CAUCHY'S THEOREM: PROOFS AND APPLICATIONS

KARUN RAM

1. Introduction

An essential idea in discussing the structure of groups is that of order: that is, for each element in the group, the minimum number of times one needs to multiply the same element to get back to the identity. It allows us to understand the nature of individual elements, occasionally associating them with physical representations as well. For example, we write the group D_{2n} as

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

The fact that the element r has order n, and that the element s has order 2, allows us to naturally associate them with rotating and reflecting an n-gon. The purpose of this example is meant simply to illustrate that an understanding of order may reveal substantial information about the nature of a group.

Lagrange's Theorem is a result that allows us to better understand what the orders of elements in a group might look like. In particular, we restrict ourselves (for the remainder of this paper) to finite groups, where every element must have finite order. Lagrange's theorem still holds in the infinite case, but with some caveats that will not be discussed in this paper.

Theorem 1.1 (Lagrange)**.** *Let $H \leq G$. Then, $\#H \mid \#G$. A corollary is that if $a \in G$, then $|a|$ divides $\#G$.*

Now, the natural question that arises is whether the converse is true; that is, if $d \mid \#G$, must there exist $a \in G$ such that $ord(a) = d$? This statement is false by counterexample. Consider A_4, the subgroup of S_4 (the symmetric group) containing only even permutations. In particular, it is easy to show that $\#A_4 = 12$, but that there is no element $a \in A_4$ such that $|a| = 6$, even though $6 \mid 12$. However (especially considering that A_4 is the smallest such group containing a counterexample to the converse statement), investigating cases in which the converse does hold appears fruitful. Thus arises Cauchy's Theorem.

Theorem 1.2 (Cauchy)**.** *Let p be a prime dividing the order of a finite group G. Then, there exists an element of order p in G. Equivalently, there exists a cyclic subgroup of order p in G.*

It is interesting to note that though Cauchy first proposed the theorem, his original proof contained a significant logical flaw. However, though Cauchy's proof was incomplete, it was not inherently incorrect. In particular, it misses on a relatively minor step claiming the existence of the element proclaimed. What is most intriguing about this error is that later theorems, such as those by Sylow, often thought to be derived from Cauchy's Theorem, were actually proved without reliance on the theorem [3].

Though it is interesting to peruse Cauchy's motivation for publishing an obviously flawed argument, we may never truly be sure. In this paper, we instead explore (correct) proofs of Cauchy's Theorem, along with some applications of the theorem in proving other meaningful results.

Contents. In section 2, we explore three proofs of Cauchy's Theorem. In section 3, we explore results that follow from Cauchy's Theorem; finally we conclude in section 4 with some brief remarks on Cauchy's Theorem and some more general philosophical remarks.

2. Proofs of Cauchy's Theorem

We explore three proofs for Cauchy's Theorem. Each proof approaches the theorem in a different manner, utilizing different tools to arrive at the same result. The first proof relies on group actions and the orbit-stabilizer theorem. The second is an inductive proof relying on the class equation and quotient groups. The third relies on a stronger result, Sylow's Theorem, to prove Cauchy's Theorem as a special case.

Proof 1. We first prove Cauchy's Theorem as outlined in [1]. Define

$$S_p = \{(x_1, x_2, ..., x_p) \mid x_i \in G, x_1x_2...x_p = 1\}.$$

We first claim that $\#S_p = (\#G)^{p-1}$. This is true by a combinatorial argument: in particular, we have free choice over each $x_1, x_2, ..., x_{p-1}$, and x_p is uniquely determined by our choice of $x_1, x_2, ..., x_{p-1}$; namely, $x_p = (x_1x_2...x_{p-1})^{-1}$. By the product principle, we have that $\#S_p = (\#G)^{p-1} \times 1 = (\#G)^{p-1}$.

Next, we define the action of the group of cyclic permutations on S_p. In particular, we define a group action

$$\alpha \colon H \times S_p \to S_p$$

where $H = \langle (1\ 2\ ...\ p) \rangle$ is the set of cyclic permutations on indices 1 through p, and where α acts by permuting the p-tuples by indices, defined by the permutation given by the element of H. Notice that each element in H, by construction, can be written as $(1\ 2\ ...\ p)^k$ for some $k \in \{0, ..., p-1\}$. We have that H acts on S_p since trivially, H is a group, $\varepsilon \cdot (x_1, x_2, ..., x_p) = (x_1, x_2, ..., x_p)$ and

$$\begin{aligned}
\sigma_1(\sigma_2(x_1, x_2, ..., x_p)) &= (1\ 2\ ...\ p)^i((1\ 2\ ...\ p)^j(x_1, x_2, ..., x_p)) \\
&= (1\ 2\ ...\ p)^i(x_{1+j}, x_{2+j}, x_p, x_1, ..., x_j) \\
&= (x_{1+j+i}, x_{2+j+i}, x_p, x_1, ..., x_{j+i}) \\
&= (1\ 2\ ...\ p)^{i+j}(x_1, x_2, ..., x_p).
\end{aligned}$$

Also, α is well-defined (the image of the map lies in the codomain) since

$$\begin{aligned}
\sigma(x_1, x_2, ..., x_p) &= (1\ 2\ ...\ p)^j(x_1, x_2, ..., x_p) \\
&= (x_{1+j}, x_{2+j}, x_p, x_1, ..., x_j)
\end{aligned}$$

which is in S_p since

$$\begin{aligned}
(x_{j+1}x_{j+2}...x_p)(x_1x_2...x_j) &= (x_1x_2...x_j)^{-1}(x_1x_2...x_j)(x_{j+1}x_{j+2}...x_p)(x_1x_2...x_j) \\
&= (x_1x_2...x_j)^{-1}1(x_1x_2...x_j) \\
&= (x_1x_2...x_j)^{-1}(x_1x_2...x_j) \\
&= 1.
\end{aligned}$$

So, H acts on S_p. We thus consider the orbits of S_p; in particular, they partition S_p.

Theorem 2.1 (Orbit-Stabilizer)**.** *Let H act on X. Then, for all $x \in X$*

$$\#H = \#Stab_H(x) \cdot \#Orb(x).$$

In particular, $\#Orb(x) \mid \#H$.

By this theorem, we have that the size of any equivalence class (orbit) must divide $\#H = p$; in particular, it must be either 1 or p. Now, we prove that $\#Orb(y) = 1 \iff y = (x, x, ..., x)$ for some $x \in G$ where $x^p = 1$.

For the forward direction, we proceed by contradiction, and so we have two cases. Either $x^p \neq 1$, in which case $y \notin S_p$. Otherwise, $Orb(y)$ contains $(..., x, x', ...)$ whose tuple contains two distinct adjacent elements (this is necessary since otherwise, every element in the tuple y would be equal). Then necessarily, there exists a cyclic permutation σ such that $\sigma(..., x, x', ...) = (x', ..., x)$, and so the equivalence class contains at least two distinct elements. By contradiction, we have the forward direction. The converse direction is trivial, so we have proven the statement.

Since orbits partition S_p, we have that $(\#G)^{p-1} = \#S_p = k + pd$, where k is the number of orbits of order 1 and d is the number of orbits of order p.

We finally conclude Cauchy's Theorem. Since we have that $S_p = (\#G)^{p-1} = k + pd$, and that $p \mid \#G$, we have that $p \mid S_p$ and $p \mid pd$. Hence, $p \mid k$. In particular, we have that $p \geq 2$ (because it is prime) and $k \geq 1$ (since $Orb((1, 1, ..., 1)) = \{(1, 1, ..., 1)\}$). Hence, since p is prime, $k \geq p$. In particular, there is at least one other orbit of the form $\{(x, x, ..., x)\}$, where $x \neq 1$ (by an earlier claim). So we have that $x^p = 1$; since $x \neq 1$, Lagrange's Theorem gives that x has order p. Thus we have Cauchy's Theorem.

Proof 2. We proceed by strong induction on the size of G. Our inductive hypothesis is that for all proper subgroups $H < G$, we have that if $p \mid \#H$, then there is an element $x' \in H$ of order p.

(Base case) Suppose $\#G = p$. Then, since $p > 1$, we have that there is an element $x \in G$ such that $x \neq 1$. In particular, by Lagrange's Theorem, we have that x has order p, since p is prime.

(Inductive case) Otherwise, suppose $\#G > p$.

Suppose that G is abelian. Then, we have two cases. Suppose there exists an element $x \in G$ such that p divides the order of x. Then we have that there exists an integer n such that $pn = |x|$; in particular, we have that $|x^n| = p$, and we have an element of order p.

Otherwise, p does not divide the order of x. Then, we consider $N = \langle x \rangle$. Since G is abelian, we have that $N \trianglelefteq G$. By Lagrange's Theorem, we have that $\#(G/N) = \frac{\#G}{\#N}$, and

since $x \neq 1$, $\#N > 1$. So, $\#(G/N) < \#G$, and $p \mid \#(G/N)$ (since $p \nmid \#N$). By the inductive hypothesis, we have that there must exist an element $\overline{y} = yN \in G/N$ of order p. In particular, $\overline{y}^p = \overline{1} \to y^p \in N$. Since $y \notin N$, we have that $\langle y^p \rangle \neq \langle y \rangle$. Hence $|y^p| < |y|$, and so $p \mid |y|$ (since $|y| = p|y^p|$). In particular, we have that $|y| = np$, and so we have that $|y^n| = p$.

Now, suppose that G is nonabelian. We rely on the class equation to resolve this case.

Theorem 2.2 (Class Equation)**.** *Let G be a group. Then*

$$\#G = \#Z(G) + \sum_{i=1}^{k} [G \colon C_G(x_i)]$$

where x_i is an element in the conjugacy class c_i.

If $p \mid Z(G)$ then we have by the previous case that $Z(G)$ (an abelian subgroup) contains an element of order p, and G must as well. Otherwise, we have that $p \nmid Z(G)$. Since $p \mid \#G$, we have (by a trivial contradiction) that at least one conjugacy class has size $[G \colon C_G(x_i)]$ such that $p \nmid [G \colon C_G(x_i)]$. In particular, since by definition $[G \colon C_G(x_i)] = \frac{\#G}{\#(C_G(x_i))}$, and since $p \mid \#G$, we have that $p \mid \#(C_G(x_i))$. Since the conjugacy class of a noncentral element must contain more than one element (again, a trivial proof by contradiction), we have that $\#(C_G(x_i)) < \#G$. So, we apply the inductive hypothesis to find that there exists $x \in C_G(x_i)$ of order p; hence x has order p in G.

The result follows from induction.

Proof 3. We prove Cauchy's Theorem as a corollary of a stronger statement, Sylow's Theorem.

Theorem 2.3 (Sylow)**.** *Let G be a group, and let p be a prime such that $p^n \mid\mid \#G$. Then there exists a Sylow p-subgroup of G of order p^n.*

Cauchy's Theorem follows by an application of Sylow's Theorem and Lagrange's Theorem. In particular, let $H \leq G$ be a subgroup with order p^n. Let $x \in H$ be a nonidentity element in H. Then by Lagrange's Theorem the order of x is equal to p^k, where $1 \leq k \leq n$. If $k = 1$, then we have an element in H, and thus in G, of order p. Otherwise, let $y = x^{p^{k-1}}$. In particular, $y \neq 1$ and $y^p = 1$, so we have that y has order p in H, and therefore in G. Hence we have Cauchy's Theorem.

Some remarks. Cauchy's Theorem is particularly interesting because it is the best possible generalizable result; in particular, it fails to hold if we extend to non-prime divisors or prime powers. For example, we consider (as described in the previous section) the group A_4. Though $6 \mid \#A_4 = 12$, we find that A_4 has no element of order 6 (and no subgroup of size 6). Similarly, we consider $D_4 = \langle r, s \mid r^2 = s^2 = 1, rs = sr^{-1} \rangle$. We have that $2^2 = 4 \mid \#D_4$, but every element in D_4 has order of either 2 (r, s, rs) or 1 (1) (note that $D_4 \cong V_4$). Hence we have that Cauchy's theorem truly is best possible; it fails for products of primes and prime powers, even in simple cases.

3. Applications

Cauchy's Theorem is widely relevant to proving other results in group theory. We explore two results that can be derived from Cauchy's Theorem.

The first result we prove is relevant to the Frobenius endomorphism [2] and the conditions in which it is an automorphism. The result has significance in number theory, among other fields:

Theorem 3.1. *Let G be a finite abelian group, and let $\phi \colon G \to G$ be a map given by $\phi(x) = x^k$ be a map. Then ϕ is an isomorphism if and only if $gcd(k, n) = 1$.*

Proof. First, suppose $\gcd(k, n) = 1$. Then, ϕ is a homomorphism because $\phi(xy) = (xy)^k = x^k y^k = \phi(x)\phi(y)$. ϕ is also bijective since k and n being coprime implies that the equation $kl \equiv 1$ mod n has a solution, and the map $\phi^{-1} \colon G \to G$ given by $x \mapsto x^l$ is trivially an inverse to ϕ.

Conversely, suppose $\gcd(k, n) > 1$. Then, in particular, we have that there exist some prime p such that $p \mid k$ and $p \mid n$. Since $p \mid n$, Cauchy's Theorem tells us that we have that there exists an element $x \in G$ of order p. Then, let $q = \frac{p}{k} \in \mathbb{Z}$ be an integer, and let $y = x^q$. Then, $\phi(y) = y^k = x^{qk} = x^p = 1$. We also have that $1^k = 1$, and hence ϕ is not injective. Thus ϕ cannot be an isomorphism. □

Another interesting result is a strengthening of Cauchy's Theorem in the case of abelian groups to a full converse of Lagrange's Theorem:

Theorem 3.2. *Let G be a finite abelian group of order n. Let m be a divisor of n. Then G has a subgroup of order m.*

Proof. We proceed by strong induction on n. Suppose that for all $1 \leq k < n$, a group of order k has a subgroup of order l for every $l \mid k$.

(Base case) The result is trivial for $n = 1$.

(Inductive case) Let G be a group of order n. We find a subgroup of order m. We divide into two cases: either m is prime or m is not.

Suppose m is prime. Then, by direct application of Cauchy's Theorem, we find an element x of order m. In particular, we have that $\langle x \rangle \leq G$ and $\#\langle x \rangle = m$, so we have a subgroup of order m.

Otherwise, let p be a prime such that $p|m$, and let $m = pd$, where $d \in \mathbb{Z}$. By Cauchy's Theorem, we have that there exists x_p in G such that $|x_p| = p$. In particular, we have that $\langle x_p \rangle$ is a normal subgroup of G with order p. Now, consider the quotient group $G/\langle x_p \rangle$. Since $p > 1$, we have that $\#(G/\langle x_p \rangle) = \frac{\#G}{p} < \#G$, and by the inductive hypothesis we have that there exists a subgroup $H \leq G/\langle x_p \rangle$ of order d, since $d \mid \#(G/\langle x_p \rangle)$. By the Fourth Isomorphism Theorem, we have that there exists a subgroup $K \leq G$ such that $K/\langle x_p \rangle \cong H$. In particular, by Lagrange's Theorem, since H has order d, K has order $dp = m$. Hence we have a subgroup of order m in G.

The result follows by induction. □

4. Conclusion

Cauchy's Theorem is not only an extremely versatile and useful result, as seen by the examples of its applications in Section 3, but it is also an intriguing mathematical exercise in applying the numerous tools available in group theory to prove a meaningful result (as we did in Section 2). In some ways, the numerous proofs for Cauchy's Theorem, along with the results that follow from it, are a microcosm for mathematical exploration as a whole: deploying a vast arsenal of mathematical devices to prove propositions that, in turn, give rise to other relevant results.

References

[1] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Hoboken, 2003.

[2] A homework problem set from Math 25 (Number Theory), Fall 2022, taught by Avinash Kulkarni

[3] https://www.sciencedirect.com/science/article/pii/S031508600300003X