Math 317 C1 John Sullivan Spring 2003

Classification of Finite Abelian Groups

(Notes based on an article by Navarro in the Amer. Math. Monthly, February 2003.)

The fundamental theorem of finite abelian groups expresses any such group as a product of cyclic groups:

Theorem. *Suppose G is a finite abelian group. Then G is (in a unique way) a direct product of cyclic groups of order p^k with p prime.*

Our first step will be a special case of Cauchy's Theorem, which we will prove later for arbitrary groups: whenever $p \,||G|$ then G has an element of order p.

Theorem (Cauchy)**.** *If G is a finite group, and $p \,||G|$ is a prime, then G has an element of order p (or, equivalently, a subgroup of order p).*

Proof when G is abelian. First note that if $|G|$ is prime, then $G \cong \mathbb{Z}_p$ and we are done. In general, we work by induction. If G has no nontrivial proper subgroups, it must be a prime cyclic group, the case we've already handled. So we can suppose there is a nontrivial subgroup H smaller than G. Either $p \,||H|$ or $p \,||G/H|$. In the first case, by induction, H has an element of order p which is also order p in G so we're done. In the second case, if $g + H$ has order p in G/H then $|g + H| \,||g|$, so $\langle g \rangle \cong \mathbb{Z}_{kp}$ for some k, and then $kg \in G$ has order p. Note that we write our abelian groups additively. □

Definition. Given a prime p, a p-group is a group in which every element has order p^k for some k.

Corollary. *A finite group is a p-group if and only if its order is a power of p.*

Proof. If $|G| = p^n$ then by Lagrange's theorem, for any $g \in G$, its order divides p^n, and thus is a (smaller) power of p. Conversely, if $|G|$ is not a power of p, then it has some other prime divisor q, so by Cauchy's theorem, G has an element of order q and thus is not a p-group. □

We know that in a cyclic group, any subgroup is determined uniquely by its order. Our first lemma proves a partial converse for p-groups.

Lemma. *If G is a finite abelian p-group and G has a unique subgroup H of order p, then G is cyclic.*

Proof. Again we proceed by induction on $|G|$, noting that the case $|G| = p$ is obvious. Define $\phi : G \to G$ by $\phi(g) = pg$, and let $K = \ker(\phi)$, which consists exactly of those elements of order p (or 1). We find that $H \leq K$, so K is nontrivial. But for any nontrivial $g \in K$, the cyclic group $\langle g \rangle$ has order p, and thus must be H. Thus we see $K = H$. If $K = G$, then $G \cong \mathbb{Z}_p$ is cyclic and we are done. Otherwise, $\phi(G)$ is a nontrivial proper subgroup of G, isomorphic to G/K. By Cauchy's theorem, $\phi(G)$ has a subgroup of order p. Since any such subgroup is also a subgroup of G, there is a unique one (namely $H = K$). Thus we can apply the inductive hypothesis to the group $\phi(G) \cong G/K$, and we conclude that this group is cyclic. If we write G/K as $\langle g + K \rangle$ for some $g \neq e$, we claim that g generates G. To check this, it suffices to prove that $K \leq \langle g \rangle$. But by Cauchy, $\langle g \rangle \leq G$ has a subgroup of order p, which by uniqueness must be K. □

Combining this lemma with Cauchy's theorem, we see that a noncyclic finite abelian p-group has more than one subgroup of order p, which is the key to the next lemma.

Lemma. *If G is a finite abelian p-group and C is a cyclic subgroup of maximal order, then $G = C \oplus H$ for some subgroup H.*

Proof. Again, we proceed by induction on $|G|$, noting that when G is cyclic, $C = G$ and $H = \{e\}$. When G is not cyclic, we have just shown it has more than one subgroup of order p, while the cyclic group C has a unique such subgroup. So let $K \leq G$ be a subgroup of order p not contained in C. Because K has prime order, $K \cap C = \{e\}$, which implies $(C + K)/K \cong C$.

Given any $g \in G$, the order of $g + K$ in G/K divides $|g|$, which is at most $|C|$. Thus the cyclic subgroup $(C+K)/K \cong C$ has maximal order in G/K, and we can apply the inductive hypothesis to prove that $G/K = (C+K)/K \oplus H'$ for some $H' \leq G/K$. The preimage of H' under the map $G \to G/K$ is a group H with $K \leq H \leq G$. But $G/K = (C+K)/K \oplus H/K$ means that $G = (C + K) + H = C + (K + H) = C + H$. Since $H \cap (C + K) = K$, we have $H \cap C = \{e\}$, so by definition $G = C \oplus H$. □

Theorem. *Any finite abelian group is a direct sum of cyclic subgroups of prime-power order.*

Proof. For any prime p dividing $|G|$, we set $G_p := \{g : |g| = p^k\}$ and $G_{p'} := \{g : p \nmid |g|\}$. Then by Cauchy's theorem, G_p is nontrivial and is a p-group. Now if $g \in G$ has order $p^k m$ (with $p \not| m$), then $p^k g \in G_{p'}$ and $mg \in G_p$. Since p^k and m are relatively prime, there are r and s with $rp^k + sm = 1$, so we can write $g = r(p^k g) + s(mg)$ as a sum of elements in $G_{p'}$ and G_p. This shows that $G = G_p \oplus G_{p'}$.

Repeating this process for the remaining primes dividing the order of $G_{p'}$ we can decompose G as a direct sum of p-groups for different p. So it suffices to prove the theorem for p-groups like G_p, which have order p^k. We do this by induction on k.

Let C be a cyclic subgroup of G_p of maximal order. By the last lemma, $G = C \oplus H$ with $|H| < |G|$. By the inductive hypothesis, H is a direct sum of cyclic subgroups, and we are done. □

We note that the decomposition of G given in the theorem is unique. Certainly, the subgroup G_p is uniquely defined for any p. Now suppose a p-group G_p has been expressed as a product of cyclic groups in two ways: as $H_1 \times \cdots \times H_m$ and as $K_1 \times \cdots \times K_n$, with $|H_i| \geq |H_j|$ and $|K_i| \geq |K_j|$ when $i < j$. Then $|H_1| = |K_1|$ since each of these must equal the maximal order of an element of G_p. Proceeding by induction, we find that the two decompositions are really the same.

However, we should note, for instance, that although $G = \mathbb{Z}_p \times \mathbb{Z}_p$ has no other expression as a product of cyclic groups, there are many pairs of subgroups H and K of order p for which $G = H \oplus K$. In this example, for any nonzero elements a and b, we have $G = \langle a \rangle \oplus \langle b \rangle$ unless a is a multiple of b.