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 старшеклассникам: 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*.

В этой заметке приводится простое доказательство следующего известного факта.

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 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]). Приводимое доказательство не претендует на новизну. Как его придумать, 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] 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 $\{x, xf, xf^2, \ldots, xf^{\operatorname{ord} f-1}\}$. 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 $\{h_1, \ldots, h_m\}$. Для любого $x \in G$ рассмотрим множество $\{xh_1, xh_2, \ldots, xh_m\}$. 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 $p_1 \ldots p_s$ различных простых. Тогда $k^q \equiv 1 \mod p_i$ для любого $i = 1, 2, \ldots, s$. 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 $i = 1, 2, \ldots, s$. 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? http://olympiads.mccme.ru/lktg/2011/6/index.htm

WHEN ANY GROUP OF N ELEMENTS IS CYCLIC? [1]

V. Bragin, Ant. Klyachko and A. Skopenkov

We give a simple proof of the well-known fact: any group of n elements is cyclic if and only if n and $\varphi(n)$ are coprime. This note is accessible for students because no knowledge of group theory is required. The note could also be an interesting easy reading for mature mathematicians.

Introduction

We call a *group* a nonempty family G of transformations (i.e. permutations or rearrangements) of some set, which family is closed with respect to composition and taking inverse transformation (i.e. if $f, g \in G$, then $f \circ g \in G$ and $f^{-1} \in G$). Common term: transformation group. Cf. [A, comment to problem 5].

If a finite group G contains an element g such that G consists of all powers of g (i.e. $G = \{g, g^2, \dots, g^n, \dots\}$, then group G is called *cyclic*.

We give a simple proof of the following well-known fact.

Theorem. *Any group consisting of n elements is cyclic if and only if n and $\varphi(n)$ are coprime.*

Here $\varphi(n)$ is the number of positive integers not exceeding n and coprime to n (the Euler function).

Note that n and $\varphi(n)$ are coprime if and only if in the prime decomposition $n = p_1 \dots p_k$

(*) all p_i are different and

(**) p_i does not divide $p_j - 1$ for any i and j.

The understanding of the proof requires no knowledge of group theory. A few necessary notions are introduced in the course of the proof. In particular, our arguments does not use the notion of a quotient group, as opposed to more traditional proofs (see, e.g., [B]). Our proof is possibly known. One can understand how to invent it from [BKKSS].

Proof of the "only if" part.

If condition (*) above is violated, e.g., $p_1 = p_2 = p$, then the following group consists of n elements and is not cyclic:

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

If condition (**) above is violated, e.g., p_1 divides $p_2 - 1$, then by the primitive root theorem there is $a \in \mathbb{Z}_{p_2}^*$ for which the powers $a, a^2, \dots, a^{p_1} = 1$ are different. Denote by G_{p_1,p_2} the group of transformations $f_{k,l} : \mathbb{Z}_{p_2}^2 \to \mathbb{Z}_{p_2}^2$ defined by the formula $f_{k,l}(x, y) := (a^k x, lx + y)$ for $k \in \mathbb{Z}_{p_1}$ and $l \in \mathbb{Z}_{p_2}$. [2] Then the following group is not cyclic (it is even nonabelian):

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

Proof of the "if" part.

We use the induction on the number of prime factors of $|G|$. If this order is prime, then the "if" part is implied by the following Lagrange Theorem.

The **order** $\operatorname{ord} a$ of an element a of a group with the identity element e is the minimal positive integer n such that $a^n = e$. If the group is finite, it is clear that such n exists.

Lagrange Theorem (particular case). *The number of elements of any finite group is divisible by the order of any its element.*

[1] We would like to acknowledge K. Kohas for useful discussions.

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

Proof. Denote the group by G. For each $x \in G$ consider the set $\{x, xf, xf^2, \dots, xf^{\operatorname{ord} f-1}\}$. By the definition of order these elements are different. Therefore this set contains $\operatorname{ord} f$ elements. If $xf^k = yf^l$, then $y = xf^{k-l}$. Therefore for different x these sets either coincide or are disjoint. Thus $|G|$ is divisible by $\operatorname{ord} f$. QED

Now suppose that the number of factors is greater than one. We need the following general version of the Lagrange Theorem.

A **subgroup** of a group G is a subset of G that is itself a group.

Lagrange Theorem. *The number of elements of any finite group is divisible by the number of elements of any subgroup.*

Proof. Denote the group by G and the subgroup by $\{h_1, h_2, \dots, h_m\}$. For each $x \in G$ consider the set $\{xh_1, xh_2, \dots, xh_m\}$. This set contains m elements. If $xh_k = yh_l$, then $y = xh_kh_l^{-1}$. Therefore for different x these sets either coincide or are disjoint. Thus $|G|$ is divisible by m. QED

A **maximal subgroup** of a group is a maximal by inclusion subgroup not coinciding with G and containing more than one element. By the induction hypothesis and the Lagrange Theorem, *each maximal subgroup is cyclic.*

For an element f of a group G let $\langle f \rangle$ be the set of all powers of f (including zero and negative ones). The element f is called **generating** for the (cyclic) subgroup $\langle f \rangle$.

Suppose to the contrary that the group G is noncyclic. Then each element is contained in a maximal subgroup.

Elements f, g of a group G are **conjugate** in G if $g = b^{-1}fb$ for some $b \in G$.

First case: *generator f of some maximal subgroup is conjugate only to (some of) its powers.* Take $h \in G \setminus \langle f \rangle$. Then $h^{\operatorname{ord} h} \in \langle f \rangle$. Let q be the minimal positive integer such that $h^n \in \langle f \rangle$. Take $k \in \mathbb{Z}$ such that $h^{-1}fh = f^k$. The inclusion $h^q \in \langle f \rangle$ implies $f = h^{-q}fh^q = f^{k^q}$ (here the last equality is proved by induction on q). Therefore $k^q \equiv 1 \mod \operatorname{ord} f$.

By condition (*) and the Lagrange Theorem $\operatorname{ord} f$ is a product $p_1 \dots p_s$ of different primes. Then $k^q \equiv 1 \mod p_i$ for any $i = 1, 2, \dots, s$. Since $|G|$ is divisible by $\operatorname{ord} h$ and $\operatorname{ord} h$ is divisible by q, by condition (*) we obtain that q is a product of different primes. By condition (**) none of these primes p_j divides none $p_i - 1$. Therefore q is coprime to each $p_i - 1$. Hence there exist integers $x = x_i$ and $y = y_i$ such that $qx + (p_i - 1)y = 1$. Therefore $k \equiv k^{qx+(p_i-1)y} \equiv 1 \mod p_i$ for any $i = 1, 2, \dots, s$. Hence $k \equiv 1 \mod \operatorname{ord} f$, i.e., $fh = hf$.

Then G contains a subgroup $\{f^ih^j \mid 1 \le i \le \operatorname{ord} f,\ 1 \le j \le q\}$ of $q \operatorname{ord} f$ elements. Hence by condition (*) and the Lagrange Theorem $\operatorname{ord} f$ is coprime to q. Since $(fh)^j = f^jh^j$ for each j, we obtain that $\operatorname{ord}(fh)$ is divisible both by q and by $\operatorname{ord} f$. $\operatorname{ord}(fh) = q \operatorname{ord} f$. Thus $\operatorname{ord}(fh) = q \operatorname{ord} f$. Since the subgroup $\langle f \rangle$ is maximal, we have $\langle fh \rangle = G$ and G is cyclic. Contradiction.

Second case: *generator of any maximal subgroup is conjugate not only to its powers.*

The **product of subsets X and Y** of a group G is the set of all products xy, where $x \in X$ and $y \in Y$. If one of these subsets consists of only one element, e.g., $Y = \{y\}$, then we write Xy instead of $X\{y\}$.

(1) Any maximal subgroup F contains the **center**

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

i.e., the set of elements commuting with each element of the group.

Proof of assertion (1). Otherwise FZ is a larger commutative subgroup. By the maximality of F we have $FZ = G$, which contradicts to the assumption of the second case. QED

(2) The intersection of two maximal subgroups equals the center.

Proof of assertion (2). A nontrivial element of the intersection commutes with all elements of both subgroups. Hence it commutes with any product of several multiples, each multiple being an element of one of our subgroups. The set of such products is a subgroup. By the maximality of our

subgroups this subgroup coincides with the entire group. Therefore the intersection is contained in the center.

Assertion (1) implies the converse inclusion. QED

(3) The number of different subgroups conjugate to a maximal subgroup F (including F) is $|G|/|F|$.

Proof of assertion (3). Consider the set

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

It is easy to verify that $N(F)$ is a subgroup. By the assumption of the second case $N(F) \neq G$. Since $N(F) \supset F$, the maximality implies that $N(F) = F$.

The conjugation by each element of G takes F to a conjugate subgroup. If the conjugation by two different elements u and v takes the F to the same subgroup, i.e., $u^{-1}Fu = v^{-1}Fv$, then $Fuv^{-1} = uv^{-1}F$. This means that $uv^{-1} \in N(F) = F$ or, equivalently, $u \in Fv$. Conversely, the condition $u \in Fv$ implies $u^{-1}Fu = v^{-1}Fv$.

Clearly, $|Fv| = |F|$. Therefore the number of elements of G conjugation by which takes F to a given subgroup equals $|F|$. Therefore the number of different subgroups conjugate to F is precisely $|F|$ times less than $|G|$. QED

(4) Denote by $\widehat{F}$ the number of elements of G conjugate to elements of a maximal subgroup F and not contained in the center. Then $|G|/2 \leq \widehat{F} < |G| - |Z|$.

Proof of assertion (4). A subgroup conjugate to a maximal subgroup is also maximal. (Indeed, if $g^{-1}Fg \subset F' \subset G$, then $F \subset gF'g^{-1} \subset G$.)

Therefore by (3) $\widehat{F} = (|F| - |Z|)\dfrac{|G|}{|F|} = |G|\left(1 - \dfrac{|Z|}{|F|}\right)$.

The inequality $|G| > |F|$ implies $\widehat{F} < |G| - |Z|$.

By the assumption of the second case, $Z \neq F$. By (1) and the Lagrange theorem, $|Z|$ divides $|F|$. Therefore $\widehat{F} \geq |G|/2$.

Conclusion of the proof of the second case: calculations. Let $F_1, \ldots, F_n$ be a maximal family of pairwise non-conjugate maximal subgroups. Recall that each element of the group is contained in some maximal subgroup. Hence the element is conjugate to some element in certain F_i. By this and (2) $|G| = |Z| + \sum_i \widehat{F}_i$. By the left inequality in (4), the number of summands is at most one. By the right inequality in (4), one summand also gives a contradiction. QED

References

[A] V. I. Arnold, Ordinary Differential Equations, The MIT Press (1978), ISBN 0-262-51018-9.

[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] D. Baranov, A. Klyachko, K. Kohas, A. Skopenkov and M. Skopenkov, When are all groups of order n cyclic? http://olympiads.mccme.ru/lktg/2011/6/index.htm