date: thursday, january 11, 2024

Fundamental Theorem of Finite Abelian Groups I

Motivating Question: How many "distinct" groups are there of order $n \geq 1$?

eg. $\mathcal{U}(8) = \{a \mid \gcd(a,8) = 1,\ a = \{0,\dots,7\}\}$
$= \{1, 3, 5, 7\}$ <-multiplicative group

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$

These groups are <u>not</u> "distinct"

$\mathcal{U}(8)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_2 \times \mathbb{Z}_2$	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

Same group if we identify:
$1 \longleftrightarrow (0,0)$
$3 \longleftrightarrow (1,0)$
$5 \longleftrightarrow (0,1)$
$7 \longleftrightarrow (1,1)$

Homomorphisms/Isomorphisms

Def^n: Let G and H be groups. Then a group homomorphism is a function $f: G \to H$ such that

$$f(a * b) = f(a) \circ f(b)$$

group operation in G   group operation in H

Properties of Homomorphisms:
Let $f: G \to H$ be a homomorphism. Then,

① $f(e_G) = e_H$
② $f(a^{-1}) = f(a)^{-1}$
③ If $G_1 \subseteq G$ is a subgroup, then $f(G_1) = \{f(g) \mid g \in G_1\} \subseteq H$ is a subgroup

④ If $H_1 \subseteq H$ is a subgroup, then $f^{-1}(H_1) = \{g \in G \mid f(g) \in H_1\}$ is a subgroup of G.

Def$^{\underline{n}}$: $\ker f = \{g \in G \mid f(g) = e_H\}$ <- kernel, $\operatorname{Im} f = \{f(g) \mid g \in G\} \subseteq H$ <- image

Facts ① $\ker f$ is a normal subgroup of G
② $\ker f = \{e_G\}$ iff f is injective
③ $\operatorname{Im} f$ is a subgroup of H

Def$^{\underline{n}}$: A homomorphism is an isomorphism if $f: G \to H$ is both injective and surjective. We say G and H are isomorphic and write $G \simeq H$.

eg. $\mathcal{U}(8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
Our motivating question <=> "distinct" means nonisomorphic

eg. $\mathbb{Z}_4 \not\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
The group $\mathbb{Z}_4$ has an element of order 4 and $\mathbb{Z}_2 \times \mathbb{Z}_2$ does not.

First Isomorphism Theorem: Let $f: G \to H$ be a group homomorphism. Then $G/\ker f \simeq \operatorname{Im} f \subseteq H$.

Fundamental Theorem of Finite Abelian Groups

Refined Motivating Question: For each integer $n \in \mathbb{N}$, list all groups G with $|G| = n$ such that any group of order n is isomorphic to one group in the list.

eg. Suppose p is prime. If $|G| = p$, then $G \simeq \mathbb{Z}_p$.

Proof
From first lecture, if $|G| = p$, then G is cyclic. So $G = \{a^0, a^1, \dots, a^{p-1}\}$. Define a map $\phi: G \to \mathbb{Z}_p$ by $\phi(a^i) = i$. This is clearly a bijection. It is also a homomorphism since if $i + j = k \bmod p$,

$$\phi(a^i a^j) = \phi(a^k) = k = i + j = \phi(a^i) + \phi(a^j).$$

$\square$

Corollary: Only one distinct group of order p.

Other small n:

n	all nonisomorphic groups
1	$\{0\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_2 \times \mathbb{Z}_3, S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_8, D_4, Q_8, \mathbb{Z}_4 \times \mathbb{Z}_2$

$\uparrow$ quaternions

eg. If G is cyclic and $|G| = n$, then $G \simeq \mathbb{Z}_n$.

Theorem: If $\gcd(m,n) = 1$, then $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. (iff)

eg. $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$

eg. $\mathbb{Z}_{12} \simeq \mathbb{Z}_{2^2} \times \mathbb{Z}_3$

Need $\gcd(m,n) = 1$

eg. $\gcd(2,2) \neq 1$ so $\mathbb{Z}_{2 \cdot 2} \not\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

Fundamental Theorem of Finite Abelian Groups: Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power orders, ie. of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}} \quad \leftarrow \text{p's may not be distinct}$$

We can answer our motivating question for abelian groups.

eg. Write out all non-isomorphic abelian groups of order 100.

$100 = 2^2 \cdot 5^2$ <- determine all ways to write 100 as a product of prime powers

$$100 = 2^2 \cdot 5^2 \longleftrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2}$$
$$= 2^1 \cdot 2^1 \cdot 5^2 \longleftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2}$$
$$= 2^1 \cdot 2^1 \cdot 5^1 \cdot 5^1 \longleftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$= 2^2 \cdot 5^1 \cdot 5^1 \longleftrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

Corollary: If n is squarefree, ie. $n = p_1^1 p_2^1 \cdots p_r^1$, then only one abelian group of order n, ie. $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$.

eg. $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$ is only abelian group of order 15