# Cyclic Groups

Rohan Mukherjee

February 20, 2024

In this paper we prove the following theorem:

**Theorem 1.** *Let $G$ be a group and $n = |G|$. If $G$ is cyclic, $G$ has precisely one group of order $d$ for each $d \mid n$, and similarly, if $G$ has $\leq 1$ subgroup for each order $d \mid n$, then $G$ is cyclic.*

The tools used to prove this theorem are actually quite complicated. Many students have seen near the beginning of an introductory group theory course that if $G$ is cyclic, then every subgroup is cyclic. Something similar is true for field extensions: If $k(\alpha)/k$ is a simple field extension, then every subextension $k(\alpha)/E/k$ is simple. This proof is relatively complicated, and depends on an important lemma. It can also be proven (see here for example) using tools of algebraic geometry. The forward direction of the proof of the above theorem is one that students still near the beginning of their group theory adventure could tackle. The reverse direction is significantly more complicated, however. We demonstrate that here.

*Proof.* Let $G = \langle a \rangle$ with $|a| = n$, and $d \mid n$. The subgroup $H = \left\langle a^{n/d} \right\rangle$ is cyclic of order $d$, showing uniqueness. Let $H'$ be another subgroup of order $d$. Consider $a^i \in H'$ with $0 < i < n$ (the case $i = 0$ is clear), and let $m = n/\gcd(i, n)$. Clearly, $a^{i \cdot m} = e$, so $|a^i| \mid m$. Suppose by contradiction that $|a^i| = m/k$ for some $1 < k \mid m$. Then $a^{i \cdot m/k} = e$, so $n \mid i \cdot m/k = \frac{n \cdot i}{k \gcd(n,i)}$. This says that $n \cdot k \cdot \gcd(n, i) \mid n \cdot i$, equivalently $k \cdot \gcd(n, i) \mid i$. Clearly, $k \mid i$, and $k \mid n/\gcd(n, i)$ by definition, so $k \cdot \gcd(n, i) \mid n, i$. But $\gcd(n, i) \cdot k > \gcd(n, i)$, a contradiction. Thus $|a^i| = n/\gcd(n, i)$. Then $n/\gcd(n, i) \mid d$. Equivalently, $nk = d \gcd(n, i)$. But this says that $n/d \mid \gcd(n, i) \mid i$, so $n/d \mid i$, which shows that $a^i \in H$, completing the proof (we only have to show subset in one direction since $|H| = |H'|$).

Now we come to the fun part. Since $G$ has $\leq 1$ subgroup of each order, each of it's Sylow $p$ subgroups are normal, which shows that $G$ is isomorphic to the direct product of its

Sylow subgroups. Since each Sylow subgroup has coprime order, we need only show that if $G$ is a $p$-group with $\leq 1$ subgroup, then $G$ is cyclic, which will complete the proof by the Chinese Remainder Theorem. We start by showing that $G$ is abelian by induction. Clearly groups of order 1 with the above property are abelian. Since $G$ is a $p$-group, $p \mid |Z(G)|$ (one can see this by a simple application of the class equation). Let $H/Z(G), H'/Z(G) \leq G/Z(G)$ with $Z(G) \leq H, H'$ be two subgroups of the same order. Since $|H| = |H/Z(G)| \cdot |Z(G)|$, we see that $|H| = |H'|$, which shows that $H = H'$ which shows that $H/Z(G) = H'/Z(G)$, so $G/Z(G)$ has the above property. By induction $G/Z(G)$ is cyclic so $G$ is abelian. With $|G| = p^n$, write

$$G \cong \mathbb{Z}/p^{n_1} \times \mathbb{Z}/p^{n_2} \times \cdots \times \mathbb{Z}/p^{n_k}$$

with $n_k \leq n_{k-1} \leq \ldots \leq n_1$ as per the fundamental theorem of abelian groups. If $n_1 < n$, the above product has at least two factors, say $H = \mathbb{Z}/p^{n_1} = \langle a \rangle$, and $N = \mathbb{Z}/p^{n_2} = \langle b \rangle$. $H$ is a subgroup of order $p^{n_1}$, but so is $\langle a^p \rangle \times \left\langle b^{p^{n_1-1}} \right\rangle$, a contradiction. This completes the proof. □

We use this to answer the following prelim question.

**Problem 7.**[Prelim 2005, 8]. For each prime $p$ and positive integer $n$, how many elements $\alpha$ are in $\mathbb{F}_{p^n}$ such that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^6}$?

Applying the lemma will show that $\mathbb{F}_{p^n}$ contains precisely one copy of $\mathbb{F}_{p^6}$ iff $6 \mid n$ (this latter half does not follow from the lemma). Clearly, $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^6}$ necessitates $\alpha \in \mathbb{F}_{p^6}$, so we can forget about the $n$ and only look at which elements $\alpha \in \mathbb{F}_{p^6}$ satisfy $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^6}$. This is equivalent to asking how many $\alpha$ satisfy $\{ 1, \alpha, \cdots, \alpha^5 \}$ are linearly independent. But this question is incredibly difficult to answer. Instead, recall that the only subfields of $\mathbb{F}_{p^6}$ are $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$. $\alpha \in \mathbb{F}_{p^6}$ will generate all of $\mathbb{F}_{p^6}$ iff $\alpha$ is not in any of those subfields. This follows since it will generate a subfield, and to generate either of the smaller ones $\alpha$ must first be in the smaller ones. The only elements common to $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ are those from $\mathbb{F}_p$ (this follows since $2 \nmid 3$, so $\mathbb{F}_{p^3}$ does not contain $\mathbb{F}_{p^2}$ as a subfield). Thus $p^6 - p^3 - p^2 + p$ (we removed the elements from $\mathbb{F}_p$ twice) elements from $\mathbb{F}_{p^6}$ (and hence those from $\mathbb{F}_{p^n}$) will generate $\mathbb{F}_{p^6}$. Notably, this gives an upper bound on the number of irreducible polynomials of degree 6 in $\mathbb{F}_p$.

**Problem 4** (2016, 2). Let $a \in \mathbb{N}, a > 0$. Compute the Galois group of the splitting field of the polynomial $f(x) = x^5 - 5a^4x + a$ over $\mathbb{Q}$.

Observe that $f'(x) = 5x^4 - 5a^4$. This polynomial has roots $\pm a, \pm ia$, only two of which are real, so this polynomial has precisely 2 real roots. Plugging these back into $f$, a quick check shows that none are roots of $f$, meaning that $f$ has no repeat roots, since repeat roots of $f$ are also roots of the derivative. Suppose that $f(x)$ had 5 real roots, labeled by $\alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 < \alpha_5$ (we may assume they are distinct by the previous sentence). Applying the intermediate value theorem 4 times will yield $\beta_1 \in (\alpha_1, \alpha_2), \beta_2 \in (\alpha_2, \alpha_3), \ldots, \beta_4 \in (\alpha_4, \alpha_5)$ so that $f'(\beta_i) = 0$. But this is a contradiction as we computed $f'$ to only have 2 real roots. Notice that $f$ cannot have (exactly) 4 real roots since complex roots come in pairs, i.e. if $z = a + bi$ is a root, then $\bar{z} = a - bi$ is another one. A short calculation shows that $\lim_{x\to-\infty} f(x) = -\infty$ and $\lim_{x\to\infty} f(x) = \infty$, that $f(a) = -4a^4 + a < 0$ and finally that $f(-a) = 4a^4 + a > 0$. By the intermediate value theorem we find 3 real roots, one in $(-a, a)$, one in $(-\infty, -a)$ and finally one in $(a, \infty)$. Thus $f$ has precisely 2 complex roots, so we may apply a theorem from class to see that $\mathrm{Gal}\left(\mathbb{Q}_f/\mathbb{Q}\right) \cong S_5$. (This theorem I have only proven for $a$ with one prime divisor with power = 1 or congruent to $3, 4 \bmod 7$ or $1, 10 \bmod 11$ however this is not a complete solution and apparently one is not known).

**Problem 19** (2007, 2). Let $K$ be a field of characteristic 0 and $f \in K[x]$ an irreducible polynomial of degree $n$. Let $L$ be a splitting field for $f$. Let $G = \mathrm{Gal}(L/K)$.

(1) Show that $G$ embeds in the symmetric group $S_n$.

Let $R$ be the set of roots of $f$, and define an action of $G$ on $R$ by $\varphi \cdot r = \varphi(r)$. Verifying that this is an action is trivial, and this action is faithful since if $\varphi, \varphi'$ agree on all roots, then they agree on the entire splitting field, since any $x \in L$ is a $K$-linear combination of the roots. This yields an injection $G \hookrightarrow S_n$.

(2) For each $n$, give an example of a field $K$ and a polynomial $f$ such that $G = S_n$.

We begin by proving the following lemma. Let $n \equiv 5 \bmod 6$. Then

$$x^n - x - 1 = (x^2 + x + 1) \sum_{\substack{i=0 \\ i\not\equiv 1 \bmod 3}}^{n-2} x^i = \sum_{\substack{i=0 \\ i\not\equiv 1 \bmod 3}}^{n-2} (x^{i+2} + x^{i+1} + x^i)$$

in $\mathbb{F}_2$.

Expanding the sum with the terms $i \equiv 1 \bmod 3$ in red,

$$\begin{aligned} &x^n + x^{n-1} + \color{red}{x^{n-2}} + \cdots + \color{red}{x^3} + x^2 \\ &\quad x^{n-1} + x^{n-2} + \color{red}{x^{n-3}} + \cdots + \color{red}{x^2} + x \\ &\qquad x^{n-2} + x^{n-3} + \color{red}{x^{n-4}} + \cdots + \color{red}{x} + 1 \end{aligned}$$

Since $2 \equiv 0 \bmod 2$, we can see that the only terms that are not added twice to themselves is $x^n$, $x$, and 1. The rest are canceled since we have exactly 2 remaining per line. The crucial use $n \equiv 5 \bmod 6$ is noting that $n - 4 \equiv 1 \bmod 6$ so $n - 4 \equiv 1 \bmod 3$, and this is the last time that terms are marked red. This establishes the above equality.

Next we prove the following lemma:

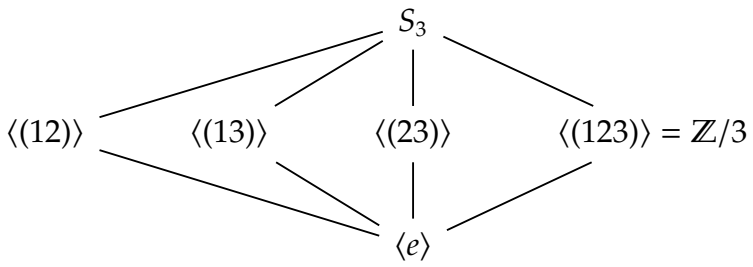
**Lemma 1.** *There are infinitely many primes $p \equiv 5 \bmod 6$.*

*Proof.* Suppose there were only finitely many, say $\{ p_1, \ldots, p_n \}$. Write $P = 6p_1 \cdots p_n - 1$. By reducing $\bmod p_i$, we see that $\gcd(P, p_i) = 1$ for each $i$. Suppose that $xy \equiv 5 \bmod 6$. Clearly, $xy \equiv 2 \bmod 3$ and $xy \equiv 1 \bmod 2$. By trying every case, this tells us that both $x, y$ are odd, and that (at least) one of $x, y \equiv 2 \bmod 3$. Suppose WLOG it is $x$. Since 5 is also a solution to $x \equiv 2 \bmod 3$, $x \equiv 1 \bmod 2$, by the Chinese remainder theorem, every other solution to this linear system is $\equiv 5 \bmod 6$, so in particular $x \equiv 5 \bmod 6$. If $P$ is composite we arise at a contradiction, since $P$ is bigger than $p_i$ for each $i$. By using this small lemma, at least one prime divisor has to be $\equiv 5 \bmod 6$. But $p$ is coprime to each prime $\equiv 5 \bmod 6$, a contradiction. □

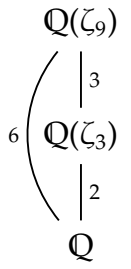
Fixing $n$, choose a prime $p \equiv 5 \bmod 6$ so that $p > n$. Let $f(x) = x^p - x - 1$, and write $f = g_1 \cdots g_n$ as the product of its irreducible factors in $\mathbb{F}_p$. Let $\alpha$ be a root of $g_1$. Since $\varphi(x) = x^p$ is an automorphism of $L = \mathbb{Q}_f$, it follows that $\varphi(\alpha) = \alpha^p = \alpha + 1$ is another root. Thus $\alpha, \alpha + 1, \cdots, \alpha + p - 1$ are all distinct roots of $g_1$, which shows that $\deg g_1 = \deg f$ which shows that $f = g_1$ is irreducible. Since $p \mid |L : \mathbb{Q}| = |G|$, $G$ has an element of order $p$, and since $S_p$ is acting on $p$ numbers, this element must be a $p$ cycle (notably, it cannot be a product of two disjoint $p$-cycles). Recall that there is an injection $\mathrm{Gal}\left(\mathbb{F}_{2,f}/\mathbb{F}_2\right) \hookrightarrow \mathrm{Gal}(L/\mathbb{Q})$. The former group contains the automorphsim sending one root of $x^2 + x + 1$ to the other one and fixing everything else, which is a 2-cycle. Thus $\mathrm{Gal}(L/\mathbb{Q})$ contains a 2-cycle and a $p$-cycle, and, using the incredibly important fact that $p$ is prime, shows that $\mathrm{Gal}(L/\mathbb{Q}) = S_p$. Taking $K = L^{S_n}$ (recalling that $S_n \leq S_p$) will yield, by the fundamental theorem of Galois theory, a field extension $L/K$ so that $\mathrm{Gal}(L/K) \cong S_n$.

(3) Let $n = 3$. What are the possible groups $G$?

Since $f(x)$ is irreducible over degree 3, the Galois group has order divisible by 3. Below is the subgroup lattice of $S_3$:




The only subgroups of $S_3$ with order divisible by 3 are $S_3$ and $\mathbb{Z}/3$. By the previous lemma we know that we can attain $S_3$, so we just have to find an extension with Galois group $\mathbb{Z}/3$. Recall the main theorem on cyclotomic extensions: importantly, that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$. We see then that $|\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})| = \varphi(9) = 6$ and $|\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})| = \varphi(3) = 2$. Then we get the following diagram of degrees:



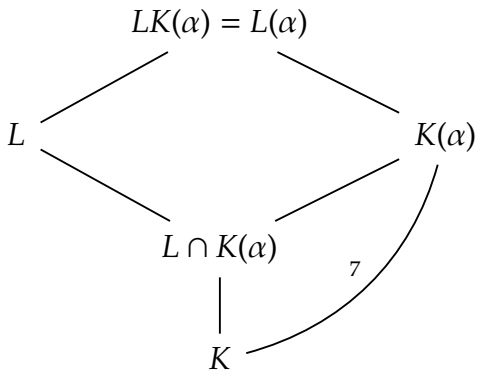

In particular, $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3))$ is a group of order 3, thus is $\mathbb{Z}/3$.

**Problem 18** (2007, 1). Let $K$ be a field and $L$ a Galois extension of $K$. Let $f$ be an irreducible polynomial in $K[x]$ of degree 7 and suppose $f$ has no zeros in $L$. Show that $f$ is irreducible in $L[x]$.

Recall that if $L/K$ is Galois, and $F/K$ is any extension, then

$$\mathrm{Gal}(LF/L) \cong \mathrm{Gal}(F/L \cap F)$$

Let $\alpha$ be a root of $f$ in some algebraic closure. Then we have the following diagram:




Where we have marked that $|K(\alpha) : K| = 7$. Since 7 is prime, it follows that $|K(\alpha) : L \cap K(\alpha)| = 1$ or 7. In the former case, $L \cap K(\alpha) = K(\alpha)$, which would say that $K(\alpha) \subset L$, meaning $\alpha \in L$, a contradiction since $L$ has no roots of $f$. Thus $|K(\alpha) : L \cap K(\alpha)| = 7$ and $L \cap K(\alpha) = K$. Then $|L(\alpha) : L| = |K(\alpha) : K| = 7$, so writing $p(x) = \mathrm{Irr}_L(\alpha)$, we know that $\deg p(x) = 7$. As $f(x)$ is another polynomial with $\alpha$ as a root, we have that $p(x) \mid f(x)$. Since $f(x)$ is monic and degree 7, we have concluded that $p(x) = f(x)$ is irreducible.