11/19
Tuesday

Def: A group G is called **simple** if the only normal subgroups are G and $\{1\}$.

Ex: $\mathbb{Z}_p$ where p is prime is simple.

pf: Let $H \leq \mathbb{Z}_p$.
Then by Lagrange $|H|$ divides $|\mathbb{Z}_p| = p$.
So, $|H| = 1$ or $|H| = p$.
Thus, $H = \{1\}$ or $H = \mathbb{Z}_p$. ∎

Ex
H=
H≤
H≠

Ex: Z
if

Hint:
n w
Let

Ex: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ is not simple.

$H = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}$

$H \trianglelefteq \mathbb{Z}_4$ since $\mathbb{Z}_4$ is abelian.

$H \neq \{\bar{0}\}$ and $H \neq \mathbb{Z}_4$.

Ex: $\mathbb{Z}_n$ is not simple if $n \geq 2$ and not prime.

Hint: Pick a divisor a of n with $a \neq 1$ and $a \neq n$.
Let $H = \langle \bar{a} \rangle$.

Fact: Let G be a group and $H \leq G$. If $|G/H| = 2$, then $H \trianglelefteq G$.

Ex: $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ is not simple.

Let $H = \langle r \rangle = \{1, r, r^2, \ldots, r^{n-1}\}$

Then $H \trianglelefteq D_{2n}$.

Check:

left cosets

$H = \{1, r, r^2, \ldots, r^{n-1}\}$

$sH = \{s, sr, sr^2, \ldots, sr^{n-1}\}$

right cosets

$H = \{1, r, r^2, \ldots, r^{n-1}\}$

$Hs = \{s, rs, r^2s, \ldots, r^{n-1}s\}$

$= \{s, sr^{-1}, sr^{-2}, \ldots, sr^{-(n-1)}\}$

$= \{s, sr^{n-1}, sr^{n-2}, \ldots, sr\} = sH$

Ex: S_n is not simple.

$A_n \trianglelefteq S_n$ (since $|A_n| = \frac{|S_n|}{2}$ so there are only two cosets)

Fact: The only non-abelian simple group of order less than 100 is A_5.

Note $|A_5| = \frac{|S_5|}{2} = \frac{5!}{2} = 60$.

Ex: $S_3 = \{\lambda, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

$A_3 = \{\lambda, (1,2,3), (1,3,2)\} = \langle (1,2,3) \rangle$

A_3 is cyclic.

Theorem (Fundamental theorem of finitely-generated Abelian groups)

Herstein
Abstract Algebra

Let G be a finitely-generated abelian group.
Then

① $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$

for some $r, n_1, n_2, \ldots, n_s$ are integers with
(a) $r \geq 0$ and $n_i \geq 2$
(b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.

② The expression in ① is unique. That is, if $G = \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_u}$ where t and m_i satisfy (a) and (b) then $t = r$ and $u = s$ and $m_i = n_i$ for all i.

Some finitely generated abelian groups

$$\mathbb{Z} = \langle 1 \rangle$$

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

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

Suppose G is a finite abelian group.
Then G is finitely generated, for example

$$G = \langle \{ g \mid g \in G \} \rangle.$$

So, if G is a finite abelian group then

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

where

(a) $n_i \geq 2$

(b) $n_2 \mid n_1$, $n_3 \mid n_2$, $n_4 \mid n_3$, $\ldots$, $n_s \mid n_{s-1}$

(c) $|G| = n_1 n_2 \cdots n_s$

This expression is unique.

Suppose we have such an expression for G.

Let p be a prime with $p \mid |G|$.

Then $p \mid n_1 n_2 \cdots n_s$

Then since p is prime,

$p \mid n_i$ for some i.

By condition (b), $p \mid n_1$.

Ex: List up to isomorphism all the abelian groups of size $180 = 2^2 \cdot 3^2 \cdot 5$.

$$\mathbb{Z}_{2^2 \cdot 3^2 \cdot 5} = \mathbb{Z}_{180}$$

$$\mathbb{Z}_{2^2 \cdot 3 \cdot 5} \times \mathbb{Z}_3 = \mathbb{Z}_{60} \times \mathbb{Z}_3$$

$$\mathbb{Z}_{2 \cdot 3^2 \cdot 5} \times \mathbb{Z}_2 = \mathbb{Z}_{90} \times \mathbb{Z}_2$$

$$\mathbb{Z}_{2 \cdot 3 \cdot 5} \times \mathbb{Z}_{2 \cdot 3} = \mathbb{Z}_{30} \times \mathbb{Z}_6$$

Ex: Same question for size $7^3 \cdot 11^2 \cdot 13 = 539{,}539$

$$\mathbb{Z}_{7^3 \cdot 11^2 \cdot 13}$$

$$\mathbb{Z}_{7^2 \cdot 11^2 \cdot 13} \times \mathbb{Z}_7$$

$$\mathbb{Z}_{7^2 \cdot 11 \cdot 13} \times \mathbb{Z}_{7 \cdot 11}$$

$$\mathbb{Z}_{7 \cdot 11^2 \cdot 13} \times \mathbb{Z}_7 \times \mathbb{Z}_7$$

$$\mathbb{Z}_{7^3 \cdot 11 \cdot 13} \times \mathbb{Z}_{11}$$

$$\mathbb{Z}_{7 \cdot 11 \cdot 13} \times \mathbb{Z}_{7 \cdot 11} \times \mathbb{Z}_7$$

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

Pf:

($\Leftarrow$) Suppose $d=\gcd(m,n)=1$.

Claim: $\langle(\bar{1},\bar{1})\rangle = \mathbb{Z}_m \times \mathbb{Z}_n$.

Suppose k is the order of $(\bar{1},\bar{1})$.

So, $\underbrace{(\bar{1},\bar{1})+(\bar{1},\bar{1})+\cdots+(\bar{1},\bar{1})}_{k \text{ times}} = (\bar{0},\bar{0})$.

So, $(\bar{k},\bar{k})=(\bar{0},\bar{0})$.

Since $\bar{k}=\bar{0}$ in $\mathbb{Z}_m$ we have $m \mid k$.

Since $\bar{k}=\bar{0}$ in $\mathbb{Z}_n$ we have $n \mid k$.

So, $\operatorname{lcm}(m,n) \mid k$.

Also, $\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = \frac{mn}{1} = mn$.

So, $mn \mid k$.

Since k is the order of $(\bar{1},\bar{1})$ and $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ we have $k \mid mn$.

Since $k \mid mn$ & $mn \mid k$ we get $k=mn$.

($\Rightarrow$)

We

Pic

Since

Note

so

Thus,

$(\bar{a}$

($\Rightarrow$) Suppose $d = gcd(m,n) \neq 1$. (Contrapositive)

We need to show $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Pick any $(\bar{a}, \bar{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

Since $d > 1$, we get $\frac{mn}{d} < mn$.

Note that $d|m$ and $d|n$ and $d|mn$

so $\frac{m}{d}, \frac{n}{d}, \frac{mn}{d} \in \mathbb{Z}$.

Thus,

$$\underbrace{(\bar{a},\bar{b}) + (\bar{a},\bar{b}) + \cdots + (\bar{a},\bar{b})}_{\frac{mn}{d} \text{ times}} = \left(\overline{\tfrac{mn}{d}}\,\bar{a}, \overline{\tfrac{mn}{d}}\,\bar{b}\right) = \left(\bar{m}\left(\overline{\tfrac{n}{d}}\right)\bar{a}, \bar{n}\left(\overline{\tfrac{m}{d}}\right)\bar{b}\right)$$

$$= \left(\underbrace{\bar{0}\left(\overline{\tfrac{n}{d}}\right)\bar{a}}_{\text{in } \mathbb{Z}_m}, \underbrace{\bar{0}\left(\overline{\tfrac{m}{d}}\right)\bar{b}}_{\text{in } \mathbb{Z}_n}\right) = (\bar{0}, \bar{0}).$$

So the order of $(\bar{a}, \bar{b})$ is at most $\frac{mn}{d} < mn$. So, $\mathbb{Z}_m \times \mathbb{Z}_n$ has no generators and isn't cyclic.