date: monday, january 15, 2024

Fundamental Theorem of Finite Abelian Groups

Recall: Our goal is to describe all finite abelian groups of order n.

Direct Products-Review

Two types: internal and external direct products

Def^{n}: Let G and H be groups. The external direct product of G and H is the group,

$$G\times H=\{(g,h)\mid g\in G,\ h\in H\}$$

where

$$\underbrace{(g_1,h_1)*(g_2,h_2)}_{*\text{ operation in } G\times H}=(\underbrace{g_1\circ g_2}_{\text{operation in } G},\underbrace{h_1\circ h_2}_{\text{operation in } H})$$

Def^{n}: Let G be a group with subgroups H and K such that

- $G=HK=\{hk\mid h\in H,\ k\in K\}$
- $H\cap K=\{e\}$
- $kh=hk$ for all $h\in H$, $k\in K$

Then G is the internal direct product of H and K.

Theorem: Suppose G is an internal direct product of H and K. Then $G\cong H\times K$.

Extension: Let G be a group with subgroup $H_1,\dots,H_n$ such that

- $G=H_1\cdots H_n=\{h_1h_2\cdots h_n\mid h_i\in H_i\}$
- $H_i\cap(\bigcup_{i\neq j}H_j)=\{e\}$
- $h_ih_j=h_jh_i$ for all $i\neq j$, $h_i\in H_i$, $h_j\in H_j$

Then G is the internal direct product of $H_1,\dots,H_n$ and $G\cong H_1\times\cdots\times H_n$.

Main Result (Fundamental Theorem of Finite Abelian Groups)
Every finite abelian group G is isomorphic to a direct product of cyclic groups of prime power orders, ie.

$$G \simeq \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_s^{a_s}} \quad \leftarrow \text{the } p\text{'s may not be distinct}$$

eg. $n = 20 = 2^2 \cdot 5$
$20 = 2^2 \cdot 5^1 \longleftrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_5$
$= 2^1 \cdot 2^1 \cdot 5^1 \longleftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$

Need partial converse of Lagrange.

Lemma: Let G be an abelian group and p a prime such that $p \mid |G|$. Then G has a subgroup of order p.

<u>Proof</u>
Do induction on $|G| = n$. If $|G| = 2$, then $G \simeq \mathbb{Z}_2$, and so result holds.
Let $|G| = n > 2$ and $e \neq g \in G$. So $|g| = qt$ for some prime q. Then $|g^t| = q$. If $q = p$, we are done! If $q \neq p$, let $N = \langle g^t \rangle \in G$. Then since G is abelian, N is normal, so G/N is a group. And

$$|G/N| = |G|/|N| = n/q$$

Now $p \mid (n/q)$ since $\gcd(p,q) = 1$. So G/N is a group where $p \mid |G/N|$ and $|G/N| < n$. By induction, G/N has an element of order p. Say $aN \in G/N$. So $(aN)^p = eN \iff a^p \in N$. Since $|N| = q$, $(a^p)^q = a^{pq} = e$. So $|a| \mid pq$. So $|a| = 1, p, q, pq$. We have $|a| \neq 1$ since $a \neq e$. If $|a| = p$, we are done. If $|a| = pq$, then $|a^q| = p$ (done). If $|a| = q$, then $(aN)^q = eN$. Since $|aN| = p$, this means $p \mid q$. But $\gcd(p,q) = 1$. So this case doesn't happen.

$\square$

Def^n: A group G is a p-group if every element of G has order a power of prime p.

eg. $\mathbb{Z}_4$ is a 2-group since $|0| = 1 = 2^0$, $|1| = 2^2$, $|2| = 2^1$, $|3| = 2^2$

eg. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a 2-group since $|(0,0)| = 2^0$, $|(1,0)| = 2^1$, $|(0,1)| = 2^1$, $|(1,1)| = 2^1$

Lemma: G is a p-group $\Leftrightarrow |G| = p^{\alpha}$ for some α

Proof

"$\Leftarrow$" Let $a \in G$. Then $|a| \mid |G| = p^{\alpha}$. So $|a| = p^{t}$.

"$\Rightarrow$" Suppose G is a p-group, but some $q \neq p$ has the property $q \mid |G|$. By the lemma, G has an element of order q. But then G is not a p-group. So no such q exists.

$\square$

Technical Lemma 1: Suppose G is a finite abelian group with $|G| = p_1^{a_1} \cdots p_r^{a_r}$ (unique factorization). For each p_i, set $G_i = \{ g \in G \mid |g| = p_i^{t} \text{ for some } t \}$. Then G is the internal direct product of $G_1, \dots, G_r$ (and each G_i a p_i-group).

Technical Lemma 2: Let G be a finite abelian p-group. Let $g \in G$ with maximal order (ie. $|g| = p^m$ and $|h| = p^n$ with $n \le m$ for all other $h \in G$). Then $G \simeq \langle g \rangle \times H \simeq \mathbb{Z}_{p^m} \times H$ with H a p-group.

Proof of the FTFAG

By technical lemma 1, $G \simeq G_1 \times G_2 \times \cdots \times G_r$ with each G_i a p-group. By technical lemma 2, we claim that for any p-group H, $H \simeq \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_s}}$ (all same prime p).

Do induction on $|H|$. If $|H| = 2$, then $H \simeq \mathbb{Z}_2$. If $|H| > 2$, take $g \in H$ with g having max order, say $|g| = p^{\ell}$. By technical lemma 2,

$$H \simeq \mathbb{Z}_{p^{\ell}} \times K \quad \text{with } |K| < |H|$$

and K a p-group. By induction applied to K, $H \simeq \mathbb{Z}_{p^{\ell}} \times \mathbb{Z}_{p^{b_1}} \times \cdots \times \mathbb{Z}_{p^{b_s}}$.

Consequently,

$$\begin{aligned} G &\simeq G_1 \times G_2 \cdots \times G_r \\ &(\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_1^{a_s}}) \times (\mathbb{Z}_{p_2^{b_1}} \times \cdots \mathbb{Z}_{p_2^{b_r}}) \times \cdots \end{aligned}$$