Day 13 June 18, 2024

Thm [The fundamental theorem of finite abelian groups]
Every finite abelian group is isomorphic to a direct product 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-necessarily-distinct primes.

Ex. There are exactly three abelian groups of order $120 = 2^3 \cdot 3 \cdot 5$, up to isomorphism:

$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \quad \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \; \& \; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

Note: $|S_5| = 120$, but S_5 is $\not\cong$ to any of these.

Proof strategy:
1. decompose a finite abelian group as an internal direct product of p-groups;
2. decompose a p-group as an internal direct product of cyclic groups.

Def We call G a p-group if every element of G has order equal to a power of p. (p prime)

Exercise. G is a p-group iff $|G|$ is a power of p.

Exercise. Let $N \trianglelefteq G$ and pick $g \in G$ with $|g| < \infty$. Then the order of gN in G/N divides $|g|$.

Thm. [Cauchy's theorem] If p is a prime which divides the order of G, then $\exists\, g \in G$ s.t. $|g| = p$.

(Proof for G abelian.)

First, $\mathbb{S}$ G has no nontrivial, proper subgroups. Pick $g \neq e$ in G and note that $\langle g \rangle = G$. So G is cyclic. But the only cyclic groups with no nontrivial, proper subgroups are those of prime order, so $|g| = |G| = p$ and we're finished.

Now we use induction on $|G|$.

Base case: $|G| = p \Rightarrow G \cong \mathbb{Z}_p \Rightarrow \exists\, g \in G$ s.t. $|g| = p$ ✓

Inductive step: $\mathbb{S}$ $H \leq G$ is a nontrivial, proper subgroup. (If none, see above.)

Recall: $|G| = |H| \cdot [G:H]$

$$p \mid |G| \Rightarrow p \mid |H| \text{ or } p \mid [G:H]$$

If $p \mid |H|$, then $\exists\, h \in H$ s.t. $|h| = p$ by inductive hypothesis (b/c $|H| < |G|$).

G abelian $\Rightarrow H \trianglelefteq G$

If $p \nmid |H|$, then $p \mid [G:H] = |G/H|$.

Since $H \neq \{e\}$, $|G/H| < |G|$.

Inductive hypothesis $\Rightarrow \exists\, gH \in G/H$ s.t. $|gH| = p$.

By exercise, $|g| = kp$. So $|g^k| = p$. ∎

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

(Proof.) Consider the homom. $\phi : G \to G$, $g \mapsto g^p$

and let $K = \ker \phi$. Note: $k \in K \Rightarrow k^p = e$
$\Rightarrow |k| = 1$ or $|k| = p$.
$\therefore \forall k \in K$ s.t. $k \neq e$, $K = \langle k \rangle$.

So $|K| = p \Rightarrow K = H$.

If $K = G$, then $G = K = H$ has order p, so $G \cong \mathbb{Z}_p$ and we're finished.

Inductive step: Assume the result holds for groups of order less than $|G|$.

We now know K to be a proper subgroup of G.

Consider $\phi(G) \leq G$. Note that $|\phi(G)| \mid |G| \Rightarrow \phi(G)$ a p-group.

By Cauchy's theorem, $\exists\, g \in \phi(G)$ s.t. $|g| = p$.

By uniqueness of H, $\langle g \rangle = H$.

So $\phi(G)$ is a proper subgroup of G with a unique subgroup of order p. By inductive hyp., $\phi(G)$ is cyclic.

OTOH, $\phi(G) \cong G/\ker\phi = G/K$.

So G/K is cyclic. Pick a generator gK and consider $\langle g \rangle \subseteq G$.

Cauchy: $\langle g \rangle$ contains a subgroup of order p. Must be H.

Given any $g_0 \in G$, $\exists\, k \geq 0$ s.t. $g^k K = g_0 K$, since gK generates G/K.

But $K = H$ is contained in $\langle g \rangle$.
So $g^k K = g_0 K \Rightarrow g^{-k} g_0 \in K \leq \langle g \rangle$

$$\therefore g_0 \in \langle g \rangle.$$

$$\text{So } \langle g \rangle = G. \qquad \blacksquare$$

<u>Prop.</u> 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 $H \leq G$.

Next time.

<u>Prop.</u> Any finite abelian group is an internal direct product of cyclic subgroups of prime-power order.

(Proof.) Given a prime p s.t. $p \mid |G|$, let

$$G_p := \{g \in G \mid |g| = p^k\} \text{ \& } G_{p'} = \{g \in G \mid p \nmid |g|\}.$$

Cauchy: $G_p \neq \{e\}$. Also, G_p is a p-group.

Claim: G is the internal direct product $G_p G_{p'}$.

Note that $G_p \cap G_{p'} = \{e\}$, so $G_p G_{p'}$ is well-defined.

Now pick $g \in G$ and write $|g| = p^k m$, with $\gcd(p^k, m) = 1$. Then $g^m \in G_p$ and $g^{p^k} \in G_{p'}$.

$\gcd(p^k, m) = 1 \Rightarrow \exists\, r, s \in \mathbb{Z}$ s.t. $rm + sp^k = 1$.

So

$$g = g^1 = g^{rm + sp^k} = g^{rm} g^{sp^k} = (g^m)^r (g^{p^k})^s \in G_p G_{p'}.$$

So $G = G_p G_{p'}$. Repeat until we've written G as an internal direct product of p-groups.

Next time: decompose these p-groups into cyclic groups.