PROOF OF CAUCHY'S THEOREM

KEITH CONRAD

The converse of Lagrange's theorem is false in general: if G is a finite group and $d \mid |G|$ then G doesn't have to contain a subgroup of order d. (For example,$|A_4| = 12$ and A_4 has no subgroup of order 6). The converse is true for prime d. This is Cauchy's theorem.

Theorem. (Cauchy) *Let G be a finite group and p be a prime factor of $|G|$. Then G contains an element of order p. Equivalently, G contains a subgroup of order p.*

The equivalence of the existence of an *element* of order p and a *subgroup* of order p is easy: an element of order p generates a subgroup of order p, and conversely a nonidentity element of a subgroup of order p has order p because p is prime.

Cauchy stated his theorem for permutation groups (*i.e.*, subgroups of S_n), not abstract finite groups, since the concept of an abstract finite group was not yet available [1], [2].

Before treating Cauchy's theorem, let's prove the special case $p = 2$. If $|G|$ is even, consider the set of pairs $\{g, g^{-1}\}$, where $g \neq g^{-1}$. This takes into account an even number of elements of G. Those g's that are *not* part of such a pair are the ones satisfying $g = g^{-1}$, *i.e.*, $g^2 = e$. Therefore if we count $|G| \bmod 2$, we can ignore the pairs $\{g, g^{-1}\}$ where $g \neq g^{-1}$ and we obtain $|G| \equiv |\{g \in G : g^2 = e\}| \bmod 2$. One solution to $g^2 = e$ is e. If it were the only solution, then $|G| \equiv 1 \bmod 2$, which is false. Therefore some $g_0 \neq e$ satisfies $g_0^2 = e$, which gives us an element of order 2.

Now we prove Cauchy's theorem.

Proof. We will induct on $|G|$.[1] Let $n = |G|$. Since $p \mid n$, $n \geq p$. The base case is $n = p$. When $|G| = p$, each nonidentity element of G has order p since p is prime. Suppose $n > p$, $p \mid n$, and the theorem is true for all groups with order less than n that is divisible by p. We treat separately abelian G (using homomorphisms) and nonabelian G (using conjugacy classes).

<u>Case 1</u>: G **is abelian.**

Assume no element of G has order p and we will get a contradiction.

No element has order divisible by p: if $g \in G$ has order r and $p \mid r$ then $g^{r/p}$ would have order p.

Let $G = \{g_1, g_2, \ldots, g_n\}$ and let g_i have order m_i, so each m_i is not divisible by p. Let m be the least common multiple of the m_i's, so m is not divisible by p and $g_i^m = e$ for all i. Because G is abelian, the function $f\colon (\mathbf{Z}/(m))^n \to G$ given by $f(\overline{a}_1, \ldots, \overline{a}_n) = g_1^{a_1} \cdots g_n^{a_n}$ is a *homomorphism*:[2]

$$f(\overline{a}_1, \ldots, \overline{a}_n) f(\overline{b}_1, \ldots, \overline{b}_n) = f(\overline{a_1 + b_1}, \ldots, \overline{a_n + b_n}).$$

That is,

$$g_1^{a_1} \cdots g_n^{a_n} g_1^{b_1} \cdots g_n^{b_n} = g_1^{a_1} g_1^{b_1} \cdots g_n^{a_n} g_n^{b_n} = g_1^{a_1+b_1} \cdots g_n^{a_n+b_n}$$

[1]Proving theorems by induction on the order of the group is a very fruitful idea in group theory.

[2]This function is well-defined because $g_i^m = e$ for all i, so $g_i^{a+mk} = g_i^a$ for any $k \in \mathbf{Z}$.

from commutativity of the g_i's. This homomorphism is surjective (each element of G is a g_i, and if $a_i = 1$ and other a_j's are 0 then $f(\overline{a}_1, \dots, \overline{a}_n) = g_i$), so by the first isomorphism theorem $(\mathbf{Z}/(m))^n/\ker f \cong G$. Therefore

$$|G| = \frac{|(\mathbf{Z}/(m))^n|}{|\ker f|} = \frac{m^n}{|\ker f|},$$

so $|G||\ker f| = m^n$. Thus $|G|$ is a factor of m^n, but p divides $|G|$ and m^n is not divisible by p, so we have a contradiction.

Case 2: G **is nonabelian.**

Assume no element of G has order p and we will get a contradiction.

In every proper subgroup H of G there is no element of order p (H may be abelian or nonabelian), so by induction *no proper subgroup of G has order divisible by p.* For each proper subgroup H, $|G| = |H|[G : H]$ and $|H|$ is not divisible by p while $|G|$ is divisible by p, so $p \mid [G : H]$ for every proper subgroup H of G.

Since G is nonabelian it has some conjugacy classes with size *greater* than 1. Let these be represented by $g_1, g_2, \dots, g_k$. Conjugacy classes in G of size 1 are the elements in $Z(G)$. Since the conjugacy classes in G form a partition of G, computing $|G|$ by adding the sizes of its conjugacy classes implies

$$|G| = |Z(G)| + \sum_{i=1}^{k}(\text{size of conj. class of } g_i) = |Z(G)| + \sum_{i=1}^{k}[G : Z(g_i)], \tag{1}$$

where $Z(g_i)$ is the centralizer of g_i. (For each $g \in G$, its conjugacy class in G has size equal to $[G : Z(g)]$.) Since the conjugacy class of each g_i has size greater than 1 we have $[G : Z(g_i)] > 1$, so $Z(g_i) \neq G$ for all i. Therefore $p \mid [G : Z(g_i)]$. In (1), the left side is divisible by p and each index in the sum on the right side is divisible by p, so $|Z(G)|$ is divisible by p. Since no proper subgroup of G has order divisible by p, $Z(G)$ has to be all of G. That means G is abelian, which is a contradiction. □

Reread this proof until you see how it hangs together. For instance, notice that we did not need the nonabelian case to treat the abelian case and the abelian case by itself did not require induction. Quite a few books prove Cauchy's theorem initially just for abelian groups before developing suitable concepts (like conjugacy classes) to prove Cauchy's theorem for nonabelian groups. We needed the abelian case as part of the nonabelian case since in the inductive step of Case 2, the proper subgroups $Z(g_i)$ of the nonabelian group G might be abelian. (All subgroups of abelian groups are abelian while subgroups of nonabelian groups can be abelian or nonabelian, so there is an asymmetry there.)

The proof above could be reorganized to treat the two cases in the reverse order, as follows. If a finite group G with order divisible by p has no element of order p then first assume G is nonabelian and run through Case 2 (assuming the theorem is proved for all groups of smaller order, abelian and nonabelian) to get a contradiction, so G must be abelian. Then run through Case 1 to get a contradiction if G is abelian.

References

[1] A. L. Cauchy, Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre, pp. 151–252 in "Exercises d'Analyse et de Physique Mathématique, Tome 3e," Bachelier, Paris, 1844. Online at https://archive.org/details/ecercicesdanaly03caucrich/page/n3/mode/2up.

[2] M. Meo, The mathematical life of Cauchy's group theorem, *Historia Math.* **31** (2004), 196–221.