Ex(1) How many hom. are there from $\mathbb{Z}_{10}$ to $\mathbb{Z}_{10}$? Which of them are onto?

$$\varphi : \underset{\langle 1 \rangle}{\mathbb{Z}_{10}} = \{0,1,\dots,9\} \longrightarrow \mathbb{Z}_{10}$$

$\varphi(1) =$ 0, 1 onto, 2, 3 onto, 4, 5, 6, 7 onto, 8, 9 onto

10 homomorphisms. 4 of them onto.

Ex(2) How many hom. are there from $\mathbb{Z}_{10}$ to $\mathbb{Z}_8$?

$$\varphi : \underset{\langle 1 \rangle}{\mathbb{Z}_{10}} \longrightarrow \mathbb{Z}_8$$

$$\varphi(1) = \begin{cases} 0 \\ 4 \end{cases} \quad \text{since } o(\varphi(1)) \mid 10 \text{ \& also } 8.$$

2 homomorphisms from $\mathbb{Z}_{10} \longrightarrow \mathbb{Z}_8$.

Ex(3) $G = \mathbb{R}_{\neq 0}$, $G' = \mathbb{R}_{>0}$

$$\varphi : \mathbb{R}_{\neq 0} \longrightarrow \mathbb{R}_{>0}$$

$$\varphi(x) = |x|$$

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y)$$

$\Rightarrow \varphi$ is a hom.

Let $a \in \mathbb{R}_{>0} \Rightarrow a \in \mathbb{R}_{\neq 0}$ & $\varphi(a) = |a| = a$

$\Rightarrow \varphi$ onto.

$$\ker\varphi = \{x \in \mathbb{R}_{\neq 0} \mid \varphi(x) = 1\} = \{1, -1\}$$

($\varphi(x) = |x|$)

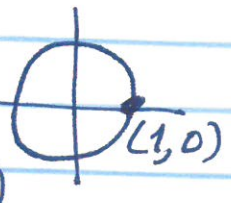
$\ker\varphi = \{1,-1\} \lhd \mathbb{R}_{\neq 0}$

Homomorphism Thm $\Rightarrow \mathbb{R}_{\neq 0}/\{1,-1\} \approx \mathbb{R}_{>0}$

Ex(4) $G = \mathbb{R}$

$$G' = S^1 = \{e^{2\pi i\theta} \mid 0 \leq \theta < 1\}$$

($e^{2\pi i\theta} = \cos(2\pi\theta) + i\sin(2\pi\theta)$)



$$\varphi : \mathbb{R} \longrightarrow S^1$$

by $\varphi(x) = e^{2\pi i x}$

$$\varphi(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x} e^{2\pi i y} = \varphi(x)\varphi(y)$$

$\Rightarrow \varphi$ hom.

Clearly φ is onto

$$\ker\varphi = \{ x \in \mathbb{R} \mid \varphi(x) = 1 \} = \mathbb{Z}$$

$$\varphi(x) = e^{2\pi i x}$$

Hom. Thm. $\Rightarrow \mathbb{R}/\mathbb{Z} \cong S^1$.

$|G| = n$, G abelian.

$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, $p_1 < p_2 < \cdots < p_r$ are primes

$k_i \in \mathbb{Z}_{>0}$

Fundamental Thm of finite abelian group

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$$

where $|G_j| = p_j^{k_j}$, $1 \le j \le r$.

$\Rightarrow$ To determine isomorphism class of G, it is enough to determine the isomorphism class of each G_j where $|G_j| = p_j^{k_j}$.

Suppose G is a finite abelian group and $|G| = p^m$, p prime, $m \in \mathbb{Z}_{>0}$

m	G
1	$\mathbb{Z}_p$
2	$\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \oplus \mathbb{Z}_p$ $(2 \quad , \quad 1+1)$
$3 = \begin{cases} 3 \\ 1+2 \\ 1+1+1 \end{cases}$	$\begin{cases} \mathbb{Z}_{p^3} \\ \mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \\ \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \end{cases}$

A partition of m is

$$m_1 + m_2 + \cdots + m_s \,, \quad m_1 \le m_2 \le \cdots \le m_s$$

and $m = m_1 + m_2 + \cdots + m_s$

P206 #8

$\operatorname{sgn} : G = S_n \longrightarrow \{1, -1\}$, $f(\sigma) = \begin{cases} 1, & \sigma \text{ even} \\ -1, & \sigma \text{ odd} \end{cases}$

$\| f$

$\sigma \in G \Rightarrow \sigma$ even or σ odd

$\sigma_1, \sigma_2 \in G$

$f(\sigma_1 \sigma_2) \stackrel{?}{=} f(\sigma_1) f(\sigma_2)$

- σ_1 even, σ_2 even $\Rightarrow \sigma_1 \sigma_2$ even.

  $f(\sigma_1) = 1$, $f(\sigma_2) = 1$, $f(\sigma_1 \sigma_2) = 1$

  $\Rightarrow f(\sigma_1 \sigma_2) = f(\sigma_1) f(\sigma_2)$

- σ_1 even, σ_2 odd $\Rightarrow \sigma_1 \sigma_2$ odd

  $-1 = f(\sigma_1 \sigma_2) = f(\sigma_1) f(\sigma_2) = (1)(-1)$

- σ_1 odd, σ_2 even $\Rightarrow \sigma_1 \sigma_2$ odd

  $-1 = f(\sigma_1 \sigma_2) = f(\sigma_1) f(\sigma_2) = (-1)(1)$

- σ_1 odd, σ_2 odd $\Rightarrow \sigma_1 \sigma_2$ even

  $1 = f(\sigma_1 \sigma_2) = f(\sigma_1) f(\sigma_2) = (-1)(-1)$

$\therefore$ f is a hom.

$\ker f = \{\sigma \in G \mid f(\sigma) = 1\} = \{\sigma \in G \mid \sigma \text{ even}\}$

$= A_n$.

Since f is onto, by Hom. Thm.

$$G/\ker f \cong \{1,-1\}$$

$$|G/\ker f| = 2 \Rightarrow A_n \text{ has index } 2 \text{ in } S_n$$

$$\Rightarrow A_n \trianglelefteq S_n.$$

G finite abelian group and

$$|G| = n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \quad p_1 < p_2 < \cdots < p_r \text{ primes}$$

$$\Rightarrow G \approx G_1 \oplus G_2 \oplus \cdots \oplus G_r$$

where $|G_1| = p_1^{k_1}$, $|G_2| = p_2^{k_2}$, ⋯

Ex(1) $|G| = 12 = 2^2 \cdot 3$, G abelian

$$G \approx G_1 \oplus G_2, \quad |G_1| = 2^2, \quad |G_2| = 3$$

$2 = 2$: $G_1 \approx \mathbb{Z}_{2^2} = \mathbb{Z}_4$

$= 1+1$: $G_1 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\Downarrow$

$G_2 \approx \mathbb{Z}_3$

Isomorphism classes for G:

- $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_{12}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_6$

Ex(2) G abelian, $|G| = 225 = 3^2 \cdot 5^2$

	3^2	5^2
$2 = 2$	$\mathbb{Z}_9$	$\mathbb{Z}_{25}$
$= 1+1$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_5 + \mathbb{Z}_5$

Isomorphism classes:

$\mathbb{Z}_9 \oplus \mathbb{Z}_{25}$

$\mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$

$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Ex(3) Determine the isom. class of $U(15)$.

$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

order: 1, 4, 2, 4, 4, 2, 4, 2

$|U(15)| = 8 = 2^3$

$3 = 3 \longrightarrow \mathbb{Z}_8$ X

$= 1+2 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_4$ ✓

$= 1+1+1 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ X

$\Rightarrow U(15) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4$

HW P220 #4, 7, 9, 10, 15abc, 19, 21

A nonempty set R equipped with two operations "addition" $+$ and "multiplication" $\cdot$ satisfying:

(1) $(R, +)$ is an abelian group.

(2) $(R, \cdot)$ satisfies

(i) $\forall\ a, b \in R,\ a \cdot b \in R$

(ii) $\forall\ a, b, c \in R,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(3) $\forall\ a, b, c \in R$

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (left distributivity)

& $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (right distributivity)

is called a <u>ring</u>.

If a ring R contains a multiplicative identity, $1 \in R$ $(\forall\ a \in R,\ a \cdot 1 = a = 1 \cdot a)$ then R is a ring with <u>unity</u>.

Ex(1) $R = \mathbb{Z}$, $(\mathbb{Z}, +, \cdot)$ is a ring with unity.

Ex(2) $R = 2\mathbb{Z}$, $(2\mathbb{Z}, +, \cdot)$ is a ring without unity.

Defn: A ring R is a commutative ring if $\forall a, b \in R$, $a \cdot b = b \cdot a$.

Ex(3) $(\mathbb{Z}, +, \cdot)$, $(2\mathbb{Z}, +, \cdot)$ are commutative rings.

Ex(4) $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$

'$+$' = matrix addition

'$\cdot$' = matrix multiplication

$M_2(\mathbb{R})$ is a ring with unity.

$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$M_2(\mathbb{R})$ not commutative.

Let R be a ring with unity $1 \in R$.

An element $a \in R$ is called a <u>unit</u> if there is $b \in R$ such that $a \cdot b = 1$

Denote

$U(R)$ = set of units in R

Then $(U(R), \cdot)$.

<u>Ex (5)</u> $R = \mathbb{Z}$ ring with unity.

$U(\mathbb{Z}) = \{1, -1\}$.

<u>Ex(6)</u> $R = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ ring with unity.

$U(\mathbb{Z}_4) = \{1, 3\} = U(4)$

<u>Thm:</u> $U(\mathbb{Z}_n) = U(n)$