ROOTS OF UNITY IN AN ARBITRARY GROUP

LEO GOLDMAKHER

ABSTRACT. Gauss famously proved that $\mathbb{F}_p^\times$ is cyclic. In fact, he proved more: for any $d \mid p-1$, there are precisely $\varphi(d)$ elements of order d in $\mathbb{F}_p^\times$. Here we consider how this generalizes to other finite groups. Among other results, we prove that a finite group is cyclic iff it doesn't have too many roots of unity.

1. GAUSS' THEOREM

Gauss explored primitive roots (mod p). Among other things, he proved the following

Theorem 1.1. *$\mathbb{F}_p^\times$ is cyclic.*

The theorem asserts that $\exists a \in \mathbb{F}_p^\times$ that generates all of $\mathbb{F}_p^\times$, i.e. such that $\overbrace{\{a^k : k \in \mathbb{Z}\}}^{\langle a \rangle} = \mathbb{F}_p^\times$. How can we find such a generator? No idea. In fact, it remains a major open problem to find a generator in some way that's significantly more efficient than trial and error.

OK, so we can't prove the existence of a generator by finding one. Instead, consider the set of all the generators:

$$A := \{a \in \mathbb{F}_p^\times : \langle a \rangle = \mathbb{F}_p^\times\}.$$

Are there any relationships among the elements of A? A bit of playing around leads to the following:

Proposition 1.2. *If $r \in A$, then $r^k \notin A$ whenever $(k, p-1) > 1$.*

Proof. We have

$$(r^k)^{\frac{p-1}{(k,p-1)}} = (r^{p-1})^{\frac{k}{(k,p-1)}} = 1.$$

Thus, if $(k, p-1) > 1$, the order of r^k must be less than $p-1$, which means r^k can't be a generator. $\square$

Corollary 1.3. $|A| \le \varphi(p-1)$.

Unfortunately, this is exactly the opposite of what we want: a *lower* bound on $|A|$. So it seems we've made no progress.

Remarkably, it turns out that we can derive an exact formula for $|A|$ from these ideas! First, though, we must generalize our argument a bit. Set

$$A_d := \{a \in \mathbb{F}_p^\times : |\langle a \rangle| = d\},$$

i.e. the set of all elements of $\mathbb{F}_p^\times$ of order d. Replacing $p-1$ by d in the proof of Proposition 1.2 yields:

Proposition 1.4. *If $r \in A_d$, then $r^k \notin A_d$ whenever $(k, d) > 1$.*

One is tempted to instantly deduce that $|A_d| \le \varphi(d)$, but there's a wrinkle: there might be elements of order d that aren't of the form r^k. In fact, it turns out this doesn't happen, as we now prove.

Corollary 1.5. $|A_d| \le \varphi(d)$.

Proof. If $A_d = \varnothing$, the claim is trivial, so we assume there exists some $r \in A_d$. If we knew that every element of order d can be expressed in the form r^k (i.e., that $A_d \subseteq \langle r \rangle$), then Proposition 1.4 would imply the claim.

Observe that $\langle r \rangle$ has precisely d elements, each of which is a root of $f(x) := x^d - 1$. On the other hand, f has at most d roots! We deduce that $\langle r \rangle$ is the set of *all* roots of $x^d - 1$, from which it follows that $A_d \subseteq \langle r \rangle$. $\square$

Now comes an amazing step: from these upper bounds we will deduce an exact formula. Observe that

$$\sum_{d|p-1} |A_d| = p - 1$$

by Lagrange's theorem. On the other hand, by considering the fractions $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots, \frac{n}{n}$ in reduced form we see

$$\sum_{d|n} \varphi(d) = n$$

for any positive integer n. Combining our previous two displayed equations yields

$$\sum_{d|p-1} (\varphi(d) - |A_d|) = 0,$$

and Corollary 1.5 shows that each term in the sum is non-negative. This is only possible if $|A_d| = \varphi(d)$ for all $d \mid p-1$! We've therefore proved:

Theorem 1.6. *The number of elements of order d in $\mathbb{F}_p^\times$ is 0 if $d \nmid p-1$, and $\varphi(d)$ if $d \mid p-1$.*

Taking $d = p-1$ instantly implies Theorem 1.1.

Note that during the course of the argument we proved that if there exists $r \in A_d$, then $A_d \subseteq \{r^k : k \in \mathbb{Z}_n^\times\}$. Since we've now proved that $|A_d| = \varphi(d)$, we deduce

Porism 1.7. *If $r \in \mathbb{F}_p^\times$ has order d, then the set $\{r^k : k \in \mathbb{Z}_n^\times\}$ is the set of* all *elements of order d.*

This tells us that while it might be hard to find an example of an element of order d, but once you do it's easy to find all the others.

2. Characterizing cyclic groups

It's natural to ask whether the above proofs go through for groups other than $\mathbb{F}_p^\times$. Right away, we see the answer must be no—the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$, for example, has no generator. But where exactly does the proof break down?

Careful inspection reveals there's only one dubious step: in the proof of Corollary 1.5, the polynomial f might have more than d roots. (This is the case in the Klein group: there are 4 roots of $x^2 - 1$.) We deduce

Proposition 2.1. *Suppose G is a finite group of order n and identity element e. If $x^d = e$ has at most d solutions for every $d \mid n$, then there are precisely $\varphi(d)$ elements of order d in G, for any $d \mid n$.*

Note that the conclusion of the proposition instantly implies that G is cyclic. But now observe that if G is a finite cyclic group—say, $G \simeq \mathbb{Z}_n$—then there are precisely d distinct solutions to $x^d = 1$ for any $d \mid n$. Thus, we've proved

Proposition 2.2. *Suppose G is a finite group of order n and identity element e. The following are equivalent:*

- *$x^d = e$ has at most d solutions for any $d \mid n$.*
- *There are $\varphi(d)$ elements of order d for any $d \mid n$.*
- *G is cyclic.*

Recall that in a field, degree n polynomials have at most n distinct roots. Proposition 2.2 instantly yields

Corollary 2.3. *Let $\mathbb{F}$ be a field. Then any finite subgroup of $\mathbb{F}^\times$ is cyclic.*

3. Roots of unity in arbitrary groups

Proposition 2.2 gives a criterion for a group to be cyclic in terms of the number of solutions to $x^d = e$. What can we say about the number of solutions for non-cyclic groups?

Theorem 3.1 (Frobenius, 1903)**.** *If G is a finite group of order n and identity element e, and $d \mid n$, then the number of solutions to $x^d = e$ is a multiple of d.*

If G is cyclic, this is trivial—there are precisely d solutions in that case—but it implies that for any noncyclic group there are at least $2d$ solutions.

The theorem quoted above is a special case of what Frobenius actually proved:

Theorem 3.2 (Frobenius, 1903)**.** *If G is a finite group, the number of solutions to $x^d = a$ is a multiple of $(d, |C(a)|)$, where $C(a)$ is the centralizer of a.*

Corollary 3.3. *If G is abelian and $a \in G$, then the number of solutions to $x^d = a$ is a multiple of $(d, |G|)$.*

Frobenius' theorem tells us about the number of d^{th} roots of a given element. What about the structure of the set of these roots? When G is abelian, the set of solutions to $x^d = e$ is a subgroup of G. If G is non-abelian, however, this might not be true:

Example 1. Consider the symmetric group S_3. The set of solutions to $x^2 = ()$ is $\{(), (1\,2), (1\,3), (2\,3)\}$, which isn't a subgroup of S_3.

Nonetheless, Frobenius conjectured that if the number of roots of $x^d - e$ is precisely d (for some $d \mid n$), then the set of these roots is not only a subgroup, but a *normal* subgroup of G. This is now known to hold, thanks to the classification of finite simple groups. Remarkably, no simpler proof has been discovered.

DEPT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA, USA 01267
Email address: `Leo.Goldmakher@williams.edu`