КОГДА ЛЮБАЯ ГРУППА ИЗ N ЭЛЕМЕНТОВ ЦИКЛИЧЕСКАЯ? [1]

В. Брагин, Ант. Клячко и А. Скопенков

В этой заметке приводится простое доказательство известного факта: любая группа из n элементов является циклической тогда и только тогда, когда n взаимно просто с $\phi(n)$. Заметка доступна школьникам: для понимания не требуется знаний по теории групп. Она может быть также интересным 'легким чтением' для профессиональных математиков.

Введение

Назовем *группой* непустое семейство G преобразований (т.е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного преобразования (т.е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$). Общепринятое название: группа преобразований. Ср. [А, стр. 49, комментарий к задаче 5].

Если в конечной группе G найдется преобразование g, из всех возможных степеней которого состоит G (т.е. $G = \{g, g^2, \dots, g^n, \dots\}$), то группа G называется *циклической*.

Мы докажем следующую теорему.

Теорема (фольклор). *Любая группа из n элементов является циклической тогда и только тогда, когда n взаимно просто с $\phi(n)$.*

Здесь $\phi(n)$ — количество целых чисел от 1 до n, взаимно простых с n (функция Эйлера).

Заметим, что условие взаимной простоты n и $\phi(n)$ равносильно тому, что в разложении числа n на простые сомножители $n = p_1 \dots p_t$

(*) все p_i различны и

(**) p_i не делит $p_j - 1$ ни для каких i и j.

Для понимания доказательства не требуется никаких знаний по теории групп. Небольшое количество необходимых понятий вводятся в процессе доказательства. В частности, наше доказательство не привлекает (явно или неявно) понятия факторгруппы, в отличие от более традиционных доказательств (см., например, [В]). Идея приводимого доказательства близка к [???]. Как придумать приводимое доказательство, видно из [BKKSS].

Доказательство части «только тогда»

Если нарушается вышеприведенное условие (*), например, $p_1 = p_2 = p$, то в качестве нециклической группы из n элементов можно взять группу

$$\left\{(1, 2, \dots, p)^i (p+1, p+2, \dots, 2p)^j (2p+1, 2p+2, \dots, 2p+\tfrac{n}{p^2})^k \mid i, j = 1, \dots, p,\ k = 1, \dots, \tfrac{n}{p^2}\right\}.$$

Если нарушается вышеприведенное условие (**), например, p_1 делит $p_2 - 1$, то по теореме о первообразном корне существует элемент $a \in \mathbb{Z}_{p_2}$, для которого степени $a, a^2, \dots, a^{p_1} = 1$ различны. Обозначим через G_{p_1,p_2} группу преобразований $f_{k,l} : \mathbb{Z}_{p_2}^2 \to \mathbb{Z}_{p_2}^2$, заданных формулой $f_{k,l}(x, y) := (a^k x, lx + y)$ для $k \in \mathbb{Z}_{p_1}$ и $l \in \mathbb{Z}_{p_2}$. [2] Тогда в качестве нециклической (даже некоммутативной) группы из n элементов можно взять группу

$$\left\{f \circ (1, 2, \dots, \frac{n}{p_1 p_2})^j \mid f \in G_{p_1,p_2},\ j = 1, 2, \dots, \frac{n}{p_1 p_2}\right\}. \quad QED$$

Доказательство части «тогда».

Через $|X|$ обозначается число элементов в множестве X. Обозначим данную группу через G. Используем индукцию по числу простых сомножителей в $n = |G|$. Если сомножитель один, то часть «тогда» вытекает из следующей теоремы Лагранжа.

Порядком $\operatorname{ord} a$ элемента a группы с единичным элементом e называется наименьшее целое положительное n, для которого $a^n = e$. Если группа конечна, то ясно, что такое n существует.

---

[1] Обновляемая версия поддерживается на www.arxiv.org. Благодарим К. Кохася за полезные замечания.

[2] Научно говоря, $G_{p_1,p_2} = \left\{ \begin{pmatrix} a^k & l \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}_{p_2}^{2\times 2} \;\middle|\; k \in \mathbb{Z}_{p_1},\ l \in \mathbb{Z}_{p_2} \right\}$.

Теорема Лагранжа (частный случай). *Число элементов конечной группы делится на порядок любого ее элемента.*

Доказательство. Обозначим данную группу через G. Для любого $x \in G$ рассмотрим множество $\{x, xf, xf^2, \dots, xf^{\operatorname{ord} f-1}\}$. По определению порядка указанные элементы различны. Значит, в этом множестве $\operatorname{ord} f$ элементов. Если $xf^k = yf^l$, то $y = xf^{k-l}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на $\operatorname{ord} f$. QED

Пусть теперь простых сомножителей в $n = |G|$ больше одного. Нам понадобится следующая общая версия теоремы Лагранжа.

Подгруппой группы называется подмножество этой группы, которое само по себе является группой.

Теорема Лагранжа. *Число элементов конечной группы делится на число элементов любой ее подгруппы.*

Доказательство. Обозначим данную группу через G, а ее подгруппу через $\{h_1, \dots, h_m\}$. Для любого $x \in G$ рассмотрим множество $\{xh_1, xh_2, \dots, xh_m\}$. В этом множестве $|H|$ элементов. Если $xh_k = yh_l$, то $y = xh_kh_l^{-1}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на m. QED

Максимальной подгруппой назовем максимальную по включению подгруппу, не совпадающую со всей группой и содержащую более одного элемента. По предположению индукции и теореме Лагранжа *каждая максимальная подгруппа является циклической.*

Для элемента f группы G обозначим через $\langle f\rangle \subset G$ множество всех его степеней (в т.ч. нулевых и отрицательных). Элемент f называется **порождающим** для (циклической) подгруппы $\langle f\rangle$.

Предположим противное, т.е. что группа G не является циклической. Тогда *каждый элемент f содержится в некоторой максимальной подгруппе* (в максимальной по включению подгруппе, содержащей $\langle f\rangle$).

Элементы f и g группы G называются **сопряженными** в G, если $g = b^{-1}fb$ для некоторого $b \in G$.

Первый случай: *порождающий элемент f некоторой максимальной подгруппы сопряжен только с некоторыми своими степенями.* Возьмем $h \in G - \langle f\rangle$. Тогда $h^{\operatorname{ord} h} \in \langle f\rangle$. Обозначим через q наименьшее из целых положительных n, для которых $h^n \in \langle f\rangle$. Возьмем $k \in \mathbb{Z}$, для которого $h^{-1}fh = f^k$. Так как $h^q \in \langle f\rangle$, то $f = h^{-q}fh^q = f^{k^q}$ (последнее равенство доказывается индукцией по q). Поэтому $k^q \equiv 1 \mod \operatorname{ord} f$.

По условию (*) и теореме Лагранжа $\operatorname{ord} f$ является произведением $p_1 \dots p_s$ различных простых. Тогда $k^q \equiv 1 \mod p_i$ для любого $i = 1, 2, \dots, s$. Так как $|G|$ делится на $\operatorname{ord} h$ и $\operatorname{ord} h$ делится на q, то по условию (*) q является произведением различных простых. По условию (**) ни одно из этих простых p_j не делит никакое $p_i - 1$. Следовательно, q взаимно просто с каждым $p_i - 1$. Поэтому существуют целые $x = x_i$ и $y = y_i$, для которых $qx + (p_i - 1)y = 1$. Значит, $k \equiv k^{qx+(p_i-1)y} \equiv 1 \mod p_i$ для любого $i = 1, 2, \dots, s$. Поэтому $k \equiv 1 \mod \operatorname{ord} f$, т.е. $fh = hf$.

Тогда в G есть подгруппа $\{f^ih^j \mid 1 \le i \le \operatorname{ord} f,\ 1 \le j \le q\}$ из $q \operatorname{ord} f$ элементов. Значит, по условию (*) и теореме Лагранжа $\operatorname{ord} f$ и q взаимно просты. Так как $(fh)^j = f^jh^j$ для любого j, то $\operatorname{ord}(fh)$ делится на q и на $\operatorname{ord} f$. Поэтому $\operatorname{ord}(fh) = q \operatorname{ord} f$. Так как подгруппа $\langle f\rangle$ максимальна, то $\langle fh\rangle = G$. Значит, G циклическая. Противоречие.

Второй случай: *порождающий элемент любой максимальной подгруппы сопряжен не только со своими степенями.*

Произведением двух подмножеств X и Y группы G называют множество всевозможных произведений xy, где $x \in X$ и $y \in Y$. Если одно из этих подмножеств состоит только из одного элемента, например, $Y = \{y\}$, то для краткости пишут Xy вместо $X\{y\}$.

(1) Любая максимальная подгруппа F содержит **центр**

$$Z = Z(G) := \{a \in G \ : \ ga = ag \text{ для любого } g \in G\},$$

т.е. множество тех элементов, которые коммутируют со всеми.

Доказательство утверждения (1). Иначе FZ — большая коммутативная подгруппа. Ввиду максимальности F имеем $FZ = G$. Противоречие с условием второго случая. QED

(2) Пересечение двух максимальных подгрупп равно центру.

Доказательство утверждения (2). Неединичный элемент в пересечении коммутирует с элементами обоих подгрупп. Значит, он коммутирует с любым произведением нескольких сомножителей, каждый из которых лежит в одной из наших подгрупп. Множество таких произведений является подгруппой. В силу максимальности наших подгрупп эта подгруппа совпадает со всей группой. Значит, пересечение содержится в центре.

Из (1) вытекает обратное включение. QED

(3) Для любой максимальной подгруппы F число различных подгрупп, сопряженных с F (включая F), равно $|G|/|F|$.

Доказательство утверждения (3). Рассмотрим множество

$$N(F) := \{a \in G \ : \ Fa = aF\}.$$

Нетрудно проверить, что $N(F)$ является подгруппой. По условию второго случая $N(F) \neq G$. Так как $N(F) \supset F$, то в силу максимальности $N(F) = F$.

Сопряжение каждым элементом группы G переводит подгруппу F в одну из сопряженных подгрупп. Если сопряжение двумя разными элементами u, v группы G переводит подгруппу F в одну и ту же подгруппу, т.е. $u^{-1}Fu = v^{-1}Fv$, то $Fuv^{-1} = uv^{-1}F$. Это означает, что $uv^{-1} \in N(F) = F$ или, что то же самое, $u \in Fv$. Обратно, условие $u \in Fv$ влечет $u^{-1}Fu = v^{-1}Fv$.

Ясно, что $|Fv| = |F|$. Поэтому число элементов в G, сопряжение с которыми переводит подгруппу F в данную фиксированную сопряженную подгруппу, равно $|F|$. Значит, число подгрупп, сопряженных к F, ровно в $|F|$ раз меньше, чем $|G|$. QED

(4) Обозначим через $\widehat{F}$ число элементов, сопряженных элементам максимальной подгруппы F и не лежащих в центре. Тогда $|G|/2 \leq \widehat{F} < |G| - |Z|$.

Доказательство утверждения (4). Подгруппа, сопряженная к максимальной, также максимальна. (Действительно, если $g^{-1}Fg \subset F' \subset G$, то $F \subset gF'g^{-1} \subset G$.)

Поэтому и ввиду (3) $\widehat{F} = (|F| - |Z|)\dfrac{|G|}{|F|} = |G|\left(1 - \dfrac{|Z|}{|F|}\right)$.

Так как $|G| > |F|$, то $\widehat{F} < |G| - |Z|$.

По условию второго случая $Z \neq F$. По (1) и теореме Лагранжа $|Z|$ делит $|F|$. Поэтому $\widehat{F} \geq |G|/2$.

Завершение разбора второго случая: подсчет. Пусть $F_1, \ldots, F_s$ — наибольший набор попарно несопряженных максимальных подгрупп. Напомним, что любой элемент группы содержится в некоторой максимальной подгруппе. Значит, он сопряжен некоторому элементу в некоторой подгруппе F_i. Тогда ввиду (2) $|G| = |Z| + \sum_i \widehat{F}_i$. Ввиду левого неравенства в (4) число слагаемых не превосходит единицы. Ввиду правого неравенства в (4) одного слагаемого тоже быть не может. QED

Литература

[A] В.И. Арнольд, Обыкновенные дифференциальные уравнения, М, Наука, 1984.

[B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/ kbrown/4340/cyclic_only_orders.pdf

[BKKSS] Д. Баранов, А. Клячко, К. Кохась, А. Скопенков и М. Скопенков, Когда любая группа из n элементов циклическая? Материалы ЛКТГ 2011, www.turgor.ru