Lagranges Theorem:

Let G be a finite group, $H \leq G$ then $|H|$ divides $|G|$

Moreover, $|G| = (\#\text{ of left cosets of } H) \cdot |H|$

Index of H in G denoted

$[G:H)$ or $(G:H)$

Example: $U_{12} = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5, \rho^6, \rho^7, \rho^8, \rho^9, \rho^{10}, \rho^{11}\}$

$\rho = e^{2\pi i/12}$, $\rho^{12} = 1$

$H = \langle \rho^3 \rangle = \{1, \rho^3, (\rho^3)^2 = \rho^6, (\rho^3)^3 = \rho^9\}$

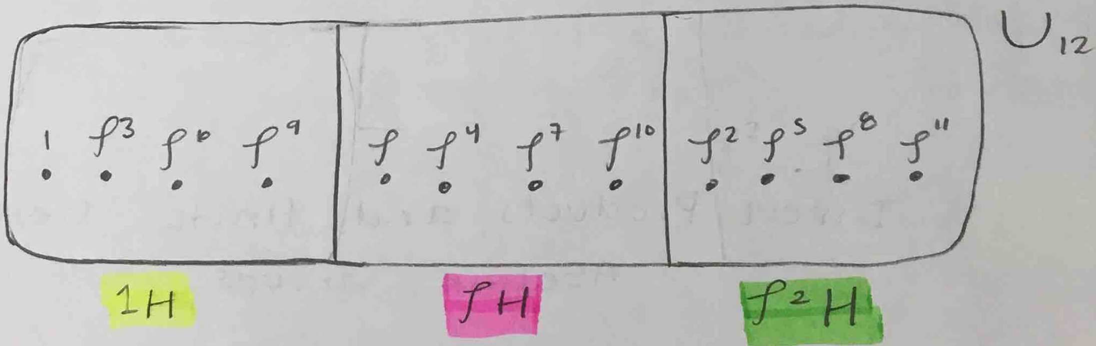
↑ we stop here because $(\rho^3)^4 = \rho^{12} = 1$ ← already in the set

left cosets of H

$1H = \{1, \rho^3, \rho^6, \rho^9\} = \rho^3 H = \rho^6 H = \rho^9 H$

$\rho H = \{\rho, \rho \cdot \rho^3, \rho \cdot \rho^6, \rho \cdot \rho^9\} = \{\rho, \rho^4, \rho^7, \rho^{10}\}$

$\rho^2 H = \{\rho^2, \rho^5, \rho^8, \rho^{11}\}$



$|U_{12}| = 3 \cdot 4 \leftarrow |H|$

↑

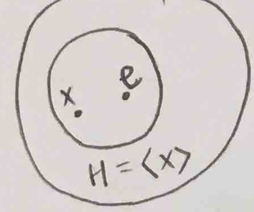
Index of H in U_{12}

$[U_{12} : H]$

Corollary to Lagrange's Theorem

Let G be a group where $|G|=p$ and p is prime
Then G is cyclic. Thus $G \simeq \mathbb{Z}_p$.

Proof:



Let e be the identity of G, let $x \in G$ where $x \neq e$ (we know such an x exists because $|G| = p \geq 2$)

Let $H = \langle x \rangle$. then $H \leq G$. so by Lagrange's theorem, $|H|$ divides $|G| = p$. Since p is prime $|H|=1$ or $|H|=p$, But H has at least 2 element: e and x so, $|H|=p$, thus $H=G$ $\therefore G = \langle x \rangle$ $\boxtimes$

Corollary to Lagrange's Theorem

Let G be a finite group. Let $x \in G$. Then the order of x divides $|G|$.

Proof: By theorem in class the order of $x = |\langle x \rangle|$
By Lagrange $|\langle x \rangle|$ divides $|G|$ $\boxtimes$

Recall: If the order of x is in n
then $\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$

Direct Products and finite Generated Abelian Groups

Def: Let $S_1, S_2, \dots, S_n$ be n sets. The cartesian product of $S_1, S_2, S_3, \dots, S_n$ is

$$S_1 \times S_2 \times \cdots \times S_n =$$

$$= \{(a_1, a_2, \dots, a_n) \mid a \in S_1, a_2 \in S_2, \dots, a_n \in S_n\}$$

10/31 P.2

* elements from $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

Example:

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

(b) $\mathbb{Z}_2 \times D_6 = \{(\bar{0},1), (\bar{0},r), (\bar{0},r^2), (\bar{0},s)\ (\bar{0},sr), (\bar{0},sr^2),$
$(\bar{1},1), (\bar{1},r), (\bar{1},r^2), (\bar{1},s), (\bar{1},sr), (\bar{1},sr^2)\}$

Theorem: Let $G_1, G_2, \dots G_n$ be groups
given $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in G_1 \times G_2 \times \dots \times G_n$
define $(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n)$
then $G_1 \times G_2 \times \dots \times G_n$ is a group under this operation

If e_i is the identity of G_i, then $(e_1, e_2, \dots e_n)$ is the identity of $G_1 \times G_2 \times \dots \times G_n$.
also: $(a_1, a_2, \dots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$

The group $G_1 \times G_2 \times \dots \times G_n$ is called the direct product of $G_1, G_2, \dots, G_n$

Example: $G_1 = \mathbb{Z}_2$, $G_2 = \mathbb{Z}_2$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{\underbrace{(\bar{0},\bar{0})}_{\text{identify element}}, (\bar{1},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{1})\}$

$(\bar{0},\bar{1}) + (\bar{1},\bar{1}) = (\bar{0}+\bar{1}, \bar{1}+\bar{1}) = (\bar{1},\bar{2}) = (\bar{1},\bar{0})$

$(\bar{1},\bar{1}) + (\bar{0},\bar{0}) = (\bar{1},\bar{1})$

* $\mathbb{Z}_2 \times \mathbb{Z}_2$ is called the Klen 4-group

order of elements

element	order
$(\bar{0},\bar{0})$	1
$(\bar{1},\bar{0})$	2
$(\bar{0},\bar{1})$	2
$(\bar{1},\bar{1})$	2

← identity always has order 1

$(\bar{1},\bar{0}) + (\bar{1},\bar{0}) = (\bar{2},\bar{0}) = (\bar{0},\bar{0})$

$\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic
$\mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian

Fact: If G and G_1 are both abelian then $G \times G_2$ is abelian

Example:

operations: addition, composition of functions

$$\underbrace{\mathbb{Z}_2}_{\text{addition}} \times \underbrace{D_6}_{\text{composition of functions}} = \{\underbrace{(\bar{0}, 1)}_{\text{identity}}, (\bar{0}, r), (\bar{0}, r^2), \dots, (\bar{1}, sr^2)\}$$

$$(\bar{1}, sr)(\bar{0}, r^2) = (\underbrace{\bar{0}+\bar{1}}_{\text{addition}}, \underbrace{sr \cdot r^2}_{\text{composition}})$$

$$(\bar{1}, sr^3) = (\bar{1}, s)$$

$r^3 = 1$ in D_6

$$(\bar{1}, s)(\bar{1}, sr) = (\bar{1}+\bar{1}, ssr) = (\bar{2}, s^2 r) = (\bar{0}, r)$$

Example:

From earlier we saw that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic since no element has order 4.

Example:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}) (\bar{1}, \bar{1}) (\bar{1}, \bar{2})\}$$

$$\langle(\bar{1}, \bar{1})\rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{1}) + (\bar{1}, \bar{1}) = (\underbrace{\bar{2}}_{\mathbb{Z}_2}, \underbrace{\bar{2}}_{\mathbb{Z}_3}) = (\bar{0}, \bar{2}),$$

$$(\bar{1}, \bar{1}) + (\bar{1}, \bar{1}) + (\bar{1}, \bar{1}) = (\bar{3}, \bar{3}) = (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{2})\} = \mathbb{Z}_2 \times \mathbb{Z}_3$$

since $\langle(\bar{1}, \bar{1})\rangle$ generates $\mathbb{Z}_2 \times \mathbb{Z}_3$ then

is cyclic

11/2 P.1 Wednesday Week 11 November 2, 2016

Theorem: $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic iff $\gcd(m,n)=1$ } when $\gcd(m,n)=1$ then $(\bar{1},\bar{1})$ will generate $\mathbb{Z}_m \times \mathbb{Z}_n$

Last time $\rightarrow$ $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic $\leftarrow \gcd(2,2)=2\neq 1$

$\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic $\leftarrow \gcd(2,3)=1$

Def: A group G is generated by the elements $g_1, g_2, \ldots, g_r \in G$ if

$$G = \{ g_{i_1}^{e_1}, g_{i_2}^{e_2}, \ldots, g_{i_k}^{e_k} \mid k \geq 1,\ e_j \in \mathbb{Z},\ 1 \leq i_j \leq r \}$$

This set is denoted by $\langle g_1, g_2, \ldots, g_r \rangle$

· If such a set exists then we say that G is finitely generated

Example:

$$\langle g_1, g_2, g_3 \rangle = \{ g_1,\ g_1^3 g_2^{100} g_1^{-2} g_3^{10},\ g_1 g_2 g_1 g_2,\ g_3^{-10{,}000}, \ldots \}$$

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

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

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

} some finitely generated groups.

Theorem: (Fundamental Theorem of finitely generated Abelian Groups)
Let G be a finitely generated Abelian group. Then G is isomorphic to a direct product of cyclic groups of the form: $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$
where the p_i are primes (not necessarily distinct) and the r_i are positive integers. The direct product is unique except for possible rearrangements of the factors. Note: If G is a finite abelian group the theorem is true but there are no $\mathbb{Z}$ factors.

If G and H are groups, then $G \times H \simeq H \times G$

-HW problem

Note: Any finite group is finitely generated. Just use all the elements of the groups as the generators

Example: Find all abelian groups of size 18 (up to isomorphism)

$18 = 2 \cdot 3^2$

$\mathbb{Z}_2 \times \mathbb{Z}_{3^2}$

$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

any abelian group of size 18 is isomorphic to one of these and these two groups are not isomorphic to each other.

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

$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if $\gcd(m,n) = 1$

That is $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if $\gcd(m,n) = 1$

- $\mathbb{Z}_9 \times \mathbb{Z}_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_9$
- $\mathbb{Z}_{3^2} \not\simeq \mathbb{Z}_3 \times \mathbb{Z}_3$

$\gcd(3,3) = 3 \neq 1$

Example:

Find all abelian groups of size 360 up to isomorphism

$360 = 2^3 \cdot 3^2 \cdot 5$

1. $\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5$
2. $\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
3. $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5$
4. $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
5. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5$
6. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

- $\mathbb{Z}_5 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \simeq$ 1
- $\mathbb{Z}_{360} = \mathbb{Z}_{2^3 \cdot 3^2 \cdot 5} \simeq$ 1

Note: • Any abelian group of size 360 will be isomorphic to exactly one of these 6 groups

Fact: Let G be a group of size 4

Then G must be abelian and so

$G \simeq \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$

Claim: Up to isomorphism, the only groups of size 4 are $\mathbb{Z}_4$ an $\mathbb{Z}_2 \times \mathbb{Z}_2$.

proof: Suppose $G = \{e, a, b, c\}$ is a group of order 4. case 1: If any of $a, b,$ or c has order 4, then G is cyclic and so is isomorphic to $\mathbb{Z}_4$. case 2: Otherwise, $a^2 = b^2 = c^2 = e$. This is enough to fill in the group table for G.

For example: Claim: $ab = c$. pf of claim: Suppose $ab = e$. Then $a^{-1} = b$. But $a^{-1} = a$ since $a^2 = e$. So, $ab \neq e$. Suppose $ab = a$. Then $b = e$. So, $ab \neq a$. Similarly $ab \neq b$. ∎

Here are the other products:

$ab = c$
$ac = b$

$ba = c$
$bc = a$
$ca = b$
$cb = a$

G	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Compare this to

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