Group Theory (Handout - 2)

References : § Naive Set Theory - Halmos Sec - 22

§ Algebra - Artin chapter - 2

1. Some Set Theory Preliminaries :-

1.1 Recall, a map of sets $f : S \to T$ is

- injective if $\forall a, b \in S$, $f(a) = f(b) \Rightarrow a = b$
  (or $a \neq b \Rightarrow f(a) \neq f(b)$)
  Write $f : S \hookrightarrow T$

- surjective if $\forall c \in T$ $\exists a \in S$ such that $f(a) = c$
  Write $f : S \twoheadrightarrow T$

- bijective if both hold
  Write $f : S \xrightarrow{\sim} T$

1.2 Two sets S and T have the same cardinality if $\exists$ bijection $f : S \to T$, and we write $|S| = |T|$.

If $\exists$ injection $f : S \hookrightarrow T$, then write $|S| \leq |T|$. This notation is valid thanks to the Schröder-Bernstein theorem

Theorem : If there exists injective maps $f : S \hookrightarrow T$ and $g : T \hookrightarrow S$ then $|S| = |T|$.

Proof Idea : Build a bijection $S \xrightarrow{\sim} T$ by using f on a subset of S and g^{-1} on the rest.

1.3 Examples :-

- $\underbrace{\mathbb{N}, \mathbb{Z} \text{ and } \mathbb{Q}}_{\text{countably infinite}}$ all have the same cardinality.

eg. Construct a bijection $\mathbb{N} \to \mathbb{Z}$ $\quad f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ -(n+1)/2 & \text{else} \end{cases}$

For $\mathbb{Q}$, see how to enumerate $\mathbb{N} \times \mathbb{N}$

- On the other hand $\mathbb{R}$ is uncountable, using Cantor's diagonal argument

No map $f : \mathbb{N} \to \mathbb{R}$ can be surjective because :

write decimal or binary expansion of

$$f(0) = a_{00} . a_{01} a_{02} a_{03} \dots$$
$$f(1) = a_{10} . a_{11} a_{12} a_{13} \dots$$
$$f(2) = a_{20} . a_{21} a_{22} a_{23} \dots$$
$$f(3) = a_{30} . a_{31} a_{32} a_{33} \dots$$

Then let $y = b_0 . b_1 b_2 b_3 \dots$ where we choose $b_j \neq a_{jj}$ $\forall j$

Look at j^{th} digit, $y \neq f(j)$ $\forall j \in \mathbb{N}$, so f can't be surjective.

$\square$

1.4 The same argument shows that there are arbitrarily large cardinals.

Given a set S, let $P(S) = \{$ subsets of $S \}$

"power set of S"

$$P(S)$$

$$\uparrow \cong \qquad f \longmapsto f^{-1}(1) \qquad A \mapsto \left(1_A : x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{else} \end{cases} \right)$$

$$\{0,1\}^S = \{ \text{maps } f : S \to \{0,1\} \}$$

If S is finite, $|S| = n$, then $|P(S)| = 2^n$

What if S is infinite?

Theorem: If S is infinite, then $|P(S)| > |S|$

Proof: (Cantor) Given $f : S \to P(S)$

Let $A = \{ x \in S \mid x \notin f(x) \}$

Assume $A = f(a)$ for some $a \in S$

Then, $a \in A$ iff $a \notin f(a) = A$. Contradiction!

So, $A \notin f(S)$, $\nexists$ surjection $\square$

2. Back to Groups

2.1 Subgroups of $\mathbb{Z}$:-

Given $a \in \mathbb{Z}_{>0}$, $\mathbb{Z}a = \{na \mid n \in \mathbb{Z}\} \subset \mathbb{Z}$ is a subgroup.

<u>Proposition</u>: All non-trivial subgroups of $(\mathbb{Z},+)$ are of this form.

<u>Proof</u>: Follows from Euclidean algorithm.

Given a non-trivial subgroup $\{0\} \neq H \subset \mathbb{Z}$, $\exists\, a \in H$ such that $a > 0$. Let a_0 be the smallest positive element of H.

Given any $b \in H$, $b = qa_0 + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < a_0$.

$\because b \in H$ and $qa_0 \in H$, $r \in H$.

$\because r < a_0$, by def^n of a_0, $r = 0$.

Hence, $b \in \mathbb{Z}a_0$, so $H \subset \mathbb{Z}a_0$, and conversely $\mathbb{Z}a_0 \subset H$, so $H = \mathbb{Z}a_0$.

$\square$

So, every subgroup of $\mathbb{Z}$ is generated by a single element a_0, in the following sense.

<u>Thm</u>: If $H, H' \subset G$ are two subgroups, then $H \cap H'$ is also a subgroup.

Proof: • $e \in H \cap H'$, so non-empty

• if $a, b \in H \cap H'$ then $ab \in H$ and $ab \in H'$,

so $ab \in H \cap H'$

• Likewise for inverses

$\square$

Similarly, for more than 2 subgroups.

2.2 Given a subset $S \subset G$ (non-empty), what is the smallest subgroup of G containing S?

Ans: $\langle S \rangle$ subgroup generated by S.

less useful

$$\langle S \rangle = \bigcap_{\substack{S \subset H < G \\ \text{subgroup}}} H$$

Take the intersection of all subgroups H of G that contains H. (Atleast G is present).

More useful

$\langle S \rangle$ must contain all products of elements of S and their inverses, and these form a subgroup of G, so $\langle S \rangle = \{ a_1 a_2 \dots a_k \mid a_i \in S \cup S^{-1} \; \forall \, 1 \le i \le k \}$

2.3 (Definition) A group is cyclic if it's generated by a single element.

Examples: $\mathbb{Z}$, $\mathbb{Z}/n$. These are infact the only cyclic groups upto isomorphism.

Exercise: $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$ can be generated by two elements.

2.4 Homomorphisms :-

Defn. already done in Handout-1

2.4.1 "Commutative diagram" : "pedantic" way to state $\varphi(ab) = \varphi(a)\varphi(b)$

$$\begin{tikzcd} G \times G \arrow[r, "\varphi \times \varphi"] \arrow[d, "m_G"'] & H \times H \arrow[d, "m_H"] \\ G \arrow[r, "\varphi"] & H \end{tikzcd}$$

"Commutative diagram" means

$$\begin{tikzcd} G \times G \arrow[r, bend left] \arrow[r, bend right] & H \end{tikzcd}$$

give the same map: it doesn't matter if we multiply first or apply φ first.

- An isomorphism is a bijective homomorphism
- " automorphism " an isomorphism $G \to G$.

2.4.2 Examples :— (Isomorphisms)

1) All groups of order 2 are isomorphic!

$$S_2 = (\{id, (12)\}, \circ) \simeq (\{\pm 1\}, \times)$$
$$\simeq (\mathbb{Z}/2, +)$$

because the table is always :-

m	e	x
e	e	x
x	x	e

2) $(\mathbb{R}, +) \xrightarrow[\exp]{\sim} (\mathbb{R}_+, \times)$

3) $(\mathbb{R}/\mathbb{Z}, +) \xrightarrow[\exp(2\pi i t)]{\sim} (S^1, \times)$

4) $S_3 \cong$ Symmetries of $\triangle$ (permutation of vertices)

<u>Examples</u> :- (Homomorphisms)

1) $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$

$a \mapsto a \bmod n$

2) if $n \mid m$, $\mathbb{Z}/m \twoheadrightarrow \mathbb{Z}/n$

3) determinant : $GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}^*, \times)$

2.4.3 (Definition) The <u>kernel</u> of a group homomorphism $\varphi : G \to H$ is

$$\ker \varphi = \{ a \in G \mid \varphi(a) = e_H \}$$

This is a <u>subgroup of G</u>. (check)

<u>Claim</u>: φ is injective iff $\ker(\varphi) = \{e_G\}$

<u>Proof</u>: Use $\varphi(a) = \varphi(b)$

$$\iff a^{-1}b \in \ker \varphi$$

(Definition) The <u>Image</u> of a group homomorphism $\varphi : G \to H$ is

$$\mathrm{Im}(\varphi) = \varphi(G) = \{ b \in H \mid \exists\, a \in G \text{ s.t. } \varphi(a) = b \}$$

This is a <u>subgroup of H</u>.

<u>Claim</u>: φ is surjective iff $\mathrm{Im}(\varphi) = H$.

<u>Remarks</u>: If φ is injective, then G is isomorphic to the subgroup $\mathrm{Im}(\varphi) \subset H$.

The isomorphism is given by the map

$$G \to \mathrm{Im}(\varphi)$$
$$a \mapsto \varphi(a)$$

Example: Let $a \in G$ be any element in a group G, then the map $\varphi : \mathbb{Z} \to G$
$n \mapsto a^n$
is a homomorphism, with image $\langle a \rangle$.

subgroup generated by a

(Definition) The <u>order</u> of $a \in G$ = smallest positive k such that $a^k = e$, if it exists. Else it has infinite order.

If a has infinite order then powers of a are all distinct, $\varphi : n \mapsto a^n$ is injective and $\langle a \rangle \cong \mathbb{Z}$.

If a has finite order k, then $\ker \varphi \cong \mathbb{Z}k$ and
$\langle a \rangle = \{ a^n \mid n = 0, \ldots k-1 \} \cong \mathbb{Z}/k$

(This completes the classification of cyclic groups btw)

Examples: $\mathbb{Z}/6 \xrightarrow{\simeq} \mathbb{Z}/2 \times \mathbb{Z}/3$
$a \longmapsto (a \bmod 2, a \bmod 3)$

(where $(1,1) \in \mathbb{Z}/2 \times \mathbb{Z}/3$ has order 6, so generates)

Similarly, $\gcd(m,n) = 1 \Rightarrow \mathbb{Z}/m \times \mathbb{Z}/n \simeq \mathbb{Z}/mn$

But $\mathbb{Z}/2 \times \mathbb{Z}/2 \not\cong \mathbb{Z}/4$

$x + x = 0 \ \forall x$ vs $1 + 1 \neq 0$

Proposition: Every finite group G is isomorphic to a subgroup of the symmetric group S_n for some n. (Infact take $n = |G|$)

Proof: Define a map $\phi : G \longrightarrow \text{Perm}(G)$

$$g \longmapsto m_g$$

permutations of G (bijections $G \to G$)

where $m_g : G \to G$

$$x \longmapsto gx \quad (\text{left multiplication by } g)$$

Claim: m_g is a permutation (verify)

Now, $\phi(gh) = m_{gh} : x \mapsto (gh)x$

same

$\phi(g) \cdot \phi(h) = m_g \cdot m_h : x \mapsto g(hx)$

$\Rightarrow \phi$ is a homomorphism.

If $g \neq g'$ then $m_g(e) = g \neq g' = m_{g'}(e)$

$$\Rightarrow \phi(g) \neq \phi(g')$$

Hence, ϕ is injective, and $G \simeq \text{Im}(\phi) < \text{Perm}(G) \simeq S_{|G|}$

$\square$

Extra (only for fun)

Classification of finite groups upto isomorphism

- Becomes increasingly difficult as $|G|$ increases.

- Every group of order 2 is isomorphic to $\mathbb{Z}/2$
- " " " order 3 " " to $\mathbb{Z}/3$.
- For order 4, we have $\mathbb{Z}/4$ and $\mathbb{Z}/2 \times \mathbb{Z}/2$

(Only 2 groups exist of order 4 upto isomorphism)

- Classification completed in 1980s taking 1000s of pages.

...