$\alpha \in S_n$ permutation

α even $\Leftrightarrow$ α is a product of $\begin{matrix}\text{(odd)}\\ \text{even}\\ \text{(odd)}\end{matrix}$ # of transpositions

Thm: $\alpha \in S_n \Rightarrow \alpha$ even or odd, but not both.

Ex (1) $S_3 = \{(1), (12), (13), (23), (132), (123)\}$

(1): even

$(12), (13), (23)$: odd

$(132) = (12)(13)$, $(123) = (13)(12)$: even

Defn: $A_n = \{\alpha \in S_n \mid \alpha \text{ even}\}$

$\alpha, \beta \in A_n \Rightarrow \alpha\beta$ even $\Rightarrow \alpha\beta \in A_n$

$e = (1) \in A_n$

α even $\Rightarrow \alpha^{-1}$ even $\Rightarrow \alpha^{-1} \in A_n$

($\alpha = \underbrace{\beta_1 \beta_2 \cdots \beta_{2m}}_{\text{transpositions}} \Rightarrow \alpha^{-1} = \beta_{2m}^{-1} \beta_{2m-1}^{-1} \cdots \beta_2^{-1} \beta_1^{-1} = \beta_{2m} \beta_{2m-1} \cdots \beta_1$)

$\therefore A_n$ subgroup of S_n.

A_n is called the "alternating" group.

$|A_n| = \frac{1}{2} n!$

Ex(2) $\alpha \in S_6$

What are the possible orders of α?

$\alpha = (1) \Rightarrow o(\alpha) = 1$

$\alpha = (12) \Rightarrow o(\alpha) = 2$

$\alpha = (123) \Rightarrow o(\alpha) = 3$

$\alpha = (1234) \Rightarrow o(\alpha) = 4$

$\alpha = (12345) \Rightarrow o(\alpha) = 5$

$\alpha = (123456) \Rightarrow o(\alpha) = 6$

Ex(3) $\alpha \in S_7$ $o(\alpha) = ?$

$\alpha = (1) \Rightarrow o(\alpha) = 1$

$\alpha = (12) \Rightarrow o(\alpha) = 2$

$\alpha = (123) \Rightarrow o(\alpha) = 3$

$\alpha = (1234) \Rightarrow o(\alpha) = 4$

$\alpha = (12345) \Rightarrow o(\alpha) = 5$

$\alpha = (123456) \Rightarrow o(\alpha) = 6$

$\alpha = (1234567) \Rightarrow o(\alpha) = 7$

$\alpha = (12)(34567) \Rightarrow o(\alpha) = 10$

$\alpha = (123)(4567) \Rightarrow o(\alpha) = 12$

Ex(4) $\alpha \in A_6$, $o(\alpha) = ?$

$\alpha = (1) \Rightarrow o(\alpha) = 1$

$\alpha = (12)(34) \Rightarrow o(\alpha) = 2$

$\alpha = (123) \Rightarrow o(\alpha) = 3$

$\alpha = (12)(3456) \Rightarrow o(\alpha) = 4$

$\alpha = (12345) \Rightarrow o(\alpha) = 5$

~~$\alpha = (12)(345)$~~

G, G' groups.

Defn: A map $f: G \longrightarrow G'$ is a homomorphism if

$\forall\, a, b \in G$, $f(ab) = f(a)f(b)$

Defn: A homomorphism $f: G \to G'$ which is 1-1 and onto is called an isomorphism.

Ex(5) $G = \langle a \rangle$, $o(a) = n$

Consider the map

$$f: G \longrightarrow \mathbb{Z}_n$$

$$f(a^i) = i \pmod n$$

(Recall $G = \{e, a, a^2, \cdots, a^{n-1}\}$ &

$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$)

Clearly f is 1-1 and onto.

Let $a^i, a^j \in G$

$$f(a^i a^j) \stackrel{?}{=} f(a^i) + f(a^j)$$

$$\| $$

$$f(a^{i+j})$$

If $(i+j) \bmod n = k$ ($\Leftrightarrow i+j = nt + k$, $0 \le k \le n-1$)

Then $a^{i+j} = a^k$ since $a^n = e$.

$$\Rightarrow f(a^i a^j) = k = (i+j) \bmod n$$

$$f(a^i) + f(a^j) = i \pmod n + j \pmod n$$

$$= (i+j) \bmod n = k$$

$$= f(a^i a^j)$$

$\therefore$ f is a hom. and hence an isomorphism.

<u>Notation:</u> $G \approx \mathbb{Z}_n$

($\approx$: isomorphic to)

Ex(6) $f : \mathbb{Z} \longrightarrow 2\mathbb{Z}$

given by $f(n) = 2n$

hom? $f(n_1 + n_2) \overset{?}{=} f(n_1) + f(n_2)$

$$\begin{array}{ccc} f(n_1+n_2) & \overset{?}{=} & f(n_1)+f(n_2) \\ \| & & \| \\ 2(n_1+n_2) & = & 2n_1 + 2n_2 \end{array}$$

Yes.

1-1? $f(n) = f(m)$

$$\begin{array}{ccc} f(n) & = & f(m) \\ \| & & \| \\ 2n & = & 2m \end{array}$$

$\therefore \; n = m$

Yes.

Onto? $2m \in 2\mathbb{Z} \Rightarrow m \in \mathbb{Z}$

and $f(m) = 2m$

Yes.

$\Rightarrow$ f is an isomorphism &

$$\mathbb{Z} \approx 2\mathbb{Z}$$

P113 #19

$\alpha, \beta \in S_n$

$\alpha = \alpha_1 \alpha_2 \cdots \alpha_r$ (product of trans.)

$\beta = \beta_1 \beta_2 \cdots \beta_s$

$\alpha\beta$ even $\iff r+s$ is even

$\iff$ r & s even
or r & s odd

$\iff$ α, β are both even
or both odd.

P114 #32.

$$\beta = (123)(145)$$
$$= (14523)$$
$$\Rightarrow \beta^5 = (1) = e$$
$$\Rightarrow \beta^{99} = \beta^{100}\beta^{-1} = \underbrace{\left(\beta^5\right)^{20}}_{(1)}\beta^{-1} = \beta^{-1}$$
$$= (32541)$$
$$= (13254)$$

G, G' group

$f: G \longrightarrow G'$ is an isomorphism if

(1) $\forall\, a, b$, $f(ab) = f(a)f(b)$

& (2) f is 1-1 and onto

Ex(1) $G = (\mathbb{R}, +)$, $G' = (\mathbb{R}_{>0}, \cdot)$

$f: \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ given by

$f(x) = e^x \quad \forall\, x \in \mathbb{R}$.

(1) Let $x, y \in \mathbb{R}$

$$f(x+y) \overset{?}{=} f(x)f(y)$$

$$\| \qquad\qquad \| \checkmark$$

$$e^{x+y} = e^x e^y$$

$\therefore$ f is a hom.

(2) 1-1: $f(x) = f(y)$

$\Rightarrow e^x = e^y$

$\Rightarrow x = y$

onto: $a \in \mathbb{R}_{>0}$ $\ln a \in \mathbb{R}$

and $f(\ln a) = e^{\ln a} = a$

$\therefore \mathbb{R} \approx \mathbb{R}_{>0}$.

Properties of isomorphism:

Suppose $f: G \longrightarrow G'$ is an isom.

Then we have:

(1) $e \in G$, $e' = f(e) \in G'$

(2) $a \in G$, $f(a^{-1}) = (f(a))^{-1}$

(3) $a \in G$, $o(a) = o(f(a))$

(4) G abelian $\Longrightarrow$ G' abelian

(5) G cyclic $\Longrightarrow$ G' cyclic

$(G = \langle a \rangle) \Rightarrow (G' = \langle f(a) \rangle)$

(6) H subgroup of G. Then

$H' = \{ f(h) \mid h \in H \}$ is a subgroup of G'.

Remark: Isomorphism among groups is an equivalence relation.

Ex(2) $U(5) = \{1, 2, 3, 4\}$

$U(10) = \{1, 3, 7, 9\}$

Is $U(10) \approx U(5)$?

$U(5)$: $o(2) = 4 \Rightarrow U(5) = \langle 2 \rangle \approx \mathbb{Z}_4$

$U(10)$: $o(3) = 4 \Rightarrow U(10) = \langle 3 \rangle \approx \mathbb{Z}_4$

$U(5) \approx \mathbb{Z}_4 \approx U(10) \Rightarrow U(5) \approx U(10)$.

Ex(3) Is $U(10)$ isom. to $U(8)$?

$U(8) = \{1, 3, 5, 7\}$

$o(3) = 2$, $o(5) = 2$, $o(7) = 2$

$\Rightarrow$ $U(8)$ not cyclic, but $U(10)$ is cyclic

$\Rightarrow U(10) \not\approx U(8)$.

Defn: An isomorphism $f: G \to G$ is called an automorphism.

Ex(4) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$1 \longrightarrow \begin{cases} 1 \\ -1 \end{cases}$ $\Rightarrow$ $\varphi_1 : \mathbb{Z} \to \mathbb{Z}$ (identity), $1 \mapsto 1$

$\Rightarrow$ $\varphi_{-1} : \mathbb{Z} \to \mathbb{Z}$, $1 \mapsto -1$

$Aut(\mathbb{Z})$ = set of all automor. on $\mathbb{Z}$

$= \{\varphi_1, \varphi_{-1}\} \approx \mathbb{Z}_2$

G group

An isom. $\varphi: G \to G$ is called an automorphism.

$$Aut(G) = \{\varphi: G \to G \mid \varphi \text{ automorphism}\}$$

$(Aut(G), \circ)$ is a group.

Ex(1) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$\varphi: \mathbb{Z} \to \mathbb{Z}$ automorphism

$$\varphi(1) = \begin{cases} 1 \\ -1 \end{cases}$$

$$\varphi_1: \mathbb{Z} \to \mathbb{Z}, \quad 1 \mapsto 1 \quad \Rightarrow \varphi_1(m) = m.$$

$$\varphi_{-1}: \mathbb{Z} \to \mathbb{Z}, \quad 1 \mapsto -1 \quad \Rightarrow \varphi_{-1}(m) = -m.$$

$$Aut(\mathbb{Z}) = \{\underbrace{\varphi_1}_{\text{"id"}}, \varphi_{-1}\}, \quad o(\varphi_{-1}) = 2$$

since $\varphi_{-1}^2(1) = \varphi_{-1}(\varphi_{-1}(1)) = \varphi_{-1}(-1) = -\varphi_1(1)$

$= 1$

$$\Rightarrow \varphi_{-1}^2 = \varphi_1$$

$$\Rightarrow Aut(\mathbb{Z}) = \langle \varphi_{-1} \rangle \approx \mathbb{Z}_2.$$

Ex(2) $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$= \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

$\varphi : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_{10}$ automorphism

$$\varphi(1) = \begin{cases} 1 \\ 3 \\ 7 \\ 9 \end{cases}$$

$\Rightarrow Aut(\mathbb{Z}_{10}) = \{\varphi_1, \varphi_3, \varphi_7, \varphi_9\}$

where $\varphi_1(1) = 1$, $\varphi_3(1) = 3$, $\varphi_7(1) = 7$, $\varphi_9(1) = 9$.

$\circ$	φ_1 (= e)	φ_3	φ_7	φ_9
$e = \varphi_1$	φ_1	φ_3	φ_7	φ_9
φ_3	φ_3	φ_9	φ_1	φ_7
φ_7	φ_7	φ_1	φ_9	φ_3
φ_9	φ_9	φ_7	φ_3	φ_1

$\varphi_3^{-1} = \varphi_7$, $o(\varphi_3) = 4$

$\varphi_9^{-1} = \varphi_9$, $o(\varphi_9) = 2$

$o(\varphi_7) = 4$

$U(10) = \{1, 3, 7, 9\}$

$f : Aut(\mathbb{Z}_{10}) \longrightarrow U(10)$

$$\left.\begin{aligned} f(\varphi_1) &= 1 \\ f(\varphi_3) &= 3 \\ f(\varphi_7) &= 7 \\ f(\varphi_9) &= 9 \end{aligned}\right\} \Rightarrow f \text{ is an isomorphism}$$

$\Rightarrow Aut(\mathbb{Z}_{10}) \approx U(10)$.

In general,

$$\mathbb{Z}_n = \langle k \rangle \iff \gcd(k,n) = 1$$

$$U(n) = \{k \in \mathbb{Z}_n \mid \gcd(k,n) = 1\}$$

Thm: $Aut(\mathbb{Z}_n) \approx U(n)$.

Cayley's Thm: Any group is isomorphic to a group of permutations.

Pf (idea)

G group. For $a \in G$ define a map $T_a : G \to G$ by $T_a(x) = ax$ $\forall x \in G$.

Then $\forall a \in G$, T_a is a 1-1 and onto map.

Set $G' = \{T_a : a \in G\}$

$(G', \circ)$ is a group (hence a permutation group.)

Define $\varphi : G \to G'$ by

$\varphi(a) = T_a$ for all $a \in G$

Claim: φ is an isomorphism.

HW P132 #1, 3, 5, 6, 8, 16, 22, 24, 30, 36, 38, 39, 41, 53

10/9

P134 #38

$$G = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$$H = \left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q}\right\}$$

$$\varphi : G \longrightarrow H, \quad \varphi(a+b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$$

Clearly φ is 1-1 & onto. (Verify)

$$\varphi\left((a+b\sqrt{2}) + (a'+b'\sqrt{2})\right) \stackrel{?}{=} \varphi(a+b\sqrt{2}) + \varphi(a'+b'\sqrt{2})$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$\varphi\left((a+a') + (b+b')\sqrt{2}\right) \qquad \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix}$$

$$\|$$

$$\begin{pmatrix} a+a' & 2b+2b' \\ b+b' & a+a' \end{pmatrix} \;//$$

$\Rightarrow$ φ is a homomorphism, hence an isomorphism.

$\Rightarrow$ $G \cong H$.

$$(a+b\sqrt{2})(a'+b'\sqrt{2}) = (aa'+2bb') + (ab'+a'b)\sqrt{2} \in G$$

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa'+2bb' & 2(ab'+a'b) \\ ab'+a'b & aa'+2bb' \end{pmatrix} \in H$$

$\Rightarrow$ G & H are closed under multiplication

$$\varphi((a+b\sqrt{2})(a'+b'\sqrt{2})) \stackrel{?}{=} \varphi(a+b\sqrt{2})\varphi(a'+b'\sqrt{2})$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$\varphi((aa'+2bb')+(ab'+a'b)\sqrt{2}) \qquad \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix}$$

$$\|$$

$$\begin{pmatrix} aa'+2bb' & 2(ab'+a'b) \\ ab'+a'b & aa'+2bb' \end{pmatrix}$$

yes

Yes, φ preserves the multiplication.

G group & H subgroup of G.

For $a, b \in G$ define

$$a \sim b \text{ if } ab^{-1} \in H$$

- $a \sim a$ since $aa^{-1} = e \in H$
- $a \sim b \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H$

  $\|$

  ba^{-1}

  $\Rightarrow b \sim a.$
- $a \sim b$ & $b \sim c \Rightarrow ab^{-1}, bc^{-1} \in H$

  $\Rightarrow \underbrace{(ab^{-1})(bc^{-1})}_{\|} \in H \Rightarrow a \sim c$

  ac^{-1}

$\therefore \sim$ is a equivalence relation on G.

For $a \in G$

$$[a] = \{x \in G \mid a \sim x\}$$
$$= \{x \in G \mid x \sim a\}$$
$$= \{x \in G \mid xa^{-1} \in H\}$$
$$= \{x \in G \mid xa^{-1} = h \in H\}$$
$$= \{ha \mid h \in H\} := Ha$$

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

Similarly, $aH = \{ah \mid h \in H\}$ is called a left coset of H in G.

Since right (left) cosets are equiv. classes we have:

- $a \in Ha \quad (a \in aH)$
- $b \in Ha \Rightarrow Ha = Hb$
- $Ha = H \Leftrightarrow a \in H$

$\quad\quad\quad\;\; \overset{\shortparallel}{He}$

Ex(1) $G = \mathbb{Z}$, $H = \langle 3 \rangle = 3\mathbb{Z}$

$0 + H = H = \{0, \pm 3, \pm 6, \cdots\}$

$1 + H = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$

$2 + H = \{\cdots, -4, -1, 2, 5, 8, \cdots\}$

$\Rightarrow \mathbb{Z} = H \cup (1+H) \cup (2+H)$