# 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 paper is accessible for high-school students because no knowledge of group theory is required. It 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 prove the following theorem.

**Theorem (folklore).** *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 uses ideas similar to [???]. One can understand how to invent this proof 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.*

*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

[1] See update version on www.arxiv.org. We would like to acknowledge K. Kohas for useful discussions.

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

$xf^k = yf^l$, 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 $y = xh_k h_l^{-1}$. 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 $\{f^i h^j \mid 1 \le i \le \operatorname{ord} f,\ 1 \le j \le q\}$ of $q \operatorname{ord} f$ elements. Hence by condition (*) and the Lagrange Theorem $\operatorname{ord} f$ is coprime to $q$. Since $(fh)^j = f^j h^j$ 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, Springer, Berlin, 19??.

[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 $n$ are cyclic? Materials of LKTG 2011, www.turgor.ru