CATEGORY THEORY
CAUCHY'S THEOREM

PAUL L. BAILEY

Lemma 1. *Let G be a finite abelian group of order $m \in \mathbb{N}$.*
Let $m \in \mathbb{Z}$ with $\gcd(m, n) = 1$.
Then the power map $\phi : G \to G$ given by $g \mapsto g^n$ is an automorphism.

Proof. Since G is abelian, ϕ is a homomorphism.

Let $g \in \ker(\phi)$, so that $g^n = 1$. Then the order of g divides n. Also the order of g divides the order of the group by LaGrange's Theorem. But this says that the order of g divides $\gcd(m, n) = 1$, so the order of g is 1, and $g = 1$. Thus ϕ is injective, and since G is finite, it is also surjective. □

Lemma 2. *Let G be a finite abelian group and let p be a prime integer.*
If $p \mid |G|$, then G has an element of order p.

Proof. Let the order of G be pm for some $m \in \mathbb{Z}$. Let $k \in G$ be a nontrivial element. If $\text{ord}(k) = pn$ for some $n \leq m$, then then k^n has order p and we are done. Thus we suppose that p does not divide the order of k. Let H be the cyclic subgroup generated by k. Then p does not divide the order of H, and since G is abelian, H is normal.

Thus p divides the order of the group G/H. By induction, we assume that G/H has an element gH of order p. Then $(gH)^p = g^p H = H$, so $g^p k^n = 1$ for some $k^n \in H$. Let h be the p^{th} root of k^n in H. Then $(gh)^p = 1$. Since $g \notin H$, $gh \neq 1$. Thus $\text{ord}(gh) = 1$. □

Date: November 27, 1995.

Theorem 1. Cauchy's Theorem
Let G be a finite group and let p be a prime integer.
Then $p \mid |G|$ if and only if G has an element of order p.

Proof.
($\Leftarrow$) If G has an element of order p, then it has a subgroup of order p, and the order of the subgroup divides the order of the group by LaGrange's Theorem.

($\Rightarrow$) Suppose that G is the smallest counter example; that is, suppose that G does not have an element of order p but that every group H with $|H| < |G|$ and $p \mid |H|$ has an element of order p.

For any subgroup $H < G$, if $p \mid |H|$, then H has an element of order p and so does G. Thus p does not divide the order of any proper subgroup of G.

Let G act on itself by conjugation. Then G acts transitively on the orbits of this action, which are the conjugacy classes in G. Since the orbits partition G, we have

$$|G| = \sum |\mathrm{orb}(g)| = \sum |g^G|,$$

where the sum is taken over a set of representatives of each class.

The points in the orbit correspond to the cosets of the stabilizer of a transitive action. The orbit of $g \in G$ is g^G and the stabilizer of g is $C_G(g)$. Thus we have a correspondence

$$g^G \leftrightarrow G/C_G(g);$$

that is, $|g^G| = |G/C_G(g)|$. Also, the points in the center of G are fixed by the action, so we have

$$|G| = |Z(G)| + \sum |G/C_G(g)|,$$

where the sum is taken over a set of representatives of conjugacy classes of noncentral elements.

If g is a noncentral element of G, then $C_G(g)$ is a proper subgroup, so p does not divide $|C_G(g)|$. Thus p divides $|G/C_G(g)|$, and so p divides $\sum |G/C_G(g)|$; since p also divides the order of G, p must divide $|Z(G)|$. Thus G has a nontrivial center. But since p divides the order of this center, it cannot be a proper subgroup. Thus $G = Z(G)$ and G is abelian. However, by Lemma 2, this implies that G has an element of order p. ☐

Department of Mathematics, University of California, Irvine
Email address: pbailey@math.uci.edu