# Abstract Algebra

MATH 205 Koç University
Duygu Sezen Islakoğlu
Instructor: Sinan Ünver

# MATH 205

## GROUPS

**DEF:** Let $G$ be a non-empty set together with an operation $*$ on $G$, i.e. $*$ is a function from $G \times G$ to $G$.

$(* : G\times G \longrightarrow G)$

However, rather than writing $\times(g,h)$ we write $g \times h$

Such that

(i) $*$ is associative, i.e. that for every $a,b,c \in G$.

$a*(b*c)=(a*b)*c$

(ii) There is an identity element $e$ for the operation, i.e. that

$\forall g \in G \quad , e*g=g=g*e \quad (1)$

NOTE If an identity exists then it is unique.

Suppose that $\exists e' \in G$ s.t.

$e'*g=g=g*e', \forall g \in G. \quad (1')$

$e \underset{\substack{(1') \\ w/ g=e}}{=} e*e' \underset{\substack{(1) \\ w/ g=e'}}{=} e'$

(iii) Every element in $G$ has an inverse, i.e

$\forall g \in G$ there exist a $g' \in G$

s.t $\quad g*g'=e=g'*g$

NOTE. If an inverse exists then it is unique.

Suppose that there exists a $g''$ s.t.

$g*g''=e=g''*g \quad (2')$

Claim $\quad g'=g''$

Proof $\quad g'*(g*g'') \underset{(2')}{=} g'*e=g'$

$\| \text{associativity}$

$(g'*g)*g''$

$\| \ (2)$

$g''=e*g''$

ABEL

**DEF:** Suppose that $(G,*)$ is a group

We say that $*$ is commutation (or $G$ is abelian) if

$\forall a,b \in G, \quad a*b=b*a$

NOTATION We sometimes denote the group operation by multiplication, i.e. We write $g \cdot h$ instead of $g \times h$, if no confusion should arise.

In this case we denote the identity by $'$, and the inverse of $g$ by $g^{-1}$

If $G$ is abelian, it is more common to denote the group operation by $+$.

In this case, we denote the identity by $0$ and the inverse of an element $g \in G$ by $-g$.

natural $\rightarrow \mathbb{N}=\{0,1,2\ldots\}$

$\mathbb{Z}:=\{\ldots -2,-1,0,1,2,\ldots\}$

$\mathbb{Q}:=\{\frac{p}{q} \mid p,q \in \mathbb{Z}, q \neq 0\}$

$\hookrightarrow$ rational numbers

$\mathbb{R}$ = real numbers

$\mathbb{C}$ = complex numbers $=\{a+ib \mid a,b \in \mathbb{R}\}$

$i^2=-1$

## EXAMPLES

(i) $(\mathbb{N}, +)$
- associative ✓
- identity ✓
- inverse ✗

not a group

(ii) $(\mathbb{Z}, +)$
$(\mathbb{Q}, +)$
$(\mathbb{R}, +)$
$(\mathbb{C}, +)$

group

(iii) $(\mathbb{Z}, \cdot)$

associative ✓
identity ✓
inverse ✗

not a group

(iv) $(\bar{\mathbb{Q}}, \cdot)$
assoc ✓
ident ✓
inverse ✗

not a group

(v) $(\mathbb{Q}\setminus\{0\}, \cdot)$ group

(vi) $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, $n \geq 1$

$\mathbb{Z}_n$ has two operations $+$ and $\cdot$.
$(\mathbb{Z}_n, +)$ is also an abelian group.

(vii) Let $S_n = \{f \mid f: \{1, \dots, n\} \to \{1, \dots, n\}$ s.t. $f$ is a bijection$\}$.

■ $|S_n| = n!$

There is a natural operation on $S_n$, defined as

$$(f \circ g)(x) = f(g(x)) \text{ for every } x \in \{1, \dots, n\}$$

### TERMINOLOGY

Suppose $f: X \to Y$

bijective
- $f$ is one-to-one $\Leftrightarrow$ $f$ is injective
- $f$ is onto $\Leftrightarrow$ $f$ is surjective

## OBSERVATION

$(S_n, \circ)$ is a group.

- $(f \circ g) \circ h = f \circ (g \circ h)$ assoc ✓

$i(x) = x$, $\forall x \in \{1, \dots, n\}$

- $f \circ i = f = i \circ f$ identity ✓
- $f \circ f^{-1} = i = f^{-1} \circ f$ inverse ✓

Note that if $n \geq 3$ then $(S_n, \circ)$ is not abelian.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}$$

$$\overset{?}{\neq} \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix}$$

### NOTATION

if $f \in S_n$ we write
$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$
instead of

$f \in S_3$ $f(1) = 3$
$f(2) = 1$
$f(3) = 2$

$$f \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$G$ always denotes a group.

Suppose that $H \subseteq G$

$$\begin{array}{ccc} H\times H & \dashrightarrow & H \\ \cap & & \cap \\ G\times G & \longrightarrow & G \\ (x,y) & \rightarrow & xy \end{array}$$

Suppose that if $x,y \in H$ then $xy \in H$, $\forall x,y \in H$

Then we can ask whether $H$ with this restricted operation is a group.

In order for this to be true, it has to have an identity, call it $e_H$

Then $e_H \cdot e_H = e_H$ in $G$.

$$e_H^{-1}(e_H e_H) = e_H^{-1} \cdot e_H = e_G \quad \text{MULTIPLY}$$

$$= \underbrace{(e_H^{-1} e_H)}\, e_H = e_G \cdot e_H = e_H = e_G$$

If $H$ is a group w/ the induced operation then

$$1 = e_G \in H$$

Moreover for any $h \in H$, it has to have an inverse i.e

$$\exists h^* \in H \text{ s.t } h^* h = 1 = h.h^*$$

$$\Rightarrow h^* = h^{-1} \in H$$

Hence if it is a group w/ induced operation, the following properties have to be satisfied.

(i) $1 \in H$

(ii) $\forall h_1, h_2 \in H \quad h_1 h_2 \in H$

(iii) $\forall h \in H$, $h^{-1} \in H$

**DEF:** If $H \subseteq G$ s.t. (i)(ii)(iii) are satisfied then we say that $H$ is a subgroup of $G \longrightarrow H \leq G$

Claim

Let $H \subseteq G$. Then

$H \leq G \Leftrightarrow$ (i) $1 \in H$

(ii) $\forall x,y \in H$ $xy^{-1} \in H$

▶ $(\mathbb{Z}, +)$ Then let $n \in \mathbb{N}$

$n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}$

then $n\mathbb{Z} \leq \mathbb{Z}$

$2\mathbb{Z} = \{ \dots, -4, -2, 0, 2, \dots \}$

$O := \{a \in \mathbb{Z} \mid a \text{ is odd}\}$

$= \{ \dots, -5, -3, \dots \} \subseteq \mathbb{Z}$

not a subgroup.

## COSETS OF A SUBGROUP

Let $H \leq G$.

Then define the following equivalence relations on $G$.

(i) $x \,{}_H\!\sim y \Leftrightarrow y^{-1}x \in H$

(ii) $x \sim_H y \Leftrightarrow yx^{-1} \in H$

Recall

Associated to $E$, we have for every $s \in S$

$[s] := \{t \in S \mid (s,t) \in E\}$
equivalence class of $s$

$$\bigcup_{s \in S} [s] = S$$

$[s] = [t] \Leftrightarrow (s,t) \in E$

$\forall s,t \in S$ there are two possibilities.

either $(s,t) \in E$ in which case $[s] = [t]$

OR $(s,t) \notin E$ $\quad [s] \cap [t] = \emptyset$

If $s_i \in S$, w/ $i \in I$ are s.t.

- $(s_i, s_j) \notin E$ for $i \neq j$
- And for every $s \in S$, $\exists i \in I$ s.t $(s, s_i) \in E$

then $S = \bigcup_{i \in I} [s_i]$

(i) ${}_H\sim$ : Let $x \in G$

$$[x] = \{ y \in G \mid x {}_H\sim y \}$$
$$= \{ y \in G \mid y^{-1}x \in H \}$$
$$= \{ y \in G \mid x^{-1}y \in H \}$$
$$= \{ y \in G \mid y \in xH \}$$
$$= xH$$

inverse

" The left coset of H in G which contains x "

$\mathcal{L}_H(G) := \{ xH \mid x \in G \}$

→ the set of left cosets of H in G.

$$\bigcup_{xH \in L_H(G)} xH = G$$

$$|G| = \sum_{xH \in L_H(G)} |xH| = \sum_{xH \in \mathcal{L}_H(G)} |H|$$
$$= |H| \cdot |\mathcal{L}_H(G)|$$

WE USE THAT CLAIM

Claim

$|xH| = |H|$

Proof

$x^t : H \longrightarrow xH$

$h \longrightarrow xh$

$x^t$ is bijective so $|xH| = |H|$ □

**DEF:** If $|G| < \infty$ then $|G|$ is called the order of $G$.

- $|\mathbb{Z}_n| = |\{0, 1, \dots n-1\}| = n$
- $|S_n| = n!$

If $|G| < \infty$, we say that $G$ is a finite group.

$\mathbb{Z}$ is not a finite group.

Proposition $\boxed{\text{(Lagrange)}}$

If $|G| < \infty$, and $H \leq G$ then

$|H| \mid |G|$

↳ divides

[**DEF** well defined
∈ or ∉ clear
input = output]

Proof

$$|G| = |H| \cdot |\mathcal{L}_H(G)|$$
$$\Rightarrow |H| \mid |G|$$

□

(ii) $\sim_H$ : Let $x \in G$

$$[x] = \{ y \in G \mid x \sim_H y \}$$
$$= \{ y \in G \mid yx^{-1} \in H \}$$
$$= Hx$$

right coset of H in G which contains x.

$\mathcal{R}_H(G) = \{ Hx \mid x \in G \}$

$$G = \bigcup_{Hx \in \mathcal{R}_H(G)} Hx$$

$|Hx| = |H|$

$\Rightarrow |G| = |H| \, |\mathcal{R}_H(G)|$

Claim $|\mathcal{L}_H(G)| = |\mathcal{R}_H(G)|$

PROOF

$\alpha : \mathcal{L}_H(G) \longrightarrow \mathcal{R}_H(G)$

$\alpha : xH \longrightarrow Hx^{-1}$

$\alpha$ is well-defined.

If $xH = x'H$, we need to show

def of $\alpha$

$Hx^{-1} = H(x')^{-1}$

Since $xH = x'H$ ; $x' = xh$

$Hx^{-1}$ and $H(x')^{-1} = H(xh)^{-1}$
$$= Hh^{-1}x^{-1}$$
$$= Hx^{-1}$$

Check : well-defined

$\beta : \mathcal{R}_H(G) \longrightarrow \mathcal{L}_H(G)$

$Hx \longrightarrow x^{-1}H$

$\beta \circ \alpha = id = \alpha \circ \beta$

□

In general

$$\mathcal{L}_H(G) \neq \mathcal{R}_H(G)$$

(If abelian for example, they are equal.)

$\blacktriangleright$ $G = S_3 = \left\{ \underset{I}{\begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix}} \underset{\sigma}{\begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix}} \underset{\sigma^2}{\begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix}} \underset{\tau_3}{\begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}} \underset{\tau_1}{\begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix}} \underset{\tau_2}{\begin{pmatrix} 1&2&3 \\ 3&2&1 \end{pmatrix}} \right\}$ $\qquad \tau_i^2 = I$

$H = \{I, \tau_3\}$ , $H \leq G$

$\mathcal{L}_H(G) = \{H, \tau_1 H, \tau_2 H\}$

$\tau_2 H \to \{\tau_2, \tau_2\tau_3\} = \{\tau_2, \sigma\}$

$\tau_1 H \to \{\tau_1, \tau_1\tau_3\} = \{\tau_1, \sigma^2\}$

All elements of $G$

$\mathcal{R}_H(G) = \{H, H\tau_1, H\tau_2\}$

$H\tau_1 \to \{\tau_1, \tau_3\tau_1\} = \{\tau_1, \sigma\}$

$H\tau_2 \to \{\tau_2, \tau_3\tau_2\} = \{\tau_2, \sigma^2\}$

$\mathcal{L}_H(G) \neq \mathcal{R}_H(G)$ "Left coset which contains $\sigma^2$ is not the right coset which contains $\sigma^2$"

**HW** $G = S_3$ . $H = \{1, \sigma, \sigma^2\}$ $H \leq G$ $\mathcal{L}_H(G) = \mathcal{R}_H(G)$

$\Rightarrow \mathcal{L}_H(G) = \{H, \tau_1 H\}$.

$\Rightarrow \mathcal{R}_H(G) =$

**DEF:** Let $H \leq G$ then we say that $H$ is normal in $G$, if $\mathcal{L}_H(G) = \mathcal{R}_H(G)$. In this case we write $H \trianglelefteq G$.

If $G$ is abelian and $H \leq G$ then

$H \trianglelefteq G$ ( b/c $\forall g \in G$ $gH = Hg$ )

**Proposition** Let $H \leq G$ then $H \trianglelefteq G \Leftrightarrow$ for every $g \in G$, $g^{-1}Hg = H$

(NOTATION for any subgroup $H \leq G$ Let $H^g = g^{-1}Hg$) $H^g \leq G$.

PROOF

($\Rightarrow$) Assume $H \trianglelefteq G$. Hence

$\mathcal{L}_H(G) = \mathcal{R}_H(G)$

Let $g \in G$. $Hg \in \mathcal{R}_H(G) = \mathcal{L}_H(G)$

$\Rightarrow Hg = gH$

$\Rightarrow g^{-1}Hg = H$

($\Leftarrow$) Suppose that $g^{-1}Hg = H$, $\forall g \in G$

WANT $\mathcal{L}_H(G) = \mathcal{R}_H(G)$

PROOF

Let $gH \in \mathcal{L}_H(G)$

$g^{-1}Hg = H \Rightarrow Hg = gH$

$\Rightarrow gH \in \mathcal{R}_H(G)$

$\mathcal{L}_H(G) \subseteq \mathcal{R}_H(G)$

similarly $\mathcal{R}_H(G) \subseteq \mathcal{L}_H(G)$

Hence $\mathcal{L}_H(G) = \mathcal{R}_H(G)$

$H \trianglelefteq G$

## Observation

Suppose $H \leq G$ and we want to define a natural group operation on $\mathcal{L}_H(G)$ (Respectively $R_H(G)$)

The operation on $\mathcal{L}_H(G)$ (respectively $R_H(G)$) would have the property,

$$(g_1H)(g_2H) := g_1g_2H$$

(resp. $(Hg_1)(Hg_2) = Hg_1g_2$)

For this operation to be well-defined; we need the following condition if $g_1H = g_1'H$ and $g_2H = g_2'H$ then

$$g_1g_2H = g_1'g_2'H$$

(Resp. if $Hg_1 = Hg_1'$ and $Hg_2 = Hg_2'$ then

$$Hg_1g_2 = Hg_1'g_2'$$

**THEOREM** 14.4 Pg 138 The above definition for the operation on $\mathcal{L}_H(G)$ (respectively for $R_H(G)$) is well-defined if and only if

$$H \trianglelefteq G$$

PROOF

(⇐) On $L_H(G)$ the operation is well defined means $\forall g_1, g_2, g_1', g_2' \in G$

$(g_1H = g_1'H$ and $g_2H = g_2'H \Rightarrow g_1g_2H = g_1'g_2'H)$

$\Leftrightarrow (g_1^{-1}g_1' \in H$ and $g_2^{-1}g_2' \in H \Rightarrow (g_1g_2)^{-1}g_1'g_2' \in H)$

$\Leftrightarrow (g_1^{-1}g_1' \in H$ and $\underbrace{g_2^{-1}g_2'}_{h_3} \in H \Rightarrow g_2^{-1}\underbrace{g_1^{-1}g_1'}_{h_1 \in H}g_2' \in H)$

(Condition is satisfied)

first side: If $H \trianglelefteq G$

$g_2^{-1} \cdot h_1 \cdot g_2'$

$= \underbrace{g_2^{-1}g_2'}_{h_3 \in H} \underbrace{(g_2')^{-1} h_1 \cdot g_2'}_{h_2 \in H} \in H$ → since $H \leq G$

$g_2'^{-1} H g_2' = H$ → since $H \trianglelefteq G$

So if $H \trianglelefteq G$ then the oper. on $\mathcal{L}_H(G)$ is well-defined.

(⇒) Conversely Suppose that the operation on $\mathcal{L}_H(G)$ is well-defined.

WANT $H \trianglelefteq G$

PROOF

Need to show that $\forall g \in G$, $g^{-1}Hg = H$

Take $g^{-1}hg \in g^{-1}Hg$.

$g^{-1}hg \in [(g^{-1}H)(gH) = eH = H]$, with $g^{-1}h \in g^{-1}H$ and $g \in gH$

$\Rightarrow g^{-1}Hg \leq H$ **(1)**, $\forall g \in G$

Replace $g$ with $g^{-1}$.

$gHg^{-1} \trianglelefteq H \Rightarrow H \leq g^{-1}Hg$ **(2)**

(1) and (2) $\Rightarrow g^{-1}Hg = H$, $\forall g \in G$

$\Rightarrow H \trianglelefteq G$

(Analogous proof for $R_H(G)$)

Observation

suppose that $H \trianglelefteq G$, then

$$\mathcal{L}_H(G) = \mathcal{R}_H(G) = G/_H$$

and $(G/_H) \times (G/_H) \to G/_H$

$$(g_1/H, g_2/H) \longrightarrow g_1g_2/H$$

$$(Hg_1, Hg_2) \longrightarrow Hg_1Hg_2$$

is well-defined.

Claim With this operation $G/_H$ is a group.

PROOF

(i) $(g_1H\, g_2H)\, g_3H = g_1g_2 H\, g_3 h = (g_1g_2)g_3H$

$= g_1(g_2g_3)H = g_1 Hg_2g_3 H = g_1H(g_2Hg_3H)$

G is assoc.

(ii) $(gH)(eH) = geH = gH = egH = (eH)(gH)$

$\Rightarrow eH = H$ is the identity.

(iii) $(gH)(g^{-1}H) = gg^{-1}H = eH = g^{-1}gH$
$= (g^{-1}H)(gH)$

$\Rightarrow (gH)^{-1} = g^{-1}H$.

▶ Let $n \geq 1$,

$n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$

$\trianglelefteq \mathbb{Z}$

$0+5k,\ 1+5k, \dots, 4+5k$

$\mathbb{Z}/_n\mathbb{Z} = \{0+n\mathbb{Z},\ 1+n\mathbb{Z}, \dots (n-1)+n\mathbb{Z}\}$

↘ arithmetic modulo $n$

## HOMOMORPHISM / ISOMORPHISM

$$\mathbb{Z}/_{2\mathbb{Z}} = \{0+2\mathbb{Z}, 1+2\mathbb{Z}\}$$

| | $0+2\mathbb{Z}$ | $1+2\mathbb{Z}$ |
|---|---|---|
| $0+2\mathbb{Z}$ | $0+2\mathbb{Z}$ | $1+2\mathbb{Z}$ |
| $1+2\mathbb{Z}$ | $1+2\mathbb{Z}$ | $0+2\mathbb{Z}$ |

Suppose that $G$ and $G'$ are two groups

Let $\phi : G \to G'$ be a bijection s.t.

$\forall g_1, g_2 \in G$

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$$

Then $\phi$ is isomorphism.

$G$ and $G'$ are isomorphic.

OBSERVATION

Being isomorphic is an equivalence relation on the set of all groups.

We say that $\phi : G \longrightarrow G'$ is a homomorphism if

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \quad \forall g_1, g_2 \in G$$

ANALOGOUS

$L : V_1 \to V_2$ linear trans.

$L(v+w) = L(v) + L(w)$

$L(\lambda . v) = \lambda L(v)$

13.12 THCO PG:128 THEOREM

Suppose $\phi : G \longrightarrow G'$ be a homomorphism

(i) $\phi(1_G) = 1_{G'}$

$\phi(1) = \phi(1.1) = \phi(1)\phi(1)$

$1_{G'} = \phi(1)^{-1}\phi(1) = \phi(1)^{-1}\phi(1)\phi(1)$
$= \phi(1_G)$

(ii) $\phi(g^{-1}) = \phi(g)^{-1}$

$1 = \phi(1) = \phi(g g^{-1}) = \phi(g)\phi(g^{-1})$

$\phi(g)^{-1}\, \phi(g) . \phi(g^{-1}) = 1$

$= 1 . \phi(g^{-1}) = \phi(g^{-1})$

(iii) $im(\phi) \leq G'$

$1_{G'} = \phi(1_G) \in im(\phi)$

Let $x, y \in im(\phi)$

$x = \phi(\alpha) \quad y = \phi(\beta)$

$xy^{-1} = \phi(\alpha)\phi(\beta)^{-1} = \phi(\alpha)\phi(\beta^{-1})$

$= \phi(\alpha\beta^{-1}) \in Im\,\phi$

(iv) $\ker\phi := \{ g \in G \mid \phi(g) = 1 \}$ 13.15 THEO PG.13 13.20 ALSO.

Claim $\ker\phi \trianglelefteq G$

Proof $1 \in \ker\phi \Leftrightarrow \phi(1) = 1$

$x, y \in \ker\phi$, $\phi(x) = 1$, $\phi(y) = 1$

$\Rightarrow \phi(y^{-1}) = \phi(y)^{-1} = 1$

$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = 1.1$

$\Rightarrow xy^{-1} \in \ker\phi$

$\ker\phi \leq G$.

In order to show $\ker\phi \trianglelefteq G$ we need to show that

$g^{-1} \ker\phi \, g \subseteq \ker\phi \quad \forall g \in G$

Let $a \in \ker\phi$ want to show

$g^{-1}ag \in \ker\phi$

$\Leftrightarrow \phi(g^{-1}ag) = 1$

$\Leftrightarrow \phi(g)^{-1} \underbrace{\phi(a)}_{1} \phi(g)$

$= \phi(g)^{-1}. \phi(g) = 1$

$N \trianglelefteq G \Leftrightarrow \forall g \in G \; g^{-1}Ng = N$

$\Leftrightarrow \forall g \in G \; g^{-1}Ng \leq N$

$g$ yerine $g^{-1}$ alınca

$gNg^{-1} \leq N$

multiply with $g^{-1}$

$N \leq g^{-1}Ng$

**Recall**

Let $H \leq G$, we would like to define an operation on $\mathcal{L}_H(G)$ (resp. $\mathcal{R}_H(G)$) s.t $(g_1H)(g_2H) = g_1g_2H$ (resp: $(Hg_1)(Hg_2) = Hg_1g_2$)

This operation is in general not well-defined. We proved that this operation on $\mathcal{L}_H(G)$ (resp on $\mathcal{R}_H(G)$) is well-defined $\Leftrightarrow H \trianglelefteq G$

And in this case, we showed that this operation makes $G/H := L_H(G) = R_H(G)$, a group. This group is called the quotient (or factor group) of $G$ by $H$.

-Let $G$ and $G'$ be two groups, we defined what it means for $\phi: G \to G'$ to be a homomorphism, i.e. $\forall x, y \in G \; \phi(x.y) = \phi(x)\phi(y)$

-We proved $\{ g \in G \mid \phi(g) = 1 \} =: \ker\phi \trianglelefteq G$

**Observation 1**

Let $\phi: G \to G'$ be a homomorphism.

CLAIM $\phi$ is injective $\Leftrightarrow \ker\phi = \{1\}$

PROOF

($\Rightarrow$) Suppose that $\phi$ is injective and $x \in \ker\phi$. Then

$\phi(x) = 1_{G'} = \phi(1_G)$

$\Rightarrow \phi(x) = \phi(1) \underset{\phi, inj}{\Rightarrow} x = 1$

So $\underset{\text{since } \ker\phi \leq G}{1 \in \ker\phi} \subseteq \{1\} \Rightarrow \ker\phi = \{1\}$

($\Leftarrow$) suppose $\ker\phi = \{1\}$

Suppose that $\phi(x) = \phi(y)$

$\Rightarrow \phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = 1 \Rightarrow xy^{-1} \in \ker\phi = \{1\}$

$\Rightarrow x$

(ii) Let $\phi: G \longrightarrow G'$ be a homomorphism

<u>CLAIM</u> $im(\phi) = \phi(G) = \{\phi(x) \mid x \in G\} \leq G'$

**Warning**

It is not in general true that $\phi(G) \trianglelefteq G'$

▶ $G' = S_3$

$\phi: G \longrightarrow S_3$

$\phi(g) = g$

$\phi(G) = G \leq S_3$

$G \ntrianglelefteq S_3$

$G = \left\{ \begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix} \begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix} \right\}$

(Previous example)

<u>PROOF</u>

$1 = \phi(1) \in im(\phi)$

Let $x, y \in im(\phi) \Rightarrow x = \phi(\alpha)$, for some $\alpha, \beta \in G$
$y = \phi(\beta)$

$xy^{-1} = \phi(\alpha)\phi(\beta)^{-1} = \phi(\alpha\beta^{-1}) \Rightarrow xy^{-1} \in im(\phi)$.

# FIRST ISOMORPHISM THEOREM

Let $\phi: G \longrightarrow G'$ be a homomorphism.

Then since $\ker\phi \trianglelefteq G$, we can form

$G/_{\ker\phi}$ and $im\,\phi$

and $\tilde{\phi}: G/_{\ker\phi} \longrightarrow im\,\phi = \phi(G)$.

$\tilde{\phi}(g\ker\phi) = \phi(g)$

<u>CLAIM</u>

$\tilde{\phi}$ is an isomorphism.

<u>PROOF</u>

- $\tilde{\phi}$ is well-defined.

$a = b$
$\tilde{\phi}(a) = \tilde{\phi}(b)$

$= \begin{array}{l} x\ker\phi = y\ker\phi \\ y^{-1}x \in \ker\phi \end{array}$

$\Rightarrow \phi(y^{-1}x) = 1$

$\Rightarrow \phi(y)^{-1} \cdot \phi(x) = 1 \Rightarrow \phi(x) = \phi(y)$

$\Rightarrow \tilde{\phi}(x\ker\phi) = \tilde{\phi}(y\ker\phi)$

So $\tilde{\phi}$ is well-defined.

- $\tilde{\phi}$ is a homomorphism.

$\tilde{\phi}(x\ker\phi \cdot y\ker\phi) \overset{\text{def of } G/\ker\phi}{=} \tilde{\phi}(xy\ker\phi) \overset{\text{def of } \tilde{\phi}}{=} \phi(xy) \underset{\text{homomorphism}}{=} \phi(x)\phi(y)$

$= \tilde{\phi}(x\ker\phi)\tilde{\phi}(y\ker\phi)$

def of $\tilde{\phi}$

$\therefore \tilde{\phi}$ is a homomorphism.

- $\tilde{\phi}$ is injective.

Enough to show that

$\ker\tilde{\phi} = \{1_{G/\ker\phi}\} = \{\ker\phi\}$

Let $x\ker\phi \in \ker\tilde{\phi}$

then $\tilde{\phi}(x\ker\phi) = 1$

$\|$ def of $\tilde{\phi}$

$\phi(x)$

$\Rightarrow$ (Def of $\ker\phi$) $x \in \ker\phi \Rightarrow x\ker\phi = \ker\phi$ .
$\phi(x) = 1_G$ $\qquad = 1_{G/\ker\phi}$

$\Rightarrow \ker\tilde{\phi} = \{1_{G/\ker\phi}\}$

So $\tilde{\phi}$ is injection.

$\tilde{\phi}$ is surjective. Let $\alpha \in \operatorname{im}\phi$

$\Rightarrow \alpha = \phi(x) = \tilde{\phi}(x\ker\phi)$ for some $x \in G$

$\alpha \in \operatorname{im}(\tilde{\phi})$, $\therefore \tilde{\phi}$ is surjective.

**Observation**

Let $H \trianglelefteq G$

$\pi : G \twoheadrightarrow G/H$ — canonical projection

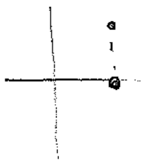
$\twoheadrightarrow$ ; $\hookrightarrow$ inj ; $\xrightarrow{\sim}$ bijective

$\pi(g) = gH$

CLAIM $\pi$ is a homom + surj = epimorphism

PROOF

- $\pi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \pi(g_1)\pi(g_2)$
  $\Rightarrow \pi$ is a homom.
- Let $gH \in G/H$ be an arbitrary element.
  $\pi(g) = gH$
  $\operatorname{im}(\pi) = G/H$



$\mathbb{R}^2$ -
$H = y$-axis
$G/H = x$ axis

$H/N$

**Observation**

Let $\phi : G \to G'$ be a homomorphism.

$$\begin{tikzcd} \ker\phi \trianglelefteq G \arrow[r, "\phi"] \arrow[d, "\pi"] & G' \\ G/\ker\phi \arrow[r, "\tilde{\phi}"] & \operatorname{im}\phi \arrow[u, hook, "i"] \end{tikzcd}$$

i for inclusion (maps to itself)

COMMUTATIVE

**Recall**

- Suppose $N \trianglelefteq G$
  Then there is a natural homom.

  $\pi : G \twoheadrightarrow G/N$ surjection

**Observation**

Let $N \trianglelefteq G$
then there is a 1-1 correspondence

$$X = \left\{\begin{array}{l}\text{subgroups}\\ \text{of } G/N\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{subgroups of}\\ G \text{ which contain}\\ N\end{array}\right\} = Y$$

since $N \trianglelefteq G$, $gN = Ng$, $\forall g \in G$
$\Rightarrow hN = Nh$, $\forall h \in H$
$\Rightarrow N \trianglelefteq H$

$H/N \leq G/N$ $\qquad \boxed{\alpha(H) = H/N}$ $\qquad N \trianglelefteq H \leq G$

$\bar{H} \leq G/N$ $\xrightarrow{\beta}$ $\pi^{-1}(\bar{H})$

$\alpha : \mathcal{Y} \to \mathcal{X}$

is a function.

$\alpha(H) = H/N \leq G/N$

WANT • $1_{G/N} = 1.N \in H/N$

- suppose $xN \in H/N$

  and $yN \in H/N$

$\Rightarrow x, y \in H$

$\Rightarrow y^{-1}x \in H \Rightarrow y^{-1}xN \in H/N$

$H \leq h$

$\Rightarrow (yN)^{-1} xN \in H/N$

$\ulcorner a \in H$

$aN \in H/N \lrcorner$

$\therefore H/N \leq G/N$

$\beta : \mathcal{X} \to \mathcal{Y}$ is a function.

Let $\bar{H} \in \mathcal{X} \Leftrightarrow \bar{H} \leq G/N$

• $\beta(\bar{H}) := \pi^{-1}(\bar{H})$ • $\pi : G \to G/N$

$/ \pi : G \twoheadrightarrow G/N$

Claim $N \leq \pi^{-1}(\bar{H}) \leq G$

Proof • $1 \in \pi^{-1}(\bar{H})$, since $\pi(1) = 1 \in \bar{H}$

since $\bar{H} \leq G/N$

since $\pi$ is a homom

• Suppose $x, y \in \pi^{-1}(\bar{H})$

$\Rightarrow \pi(x), \pi(y) \in \bar{H} \Rightarrow \pi(y)^{-1} \pi(x) \in H$

$H \leq G/N$ $\quad \| \pi$ is homom

$\pi(y^{-1}x)$

$\Rightarrow y^{-1}x \in \pi^{-1}(\bar{H}) \quad \therefore \pi^{-1}(\bar{H}) \leq G$

$N = \ker \pi = \pi^{-1}(\{1\}) \subseteq \pi^{-1}(H)$

In order to finish the proof, we need to show

(i) $\beta \circ \alpha = id$

(ii) $\alpha \circ \beta = id$

"$\beta \circ \alpha = id$ ise

$H = S$ olmalı."

(i) $(\beta \circ \alpha)(H) = \beta(\alpha(H))$

$= \beta(H/N)$

• $= \pi^{-1}(H/N) = \{x \in G \mid \pi(x) \in H/N\}$

$= \{x \in G \mid xN \in H/N\}$

$= \{x \in G \mid \exists h \in H \text{ s.t. } xN = hN\}$

$= \{x \in G \mid \exists h \in H \ h^{-1}x \in N\} = S$

I claim that

$S = H$

a) $S \subseteq H$.

Let $x \in S \Rightarrow \exists h \in H, h^{-1}x \in N \subseteq H$

$\Rightarrow \boxed{x \in H}$

since $H \leq G$

b) $H \subseteq S$

Let $h \in H$, $h^{-1}h = 1 \in N$

$\Rightarrow h \in S$

So $\beta \circ \alpha = id$

(ii) $\alpha \circ \beta = id$

$(\alpha \circ \beta)(\bar{H})$

$= \alpha(\beta(\bar{H}))$

$= \alpha(\pi^{-1}(\bar{H}))$

$= \pi^{-1}(\bar{H})/N$

$\pi : G \longrightarrow G/H$

$\qquad\qquad\quad \text{VI}$

$\qquad\qquad\quad \bar{H}$

CLAIM

$\pi^{-1}(\bar{H})/N = \bar{H}$

PROOF

First $\quad N \trianglelefteq \pi^{-1}(\bar{H})/N \leq G$

(a) $\pi^{-1}(\bar{H})/N \subseteq \bar{H}$

Let $xN \in \pi^{-1}(\bar{H})/N$

$\Rightarrow \exists y \in \pi^{-1}(\bar{H})$ s.t $\quad xN = yN$

$\Rightarrow \exists y \in \pi^{-1}(\bar{H})$ s.t $\quad y^{-1}x \in N$

Let $xN \in \pi^{-1}(\bar{H})/N \subseteq \bar{H}$ s.t. $\quad x \in \pi^{-1}(\bar{H})$

$\Rightarrow \pi(x) \in \bar{H}$

$\Rightarrow xN \in \bar{H}$

$\pi(x) = xN$

—o—

(b) $\bar{H} \subseteq \pi^{-1}(\bar{H})/N$,

Note $\bar{H} \leq G/N$

Let $xN \in \bar{H} \Rightarrow x \in \pi^{-1}(\bar{H}) \Rightarrow xN \in \pi^{-1}(\bar{H})/N$

$\pi(x) = xN$

▶ Let us try to find all subgroups of $(\mathbb{Z}, +)$

cyclic

also $\begin{pmatrix}\mathbb{Z}_n \\ +\end{pmatrix}$ cyclic

$\boxed{n\mathbb{Z} : \text{cyclic}}$

First of all, if $n \in \mathbb{N}$

then $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} \leq \mathbb{Z}$

CLAIM

if $H \leq \mathbb{Z}$

then $H = n\mathbb{Z}$, for some unique $n \in \mathbb{N}$

warning

$2\mathbb{Z} = (-2)\mathbb{Z}$

but $-2 \notin \mathbb{N}$

PROOF $\quad H \neq \{0\}$

Let $|H|^* = \{|h| \mid h \in H\} \setminus \{0\} \subseteq \mathbb{N}$

Let $n$ be the smallest element of $|H|^*$

We want to show that $H = n\mathbb{Z}$.

(a) $H \subseteq n\mathbb{Z}$

(b) $n\mathbb{Z} \subseteq H$

(b) $n \in |H|^*$

$\Rightarrow \exists h \in H$ s.t.

$n = |h|$

$\Rightarrow n = h$ or $n = -h$

for some $h \in H$

$\Rightarrow n \in H$

$\overbrace{n + n + \cdots}^{m \text{ times}} \in H$

and

$\underbrace{(-n) + (-n) + \cdots}_{m \text{ times}} \in H$

(a) Let $h \in H \Rightarrow |h| \in |H|^*$

$|h| = n.q + r$, for some $q \in \mathbb{N}$

and

$0 \leq r < n$.

$\Rightarrow \quad r = (\underset{\substack{\cap \\ H}}{|h|} - \underset{\substack{\cap \\ H}}{n}.q) \in H$

$\Rightarrow r = 0$ or $r \in |H|^* \Rightarrow r = 0$ or $\cancel{n = \min(|H|^*) \leq r}$

Bunun keşulu

ama buna ters düşüyor.

$\Rightarrow |h| = n.q \Rightarrow n \in n\mathbb{Z}$

Observation

Since $(\mathbb{Z}, +)$ is abelian,
all the subgroups of $n\mathbb{Z}$ are normal.

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$

$\varphi(a) = \bar{a}$

$\varphi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \varphi(a) + \varphi(b)$

$\ker \varphi = n\mathbb{Z}$

$\mathbb{Z}/_{n\mathbb{Z}} \xrightarrow{\sim} \mathbb{Z}_n$ First isomorphism

**DEF:** $G$ is cyclic if $\exists g \in G$

s.t. $\langle g \rangle = G$

$\{g^n \mid n \in \mathbb{Z}\}$

**Remark:** If $G$ is a group and $X \subseteq G$

similar to subspace spanned by a set.

$\langle X \rangle = \{ x_1^{\varepsilon_1}, \dots, x_n^{\varepsilon_n} \mid x_1, \dots, x_n \in X$
$\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\} \}$

the subgroup generated by $X$

$\subseteq G$

In fact $\langle X \rangle \leq G$

$1 \in \langle X \rangle$. Let $x \in X$, $1 = x^1 x^{-1} \in \langle X \rangle$

If $\alpha, \beta \in \langle X \rangle$ then

$\alpha = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ and $\beta = x_{n+1}^{\varepsilon_{n+1}} \dots x_{n+m}^{\varepsilon_{n+m}}$

where $x_1, \dots x_{m+n} \in X$ and $\varepsilon_i \in \{\pm 1\}$

$$\alpha^{-1}\beta = (x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n})^{-1} x_{n+1}^{\varepsilon_{n+1}} \dots x_{n+m}^{\varepsilon_{n+m}}$$

$$= x_1^{-\varepsilon_1} \dots x_n^{-\varepsilon_n} \cdot x_{n+1}^{\varepsilon_{n+1}} \dots x_{n+m}^{\varepsilon_{n+m}}$$

$$\in \langle X \rangle$$

If $X = \{g\}$

$\langle X \rangle = \{ g^{\varepsilon_1} \dots g^{\varepsilon_n} \mid$ where $\varepsilon_i \in \{\pm 1\} \}$

$= \{ g^n \mid$ for some $n \in \mathbb{Z} \}$

$= \langle g \rangle$

▶ Let $X = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

Find $\underbrace{\langle X \rangle}_{} \leq S_3$

$\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\rangle$

**DEF:** - Let $g \in G$, then if $|G| < \infty$

then $|\langle g \rangle| \mid |G|$ By Lagrange.

- suppose that $G$ is an arbitrary group and let $g \in G$.

Then there are two possibilities.

(i) $|\langle g \rangle| < \infty$

(ii) $|\langle g \rangle|$ is not finite.

(i) If $|\langle g \rangle| < \infty$

Let $n = |\langle g \rangle|$

CLAIM $n = \min \{ m \mid g^m = 1, m \in \mathbb{N}_{>0} \}$

PROOF

Let $n_0 = \min\{m \mid g^m = 1, m \in \mathbb{N}_{>0}\}$

(Remark: $\{m \mid g^m = 1, m \in \mathbb{N}_{>0}\} \neq \emptyset$

$\{1, g, g^2 \dots g^n\} \leq \langle g \rangle$

n elements

They cannot be all distinct (eleman sayısı olarak)

$\Rightarrow \exists \quad 0 \leq a < b \leq n$

s.t $g^a = g^b$

$\Rightarrow 1 = g^{b-a}, \ b-a \in \mathbb{N}_{>0}$

$b-a \in \{m \mid g^m = 1, m \in \mathbb{N}_{>0}\}$ cannot be empty set.

WANT

$n = n_0$

PROOF

Know

(i) $g^{n_0} = 1$,

(*)(ii) if $g^m = 1$, with $1 \leq m$ then $n_0 \leq m$

$g^a = g^{n_0 q + r} = (g^{n_0})^q \cdot g^r$

$= g^r$

$\langle g \rangle = \{1, g, \dots, g^{n_0 - 1}\}$ n elements

If we can show that

$1, g, \dots, g^{n_0-1}$ are distinct then

$n = |\langle g \rangle| = |\{\dots\}| = n_0$

If $g^a = g^b$, for some $1 \leq a < b \leq n_0 - 1$ — en fazla derece farkı

$1 \leq b - a < n_0$

CONTRADICTS (ii)(*)

So the elements are distinct

$|\langle g \rangle| = |g|$, this is called the order of $g$.

If $|\langle g \rangle| < \infty$

Then $|g| = \min\{m \mid g^m = 1, m \in \mathbb{N}_{>0}\}$

(ii) If $|\langle g \rangle| = 0$ Then we say that $g$ has infinite order and write $|g| = \infty$

**Corollary**

If $|\langle g \rangle| < \infty$, then

if $g^m = 1$, for some $m \in \mathbb{N}_{>0}$

then $|g| \mid m$

PROOF

Let $n = |g|$, $m = n \cdot q + r$ where $0 \leq r < n$

$1 = g^m = g^{nq+r} = (g^n)^q \cdot g^r = g^r$

If $r \neq 0$, then $r \in \{m \mid g^m = 1, m \in \mathbb{N}_{>0}\}$ → smallest element is $n$. but $r < n$ contradiction

Then $r$ cannot be non-zero

$r = 0$

$\Rightarrow n \mid m$

BACK TO EXAMPLE $\langle x \rangle =: H \leq S_3$

Lagrange Theorem $|H| \,\big|\, |S_3| = 6$

$x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in H$

$y = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in H$

$|\langle x \rangle| = |x| = 2$ because $x^1, x^2 = 1$

$2 = |\langle x \rangle| \,\big|\, |H|$ Lagrange

$z = xy \in H$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$z = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$z^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$z^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1$

$|z| = 3 = |\langle z \rangle| \,\big|\, |H|$

2 divides, 3 divides

Then 6 divides $|H|$

$6 \mid |H| \rightarrow |H| = 6$

$|H| \leq 6$

$\Rightarrow H = S_3$

$\left|\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right| = \left|\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right| = \left|\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right| = 2$

$\left|\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right| = \left|\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right| = 3$

$\left|\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\right| = 1$

$S_3$ is not cyclic.

## CYCLIC GROUPS

Every cyclic group is isomorphic to exactly one of the groups below

$$\mathbb{Z},\ \mathbb{Z}_n,\ n \in \mathbb{N}_{>0}$$
$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

Suppose that $G$ is cyclic then $G = \langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$

$\phi : \mathbb{Z} \twoheadrightarrow G$

$\phi(n) = g^n \quad , \forall n \in \mathbb{Z}$

$\phi(n+m) = g^{n+m} = g^n \cdot g^m = \phi(n)\phi(m)$

$\phi$ is a homom.

First isomorphism theorem

$$\mathbb{Z}/\ker\phi \simeq \operatorname{im}\phi = G$$

$\underline{\ker\phi = n\mathbb{Z}}$ , for some $n \in \mathbb{N}$

(i) If $n=0$ then $\ker\phi = \{0\}$ and $\phi$ is $\boxed{\text{injective}}$

$$\mathbb{Z} \xrightarrow{\sim} G \ ,\ |\mathbb{Z}| = \infty$$

(ii) If $n>0$ then

$$\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G \ :$$
$$|\mathbb{Z}_n| = n$$

*Recall*

If $G$ is cyclic then it is abelian.

*Observations*

(i) CLAIM If $G$ is cyclic and $H \leq G$ then $H$ is cyclic also $G/H$ is cyclic.
Also: $(H \trianglelefteq G)$

PROOF

We only need to prove this for $\mathbb{Z}$ and $\mathbb{Z}_n$ , for some $n>0$

(a) if $G = \mathbb{Z}$ then $H = d\mathbb{Z}$ for some $d \in \mathbb{N}$. subgroup

INFINITE ORDER $\Big\{$ $G/H = \mathbb{Z} \longleftarrow$ If $d=0$ then $H = \{0\}$, so is cyclic

If $d>0$ then $H \xrightarrow{\sim} \mathbb{Z}$ ▶ $\mathbb{Z} \xrightarrow{\sim} 5\mathbb{Z}$

$a \mapsto \frac{a}{d}$

$G/H = \mathbb{Z}/d\mathbb{Z} \simeq \mathbb{Z}_d$

(b) If $G = \mathbb{Z}_n$

$\phi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_n$

if $\bar{H} \leq \mathbb{Z}_n$ , then we proved that $\bar{H} = H/n\mathbb{Z}$

for some $n\mathbb{Z} \leq H \leq \mathbb{Z}$

$H = d\mathbb{Z}$ for some $d \in \mathbb{N}$

$n = dn'$

$\bar{H} = d\mathbb{Z}/n\mathbb{Z} \leftarrow \mathbb{Z}/n\mathbb{Z}$

<u>CLAIM</u> $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} d\mathbb{Z}/n\mathbb{Z}$

$a \longrightarrow da$

$$\begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[dr, "\varphi"'] & d\mathbb{Z} \arrow[d] \\ & d\mathbb{Z}/n\mathbb{Z} \end{tikzcd}$$

$\alpha \in \ker \varphi \Leftrightarrow d\alpha + n\mathbb{Z} = 0 + n\mathbb{Z}$
$\Leftrightarrow d\alpha \in n\mathbb{Z}$
$\Leftrightarrow n \mid d\alpha \Leftrightarrow (\frac{n}{d} \mid \alpha)$
$\Leftrightarrow n' \mid \alpha \Leftrightarrow \alpha \in n'\mathbb{Z}$

$n = dn'$

$\ker \varphi = n'\mathbb{Z}$ (1st isomorphism)

$\mathbb{Z}/n'\mathbb{Z} \xrightarrow{\sim} d\mathbb{Z}/n\mathbb{Z} = \bar{H}$

So $\bar{H}$ is cyclic.

$\mathbb{Z}_n/\bar{H} = \mathbb{Z}_n / d\mathbb{Z}_n = \langle 1 + d\mathbb{Z}_n \rangle$

So $\mathbb{Z}_n/\bar{H}$ is cyclic.

If $G$ is cyclic, every subgroup and every quotient of $G$ is cyclic as well.

(ii) Suppose that $G$ is a cyclic group of order $n$. Then for every $d \mid n$ $G$ has a unique subgroup $H \leq G$ s.t. $|H| = d$.
Moreover, if $\langle g \rangle = G$ then $H = \langle g^{n/d} \rangle$

First of all if $H \leq G$ then by Lagrange, $|H| \mid |G| = n$

Suppose $d \mid n$

Let $H = \langle g^{n/d} \rangle$

$|H| = |\langle g^{n/d} \rangle| = |g^{n/d}|$

$= \min \{ a \mid \underbrace{(g^{n/d})^a = 1} \} = \min \{ a \mid g^{\frac{n \cdot a}{d}} = 1 \}$ $\qquad g^n = 1$

$= \min \{ a \mid n = |g| \mid (\frac{n \cdot a}{d}) \} = \min \{ a \mid n \mid (\frac{n \cdot a}{d}) \}$

$= \min \{ a \mid d \mid a \} = a$

Suppose $H' \leq G$ s.t. $|H'| = d$. Since $H' \leq G$, $H'$ is cyclic.

$\therefore \exists h' \in G = \langle g \rangle$ s.t $\langle h' \rangle = H'$

$\Rightarrow \exists h' = g^a$, for some $a$ s.t $\langle g^a \rangle = \langle h' \rangle = H'$

$d = |H'| = |\langle g^a \rangle| = |g^a| = \frac{n}{(n,a)}$ $\triangle$ CLAIM

Let $\alpha = \gcd(a,n) = (a,n)$
$a = \alpha \cdot a'$
$n = \alpha \cdot n'$ , $\alpha(a', n') = 1$

$\therefore (n,a) = \frac{n}{d}$

$\triangle$ <u>CLAIM</u>

$|g^a| = n' = \frac{n}{(a,n)} = \frac{|g|}{(a,|g|)}$

Proof of the claim

$$|g^a| = \min\{b \mid (g^a)^b = 1\}$$
$$= \min\{b \mid g^{ab} = 1\}$$
$$= \min\{b \mid n \mid ab\}$$
$$= \min\{b \mid (\alpha n') \mid (\alpha a' b)\}$$
$$= \min\{b \mid n' \mid a'b\}$$
$$= \min\{b \mid n' \mid b\} = n' = \frac{n}{(n,a)}$$
$((n',a')=1)$

■

Recall (Euclidean algorithm)

if $a,b \in \mathbb{Z}$ and $d=(a,b)$
$\exists\, x,y \in \mathbb{Z}$
$ax+by=d$

$\exists\, x,y \in \mathbb{Z}$, s.t.

⊛ $nx + ay = n/d$

WANT $\langle g^a \rangle = \langle g^{n/d} \rangle$

PROOF

$$g^{n/d} \overset{⊛}{=} g^{nx+ay} = (g^n)^x \cdot g^{ay} = (g^a)^y$$
$g^n = 1$

$\Rightarrow g^{n/a} \in \langle g^a \rangle$ $\quad \in \langle g^a \rangle$

$\Rightarrow H = \langle g^{n/a} \rangle \subseteq \langle g^a \rangle = H'$

But $|H| = |H'| = d$

$\underset{H \subseteq H'}{\Longrightarrow} H = H'$

---

(iii) Let $G$ be a finite group such that $|G| = p$ (prime number) then $G$ is a cyclic group

Hence $G \xrightarrow{\sim} \mathbb{Z}_p$

PROOF of (iii) $g \in G \setminus \{1\}$, $1 \neq |\langle g \rangle| \mid |G| = \text{prime}$

↳ Lagrange

$$\underset{p \text{ is prime}}{\Longrightarrow} |\langle g \rangle| = p = |G| \Rightarrow \langle g \rangle = G.$$

(iv) Suppose that $G$ is cyclic and $|G| = n$

Q: How many generators does $G$ have

(!) i.e $|\{g \mid \langle g \rangle = G\}| = ?$

▶ $\mathbb{Z}_6$ has two generators.

$\langle 1 \rangle$ $\langle 5 \rangle$

**DEF:** Let $\varphi: \mathbb{N}_{>0} \longrightarrow \mathbb{N}_{>0}$ be defined as $\varphi(n) := |\{m \mid 0 \le m < n,\ (m,n) = 1\}|$

$\varphi(p) = p - 1$
↳ if $p$ is prime.

$\boxed{1}$ $\varphi(1) = 1$ $\quad$ $\varphi(5) = 4$ $\boxed{1|2|3|4}$

$\boxed{1|\ }$ $\varphi(2) = 1$ $\quad$ $\varphi(6) = 2$ $\boxed{1|5}$

$\boxed{1|2}$ $\varphi(3) = 2$

$\boxed{1|3}$ $\varphi(4) = 2$

$$\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$$
prime

(!) $G = \langle g \rangle$

$$\left| \{ h \mid \langle h \rangle = G \} \right| = \left| \{ g^a \mid \langle g^a \rangle = G, \ 0 \le a < n \} \right|$$

$$= \left| \{ g^a \mid |\langle g^a \rangle| = |G| = n \} \right|$$

$$= \left| \{ a \mid \tfrac{n}{(n,a)} = n, \ 0 \le a < n \} \right|$$

Claim
$$|g^a| = \frac{n}{(a,n)}$$

$$= \left| \{ a \mid (n,a) = 1, \ 0 \le a < n \} \right| = \varphi(n)$$

□

Recall

$n \in \mathbb{N}_{>0}$, $\varphi(n) = |\{ r \mid 0 \le r < n, (r,n) = 1 \}|$

$\varphi(n) = \#$ of generators of $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

$\varphi(p^k) = p^k - p^{k-1}$

**DIRECT PRODUCT OF GROUPS**

Let $G_1, G_2$ be two groups, we define a group structure on $G_1 \times G_2 = \{ (g_1, g_2) \mid g_1 \in G_1 \text{ and } g_2 \in G_2 \}$

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

Direct product $G_1 \times G_2$ is another group

e.g. $(e_{G_1}, e_{G_2})$ is the identity of $G_1 \times G_2$

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$$

▶ $V = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{ (0,0), (0,1), (1,0), (1,1) \}$ ABELIAN GROUP BUT NOT CYCLIC

| + | (0,0) | (0,1) | (1,0) | (1,1) |
|---|---|---|---|---|
| (0,0) | (0,0) | | | |
| (0,1) | (0,1) | | | |
| (1,0) | | | | |
| (1,1) | | | | (0,0) |

If $\alpha \in V \setminus \{0,0\}$, then $|\alpha| = 2$

$|V| = 4$

$a^2 = I, \forall a$

Later we will show that up to isomorphism there are only two groups of order 4 : $\mathbb{Z}_4 \to$ cyclic group of order 4.

$\mathbb{Z}_2 \times \mathbb{Z}_2 (= V) \to$ Klein 4 group

CLAIM If $(n,m) = 1$, $\varphi(nm) = \varphi(n) \cdot \varphi(m)$

PROOF
$$\psi : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$$
$$a \to (a,a)$$

$$\psi(a+b) = (a+b, a+b) = (a,a) + (b,b) = \psi(a) + \psi(b)$$

$\psi$ is a homomorphism.

$$a \in \ker \psi \iff (a,a) = (0,0) \text{ in } \mathbb{Z}_n \times \mathbb{Z}_m$$
$$\iff n \mid a, \ m \mid a$$
$$\underset{(n,m)=1}{\iff} nm \mid a$$
$$\iff a = 0 \text{ in } \mathbb{Z}_{nm}$$

$$\Rightarrow \psi : \mathbb{Z}_{nm} \hookrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$$

$$\Rightarrow |\mathbb{Z}_{nm}| = nm = |\mathbb{Z}_n| |\mathbb{Z}_m|$$

$$\Rightarrow \psi : \mathbb{Z}_{nm} \xrightarrow{\sim} \mathbb{Z}_n \times \mathbb{Z}_m \quad (\text{If } (n,m) = 1)$$

$\varphi(nm) = \#$ of generators of $\mathbb{Z}_{nm}$

$= \#$ of generators of $\mathbb{Z}_n \times \mathbb{Z}_m$

CLAIM $(a,b)$ is the generator of $\mathbb{Z}_n \times \mathbb{Z}_m$

$\Leftrightarrow (a,n)=1$ and $(b,m)=1$

PROOF $(a,b)$ is a generator of $\mathbb{Z}_n \times \mathbb{Z}_m$

$\Leftrightarrow |(a,b)| = nm$

$|(a,b)| =$ the smallest $r$ s.t $(ra,rb)=(0,0)$

$=$ // // $n \mid ra$, $m \mid rb$

$=$ // // $\frac{n}{(n,a)} \mid r$ and $\frac{m}{(m,b)} \mid r$

$= \operatorname{lcm}\left(\frac{n}{(n,a)}, \frac{m}{(m,b)}\right)$

$= \frac{n.m}{(n,a)(m,b)}$

$(a,b)$ is a generator of $\mathbb{Z}_n \times \mathbb{Z}_m$

$\Leftrightarrow \frac{nm}{(n,a)(m,b)} = nm$

$\Leftrightarrow (n,a)(m,b)=1$

$\Leftrightarrow (n,a)=1 \quad (m,b)=1$ $\square$

$\#$ of generators of $\mathbb{Z}_n \times \mathbb{Z}_m = \varphi(n)\varphi(m)$

$= \#$ of generators of $\mathbb{Z}_{nm} = \varphi(nm)$ $\square$

$\varphi(p_1^{r_1} \cdots p_k^{r_k}) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k})$

$= (p_1^{r_1} - p_1^{r_1 - 1}) \cdots (p_k^{r_k} - p_k^{r_k - 1})$

## PERMUTATION GROUPS

$S_n = \{\sigma \mid \sigma : \{1,2,..n\} \to \{1,2,\dots n\}$ is a bijection$\}$

$(S_n, \circ)$ is a group.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

## CAYLEY'S THEOREM:

If $G$ is a finite group of order $n$, then $G$ is isomorphic to a subgroup of $S_n$.

PROOF Let $G$ be a group. Define a homomorphism

$\varphi : G \to \text{Perm}(G) \cong S_n$

Let $g \in G$ $\varphi(g)(x) = gx, \forall x \in G$

WANT

$\varphi(hg) = \varphi(h) \circ \varphi(g)$

CLAIM

$\varphi(g) \in \text{Perm}(G)$

PROOF

- $\varphi(g)$ is injective

  Because if $\varphi(g)(x) = \varphi(g)(y)$

  $\Rightarrow gx = gy$.

  $\Rightarrow x = y$

- $\varphi(g)$ is surjective

PROOF for WANT

$$(\varphi(h)\circ\varphi(g))(x)$$
$$= \varphi(h)(\varphi(g)(x)) = \varphi(h)(gx)$$
$$= h(gx) = (hg)(x) = \varphi(hg)(x)$$
□

- $g \in \ker\varphi \Rightarrow \varphi(g) = id$
$$\Rightarrow \varphi(g)(1) = id(1)$$
$$\Rightarrow g = 1$$

$\varphi$ is injective.

$$\Rightarrow G \hookrightarrow \mathrm{Perm}(G) \simeq S_n$$

▶ $(1\ 2\ 3) \in S_5$ is the permutation

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

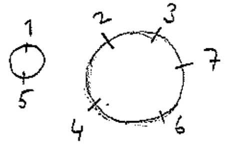
▶ $(1\ 3)(1\ 2) = (1\ 2\ 3)$

▨ 2-cycle is called a transposition

▶ $(3\ 4)(1\ 2)$ cannot be expressed as a cycle.

We will see that we can write every permutation in $S_n$ as a product of disjoint cycles. This decomposition is unique up to ordering $\Longrightarrow$ order does not matter.

▶ $$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 2 & 1 & 4 & 6 \end{pmatrix}$$




Order: $2.5 = 10$

▶ $(1\,9\,5)(2\,7\,4\,3\,6)(8)$ $\{1,9,5\}, \{2,7,4,3,6\}, \{8\}$ equivalence classes for $\sim_\sigma$

disjoint since $\{1,9,5\} \cap \{2,7,4,3,6\} = \emptyset$

Suppose that we are given $\sigma \in S_n$

Define an equivalence relation on $\{1,2,\dots,n\}$ s.t.

$$a \sim_\sigma b \Leftrightarrow \exists\, i \in \mathbb{Z} \text{ s.t. } \sigma(a) = b$$

Reflexive
Symmetric
Transitive

The equivalence relation decomposes $\{1,2,\dots,n\}$ into disjoint equivalence classes, i.e. → disjoint union

$$\{1,2,\dots,n\} = \{i_1,\dots,i_k\} \,\dot\cup\, \dots \,\dot\cup\, \{j_1,\dots,j_L\}$$

CLAIM

$\sigma|_{\{i_1,\dots,i_k\}}$ is a cycle. Let us define
$$i_2 = \sigma(i_1)$$
$$i_3 = \sigma(i_2)$$
$$\vdots$$
$$i_k = \sigma(i_{k-1})$$
$$i_1 = \sigma(i_k)$$

▶ $\{1,2,3,4\}$
$\sigma(1) = 3$
$\sigma(2) = 2$
$\sigma(3) = 4$
$\sigma(4) = 1$

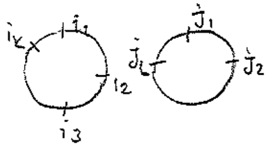
| | |
|---|---|
| First element | : 1 |
| 2nd // | : 3 |
| 3rd // | : 4 |
| 4th // | : 1 |

$$\sigma = (i_1\, i_2 \dots i_k) \cdots (j_1\, j_2 \cdots j_L)$$
disjoint decomposition

□

suppose we have a decomposition

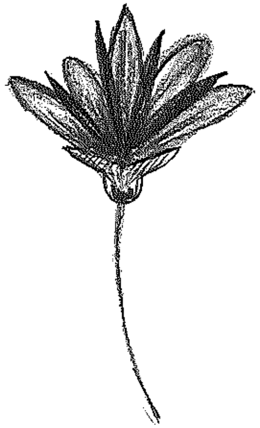
$\sigma = \gamma_1 \cdots \gamma_n$ s.t. $\gamma_1, \dots, \gamma_r$ are disjoint cycles.



If say

$\gamma_1 = (i_1, \dots, i_k)$ then $\{i_1, \dots, i_k\}$ is one of the equivalence classes for $\sim_\sigma$

Similarly, for the other cycles.



**Observation**

Suppose $g, h \in G$.
s.t. $gh = hg$
$\langle g \rangle \cap \langle h \rangle = \{1\}$
Also suppose $|g|, |h| < \infty$
then $|gh| < \infty$ and $|gh| = \mathrm{lcm}(|g|, |h|)$

**Warning**

The statement is not necessarily true if $gh \neq hg$

$\underset{g}{(1\,2)}\underset{h}{(1\,3)}$ $\quad gh = (1\,3\,2)$

$|g| = |h| = 2 \quad |gh| = 3$

$\langle g \rangle \cap \langle h \rangle = \{1\}$

PROOF Let $a = |g|$
$b = |h|$
$c = \mathrm{lcm}(a, b)$

WANT $|gh| = c$

PROOF

$(gh)^c = \underbrace{(gh)(gh)\dots(gh)}_{c \text{ times}}$

$= \underbrace{g \cdot g \cdot g \cdots g}_{c \text{ times}} \underbrace{h \dots h}_{c \text{ times}} = g^c h^c$

$= (g^a)^{\frac{c}{a}} (h^b)^{\frac{c}{b}}$

$= 1^{\frac{c}{a}} 1^{\frac{c}{b}} = 1$

so $|gh| \mid c$ (1)

suppose that

$(gh)^n = 1$

$\underset{gh=hg}{\Longrightarrow} g^n h^n$

$\Rightarrow g^n = h^{-n} \in \langle g \rangle \cap \langle h \rangle = \{1\}$

$\Rightarrow g^n = h^{-n} = 1$

$\Rightarrow a \mid n,\ b \mid n \Rightarrow c \mid n$ (2)

$c = \mathrm{lcm}(a, b)$

(1) + (2) $\Rightarrow |gh| = c$

## Observation

(i) $|(i_1 \dots i_k)| = k$

(ii) If $\sigma = \gamma_1 \dots \gamma_r$ is a product of disjoint cycles.

Then $|\sigma| = \text{lcm}(|\gamma_1|, \dots, |\gamma_r|)$
$= \text{lcm}(k_1, \dots, k_r)$

**PROPOSITION**

Every permutations $\sigma \in S_n$ can be written as a product of (not necessarily disjoint) transpositions.

PROOF

Let $\gamma \in S_n$ we can write $\sigma$ as a product of cycles

$$\sigma = (i_1 \dots i_k) \dots (j_1, \dots j_k)$$

Enough to show that every cycle can be written as a product of transpositions.

$$(i_1 \dots i_k)$$
$$= (i_1\, i_k) \dots (i_1\, i_3)(i_1\, i_2)$$

This decomposition is not unique. Moreover, the number of $r$ ($\sigma = \tau_1 \tau_2 .. \tau_r$) is not unique either.

However we will show that $(-1)^r$ is unique.

In other words, if

$\sigma = \tau_1, \dots \tau_r$
$= \gamma_1 \dots \gamma_j$

where $\tau_i, \gamma_j$ are transpositions.
then $(-1)^r = (-1)^s$, i.e $2 \mid \underbrace{(r-s)}_{\text{even}}$

$$(1\,2) = (1\,2)(2\,3)(3\,2)$$

We will define a homomorphism

$$\varepsilon : S_n \longrightarrow \underbrace{\{\pm 1\}}_{\text{group under multiplication}}$$

Let

$$\delta(x_1 \to x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

- if $n=2$
$\delta(x_1, x_2) = x_1 - x_2$

- $n=3$
$\delta(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$

Let $\sigma \in S_n$, $\varepsilon(\sigma) = \dfrac{\delta(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{\delta(x_1, \dots, x_n)} \in \{\pm 1\}$

- $\sigma = (1,2,3)$ Bunla başla, hepsini dolaş. (all pairs)

$$\varepsilon(\sigma) = \frac{\delta(x_2, x_3, x_1)}{\delta(x_1, x_2, x_3)} = \frac{(x_2 - x_3)(x_2 - x_1)(x_3 - x_1)}{(x_1 - x_2)(x_1 - x_2)(x_2 - x_3)} = +1$$

- Let $\tilde{\delta}(x_1, x_2, x_3) = (x_2 - x_1)(x_1 - x_3)(x_3 - x_2)$

$$\varepsilon(\sigma) := \frac{\tilde{\delta}(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})}{\tilde{\delta}(x_1, x_2, x_3)}$$

$$= \frac{(x_1 - x_2)(x_3 - x_1)(x_3 - x_2)}{(x_2 - x_1)(x_1 - x_3)(x_3 - x_2)} = +1$$

*Lemma*

Let $\gamma \in S_n$, then $\forall \sigma \in S_n$

$$\frac{\delta(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{\delta(x_1, x_2, \dots, x_n)} = \frac{\delta(x_{\sigma(\gamma(1))}, \dots, x_{\sigma(\gamma(n))})}{\delta(x_{\gamma(1)}, \dots, x_{\gamma(n)})}$$

PROOF of Lemma

$$f(x_{\sigma(1)},\dots,x_{\sigma(n)})$$

$$= \prod_{1\le i<j\le n} (x_{\gamma(i)} - x_{\gamma(j)})$$

$$= \pm \prod_{1\le i<j\le n} (x_i - x_j)$$

then

$$\frac{\sigma(f(x_{\gamma(1)},\dots,x_{\gamma(n)}))}{f(x_{\gamma(1)},\dots,x_{\gamma(n)})} = \frac{\gamma(\mp f(x_1,\dots,x_n))}{\pm f(x_1,\dots,x_n)} = \frac{\pm f(x_{\sigma(1)}\cdots x_{\sigma(n)})}{\pm f(x_1,\dots,x_n)}$$

$$= + \frac{f(x_{\sigma(1)},\dots,x_{\sigma(n)})}{f(x_1,x_2,\dots,x_n)}$$

□

▶ $f(x_1,x_2,x_3) = (x_1-x_2)(x_1-x_3)(x_2-x_3)$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad (x_2-x_1)(x_2-x_3)(x_1-x_3)$$

Let $\gamma, \sigma \in S_n$

$$\varepsilon(\sigma\gamma) = \frac{f(x_{\sigma\gamma(1)},\dots,x_{\sigma\gamma(n)})}{f(x_1,\dots,x_n)}$$

$$= \frac{f(x_{\sigma\gamma(1)},\dots,x_{\sigma\gamma(n)})}{f(x_{\gamma(1)}\cdots x_{\gamma(n)})} \frac{f(x_{\gamma(1)}\cdots x_{\gamma(n)})}{f(x_1,\dots,x_n)}$$

$$\underset{\text{Lemma}}{=} \frac{f(x_{\sigma(1)}\cdots x_{\sigma(n)})}{f(x_1,\dots,x_n)} \cdot \frac{f(x_{\gamma(1)},\dots,x_{\gamma(n)})}{f(x_1,\dots,x_n)}$$

$$= \varepsilon(\sigma)\,\varepsilon(\gamma)$$

HOMOMORPHISM

(*) Corollary

If $\tau_1,\dots,\tau_r = \theta_1\cdots\theta_s$ where

$\tau_1, \theta_s$ are transpositions then

$$(-1)^r = (-1)^s$$

PROOF

WANT:

If $\tau \in S_n$, and $\tau$ is a transposition then

$\varepsilon(\tau) = -1$

PROOF

suppose that

$$\tau = (i\ j) \qquad f = \begin{pmatrix} \cdots & i & \cdots & j & \cdots \\ \cdots & 1 & \cdots & 2 & \cdots \end{pmatrix}$$

$$f\tau f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots \\ 2 & 1 & 3 & 4 & \cdots \end{pmatrix} = (1\,2)$$

ADVANTAGE

$$\varepsilon((1\,2))$$

$$\varepsilon(f\tau f^{-1}) = \varepsilon(f)\varepsilon(\tau)\varepsilon(f^{-1})$$
$$= \varepsilon(f)\varepsilon(\tau)\varepsilon(f)^{-1}$$
$$= \varepsilon(\tau)$$

$$\varepsilon((1\,2)) = \frac{(x_2-x_1)(x_2-x_3)\cdots(x_{n-1}-x_n)}{(x_1-x_2)(x_1-x_3)\cdots(x_{n-1}-x_n)}$$

NOTE: $\varepsilon$ is sign.

(*) PROOF

$$(-1)^r = \varepsilon(\tau_1)\cdots\varepsilon(\tau_r) = \varepsilon(\tau_1\cdots\tau_r) = \varepsilon(\theta_1\cdots\theta_s)$$
$$= \varepsilon(\theta_1)\cdots\varepsilon(\theta_s)$$
$$= (-1)^s$$

**DEF**

We say that $\sigma$ is an even permutation (respectively odd)

if $\varepsilon(\gamma) = +1$ ( " $\varepsilon(\gamma) = -1$ )

Let $\ker(\varepsilon) = A_n \trianglelefteq S_n$ called the alternating group

$S_n / A_n \xrightarrow{\sim} \{\pm 1\}$ First Isomorphism

$(S_n : A_n) = 2$

- $A_3 = \{1, (123), (132)\}$

$A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$ daima cift

conjugate in $S_4$

$\underbrace{\sigma 1 \sigma^{-1}}_{1}$

1 is conjugate to itself only.

**DEF**

Let $G$ be a group then we say that $g_1$ and $g_2$ are conjugate in $G$, if $\exists \alpha \in G$ s.t.

$$\alpha^{-1} g_1 \alpha = g_2$$

equivalence relation

another notation: $g^{\alpha} = \alpha^{-1} g \alpha$

$(g^{\alpha})^{f} = g^{\alpha f}$

$(gh)^{\alpha} = g^{\alpha} h^{\alpha}$

Observation (Let $\sigma \in S_n$ — Permutation)

$$\underbrace{\sigma (i_1, \dots, i_r) \sigma^{-1}}_{\text{another notation } (i_1, \dots, i_r)^{\sigma^{-1}}} = (\sigma(i_1)\, \sigma(i_2)\, \sigma(i_3) \dots \sigma(i_r))$$

Rest is fixed!

- $n=4$ $\quad \sigma = (13)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$$\sigma (123) \sigma^{-1} = (341)$$

We can generalize as follows

$$\sigma \overbrace{(i_{11} \dots i_{1r_1})(i_{21} \dots i_{2r_2}) \dots (i_{n1} \dots i_{nr_n})}^{A} \sigma^{-1}$$

$$\overset{\text{NOTATION}}{=} [(i_{11} \dots i_{1r_1}) \dots (i_{n1} \dots i_{nr_n})]^{\sigma^{-1}}$$

$$= (i_{11} \dots i_{1r_1})^{\sigma^{-1}} \dots (i_{n1} \dots i_{nr_n})^{\sigma^{-1}}$$

$$= (\sigma(i_{11}) \dots \sigma(i_{1r_1})) \dots (\sigma(i_{n1}) \dots \sigma(i_{nr_n})) \quad (*)$$

If $A$ is a disjoint cycle decomposition then so is $(*)$

In other words, if $\gamma$ is a permutation with a disjoint cycle decomposition of type $r_1, \dots, r_k$ then so is $\gamma^{\sigma^{-1}}$ for any $\sigma \in S_n$

- $2, 2, 3, 4$

$\gamma = (32)(145)(69)(78\,10\,11)$ disjoint cycle decomposition

If $\sigma \in S_{11}$, $\gamma^{\sigma^{-1}}$ will also have a disjoint cycle decom of type $2, 2, 3, 4$

conversely suppose that $\gamma_1$ and $\gamma_2$ have the same disjoint cycle decomposition type.

Then is it true that $\gamma_1$ and $\gamma_2$ are conjugate, i.e. is it true that $\exists \sigma^{-1} \in S_n$, s.t.

$$\gamma_1^{\sigma^{-1}} = \gamma_2$$

$$\gamma_1 = (i_{11}, \dots, i_{1r}) \cdots (i_{k_1} \cdots i_{kr})$$

$$\gamma_2 = (j_{11} \cdots j_{1r}) \cdots (j_{k_1} \cdots j_{kr})$$

s.t. $i_{\alpha\beta} \neq i_{\alpha'\beta'}$ if $\alpha \neq \alpha'$ OR $\beta \neq \beta'$

also $J_{\alpha\beta} \neq J_{\alpha'\beta'}$ if $\alpha \neq \alpha'$ OR $\beta \neq \beta'$

Let be s.t

$$\sigma(i_{\alpha\beta}) = J_{\alpha\beta}$$

and $\sigma$ sends the other elements arbitrarily s.t. $\sigma$ is a permutation of $\{1, \dots, n\}$

$$\gamma_1^{\sigma^{-1}} = (\sigma(i_{11}) \cdots \sigma(i_{1r_1})) \cdots (\sigma(i_{k_1}) \cdots \sigma(i_{kr_k}))$$

$$= (J_{11} \cdots J_{1r_1}) \cdots (J_{k1} \cdots J_{kr_k})$$

$$= \gamma_2$$

$\gamma_1, \gamma_2 \in S_n$ are conjugate in $S_n$
$\Leftrightarrow$ $\gamma_1$ and $\gamma_2$ have the same disjoint cycle decomposition type.

▶ Determine all the conjugacy classes (i.e. the equivalence classes of elements which are conjugate to each other) in $S_4$.

| | |
|---|---|
| $\{1\}$ | 1 |
| $\{(12), (13) \dots\}$ | 6 |
| $\{(12)(34), \dots\}$ | 3 |
| $\{(123), \dots\}$ | 8 |
| $\{(1234) \dots\}$ | 6 |

▶ $A_4$ (Page 24)

$|A_4| = 12$

$A_4$ is non-abelian.

$(124)(123) \neq (123)(124)$

Let

$$V = \{1, \underbrace{(12)(34)}_{a}, \underbrace{(13)(24)}_{b}, \underbrace{(14)(23)}_{c}\}$$

CLAIM $V \trianglelefteq A_4$

$a^2 = b^2 = c^2$

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

V forms an abelian group of order 4.

$$V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

$(12)(34) \longrightarrow (0,0)$
$(13)(24) \longrightarrow (1,0)$
$(14)(23) \longrightarrow (0,1)$
$(14)(23) \longrightarrow (1,1)$

$\left.\begin{array}{l}\mathbb{Z}_p \times \mathbb{Z}_p \\ \text{or} \\ \mathbb{Z}_{p^2}\end{array}\right\}$ ABELIAN

Recall that by Lagrange Theorem,

if $H \leq A_4$ then

$|H| \mid |A_4| = 12$

We will show that the naive converse to Lagrange Theorem need not be true. In fact $A_4$ does not have a subgroup of order 6.

Suppose that

$H \leq A_4$ and $|H| = 6$

$\Rightarrow (A_4 : H) = 2 \Rightarrow H \trianglelefteq A_4$

$1 \in H$ and $H$ has to contain an element of the form

$(i\ j\ k)$

$\longrightarrow$ Let represent it as $(1\ 2\ 3)$

$(123) \in H \Rightarrow (132) \in H$

Let $\sigma = (12)(34) \in A_4$ $\longrightarrow$ since $H$ is normal subgroup and $\sigma$ is element of $A_4$. ($\blacktriangleright$ $gHg^{-1}$)

$\sigma(123)\sigma^{-1} = (214) \in H$

$\Downarrow$

$(241)^{(\text{karesi})} \in H$

since $H \trianglelefteq A_4$.

$\tau = (13)(24) \in A_4$

$\tau(123)\tau^{-1} = (341) \in H \Rightarrow (314) \in H$

$1, (123), (132), (214), (241), (341), (314) \in H$

so such a subgroup $H \leq A_4$ w/ $|H| = 6$ does not exist.

# DIRECT PRODUCT OF GROUPS AND THE FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUP.

**DEF:** Let $G_1, \dots, G_n$ be groups. The direct product (direct sum) of $G_1, \dots, G_n$, is the cartesian product.

$G_1 \times \dots \times G_n = \{(g_1 \dots g_n) \mid g_i \in G_i\}$

together with the operation.

$(g_1 \dots g_n) \cdot (h_1 \dots h_n)$

$= (g_1h_1, g_2h_2, \dots, g_nh_n)$

$\in G_1 \times \dots \times G_n$

This makes $G_1 \times \dots \times G_n$ a group.

Observation

If $|g| < \infty$ for all $1 \leq i \leq n$

$|(g_1 \dots g_n)| = \operatorname{lcm}(|g_1| \dots |g_n|)$

Let $|g_i| = r_i$ and let $r = \operatorname{lcm}(r_1, \dots, r_n)$

WANT

$r = |g|$

PROOF

$(g_1, \dots g_n)^a = 1$

$\Leftrightarrow (g_1^a, \dots, g_n^a) = (1, 1, 1, \dots)$

$\Leftrightarrow g_i^a = 1$, for all $1 \leq i \leq n$

$\Leftrightarrow |g_i| \mid a$ for all $1 \leq i \leq n$

$\Leftrightarrow r_i \mid a$ for all $1 \leq i \leq n$

$\Leftrightarrow r \mid a$

$r = |(g_1, \dots, g_n)|$

▶ (i) $(2,6) \in \mathbb{Z}_4 \times \mathbb{Z}_{12}$
(ii) $(2,3) \in \mathbb{Z}_6 \times \mathbb{Z}_{15}$
(iii) $(8,10) \in \mathbb{Z}_{12} \times \mathbb{Z}_{18}$
(iv) $(3,10,9) \in \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$
(v) $(3,6,12,16) \in \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$

} NOT CYCLIC

(i) $|(2,6)| = \operatorname{lcm}(|2|, |6|)$

$$= \operatorname{lcm}\left(\frac{4}{(4,2)}, \frac{12}{(6,12)}\right)$$

$$= \operatorname{lcm}(2,2) = 2$$

(ii) 15

(iii) 9

(iv) 60

(v) 60

□ $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ is a cyclic group

$\Leftrightarrow (m_i, m_j) = 1$ for every $i \neq j$

PROOF

($\Leftarrow$) $|(1,1,1,1)| = \operatorname{lcm}((1)(1)\cdots(1))$

$$= \operatorname{lcm}(m_1, m_2, \dots m_r)$$

$$= m_1 \cdot m_2 \cdots m_r$$

Since $(m_i, m_j) = 1$ for every $i \neq j$

$$|\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}| = |\mathbb{Z}_{m_1}| \cdots |\mathbb{Z}_{m_r}|$$

$$= m_1 \cdots m_r$$

$$\langle (1, \dots, 1) \rangle = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cdots \times \mathbb{Z}_{m_r}$$

so

$\mathbb{Z}_{m_1} \times \dots \mathbb{Z}_{m_r}$ is cyclic hence

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_r} \simeq \mathbb{Z}_{m_1 m_2 \dots m_r}$$

($\Rightarrow$) If $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r}$ is cyclic then $\exists (a_1, \dots, a_r) \in \mathbb{Z}_{m_1} \times \dots \mathbb{Z}_{m_r}$

s.t.

$$\operatorname{lcm}\left(\frac{m_1}{(m_1, a_1)}, \dots \frac{m_r}{(m_r, a_r)}\right) = |(a_1 \dots a_r)| = |\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r}|$$

$$\Rightarrow \operatorname{lcm}(m_1, \dots m_r) = m_1 \dots m_r$$

$$\Rightarrow (m_i, m_j) = 1 \quad \text{for} \quad i \neq j$$

▶ $\mathbb{Z}_3 \times \mathbb{Z}_{77} \times \mathbb{Z}_{26} \simeq \mathbb{Z}_{3 \times 77 \times 26}$

**THEOREM** *Fundamental Theorem*

Let $A$ be a finitely generated Abelian group then

$A$ is isomorphic to a group of type

$$\underbrace{\mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}}_{r \text{ times}} \times (\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_1^{r_2}} \times \dots \times \mathbb{Z}_{p_1^{r_{k_1}}})$$
$$\times (\mathbb{Z}_{p_2^{s_1}} \times \dots \times \mathbb{Z}_{p_2^{s_{k_2}}})$$
$$\times$$
$$\times (\mathbb{Z}_{p_\ell^{t_1}} \times \dots \mathbb{Z}_{p_\ell^{t_{k_\ell}}})$$

s.t.

$p_i$ are prime   $r_1 \leq r_2 \leq \dots \leq r_{k_1}$
$p_1 < p_2 \dots < p_\ell$ and   $s_1 \leq s_2 \leq \dots \leq s_{k_2}$
  $t_1 \leq t_2 \leq \dots \leq t_{k_\ell}$

and this decomposition is unique.

**DEF** $r$ is called the rank of $A$ (book calls it Betti number)

We can also write $A$ in the statement as

$$\mathbb{Z} \times \dots \times \mathbb{Z} \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_g}$$

with $m_1 | m_2 | m_3 \dots | \underbrace{m_g}_{r}$

This is also unique

**III** If $A$ is abelian, and

$|A| = n < \infty$

if $m \mid n$ then

$A$ has a subgroup of order $m$.

PROOF

$$A = (\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_1^{r_k}}) \times \dots \times (\mathbb{Z}_{p_\ell^{t_1}} \times \dots \times \mathbb{Z}_{p_\ell^{t_{k_\ell}}})$$

$(r=0)$

$n = |A| = p_1^{r_1} \cdots p_\ell^{r_\ell} \cdots p_\ell^{t_1} \cdots p_\ell^{t_{k_\ell}}$

$m \mid n \quad m = p_1^{r_1'} \cdots p_\ell^{t_\ell'}$

$r_1' \le r_1$
$r_2' \le r_2$
$\vdots$
$t_{k_\ell}' \le t_{k_\ell}$

$\boxed{\langle p_1^{r_1 - r_1'} \rangle \le \mathbb{Z}_{p_1^{r_1}}}$, $|\langle p_1^{r_1-r_1'} \rangle| = p_1^{r_1'}$

$B = \langle p_1^{r_1 - r_1'} \rangle \times \langle p_1^{r_2 - r_2'} \rangle \times \dots \times \quad \le A$

$|B| = p_1^{r_1'} \cdots p_\ell^{t_{k_\ell}} = m$

$\square$

▶ Find all abelian groups up to isomorphism of order 72.

$72 = 2^3 \cdot 3^2$

$\mathbb{Z}_{2^3}$ $\qquad$ $\mathbb{Z}_{3^2}$

$\mathbb{Z}_2 \times \mathbb{Z}_{2^2}$ $\qquad$ $\mathbb{Z}_3 \times \mathbb{Z}_3$

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

▶ Determine which abelian group is

$$A = \mathbb{Z}_6 \times \mathbb{Z}_{12} / \langle (3,4) \rangle$$

isomorphic to?

$|\langle (3,4) \rangle| = |(3,4)|$

$= \operatorname{lcm}\left(\frac{6}{(6,3)}, \frac{12}{(4,12)}\right)$

$= \operatorname{lcm}(2,3) = 6$

72 distinct pair

$$\left| \mathbb{Z}_6 \times \mathbb{Z}_{12} / \langle (3,4) \rangle \right| = \frac{6 \cdot 12}{6} = 12 \longleftarrow$$

So $A$ is isomorphic to either $\mathbb{Z}_{2^2} \times \mathbb{Z}_3$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

this has an element of order 4 $\qquad$ this does not have

Does $A$ have an element of order 4?

if $(a,b) \in A$ in of order 4 then

$4(a,b) = 0$ in $A$ but $2(a,b) \neq 0$ in $A$

$(4a, 4b) \in \langle (3,4) \rangle = \{(0,0)(3,4)(0,8)(3,0)(0,4)(3,8)\} \Rightarrow (4a,4b) = (0,0)$ $(0,8)$ or $(0,4)$

Let $(a,b) = (0,1)$ then $4(a,b) = 4(0,1) = (0,4) \in \langle (3,4) \rangle$

but $2(a,b) = 2(0,1) = (0,2) \notin \langle (3,4) \rangle$

**DEF:**

We say that a group $G$ is simple if

$N \trianglelefteq G \Rightarrow N = \{1\}$ or $N = G$

▶ If $|G| = p$, then $G$ is simple

Let $N \trianglelefteq G$

$|N| \mid |G| = p$

$\Rightarrow |N| = 1 \Rightarrow N = \{1\}$

$|N| = p \quad N = \{G\}$

**DEF:**

Let $G$ be a group

$Z(G) = \{g \in G \mid gh = hg, \forall h \in G\}$

$Z(G) \leq G$

if $g \in Z(G)$ and $\alpha \in G$

$g^\alpha = \alpha^{-1} g \alpha = g \in Z(G)$

$Z(G)^\alpha = Z(G), \forall \alpha \in G$

$\Rightarrow Z(G) \trianglelefteq G$

↳ center of $G$.

▨ $G$ is abelian $\Leftrightarrow Z(G) = G$

$Z(G)$ measures how close to being abelian $G$.

**DEF:** Let $g, h \in G$

$[g,h] = ghg^{-1}h^{-1} \in G$

↳ called the commutator of $g$ and $h$

*Note*

$gh = hg \Leftrightarrow [g,h] = 1$

$[G,G] = \langle [g,h] \mid g,h \in G \rangle$ is called the commutator subgroup of $G$.

__Claim__

$[G,G] \trianglelefteq G$

__PROOF__

$[g,h]^\alpha = (ghg^{-1}h^{-1})^\alpha$

$= g^\alpha h^\alpha (g^\alpha)^{-1} (h^\alpha)^{-1} = [g^\alpha, h^\alpha]$

Let $x \in [G,G]$

$\Rightarrow x = [g_1,h_1]^{\varepsilon_1} \cdots [g_n,h_n]^{\varepsilon_n}$ w/ $\varepsilon_i \in \mathbb{Z}$

$x^\alpha = ([g_1,h_1]^{\varepsilon_1} \cdots [g_n,h_n]^{\varepsilon_n})^\alpha = [g_1^\alpha, h_1^\alpha]^{\varepsilon_1} \cdots [g_n^\alpha, h_n^\alpha]^{\varepsilon_n}$

$= [G,G]$

● $[G,G] \trianglelefteq G$

$G$ is abelian $\Rightarrow [G,G] = \{1\}$

__PROPOSITION__

$G/[G,G]$ is abelian.

__PROOF__

Let $x[G,G], y[G,G] \in G/_{[G,G]}$

__WANT__

$[x[G,G], y[G,G]] = 1$ in $G/_{[G,G]}$

$\Leftrightarrow x[G,G]\, y[G,G]\, (x[G,G])^{-1} (y[G,G])^{-1} = 1[G,G]$ in $G/[G,G]$

$\Leftrightarrow [x,y] = [G,G] = 1[G,G]$ in $G/[G,G]$

$\Leftrightarrow [x,y] \in [G,G]$ □

**THEOREM**

$A_n$ is simple for $n \geq 5$

*Recall*

Note that $A_4$ is not simple.

$$V = \{1, (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4$$

PROOF

- $A_n$ is generated by 3-cycles.

Let $\sigma \in A_n$, we know that $\sigma$ can be written as a product of an even number of transpositions.

Therefore it is enough to show that a product of two transpositions can be written as a product of 3-cycles.

CASE 1: $(ik)(ij) = 1 = (ijk)(ikj)$

CASE 2: $(ij)(ik) = (ikj)$

CASE 3: $(ij)(k\ell) = (ikj)(k\ell i)$

$\therefore$ $A_n$ is generated by 3-cycles.

- Any two 3-cycles in $A_n$ are conjugate to each other in $A_n$.

Let $(ijk)$ and $(i'j'k')$ be two 3 cycles in $A_n$.

Know $\exists\, \sigma \in S_n$ s.t. $(ijk)^\sigma = (i'j'k')$

If $\sigma \in A_n$ then we are done.

So suppose $\sigma \notin A_n \Rightarrow \sigma$ is odd.

Let $\{r,s\} \cap \{i',j',k'\} = \emptyset$

$\sigma(rs) \in A_n$

$$(ijk)^{\sigma(rs)} = \left((ijk)^\sigma\right)^{(rs)} = (i'j'k')^{(rs)} = (i'j'k')$$

$\therefore$ $(i'j'k')$ and $(ijk)$ are conjugate in $A_n$ $\square$

CLAIM

If $N \trianglelefteq A$ and $N$ contains a 3-cycle $\Rightarrow N = A_n$.

PROOF

Since $N \trianglelefteq A_n$, $\forall \sigma \in A_n$

$N^\sigma = N \Rightarrow$

if $(ijk) \in N \Rightarrow (ijk)^\sigma \in N$ $\forall \sigma \in A_n$

$\Rightarrow$ since $\forall (i'j'k')$ $\exists\, \sigma \in A_n$ s.t. $(i'j'k') = (ijk)^\sigma$

So suppose

$1 \neq N \trianglelefteq A_n$

Let $1 \neq \sigma \in N$ s.t. $\sigma$ fixes the maximal # of elements in $\{1, 2, \dots, n\}$

We want to show that $\sigma$ is a 3 cycle.

Look at the disjoint cycle decomposition of $\sigma$.

(i) If this dec. contains a cycle w/ at least 5 elements.

$\sigma = (1234\dots)$

$$\gamma = \underbrace{(132)\left[(12345\dots)\dots\right](123)}_{\in N}\sigma^{-1}$$

$$= \left[(31245\dots)\dots\right]\sigma^{-1}$$

$$= \left[(31245\dots)\dots\right](54321\dots)(\dots$$

$$\dots(\dots)\cdot(22)\dots \in N$$

$$\neq I$$

This new element $\gamma \neq 1 \in N$ and fixes more elements than $\sigma$.

$\times$

(ii) There is an orbit in $\sigma$ that contains exactly 3 elements and another orbit.

$\sigma = (123)(45\dots)\dots$

$\gamma = \left[(123)(45\dots)\right]^{(145)}\sigma^{-1} \in N$

$= (523)(\dots)\sigma^{-1} \in N$

$= \dots(33)$

$\neq 1$

$\gamma$ fixes more elements than $\sigma$

(iii)

There are at least two transpositions appearing in $\sigma$:

$$\sigma = (12)(34)\cdots$$

$$1 \neq \underset{\substack{\| \\ (51)(34)\cdots\sigma^{-1}}}{\sigma^{(125)}\cdot\sigma^{-1}} \in N$$

$(51)(34)\ldots\sigma^{-1} \in N$

fixes at least two more elements than $\sigma$.

**EXAM**

1)(a) Let $A$ be an abelian group w/ $H, K \leq A$ s.t. $|H|=r, |K|=s$, $(r,s)=1$ and $H$ and $K$ are cyclic. Show that $A$ has a cyclic subgroup of order $rs$.

HAVE

$\langle h\rangle = H$, $\langle k\rangle = K$, $|h| = |\langle h\rangle| = |H| = r$
$|k| = |\langle k\rangle| = |K| = s$

CLAIM

$|hk| = rs$

PROOF

Need to show that two things.

(i) $(hk)^{rs}=1$ ✓

(ii) If $(hk)^n = 1$ then $rs \mid n$.

(i) $\underbrace{(hk)^{rs} = h^{rs}k^{rs}}_{\text{since } A \text{ is abelian}} = (h^r)^s \cdot (k^s)^r$

$= 1^s \cdot 1^s = 1$

(ii) If $(hk)^n = 1 \Rightarrow h^n = k^{-n} \in H\cap K$

$|H\cap K| \mid |H| = r$
$|H\cap K| \mid |K| = s$ $\xRightarrow[(r,s)=1]{} |H\cap K| = 1$

$H\cap K = \{1\}$

$\Rightarrow h^n = k^{-n} \in H\cap K = \{1\}$

$\Rightarrow h^n = k^{-n} = 1$

$\Rightarrow h^n = 1,\ k^{-n} = 1 \Rightarrow r\mid n$ and $s \mid n \xRightarrow[(r,s)=1]{} rs \mid n$

□

---

$|\langle hk\rangle| = |hk| = rs$

$\langle hk\rangle$ is a subgroup of order $n$.

$|h| = r$, $|k| = s$ and $(r,s)=1$ and $hk = kh$ then $|hk| = rs$

(b) Prove that this need not be true if $r$ and $s$ are <u>not</u> relatively prime

Take $A = V = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2}_{\text{This is abelian}}$

$r = s = 2$

It has cyclic subgroups of order $r$ and $s$. But no cyclic subgroup of order 4.

2) Prove $(\mathbb{C}^\times, \cdot)$ and $(\mathbb{R}, +)$ are not isomorphic.

Suppose that they are isomorphic then $\exists\, \phi: \mathbb{C}^\times \to \mathbb{R}$ which is an isomorphism.

$-1 \in \mathbb{C}^\times$ has order 2.

$\Rightarrow \phi(-1)$ has order 2 in $\mathbb{R}$.

$(\mathbb{R}, +)$ does not have any element of order 2 since $x + x = 0 \Rightarrow x = 0$ in $\mathbb{R}$.

3) Show that if $\sigma \in S_n$ is a cycle of odd order then so is $\sigma^2$

$\sigma = (a_1\ a_2 \dots a_{2k+1})$

$\sigma^2 = (a_1 a_3 a_5 \dots a_2 a_4 \dots)$

4) $A = (\mathbb{Z}_4 \times \mathbb{Z}_{12}) / (\langle 2\rangle \times \langle 2\rangle)$ as a product of cyclic groups.

$|\langle 2\rangle \times \langle 2\rangle| = |\langle 2\rangle| \cdot |\langle 2\rangle|$
$= |\{0,2\}| \cdot |\{0,2,4,6,8,10\}|$
$= 12$

$|A| = \frac{4 \cdot 12}{12} = 4$

$A \simeq \mathbb{Z}_4$
OR
$\mathbb{Z}_2 \times \mathbb{Z}_2$

Let $(a,b) + (\langle 2\rangle \times \langle 2\rangle) \in A$
$2(a,b) + (\langle 2\rangle \times \langle 2\rangle)$
$= (2a, 2b) + (\langle 2\rangle \times \langle 2\rangle)$
$= 0 + (\langle 2\rangle \times \langle 2\rangle)$
So if $a \in A$, $|a| = 1$ OR $2$

$\Rightarrow A \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

5) Is there a non-zero homomorphism $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_5$ ?

Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_5$ be a homomorphism

$\mathbb{Z}_{12}/\ker\phi \simeq \operatorname{im}(\phi) \leq \mathbb{Z}_5$

$\Rightarrow |\operatorname{im}\phi| \mid |\mathbb{Z}_5| = 5$

$\Rightarrow |\operatorname{im}\phi| = 1$ OR $|\operatorname{im}\phi| = 5$

$\Rightarrow$ if $|\operatorname{im}\phi| = 1$ then $\phi$ is the 0 homomorphism.

Suppose $|\operatorname{im}\phi| = 5$ $\quad \frac{12}{\ \ } = |\mathbb{Z}_{12}/\ker\phi| = 5$

# GROUP ACTIONS ON SETS

**DEF:** Let $G$ be a group and $X$ be a set. Then an action of $G$ or $X$ is a function:

$$G \times X \to X$$
$$(g, x) \longrightarrow g * x$$

s.t

(i) $e * x = x$, for every $x \in X$

(ii) for every $g_1, g_2 \in G$ and $x \in X$

$$(g_1 \cdot g_2) * x = g_1 * (g_2 * x)$$

► (i) If $G$ is a group then $G$ acts on itself.

$$G \times G \longrightarrow G$$
$$(g, x) \longrightarrow gx$$

► (ii) Let $H \leq G$, then $G$ acts on $\underbrace{\mathcal{L}_H(G)}_{\text{only a set}}$

$$G \times \mathcal{L}_H(G) \longrightarrow \mathcal{L}_H(G)$$

$$\ell * (kH) \longrightarrow (\ell k) \cdot H$$

$e * (kH) = (ek)H = kH$ (i)✓

$(\ell_1 \ell_2) * (k \cdot H) = (\ell_1 \ell_2) kH = \ell_1 (\ell_2 k) H$
$= \ell_1 * ((\ell_2 \cdot k) \cdot H) = \ell_1 * (\ell_2 * kH)$ (ii)✓

**Observation** — $\triangleright$ R to plane

(i) Suppose that G acts on X. We have

$$G \times X \to X$$
$$(g, x) \to g * X$$

CLAIM

fix $g \in G$

Let $\tau_g : X \to X$

$$\tau_g(x) := g * x$$

Then $\tau_g$ is a bijection — faithful

PROOF

$$(\tau_{g^{-1}} \circ \tau_g)(x)$$
$$= \tau_{g^{-1}}(\tau_g(x))$$
$$= \tau_{g^{-1}}(g * x)$$
$$= g^{-1} * (g * x)$$
$$= (g^{-1} \cdot g) * x$$
(ii)
$$= e * x$$
$$= x$$
(i)

$$\tau_{g^{-1}} \circ \tau_g = id$$
$$\Rightarrow \tau_g \circ \tau_{g^{-1}} = id$$
$$\therefore \tau_g = (\tau_{g^{-1}})^{-1}$$

So $\tau_g$ is a bijection.

(ii) Suppose that G acts on X.

Then $G \longrightarrow \text{Perm}(X)$

$$:= \{ f \mid f : X \to X \text{ s.t. } f \text{ is a bijection} \}$$

$$\phi : g \longrightarrow \tau_g$$

$\phi$ is a homomorphism

$$\phi(gh)(x) = \tau_{gh}(x)$$
$$= (gh) * x$$
$$\underset{(ii)}{=} g * (h * x) = g * (\tau_h(x)) = \tau_g(\tau_h(x))$$
$$= (\tau_g \circ \tau_h)(x)$$
$$= (\phi(g) \circ \phi(h))(x)$$

$\forall x \in X$

$\Rightarrow \phi(gh) = \phi(g) \cdot \phi(h)$

So $\phi$ is a homomorphism.

---

Therefore, if G acts on X, then we get a homomorphism

$$\phi : G \longrightarrow \text{Perm}(X)$$

Conversely, let G be a group and $\phi : G \to \text{Perm}(X)$ be any homomorphism, then we can define an action of G on X:

$$g * x = \phi(g)(x)$$

(i) $e * x = \phi(e)(x) = id(x) = x$

Homomorphism then $\phi(e) = id$

(ii) $(g \cdot h) * x = \phi(g \cdot h)(x) = (\phi(g) \circ \phi(h))(x)$

$$= \phi(g)(\phi(h)(x)) = \phi(g)(h * x) = g * (h * x)$$

$\square$

"An action of G on X is the same thing as a homomorphism
$G \longrightarrow \text{Perm}(X)$"

We say that the action of G on X is *faithful*
if $\phi : G \longrightarrow \text{Perm}(X)$
is injective

($\Leftrightarrow$ if $\phi(g) = id$ then $g = 1$
$\Leftrightarrow$ if $\phi(g)(x) = x, \forall x \in X$ then $g = 1$
$\Leftrightarrow$ if $g * x = x, \forall x \in X$ then $g = 1$)

We say that the action is *transitive* if given any $x, y \in X$
$\exists g \in G$, s.t $g * x = y$

"iki eleman alsam birini diğerine götüren bir eleman var mı?"

OBSERVATION

If $G \leq S_n = \text{Perm}(\{1, 2, \dots\})$
then G acts on $\{1, 2, \dots, n\}$

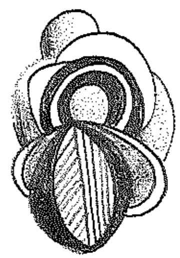
(i) $V = \{1, (12)(34), (13)(24), (14)(23)\} \leq S_4$

V acts on $\{1,2,3,4\}$ set

$(12)(34) * 1 = 2$
$(12)(34) * 2 = 1$
$(12)(34) * 3 = 4$
$(12)(34) * 4 = 3$

Look at each one

Is this action transitive?
Yes.



(ii) $\{1, (123), (132)\} \leq S_4$

$\{1, (123), (132)\}$ acts on $\{1, 2, 3, 4\}$
This action is not transitive.

(iii) Let $G = \mathbb{Z}$ and $X = \{a, b\}$

$\phi : \mathbb{Z} \longrightarrow \text{Perm}(X)$
$\phi(z) = id, \forall z \in \mathbb{Z}$
This is not faithful.

Observation

Suppose that G acts on X. Then we have an equivalence relation on X:

$$x \sim y \Leftrightarrow \exists g \in G \text{ s.t } g * x = y$$

This is an equivalence relation. So this partitions X into equivalence classes $[x]$ for $x \in X$

$[x]$ is called the orbit of x under G
There is a single orbit in X $\Leftrightarrow$ the action of G on X is transitive.

▶ $G = \{1, (12), (34), (12)(34)\} \leq S_4$
then G acts on $\{1, 2, 3, 4\}$

$$\{1,2,3,4\} = \{1,2\} \,\dot\cup\, \{3,4\}$$
$$= [1] \,\dot\cup\, [3]$$

- Let $G = \langle \sigma \rangle \leq S_n$

  then the equivalence classes in $\{1, 2, \dots, n\}$ under the action of $G$

  are the sets that appear in the disjoint cycle decomposition of $\sigma$.

- $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{l} a, b, c, d \in \mathbb{R} \\ ad - bc \neq 0 \end{array} \right\} = GL_2(\mathbb{R})$

- $\mathcal{H} := \{ z \in \mathbb{C} \mid \operatorname{Im}(z) > 0 \}$

  upper half plane

  $G \times \mathcal{H} \to \mathcal{H}$

  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} * z = \dfrac{az + b}{cz + d}$

Recall

$[x] = Gx$ New notation

**NOTATION / DEFINATION**

Given $x \in X$

$G_x = \{ g \in G \mid gx = x \}$

(stabilizer of $x$ is $G$ (= isotropy group of $G$)

PROPOSITION

$G_x \leq G$

PROOF

- $e \in G_x$, since $ex = x$
- if $g, h \in G_x$, then $gx = x$ and $hx = x$

Since $hx = x$

$x = ex$

$(h^{-1}h)x = h^{-1}(hx) = h^{-1}x$

$\Rightarrow h^{-1}x = x$

$(gh^{-1})x = g(h^{-1}x) = gx = x$

$h^{-1}x = x$

$\Rightarrow gh^{-1} \in G_x$

$\therefore G_x \leq G$

PROPOSITION

There is a natural 1-1, correspondence between

$\mathcal{L}_{G_x}(G)$ and $Gx$

COROLLARY

$(G : G_x) = |Gx|$

PROOF

$(G : G_x) = |\mathcal{L}_{G_x}(G)| = |Gx|$

PROOF

$$\mathcal{L}_{G_x}(G) = \{ g\, G_x \mid g \in G \} \underset{\alpha}{\overset{\beta}{\rightleftarrows}} Gx = \{ gx \mid g \in G \}$$

$\alpha(g . G_x) = gx$

$\beta(g . x) = g G_x$

Well-defined

- If $gG_x = g'G_x$ then $g^{-1}g' \in G_x \Rightarrow (g^{-1}g').x \Rightarrow g'x = gx$

  $\Rightarrow \alpha(gGx) = \alpha(g'Gx)$

- If $gx = g'x$ then $g^{-1}g'x = x \Rightarrow g^{-1}g' \in G_x \Rightarrow g'G_x = gG_x$

  $\Rightarrow \beta(gx) = \beta(g'x)$

- $(\beta \circ \alpha)(gG_x) = \beta(\alpha(g.G_x)) = \beta(gx) = gG_x \quad \therefore \beta \circ \alpha = id$

- $(\alpha \circ \beta)(gx) = \alpha(\beta(gx)) = \alpha(g.G_x) = gx \quad \therefore \alpha \circ \beta = id$

So $\alpha$ and $\beta$ are inverses of each other.

**DEF** Let $X_G = \{x \in X \mid gx = x, \forall g \in G\}$ $\longrightarrow$ $X_G = \{x \in X \mid Gx = \{x\}\}$
$= \{x \in X \mid G_x = G\}$

the set of fixed points of $X$ under the $G$-action.

Corollary

If $|X|, |G| < \infty$ then $|[x]| = |Gx| \mid |G|$

Proof

$|Gx| = (G:G_x) \mid |G|$

Observation

Suppose $|X|, |G| < \infty$

$X = \bigsqcup_{i \in I} Gx_i$

$= \dot{\bigcup}_{i \in A} Gx_i \sqcup \bigsqcup_{i \in B} Gx_i = X_G \sqcup \bigsqcup_{i \in B} Gx_i$

s.t. $|Gx_i| = 1$, for all $i \in A$ and $|Gx_i| > 1$ for all $i \in B$ such that $|Gx_i| > 1$

$|X| = |X_G| + \sum_{i \in B} |Gx_i|$

$= |X_G| + \sum_{i \in B} \underbrace{(G:G_{x_i})}$

$(G:G_{x_i}) > 1$
and
$(G:G_{x_i}) \mid |G|$

If $|G| = p^n$
$\Rightarrow p \mid (G:G_{x_i})$

$\bullet \Rightarrow |X| \equiv |X_G| \pmod p$

**CAUCHY'S THEOREM**

If $|G| < \infty$ and $p \mid |G|$ then $G$ has an element of order $p$.

Corollary

If $|G| < \infty$ and $p \mid |G|$ then $\exists H \leq G$, s.t. $|H| = p$

Proof

$\exists g \in G$ s.t. $|\langle g \rangle| = |g| = p$ "elemanın oluşturduğu subgroup"

Take $H = \langle g \rangle$ $\square$

PROOF

Let

$X = \{(g_1, \dots, g_p) \mid g_1 g_2 \cdots g_p = 1, g_i \in G\}$

Let

$C = \langle (1\,2 \dots p) \rangle \leq S_p$ $\quad \sigma = (1 \dots p)$
$= \langle \sigma \rangle$
$|C| = p$

Then $C$ acts on $X$

$\alpha \in C$, $(g_1, g_2 \dots g_p) \in X$

$\alpha \cdot (g_1, \dots, g_p) = g_{\alpha(1)} \cdots g_{\alpha(p)}$
$\in X$

$C$ acts on $X$ and $|C| = p$

$\therefore$ $|X| \equiv |X_C| \pmod p$ ⊛

$X = \{(g_1, \dots, g_p) \mid g_1 \cdots g_p = 1\}$
$= \{(g_1, \dots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}) \mid g_1 \dots g_p = 1\}$

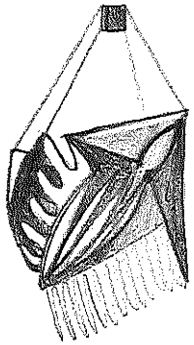
$|X| = |G|^{p-1}$ $\quad p \mid |G| \Rightarrow p \mid |X|$

⊛ $\Rightarrow p \mid |X_c|$

$$X_c = \{(g_1,\dots,g_p) \mid \forall \alpha \in C \ (g_1,\dots g_p) = (g_{\alpha(1)} \cdots g_{\alpha(p)})\}$$

$$= \{(g,\dots,g) \mid g\cdots g = 1\}$$
$$= \{(g,\dots,g) \mid g^p = 1\}$$

$1 < |X_c|$ , $\exists g \neq 1$ s.t. $(g,\dots,g) \in X_c$ then $|g| = p$



Recall

If $|G| = p^n$ acting on $X$, a finite set then

$|X| \equiv |X_G| \pmod p$

$X_G = \{x \in X \mid gx = x \ \forall g \in G\}$

- If $G$ is a finite group and $p \mid |G|$ then $G$ has an element of order $p$.

a conjugate of $H$

$$H^g = \{h^g \mid h \in H\} = \{g^{-1}hg \mid h \in H\}$$

**DEF:** Let $H \leq G$, then the normalizer of $H$ in $G$, denoted by

$$N_G(H) = \{g \in G \mid H^g = H\}$$

Let $X = \{H \mid H \leq G\}$ → the set of all subgroups of $G$.

$$G \times X \longrightarrow X$$
$$g \cdot H \longrightarrow H^{g^{-1}}$$

$$g_2(g_1H) = g_2(H^{g_1^{-1}}) = (H^{g_1^{-1}})^{g_2^{-1}} = H^{g_1^{-1}g_2^{-1}} = H^{(g_1g_2)^{-1}} = (g_2g_1)H$$

Let $H \in X$

What is $G_H = \{g \in G \mid H^g = H\} = N_G(H) \leq G$.

↑isotropy group of $H$

$$(G : N_G(H)) = (G : G_H) = |\underbrace{G.H}_{\text{orbit of } H \text{ under the action of } G.}| = |\{H^g \mid g \in G\}| = \#\text{of conjugates of } H$$

So $H \trianglelefteq G \iff N_G(H) = G$
$\iff$ # of conjugates of $H$ is 1

PROPOSITION

Let $H \leq G$, s.t. $|H| = p^k$ then $(G:H) \equiv (N_G(H):H) \pmod p$

PROOF

Let $H$ act on $\mathcal{L}_H(G)$ as

$$H \times \mathcal{L}_H(G) \longrightarrow \mathcal{L}_H(G)$$
$$(h, gH) \longrightarrow hgH \qquad |H| = p^k$$

$\therefore$ By the lemma from the prev class

$$|\mathcal{L}_H(G)| \equiv |(\mathcal{L}_H(G))_H| \pmod{p}$$

$$(\mathcal{L}_H(G))_H = \{gH \mid h(gH) = gH \ \forall h \in H\}$$

$$= \{gH \mid g^{-1}hg\, H = H,\ \forall h \in H\}$$
$$= \{gH \mid g^{-1}hg \in H,\ \forall h \in H\}$$
$$= \{gH \mid g^{-1}Hg = H,\ \forall h \in H\}$$
$$= \{gH \mid g^{-1} \in N_G(H)\}$$
$$= \{gH \mid g \in N_G(H)\} = \mathcal{L}_H(N_G(H))$$

$$\underset{\displaystyle |\mathcal{L}_H(G)|}{\overset{(G:H)}{\parallel}} \equiv |\mathcal{L}_H(N_G(H))| \pmod{p}$$
$$= (N_G(H):H)$$

*Corollary*

Let $H \leq G$, $|H| = p^h$ suppose that $p \mid (G:H)$

$\Rightarrow$ $p \mid (N_G(H):H)$

**SYLOW THEOREM (1)**

Let $G$ be a finite group of order $|G| = p^n m$ with $1 \leq n$ and $(m,p) = 1$

1- $G$ contains a subgroup of order $p^i$ for every $1 \leq i \leq n$

2- If $H$ is a subgroup of order $p^i$, w/ $1 \leq i < n$ then $\exists H' \leq G$ s.t. $|H'| = p^{i+1}$ and $H \trianglelefteq H'$.

PROOF

(1) We will do induction on $n$

$n=1$, follows by Cauchy

In general, if $n>1$,
use Cauchy's theorem to find a subgroup

$$J \leq G \quad \text{s.t.} \quad |J| = p$$

$$0 \underset{\substack{\text{since}\\ n>1}}{\equiv} (\underset{p^{n-1}m}{G:J}) \equiv (N_G(J):J) \pmod{p}$$

$$\Rightarrow p \mid (N_G(J):J)$$

But $J \trianglelefteq N_G(J)$

$$|N_G(J)/J| = p^{\alpha} m'$$
$$(m', p) = 1$$
$$1 \leq \alpha < n$$

By the induction hypothesis $\Rightarrow N_G(J)$ has a subgroup of order $p^i$ for every order $1 \leq i \leq \alpha$.

$\Rightarrow$ $G$ has a subgroup of order $1 \leq i \leq \alpha + 1$

If $\alpha + 1 = n$, then we are done, if not then we can continue to the argument by taking $J$ a subgroup of order $\alpha + 1 < n$

$J \trianglelefteq N_G(J)$ and $p \mid (N_G(J):J)$

$\Rightarrow H' \trianglelefteq N_G(\mathcal{F})/\mathcal{F}$

Cauchy's Theorem $|H'| = p$

Remember one to one correspondence

$\mathcal{F} \leq \pi^{-1}(H') \leq G$ $\quad \pi : N_G(\mathcal{F}) \longrightarrow N_G(\mathcal{F})/\mathcal{F}$

$|\pi^{-1}(H')| = p^{(\alpha+1)+1}$

(2) $H \leq G$

$|H| = p^i$

$p \mid (G:H)$

$\Rightarrow p \mid (N_G(H):H)$

$\Rightarrow p \mid (N_G(H)/H|$

$\Rightarrow \mathcal{F} \leq N_G(H)/H$

Cauchy $|\mathcal{F}| = p$

$$\pi : N_G(H) \longrightarrow N_G(H)/H \geq \mathcal{F}$$

$H \leq \pi^{-1}(\mathcal{F}) \leq N_G(H)$

$\underbrace{\pi^{-1}(\mathcal{F})/H}_{\text{order } p} \xrightarrow{\sim} \mathcal{F}$ has order $p$

$|H'| = |\pi^{-1}(\mathcal{F})| = |\pi^{-1}(\mathcal{F})/H| \; |H|$

$= p \cdot p^{1} = p^{1+1}$

since $\boxed{H \trianglelefteq N_G(H)}$ and

$H' \leq N_G(H) \Rightarrow H \trianglelefteq H'$

**DEF** With notation as above if $H \leq G$ w/ $|H| = p^n$

Then $H$ is called a Sylow $p$-subgroup of $G$.

$|X| \equiv |X_G| \pmod p$

## SYLOW THEOREM (2)

If $P_1$ and $P_2$ are two sylow $p$-subgroups of $G$ Then $P_1$ and $P_2$ are conjugate.

<u>PROOF</u> Let $P_1$ act on $\mathcal{L}_{P_2}(G)$

$$P_1 \times \mathcal{L}_{P_2}(G) \longrightarrow \mathcal{L}_{P_2}(G)$$
$$(\alpha, gP_2) \rightarrow \alpha g P_2$$

$|P_1| = p^n$ so

$(\underset{=m}{G:P_2}) = |\mathcal{L}_{P_2}(G)| \equiv |(\mathcal{L}_{P_2}(G))_{P_1}| \pmod p$

$p \nmid m \Rightarrow p \nmid |(\mathcal{L}_{P_2}(G))_{P_1}|$

$\Rightarrow (\mathcal{L}_{P_2}(G))_{P_1} \neq \emptyset$

$$\begin{aligned}(\mathcal{L}_{P_2}(G))_{P_1} &= \{gP_2 \mid p_1 g P_2 = g P_2, \forall p_1 \in P_1\} \\ &= \{gP_2 \mid g^{-1} p_1 g P_2 = P_2, \forall p_1 \in P_1\} \\ &= \{gP_2 \mid g^{-1} p_1 g \in P_2, \forall p_1 \in P_1\} \\ &= \{gP_2 \mid g^{-1} P_1 g \leq P_2\} = \{gP_2 \mid g^{-1} P_1 g = P_2\}\end{aligned}$$

$\Rightarrow \exists g \in G$ s.t. $g^{-1} P_1 g = P_2$

Observation

Let $\mathcal{S}_p$ denote the set of all sylow p-subgroups of G

$$\mathcal{S}_p = \{H \mid H \leq G, |H| = p^n\}$$

G acts on $\mathcal{S}_p$ by conjugation

$$*: G \times \mathcal{S}_p \to \mathcal{S}_p$$
$$(g, H) \longrightarrow H^{g^{-1}} \quad \text{this is an action}$$
$$|H^{g^{-1}}| = |H| = p^n$$

Let $P \in \mathcal{S}_p$ and $Q \in \mathcal{S}_p$

$$\Longrightarrow \quad P^{g^{-1}} = Q$$

$\exists g \in G$

$\therefore$ The orbit of $P$ under the action $(*)$ is all of $\mathcal{S}_p$.

i.e

$$G * P = \{P^{g^{-1}} \mid g \in G\} = \mathcal{S}_p$$

$$(G : G_P) = |G * P| = |\mathcal{S}_p| = n_p$$

isotrophy

$n_p$ = # of Sylow P-subgroup

Corollary $n_p = [G : N_G(P)] \mid |G|$

**SYLOW THEOREM (3)** If G is a finite group and $p \mid |G|$ then $n_p \equiv 1 \pmod{p}$ and $n_p = [G : N_G(P)] \mid |G|$

PROOF

Let $\mathcal{P} \in \mathcal{S}_p$ and let $\mathcal{P}$ act on $\mathcal{S}_p$ by conjugation

$$\mathcal{P} \times \mathcal{S}_p \longrightarrow \mathcal{S}_p$$
$$(g, H) \longrightarrow H^{g^{-1}}$$

$$|\mathcal{P}| = p^n$$

$$\Rightarrow |\mathcal{S}_p| \equiv |(\mathcal{S}_p)_{\mathcal{P}}| \pmod{p}$$

$$(\mathcal{S}_p)_{\mathcal{P}} = \{H \in \mathcal{S}_p \mid \forall g \in \mathcal{P}, H^{g^{-1}} = H\}$$
$$= \{H \mid H \leq G, |H| = p^n, H^{g^{-1}} = H, \forall g \in \mathcal{P}\}$$
$$= \{H \mid H \leq G, |H| = p^n, \mathcal{P} \leq N_G(H)\}$$

$$H \leq N_G(H) \leq G$$

$p^n = |H| \quad |N_G(H)| = p^n m' \quad p^n m = |G|$

$(p, m') = 1 \quad (p, m) = 1$

So H is a sylow p-subgroup of $N_G(H)$

But $|\mathcal{P}| = |H| = p^n$

So since

$\mathcal{P} \leq N_G(H)$

$\mathcal{P}$ is also a sylow P-subgroup of $N_G(H)$.

By Sylow theorem (2) applied to $P$, $H$ and $N_G(H)$ $P$ and $H$ are conjugate in $N_G(H)$, i.e. $\exists g \in N_G(H)$ s.t.

$$H = H^g = P$$

$g \in N_G(H)$

**THEOREM** If $G$ is a finite $p$-group, i.e.

$$|G| = p^n, \text{ then}$$

$$Z(G) \neq 1$$

PROOF

Let $G$ act on $G$ by conjugation

$$G \times G^{(=X)} \longrightarrow G^{(=X)}$$

$$(g, \alpha) \longrightarrow \alpha^{g^{-1}}$$

Since $G$ is a $p$-group

$$0 \equiv p^n = |G| \equiv |G_G^{(=X)}| \pmod p$$

$$\begin{aligned} G_G &= \{\alpha \in G \mid \alpha^{g^{-1}} = \alpha, \forall g \in G\} \\ &= \{\alpha \in G \mid g\alpha g^{-1} = \alpha \ \forall g \in G\} \\ &= \{\alpha \in G \mid g\alpha = \alpha g \ \forall g \in G\} \\ &= Z(G) \end{aligned}$$

$|Z(G)| \equiv 0 \pmod p$

$\Rightarrow p \mid |Z(G)|$

$\Rightarrow \{1\} \neq Z(G)$ $\square$

*Lemma*

Suppose $H, K \trianglelefteq G$ s.t. $H \cap K = 1$, and

$$HK = \{hk \mid h \in H, k \in K\} = G$$

Biri normalise subgroup oluyor.

then

$$G \xleftarrow{\sim} H \times K$$

PROOF

Let $h \in H, k \in K$

$\underbrace{hkh^{-1}}_{\in K}k^{-1} \in K$

(since $K \trianglelefteq G$)

$h\underbrace{kh^{-1}k^{-1}}_{\in H} \in H$

$\therefore hkh^{-1}k^{-1} \in H \cap K = \{1\}$

$\Rightarrow hk = kh$

Define

$$\varphi : H \times K \longrightarrow G$$

$$\varphi(h, k) = hk$$

$$\varphi((h_1 k_1)(h_2 k_2))$$

$$= \varphi(h_1 h_2, k_1, k_2) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \varphi(h_1 k_1)\varphi(h_2, k_2)$$

$\therefore$ Homomorphism.

$$\begin{aligned} \ker\varphi :&= \{(h, k) \mid \varphi(h, k) = 1\} \\ &= \{(h, k) \mid hk = 1\} \\ &= \{(h, k) \mid \underset{\in H}{h} = \underset{\in K}{k^{-1}}\} \\ &= \{(1, 1)\} \end{aligned}$$

$\therefore \varphi$ is injective

Since $HK = G$ $\therefore \varphi$ is surjective

$\therefore \varphi$ is isomorphism

**THEOREM**

If $|G|=p^2$ then $G$ is abelian $\left( \begin{array}{l} \text{FTFGAP} \\ \Rightarrow G \simeq \mathbb{Z}/p \times \mathbb{Z}/p \\ G \simeq \mathbb{Z}/p^2 \end{array} \right)$

PROOF

Suppose $G$ is not cyclic (b/c if $G$ is cyclic then $G \simeq \mathbb{Z}/p^2$ so is abelian)

Then if $g \in G \setminus \{1\}$ then $|g|=p$

Take $\alpha \in G \setminus \{1\}$, $|\langle\alpha\rangle|=p$

take $\beta \in G \setminus \langle\alpha\rangle$, $|\langle\beta\rangle|=p$

$H=\langle\alpha\rangle \trianglelefteq G$ (By Sylow 1)

$K=\langle\beta\rangle \trianglelefteq G$ (By Sylow 1)

$H \cap K = \{1\}$ ($\mathbb{Z}_p \times \mathbb{Z}_p$ formatında)

**Proposition**

$H \leq G$, $N \trianglelefteq G$

$HN \leq G$

PROOF

Let $h_1 n_1 h_2 n_2$

$= \underbrace{h_1 h_2}_{\in H} \underbrace{h_2^{-1} n_1 h_2}_{\in N} \underbrace{n_2}_{\in N}$

$(h n)^{-1} = n^{-1} h^{-1}$

$= h^{-1} \underbrace{h n^{-1} h^{-1}}_{\in N} \in HN$

$(N \trianglelefteq G)$

▶ If $|G|=15$ then $G$ is cyclic
$\quad = 3 \cdot 5$

Let $P_3$ be a Sylow 3-subgroup of $G$

$P_5$ " " 5 " "

$n_3 \mid 15 \quad n_3 \equiv 1 \pmod 3 \Rightarrow n_3 \mid 5 \Rightarrow n_3 = 1$

$n_5 \mid 15 \quad n_5 \equiv 1 \pmod 5 \Rightarrow n_5 \mid 3 \Rightarrow n_5 = 1$

This implies that

$\Rightarrow P_3 \trianglelefteq G$ ⟶ Then $G$ is not simple.

$n_3 = 1$ ise
$N_G(P_3) = G$
$P_3 \trianglelefteq G$

$P_5 \trianglelefteq G$

$\boxed{\begin{array}{l} P_3 \cap P_5 \leq P_3 \\ \qquad\quad\ \leq P_5 \end{array}}$

$|P_3 \cap P_5| \mid 3$ and $|P_3 \cap P_5| \mid 5$

$\Rightarrow P_3 \cap P_5 = 1$

$P_3 \leq P_3 P_5 \leq G \qquad 3 \mid |P_3 P_5| \qquad |P_3 P_5| \mid 15$

$P_5 \leq P_3 P_5 \qquad 5 \mid |P_3 P_5| \qquad$ Then $|P_3 P_5| = 15 \Rightarrow P_3 P_5 = G$

$G \simeq P_3 \times P_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$
$\simeq \mathbb{Z}_{15}$

▶ Do it for $P_3$ and $P_7$

$n_3 \mid 21 \quad n_3 \equiv 1 \pmod 3 \quad n_3 \mid 7$

$n_7 \mid 21 \quad n_7 \equiv 1 \pmod 7$

7 de olabilir 1 de. aynı sebepten olmaz

▶ Find the Sylow 2 and 3 subgroup of $S_3$

$|S_3| = 6$

$\mathcal{S}_2 = \{\{1,(12)\}, \{1,(13)\}, \{1,(23)\}\}$

$\mathcal{S}_3 = \{\{1, (123), (132)\}\}$

$n_2 = 3 \quad (n_2 \mid 6 \quad n_2 \equiv 1 \pmod 2)$

$n_3 = 1 \quad (n_3 \mid 6 \quad n_3 \equiv 1 \pmod 3)$

▶ If $|G| = p \cdot q$ with $p<q$

then if $P_q$ is a Sylow $q$-subgroup then

$P_q \trianglelefteq G$

$n_q \mid p \cdot q$, $n_q \equiv 1 \pmod q$, $\Rightarrow n_q \mid p$
$\Rightarrow n_q = 1$

$\boxed{\begin{array}{c} n_q = p \\ \text{olamaz} \\ \text{çünkü} \\ p<q \end{array}}$

# FUNDAMENTAL THEOREM OF FINITELY GENERATED ABALIAN GROUPS

Proposition

Suppose that $A$ is an abelian group and $X \subseteq A$. Then the following are equivalent

(i) $\forall a \in A$, there exists unique $x_1, \dots, x_n \in X$ (pairwise distinct) and $k_1, \dots, k_n \in \mathbb{Z}$ s.t. $a = k_1 x_1 + \cdots k_n x_n$

(ii) $X$ generates $A$ and if $k_1 x_1 + \dots + k_n x_n = 0$ w/ $x_i \in X$ (and $x_i \neq x_j$ for $i \neq j$) and $k_1, \dots, k_n \in \mathbb{Z}$ then $k_1 = k_2 = \dots = k_n = 0$

(i) $\Rightarrow$ (ii): o.k.

(ii) $\Rightarrow$ (i) Let $a \in A$. since $X$ generates $A$,

$$a = k_1 x_1 + \dots + k_n x_n \quad \text{for some } k_1, k_2, \dots, k_n \in \mathbb{Z}$$

Suppose $a = k_1' x_1 + \dots k_n' x_n$

$$0 = (k_1' - k_1) x_1 + \dots + \dots (k_n' - k_n) x_n$$

$\Rightarrow k_i' - k_i = 0$, for all $1 \leq i \leq n$

$\Rightarrow k_i' = k_i$, for all $1 \leq i \leq n$

**DEF:** We say $A$ is a free abelian group w/ basis $X$ if $X \subseteq A$ satisfies the hypothesis above

▶ $\mathbb{Z} \oplus \mathbb{Z}$ is free abelian group with basis $\{(1,0), (0,1)\}$

▶ $\mathbb{Z}_6$ is not a free abelian group (with any basis)

▷ $6 \cdot x = 0$ $\forall x \in \mathbb{Z}_6$ and $n \neq 0$

**DEF** A group $G$ is called torsion-free if

$$G_{tors} = \{ g \in G \mid |g| < \infty \} = \{1\}$$

PROPOSITION

If $A$ is a free abelian group with basis $X$, then $A$ is torsion-free

PROOF

Suppose $a \in A$ has finite order, $m \in \mathbb{N}$ and write

$$a = k_1 x_1 + \dots + k_n x_n$$

$$0 = m.a = (mk_1) x_1 + \dots + (mk_n) x_n$$

$\Rightarrow mk_i = 0$, for all $i$

$\Rightarrow k_i = 0$, for all $i$

$\Rightarrow a = 0$

**HW**

- $(\mathbb{Q}, +)$ is torsion free but not free abelian
- Prove that if $A$ is abelian and f.g and torsion free then $A$ is free abelian

**FACT**

If $A$ is a free abelian group w/ basis $X$ and also a free abelian group w/ basis $Y$ then

$$|X| = |Y|$$

We will prove this when $|X| < \infty$

OBSERVATION

Suppose $|X| < \infty$ and $A$ is a free abelian group w/ basis $X$, then

$$A \simeq \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}} \qquad \text{where } |X| = n$$

suppose $X = \{x_1, \dots, x_n\}$

$$\mathbb{Z} \oplus \mathbb{Z} \oplus \dots \mathbb{Z} \xrightarrow{\phi} A$$
$$(k_1, \dots, k_n) \longmapsto k_1x_1 + \dots + k_nx_n$$

$$\mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z} \xleftarrow{\psi} A$$
$$(k_1, \dots, k_n) \qquad \theta = k_1x_1 + \dots k_nx_n$$

$$\psi \circ \phi = id = \phi \circ \psi$$

suppose that $A$ is any abelian group and $m \in \mathbb{N}$

$$mA = \{ma \mid a \in A\} \leq A$$

$$(m \cdot a + m \cdot b = m(a+b) \in mA)$$
A is abelian

$A/mA$ makes sense.

If $A$ is a free abelian group w/ basis $X$, then $A \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \dots \mathbb{Z}$

$$A/mA \simeq (\mathbb{Z} \oplus \dots \oplus \mathbb{Z}) / m(\mathbb{Z} \oplus \dots \oplus \mathbb{Z})$$

$$(\mathbb{Z} \oplus \dots \oplus \mathbb{Z}) / m(\mathbb{Z} \oplus \dots \oplus \mathbb{Z})$$

$$\simeq (\mathbb{Z} \oplus \dots \oplus \mathbb{Z}) / \{(mk_1, \dots, mk_n) \mid k_i \in \mathbb{Z}\}$$

$$\simeq \underbrace{\mathbb{Z}_m \oplus \dots \oplus \mathbb{Z}_m}_{n \text{ times}}$$

$$|A/mA| = m^n = m^{|X|}$$

If $Y$ is another basis then

$$|A/mA| = m^{|Y|}$$

$$\Rightarrow |Y| = |X|$$

**DEF:** If $A$ is a free abelian group w/ basis $X$, we call the cardinality $|X|$ of $X$, the rank of $A$

("some" people, namely Lang, calls it Betti number)

THE FILE

*Lemma*

suppose that $\{x_1, \dots, x_n\}$ is a basis for $A$, let $i \neq j$ and $t \in \mathbb{Z}$. then

$$X' = \{x_1, \dots, x_{i-1}, x_i + tx_j, x_{i+1}, \dots, x_j, \dots x_n\}$$

is also a basis for $A$.

PROOF

Need to show that $X'$ generates $A$

Let $a \in A$, since $X$ generates $A$

$\exists k_1, \dots, k_n \in \mathbb{Z}$ s.t.

$$a = k_1x_1 + \dots + k_nx_n$$
$$= k_1x_1 + \dots k_ix_i + \dots k_nx_n$$
$$= k_1x_1 + \dots + k_i(x_i + tx_j) + \dots + (k_j + tk_i)x_j + \dots + k_n \underbrace{x_n}_{\in X'}$$

UNIQUENESS

suppose

$$0 = k_1x_1 + \dots + k_{i-1}x_{i-1} + k_i(x_i + tx_j) + \dots + k_nx_n$$
$$= k_1x_1 + \dots + k_{i-1}x_{i-1} + k_ix_i + \dots + (k_it + k_j)x_j + \dots$$

$\underset{X \text{ is a basis}}{\Longrightarrow}$ $k_1 = 0, \dots k_{i-1} = 0, k_i = 0$

$k_it + k_j = 0 \quad \dots \; k_n = 0$

$\Longrightarrow k_1 = k_2 = \dots = k_n = 0$

**THEOREM** If $A$ is a finitely generated abelian group then

$$A \simeq \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z} \oplus \mathbb{Z}$$

s.t. $d_1 | d_2, d_2 | d_3 | \ldots, d_{k-1} | d_k$
and $d_1, \ldots d_k$ are unique and also $n$ is unique,

(n is called the rank of the Betti number of A)

It sufficies to prove the following Lemma

*Lemma*: If $F \leq \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{m\text{-times}} = A$

then there exists a basis

$x_1, \ldots, x_m$ of $\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots + \mathbb{Z}$

and $d_1, \ldots, d_k$ s.t $d_1 | d_2, \ldots, d_{k-1} | d_k$
and $\{d_1 x_1, \ldots, d_k x_k\}$ is a basis for $F$.

In particular, $F$ is a free abelian group.

$$\Rightarrow (\mathbb{Z} \oplus \cdots \oplus \mathbb{Z})/F$$

$$\simeq \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \big/ (d_1 a_1, d_2 a_2, \ldots, d_k a_k, 0, 0, \ldots 0)$$

$$\simeq \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

Consider all possible bases for $A$, $\{y_i\}_{1 \leq i \leq n}$

and all possible combinations

$$a_1 y_1 + \cdots + a_m y_m \in F$$

and among these let $|a_1|$ be the smallest positive integer

$$|a_1| = d_1$$

then

$$d_1 y_1 + a_2 y_2 + \cdots + a_m y_m \in F.$$

Claim $d_1 | a_i$, for every $y$

PROOF

$$a_i = d_i q_i + r_i$$

$$d_1 y_1 + a_2 y_2 + \cdots + a_m y_m \in F$$

$$d_1 y_1 + (d_1 q_2 + r_2) y_2 + \cdots + a_m y_m \in F$$

$$d_1 \underbrace{(y_1 + q_2 y_2)}_{= y_1'} + r_2 y_2 + \cdots + a_m y_m$$

$\{y_1', y_2, \ldots, y_n\}$ is another basis for $A$

$$\underset{r_2 < d_1}{\Longrightarrow} r_2 = 0 \Longrightarrow d_1 | a_2$$

$$d_1 | a_i, \text{ for every } 2 \leq i \leq m$$

Consider now all bases.

$$\{y_1, z_2, \ldots, z_m\}$$

s.t. $\exists\ d_1 y_1 + a_2 z_2 + \cdots + a_m z_m \in F$

(NOTE THAT This implies $d_1 | a_i$, for all $i$)

Among all these expressions let $|a_2| = d_2$ be the smallest one possible then $d_1 | d_2$

CLAIM

If

$$d_1y_1 + d_2y_2 + \underset{\overset{\|}{d_2q_2+r_3}}{a_3} z_3 + \dots +$$

then $d_2 \mid a_i$ for all $3 \le i \le m$

$0 \le r_3 < d_2$

$$d_1y_1 + d_2\underset{\overset{\|}{y_2'}}{(y_2+q_3z_3)} + r_3z_3 + \dots + a_mz_m \in F$$

$\{y_1, y_2', z_3, \dots, z_m\}$ is another basis

for $F \underset{r_3<d_2}{\Longrightarrow} r_3 = 0$

$\Longrightarrow d_2 \mid a_i$, for all $i$

By induction, we arrive at the desired basis.

Corollary If $B$ is a f.g. abelian group then

$$B \xrightarrow{\sim} \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \dots \oplus \mathbb{Z} \dots \oplus \mathbb{Z}$$

s.t $d_i \mid d_{i+1}$

Recall If $n = p_1^{s_1} \cdots p_r^{s_r}$

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p_r^{s_r}}$$

Corollary

Then if $B$ is a finitely generated abelian group

$$B \simeq \mathbb{Z}_{p_1^{t_1}} \oplus \dots \oplus \mathbb{Z}_{p_\ell^{t_\ell}} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$$

Uniqueness

If

$$\mathbb{Z}_{p_1^{t_1}} \oplus \dots \oplus \mathbb{Z}_{p_\ell^{t_\ell}} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{a \text{ copies}}$$

$$\simeq \mathbb{Z}_{q_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{q_m^{s_m}} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{b \text{ copies}}$$

where $p_1 \le p_2 \le \dots \le p_\ell$

$q_1 \le \dots \le q_m$

and if $p_i = p_{i+1}$ then $t_i \le t_{i+1}$

if $q_i = q_{i+1}$ then $s_i \le s_{i+1}$

then $a = b$,

$p_i = q_i$ and $t_i = s_i$

PROOF

$$A_{tors} = \{a \in A \mid |a| < \infty\} \le A$$

True if A is abelian

$$B_{1,tors} \simeq \mathbb{Z}_{p_1^{t_1}} \oplus \dots \oplus \mathbb{Z}_{p_\ell^{t_\ell}}$$

$$B_{2,tors} \simeq \mathbb{Z}_{q_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{q_m^{s_m}}$$

$$B_{1,tors} \simeq B_{2,tors}$$

$$\mathbb{Z}_{p_1^{t_1}} \oplus \dots \oplus \mathbb{Z}_{p_\ell^{t_\ell}} \xrightarrow{\sim} \mathbb{Z}_{q_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{q_m^{s_m}}$$

$$\underset{\overset{\|}{\underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{a \text{ copies}}}}{B_1/B_{1,tors}} \simeq \underset{\overset{\|}{\underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{b \text{ copies}}}}{B_2/B_{2,tors}}$$

Then $a = b$

WLOG
$a=b=0$

$$\begin{array}{ccc} A_1 & \simeq & A_2 \\ \| & & \| \\ \mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{t_l}} & & \mathbb{Z}_{q_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{q_m^{s_m}} \end{array}$$

$$\Longrightarrow \begin{array}{ccc} A_1(p_1) & \simeq & A_2(p_1) \\ \wr\wr & & \wr\wr \\ \mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{t_g}} & & \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{s_h}} \end{array}$$

$t_1 \le \cdots \le t_g$ $\qquad$ $s_1 \le \cdots \le s_h$

$p_1^{t_g}$ is the order of the largest cyclic subgroup in $A_1(p_1)$

$p_1^{s_h}$ is the order of the largest cyclic subgroup in $A_2(p_1)$

$$\Longrightarrow p_1^{t_g} = p_1^{s_h}$$

Let $c_i \le A_i(p_1)$ s.t. $c_i$ is cyclic and $|c_i| = p_1^{t_g} = p_1^{s_h}$

$$A_1(p_1)/c_1 \simeq \mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{t_{g-1}}}$$
$$\wr\wr$$
$$A_2(p_1)/c_2 \simeq \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{s_{m-1}}}$$

By induction

**THEOREM** If $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{a \text{ copies}}$

$$\simeq \mathbb{Z}_{e_1} \oplus \cdots \oplus \mathbb{Z}_{e_n} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{b \text{ copies}}$$

w/ $d_i \mid d_{i+1}$, $e_i \mid e_{i+1}$, for all $i$

Then $a=b$ and $d_i = e_i$ for all $i$.

## RINGS AND FIELDS

**RING:** A ring $(R,+,\cdot)$ is a non-empty set $R$, together with two operations, $+,\cdot$ on $R$, such that

(i) $(R,+)$ is an abelian group

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

(iii) Distributive Law $\forall a,b,c \in R$, $(a+b)c = a\cdot c + bc$ and $a(b+c) = ab+ac$

If there exists a $1 \in R$ s.t. $\forall a \in R$ $1a = a = a1$
Then we say that $R$ is a ring with unity

If for every $a,b \in R$,
$ab = b\cdot a$
Then we say that $R$ is commutative.

For us the most important type of rings will be commutative rings with unity.

▶ $(\mathbb{Z}, +, \cdot)$ commutative ring with unity

• $(M_{22}(\mathbb{R}), +, \cdot)$

2x2 matrices with entries from $\mathbb{R}$

A ring with unity, but it is non-commutative

$$\begin{bmatrix}0&1\\0&0\end{bmatrix}\begin{bmatrix}0&0\\1&0\end{bmatrix}=\begin{bmatrix}1&0\\0&0\end{bmatrix}$$
$$\neq$$
$$\begin{bmatrix}0&0\\1&0\end{bmatrix}\begin{bmatrix}0&1\\0&0\end{bmatrix}=\begin{bmatrix}0&0\\0&1\end{bmatrix}$$

• $LM(V,V)$ – not commutative ring w/unity.

• $(\mathbb{Z}_n, +, \cdot)$ commutative ring w/unity

*Observation*

(i) Note

$0 \cdot r = (0+0) \cdot r = 0 \cdot r + 0 \cdot r$

$$0 = (-0\cdot r) + 0\cdot r = -(0\cdot r) + (0\cdot r + 0\cdot r)$$
$$= (-0\cdot r + 0\cdot r) + 0\cdot r$$
$$= 0 + 0\cdot r = 0\cdot r$$

similarly, $r \cdot 0 = 0$, $\forall r \in R$

(ii) Suppose $R$ has a unity $1$

$1_R = 0 \Leftrightarrow R = \{0\}$ called trivial ring

$(\Rightarrow r = r\cdot 1 = r\cdot 0 = 0,\ R = \{0\})$

$\Leftarrow$ Trivial

(iii) Suppose that $R$ is a comm. ring with unity, then we let

$R^\times = \{r \in R \mid \exists s \in R,\ w/\ r\cdot s = 1\}$

called the invertible elements
– called the units

▨ $(R^\times, \cdot)$ is a group

$\cdot\ r_1, r_2 \in R^\times$

then $\exists s_1, s_2 \in R^\times$ s.t.

$r_i s_i = 1$

$r_1 \cdot r_2 s_2 s_1 = r_1 \cdot 1 \cdot s_1 = r_1 s_1 = 1$

$\Rightarrow r_1 r_2 \in R^\times$

$(R^\times, \cdot)$ is closed

- ASSOC
- $1 \in R^\times$
- If $r \in R^\times$, then $\exists s \in R$ w/ $rs = 1$, $\Rightarrow s \in R^\times$

So every element has an inverse

$\therefore (R^\times, \cdot)$ is a group

It is comm. since $(R, \cdot)$ is commutative.

▶ – $(\mathbb{Z}, +, \cdot)$, $\mathbb{Z}^\times = \{\pm 1\}$

– $(\mathbb{R}, +, \cdot)$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

– $(\mathbb{Z}_n, +, \cdot)$, $\mathbb{Z}_n^\times = \{m \mid 0 \le m < n,\ (m,n) = 1\}$

$|\mathbb{Z}_n^\times| = \varphi(n) \Rightarrow \forall 0 \le a < n,$

$a^{\varphi(n)} \equiv 1 \pmod{n}$

EULER'S THEOREM

**DEF** We say that $R$ is an <u>integral domain</u>, if $R$ is a commutative ring w/ unity, s.t. $R \neq \{0\}$ and $\forall r, s \in R$,

$r \cdot s = 0 \Rightarrow r = 0$ or $s = 0$

▶ • $(\mathbb{Z}, +, \cdot)$ integral domain

• $(\mathbb{Z}_n, +, \cdot)$ is not an integral domain

$\Longleftrightarrow$ n is composite

$(a \cdot b = 0$ in $\mathbb{Z}_n \Leftrightarrow n \mid a \cdot b)$

$2 \cdot 3 = 0$ in $\mathbb{Z}_6$

• $(M_{2\times 2}, +, \cdot)$

$$\begin{bmatrix}1&0\\0&0\end{bmatrix}\begin{bmatrix}0&0\\0&1\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$

• $R = \{a + b\alpha,\ a, b \in \mathbb{R}\}$

$(a+b\alpha)(c+d\alpha) = ac + (bc+ad)\alpha$

$(a+b\alpha) + (c+d\alpha) = (a+c) + (b+d)\alpha$

$\alpha \cdot \alpha = 0$

$(\mathbb{R}, +, \cdot)$ comm w/ unity but

not integral domain

**DEF**

We say that $(F,+,\cdot)$ is <u>a field</u> if $F \neq \{0\}$ and $(F,+,\cdot)$ is a comm. ring w/unity s.t.

$$F^{\times} = F \setminus \{0\}$$

- $(\mathbb{Z},+,\cdot)$ not a field

$(\mathbb{Q},+,\cdot)$, $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$ Field

$(\mathbb{R},+,\cdot)$, $\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\}$ Field

$\mathbb{C}^{\times} = \mathbb{C} \setminus \{0\}$ Field

*Remark*

If $F$ is a field then $F$ is an integral domain

If $r.s = 0$ in $F$ and $r \neq 0 \Rightarrow r \in \underbrace{F \setminus \{0\}} = F^{\times}$

$\Rightarrow \exists r' \in F$ s.t. $r'.r = 1$

$\Rightarrow 0 = r'.0 = r'.r.s = 1.s = s$

- $(\mathbb{Z}_p,+,\cdot)$ is a field

If $r \in \mathbb{Z}_p \setminus \{0\}$

$\Rightarrow (r,p) = 1$

$\Rightarrow \exists x,y \in \mathbb{Z}$ s.t.

$r.x + p.y = 1$

$r.x = 1 \pmod p$

$\Rightarrow r \in \mathbb{Z}_p^{\times}$

$(\mathbb{Z}_p,+,\cdot)$ is a field.

**NOTE**: We will show that there is a field of order $p^n$, for every prime power $p^n$.

*Warning* This is not

$(\mathbb{Z}_{p^n},+,\cdot)$.

Not a field.

$p.p^{n-1} = 0$ in $\mathbb{Z}_{p^n}$

**HOMOMORPHISM**

*Let $R$ and $S$ be two rings*

*A homomorphism $\varphi$ from $R$ to $S$ is a function*

$$\varphi : R \to S$$

s.t.

(i) $\varphi(r_1+r_2) = \varphi(r_1) + \varphi(r_2)$ $(\Rightarrow \varphi(0) = 0)$

(ii) $\varphi(r_1.r_2) = \varphi(r_1).\varphi(r_2)$

(iii) $\varphi(1) = 1$

$\ker \varphi = \{r \in R \mid \varphi(r) = 0\}$

$\varphi : \mathbb{Z} \to \mathbb{Z}_n$

$\quad a \to a \pmod n$

$\ker \varphi = n\mathbb{Z}$

**DEF** Let $R$ be a ring, <u>an ideal</u> $\emptyset \neq I \subseteq R$ is a subset satisfying

(i) $(I,+)$ is a subgroup of $(R,+)$

(ii) If $\alpha \in I$ and $r \in R$

$\alpha.r \in I$

<u>PROPOSITION</u>

If $\varphi : R \to S$ is a homomorphism then $\ker \varphi \subseteq R$ is an ideal

<u>PROOF</u>

Recall $\ker \varphi = \{\alpha \in R \mid \varphi(\alpha) = 0\}$

- If $r \in R$, $\alpha \in \ker \varphi$ then

$\varphi(r.\alpha) = \varphi(r)\varphi(\alpha)$
$= \varphi(r).0 = 0$

$\Rightarrow r\alpha \in \ker \varphi$

- If $\alpha, \beta \in \ker \varphi$ then $\varphi(\alpha+\beta)$
$= \varphi(\alpha) + \varphi(\beta)$
$= 0 + 0 = 0$

$\Rightarrow \alpha + \beta \in \ker \varphi$

If $\alpha \in \ker \varphi$ then

$\varphi(-\alpha) = -\varphi(\alpha) = 0$

$\Rightarrow -\alpha \in \ker \varphi$

So <u>$\ker \varphi \subseteq R$ is an ideal.</u>

<u>CONSTRUCTION</u>

Let $I \subseteq R$ be

$\Rightarrow (I,+) \leq (R,+)$

$\Rightarrow (I,+) \trianglelefteq (R,+)$

$+$ is comm.

$(R/I, +)$ is a group

We can define a ring structure on $(R/_I, +)$ as follows

$$(r+I)(s+I) = rs+I$$

Is this well-defined?

Suppose that $r'+I = r+I$ ①
and
$s'+I = s+I$ ②

Is it true that
$rs+I = r's'+I$

$r'+I = r+I$
$\Leftrightarrow r'-r \in I$
$\exists \varepsilon \in I$

$r'-r = \varepsilon$

$s'+I = s+I$
$\Leftrightarrow s'-s \in I$
$\Leftrightarrow \exists \delta \in I$ s.t.
$s'-s = \delta$
$\Leftrightarrow s' = s+\delta$

• $r's'+I = (r+\varepsilon)(s+\delta)+I$
$= (rs + \underbrace{\varepsilon s + r\delta + \varepsilon\delta}_{\in I}) + I$
$= rs+I$

So we have an addition and multiplication on $R/_I$

CLAIM $(R/_I, +, \cdot)$ is a ring

$[(r+I)(s+I)][t+I] = (rs+I)(t+I)$
$= (rs)t + I = r(st)+I$
$= (r+I)+(s+I) = (r+I)((s+I)(t+I))$ Assoc.

DISTR. 1

$(r+I)((a+I)+(b+I))$
$= (r+I)((a+b)+I)$
$= r(a+b)+I$
$= (r.a+r.b)+I = (r.a+I)+(r.b+I)$
$= (r+I)(a+I)+(r+I)(b+I)$

DISTR. 2

$((a+I)+(b+I))(r+I)$
$= (a+I)(r+I)+(b+I)(r+I)$

• If $R$ has a unity then $R/_I$ has a unity.

(If $1.r = r.1 = r \quad \forall r \in R$ then $(1+I)(r+I) = (r+I)(1+I) = r+I$)

• Similarly if $R$ is comm then so is $R/_I$

$(r+I)(s+I) = rs+I = sr+I = (s+I)(r+I)$

Moreover there is a canonical homom.

$$\pi : R \twoheadrightarrow R/_I$$
$$r \longrightarrow r+I$$

• $\pi(r+s) = (r+s)+I$
$= (r+I)+(s+I)$
$= \pi(r)+\pi(s)$

• $\pi(r.s) = rs+I = (r+I)(s+I)$
$= \pi(r).\pi(s)$

• $\pi(1) = 1+I$

$\ker \pi = \{\alpha \in R \mid \alpha + I = 0 \text{ in } R/_I\} = I$

$$\begin{tikzcd} R \arrow[r, two heads, "\pi"] \arrow[dr, "\varphi"'] & R/I \arrow[d, dashed, "\psi"] \\ & S \end{tikzcd}$$

$\exists\, \psi : R/I \longrightarrow S$

s.t. $\psi \circ \pi = \varphi$

$\Leftrightarrow I \subseteq \ker \varphi$

Suppose

$\exists\, \psi$ s.t

$\psi \circ \pi = \varphi$

if $\alpha \in I \Rightarrow$

$\alpha \in \ker \pi$

$\varphi(\alpha) = (\psi \circ \pi)(\alpha)$

$= \psi(\pi(\alpha))$

$= \psi(0)$

$= 0$

$\Rightarrow \alpha \in \ker \varphi$

$\therefore I \subseteq \ker \varphi$

Suppose that $I \subseteq \ker \varphi$

Define $\psi : R/_I \to S$

as $\psi(r+I) = \varphi(r)$

Is this well-defined?

If $r'+I = r+I$ then $\exists\, \varepsilon \in I$ s.t

$r' = r + \varepsilon$

$\psi(r'+I) = \varphi(r') = \varphi(r+\varepsilon) = \varphi(r) + \varphi(\varepsilon)$

$= \varphi(r) + 0 = \varphi(r) = \psi(r+I)$

$\Rightarrow \varepsilon \in I \subseteq \ker \varphi$

$\therefore$ So $\psi$ is well-defined.

$\psi$ is a homomorphism

▽ $\psi((r+I)+(s+I))$

$= \psi((r+s)+I)$

$= \varphi(r+s) = \varphi(r) + \varphi(s)$

$= \psi(r+I) + \psi(s+I)$

▽ $\psi((r+I)(s+I))$

$= \psi(rs+I) = \varphi(rs)$

$= \varphi(r) \cdot \varphi(s)$

$= \psi(r+I)\,\psi(s+I)$

▽ $\psi(1+I) = \varphi(1) = 1$

Note if such a $\psi$ exists then it is unique since $\pi$ is surjective

▶ What are the ideals of $\mathbb{Z}$?

$n\mathbb{Z}$, for some $n \in \mathbb{N}_0$

▶ What are the ideals of $F$, if $F$ is a field

if $(0) \subsetneq I \subseteq F$

then $\exists\, \alpha \in I \setminus \{0\}$

$\Rightarrow 1 = \underset{\in F}{\alpha^{-1}} \cdot \underset{\in I}{\alpha} \in I$

If $r \in F$, $r = \underset{\in F\ \in I}{r \cdot 1} \in I$

$\Rightarrow I = F$

$\mathbb{Z} \subseteq \mathbb{Q}$

## Field of fractions

Let $A$ be an integral domain will construct a field $F$ s.t

$i : A \hookrightarrow F$

and it will have the property

$$\begin{tikzcd} A \arrow[r, hook, "i"] \arrow[dr, "j"'] & F \arrow[d, dashed, "\psi"] \\ & K \end{tikzcd}$$

$K$ - field

**CONSTRUCTION**

$F = \left\{ \frac{a}{b} \,\middle|\, a \in A, b \in A \setminus \{0\} \right\}$

$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad - bc = 0$

$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}$

$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'}$

These are well-defined

▷ If $\frac{a}{b} \sim \frac{c}{d}$ $\frac{a'}{b'} \sim \frac{c'}{d'}$

$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$

$ad = bc$

$a'd' = b'c'$

$\frac{c}{d} + \frac{c'}{d'} = \frac{cd' + c'd}{dd'}$

$$\frac{ab'+a'b}{bb'} \sim \frac{cd'+c'd}{dd'} \iff (ab'+a'b)\,dd' \stackrel{?}{=} (cd'+c'd)\,bb'$$

$$\iff adb'd' + a'd'bd \stackrel{?}{=} bcdb' + b'c'bd$$

$$= bcb'd' + b'c'bd$$

$$\frac{0}{a} = \frac{0}{1} = 0$$

if $\frac{a}{b} \in F \setminus \{0\}$

$\implies a=0$

$\frac{b}{a} \in F \quad \frac{b}{a}\cdot\frac{a}{b} = \frac{1}{1}$ unit in F

F is a field

$$i : A \hookrightarrow F$$
$$a \longmapsto \frac{a}{1}$$

$$\ker i = \{\, a \in A \mid i(a) = \tfrac{0}{1} \text{ in } F \,\}$$
$$= \{\, a \in A \mid \tfrac{a}{1} = \tfrac{0}{1} \text{ in } F \,\}$$
$$= \{0\}$$

Now suppose

$$\begin{tikzcd} A \arrow[r, hook, "i"] \arrow[dr, "J"'] & F \arrow[d, dashed, "\varphi"] \\ & K \end{tikzcd}$$

field of fractions

field

UNIQUENESS

$$\varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{a}{1}\cdot\frac{1}{b}\right)$$
$$= \varphi\left(\frac{a}{1}\right)\varphi\left(\frac{1}{b}\right)$$
$$= \varphi\circ i(a)\cdot\varphi\big(i(b)\big)^{-1}$$
$$= J(a)\big(J(b)\big)^{-1}$$

**DEFINE**

$$\varphi\left(\frac{a}{b}\right) = J(a)\cdot J(b)^{-1}$$

is this well-defined?

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc$$

$b \neq 0$

$d \neq 0$

$$\Rightarrow J(a)\cdot J(d) = J(b)\,J(c)$$

$$\Rightarrow J(b) \neq 0,\ J(d) \neq 0$$

J is injective

$$\underbrace{J(a)\ J(b)^{-1}}_{\varphi\left(\frac{a}{b}\right)} = \underbrace{J(c)\ J(d)^{-1}}_{\varphi\left(\frac{c}{d}\right)}$$

In this lecture suppose that $R$ is a commutative ring with unity.

Let $R[x] = \{a_0 + a_1 x + \dots + a_n x^n \mid a_0, \dots, a_n \in R\}$

For example, if $R = \mathbb{Z}$

then $2 - 3x \in \mathbb{Z}[x]$

$-2 + 5x^3 - 7x^8 \in \mathbb{Z}[x]$

We define addition in $R[x]$ as follows

$(a_0 + a_1 x + \dots + a_n x^n) + (b_0 + b_1 x + \dots + b_m x^m)$

$= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_\ell + b_\ell)x^\ell$

s.t. $\ell = \max(n, m)$

if $n < r$, $a_r = 0$

$m < r$, $b_r = 0$

$(2 - 3x) + (-2 + 5x^3 - 7x^8) = -3x + 5x^3 - 7x^8$

$\left[ R[x] = \{\sum_{0 \le i} a_i x^i \mid a_i = 0 \text{ except for finitely many}\} \right]$

$\left[ \sum_{0 \le i} a_i x^i + \sum_{0 \le i} b_i x^i = \sum_{0 \le i} (a_i + b_i) x^i \in R[x] \right]$

We can also define an multiplication on $R[x]$, as

$$\sum_{0 \le i} a_i x^i \sum_{0 \le j} b_j x^j = \sum_{0 \le n} c_n x^n$$

$$c_n = \sum_{0 \le i \le n} a_i b_{n-i}$$

$(2 - 3x)(-2 + 5x^3 - 7x^8)$

$= -4 + 6x + 10x^2 + \dots$

PROPOSITION

$R[x]$ is a commutative ring with unity.

PROOF

$0 = 0 + 0 \cdot x + \dots$

$$\left(\sum_{0 \le i} \alpha_i x^i \sum_{0 \le i} \beta_i x^i\right)\left(\sum_{0 \le i} \gamma_i x^i\right) = \sum_{0 \le j} \left(\sum_{0 \le i \le j} \alpha_i \beta_{j-i}\right) x^j \sum_{0 \le i} \gamma_i x^i = \sum_{0 \le k} \sum_{0 \le i \le j} (\alpha_i \beta_{j-i}) \times_{k-j} x^k$$

$$\sum_{0 \le j \le k} \left(\sum_{0 \le i \le j} \alpha_i \beta_{j-i}\right) \gamma_{k-j} = \sum_{0 \le i_1, i_2, i_3} (\alpha_{i_1} \beta_{i_2}) \gamma_{i_3}$$

$$\left(\sum_{0 \le i} \alpha_i x^i\right)\left(\sum_{0 \le i} \beta_i x^i \sum_{0 \le i} \gamma_i x^i\right) = \sum_{0 \le i} \alpha_i x^i \sum_{0 \le i} \left(\sum_{b+c=i} \beta_b \gamma_c\right) x^i$$

$$= \sum_{0 \le i} \left(\sum_{\substack{0 \le a, b, c \\ a+b+c=i}} \alpha_a (\beta_b \gamma_c)\right) x^i$$

Define

$\deg : R[x] \longrightarrow \mathbb{N}_{\ge 0} \cup \{-\infty\}$

- $\deg(0) = -\infty$

$\deg\left(\sum_{0 \le i} a_i x^i\right) = \max\{i \mid a_i \ne 0\}$

$\deg(f+g) \le \max(\deg(f), \deg(g))$

- If $R$ is an integral domain then

$\deg(f(x) \cdot g(x)) = \deg((f(x)) + \deg((g(x))$

*Warning*

This need not be true if $R$ is not an integral domain

$R = \mathbb{Z}_6$,

$2x, 3x \in \mathbb{Z}_6[x]$

$(2x)(3x) = 6x^2 = 0$

$\deg(2x \cdot 3x) = -\infty$

Suppose $R$ is an integral domain

$$\underbrace{(a_0 + \dots + a_n x^n)}_{f(x)} \underbrace{(b_0 + \dots + b_m x^m)}_{g(x)} = a_0 b_0 + \dots + (a_n b_m) x^{n+m}$$

$\deg f(x) = n$ , $a_n \neq 0$

$\deg g(x) = m$ , $b_m \neq 0$

$a_n \cdot b_m \neq 0$

$\#\ \ \#$

$0\ \ 0$

$\deg f(x)g(x) = n+m = \deg f(x) + \deg g(x)$

Let us look at the case

$F[x]$ field

In this case we have the division algorithm

PROPOSITION

Let $a(x), b(x) \in F[x]$, $b(x) \neq 0$

then there exist unique $q(x)$ and $r(x)$ s.t.

$a(x) = b(x)q(x) + r(x)$ s.t.

$\deg r(x) < \deg b(x)$

$a, b \in \mathbb{Z}$, $b \neq 0$

$\exists!\ q, r \in \mathbb{Z}$ s.t. $0 \leq r < |b|$

and

$a = bq + r$

Why are $q(x)$ and $r(x)$ unique?

Suppose that $\tilde{q}(x)$ and $\tilde{r}(x)$ also satisfy

$a(x) = b(x)\tilde{q}(x) + \tilde{r}(x)$ with $\deg \tilde{r}(x) < \deg b(x)$

$b(x)q(x) + r(x) = a(x) = b(x)\tilde{q}(x) + \tilde{r}(x)$

$$b(x)(q(x) - \tilde{q}(x)) = \underbrace{\tilde{r}(x) - r(x)}_{< \deg b(x)}$$

$\Longrightarrow q(x) - \tilde{q}(x) = 0$

$\Longrightarrow q(x) = \tilde{q}(x)$

and

$r(x) = \tilde{r}(x)$

▶ $\mathbb{Z}[x]$ $\quad x^2+3 \,|\, 2x+1$

It is important to have a field here because it does not contain inverse of 2

**DEF:** Let $a(x), b(x) \in F(x)$

We say that $b(x) | a(x)$ (divides)

if $a(x) = b(x)q(x)$

PROPOSITION

If $I \subseteq F[x]$ is an ideal then $I = (f(x))$
$= \{f(x)g(x) \mid g(x) \in F[x]\}$

PROOF

Trivial if $I = \{0\}$

Suppose $I \neq 0$

If $I \subseteq \mathbb{Z}$ an ideal then $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$
$= \{na \mid a \in \mathbb{Z}\}$

Let $\min\{\deg a(x) \mid a(x) \in I \setminus \{0\}\} = m$

Let $f(x) \in I \setminus \{0\}$

s.t. $\deg f(x) = m$

then if $\alpha(x) \in I$

then $\alpha(x) = \overset{\in I}{f(x)}\, q(x) + r(x)$ s.t. $\deg r(x) < \deg f(x) = m$

$\Rightarrow r(x) \in I$, $\deg r(x) < m \Rightarrow r(x) = 0$

$\alpha(x) = f(x)q(x)$

$\Rightarrow \alpha(x) \in (f(x))$

$\therefore\ I \subseteq (f(x))$

$\Rightarrow I = (f(x))$

$(f(x)) \subseteq I$

## Observation

Let $a \in F$, we have $\varphi_\alpha : F[x] \longrightarrow F$

$f(x) \longrightarrow f(\alpha)$

$\varphi_\alpha(f(x)) = f(\alpha)$

$\varphi_\alpha\left(\sum_{0 \leq i} a_i x^i\right) = \sum_{0 \leq i} a_i \alpha^i \in F$

$\ker \varphi_\alpha = \{ f(x) \mid f(\alpha) = 0 \}$

$f(x) = (x - \alpha)q(x) + \lambda$ $\quad \lambda \in F$

$f(\alpha) = (\alpha - \alpha)q(\alpha) + \lambda = \lambda$

$\Rightarrow f(x) = (x - \alpha)q(x) + f(\alpha)$

So $f(\alpha) = 0 \Leftrightarrow (x - \alpha) \mid f(x)$

$\Leftrightarrow (x - \alpha) \in f(x)$

**OBSERVATION**

$(F[x])^\times = F^\times$ invertible elements

**DEF:** Let $f(x) \in F[x] \setminus F$ then we say that (i.e $\deg f \geq 1$)

$f(x)$ is <u>irreducible</u> if whenever $f(x) = a(x)b(x)$ then

$a(x) \in F[x]^\times$ OR $b(x) \in F[x]^\times$

(1) If $\deg f(x) = 1$ then $f(x)$ is irreducible

(2) $x^2 - 3x + 2 \in \mathbb{Q}[x]$

$= (x-1)(x-2)$ is <u>not</u> irreducible.

**THEOREM** [214] If $f(x) \in F[x]$ and $2 \leq \deg f(x) \leq 3$ then $f$ is irreducible

$\Longleftrightarrow f$ does not have a root in $F$, i.e.

$f(a) \neq 0,\ \forall a \in F$

PROOF

$(\Rightarrow)$ If $f(x)$ is irreducible

Let $a \in F$

$f(x) = (x-a)q(x) + f(a)$

if $f(a) = 0 \Rightarrow f(x) = (x-a)q(x)$

$(\Leftarrow)$ Suppose $\forall a \in F$ $f(a) \neq 0$

Suppose $f(x)$ is not irreducible then $f(x) = a(x)b(x)$,

w/ $1 \leq \deg a(x)$

$1 \leq \deg b(x)$

WLOG $\deg a(x) = 1$

$a(x) = ax + b \Rightarrow f(-b/a) = 0$

$(x^2+1)^2 \in \mathbb{R}[x]$ does not have a root in $\mathbb{R}$ but not irreducible.

Recall

- We fixed a field F. We want to understand $F[x]$

- Note that $(F[x])^\times = F^\times$

- We have showed that if $I \subseteq F[x]$ then $\exists f(x) \in F[x]$ s.t. $I = (f(x))$

**DEF**

Suppose that $f(x), g(x) \in F[x] \setminus \{0\}$

We say that $d(x)$ is a greatest common divisor if

$d(x) \mid f(x)$ & $d(x) \mid g(x)$ also has the property

that whenever $e(x) \mid f(x)$ and $e(x) \mid g(x) \Rightarrow e(x) \mid d(x)$

$\Leftrightarrow \{e(x) \mid e(x) \mid f(x) \text{ and } e(x) \mid g(x)\} = \{e(x) \mid e(x) \mid d(x)\}$

Does a gcd exist and is it unique?

*Observation*

Even if a gcd of $f(x)$ and $g(x)$ exists, it is $\boxed{\text{not unique}}$

b/c if $d(x)$ satisfy the above hypothesis then

so does $\lambda \cdot d(x)$ for any $\lambda \in F[x]^{\times} = F^{\times}$

(Note that if $\lambda \in F[x]^{\times}$ then $a(x) \mid b(x) \Leftrightarrow \lambda a(x) \mid b(x)$
$\Leftrightarrow a(x) \mid \lambda b(x)$

---

*Lemma*

If $d(x)$ and $\tilde{d}(x)$ are two greatest common divisors of $f(x)$ and $g(x)$ then $\exists \lambda \in F[x]^{\times}$ s.t. $\tilde{d}(x) = \lambda d(x)$

PROOF

Since $\tilde{d}(x)$ is a common divisor of $f(x)$ and $g(x)$

$\Rightarrow \tilde{d}(x) \mid f(x)$ and $\tilde{d}(x) \mid g(x)$

$\Rightarrow \tilde{d}(x) \mid d(x)$ (1)

$d(x)$ is a gcd.

By symmetry

$d(x) \mid \tilde{d}(x)$ (2)

(1) $\Rightarrow d(x) = \tilde{d}(x) \cdot a(x)$

(2) $\Rightarrow \tilde{d}(x) = d(x) \cdot b(x)$

$d(x) = a(x) b(x) d(x)$

$\Rightarrow d(x)(1 - a(x)b(x)) = 0$

$\underset{\substack{d(x) \neq 0 \\ F[x] \text{ int. dom}}}{\Longrightarrow} 1 - a(x)b(x) = 0 \Rightarrow a(x)b(x) \in F[x]^{\times}$

*Existence of G.C.D*

Let $f(x), g(x)$ $\neq 0$

then $I = (f(x), g(x))$
$= \{a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in F[x]\}$
$\subseteq F[x]$

$\underset{\substack{\text{ideals in } F[x] \\ \text{are principal} \\ \text{generated by an element}}}{\Longrightarrow}$ $\exists d(x)$ s.t

$(d(x)) = (f(x), g(x)) = I$

CLAIM $d(x)$ is a gcd of $f(x)$ and $g(x)$.

PROOF $f(x), g(x) \in I = (d(x)) \Rightarrow d(x) \mid f(x)$ and $g(x)$

Suppose $e(x) | f(x)$ and $e(x) | g(x)$

$\Rightarrow \exists\ r(x), s(x) \in F[x]$ s.t.

$e(x).r(x) = f(x)$

$e(x).s(x) = g(x)$

But $d(x) \in (f(x), g(x))$

$\Rightarrow \exists\ a(x), b(x)$ s.t.

$\Rightarrow d(x) = a(x) f(x) + b(x) g(x)$

$= a(x) r(x) e(x) + b(x) s(x) e(x)$

$= (a(x) r(x) + b(x) s(x)) e(x)$

$\Rightarrow e(x) | d(x)$

Therefore gcd of $f(x)$ and $g(x)$ exist

Moreover, if $d(x)$ is a gcd then

$(f(x), g(x)) = (d(x))$

**DEF** We say that $f(x)$ and $g(x)$ are relatively prime if $\gcd(f(x), g(x)) = 1$

$\Leftrightarrow (f(x), g(x)) = F[x]$

$\Leftrightarrow \exists\ a(x), b(x) \in F[x]$ s.t

$a(x) f(x) + b(x) g(x) = 1$

*Lemma*

Suppose that $p(x) \in F[x]$ is irreducible and $p(x) | f(x) g(x)$ then either $p(x) | f(x)$ or $p(x) | g(x)$

PROOF

Suppose $p(x) \nmid f(x)$

$d(x) = (p(x), f(x))$

$d(x) | p(x) \Rightarrow$

$\exists\ a(x)$ s.t.

$d(x) a(x) = p(x)$

$\Rightarrow$ either $d(x) \in F[x]^\times$

or $a(x) \in F[x]^\times$

Suppose $a(x) \in F[x]^\times$

$\Rightarrow p(x) | d(x)$, $d(x) | f(x)$

since $d(x) = (p(x), f(x))$

$\Rightarrow p(x) | f(x)$

$\therefore d(x) \in F[x]^\times \Rightarrow 1 = (p(x), f(x))$

$\Rightarrow \exists\ a(x), b(x) \in F[x]$ s.t $1 = a(x) p(x) + b(x) f(x)$

$\Rightarrow g(x) = \underbrace{g(x) a(x) . p(x)}_{p(x)|} + \underbrace{b(x) f(x) g(x)}_{p(x)|} \Rightarrow p(x) | g(x)$

217 **THEOREM** (Analog of the main theorem of arithmetic)

Let $f(x) \in F[x] \setminus F$

then $f(x) = p_1(x) \dots p_r(x)$ s.t. all $p_i(x)$ are irreducible

Moreover this decomposition into irreducibles is unique up to ordering and up to multiplication by a unit.

PROOF

*Existence*

Suppose that there is an $f(x) \in F(x) \setminus F$ s.t. $f(x)$ cannot be written as a product of irreducibles.

$$\mathcal{S} = \left\{ a(x) \,\middle|\, \begin{array}{l} a(x) \in F[x] \setminus F \\ a(x) \text{ cannot be written} \\ \text{as a product of irreducibles} \end{array} \right\}$$

$\mathcal{S} \neq \emptyset$

Let $r(x) \in \mathcal{S}$ s.t. $\deg r(x)$ is smallest among all $a(x) \in \mathcal{S}$

$r(x)$ is not irreducible then

$$r(x) = s_1(x) s_2(x) \quad \text{s.t. } \deg s_i(x) \geq 1$$

$\Longrightarrow \deg s_i(x) < \deg r(x)$

$\Longrightarrow s_i(x) \notin \mathcal{S}$

$\Longrightarrow s_1(x) = t_1(x) \cdots t_k(x)$

$s_2(x) = q_1(x) \cdots q_\ell(x)$

s.t. $t_i(x), q_j(x)$ are irred.

$$r(x) = s_1(x) s_2(x) = t_1(x) \cdots t_k(x) q_1(x) \cdots q_j(x)$$

UNIQUENESS

Suppose

① $f(x) = p_1(x) \cdots p_r(x)$

② $f(x) = q_1(x) \cdots q_s(x)$

① $\Rightarrow p_1(x) \mid f(x) = q_i(x) \cdots q_s(x)$

$\Rightarrow p_1(x) \mid q_i(x)$ WLOG assume $i=1$

A poly. previous lemma $(s-1)$ times

$\Longrightarrow p_1(x) \mid q_1(x) \underset{\text{both irred}}{\Longrightarrow} \exists \lambda \in F[x]^\times$ s.t.

$q_1(x) = \lambda p_1(\lambda)$

cancel $p_1(x)$, continue ...