ЛЕКЦИЯ 11

ПРОСТОТА ГРУППЫ $\mathbf{A}_n$

ДОКАЗАТЕЛЬСТВО НЕПРОСТОТЫ НЕКОТОРЫХ КОНЕЧНЫХ ГРУПП

ПРОСТОТА ГРУППЫ $\mathbf{SO}_3$

ПРОСТОТА ГРУППЫ $\mathbf{A}_n$

Мы доказываем теорему о том, что при $n \geqslant 5$ группа $\mathbf{A}_n$ является простой.

Теорема 1. $\mathbf{A}_n$, $n \geqslant 5$, — *простая* (*некоммутативная*) *группа.*

Доказательство. Пусть $\{e\} \neq H \lhd \mathbf{A}_n$.

Если $\sigma = (a\,b\,c) \in H$, то теорема доказана, так как циклы длины три сопряжены в A_n, $n \geqslant 5$, и порождают A_n.

Пусть H содержит некоторую подстановку σ, в разложении которой на непересекающиеся циклы есть цикл длины $\geqslant 4$, т. е. $\sigma = (a\,b\,c\,d\,\ldots)\sigma_2 \ldots \sigma_k$.

Тогда

$$\sigma' = (a\,b\,c)\sigma(c\,b\,a) = (a\,b\,c)(a\,b\,c\,d\,\ldots)(c\,b\,a)\sigma_2 \ldots \sigma_k = \\ = (b\,c\,a\,d\,\ldots)\sigma_2 \ldots \sigma_k \in H,$$

откуда

$$\sigma'\sigma^{-1} = (b\,c\,a\,d\,\ldots)(a\,b\,c\,d\,\ldots)^{-1} = (b\,d\,a) \in H,$$

т.е. $H = \mathbf{A}_n$.

Таким образом, мы можем считать, что в подгруппе H все подстановки при разложении в произведение непересекающихся циклов имеют только циклы длин два и три.

Если подстановка $\sigma \in H$ состоит не только из циклов длины три, то в ее разложении есть по крайней мере две траспозиции (так как она четна):

$$\sigma = (a\,b)(c\,d)\sigma_3 \ldots \sigma_k.$$

В этом случае

$$\sigma' = (a\,b\,c)\sigma(c\,b\,a) = (a\,b\,c)(a\,b)(c\,d)(c\,b\,a)\sigma_3 \ldots \sigma_k = \\ = (a\,d)(c\,b)\sigma_3 \ldots \sigma_k \in H,$$

откуда в H содержится подстановка $\sigma'\sigma^{-1}$, равная $(a\,c)(b\,d)$.

Таким образом, подгруппа H содержит все пары непересекающихся транспозиций, которые порождают $\mathbf{A}_n$.

Остался только случай, когда σ есть произведение непересекающихся циклов длины три, где циклов в разложении больше одного:

$$\sigma = (a\,b\,c)(d\,e\,f)\sigma_3 \ldots \sigma_k \in H.$$

Тогда

$$\sigma' = (b\,c\,d)\sigma(d\,c\,b) = (b\,c\,d)(a\,b\,c)(d\,e\,f)(d\,c\,b)\sigma_3 \ldots \sigma_k = \\ = (a\,c\,d)(b\,e\,f)\sigma_3 \ldots \sigma_k \in H,$$

после чего

$$\sigma'\sigma^{-1} = (a\,c\,d)(b\,e\,f)(c\,b\,a)(f\,e\,d) = (a\,d\,b\,c\,e) \in H,$$

откуда по предудыщему $H = \mathbf{A}_n$. □

ПРИМЕНЕНИЕ ТЕОРЕМ СИЛОВА ДЛЯ ДОКАЗАТЕЛЬСТВА НЕПРОСТОТЫ КОНЕЧНОЙ ГРУППЫ

Лемма 1. *Не существует неабелевых простых групп G порядка $|G| = p^l m$, где p — простое число, p не делит m, p^l не делит $(m-1)!$.*

Доказательство. Допустим противное, пусть G — такая группа.

Тогда G содержит силовскую p-подгруппу S,

$$|S| = p^l, \quad (G : S) = m.$$

Так как конечные неабелевы p-группы не являются простыми (центр является нетривиальной нормальной подгруппой), то можно считать, что $m > 1$.

Ясно (действие на множестве смежных классов G по S), что существует гомоморфизм $\varphi\colon G \to \mathbf{S}_m$ такой, что $\ker\varphi \subseteq S$.

Так как G — простая группа, то $\ker\varphi = \{e\}$, т. е. φ — инъекция.

Поэтому $G \cong \varphi(G) \subseteq \mathbf{S}_m$.

По теореме Лагранжа $p^l m \mid m!$, следовательно, $p^l \mid (m-1)!$, что противоречит нашему предположению. □

Теорема 2. *Среди конечных групп G, порядок которых меньше чем 60, $|G| < 60$, нет неабелевых простых групп.*

Доказательство. В силу двух предшествующих лемм из чисел $2, 3, \ldots, 59$ надо рассмотреть лишь случаи $n = |G| = 30, 40, 56$.

а) Пусть есть простая группа G, $n = |G| = 30 = 2 \cdot 3 \cdot 5$. Пусть S — силовская 5-подгруппа простой группы G, $|S| = 5$. Число r_5 сопряженных силовских 5-подгрупп (как делитель 30 и $r_5 \equiv 1 \pmod 5$) равно 1 или 6. Но если $r_5 = 1$, то $S \lhd G$, что противоречит простоте группы G. Итак, $r_5 = 6$, при этом пересечение любых двух различных силовских 5-подгрупп из пяти элементов каждая равно $\{e\}$. Итак, их объединение содержит 24 неединичных элемента.

Аналогично число r_3 силовских 3-подгрупп равно 10 ($r_3 \neq 1$, r_3 — делитель 30, $r_3 \equiv 1 \pmod 3$), в их объединении 20 неединичных элементов.

Так как $24 + 20 = 44 > 30$, то получаем противоречие. Итак, группа G с $|G| = 30$ не может быть простой.

б) Пусть есть простая группа G, $n = |G| = 40 = 2^3 \cdot 5$. Пусть S — силовская 5-подгруппа группы G. Так как $r_5 = 1$ ($r \mid 40$, $r \equiv 1 \pmod 5$), то $P \lhd G$, и поэтому группа G не может быть простой.

в) Пусть есть простая группа G, $n = |G| = 56 = 2^3 \cdot 7$. Пусть S — силовская 7-подгруппа группы G. Так как $r_7 = 8$ ($r_7 \mid 56$, $r_7 \equiv 1 \pmod 7$) и пересечение любых двух различных подгрупп из семи элементов равно $\{e\}$, то их объединение содержит 48 неединичных элементов.

Силовская 2-подгруппа содержит восемь элементов, поэтому $48 + 8 = 56 = |G|$, но $r_8 > 1$ (если $r_8 = 1$, то эта силовская подгруппа из восьми элементов нормальна, что противоречит простоте нашей группы G), однако для неединичных элементов второй силовской 2-подгруппы в нашем балансе подсчета элементов уже нет места. Получили противоречие. $\square$

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 $[0, 2\alpha]$. 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 3. *Группа* $\mathbf{SO}_3$ *проста.*

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