

8. Восьмая лекция, 12 февраля 2019 г.

8.1. Действия групп на множествах. Напомним несколько определений из предыдущего семестра.

ОПРЕДЕЛЕНИЕ 8.1. Говорят, что группа G действует на множестве X (обозначение: $G \curvearrowright X$, раньше ещё часто писали $G : X$), если задано отображение $G \times X \rightarrow X$, $(g, x) \mapsto y = g \circ x$, удовлетворяющее следующим требованиям: $g \circ (g' \circ x) = (gg') \circ x$, и $e \circ x = x$ для любых $g, g' \in G$ и $x \in X$.

Множество $Gx = \{y \in X \mid y = g \circ x\} \subset X$ называется *орбитой* элемента x . Множество элементов группы G , оставляющих x на месте, называется *стабилизатором* элемента x и обозначается $\text{Stab}_G x$ или G_x :

$$\text{Stab}_G x = G_x = \{g \in G \mid g \circ x = x\} \subset G.$$

Очевидно, что это подгруппа в G .

Теорема Лагранжа утверждает, что если группа G конечна, то $|G| = |Gx| \cdot |\text{Stab}_G x|$ для любого элемента $x \in X$.

Если $X = Gx$, то есть все элементы X образуют одну орбиту, действие называется *транзитивным*.

Вот пример важного *нетранзитивного* действия.

ПРИМЕР 8.2. Группа действует на себе сопряжениями: $G \curvearrowright G$, $g \circ h = ghg^{-1}$. Это действие не транзитивно, т.к. $Ge = \{e\}$. Орбита элемента h для этого действия называется его *классом сопряжённости* и обозначается через $C(h)$, а стабилизатор — *централизатором* элемента h и обозначается через $Z(h)$. Ясно, что $Z(h) = \{g \in G \mid gh = hg\}$.

Одноточечные орбиты этого действия суть в точности элементы центра $Z(G)$ (это элементы группы, коммутирующие со всеми элементами).

Для конечных групп теорема Лагранжа утверждает, что $|Z(h)| \cdot |C(h)| = |G|$. В частности, $|C(h)|$ делит $|G|$. Это нам ещё неоднократно пригодится.

8.2. p -группы. Пусть G — конечная группа. Её порядок, как известно, делится на порядок любой подгруппы в G . Можно задать обратный вопрос: для всякого ли делителя $|G|$ найдётся подгруппа $H \in G$ соответствующего порядка? Несложно понять, что ответ будет отрицательным: так, например, группа A_5 имеет порядок 60, а подгруппы порядка 30 в ней нет: если бы такая подгруппа была, она была бы нормальной, а группа A_5 , как известно, проста.

Однако в некоторых случаях — в частности, для делителей числа $|G|$, имеющих вид p^k — подгруппа соответствующего порядка всегда существует. Чтобы доказать это, подробнее изучим группы порядка p^k .

ОПРЕДЕЛЕНИЕ 8.3. Группа G называется *p -группой*, где p — простое число, если $|G| = p^k$.

ТЕОРЕМА 8.4. *Нетривиальная p -группа имеет нетривиальный центр: если $|G| = p^k$, то $Z = Z(G) \neq \{e\}$.*

ДОКАЗАТЕЛЬСТВО. $G \setminus Z$ распадается на классы сопряжённости, содержащие более одного элемента (все одноэлементные классы лежат в центре). Порядок каждого из них $|C(x)|$ делит порядок группы, значит, $|C(x)| \vdots p$. Но $|G| \vdots p$. Поэтому и порядок центра кратен p . А значит, Z нетривиален. $\square$

СЛЕДСТВИЕ 8.5. *Всякая p -группа разрешима.*

ДОКАЗАТЕЛЬСТВО. Индукция по $\log_p |G|$. База очевидна: если $|G| = p$, то $G = \mathbb{Z}/p\mathbb{Z}$. Переход: центр $Z \subset G$ является нормальной абелевой подгруппой в G , в частности, он разрешим. Но G/Z — это p -группа, но уже меньшего порядка (предположение индукции!). Из разрешимости Z и G/Z следует разрешимость G . $\square$

СЛЕДСТВИЕ 8.6. *Всякая группа порядка p^2 абелева.*

ДОКАЗАТЕЛЬСТВО. Предположим, что $|G| = p^2$ и $Z \neq G$. Тогда $|Z| = p$ и $|G/Z| = p$, то есть G/Z — циклическая группа. Пусть aZ — её порождающий элемент. Тогда любой элемент из G представим в виде $a^k z$, где $z \in Z$. Но любые два таких элемента коммутируют — противоречие. $\square$

8.3. Силовские подгруппы. Теорема Лагранжа утверждает, что порядок подгруппы делит порядок группы. Можно поставить обратный вопрос: верно ли, что для всякого числа m , делящего порядок группы G , в G найдется подгруппа порядка m ?

УПРАЖНЕНИЕ 8.7. Докажите это утверждение в предположении, что группа G абелева.

Если же группа G неабелева, это неверно. В качестве простого примера можно привести группу A_5 . Она имеет порядок 60, но при этом в ней не будет подгруппы порядка 30. Действительно, если бы она была, то она была бы нормальной (как подгруппа индекса 2). Но, как мы покажем в следующей лекции, в A_5 нет нормальных подгрупп.

Оказывается, что в некоторых ситуациях «обратная теорема Лагранжа» всё-таки верна. Одна из таких ситуаций описывается теоремами Силова.

Пусть $|G| = p^n m$, причём $(p, m) = 1$.

ОПРЕДЕЛЕНИЕ 8.8. *Силовская p -подгруппа* группы G — это любая её подгруппа порядка p^n .

ТЕОРЕМА 8.9 (первая теорема Силова). *Силовская p -подгруппа существует.*

ДОКАЗАТЕЛЬСТВО. Если группа G абелева, теорема следует из теоремы о структуре конечных абелевых групп: её силовская подгруппа — это $\text{Tors}_p G$. В общем случае воспользуемся индукцией по $|G|$.

Пусть $|G| > 1$. Рассмотрим разбиение G на классы сопряжённых элементов: $G = \bigcup C(x_i)$.

Случай 1: найдётся такой нетривиальный класс $C(x)$, число элементов в котором не делится на p . Тогда $|Z(x)| \cdot p^n$, и в $Z(x)$ по предположению индукции есть подгруппа порядка p^n — она-то и будет силовской подгруппой в G .

Случай 2: такого класса нет. Тогда $|C(x_i)| \cdot p$, и поэтому $|Z| \cdot p$ (рассуждение аналогично доказательству теоремы о нетривиальности центра p -группы). Пускай $|Z| = p^{n_0} m_0$. Выберем в Z силовскую подгруппу Z_1 : порядок Z_1 равен p^{n_0} . В G/Z_1 по предположению индукции существует подгруппа порядка p^{n-n_0} . Её полный прообраз при каноническом эпиморфизме $G \rightarrow G/Z_1$ и будет искомой силовской p -подгруппой. $\square$

ТЕОРЕМА 8.10 (вторая теорема Силова). *Всякая p -подгруппа содержится в некоторой силовской p -подгруппе. Все силовские p -подгруппы сопряжены.*

ДОКАЗАТЕЛЬСТВО. Пусть $S \subset G$ — фиксированная силовская p -подгруппа, $H \subset G$ — произвольная p -подгруппа.

Рассмотрим действие $S_1 \curvearrowright G/S$ на левых смежных классах по S . Число элементов любой нетривиальной H -орбиты делится на p , а число элементов в G/S равно m и поэтому на p не делится. Значит, H имеет в G/S неподвижные точки. Пусть gS — такая точка. Тогда $hgS = gS$ для любого $h \in H$, то есть $H \subset gSg^{-1}$, откуда следует первое утверждение теоремы. Если H силовская подгруппа, то из сравнения порядков групп заключаем, что $H = gSg^{-1}$. $\square$

ТЕОРЕМА 8.11 (третья теорема Силова). *Число силовских подгрупп сравнимо с 1 по модулю p .*

ДОКАЗАТЕЛЬСТВО. Пусть S — силовская подгруппа, $C(S)$ — класс подгрупп, сопряжённых S . По предыдущей теореме это и есть множество всех силовских подгрупп. При действии G на $C(S)$ сопряжениями стабилизатор каждой подгруппы $S' \in C(S)$ служит её нормализатор $N(S')$. Ограничим это действие на S . Тогда $C(S)$ как-то разобьётся на нетривиальные S -орбиты, число элементов в каждой из которых кратно p , и неподвижные

точки. Покажем, что неподвижная точка будет ровно одна — сама подгруппа S . Отсюда и будет следовать утверждение теоремы.

Пусть $S' \in C(S)$ — неподвижная точка. Это значит, что $S \subset N(S')$. Тогда S и S' — силовские подгруппы в $N(S')$, а значит, что они в ней сопряжены. Но S' — нормальная подгруппа в $N(S')$. Поэтому $S = S'$. $\square$

8.4. Применение теорем Силова.

ПРИМЕР 8.12. Пусть $|G| = n$, и p — наименьший простой делитель числа n . Покажем, что всякая подгруппа H индекса p нормальна. Действительно, рассмотрим действие H на левых смежных классах G/H . Число элементов каждой орбиты делит $|H|$, то есть оно либо равно 1, либо не меньше p . Но, поскольку $|G/H| = p$ и действие имеет неподвижную точку eH , то оно тривиально.

ПРИМЕР 8.13. Покажем, что всякая группа G порядка pq , где p и q — различные простые числа, является полупрямым произведением циклических групп порядка p и q . Пусть $p > q$. Тогда силовская p -подгруппа G_p нормальна в силу предыдущего примера. Если G_q — силовская q -подгруппа, то $G_p \cap G_q = \{e\}$, а поэтому $|G_p G_q| = pq = |G|$. Значит, $G = G_p \ltimes G_q$.

ПРИМЕР 8.14. Докажем, что каждая группа порядка 45 абелева. Действительно, пусть n_3 и n_5 — число её силовских 3-подгрупп и 5-подгрупп соответственно. Тогда $n_3 \equiv 1 \pmod 3$ и $n_3 | 5$, откуда $n_3 = 1$. Значит, имеется единственная силовская 3-подгруппа, которая тем самым нормальна. Аналогично из условий $n_5 \equiv 1 \pmod 5$ и $n_5 | 9$ получаем, что силовская 5-подгруппа нормальна и поэтому единственна. Поэтому вся группа будет прямым произведением этих двух подгрупп, следовательно, будет абелевой.

ПРИМЕР 8.15. Докажем, что не существует простых групп порядка 30. Для этого покажем, что в каждой группе G порядка 30 есть нормальная подгруппа. Рассмотрим силовские 5-подгруппы в G . Они все суть циклические подгруппы порядка 5. Ясно, что пересекаться они могут только по единице. Их число, по третьей теореме Силова, даёт остаток 1 от деления на 5. Предположим, что оно больше 1. Тогда оно может равняться только шести, что даст нам 24 элемента порядка 5 в G . Теперь посмотрим на силовские 3-подгруппы. В каждой из них два элемента порядка 3. Если силовская подгруппа не одна, то их не менее 4, что даёт ещё 8 элементов порядка 2. Но в группе всего 30 элементов, что меньше, чем $24 + 8$. Противоречие. Значит, в G есть нормальная подгруппа.

E-mail address: esmirnov@hse.ru