Plan for today

- finitely generated abelian groups
- cosets
- normal subgroups

Recap: $\mathbb{Z}$, $\mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}$

Theorem (Structure Theorem for FGAG - prime divisor version)

If G is FGAG, then

$$G \cong \mathbb{Z}_{p_1^{m_1}} \oplus \mathbb{Z}_{p_2^{m_2}} \oplus \dots \oplus \mathbb{Z}_{p_r^{m_r}} \oplus \mathbb{Z}^s$$

The summands are unique (up to reordering).

Ex: $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2$$

Ex: Find all the abelian groups of order 1000.

$1000 = 10 \cdot 10 \cdot 10 = 2^3 5^3$

$2\,2^2\,5^3$ $\quad$ $2\,2\,2\,5^3$ $\quad$ $2^3\,5\,5^2$ $\quad$ $2^3\,5\,5\,5$

$2\,2^2\,5\,5^2$ $\quad$ $2\,2^2\,5\,5\,5$ $\quad$ $2\,2\,2\,5\,5^2$ $\quad$ $2\,2\,2\,5\,5\,5$

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{5^3}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{5^3}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{5^3}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{5^2}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, ...

Theorem (Structure Theorem for FGAG - invariant factor version)

If G is a finitely generated abelian group. Then

$$G \cong \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \dots \oplus \mathbb{Z}_{a_m} \oplus \mathbb{Z}^s$$

where here $a_j \mid a_{j+1}$ for $1 \leq j < m$.

THIS REPRESENTATION IS UNIQUE.

Ex: Abelian Groups of order 100 (up to isomorphism)

$100 = 2^2 \cdot 5^2$

- $\mathbb{Z}_{100}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_{50}$
- $\mathbb{Z}_5 \oplus \mathbb{Z}_{20}$
- $\mathbb{Z}_{10} \oplus \mathbb{Z}_{10}$

- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{5^2}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{5^2}$
- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Theorem: $\mathbb{Z}_a \oplus \mathbb{Z}_b \cong \mathbb{Z}_{ab} \iff a, b$ relatively prime.

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{50} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{5^2}$$

Proof:

2, 25 relatively prime! $\mathbb{Z}_2 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_{50}$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{50} \cong \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_{25}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$$

Ex: Put the group $\mathbb{Z}_{14} \oplus \mathbb{Z}_{28}$ in prime divisor form.

$$\mathbb{Z}_{14} \oplus \mathbb{Z}_{28} \cong \mathbb{Z}_7 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{28} \cong \mathbb{Z}_7 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_4$$
$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$$

Put into invariant factor form Haha, jk.

$$\underline{\mathbb{Z}_2 \oplus \mathbb{Z}_{14}} \oplus \mathbb{Z}_{14} \not\cong \mathbb{Z}_{14} \oplus \underline{\mathbb{Z}_{28}}$$

Cosets

Let H be a subgroup of G.

Def: The left coset of $a \in G$ with respect to H is
$aH = \{ah \mid h \in H\}$

The right coset of $a \in G$ is
$Ha = \{ha \mid h \in H\}$

Notation: if G is abelian, w/ group operation $+$ we write $a+H$ instead of aH.
$a+H = \{a+h \mid h \in H\}$.

Ex: $G = \mathbb{Z}$, $H = 5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

Then

✓ $0+H = \{0+h \mid h \in H\} = \boxed{\{\ldots, -10, -5, 0, 5, 10, \ldots\}}$

✓ $1+H = \{1+h \mid h \in H\} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$

✓ $2+H = \{2+h \mid h \in H\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$

✓ $4+H = \{4+h \mid h \in H\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

$5+H = \{5+h \mid h \in H\} = \boxed{\{\ldots, -5, 0, 5, 10, 15, \ldots\}}$

$11+H = \{11+h \mid h \in H\} = \{\ldots, 1, 6, 11, 16, 21, \ldots\}$

$5+H = 0+H$. $\quad j+H = k+H \iff j \equiv k \mod 5.$

✓ $3+H = \{3+h \mid h \in H\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$

Theorem: Let $H < G$. The relations

- $a \sim_L b \Leftrightarrow a^{-1}b \in H$

- $a \sim_R b \Leftrightarrow ba^{-1} \in H$

are equivalence relations on G.

The equivalence classes are the left and right cosets of H in G, respectively

Ex: G = group of symmetries of the square.

$$G = \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}, S_0, S_{\pi/2}, S_\pi, S_{3\pi/2}\}$$

$$S_0^2 = R_0 \quad \text{so} \qquad H = \{R_0, S_0\} \leq G.$$

Left cosets of H in G are	Right cosets of H in G are
$R_0H = \{R_0, S_0\}$	$HR_0 = \{R_0, S_0\}$
$R_{\pi/2}H = \{R_{\pi/2}, S_{3\pi/2}\}$	$HR_{\pi/2} = \{R_{\pi/2}, S_{\pi/2}\}$
$R_\pi H = \{R_\pi, S_\pi\}$	$HR_\pi = \{R_\pi, S_\pi\}$
$R_{3\pi/2}H = \{R_{3\pi/2}, S_{\pi/2}\}$	$HR_{3\pi/2} = \{R_{3\pi/2}, S_{3\pi/2}\}$

Def: The <u>index</u> of H in G is the number of (left) cosets of H in G.

Notation: the index of H in G is denoted $[G:H]$.

Theorem (Lagrange's Theorem): Let $H < G$. Then

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

<u>Corollary</u>: Suppose $|G| = p$ with $p > 1$ prime. Then G is cyclic.

<u>Proof</u>: Choose $g \in G$ w/ $g \neq e$.
Then $\langle g \rangle \leq G$.
By Lagrange's theorem $|\langle g \rangle|$ divides $|G| = p$.
So $|\langle g \rangle| = \cancel{1}$ or p. so $|\langle g \rangle| = p = |G|$.

So $\langle g \rangle = G$. $\therefore$ G cyclic

$\square$

<u>Proof of Lagrange's Theorem</u>:

<u>Claim</u>: If $a \in G$, then $|aH| = |H|$.

<u>Proof</u>: Let $f : aH \to H$, $x \mapsto a^{-1}x$; $g : H \to aH$, $y \mapsto ay$.
f and g are inverse functions! $\therefore$ f bijection
so $|aH| = |H|$.

Choose $a_1, a_2, \ldots, a_r \in H$ so that $\{a_1H, a_2H, \ldots, a_rH\}$ are all the left cosets of H.
This is a partition so

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|$$

$$|G| = r|H| \qquad r = [G:H].$$

$\square$

$$\{1, 2, 3, \dots, n\}$$

$$(a_k a_{k+1} \cdots a_n)(a_{k-1} a_n) = (a_{k-1} a_k a_{k+1} \cdots a_n)$$

$$(a_k a_{k+1} a_{k+2} \cdots a_n)(a_{k-1} a_n) : \quad \begin{aligned} a_k &\mapsto a_k \mapsto a_{k+1} \\ a_{k+1} &\mapsto a_{k+1} \mapsto a_{k+2} \\ &\vdots \\ a_{k-1} &\mapsto a_n \mapsto a_k \\ a_n &\mapsto a_{k-1} \mapsto a_{k-1} \end{aligned}$$

$$(a_{k-1} a_k a_{k+1} \cdots a_n) : \quad \begin{aligned} a_k &\mapsto a_{k+1} \\ a_{k+1} &\mapsto a_{k+2} \\ &\vdots \\ a_{k-1} &\mapsto a_k \\ a_n &\mapsto a_{k-1} \end{aligned}$$

$$(a_{k-1} a_k a_{k+1} \cdots a_n) = (a_k a_{k+1} \cdots a_n)(a_{k-1} a_n).$$

$$\begin{aligned} (a_1 a_2 a_3 a_4 \cdots a_n) &= (a_2 a_3 a_4 a_5 \cdots a_n)(a_1 a_n) \\ &= (a_3 a_4 a_5 \cdots a_n)(a_2 a_n)(a_1 a_n) \\ &= (a_{n-1} a_n)(a_{n-2} a_n)(a_{n-3} a_n) \cdots (a_2 a_n)(a_1 a_n) \end{aligned}$$

- $\{66, 12, 11, 9, 7, 4, 3, 2, 1, 0\}$

$\uparrow$

- $\{1, 3, 2, 7, 9, 4, 12, 11, 0, 66\} \longrightarrow \{0, 1, 2, 3, 4, 7, 9, 11, 12, 66\}$.
- $\{1, 2, 3, 9, 11, 0, 66, 5, 12\} \longrightarrow \{0, 1, 2, 3, 5, 9, 11, 12, 66\}$.

$\downarrow$

- $\{66, 12, 11, 9, 5, 3, 2, 1, 0\}$

- $\mathbb{Z}_{32} \oplus \mathbb{Z}_{14} \oplus \mathbb{Z}_{6} \rightsquigarrow \mathbb{Z}_{32} \oplus \mathbb{Z}_{14} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{3}$

$$\rightsquigarrow \underbrace{\mathbb{Z}_{32} \oplus \mathbb{Z}_{7}} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{3}$$

$$\mathbb{Z}_{7\cdot 2^5} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{3}$$

$$\mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{7\cdot 2^5\cdot 3}$$

a, b relatively prime
means
if $r | a$ and $r | b \Rightarrow r = 1$

- $\mathbb{Z}_{96} \oplus \mathbb{Z}_{7} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2}$

$$\mathbb{Z}_{2^5\cdot 3\cdot 7} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2}$$

$$\mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2^5\cdot 3\cdot 7}$$

$\mathbb{Z}_{a} \oplus \mathbb{Z}_{b} \oplus \mathbb{Z}_{c} \oplus \dots$

$a | b$
$b | c$
$\vdots$