CAUCHY'S THEOREM FOR ABELIAN GROUPS

MATH 457

We start with the following simple lemma:

Lemma 1. *If G has an element of order m, then for every divisor d of m, G has an element of order d.*

Proof. If $|g| = m$ and $d \mid m$, then

$$\left|g^{m/d}\right| = \frac{|g|}{(|g|\,, m/d)} = \frac{m}{(m, m/d)} = \frac{m}{m/d} = d.$$

$\square$

We will need the following for the proof of Cauchy's theorem.

Definition 2. Let $n \in \mathbb{Z}_{>1}$. By the *Fundamental Theorem of Arithmetic*, we can write $n = p_1^{e_1} \cdots p_k^{e_k}$, with p_i's *distinct* primes and $e_i \in \mathbb{Z}_{>0}$ in a *unique* way. Define then

$$P(n) \stackrel{\text{def}}{=} e_1 + \cdots + e_n.$$

In other words, $P(n)$ is the number of times n can be divided by [not necessarily distinct] primes.

Theorem 3 (Cauchy's Theorem for Abelian Groups)**.** *Let G be an Abelian group of order $1 < |G| = n < \infty$. Then, if p is a prime dividing n, we have that there is an element $g \in G$ of order p.*

Proof. [We will use *additive* notation!]

We prove it by induction on $P(|G|)$.

If $P(|G|) = 1$, then G has prime order, say p, and hence is cyclic, with a generator g of order p.

Now assume the statement is true for all groups G' with $P(|G'|) < P(n)$. Let $x \in G$, $x \neq 0$. If $p \mid |x|$, then we are done by the lemma above. So, suppose that $p \nmid m \stackrel{\text{def}}{=} |x|$. Since G is Abelian, we have that $H \stackrel{\text{def}}{=} \langle x \rangle \triangleleft G$. Now $P(|G/H|) < P(|G|)$

[as $|H| = m > 1$]. Moreover $p \mid |G/H| = |G| / |H|$, since $p \mid |G|$ but $p \nmid m = |H|$. Hence, by the induction hypothesis, there is $y + H \in G/H$ of order p [for some $y \in G$]. But then, $p = |y + H| \mid |y|$ [as we've seen in class], and we have an element of order p in G by the lemma.

$\square$

Note: This idea of doing an induction on $P(|G|)$ can be useful in many situations!

Corollary 4. *G is a finite p-group if and only if $|G| = p^r$ for some $r \in \mathbb{Z}_{\geq 0}$.*

Proof. [$\Rightarrow$:] If q is prime different from p such that $q \nmid |G|$, by the theorem G has an element of order q, and hence G cannot be a p-group.

[$\Leftarrow$:] This is a consequence of Lagrange's Theorem. $\square$