Теория групп. Лекция 12

Штепин Вадим Владимирович

21 ноября 2019 г.

1 Теоремы Силова

Пусть G — конечная группа, $|G| = p^n m$, где p — простое и m не делится на p.

Замечание

В общем случае нельзя говорить о том, что для любого делителя размера группы есть подгруппа такого размера.

Пример

В A_4 нет подгруппы порядка 6

Опр. В группе G порядка $p^n m$, p — простое и m не делится на p подгруппа H порядка p^n — **силовская p-подгруппа**

Лемма

Пусть $q = p^n$ и Ω_q — множество всех q-элементных подмножеств в G. Тогда $|\Omega_q| = C_{p^n m}^{p^n} \equiv m \ (mod\ p)$. В частности, $|\Omega_q|$ не делится на p

Доказательство

В $(1+x)^{p^n m}$ коэффициентом при x^{p^n} является $C_{p^n m}^{p^n}$ — искомое число подмножеств. Будем раскрывать этот бином над Z_p. Было доказано, что $(a+b)^p \equiv a^p + b^p \ (mod\ p)$

$(1+x)^{p^n m} = ((1+x)^p)^{p^{n-1}m} = (1+x^p)^{p^{n-1}m} = ... = (1+x^{p^n})^m = 1 + mx^{p^n} + ...$ Коэффициент при x^{p^n} — это m. Значит, $|\Omega_q| \equiv m \ (mod\ p)$.

Теорема (первая теорема Силова)

Пусть G — конечная группа, p — простое, m не делится на p и $q = p^n$. Тогда G имеет силовскую p-подгруппу.

Доказательство

Рассмотрим действие $I : G \to S(\Omega_q)$ $I(a) : S \to aS$. По формуле орбит: $\Omega_q = G(S_1) \cup G(S_2) \cup ... \cup G(S_l)$ — объединение попарно непересекающихся орбит.

$|\Omega_q| = \sum\limits_{i=1}^{l_1} |G(S_i)|$. Если $\forall i$ $|G(S_i)|$ делится на p, то $|\Omega_q|$ тоже делится на p, а это невозможно по лемме. Значит, $\exists S : |G(S)|$ не делится на p. Пусть $St(S)$ — стабилизатор подмножества S.

По теореме о мощности орбиты, $|G(S)| = \frac{|G|}{|St(S)|} = \frac{p^n m}{|St(S)|} = k$, причем k не делится на p.

$|St(S)| = \frac{p^n m}{k} \in N$, а значит m делится на k, так как k не делится на p.

С другой стороны, $\forall g \in St(S)$ верно $gS \subset S \Rightarrow St(S)S \subset S \Rightarrow \forall s \in S$ $St(S)s \subset S$. Так как левые сдвиги — инъективное отображение, то $|St(S)| = |St(S)s| \leq |S| = p^n$. Но, так как m делится на k, то $|St(S)| \geq p^n$, а значит $|St(S)| = p^n$ и это силовская p-подгруппа.

Замечание

1. $|G(s) = \frac{p^n m}{|St(S)|} = m$ — орбита, содержащая элемент, стабилизатор которого — силовская p-подгруппа.

2. $St(S)s = S$

Теорема (третья теорема Силова)

$|G| = p^n m$, m не делится на p. Пусть N_p — число силовских p-подгрупп в G. Тогда $N_p \equiv 1$ $(mod\ p)$.

Доказательство

Ω_q — множество q-элементных подмножеств в G, $q = p^n$, $I : G \to S(\Omega_q)$, $I_a(S) = aS$. Разобьем орбиты на два типа: мощность которых делится на p (первый тип) и мощность которых не делится(второй тип).

Будет доказано, что каждая орбита второго типа содержит (как элемент) единственную силовскую p-подгруппу, а каждая орбита первого типа нет.

$St(S)s = S$, где S — множество из орбиты второго типа.

$s^{-1}St(S)s = s^{-1}S \in G(S)$. Поскольку сопряжение не меняет мощности, то $s^{-1}St(S)s$ — силовская подгруппа.

Покажем, что в орбите второго типа нет двух различных силовских p-подгрупп. Пусть не так, значит $P_1, P_2 \in G(S)$ — силовские p-подгруппы. Значит, $\exists a \in G$ $P_1 = aP_2$. Так как P_1, P_2 — подгруппы, то $e \in aP_2 (= P_1)$ и $e \in P_2$. Значит, $aP_2 \cup P_2 \neq \emptyset$. По свойствам левых смежных классов, $P_2 = aP_2 = P_1$.

По замечанию, $|G(S)| = m$ — мощность орбит второго типа.

Осталось доказать, что орбиты первого типа силовских p-подгрупп не содержат.

Пусть P — силовская p-подгруппа, $G(P)$ — орбита первого типа, содержащая P, то есть $|G(P)| \vdots p$, а $St(P)$ — стабилизатор P.

$|G(P)| = \frac{|G|}{|St(P)|} = \frac{p^n m}{p^n} = m$ — противоречие.

По определению стабилизатора, $\forall p \in P$ $St(P)p \subset P \Rightarrow |St(P)| \leq |P|$, но, очевидно, что P стабилизирует саму себя, а значит $P \subset St(P) \Rightarrow P = St(P)$.

$|\Omega_q| = \sum |G(S)|$ — сумма мощностей орбит первого типа и орбит второго типа, и $|\Omega_q| \equiv m$ $(mod\ p)$. Так как мощности орбит первого типа делятся на p, то $m|N_p| \equiv m$ $(mod\ p)$ и $|N_p| \equiv 1$ $(mod\ p)$, так как силовских подгрупп столько же, сколько орбит второго типа.