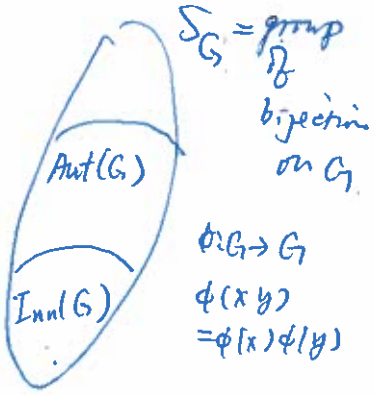
Define: A group isom. $\phi: G \to G$ is called a group automorphism

Definition Let G be a group, and $a \in G$. Then $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is an automorphism. (called an inner automorphism)

Theorem 6.4 Under function composition, the set $Aut(G)$ of group automorphisms is a group, and the set $Inn(G)$ of inner automorphisms is a subgroup. $\subseteq S_G$

~~Fact~~

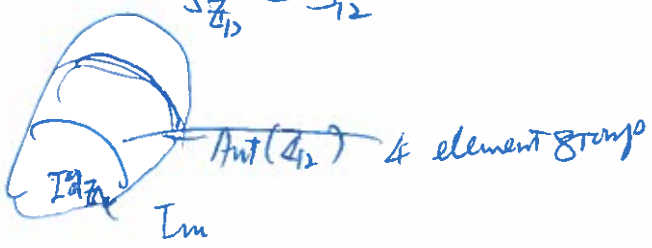


Theorem 6.5 [**Automorphisms of $\mathbb{Z}_n$**] The groups $Aut(\mathbb{Z}_n)$ is isomorphic to $(U(n), \cdot)$ with

$$U(n) = \{k \in \mathbb{Z}_n : \gcd(k, n) = 1\}.$$ under multiplication (mod n)

Example: $\mathbb{Z}_{12} = \{\bar{0}, \cdots, \bar{11}\}$ under +

$U(12) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$ under ·



Fact: $Aut(G) = \{\phi : \phi \text{ is an isomorphism from } G \text{ to } G\}$.

$Aut(G) \leq S_G$.

Clearly. $Aut(G) \subseteq S_G$

1° $Aut(G)$ is non-empty because $Id_G : G \to G$.
defined by $Id_G(x) = x \ \forall x \in G$ satisfies:

Id $Id_G(xy) = xy = Id_G(x)\, Id_G(y)$
$\forall x, y \in G$.

& Id_G is bijective. ✓

2° Suppose $f, g \in Aut(G)$. $f, g : G \to G$

Then f, g are bijections
&
$f(xy) = f(x) f(y)$
$g(xy) = g(x) g(y)$ $\forall x, y \in G$

$\therefore$ $f \circ g : G \to G$ is a bijection

& $(f \circ g)(xy) = f(g(xy)) = f(g(x) g(y))$
$= f(g(x)) f(g(y)) = (f \circ g)(x)(f \circ g)(y)$

$\forall x, y \in G$

3° $f : G \to G$ is isomorphism.
Then $f^{-1} : G \to G$ is an isom.

By 1°–3°, $Aut(G) \leq S_G$.

~~$f_a: G \to G$~~
~~$f_a(x) = ax$~~

Fact (cont'd).

Let $a \in G$.

Define $\phi_a : G \to G$ by $\phi_a(x) = axa^{-1}$ $\forall\, x \in G$.

Then ϕ_a ~~is a group~~ $\in Aut(G)$

because 1° ϕ_a is bijective.

& 2° $\phi_a(xy) = \phi_a(x)\phi_a(y)$ $\forall x, y \in G$.

as illustrated in the following.

1.1° $\forall x \in G$ then $\phi_a(x) = axa^{-1} \in G$. So ϕ_a is well-defined

1.2° one-one: $\phi_a(x) = \phi_a(y)$

$\Rightarrow$ $axa^{-1} = aya^{-1}$

$\Rightarrow$ $ax = ay$ by right cancellation

$\Rightarrow$ $x = y$ by left cancellation.

1.3° For any $b \in G$, let $x \in G$ with $x = aba^{-1}$

$\phi_a(x) = axa^{-1} = b$.

2° $\forall x, y \in G$,

$\phi_a(xy) = a(xy)a^{-1}$

$= ax(aa^{-1})ya^{-1}$

$= (axa^{-1})(aya^{-1})$

$= \phi_a(x)\phi_a(y)$

Next. Prove $Inn(G) = \{\phi_a : a \in G\} \leq Aut(G)$

If G is Abelian then $Inn(G) = \{Id_G\}$

To prove $Inn(G) \leq Aut(G)$.

1° $Inn(G)$ contains $Id_G = \phi_e$, $e \in G$ because

$\phi_e(x) = exe^{-1} = x \quad \forall x \in G$.

2° Let $\phi_a, \phi_b \in Inn(G)$.

Then $\phi_a \circ \phi_b(x) = \phi_a(bxb^{-1})$

$= a(bxb^{-1}a^{-1}) = cxc^{-1} \quad \forall x \in G$

for $c = ab$

$\therefore \phi_a \circ \phi_b = \phi_c \in Inn(G)$

with $c = ab$.

3° Let $\phi_a \in Inn(G)$

Then $\phi_a \circ \phi_{a^{-1}}(x)$

~~$\phi_a^{-1}(x) = a$~~

$= \phi_a(a^{-1}x(a^{-1})^{-1})$

$= \phi_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$

$\forall x$.

$\therefore (\phi_a)^{-1} \in Inn(G)$

$\therefore \phi_a \circ \phi_{a^{-1}} = \phi_a \circ (\phi_a)^{-1} = Id_G$

By left cancellation

$(\phi_a)^{-1} = \phi_{a^{-1}} = \phi_c \in Inn(G)$.

$c = a^{-1}$

Proof:

Consider $Aut(\mathbb{Z}_n)$.

Let $\phi: \mathbb{Z}_n \to \mathbb{Z}_n$ be an automorphism.

Suppose $\phi(\bar{1}) = \bar{m} \in \mathbb{Z}_n$.

Then $\phi(\bar{k}) = \phi(\bar{1} + \cdots + \bar{1})$ (k terms)

$= \phi(\bar{1}) + \cdots + \phi(\bar{1}) = \overline{km}$ (k terms).

So, $\{\underbrace{\phi(\bar{1}) + \cdots + \phi(\bar{1})}_{m} : m = 0, \ldots, n-1\}$

$= \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$.

$\therefore$ $\phi(\bar{1}) = \bar{k}$ is a generator of $\mathbb{Z}_n$

$\therefore$ $\gcd(n,k) = 1$.

Every k with $\gcd(n,k)=1$ corresponds to one automorphism of $\mathbb{Z}_n$.

Define $\bar{\Phi}: \mathcal{U}(n) \to Aut(\mathbb{Z}_n)$

by $\bar{\Phi}(\bar{k}) = f_{\bar{k}}$

such that $f_{\bar{k}}: \mathbb{Z}_n \to \mathbb{Z}_n$ satisfying

$f_{\bar{k}}(\bar{m}) = \overline{km}$ $\forall \bar{m} \in \mathbb{Z}_n$.

Then $f_{\bar{k}} \in Aut(G)$.

$\phi: G_1 \to G_2$ is an

$G_1 = \langle a \rangle$

$\langle \phi(a) \rangle = G_2$

$\mathbb{Z}_{12} \to \mathbb{Z}_{12}$

$1, 3, 5, 7 \in \mathcal{U}(12)$

$\updownarrow$

$f_{\bar{1}}(\bar{m}) = Id_{\mathbb{Z}_{12}}$

$f_{\bar{5}}(\bar{m}) = \overline{5m}$ $\forall m \in \mathbb{Z}_{12}$

$f_{\bar{7}}(\bar{m}) = \overline{7m}$ $\forall m \in \mathbb{Z}_{12}$

$f_{\overline{11}}(\bar{m}) = \overline{11m}$ $\forall m \in \mathbb{Z}_{12}$

So $\bar{\Phi} : \mathcal{U}(n) \to \mathrm{Aut}(\mathbb{Z}_n)$ is well-defined

[Check $f_{\bar{k}}$ is an automorphism]

Next. Show that $\bar{\Phi}$ is bijective, clear. ✓

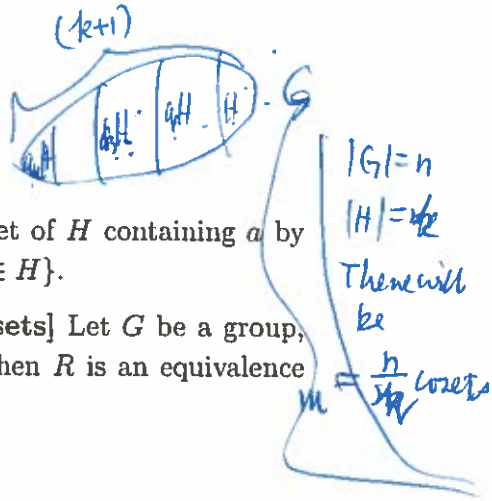
Check: $\bar{\Phi}(\bar{k}_1 \cdot \bar{k}_2) = \bar{\Phi}(\bar{k}_1) \circ \bar{\Phi}(\bar{k}_2) \quad \forall \bar{k}_1, \bar{k}_2 \in \mathcal{U}(n)$

$\bar{\Phi}(\bar{k}_1 \cdot \bar{k}_2) = f_{\bar{k}_1 \cdot \bar{k}_2}$ s.t.

$f_{\bar{k}_1 \bar{k}_2}(\bar{x}) = \overline{k_1 k_2 x} \quad \forall \bar{x} \in \mathbb{Z}_n$

$\bar{\Phi}(\bar{k}_1) \cdot \bar{\Phi}(\bar{k}_2) = f_{\bar{k}_1} \circ f_{\bar{k}_2}$ s.t.

$f_{\bar{k}_1} \circ f_{\bar{k}_2}(\bar{x}) = f_{\bar{k}_1}(\bar{k}_2 \bar{x}) = \overline{k_1 (k_2 x)} = \overline{k_1 k_2 x} \quad \forall x \in \mathbb{Z}_n$



Chapter 7 Cosets and Lagrange's Theorem

Definition Let G be a group and $H \leq G$. For $a \in G$ define the left coset of H containing a by $aH = \{ah : h \in H\}$ and the right coset of H containing by $Ha = \{ha : h \in H\}$.

Theorem 7.1 [LaGrange's Theoerem and other properties of cosets] Let G be a group, and $H \leq G$. Define a relation on R on G by $(a, b) \in R$ if $a^{-1}b \in H$. Then R is an equivalence relation so that the left cosets are equivalence classes.

(a) We have $aH = bH$ if and only if $a^{-1}b \in H$.

(b) The group G is a union of disjoint left cosets of H.

(c) The map $ah \mapsto bh$ is a bijection between two cosets aH and bH.

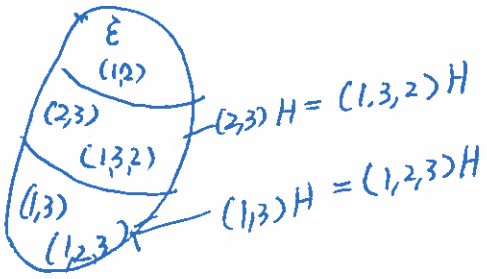
(d) If G is finite, then it is a disjoint union of m left cosets of H with $m = |G|/|H|$.

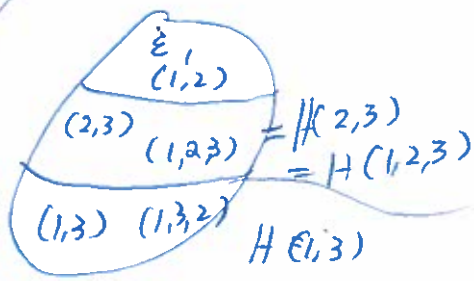
$(2,3)(1,2) = (1,3,2)$.

Example S_3 $G = S_3$, $H = \{\varepsilon, (1,2)\}$

$(2,3)H = \{(2,3), (1,2,3)\}$ $\quad H(2,3) = \{(2,3), (1,2,3)\}$

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





Proof: Define R on G by $(a,b) \in R$ if $a^{-1}b \in H$.

Reflexive: For every $a \in G$, $a^{-1}a = e \in H$, $\therefore (a,a) \in R$

Symmetric: Suppose $(a,b) \in R$, i.e., $a^{-1}b \in H$, $(a^{-1}b)^{-1} \in H$, $\therefore b^{-1}a \in H$, $\therefore (b,a) \in R$

Transitive: Suppose $(a,b), (b,c) \in R$.

Then $a^{-1}b \in H$, $b^{-1}c \in H$, $\therefore (a^{-1}b)(b^{-1}c) \in H$, $\therefore (a,c) \in R$

$a^{-1}c$

$\therefore$ R is an equivalence relation on G.

(a) Let $a \in G$. The equivalence class

$$[a] = \{x \in G : (a,x) \in R\}$$
$$= \{x \in G : a^{-1}x \in H\}$$
$$= \{x \in G : a^{-1}x = h \text{ for some } h \in H\}$$
$$= \{x \in G : x = ah, h \in H\} = \{ah : h \in H\}.$$

Example: $G = \mathbb{Z}$. Infinite;

$H = \{\text{even integers}\}$

$H, \quad 1+H$

For $H = \langle k \rangle = k\mathbb{Z}$

$0 + \langle k \rangle = \bar{0}$

$1 + \langle k \rangle = \bar{1}$

$\vdots$

$k-1 + \langle k \rangle = \overline{k-1} \quad \in \mathbb{Z}_k$

Fact — There are finitely many cosets.

Example.

G - infinite

$H \leq G$

Infinitely many cosets of H