PROOF OF CAUCHY'S THEOREM

KEITH CONRAD

The converse of Lagrange's theorem is false in general: when $d|\#G$, G doesn't have to contain a subgroup of size d. The most basic valid converse to Lagrange's theorem occurs for prime divisors. This is Cauchy's theorem.

Theorem 1 (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 size p.*

The equivalence of the existence of an *element* of order p and a *subgroup* of size p is easy: an element of order p generates a subgroup of size p, while conversely a subgroup of size p contains elements of order p since p is prime.

Before treating the general case, let's see that the case $p = 2$ of Cauchy's theorem 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 which are not part of such a pair are the ones satisfying $g = g^{-1}$, *i.e.*, $g^2 = e$. One such element is e. If it was the only one, then G would have odd size (why?). Since we are told G has even size, there must be $g_0 \neq e$ such that $g_0 = g_0^{-1}$, so $g_0^2 = e$ and g_0 has order 2.

Although there is always a subgroup of order p when $p|\#G$, there need not be a subgroup of index p. For example, A_4 has order 12 but no subgroup of index 2.

Now we prove Cauchy's theorem.

Proof. We will prove Cauchy's theorem by induction on $\#G$, treating separately abelian G (using quotient groups) and non-abelian G (using the class equation).

Let $n = \#G$. Since $p|n$, $n \geq p$. The base case is $n = p$. When $\#G = p$, any non-identity element of G has order p because p is prime.

Now suppose $n > p$, $p|n$, and the theorem is true for all groups with size less than n and divisible by p. Let G be a group of size n.

<u>Case 1</u>: G is abelian. Since $p|n$ and $n > p$, $\#G$ is not prime. Therefore G has a proper non-trivial subgroup, say H. Since G is abelian, G/H is a group. Since

$$\#H \cdot \#(G/H) = \#G = n,$$

the prime p divides either $\#H$ or $\#(G/H)$ (we don't know which). Therefore, by induction, H or G/H has an element with order p. If H does, then so does G. If G/H has an element with order p, say $\overline{g}$, then what can we say about the order of g (in G)? Let m be the order of g. Then

$$g^m = e \text{ in } G \Longrightarrow \overline{g}^m = \overline{e} \text{ in } G/H \Longrightarrow p|m.$$

Thus, g has order divisible by p, so $g^{m/p}$ is an element of G with order p.

<u>Case 2</u>: G is non-abelian. Since $\#G$ is not a prime, G has a non-trivial proper subgroup, say H. Since $\#G = \#H \cdot [G : H]$, p divides either H or $[G : H]$. If p divides H, we're done by induction. In other words, if G has a proper subgroup with size divisible by p, we're done by induction.

But if, instead, $p|[G : H]$ for every non-trivial proper subgroup H, then the argument from the abelian case breaks down since H need not be a normal subgroup of G, so we can't apply induction with the smaller group G/H.

Happily, we can take advantage of the non-commutativity to show that this problem does not arise: when G is a non-abelian group and $p|\#G$, there is always a non-trivial proper subgroup with size divisible by p. That is what the rest of the proof will demonstrate.

Since G is non-abelian, its center $Z(G)$ is a proper subgroup. For each $g \in G$, the centralizer of g

$$Z(g) = \{h \in G : hg = gh\}$$

is a subgroup of G, and this is a proper subgroup when $g \notin Z(G)$. If $p|\#Z(g)$ for some $g \notin Z(G)$, then $Z(g)$ is a proper subgroup of G and its size is divisible by p so we're done. If $p|\#Z(G)$, then again we're done. We will use the class equation to show one of these possibilities ($p|\#Z(g)$ for some $g \notin Z(G)$ or $p|\#Z(G)$) must happen.

Let the conjugacy classes in G with size *greater* than 1 be represented by $g_1, g_2, \ldots, g_r$. Then the class equation for G says

$$\#G = \#Z(G) + \sum_{i=1}^{r} [G : Z(g_i)] = \#Z(G) + \sum_{i=1}^{r} \frac{\#G}{\#Z(g_i)}.$$

We look at p-divisibility of the terms in this equation. The left side is divisible by p. If some $Z(g_i)$ has size divisible by p, we'd be done. On the other hand, if each $Z(g_i)$ has size not divisible by p, then each index $[G : Z(g_i)]$ is divisible by p. Therefore the remaining term, $\#Z(G)$, must be divisible by p. $\square$

It is worthwhile reading and re-reading this proof until you see how it hangs together. For instance, notice that in the proof for abelian G, the smaller groups which we used are subgroups H and quotient groups G/H. Both of these are abelian when G is abelian, so inductively we did not need the non-abelian 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 the class equation) to handle Cauchy's theorem for non-abelian groups.