Group Theory (Handout 1)

References: § M. Artin Algebra Chapter 2

1. **Groups**: Abstract structure that helps us model the common properties of concrete mathematical objects like numbers, permutations, linear transformations, symmetries etc.

2. Definition (Group)

A group G consists of a set S along with a map (also known as law of composition)

$$* : S \times S \to S$$
$$(a,b) \mapsto a * b$$

that satisfies the following axioms :-

(i) Identity exists $e \in S$

$$\forall a \in S, \quad ae = ea = a$$

(ae simply means $a * e$)

Remark: e is unique! (Prove it)

(ii) Inverses exist

$$\forall a \in S, \ \exists b \in S \text{ s.t. } ab = ba = e$$

(Write $b = a^{-1}$)

(iii) Associativity $\forall a,b,c \in S$

$$(ab)c = a(bc)$$

Just write abc

Remark: ① Associativity implies cancellation law!

$\forall a, b, c \in S$

$$ab = ac \Rightarrow b = c$$

Proof: $a^{-1}(ab) = a^{-1}(ac)$

$$\Rightarrow eb = ec \Rightarrow b = c$$

② Technically, the group is a pair $G = (S, *)$ but we'll just write G for the set and talk about elements of G.

Note: (i) Neglect the 2nd axiom (Inverses)

$\Rightarrow$ Monoid

(ii) Omit the first and second axiom (keep 3rd)

$\Rightarrow$ semi-group

(iii) If the composition law is commutative i.e.,

$\forall a, b \in S$, $a * b = b * a$

then G is Abelian.

3. **Examples:** 0) Trivial group $G = \{e\}$

$e \cdot e = e$

1) Number Systems

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

Remark: $(\mathbb{N}, +)$ is a semi-group.

2) (Exercise) Come up with an example of a group with 2 elements.

3) $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$

$$:= \{0, 1, 2, \dots n-1\}$$

Group law : Addition modulo n. i.e.,

$$(a,b) \longmapsto \begin{cases} a+b & \text{if } a+b \leq n-1 \\ a+b-n & \text{else} \end{cases}$$

Similarly, $\mathbb{R}/\mathbb{Z} := S = [0,1) \subset \mathbb{R}$ with addition

$$(a,b) \longmapsto \begin{cases} a+b & \text{if } a+b<1 \\ a+b-1 & \text{else} \end{cases}$$

4) Non-zero numbers

$$\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}, \mathbb{R}^*, \mathbb{C}^*$$

with multiplication

identity $= 1$
Inverse (of x) $= 1/x$

Inside $\mathbb{C}^*$, the unit circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is also a group for multiplication.

These are still <u>Abelian</u>, except $\mathbb{H}^*$ (non-zero quaternions)

5) Symmetries and Permutations :-

Recall,

$f : A \to B$ is (i) injective if $\forall x, y \in A$
$x \neq y \Rightarrow f(x) \neq f(y)$

(ii) surjective if $\forall b \in B, \exists x \in A$ s.t. $f(x) = b$

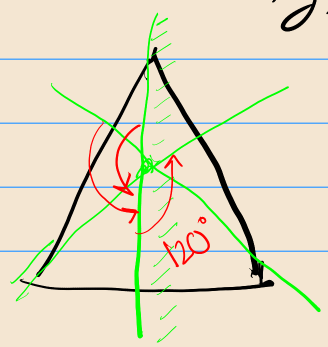
(iii) bijective if (i) and (ii) holds.

A permutation of a set A is a bijection $f : A \to A$.
The set of permutations of A, with operation = composition is a group $Perm(A)$.

The symmetric group on n elements S_n.

$$S_n = Perm(\{1, 2, \dots n\})$$

- S_3 has a geometric interpretation.
  - Think of symmetries of an equilateral triangle = Rotations which preserve it (3 including identity) and reflections (3 of these)



- Symmetries permute the vertices, and every permutation of the set of vertices arises from exactly one symmetry (+ composition laws agree)

So, S_3 also occurs as the group of symmetries of Δ.

(other groups arise from symmetries of other geometric figures in $\mathbb{R}^2$ and $\mathbb{R}^3$)

6) Groups of matrices

$GL_n(\mathbb{R}) = \{$ invertible $n \times n$ matrices with real coeff. $\}$

"General Linear group" (with matrix multiplication)

also $SL_n(\mathbb{R}) = \{ n \times n$ real matrices with $\det = 1\}$

"Special Linear group"

also $GL_n(\mathbb{C})$, $SL_n(\mathbb{C})$ for matrices with complex coeff. or $\mathbb{Q}$ or $\mathbb{Z}/n$ coeff.

4. Product of groups :-

- Given two groups G and H, the product group is $G \times H$.

$$G \times H := \{ (g, h) \mid g \in G, h \in H \}$$

with composition law

$$(g, h) * (g', h') = (gg', hh')$$

If G, H are finite of order $m = |G|$ and $n = |H|$, then $G \times H$ is a finite group of order mn.

- Similarly, for product of n groups:

Example: $\mathbb{Z}^n = \{ (a_1, a_2, \dots a_n) \mid a_i \in \mathbb{Z} \}$

$$(a_1, a_2 \dots a_n) + (b_1, b_2 \dots b_n) = (a_1 + b_1, \dots a_n + b_n)$$

Similarly $\mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$ with componentwise addition.

- Given infinitely many groups $G_1, G_2, \dots$ there are two different notions :-

1) Direct product

$$\prod_{i=1}^{\infty} G_i = \{ (a_1, a_2, a_3 \dots) \mid a_i \in G_i \}$$

2) Direct sum

$$\bigoplus_{i=1}^{\infty} G_i = \{(a_1, a_2, \dots) \mid a_i \in G_i \text{, all but finitely many are identity}\}$$

Example: Consider $G_0 = G_1 = \dots = (\mathbb{R}, +)$

Denote $(a_0, a_1, a_2 \dots)$ by $\sum a_i x^i$

Then $\prod_{i=0}^{\infty} \mathbb{R} = \mathbb{R}[[x]]$

Formal Power Series

$\sum_{i=0} a_i x^i$ (w/ addition)

$\bigoplus_{i=0}^{\infty} \mathbb{R} = \mathbb{R}[x]$ polynomials

$\sum_{\text{finite}} a_i x^i$

5. Subgroups and Homomorphisms

5.1. (Defn) (Subgroup)

A subgroup H of a group G is a non-empty subset $H \subset G$ which is closed under composition (i.e., $a, b \in H \Rightarrow ab \in H$) and inversion (i.e., $a \in H \Rightarrow a^{-1} \in H$).

$\because H \neq \phi$, these 2 conditions imply $e \in H$. So, H (with same operation) is a group.

- We say H is a proper subgroup of G if $H \subsetneq G$.

5.2. (Def n) (Homomorphism)

Given 2 groups G, H, a homomorphism $\varphi : G \to H$ is a map which respects the composition law : $\forall a, b \in G$ $\varphi(ab) = \varphi(a)\varphi(b)$.

(This implies $\varphi(e_G) = e_H$, and $\varphi(a^{-1}) = \varphi(a)^{-1}$)

- An isomorphism is a bijective homomorphism.

[If G and H are isomorphic, then they are "secretly" the "same" group even if elements ~~and~~ law may have different names].

Examples: (Subgroups)

1. $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$
2. $(\mathbb{Q}^*, \times) \subset (\mathbb{R}^*, \times) \subset (\mathbb{C}^*, \times)$
3. $\{e\} \subset G$ (Trivial subgroup)
4. $H_i \subset G_i \Rightarrow H_1 \times H_2 \times \cdots H_n \subset G_1 \times G_2 \cdots \times G_n$
5. $\bigoplus G_i \subset \prod G_i$