Fundamental theorem of finite abelian groups

Thm. Every finite abelian group is isomorphic to a direct of the form

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}},$$

where $p_1, \ldots, p_n$ are not-nec.-distinct primes.

Ex. If G is abelian and $|G| = 120$, then G is isomorphic to one of:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_8 \times \mathbb{Z}_{15}$$

$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \leftrightarrow \gcd(m,n) = 1$

Only applies when G is abelian! $|S_5| = 120$, but S_5 is not isomorphic to any of these.

Two steps to our proof:

1. decompose G as an internal direct product of subgroups with prime-power order;
2. decompose these pieces as internal direct products of cyclic subgroups.

Def. A **p-group**, for any prime p, is a group in which every element has order equal to some power of p.

Exercise. A finite group G is a p-group iff $|G| = p^n$, for some $n \geq 0$.

Here's a partial converse to the fact that

$$g \in G \Rightarrow |g| \mid |G| :$$

Thm (Cauchy) If G is a finite group and p is a prime which divides $|G|$, then G has an elt. of order p.

Exercise. Let $N \leq G$ be a normal subgroup and take $g \in G$ with finite order $|g|$. Then the order of gN in G/N divides $|g|$.

(Proof of Cauchy's theorem in abelian case.)

Induction on $|G|$.

Base case: $|G| = p \Rightarrow G \cong \mathbb{Z}_p \Rightarrow$ every non-id. elt has order p.

Notice that if G has no nontrivial, proper subgroups, then any non-identity elt of G generates G. So G is cyclic. The only cyclic groups with no nontrivial,

proper subgroups are those of the form $\mathbb{Z}_p$. So we're back in the base case.

Inductive step: $|G| > p \Rightarrow \exists$ non-trivial, proper subgroup $H \leq G$.

$|G| = |H| \cdot [G:H] \Rightarrow p \mid |H|$ or $p \mid [G:H]$

If $p \mid |H|$, then the inductive hypothesis gives us $h \in H$ with order p. The order of h in G is thus p.

If $p \nmid |H|$, $p \mid [G:H] = |G/H|$. (G abelian $\Rightarrow H \leq G$ is normal)

So G/H is a group with order divisible by p and smaller than $|G|$.

Inductive hypothesis: $gH \in G/H$ s.t.

order of gH in G/H is p.

By exercise, $|g| = kp$, for some k.

So $g^k \in G$ has order p. ▨

When is a p-group cyclic?

Lemma ① If G is a finite abelian p-group with a unique subgroup H of order p, then G is cyclic.

(Proof.) Again, induction on $|G|$.

Consider $\phi : G \longrightarrow G$ Note that $H \leq \ker \phi$.
$g \mapsto g^p$

Conversely, $\ker \phi$ has order p, so in fact $H = \ker \phi$.

If $\ker \phi = G$, then $|G| = p$, so $G \cong \mathbb{Z}_p$ and we're finished.
This is our base case. For induction, suppose that
$H = \ker \phi$ is a proper subgroup, and that the result
holds for order less than $|G|$.

Consider $\phi(G) \leq G$. G a p-group $\Rightarrow \phi(G)$ a p-group.
Cauchy: $\phi(G)$ contains a subgroup of order p.

By the uniqueness of H, $H \leq \phi(G)$ is the unique subgroup of $\phi(G)$ of order p. So the inductive hypothesis applies to $\phi(G)$. i.e., $\phi(G)$ is cyclic.

First iso. thm: $\phi(G) \cong G/\ker \phi$.

So $G/\ker \phi$ is cyclic.

Exercise: If $g \ker \phi$ generates $G/\ker \phi$, then
g generates G. ∎

Example. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a p-group, but not cyclic.

Two subgroups of order 2: $\mathbb{Z}_2 \times \{0\}$; $\{0\} \times \mathbb{Z}_2$.

Prop ② If G is a finite abelian p-group and $C \leq G$ is a cyclic subgroup of maximal order, then G is the internal direct product CH, for some subgroup $H \leq G$.

(Proof.) Again, induction on $|G|$.

If G is cyclic, then $C = G$ and we can take $H = \{e\}$.

If G is not cyclic, statement holds for smaller p-groups.

Lemma ①: $\exists$ more than 1 subgroup of G of order p.

OTOH, $C \leq G$ contains a unique subgroup of order p.

So G has a subgroup K with $|K| = p$ and $K \not\subseteq C$.

Check: $K \cap C = \{e\}$.

Second isom. theorem: $CK/K \cong C/(C \cap K) \cong C$.

$\forall\, g \in G$, $|g| \leq |C|$. Otherwise, $\langle g \rangle$ would be a cyclic subgroup of order $> |C|$.

The order of gK in G/K divides $|g|$, and $\therefore$ is also $\leq |C|$.

So G/K has no cyclic subgroups of order $> |C|$.

$\therefore$ $CK/K \leq G/K$ is a cyclic subgroup of maximal order.

By inductive hypothesis,

$$G/K = (CK/K)\,H',$$

for some $H' \leq G/K$ with $H' \cap (CK/K) = \{K\}$.

By correspondence theorem, $\exists\, H \leq G$ s.t.
H contains K and $H' = H/K \leq G/K$.

So in fact

$$G/K = (CK/K)(H/K),$$

and thus $G = (CK)H = CH$.
↑ b/c $K \leq H$.

Check: $C \cap H = \{e\}$.

So G is the internal direct product CH. ∎