ЛЕКЦИЯ 11

ПРОСТОТА ГРУППЫ SO_3

ГРУППЫ ИЗ ВОСЬМИ ЭЛЕМЕНТОВ

ПОЛУПРЯМЫЕ ПРОИЗВЕДЕНИЯ

ГРУППЫ ИЗ 12 ЭЛЕМЕНТОВ

ПРОСТОТА ГРУППЫ $\mathbf{SO}_3$

В качестве примера использования геометрических соображений для доказательства простоты группы докажем, что группа $\mathbf{SO}_3$ проста.

$\mathbf{SO}_n$ — это группа всех движений евклидова пространства $\mathbb{R}^n$, сохраняющих ориентацию пространства.

В частности, интересующая нас сейчас группа $\mathbf{SO}_3$ — это группа движений трехмерного пространства, сохраняющих ориентацию пространства.

Рассмотрим произвольную матрицу $A \in \mathbf{SO}_3$. Если представить ее как комплексную матрицу, то она имеет три собственных значения: $\alpha_1, \alpha_2, \alpha_3$ (корни характеристического многочлена).

Заметим, что в курсе линейной алгебры доказывалось, что ортогональное пребразование всегда диагонализируемо на $\mathbb{C}$ (так как любое подпространство, являющееся ортогональным дополнением к инвариантному, само является инвариантным).

Если α — какое-то собственное значение, а v_α — соответствующий собственный вектор (возможно, с комплексными координатами), то $|\alpha| = 1$ (так как собственный вектор под действием движения не может изменять длину). Значит, возможны следующие корни характеристического многочлена (с учетом того, что их произведение равно единице, и что невещественные корни могут встречаться только в парах со своими сопряженными):

— $1, 1, 1$ (и тогда преобразование тождественно);

— $1, -1, -1$;

— $1, \cos\theta + i\sin\theta, \cos\theta - i\sin\theta$.

Таким образом, мы видим, что всегда существует собственный вектор с единичным собственным значением, т.е. прямая, точки которой отсаются на месте при преобразовании A.

Ортогональное дополнение к этой прямой (перпендикулярная плоскость) будет инвариантным подпространством для A. Ясно, что на нем A действует как поворот на угол θ, а матрица A принимает вид

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

Таким образом, мы доказали, что любой элемент группы $\mathbf{SO}_3$ есть поворот вокруг какой-то оси на определенный угол α.

Преобразование, сопряженное с помощью элемента $g \in \mathbf{SO}_3$ повороту на угол α вокруг оси l, — это поворот на тот же угол вокруг оси gl.

Действительно, ясно, что у сопряженного отображения те же собственные значения, что и у исходного, поэтому поворот будет на тот же угол, что и у исходного. Осталось понять, какой вектор будет неподвижным (собственным со значением 1) у сопряженного отображения.

Пусть v — неподвижный вектор отображения A. Рассмотрим вектор gv. Тогда отображение gAg^{-1} действует на него так:

$$gAg^{-1}(gv) = gA(v) = gv,$$

т.е. прямая gl — неподвижная для сопряженного отображения.

Значит, всякая нормальная подгруппа группы $\mathbf{SO}_3$ вместе с поворотом на угол α вокруг какой-либо оси должна содержать поворот на угол α вокруг любой оси.

Легко видеть, что произведение поворотов на π вокруг осей m и m', образующих угол γ, есть поворот на угол 2γ вокруг оси, перпендикулярной плоскости осей m и m': ось, перпендикулярная прямым m и m', останется недвижимой, так как повернется два раза подряд на угол π; ось m сначала останется на месте, а под действием второго преобразования повернется на 2γ (так как это будет отражение оси m относительно оси m').

Предположим теперь, что $N \lhd \mathbf{SO}_3$ — нормальная подгруппа, содержащая поворот на угол $\alpha \in (0, 2\pi)$ вокруг какой-то оси l.

Пусть g — поворот на π вокруг оси m, образующей с осью l угол $\theta \in [0, \pi/2]$. Тогда

$$h = g(sgs^{-1}) = (gsg^{-1})s^{-1} \in N;$$

но так как sgs^{-1} есть поворот на π вокруг оси sm, то, согласно предыдущему замечанию, h есть поворот на угол 2γ, где γ — угол между m и sm. Угол γ равен нулю при $\theta = 0$ и равен α при $\theta = \pi/2$. Из соображений непрерывности следует, что он может принимать все значения на отрезке $[0, \alpha]$. Следовательно, группа N содержит повороты на все углы из отрезка $[0, 2\pi]$. Возведением этих поворотов в степени можно получить поворот на любой угол. Это показывает, что $N = \mathbf{SO}_3$.

Таким образом, мы доказали следующую теорему:

Теорема 1. *Группа* $\mathbf{SO}_3$ *проста.*

Можно показать, что группа $\mathbf{SO}_n$ проста при любом $n \geq 3$, за исключением $n = 4$.

ГРУППЫ ИЗ 8 ЭЛЕМЕНТОВ

Теорема 2 (классификация групп из 8 элементов). *Любая группа из 8 элементов изоморфна одной из следующих*:

1) $\mathbb{Z}_8$;
2) $\mathbb{Z}_4 \oplus \mathbb{Z}_2$;
3) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$;
4) $\mathbf{D}_4$;
5) $\mathbb{Q}_8$.

Никакие две из пересиленных выше групп не изоморфны друг другу.

Доказательство. Пусть $|G| = 8$.

Если группа G абелева, то она изоморфна одной из первых трех перечиленных выше групп, по теореме о классификации конечных абелевых групп. Ясно, что эти группы не изоморфны друг другу и оставшимся двум группам.

Пусть теперь G — неабелева.

Если бы в группе G имелся бы элемент порядка восемь, то она оказалась бы циклической, т.е. абелевой, что невозможно.

Если бы в группе G все элементы имели бы порядок два, то она также была бы абелева.

Значит, в группе G все элементы имеют либо порядок два, либо четыре, при этом есть хотя бы один элемент порядка четыре. Обозначим его через a. Подгруппа $\langle a \rangle$ состоит из четырех элементов.

Пусть вне этой подгруппы имеется элемент b порядка два.

В этом случае все элементы

$$a^k b^l, \qquad k = 0, 1, 2, 3, \quad l = 0, 1,$$

различны. Так как их всего восемь, то любой элемент группы представляется в виде $a^k b^l$.

Подгруппа $\langle a \rangle$ имеет в группе G индекс два, поэтому она нормальна. Значит,

$$bab^{-1} = a^k.$$

Это означает, что либо $bab^{-1} = a$, либо $bab^{-1} = a^{-1}$. Первый случай невозможен, так как группа неабелева. Значит, выполнено второе соотношение.

Таким образом, данная группа изоморфна группе $\mathbf{D}_4$ движений квадрата.

Теперь рассмотрим оставшийся случай: вне подгруппы $\langle a \rangle$ все элементы имеют порядок четыре. Рассмотрим произвольный элемент $b \in G \backslash \langle a \rangle$. Ясно, что b^2 (как элемент порядка два) должен совпасть с a^2. Таким образом, $a^2 = b^2 = c$ — это элемент центра групп G. Как и в предыдущем случае, $bab^{-1} = a^{-1} = ca$.

Если мы обозначим c через -1, a — через i, b — через j, а ab — через k, то полученная группа совпадет с $\mathbb{Q}_8$. $\square$

ПОЛУПРЯМЫЕ ПРОИЗВЕДЕНИЯ ГРУПП

Ранее мы описывали ситуации, когда в группе G есть две подгруппы — N_1 и N_2, такие, что:

- N_1, N_2 обе нормальны в G;
- $N_1 \cap N_2 = \{e\}$;
- $N_1 N_2 = G$ (или $|N_1| \cdot |N_2| = |G|$).

В этом случае оказывалось, что группа G является прямым произведением $N_1 \times N_2$.

Мы сейчас обсудим чуть более общую ситуацию — когда в группе G есть две подгруппы N и H такие, что:

- N нормальна в G;
- $N \cap H = \{e\}$;
- $NH = G$ (или $|N| \cdot |H| = |G|$).

Лемма 1. *При таких условиях любой элемент g группы G однозначно представляется в виде $g = nh$, где $n \in N$, $h \in H$.*

Доказательство. Действительно, если $nh = n'h'$, то ${n'}^{-1}n = h'h^{-1}$, т.е. элемент из группы H равен элементу из группы N. Так как эти группы пересекаются только по единице, мы имеем ${n'}^{-1}n = h'h^{-1} = e$. Отсюда $n = n'$, $h = h'$. $\square$

Лемма 2. *В описанной выше ситуации существует гомоморфизм*

$$\varphi : H \to \operatorname{Aut} N$$

из подгруппы H в группу автоморфизмов группы N такой, что для любых $g = nh$, $g' = n'h'$, $n, n' \in N$, $h, h' \in H$, выполнено

$$gg' = nhn'h' = n(\varphi(h))(n')hh'.$$

Таким образом, группа G полностью определяется подгруппами N, H и гомоморфизмом φ.

Доказательство. Действительно, пусть $g = nh$, $g' = n'h'$. Тогда

$$gg' = nhn'h' = n(hnh^{-1})hh'.$$

Так как подгруппа N нормальна в G, то $hnh^{-1} \in N$. Ясно, что для каждого $h \in H$ отображение, сопоставляющее каждому $n \in N$ элемент $hnh^{-1} \in N$, является автоморфизмом.

Это означает, что мы можем построить отображение $\varphi : H \to \operatorname{Aut} N$, сопоставляющее каждому $h \in H$ соответствующий автоморфизм. Ясно, что это отображение является гомоморфизмом. □

Лемма 3. *Если фиксированы две группы — N и H — и некоторый гомоморфизм $\varphi : H \to \operatorname{Aut} N$, то по ним однозначно (с точностью до изоморфизма) строится группа G, содержащая подгруппы, изоморфные N и H такими, что $N \lhd G$, $N \cap H = \{e\}$, $NH = G$, для всех $g = nh, g'n'h'$*

$$gg' = nhn'h' = n(\varphi(h))(n')hh'.$$

Доказательство. Сначала докажем, что такая группа всегда существует.

Действительно, группу G можно задавать как состоящую из пар (n, h), $n \in N$, $h \in H$, с законом умножения

$$g \cdot g' = (n, h)(n', h') = (n(\varphi(h))(n'), hh').$$

Нам требуется доказать, что такой закон задает группу, то есть проверить ассоциативность, существование единицы и существование обратного.

- *Ассоциативность.*

$$\begin{gathered}((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) = (n_1(\varphi(h_1))(n_2), h_1h_2) \cdot (n_3, h_3) = \\ = (n_1(\varphi(h_1))(n_2)(\varphi(h_1h_2))(n_3), h_1h_2h_3) = \\ = (n_1(\varphi(h_1))(n_2(\varphi(h_2))(n_3)), h_1h_2h_3) = \\ = (n_1, h_1) \cdot (n_2(\varphi(h_2))(n_3), h_2h_3) = (n_1, h_1) \cdot ((n_2, h_2) \cdot (n_3, h_3)).\end{gathered}$$

- *Нейтральный элемент.*

$$(e_N, e_H) \cdot (n, h) = (e_N(\varphi(e_H))(n), e_Hh) = (n, h).$$

- *Наличие обратного.*

$$\begin{aligned}&(n, h) \cdot ((\varphi^{-1}(h))(n^{-1}), h^{-1}) = \\ &\qquad = (n \cdot (\varphi(h))(\varphi^{-1}(h))(n^{-1}), hh^{-1}) = (nn^{-1}, e_H) = (e_N, e_H).\end{aligned}$$

Таким образом, искомое полупрямое произведение всегда существует.

Очевидно, что построенная группа единственна с точностью до изоморфизма, так как ее таблица умножения (как мы видели выше) задается однозначно.

□

ГРУППЫ ИЗ 12 ЭЛЕМЕНТОВ

Теперь поставим задачу найти все группы из 12 элементов.

В группе из 12 элементов число n_2 силовских 2-подгрупп (из четырех элементов) может быть равно единице или трем, а число n_3 силовских 3-подгрупп (из трех элементов) — одному или четырем. Случай $1 : 1$ означает, что обе подгруппы нормальны, то есть группа G есть прямое произведение своих силовских подгрупп. Так как группы из трех и четырех элементов — абелевы, то мы получи в результате абелеву группу, т.е. одну из двух: $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_{12}$ или $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

Пусть теперь группа не является прямым произведением. Для начала предположим, что $n_2 = 3$, $n_3 = 4$.

В этом случае мы имеем четыре группы из трех элементов, пересекающиеся только по единичному. Таким образом, элементов порядка три должно быть восемь штук. Остается всего 4 элемента, которые могут образовать не более одной группы порядка четыре. Значит, такой случай невозможен.

Остается четыре случая:

- нормальна подгруппа порядка три (изоморфная $\mathbb{Z}_3$), а подгруппа порядка четыре изоморфна $\mathbb{Z}_4$;
- нормальна подгруппа порядка три (изоморфная $\mathbb{Z}_3$), а подгруппа порядка четыре изоморфна $\mathbf{V}_4$;
- нормальна подгруппа порядка четыре, изоморфная $\mathbb{Z}_4$;
- нормальна подгруппа порядка четыре, изоморфная $\mathbf{V}_4$.

В первом случае мы получаем полупрямое произведение группы $\mathbb{Z}_3$ на группу $\mathbb{Z}_4$, т.е. группа $\mathbb{Z}_4$ действует сопряжениями на группу $\mathbb{Z}_3$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbb{Z}_4$ в группу автоморфизмов группы $\mathbb{Z}_3$.

Группа автоморфизмов группы $\mathbb{Z}_3$ изоморфна $\mathbb{Z}_2$ (единственным нетривиальным автоморфизмом является перестановка элементов 1 и 2 в $\mathbb{Z}_3$).

Именно в этот автоморфизм может отобразиться образующий из $\mathbb{Z}_4$.

Таким образом, группа G в данном случае задается следующими образующими и соотношениями:

$$a, b; \qquad a^3 = b^4 = e, \quad bab^{-1} = a^{-1}.$$

Названия у данной группы нет, ее центр состоит из двух элементов: $\{b^2, e\}$, коммутант порождается элементом a.

Во втором случае мы получаем полупрямое произведение группы $\mathbb{Z}_3$ на группу $\mathbf{V}_4$, т.е. группа $\mathbf{V}_4$ действует сопряжениями на группу $\mathbb{Z}_3$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbf{V}_4$ в группу автоморфизмов группы $\mathbb{Z}_3$.

Если обозначить образующий группы $\mathbb{Z}_3$ за a, нетривиальный автоморфизм этой группы - за ξ, образующие группы $\mathbf{V}_4$ — за b и c, то видим, что каждая из образующих b и c отображается либо в ξ, либо в e.

Пусть b отображается в ξ. Тогда если c отображается вξ, то bc отображается в e, а если c отображается в e, то bc отображается в ξ. Оба такие гомоморфизмы дадут в результате изоморфные группы, так как замена местами c и bc — это автоморфизм группы $\mathbf{V}_4$.

Значит, рассмотрим гомоморфизм

$$b \mapsto \xi, \quad c \mapsto e.$$

Он задаст группу G в виде образующих и соотношений:

$$a, b, c; \qquad a^3 = b^2 = c^2 = e, \quad bc = cb \quad ac = ca, \quad bab^{-1} = a^{-1}.$$

Сразу видно, что подгруппа (порядка два), порожденная элементом c, коммутирует со всеми остальными образующими, т.е. выделяется прямым слагаемым.

Образующие b и a порождают группу $\mathbf{D}_3 = \mathbf{S}_3$. Таким образом, мы получаем группу $\mathbf{D}_3 \oplus \mathbb{Z}_2 = \mathbf{D}_6$.

Во третьем случае мы получаем полупрямое произведение группы $\mathbb{Z}_4$ на группу $\mathbb{Z}_3$, т.е. группа $\mathbb{Z}_3$ действует сопряжениями на группу $\mathbb{Z}_4$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbb{Z}_3$ в группу автоморфизмов группы $\mathbb{Z}_4$.

У группы $\mathbb{Z}_4$ есть (как и у $\mathbb{Z}_3$) лишь один нетривиальный автоморфизм, при котором 1 и 3 меняются местами. Этот автоморфизм имеет порядок два.

Однако мы не можем построить нетривиальный гомоморфизм из группы $\mathbb{Z}_3$ в группу $\mathbb{Z}_2$, поэтому никакого нетривиального полупрямого произведения не может возникнуть.

Во последнем случае мы имеем полупрямое произведение группы $\mathbf{V}_4$ на группу $\mathbb{Z}_3$, т.е. группа $\mathbb{Z}_3$ действует сопряжениями на группу $\mathbf{V}_4$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbb{Z}_3$ в группу автоморфизмов группы $\mathbf{V}_4$.

Как мы помним, группа автоморфизм группы $\mathbf{V}_4$ изоморфна $\mathbf{S}_3$ (можно произвольным образом переставить три неединичных элемента), поэтому нетривиальный гомоморфизм из $\mathbb{Z}_3$ можно устроить, переведя образующий этой группы (обозначим его через a) в “цикл длины три”.

В виде образующих и соотношений это будет означать следующее:

$$a, b, c; \qquad a^3 = b^2 = c^2 = e, \\ bc = cb, \quad aba^{-1} = c, \quad aca^{-1} = bc, \quad a(bc)a^{-1} = b.$$

Легко доказать, что эта группа изоморфна $\mathbf{A}_4$ ($a \mapsto (123)$, $b \mapsto (12)(34)$, $c \mapsto (14)(23)$).

Таким образом, мы доказали следующую теорему:

Теорема 3 (классификация групп из 12 элементов). *Любая группа из* 12 *элементов изоморфна одной из следующих*:
1) $\mathbb{Z}_12$;
2) $\mathbb{Z}_2 \oplus \mathbb{Z}_6$;
3) $\langle a, b \mid a^3 = b^4 = e,\ bab^{-1} = a^{-1} \rangle$;
4) $\mathbf{D}_6$;
5) $\mathbf{A}_4$.

Никакие две из перечисленных выше групп не изоморфны друг другу.