Group Theory

Week #3, Class #10

I Group Homomorphisms, Isomorphisms, and Automorphisms

Recall some definitions:

1. Hom A homomorphism is a function $\varphi: G_1 \longrightarrow G_2$ between two groups, satisfying:

$$(*) \quad \boxed{\varphi(ab) = \varphi(a)\cdot\varphi(b) \qquad \forall a,b \in G_1}$$

Here we use $\cdot$ for the operation on both sides. If the groups are abelian (i.e., commutative), we usually use $+$ for the respective ops, and $(*)$ is written as

$$(**) \quad \boxed{\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \forall a,b \in G_1}$$

Extended example (connection w/ Linear Algebra)

- Let V be a vector space (over a field F)
  (usually $F=\mathbb{R}$ but could also be $F=\mathbb{Q}$, $\mathbb{C}$, or $F=\mathbb{Z}_p$)

- $F = (F, +, \circ)$
  - $(F, +, 0)$ abelian group
  - $(F^\times, \circ, 1)$ also abelian group
    - distributes through sums $a(b+c) = ab + ac$

- Eg: $V = \mathbb{R}^n, \mathbb{Q}^n, \mathbb{C}^n, \mathbb{Z}_p^n$

- Then V has two ops: $\begin{cases} + & \text{(vector) addition} \\ \cdot & \text{scalar multiplication} \end{cases}$

$$V \times V \xrightarrow{+} V \qquad (v,w) \longmapsto v+w$$

$$F \times V \longrightarrow F \qquad (k,v) \longmapsto k\cdot v$$

- $V = (V, +, 0)$ is an abelian group (The underlying group of the v. space V)

- Also recall: A *linear transformation* between two vector spaces is a function $L: V \longrightarrow W$ which satisfies:

(1) $L(v_1+v_2) = L(v_1)+L(v_2)$, $\forall v_1, v_2 \in V$

(2) $L(kv) = k \cdot L(v)$, $\forall v \in V$, $\forall k \in F$

- Just retaining condition (1) [which is the same as (**)], we see that L is a homomorphism of the underlying groups.

Eg $L: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ $\quad L(x,y) = (x+2y, y-x)$ is lin transf, so also a hom.

note: $L\vec{v} = A\vec{v}$ for some matrix A

more precisely: $L: \mathbb{R}^m \longrightarrow \mathbb{R}^n$ then A is $n \times m$ matrix

in the above example: $A = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}$

check: $\begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x+2y \\ -x+y \end{bmatrix}$ ✓

Remark Not every group hom between two vector spaces is a linear transformation! $\boxed{z = x+iy \to \bar{z} = x-iy}$

Example $\varphi: \mathbb{C} \longrightarrow \mathbb{C}$ $\quad \varphi(z) = \bar{z}$ $\quad$ a group hom (or, an additive function)

i.e. $\varphi(z+w) = \varphi(z)+\varphi(w)$, since $\overline{z+w} = \bar{z}+\bar{w}$

But φ is not a $\mathbb{C}$-linear transformation between those two $\mathbb{C}$-vector spaces, since, e.g.:

$$\varphi(iz) = \overline{iz} = \bar{i}\,\bar{z} = -i\,\bar{z} \neq i\bar{z} = i\,\varphi(z) \quad (\text{if } z \neq 0)$$

Example Recall: $\exp: (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}_{>0}, \cdot, 1)$
$$x \longmapsto e^x$$
is a hom., since $e^{x+y} = e^x \cdot e^y$. In fact exp is an iso.

Example For any $a \in G$, we have a hom. $\varphi_a: \mathbb{Z} \longrightarrow G$, $\quad \varphi_a(n) = a^n$. Its image is $\varphi_a(\mathbb{Z}) = \langle a \rangle$

$\boxed{2. \text{ Iso}}$ **Def** An <u>isomorphism</u> is a function $\varphi: G_1 \to G_2$ between two groups which is both a homomorphism and a bijection.

- We saw that: (*) $\boxed{\text{If } \varphi: G_1 \to G_2 \text{ iso, then } \varphi^{-1}: G_2 \to G_1 \text{ iso}}$

<u>Lemma</u> (1) If $\varphi_1: G_1 \to G_2$ and $\varphi_2: G_2 \to G_3$ are hom, then $\varphi_2 \circ \varphi_1$ is also a hom.

(2) Moreover, if both φ_1 & φ_2 are isos then $\varphi_2 \circ \varphi_1$ is also an iso.

Proof (1)
$$(\varphi_2 \circ \varphi_1)(ab) \underset{\text{by def of } \circ}{=} \varphi_2(\varphi_1(ab)) \underset{\varphi_1 \text{ is hom}}{=} \varphi_2(\varphi_1(a)\varphi_1(b))$$
$$\underset{\varphi_2 \text{ is hom}}{=} \varphi_2(\varphi_1(a)) \cdot \varphi_2(\varphi_1(b))$$
$$\underset{\text{by def of } \circ}{=} (\varphi_2 \circ \varphi_1)(a) \cdot (\varphi_2 \circ \varphi_1)(b)$$

(2) The composition of any two bijections is again a bijection $\left(\underset{\text{bij}}{f_1: S_1 \to S_2},\ \underset{\text{bij}}{f_2: S_2 \to S_3} \Rightarrow (f_2 \circ f_1)^{-1} = f_1^{-1} \circ f_2^{-1} \right)$

$\boxed{\checkmark}$

Def Two groups are said to be <u>isomorphic</u> if there is an isomorphism between them:

$$G_1 \cong G_2 \overset{\text{def}}{\Longleftrightarrow} \exists\, \varphi: G_1 \to G_2 \text{ isomorphism}$$

<u>Lemma</u> $\cong$ is an equivalence relation on groups.

Proof
- Reflexivity ($G \cong G$): $id_G: G \to G$ is an iso
- Symmetry ($G_1 \cong G_2 \Rightarrow G_2 \cong G_1$): if $\varphi: G_1 \to G_2$ iso, then $\varphi^{-1}: G_2 \to G_1$ is also an iso by (*)
- Transitivity ($G_1 \cong G_2$ & $G_2 \cong G_3 \Rightarrow G_1 \cong G_3$): By Lemma, part (2) above

$\boxed{\checkmark}$

The equivalence classes under $\cong$ are called isomorphism classes of groups.

Examples (1) $\mathbb{Z}_4 \cong \langle i \rangle$ where $\mathbb{Z}_4 = (\{[0]_4, [1]_4, [2]_4, [3]_4\}, +, [0])$
$\langle i \rangle = (\{1, i, -1, -i\}, \cdot, 1)$

isomorphism: $\varphi: \mathbb{Z}_4 \longrightarrow \langle i \rangle$
$\varphi([k]_4) = i^k$

i.e. $[0]_4 \longmapsto 1$, $[1]_4 \longmapsto i$, $[2]_4 \longmapsto -1$, $[3]_4 \longmapsto -i$

another iso: $\psi: \mathbb{Z}_4 \longrightarrow \langle i \rangle$, $\psi([k]_4) = (-i)^k$

$\#\{\text{isos from } \mathbb{Z}_4 \text{ to } \langle i \rangle\} = |\mathbb{Z}_4^\times| = \phi(4) = 2$

Example Any group G of prime order p is isomorphic to $\mathbb{Z}_p$.

reason: Since $|G| = p$ is prime, G must be cyclic (by Lagrange), say, $G = \langle a \rangle$. Then define $\varphi: \mathbb{Z}_p \longrightarrow G$, $\varphi([k]_p) = a^k$. This is an iso, with inverse $\varphi^{-1}(a^k) = [k]_p$.

Example On the other hand, we saw that $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$. In fact, these are the only groups of order 4, up to isomorphism:
i.e. if $|G| = 4$, then $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Groups of low order

$\lvert G \rvert$	1	2	3	4	5	6	7	8
G	$\{1\}$	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4$ $\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_5$	$\mathbb{Z}_6$ S_3	$\mathbb{Z}_7$	$\mathbb{Z}_8$ $\mathbb{Z}_4 \times \mathbb{Z}_2$ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ Q_8 D_8

Remark We can distinguish oftentimes iso classes of groups G by looking at the number of elements of given order $k \mid |G|$

$$t_k(G) := \#\{a \in G \mid o(a) = k\}$$

This method shows that $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, Q_8, D_8$ are not pairwise isomorphic $\left(\begin{array}{l} Q_8 = \{\pm 1, \pm j, \pm k, \pm \ell\} \\ D_8 = \text{Symmetries of square} \end{array} \right)$

Computational Challenge Find a pair of finite groups, $G_1 \& G_2$, which are not iso, but the t_k-functions are the same.

Example Recall $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$, since $\exp: \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ is an iso

How about $(\mathbb{R}, +)$ and $(\mathbb{R}^\times, \cdot)$, are they iso?

Answer: no! Reason:

- $(\mathbb{R}, +)$ has no elements of finite order, except 0 (since $\underset{x \neq 0}{o(x) = n} \Rightarrow nx = 0 \underset{x \neq 0}{\Rightarrow} n = 0$)
- $(\mathbb{R}^\times, \cdot)$ has an element of finite order, and different from 1 namely $x = -1$: $(-1)^2 = 1$, so $o(x) = 2$.

III Autos **Def** An *automorphism* is an isomorphism from a group to itself:

$$\boxed{\varphi \text{ auto} \overset{\text{def}}{\Longleftrightarrow} \varphi: G \longrightarrow G \text{ iso}}$$

Rem A more general notion is that of an *endomorphism*, i.e., a homomorphism $\varphi: G \to G$.

Define: $\boxed{\mathrm{Aut}(G) := \{\varphi: G \longrightarrow G : \varphi \text{ automorphism}\}}$

Lemma $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Sym}(G)$.

$$\boxed{\mathrm{Aut}(G) = \{\varphi \in \mathrm{Sym}(G) : \varphi \text{ a hom}\}}$$

Proof Recall $\mathrm{Sym}(G) = \{\text{all bijections } G \to G\}$ is a group with $* = \circ$ and $e = id_G$

So $\mathrm{Aut}(G)$ inherits this operation from $\mathrm{Sym}(G)$ and is clearly closed under compositions & inverses.

$\square$

Example $\boxed{\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2}$

recall that any hom $\varphi: \mathbb{Z} \to \mathbb{Z}$ is of the form $\varphi(a) = n a$, for some $n \in \mathbb{Z}$

Such a map is surjective $\iff n = 1$ or -1

Example $\boxed{\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times}$

recall that any hom $\varphi: \mathbb{Z}_n \to \mathbb{Z}_n$ is of the form $\varphi([k]_n) = [r k]_n$ for some $0 \le r \le n-1$

Such a map is a bijection $\iff \gcd(r, n) = 1$
$\iff [r]_n \in \mathbb{Z}_n^\times$

Example $\boxed{\mathrm{Aut}(\mathbb{Z}^n) = GL_n(\mathbb{Z})}$