26 является гомоморфизмом колец, $\ker \pi = I$. (алгебр).

ТЕОРЕМА 5.28 (Теорема о гомоморфизмах). Пусть $\phi : R \rightarrow R'$ – гомоморфизм колец (алгебр). Тогда $\text{Im } \phi \simeq R/\ker \phi$.

ДОКАЗАТЕЛЬСТВО. По теореме 1.70 отображение $\zeta : f(R) \rightarrow R/\ker \phi$, задаваемое по правилу $\zeta(\phi(x)) = \phi^{-1}(\phi(x)) = x \ker \phi$ является изоморфизмом аддитивных групп $\text{Im } \phi$ и R/I . Остается показать, что $\zeta(ab) = \zeta(a)\zeta(b)$, и

$$\alpha\zeta(a) = \zeta(\alpha a) \quad (18)$$

для всех $a, b \in \text{Im } \phi, \alpha \in k$. Пусть $a = \phi(x), b = \phi(y)$, где $x, y \in R$. Так как $\phi(x)\phi(y) = \phi(xy)$, то $\zeta(a)\zeta(b) = \phi^{-1}(\phi(x))\phi^{-1}(\phi(y)) = \phi^{-1}\phi(xy) = \zeta(ab)$. Аналогично проверяется (18). \square

ПРИМЕРЫ 5.29. Доказать, что

1. $\mathbb{C}[X, Y]/(X) \simeq \mathbb{C}[Y]$;
2. $\mathbb{R}[X]/(X^2 + X + 1) \simeq \mathbb{C}$.

2. Теорема Фробениуса

Опишем конечномерные тела над полем вещественных чисел.

ОПРЕДЕЛЕНИЕ 5.30. Пусть \mathbb{H} – множество всех комплексных матриц

$$z = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \quad (19)$$

ТЕОРЕМА 5.31. \mathbb{H} является подалгеброй в \mathbb{R} -алгебре всех комплексных матриц $\text{Mat}(2, \mathbb{C})$. Более того, \mathbb{H} является телом с центром \mathbb{R} .

ДОКАЗАТЕЛЬСТВО. Для $z \in \mathbb{H}$ из (19) через $\|z\|$ обозначим

$$\sqrt{\det z} = \sqrt{|a|^2 + |b|^2}.$$

Тогда $\|z\| > 0$, если $z \neq 0$, $\|z_1 z_2\| = \|z_1\| \|z_2\|$.

Если z из (19), то положим

$$\bar{z} = \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}$$

Нетрудно видеть, что $z\bar{z} = \|z\|^2$. Таким образом, если $z \neq 0$, то $z^{-1} = \frac{\bar{z}}{\|z\|^2}$.

Следовательно, \mathbb{H} – тело. Оно некоммутативно, так как если

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad (20)$$

то $IJ = -JI$.

Найдем центр \mathbb{H} . Он состоит из всех матриц

$$w = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix},$$

что $wz = zw$ для всех матриц z из eqref(19). Непосредственная проверка показывает, что $w = \lambda E$, $\lambda \in \mathbb{R}$. \square

УПРАЖНЕНИЕ 5.32. Доказать, что матрицы E, I, J, K , где I, J из (20) и

$$K = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix},$$

составляют базис \mathbb{H} над \mathbb{R} , причем

$$IJ = K, \quad JK = I, \quad I^2 = J^2 = K^2 = -E.$$

Нам потребуется ряд утверждений.

ОПРЕДЕЛЕНИЕ 5.33. Пусть A – ассоциативная k -алгебра с 1. Элемент $z \in A$ называется *алгебраическим* над k , если существует такой ненулевой многочлен $f \in k[X]$, что $f(z) = 0$. *Минимальным* многочленом алгебраического элемента z над k называется такой многочлен $f(X) \in k[X]$ минимальной степени со старшим коэффициентом 1, что $f(z) = 0$.

УПРАЖНЕНИЕ 5.34. Пусть $f \in k[X]$ – имеет старший коэффициент 1, и $z = X + (p) \in k[X]/(f)$. Тогда минимальный элемент для z равен f .

ПРЕДЛОЖЕНИЕ 5.35. Пусть A – область над полем k , и $z \in K$ – алгебраический элемент с минимальным многочленом $f(X)$. Тогда f неприводим. Положим $k[z] = \{a_0 + a_1z + \dots + a_{n-1}z^{n-1} \mid a_i \in k, n = \deg f\}$. Тогда $k[z]$ является подполем в K , содержащим k , и

$$k[z] \simeq k[X]/(f). \quad (21)$$

ПРЕДЛОЖЕНИЕ 5.36. Пусть A конечномерное тело над \mathbb{R} , и $a \in A \setminus \mathbb{R}$. Тогда минимальный многочлен над a имеет степень два. Кроме того, $\mathbb{R}[a] \simeq \mathbb{C}$.

ДОКАЗАТЕЛЬСТВО. Так как A конечномерно, все степени a зависимы. Следовательно, a алгебраично. Минимальный многочлен p для a неприводим и потому имеет степень не выше 2 в силу предложения 5.35. Так как $a \notin \mathbb{R}$, то степень p равна 2. Поэтому $a^2 + \alpha a + \beta = 0$, где $p = X^2 + \alpha X + \beta \in \mathbb{R}[X]$. Положим

$$I = \frac{2a + \alpha}{\sqrt{4\beta - \alpha^2}}.$$

Тогда $I^2 = -1$, причем по предложению 5.35

$$\mathbb{R}[a] = \mathbb{R}[I] \simeq \mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}.$$

\square

ТЕОРЕМА 5.37. Пусть поле A является алгебраическим расширением поля \mathbb{R} . Тогда либо $A = \mathbb{R}$, либо $A = \mathbb{C}$.

ДОКАЗАТЕЛЬСТВО. Заметим, что $A \supseteq \mathbb{R}1 = \mathbb{R}$. Можно считать, что $A \neq \mathbb{R}$. По предложению 5.36 $A \supseteq \mathbb{C}$. Итак, A является конечным расширением \mathbb{C} . Если $a \in A \setminus \mathbb{C}$, то минимальный многочлен f для a имеет комплексный корень λ . Отсюда $0 = f(a) = (a - \lambda)g(a)$, где $g \in \mathbb{C}[X]$. Так как в A нет делителей нуля, то $a - \lambda = 0$ и $a = \lambda \in \mathbb{C}$. \square

ТЕОРЕМА 5.38 (Фробениус). Пусть A – конечномерное тело над \mathbb{R} . Тогда A – одно из тел $\mathbb{R}, \mathbb{C}, \mathbb{H}$.

ДОКАЗАТЕЛЬСТВО. Можно считать, что A не коммутативно. Как и в предыдущей теореме 5.37 $A \supseteq \mathbb{R}1 = \mathbb{R}$. Можно считать, что $A \neq \mathbb{R}$. По предложению 5.36 $A \supseteq \mathbb{C}$. Если $A = \mathbb{C}$, то теорема доказана. Пусть $A \neq \mathbb{C}$. В этом случае A является левым векторным пространством над \mathbb{C} . Рассмотрим в A линейный оператор $\mathcal{L}(x) = xi$, $i \in \mathbb{C}$. Заметим, что $\mathcal{L}^4 = 1$. Поэтому получается комплексное конечномерное представление циклической группы G порядка 4. Следовательно, A разлагается в прямую сумму

$$A = A_1 \oplus A_{-1} \oplus A_i \oplus A_{-i}, \quad \text{где } A_j = \{x \in A \mid xi = jx\}.$$

Пусть $y \in A_1$. Тогда $yi = y$, откуда $y(i - 1) = 0$, т. е. $y = 0$. Пусть $y \in A_{-1}$. Тогда $yi = -y$, откуда $y(i + 1) = 0$, т. е. $y = 0$. Итак, $A_1 = A_{-1} = 0$, и

$$A = A_i \oplus A_{-i}, \quad \mathbb{C} \subseteq A_i.$$

ЛЕММА 5.39. $A_i = \mathbb{C}$.

ДОКАЗАТЕЛЬСТВО. Пусть $a \in A_i$. Тогда $ai = ia$, т. е. поле $\mathbb{C}[a]$ является конечным расширением \mathbb{C} . По теореме 5.37 получаем $A_i = \mathbb{C}$. \square

ЛЕММА 5.40. Пусть $y \in A_{\varepsilon i}, z \in A_{\tau i}$, где $\varepsilon, \tau = \pm 1$. Тогда $yz \in A_{\varepsilon\tau i}$.

ДОКАЗАТЕЛЬСТВО. Имеем $(yz)i = y(zi) = y(\tau ia) = \tau(yi)a = \tau\varepsilon i(ya)$. \square

ЛЕММА 5.41. Пусть $y \in A_{\varepsilon i}$. Тогда $yA_{\varepsilon i} = A_i, yA_{-\varepsilon i} = A_{-i}$.

ДОКАЗАТЕЛЬСТВО. По лемме 5.40 получаем $yA_{\varepsilon i} \subseteq A_i, yA_{-\varepsilon i} \subseteq A_{-\varepsilon i}$. Так как в A нет делителей нуля, то

$$\dim_{\mathbb{C}} A_{\varepsilon i} = \dim_{\mathbb{C}} (yA_{\varepsilon i}) \leq \dim_{\mathbb{C}} A_i = \dim_{\mathbb{C}} (yA_i) \leq \dim_{\mathbb{C}} A_{\varepsilon i}.$$

Отсюда следует утверждение. \square

СЛЕДСТВИЕ 5.42. $\dim_{\mathbb{C}} A_i = \dim_{\mathbb{C}} A_{-i} = 1$.

Завершим доказательство теоремы. Пусть $j \in A_{-i}$. По леммам 5.40, 5.39 $j^2 \in \mathbb{C}$. Тогда $ji = -ij$. По лемме 5.40 можно считать, что $j^2 = -1$. Положим $k = ij \in A_{-i}$. Тогда $ki = -ik$. Кроме того, $k^2 = ijij = i(-ij)j = -i^2j^2 = -1$, и $jk = j(ij) = (ji)j = -ij^2 = i, kj = (ij)j = ij^2 = -i$. Итак, $A_i = \mathbb{C} = \mathbb{R}1 + \mathbb{R}i, A_{-i} = \mathbb{C}j = \mathbb{R}j + \mathbb{R}k$ в силу следствия 5.42. Отсюда $a \simeq \mathbb{H}$. \square

3. Алгебры Ли

ОПРЕДЕЛЕНИЕ 5.43. Алгеброй Ли L называется неассоциативная алгебра с умножением $[x, y]$, удовлетворяющая тождествам

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

ПРИМЕР 5.44. Алгебра $A^{(-)}$, алгебра $\mathbb{R}^3, [x, y] = x \times y$.

УПРАЖНЕНИЕ 5.45. В алгебре Ли выполнено тождество антикоммутативности $[x, y] = -[y, x]$.

ОПРЕДЕЛЕНИЕ 5.46. Пусть A – произвольная алгебра. Линейный оператор D на A называется *дифференцированием*, если $D(xy) = D(x)y + xD(y)$. Через $\text{Der}(A)$ обозначается множество всех дифференцирований алгебры A .

ПРЕДЛОЖЕНИЕ 5.47. $\text{Der}(A)$ является подалгеброй Ли в алгебре Ли всех линейных операторов $\mathcal{L}(A)^{(-)}$ на A .

УПРАЖНЕНИЕ 5.48. Пусть f – квадратичная форма на n -мерном пространстве k^n , где k – поле. Через $o(n, f)$ обозначается множество всех кососимметричных относительно f линейных операторов в k^n , т. е. множество всех таких линейных операторов C в k^n , что $f(Cx, y) = -f(x, Cy)$. Доказать, что $o(n, f)$ – подалгебра Ли в $\text{Mat}(n, k)^{(-)}$.

УПРАЖНЕНИЕ 5.49. Пусть f – полуторалинейная эрмитова форма на n -мерном комплексном пространстве \mathbb{C}^n . Через $su(n, f)$ обозначим множество всех кососимметричных относительно f линейных операторов в \mathbb{C}^n , т. е. множество всех таких линейных операторов A в \mathbb{C}^n , что $f(Ax, y) = -f(x, Ay)$. Доказать, что $su(n, f)$ – подалгебра Ли в $\text{Mat}(2n, \mathbb{R})^{(-)}$.

ОБОЗНАЧЕНИЕ 5.50. Через $sl(n, k)$ обозначается множество всех матриц из $\text{Mat}(n, k)$ со следом 0.

УПРАЖНЕНИЕ 5.51. $sl(n, k)$ является подалгеброй Ли в $\text{Mat}(n, k)^{(-)}$.

ПРЕДЛОЖЕНИЕ 5.52. Пусть k – поле характеристики $\neq 2$, и

$$H = E_{11} - E_{22}, \quad X = E_{12}, \quad Y = E_{21} \in \text{Mat}(2, k).$$

Доказать, что

$$[X, Y] = H, \quad [H, X] = 2X, \quad [H, Y] = -2Y. \quad (22)$$

ТЕОРЕМА 5.53. Алгебра $sl(2, k)$ проста, если $\text{char } k \neq 2$.

ДОКАЗАТЕЛЬСТВО. Пусть $0 \neq I \triangleleft sl(2, k)$, и $u = \alpha X + \beta Y + \gamma H \in I \setminus 0$. Тогда по (22)

$$[X, u] = \beta[X, Y] + \gamma[X, H] = \beta H - 2\gamma X \in I. \quad (23)$$

Кроме того, $[X, [X, u]] = \beta[H, X] = 2\beta X \in I$. Если $\beta \neq 0$, то $X \in I$, и тогда $I = sl(2, k)$ в силу (22).

Пусть $\beta = 0$. По (23) получаем, что $[X, u] = -2\gamma X \in I$. Если $\gamma \neq 0$, то $X \in I$, и поэтому $I = sl(2, k)$.

Пусть $\beta = \gamma = 0$, $\alpha \neq 0$. Тогда снова $X \in I$. \square

ТЕОРЕМА 5.54. Алгебра Ли (\mathbb{R}^3, \times) проста.

ДОКАЗАТЕЛЬСТВО. Убедимся сначала, что (\mathbb{R}^3, \times) – алгебра Ли. Пусть e_1, e_2, e_3 – ортонормированный базис в \mathbb{R}^3 . Тогда можно считать, что

$$[e_1, e_2] = e_3, \quad [e_2, e_3] = e_1, \quad [e_3, e_1] = e_2.$$

Непосредственная проверка показывает, что

$$[x, x] = J(e_1, e_2, e_3) = [[e_1, e_2], e_3] + [[e_2, e_3], e_1] + [[e_3, e_1], e_2] = 0.$$

Кроме того, Якобиан $J(x, y, z)$ кососимметричен. Отсюда выводится (\mathbb{R}^3, \times) – алгебра Ли.

Пусть I – ненулевой идеал в (\mathbb{R}^3, \times) . Можно считать, что $e_1 \in I$. Тогда I содержит $e_3 = [e_1, e_2], e_2 = [e_3, e_1] \in I$. Следовательно, $I = (\mathbb{R}^3, \times)$. \square

Линейные группы и их алгебры Ли

Всюду в этой работе под F понимается либо поле вещественных чисел \mathbb{R} , либо поле комплексных чисел \mathbb{C} .

1. Касательные пространства

ОПРЕДЕЛЕНИЕ 6.1. Подгруппа G в полной линейной группе $\text{GL}(n, F)$ называется *линейной*, если существует такая конечная система многочленов

$$f_s(X_{ij}) \in F[X_{ij} | 1 \leq i, j \leq n], \quad s = 1, \dots, N, \quad (24)$$

что матрица $A = (a_{ij})$ принадлежит G тогда и только тогда, когда $f_s(a_{ij}) = 0$ для всех $s = 1, \dots, N$.

ПРИМЕРЫ 6.2. Подгруппы $O(n, \mathbb{R})$, $SO(n, \mathbb{R})$, $SL(n, F)$ линейны.

ОПРЕДЕЛЕНИЕ 6.3. Если G линейная группа, заданная системой уравнений (24), и $g \in G$, то *касательным пространством* T_g к G в точке g называется линейное пространство, состоящее из всех матриц $dX = (dx_{pq}) \in \text{Mat}(n, F)$ с условием

$$\sum_{p,q} \frac{\partial f_i}{\partial x_{pq}}(g) dx_{pq} = 0, \quad i = 1, \dots, r. \quad (25)$$

Рассмотрим пространство T_E для различных линейных групп.

ПРИМЕР 6.4. Если $G = SL(n, F)$, то G задается одним уравнением

$$f = \det X - 1 = 0.$$

Отсюда T_E задается одним уравнением

$$\frac{\partial f}{\partial x_{pq}} = \frac{\partial(\det X)}{\partial x_{pq}} = \frac{\partial(\sum_{i=1}^n A_{iq} x_{iq})}{\partial x_{pq}} = A_{pq}.$$

Таким образом, $\frac{\partial f}{\partial x_{pq}} = \delta_{pq}$, откуда

$$\sum_{p,q} \frac{\partial f}{\partial x_{pq}} dx_{pq} = \sum_{p,q} \delta_{pq} dx_{pq} = \sum_p dx_{pp} = \text{tr}(dX),$$

т. е. T_E задается уравнением $\text{tr}(dX) = 0$.

ПРИМЕР 6.5. Если $G = O(n, \mathbb{R})$, то G задается одним уравнением ${}^t X \cdot X = E$. Это означает, что для $i, j = 1, \dots, n$

$$\sum_{t=1}^n x_{ti} x_{tj} - \delta_{ij} = 0.$$

Таким образом,

$$\frac{\partial}{\partial x_{rs}} \left(\sum_{t=1}^n x_{ti} x_{tj} - \delta_{ij} \right) = \sum_{t=1}^n \left(\frac{\partial x_{ti}}{\partial x_{rs}} x_{tj} + x_{ti} \frac{\partial x_{tj}}{\partial x_{rs}} \right) = \sum_{t=1}^n (\delta_{tr} \delta_{is} x_{tj} + x_{ti} \delta_{tr} \delta_{js}).$$

Итак,

$$\frac{\partial}{\partial x_{rs}} \left(\sum_{t=1}^n x_{ti} x_{tj} - \delta_{ij} \right) \Big|_E = \sum_{t=1}^n (\delta_{tr} \delta_{is} \delta_{tj} + \delta_{ti} \delta_{tr} \delta_{js}).$$

Отсюда вытекает, что T_E задается уравнениями

$$0 = \sum_{t,s,r=1}^n (\delta_{tr} \delta_{is} \delta_{tj} + \delta_{ti} \delta_{tr} \delta_{js}) dx_{rs} = dx_{ji} + dx_{ij}.$$

Следовательно, T_E состоит из всех кососимметрических матриц $dX = (dx_{ij})$.

Зафиксируем элемент g линейной группы G . Отображение правого сдвига $R_g : G \rightarrow G$, $x \mapsto xg$, является дифференцируемым отображением, поскольку умножение матриц задается линейными функциями от коэффициентов матрицы $x \in G$. Поэтому дифференциал dR_g этого отображения совпадает с матрицей g , т. е.

$$dR_g : T_x \rightarrow T_{xg}, \quad dR_g(dX) = (dX)g. \quad (26)$$

Но $R_{g_1 g_2} = R_{g_1} R_{g_2}$. Следовательно, dR_g задает линейный изоморфизм T_E и T_g , т. е.

$$T_g = T_E g \quad (27)$$

для любого $g \in G$. В частности, справедливо

ПРЕДЛОЖЕНИЕ 6.6. $\dim T_E = \dim T_g$ для любого $g \in G$.

ОПРЕДЕЛЕНИЕ 6.7. Пусть G – линейная группа. Путем из элемента E в элемент $g \in G$ называется такое дифференцируемое отображение $p : [0, 1] \rightarrow G$, что $p(0) = E, p(1) = g$. *Связной компонентой E в G* называется множество всех элементов $g \in G$, обладающим путем из E в g . Группа G *связна*, если $G_E = G$.

ТЕОРЕМА 6.8. *Связная компонента G_E единичного элемента E является нормальной подгруппой в G .*

ДОКАЗАТЕЛЬСТВО. Пусть G_E – связная компонента E , и $g, h \in G_E$ с путями

$$x(t), y(t) : [0, 1] \rightarrow G, \quad x(0) = y(0) = E, \quad x(1) = g, \quad y(1) = h.$$

Тогда $x(t)y(t)$ – дифференцируемый путь из E в gh . Кроме того, получаем дифференцированные пути

$$E \xrightarrow{x(t)^{-1}} X^{-1}, \quad E \xrightarrow{Zx(t)Z^{-1}} ZXZ^{-1}.$$

□

Так как имеется локальная биекция G и T_E в окрестности E , то $T_E(G_E) = T_E(G)$.

УПРАЖНЕНИЕ 6.9. Доказать, что

1. G_E имеет конечный индекс в G ;
2. $O(n, \mathbb{R})$ не связно, а $SO(n, \mathbb{R})$ связно.

УПРАЖНЕНИЕ 6.10. Будет ли группа $SL(n, \mathbb{R})$ связна?

ПРЕДЛОЖЕНИЕ 6.11. Пусть $x : [0, 1] \rightarrow G$ — дифференцируемый путь в группе G . Если $t_0 \in [0, 1]$ и $g = x(t_0) \in G$, то $x'(t_0) \in T_g(G)$.

ДОКАЗАТЕЛЬСТВО. Пусть G задается системой алгебраических уравнений (24), и $x(t) = (x_{ij}(t))$. Тогда

$$f_s(x_{ij}(t)) = 0, \quad i = 1, \dots, N,$$

для любого $t \in [0, 1]$. Следовательно, используя правило дифференцирования сложной функции, для любого $s = 1, \dots, N$ получаем

$$\frac{\partial f_s}{\partial x_{pq}}(g)x'_{pq}(t_0) = 0.$$

Отсюда в силу определения 6.3 получаем требуемое утверждение. \square

ТЕОРЕМА 6.12. Пусть группа G связна. Тогда G определяется T_E .

ДОКАЗАТЕЛЬСТВО. Пусть $X \in G$ и $x(t)$ — путь из E в X . Тогда

$$x(t)' \in T_{x(t)} = T_E x(t)$$

для всех $t \in [0, 1]$ в силу (27). Итак,

$$x(t)' = A(t)x(t), \quad A(t) \in T_E \text{ для всех } t \in [0, 1]. \quad (28)$$

Обратно, если $A \in T_E$, то рассмотрим дифференциальное уравнение (28), где $A(t) = A$ с начальным условием $x(0) = E$. Оно имеет и притом единственное решение.

Выберем в векторном пространстве $\text{Mat}(n, F)$ такую новую систему координат $y_j, j = 1, \dots, n^2$, что T_E задается системой уравнений $y_i = 0$, где i пробегает первые d индексов. Тогда существует локальная биекция T_E и G . Поэтому решение (28) лежит в G .

Но это решение есть $\exp At$. Таким образом, $\exp : T_E \rightarrow G$ является локальной биекцией в окрестности U точки E . Так как отображение $x \mapsto x^{-1}$ непрерывно дифференцируемо, то можно считать, что $U^{-1} \subseteq U$. Обозначим через H множество всех произведений элементов из U . Если $x \in H$, то $xU \subseteq H$ является открытым подмножеством в G .

Пусть $G \setminus H$ непусто и $z \in G \setminus H$. Если $zU \cap H$ непусто, то $zu = u_1 \cdots u_t$, где $u, u_j \in U$. Отсюда $z = u_1 \cdots u_t u^{-1} \in H$, так как $u^{-1} \in U$. Следовательно, $zU \cap H$ пусто. Итак, G является объединением двух непересекающихся открытых подмножеств $G = H \cup (G \setminus H)$. Пусть $g \in G \setminus H$ и $x : [0, 1] \rightarrow G$, где $x(0) = E$, $x(1) = g$. Тогда отрезок $[0, 1]$ является объединением двух непересекающихся открытых непустых подмножеств $x^{-1}(H)$, $x^{-1}(G \setminus H)$, что невозможно. \square

ПРИМЕРЫ 6.13. Рассмотрим экспоненциальное для ряда групп их порождающих элементов.

1. Пусть $G = \text{SL}(n, \mathbb{C})$. Тогда $T_E = \text{sl}(n, \mathbb{C})$. Базис $\text{sl}(n, \mathbb{C})$ составляют матрицы E_{ij} , $1 \leq i \neq j \leq n$, $E_{ii} - E_{jj}$, $1 \leq i < j \leq n$. При том

$$\exp(E_{ij}) = E + E_{ij}, \quad i \neq j,$$

$$\exp(E_{ii} - E_{jj}) = \text{diag}(1, \dots, 1, \overset{i}{e}, 1, \dots, 1, \overset{j}{e}, 1, \dots, 1).$$

2. Пусть $G = \text{O}(2, \mathbb{R})$, $T_E = \text{o}(2, \mathbb{R})$. Тогда

$$\begin{aligned} \exp \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} &= \exp \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}^{-1} \begin{pmatrix} i\alpha & 0 \\ 0 & -i\alpha \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \right] = \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}^{-1} \begin{pmatrix} \exp(i\alpha) & 0 \\ 0 & \exp(-i\alpha) \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \end{aligned}$$

2. Структура алгебры Ли на T_E

ТЕОРЕМА 6.14. Пусть G – линейная группа, и $A, B \in T_E$. Тогда $[A, B] \in T_E$.

ДОКАЗАТЕЛЬСТВО. Как и в доказательстве теоремы 6.12 $\exp(At), \exp(Bt) \in G$ для всех $t \in \mathbb{F}$. Следовательно,

$$[\exp(A\sqrt{t}), \exp(B\sqrt{t})] \in G \text{ для всех } t \in \mathbb{F}. \quad (29)$$

Вычислим касательный вектор к (29) в точке E . Имеем

$$\exp(A\sqrt{t}) = E + A\sqrt{t} + \frac{A^2 t}{2} + o(t);$$

$$\exp(B\sqrt{t}) = E + B\sqrt{t} + \frac{B^2 t}{2} + o(t);$$

$$\exp(A\sqrt{t})^{-1} = \exp(-A\sqrt{t}) = E - A\sqrt{t} + \frac{A^2 t}{2} + o(t);$$

$$\exp(B\sqrt{t})^{-1} = \exp(-B\sqrt{t}) = E - B\sqrt{t} + \frac{B^2 t}{2} + o(t);$$

Таким образом,

$$\begin{aligned} [\exp(A\sqrt{t}), \exp(B\sqrt{t})] &= \exp(A\sqrt{t}) \exp(B\sqrt{t}) \exp(A\sqrt{t})^{-1} \exp(B\sqrt{t})^{-1} = \\ &= E + (A + B - A - B)\sqrt{t} + \\ &= \left(\frac{A^2}{2} + \frac{B^2}{2} + \frac{A^2}{2} + \frac{B^2}{2} + AB - A^2 - AB - BA - B^2 + AB \right) t + o(t) = \\ &= E + (AB - BA)t + o(t). \end{aligned}$$

□

ОПРЕДЕЛЕНИЕ 6.15. Пусть $G_1 \subseteq \text{GL}(n_1, F)$, $G_2 \subseteq \text{GL}(n_2, F)$, – линейные группы. Гомоморфизм групп $f: G_1 \rightarrow G_2$ называется *гомоморфизм линейных групп*, если существуют такие многочлены

$$f_{ij}(X_{rs}) \in F[X_{rs} | 1 \leq r, s \leq n_1], \quad 1 \leq i, j \leq n_2,$$

что для любого $g = (g_{rs}) \in G_1$ (i, j) -ый коэффициент матрицы $f(g)$ равен $f_{ij}(g_{rs})$.

ТЕОРЕМА 6.16. Если $f: G_1 \rightarrow G_2$ – гомоморфизм линейных групп, то $df|_E: T_E(G_1) \rightarrow T_E(G_2)$ является гомоморфизмом алгебр Ли.

ДОКАЗАТЕЛЬСТВО. Пусть $A \in T_E(G_1)$. Тогда $df|_E(A) = J_E(f)A$, где $J_E(f)$ – значение Якобиана отображения f в точке E . Таким образом, отображение $df|_E$ линейно. Кроме того, $f(\exp(At)) = \exp(df|_E(A)t)$ для любого $t \in F$. Отсюда

$$f([\exp(A\sqrt{t}), \exp(B\sqrt{t})]) = [f(\exp(A\sqrt{t})), f(\exp(B\sqrt{t}))] = [\exp(df|_E(A\sqrt{t})), \exp(df|_E(B\sqrt{t}))]. \quad (30)$$

Дифференцируя равенство (30) по t и полагая $t = 0$ получаем $df|_E([A, B]) = [df|_E(A), df|_E(B)]$, как и в доказательстве теоремы 6.14. \square

СЛЕДСТВИЕ 6.17. Пусть $f : G_1 \rightarrow G_2$ – гомоморфизм линейных групп, причем группа G_1 связна. Тогда $df|_E$ однозначно определяет f .

ТЕОРЕМА 6.18. Пусть A – конечномерная, не обязательно ассоциативная F -алгебра, G – группа ее автоморфизмов, и $\text{Der } A$ – алгебра Ли ее дифференцирований. Тогда группа G линейна и $T_E = \text{Der } A$ – ее алгебра Ли.

ДОКАЗАТЕЛЬСТВО. Пусть $\mathbf{e} = (e_1, \dots, e_n)$ – произвольный базис в A . Тогда для любых $i, j = 1, \dots, n$

$$e_i e_j = \sum_{k=1}^n c_{ij}^k e_k, \quad c_{ij}^k \in F. \quad (31)$$

Если $\alpha \in G$ имеет в базисе \mathbf{e} матрицу (a_{ij}) , то

$$\alpha e_i = \sum_{k=1}^n e_k a_{ki}$$

Следовательно, для всех i, j

$$\begin{aligned} \alpha(e_i)\alpha(e_j) &= \sum_{t,s} e_s a_{si} e_t a_{tj} = \\ &= \sum_{t,s} e_s e_t a_{si} a_{tj} = \sum_{t,s,k} c_{st}^k a_{si} a_{tj} e_k. \end{aligned} \quad (32)$$

С другой стороны, $\alpha(e_i e_j) = \sum_k c_{ij}^k \alpha(e_k) = \sum_{k,l} c_{ij}^k e_l a_{lk}$. Поэтому коэффициенты a_{ij} матрицы α удовлетворяют уравнениями

$$\sum_{k,l} c_{ij}^k e_l a_{lk} = \sum_{t,s,k} c_{st}^k a_{si} a_{tj},$$

и потому группа $G \subseteq \text{GL}(n, F)$ линейна.

Найдем ее алгебру Ли. Элемент

$$D \in T_E \iff \exp(Dt) \in G = \text{Aut } A \text{ для всех } t \in F.$$

Это означает, что для всех $a, b \in A$

$$\exp(Dt)(ab) = \exp(Dt)(a) \exp(Dt)(b).$$

Таким образом,

$$\begin{aligned} (E + \frac{Dt}{1!} + \frac{D^2 t^2}{2!} + \dots)(ab) &= \\ (E + \frac{Dt}{1!} + \frac{D^2 t^2}{2!} + \dots)(a)(E + \frac{Dt}{1!} + \frac{D^2 t^2}{2!} + \dots)(b). \end{aligned} \quad (33)$$

Дифференцируя равенство (33) по t и полагая $t = 0$, получаем

$$D(ab) = D(a)b + aD(b).$$

Итак, $T_E \subseteq \text{Der } A$.

Обратно, пусть $D \in \text{Der } A$. Тогда $Dt \in \text{Der } A$ для всех $t \in F$. Отсюда по формуле Лейбница

$$\begin{aligned} \exp(Dt)(ab) &= \left(E + \frac{Dt}{1!} + \frac{D^2t^2}{2!} + \dots\right)(ab) = \\ &= ab + (D(a)b + aD(b))t + \frac{1}{2!}(D^2(a)b + 2D(a)d(b) + aD^2(bt^n))t^2 + \dots \\ &\quad + \frac{1}{n!}(\sum_{i=0}^n \binom{n}{i} D^i(a)D^{n-i}(b)) + \dots \\ &= \left(a + D(a)t + \frac{D^2(a)t^2}{2!} + \dots\right)\left(b + D(b)t + \frac{D^2(b)t^2}{2!} + \dots\right) = \\ &= \exp(Dt)(a) \exp(Dt)(b). \end{aligned}$$

Итак, $\exp(Dt) \in G$. □

Рассмотрим подробнее свойства связных и несвязных групп Ли.

ТЕОРЕМА 6.19. *Группы*

$$\text{SL}(n, \mathbb{C}), \quad \text{GL}(n, \mathbb{C}), \quad \text{SO}(n, \mathbb{R}), \quad \text{U}(n, \mathbb{C}), \quad \text{SU}(n, \mathbb{C})$$

связны. Группы $\text{GL}(n, \mathbb{R}), \text{O}(n, \mathbb{R})$ несвязны.

ТЕОРЕМА 6.20. *Любая компактная комплексная группа Ли изоморфна абелевой группе \mathbb{C}^n/Γ , где Γ – дискретная подгруппа ранга $2n$ в \mathbb{C}^n .*

ОПРЕДЕЛЕНИЕ 6.21. Гомоморфизм групп Ли $f : G \rightarrow H$ называется *накрывающим*, если выполнено одно из эквивалентных условий:

1. подгруппа $\ker f$ дискретна;
2. $df : T_1(G) \rightarrow T_2(G)$ является изоморфизмом векторных пространств;
3. f индуцирует диффеоморфизм окрестностей x и $f(x)$.

ПРИМЕР 6.22. Гомоморфизм $f : \mathbb{R} \rightarrow \text{U}(1, \mathbb{C})$, $f(x) = \exp(2\pi i x)$ является накрытием.

ТЕОРЕМА 6.23. *Существует накрывающий гомоморфизм $f : \text{SL}(2, \mathbb{C}) \rightarrow \text{SO}(3, \mathbb{C})$ с ядром $\ker f = \pm 1$. При этом $f(\text{SU}(2, \mathbb{C})) = \text{SO}(3, \mathbb{R})$.*

ДОКАЗАТЕЛЬСТВО. Пусть $L = \mathfrak{sl}(2, \mathbb{C})$ – множество матриц со следом нуль, т. е.

$$\mathfrak{sl}(2, \mathbb{C}) = \left\{ \begin{pmatrix} a & c \\ b & -a \end{pmatrix} \mid a, b, c \in \mathbb{C} \right\}.$$

Рассмотрим представление Ad группы $G = \text{SL}(2, \mathbb{C})$ в L по правилу $(\text{Ad } g)(x) = gxg^{-1}$. Заметим, что Ad сохраняет билинейную функцию

$$\begin{vmatrix} a & c \\ b & -a \end{vmatrix} = -a^2 - bc = (ia)^2 + \left[\frac{i(b-c)}{\sqrt{2}} \right]^2 + \left[\frac{i(b+c)}{\sqrt{2}} \right]^2.$$

Следовательно, $\text{Ad } g \in \text{SO}(3, \mathbb{C})$.

Ясно, что $\ker \text{Ad} = \pm 1$. При этом $\text{Im } \text{Ad} = \text{SO}(3, \mathbb{C})$. □

Эта конструкция обобщается на произвольное $n \geq 2$. Именно, пусть C_n – алгебра Клиффорда от стандартной билинейной функции $(x, y) = \sum_{j=1}^n x_j y_j$

на n -мерном пространстве \mathbb{C}^n со стандартным базисом e_1, \dots, e_n . Тогда базис C_n составляют одночлены

$$e_{i_1} \cdots e_{i_m}, \quad 1 \leq i_1 < \dots < i_m \leq n, \quad (34)$$

причем $e_k e_j = -e_j e_k$, при $1 \leq k \neq j \leq n$, $e_j^2 = 1$. Поэтому $\dim C_n = 2^n$, и $C_n = C_n^0 \oplus C_n^1$, где базис C_n^k составляют одночлены (34), у которых $m \equiv k \pmod{2}$. В C_n имеется инволюция,

$$\overline{e_{i_1} \cdots e_{i_m}} = e_{i_m} \cdots e_{i_1}.$$

Положим $N(u) = u\bar{u}$ для любого $u \in C_n$.

Пусть C_n^* – группа обратимых элементов алгебры C_n . Через $\text{Spin}(n, \mathbb{C})$ обозначим подгруппу всех таких

$$u \in (C_n^0)^*, \quad \text{что } N(u) = 1 \text{ и } uC_n u^{-1} = C_n, \quad (35)$$

где \mathbb{C}^n – комплексная линейная оболочка векторов e_1, \dots, e_n .

ОПРЕДЕЛЕНИЕ 6.24. Группа $\text{Spin}(n, \mathbb{C})$ называется *комплексной спинорной группой*.

В силу (35) получается гомоморфизм $\pi : \text{Spin}(n, \mathbb{C}) \rightarrow \text{SO}(n, \mathbb{C})$. Можно показать, что гомоморфизм π сюръективен, и группа $\text{Spin}(n, \mathbb{C})$ связна, $\ker \pi = \pm 1$.

Для описания элементов $\text{Spin}(n, \mathbb{C})$ обозначим через Q^{n-1} все такие $y \in \mathbb{C}^n$, что $y = \sum y_j e_j$ и $\sum y_j^2 = 1$. В этом случае $y \in C_n^*$, и $\text{Spin}(n, \mathbb{C})$ состоит из произведения четного числа элементов Q^{n-1} .

Пусть $n = 2l + 1$ – нечетно. Тогда алгебра $C_n^0 \simeq \text{Mat}(2^l, \mathbb{C})$. Следовательно, в ней имеется простой левый идеал I размерности 2^l . Тем самым возникает неприводимое представление $\text{Spin}(2l + 1, \mathbb{C})$, называется *спинорным представлением*.

Если $n = 2l$, то алгебра C_n проста, и поэтому имеется представление $\text{Spin}(2l, \mathbb{C})$ в простом левом идеале J размерности 2^l . Снова возникает спинорное представление, но оно приводимо и разлагается в прямую сумму двух подпредставлений

$$J = (J \cap C_n^0) \oplus (J \cap C_n^1).$$

ОПРЕДЕЛЕНИЕ 6.25. Группа Ли G *односвязна*, если в G любой путь стягивается в точку.

ТЕОРЕМА 6.26. *Любая связная группа Ли G имеет вид $G \simeq \tilde{G}/N$, где \tilde{G} – односвязная группа Ли, и N – дискретный центральный нормальный делитель. Пара \tilde{G}, N определена однозначно.*

ОПРЕДЕЛЕНИЕ 6.27. Группа \tilde{G} называется *односвязным накрытием G* .

ПРИМЕРЫ 6.28. Следующие группы односвязны: $\text{SL}(n, \mathbb{C})$, $\text{SU}(n, \mathbb{C})$, $\text{Spin}(n, \mathbb{C})$. Имеются следующие односвязные накрытия:

1. $\mathbb{R} \rightarrow \text{U}(1, \mathbb{C})$;
2. $\text{SL}(2, \mathbb{C}) \rightarrow \text{SO}(3, \mathbb{C})$;
3. $\text{SU}(2, \mathbb{C}) \rightarrow \text{SO}(3, \mathbb{R})$;
4. $\text{SL}(2, \mathbb{C}) \times \text{SL}(2, \mathbb{C}) \rightarrow \text{SO}(4, \mathbb{C})$;
5. $\text{SL}(4, \mathbb{C}) \rightarrow \text{SO}(6, \mathbb{C})$.

При этом в силу единственности накрытия

$$\begin{aligned}\mathrm{Spin}(3, \mathbb{C}) &\simeq \mathrm{SL}(2, \mathbb{C}), & \mathrm{Spin}(4, \mathbb{C}) &\simeq \mathrm{SL}(2, \mathbb{C}) \times \mathrm{SL}(2, \mathbb{C}), \\ \mathrm{Spin}(6, \mathbb{C}) &\simeq \mathrm{SL}(4, \mathbb{C}).\end{aligned}$$

3. Представления групп Ли

ОПРЕДЕЛЕНИЕ 6.29. *Представлением* линейной группы G в комплексном пространстве V называется гомоморфизм линейных групп $\phi : G \rightarrow \mathrm{GL}(V)$ в смысле определения 6.15. Другими словами, если в V выбран базис, то ϕ задает гомоморфизм линейных групп $\phi : G \rightarrow \mathrm{GL}(n, \mathbb{C})$

ТЕОРЕМА 6.30. *Пусть G компактная группа Ли. Тогда на G существует и единственный такой интеграл $\int_G f(g)dg$ для каждой аналитической функции f на G , что он*

1. *линеен относительно функции f ;*
2. *$\int_G dg = 1$, $\int_G |f(g)|^2 dg > 0$, если $f \neq 0$;*
3. *$\int_G f(g)dg = \int_G f(g^{-1})dg = \int_G f(gh)dg = \int_G f(hg)dg$, если $h \in G$.*

СЛЕДСТВИЕ 6.31. *Пусть задано представление $\phi : G \rightarrow \mathrm{GL}(V)$, где $\dim V < \infty$. Вводится скалярное произведение (x, y) . Введем новое скалярное произведение $\langle x, y \rangle = \int_G (\phi(g)x, \phi(g)y)dg$. В силу свойств интеграла каждый оператор $\phi(h)$, $h \in G$, унитарен.*

СЛЕДСТВИЕ 6.32. *Любое конечномерное представление компактной группы Ли вполне приводимо.*

ТЕОРЕМА 6.33. *Любое неприводимое комплексное представление компактной группы Ли конечномерно.*

ТЕОРЕМА 6.34. *Группа всех унитарных матриц $\mathrm{U}(n, \mathbb{C})$ является максимальной компактной подгруппой в $\mathrm{GL}(n, \mathbb{C})$. Любая другая максимальная компактная подгруппа в $\mathrm{GL}(n, \mathbb{C})$ сопряжена с $\mathrm{U}(n, \mathbb{C})$. Группа всех ортогональных матриц $\mathrm{O}(n, \mathbb{R})$ является максимальной компактной подгруппой в $\mathrm{GL}(n, \mathbb{R})$. Любая другая максимальная компактная подгруппа в $\mathrm{GL}(n, \mathbb{R})$ сопряжена с $\mathrm{O}(n, \mathbb{R})$.*

ОПРЕДЕЛЕНИЕ 6.35. *Группа Ли полупроста, если в ней нет неединичных связных нормальных абелевых подгрупп.*

ПРИМЕР 6.36. *Группы $\mathrm{SL}(n, \mathbb{C})$, $\mathrm{SU}(n, \mathbb{C})$, $\mathrm{SO}(3, \mathbb{R})$ полупросты.*

ТЕОРЕМА 6.37. *Любая связная полупростая группа Ли допускает точное линейное представление.*

ОПРЕДЕЛЕНИЕ 6.38. *Максимальным тором* в группе Ли G называется максимальная подгруппа Ли, являющаяся прямым произведением групп \mathbb{C}^* .

ПРИМЕРЫ 6.39. *Максимальный тор*

- в $\mathrm{GL}(n, \mathbb{C})$ – подгруппа диагональных матриц $D(n, \mathbb{C})$,*
- в $\mathrm{SL}(n, \mathbb{C})$ – подгруппа диагональных матриц $D(n, \mathbb{C}) \cap \mathrm{SL}(n, \mathbb{C})$,*
- в $\mathrm{SO}(n, \mathbb{C})$ – подгруппа диагональных матриц $D(n, \mathbb{C}) \cap \mathrm{SO}(n, \mathbb{C})$.*

ТЕОРЕМА 6.40. *В связной компактной группе Ли максимальный тор является максимальной связной коммутативной подгруппой Ли. Все такие подгруппы сопряжены.*

ОПРЕДЕЛЕНИЕ 6.41. Максимальная связная разрешимая подгруппа Ли B^+ в группе Ли G называется *подгруппой Бореля*.

Заметим, что B^+ содержит максимальный тор H .

ТЕОРЕМА 6.42 (Морозов, Борель). Все подгруппы Бореля B^+ связной комплексной группы Ли G сопряжены между собой в G .

ПРИМЕРЫ 6.43. Если $G = \mathrm{GL}(n, \mathbb{C})$, то $B^+ = T(n, \mathbb{C})$. Если G – одна из групп $\mathrm{SO}(n, \mathbb{C})$, $\mathrm{SL}(n, \mathbb{C})$, $\mathrm{SU}(n, \mathbb{C})$, то $B^+ = T(n, \mathbb{C}) \cap G$.

ОПРЕДЕЛЕНИЕ 6.44. Пусть $\phi : G \rightarrow \mathrm{GL}(n, \mathbb{C})$ – комплексное представление группы Ли G . Для любого гомоморфизма $\chi : G \rightarrow \mathbb{C}^*$ через V_χ обозначим подпространство

$$V_\chi = \{v \in V \mid \phi(g)v = \chi(g)v \text{ для любого } g \in G\}.$$

Ненулевое подпространство V_χ называется *весовым*, ненулевые векторы из V_χ называются *весовыми*, а функция χ в этом случае называется *весом*.

Если H – максимальный тор в G , то H является компактной абелевой группой. Следовательно, все ее неприводимые представления одномерны. Поэтому если задано конечномерное представление $\phi : G \rightarrow \mathrm{GL}(V)$ связной компактной группы Ли G с максимальным тором H , то

$$V = \bigoplus_{j=1}^s V_{\lambda_j}(H).$$

ОПРЕДЕЛЕНИЕ 6.45. Весовой вектор $v \in V_{\lambda_j} \setminus 0$ для H называется *старшим*, если для каждого элемента $g \in B^+$ найдется такое число $\chi_g \in \mathbb{C}$, что $\phi(g)v = \chi_g v$.

В частности, старший вес задает гомоморфизм $\chi : B^+ \rightarrow \mathbb{C}^*$.

ТЕОРЕМА 6.46. Неприводимое конечномерное представление связной полупростой алгебраической группы G однозначно, с точностью до эквивалентности определяется своим старшим весом.

ПРИМЕР 6.47. Пусть $G = \mathrm{SL}(2, \mathbb{C})$. Тогда имеется естественное представление G в пространстве P_n однородных комплексных многочленов от X, Y степени n , именно,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ f(X, Y) = f(aX + bY, cX + dY).$$

Борелевская подгруппа B^+ состоит из всех верхнетреугольных матриц

$$B = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad a, d \in \mathbb{C}^*, \quad b \in \mathbb{C}.$$

Старшим вектором этого представления является многочлен Y^n , так как $B \circ Y^n = a^{-n} Y^n$.

Легко видеть, что $-E$ действует при этом представлении тождественно, если n четно. Следовательно, при четном $n = 2k$ получается неприводимое представление $\mathrm{SO}(3, \mathbb{C}) \simeq \mathrm{SL}(2, \mathbb{C})/\{\pm E\}$ степени $2k + 1$.

ПРИМЕР 6.48. Пусть P_n как и выше. Заметим, что $\mathrm{SU}(2, \mathbb{C})$ состоит из всех матриц вида

$$\begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix}, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1.$$

Определим представление $SU(2, \mathbb{C})$ в P_n как ограничение представления $SL(2, \mathbb{C})$ из примера 6.47 на подгруппу $SU(2, \mathbb{C})$. Получается неприводимое представление $SU(2, \mathbb{C})$ со старшим вектором X^n . Действительно,

$$B^+ = SU(2, \mathbb{C}) \cap T(2, \mathbb{C}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & \bar{a} \end{pmatrix} \mid a \in \mathbb{C}, \quad |a| = 1 \right\},$$

и поэтому

$$\begin{pmatrix} a & 0 \\ 0 & \bar{a} \end{pmatrix} \circ X^n = a^n X^n.$$

При четном $n = 2k$ получается неприводимое комплексное представление $SO(3, \mathbb{R})$ степени $2k + 1$.

Представление из примера 6.48 можно описать по-другому. Пусть H_n – пространство всех однородных комплексных многочленов f степени n , удовлетворяющих дифференциальному уравнению

$$\Delta f = 0, \quad \Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}.$$

Действие $SO(3, \mathbb{R})$ индуцировано естественным действием на координатах трехмерных векторов. Это представление имеет степень $2n + 1$ над \mathbb{R} , и оно эквивалентно представлению в P_n . Таким образом, получаются все неприводимые представления $SO(3, \mathbb{R})$.

Литература

- [1] Бурбаки Н. Группы и алгебры Ли. Главы 1 - 3. М.: Мир, 1976.
- [2] Бурбаки Н. Группы и алгебры Ли. Главы 4 - 6. М.: Мир, 1972.
- [3] Бурбаки Н. Группы и алгебры Ли. Главы 7, 8. М.: Мир, 1978.
- [4] Бурбаки Н. Группы и алгебры Ли. Глава 9. М.: Мир, 1986.
- [5] Винберг Э. Б., Онищик А. Л. Основы теории групп. В кн.: Итоги науки и техники, Современные проблемы математики. Фундментальные направления. т. 20, Группы и алгебры Ли 1. 1988, М.: ВИНТИ, С. 5-101.
- [6] Винберг Э. Б., Горбацевич В. В., Шварцман О. В. Дискретные подгруппы групп Ли. В кн.: Итоги науки и техники, Современные проблемы математики. Фундментальные направления. т. 21, Группы и алгебры Ли 2. 1988, М.: ВИНТИ, С. 7-120.
- [7] Винберг Э. Б., Горбацевич В. В., Онищик А. Л. Строение групп и алгебр Ли. В кн.: Итоги науки и техники, Современные проблемы математики. Фундментальные направления. т. 41, Группы и алгебры Ли 3. 1990, М.: ВИНТИ, С. 5-255.
- [8] Кострикин А. И. Введение в алгебру. М.: Наука, 1977.
- [9] Курош А. Г. Теория групп. М.: Наука, 1967.
- [10] Лейтес Д. А. Супералгебры Ли. В кн.: Итоги науки и техники, Современные проблемы математики. Новейшие достижения. т. 25, 1984, М.: ВИНТИ, С. 3-49.
- [11] Лезнов А. Н., Савельев М. В. Групповые методы интегрирования нелинейных динамических систем. М.: Наука, 1985.
- [12] Манин Ю. И. Калибровочные поля и комплексная геометрия. М.: Наука, 1984.
- [13] Шафаревич И. Р. Основные понятия алгебры. В кн.: Итоги науки и техники, Современные проблемы математики. Фундаментальные направления. т. 11, 1986, М.: ВИНТИ, 288С.
- [14] Уэст П. Введение в супергеометрию и супергравитацию. М.: Мир, 1989.
- [15] Петрашень М. И., Трифонов Е. Д. Применение теории групп в квантовой механике. 1999, М.: УРСС.