PROOF OF CAUCHY'S THEOREM

KEITH CONRAD

The converse of Lagrange's theorem is false in general: when $d \mid |G|$, G doesn't have to contain a subgroup of order d. There is a converse when d is prime. This is Cauchy's theorem.

Theorem. (Cauchy 1845) *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, while conversely any nonidentity element of a subgroup of order p has order p because p is prime.

Before treating Cauchy's theorem, let's see that the special case for $p = 2$ can be proved in a simple way. 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 use induction on $|G|$.[1] Let $n = |G|$. Since $p \mid n$, $n \geq p$. The base case is $n = p$. When $|G| = p$, any nonidentity element of G has order p because p is prime. Now suppose $n > p$, $p \mid n$, and the theorem is true for all groups having order less than n that is divisible by p. We will treat separately abelian G (using homomorphisms) and nonabelian G (using conjugacy classes).

Case 1: G **is abelian.** Assume no element of G has order p. Then 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 m_i is not divisible by p. Set m to 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 $f(\overline{a}_1, \ldots, \overline{a}_n) = g_1^{a_1} \cdots g_r^{a_r}$ 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,

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

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 $f(\overline{a}_1, \ldots, \overline{a}_n) = g_i$), so by the first isomorphism

[1] Proving a theorem on groups 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 $k \in \mathbf{Z}$.

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.**

If a proper subgroup H of G has order divisible by p, then by induction there is an element of order p in H, which gives us an element of order p in G. Thus we may assume *no proper subgroup of G has order divisible by p*. For any proper subgroup H, $|G| = |H|[G : H]$ and $|H|$ is not divisible by p, so $p \mid [G : H]$ for every proper subgroup H of G.

Let the conjugacy classes in G with size *greater* than 1 be represented by $g_1, g_2, \ldots, g_k$. Conjugacy classes of size 1 are the elements in $Z(G)$. Since the conjugacy classes in G form a partition of G, counting $|G|$ by counting 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 proper subgroups of G don't have order divisible by p, $Z(G)$ has to be all of G. That means G is abelian, which is a contradiction. $\square$

It is worthwhile reading and re-reading 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. In fact, quite a few books prove Cauchy's theorem for abelian groups before they develop suitable material (like conjugacy classes) to handle Cauchy's theorem for nonabelian groups.