Lecture 0

§0.0 Definition. A <u>group G</u> is a set G together with a <u>map</u> (law of composition)

$$p : G \times G \longrightarrow G \qquad \text{such that}$$

(i) p is <u>associative</u>, i.e. $\forall\, x, y, z \in G$

$$p(x, p(y,z)) = p(p(x,y), z)$$

(ii) There exists $e \in G$ (<u>identity element</u>) s.t.

$$p(e,x) = x = p(x,e)$$

(iii) $\forall\, x \in G$, $\exists\, y \in G$ s.t. $p(x,y) = e = p(y,x)$

(<u>inverse of x</u>, usually denoted by x^{-1}, if the law of composition is written multiplicatively: $xy = p(x,y)$; or by $-x$, if the law of composition is written additively: $x+y = p(x,y)$).

<u>Monoid</u>: set X together with a law of composition $p : X \times X \to X$ satisfying (i) and (ii) above.

<u>Semigroup</u>: set X together with a law of composition $p : X \times X \to X$ satisfying only (i)

Sometimes a set X with a law of composition with no other axiom is called a magma.

§0.1 Examples.

(a) $\mathbb{N} = \{0, 1, 2, \cdots\}$ $\quad p(x,y) = x + y$

is a monoid but not a group.

(b) $\mathbb{N}$, $p(x,y) = xy$: monoid

(c) $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ with $p(x,y) = x+y$

is a group.

(d) Let E be a set and $X = \mathcal{P}(E)$ = set of all subsets of E. $\quad (A,B) \longmapsto A \cup B$

$(\mathcal{P}(E), \cup)$ is a monoid. (ϕ is the unit).

(e)* examples of a non-associative law of composition

$X = \mathbb{N}$, $\quad p(a,b) = a^b$

$X = M_2(\mathbb{Z})$ = 2x2 matrices with integer entries

$p(A,B) = AB - BA$

(f) Let K be a field, $GL_n(K)$ = set of $n \times n$ matrices with entries from K and non-zero determinant

$n \geq 2$

$GL_n(K)$ together with matrix multiplication is a group.

(g) S_n = permutations of $\{1, \dots, n\}$

= set of bijective maps $\{1, \dots, n\} \to \{1, \dots, n\}$

together with composition of bijective maps as the law of composition is a group.

§0.2 Lemma (i) In a monoid M, the identity element is unique.

(ii) Let G be a group and $x \in G$, then the inverse of x is unique.

Proof (i) Let $e, e' \in M$ be two identity elts.

$e = p(e, e') = e'$.

(ii) Let y and z be two inverses of x. Then

$$y = p(y, e) = p(y, p(x, z)) = p(p(y, x), z)$$

$$= p(e, z) = z.$$

□

§0.3. Definition. Let G and G' be two groups.

A <u>group homomorphism</u> (or just homomorphism) is a set map $\varphi : G \longrightarrow G'$ s.t.

$$\varphi(p(a,b)) = p'(\varphi(a), \varphi(b)) \quad \forall\ a,b \in G$$

where p and p' are the laws of composition on G and G' respectively. When law of composition is written multiplicatively, the condition on φ becomes

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

($\cdot$ in G on the left; $\cdot$ in G' on the right)

§0.4 Lemma. Let $\varphi : G \to G'$ be a group hom.

Then $\varphi(e) = e'$ ($e \in G$, $e' \in G'$ are identity elts.)

and $\forall\ x \in G$, $\varphi(x)^{-1} = \varphi(x^{-1})$.

Proof. $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \Rightarrow \varphi(e)$ is the identity elt. of G'.

$$e' = \varphi(e) = \varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$$
$$= \varphi(x^{-1} \cdot x) = \varphi(x^{-1}) \cdot \varphi(x)$$

$\Rightarrow \varphi(x^{-1})$ is the inverse of $\varphi(x)$. $\square$

The first assertion of the lemma would be false for monoids. e.g. $(P(E), \cup)$ and $\varphi(A) = E$ $\forall\ A \in P(E)$ is a hom. which does not map the identity element ϕ to itself

§ 0.5 Subgroup. Let G be a group and $H \subset G$.

Then H is a subgroup of G if

(i) $e \in H$

(ii) $x, y \in H \Rightarrow x \cdot y \in H$

(iii) $x \in H \Rightarrow x^{-1} \in H$.

Note : (ii) and (iii) can be written collectively as

$x, y \in H \Rightarrow x y^{-1} \in H$.

Notation : $H < G$ for H is a subgroup of G.

A subgroup $H < G$ is called normal if

$\forall\ a \in G,\ b \in H,$ we have $a b a^{-1} \in H$.

Notation : $H \lhd G$ for H is a normal subgroup of G.

§0.6 **Lemma.** Let $\varphi : G \longrightarrow G'$ be a hom.

Define $\ker(\varphi) = \{x \in G \text{ s.t. } \varphi(x) = e'\}$: Kernel of φ

$\operatorname{Im}(\varphi) = \{\varphi(x) \text{ s.t. } x \in G\}$: Image of φ

Then $\ker(\varphi) \lhd G$ and $\operatorname{Im}(\varphi) < G'$.

Proof. $\underline{\ker(\varphi) < G}$. Let $a, b \in \ker(\varphi)$. Then

$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = e' \cdot e' = e' \Rightarrow a \cdot b \in \ker(\varphi)$.

($e \in \ker(\varphi)$ since $\varphi(e) = e'$). Finally if $x \in \ker(\varphi)$

then $\varphi(x^{-1}) = \varphi(x)^{-1} = (e')^{-1} = e'$. Hence $x^{-1} \in \ker(\varphi)$.

This proves that $\ker(\varphi) < G$. Now if $a \in G$, $b \in \ker(\varphi)$

then $\varphi(a b a^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1} = \varphi(a) \cdot e' \cdot \varphi(a)^{-1}$

$= \varphi(a) \cdot \varphi(a)^{-1} = e'$

$\Rightarrow a b a^{-1} \in \ker(\varphi)$. Hence $\ker(\varphi)$ is a normal

subgroup of G.

$\operatorname{Im}(\varphi) < G'$: left as an exercise $\square$

Rk $\operatorname{Im}(\varphi)$ need not be normal. For example, let

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{C},\ a, c \neq 0 \right\} \xhookrightarrow{\varphi} GL_2(\mathbb{C}).$$

- G is commutative (or abelian) if $p(x,y) = p(y,x)$ $\forall\ x, y \in G$. It is usually for abelian groups that $+$ is used instead of p and 0 denotes the identity element.

- $\underset{Gps}{Hom}(G, G')$ (or just $Hom(G, G')$) denotes the set of all group homomorphisms $G \to G'$.

- $\varphi \in Hom(G, G')$ is said to be an isomorphism if $\exists\ \varphi' \in Hom(G', G)$ s.t. $\varphi \circ \varphi' = Id_{G'}$ and $\varphi' \circ \varphi = Id_G$

In this case G and G' are said to be isomorphic ($G \simeq G'$).

$End(G) = Hom(G, G)$ is a monoid under composition.

$Aut(G) =$ isomorphisms in $Hom(G, G)$ is a group.