Contents

Chapter 1

Introduction

Lecture 1: General Overview
08:10 AM Thu, Sep 25 2025

Let $E \neq \emptyset$ a set.

A binary operation $\cdot$ on E is any map from $E \times E$ into E,

$$\begin{array}{rccc} (\cdot): & E \times E & \longrightarrow & E \\ & (x, y) & \longmapsto & x \cdot y \end{array}$$

Let $A \subset E$, we say A is a stable by $(\cdot)$if $(\cdot)$ is also a Binary Operation on A,

$$\begin{array}{rccc} (\cdot_A): & A \times A & \longrightarrow & A \\ & (x, y) & \longmapsto & x \cdot_A y = x \cdot y \end{array}$$

Definition 1.0.1 (Group) : *Let $G \neq \emptyset$ a set with a Binary Operation $(*)$, we say that G is a group if :*

1. *$(*)$ is associative, if :*

$$\forall x, y, z \in G : \quad (x * y) * z = x * (y * z)$$

2. *$(*)$ admits a netural elements if :*

$$\exists e \in G, \forall x \in G : \quad x * e = e * x = x$$

3.

$$\forall x \in G, \exists x' \in G : \quad x * x' = x' * x = e$$

if $(*)$ is commutative i.e.:

$$\forall x, y \in G : \quad x * y = y * x$$

then G is called an Abelian Group.

Notation: We denote $(*)$ by $(\cdot)$ if its multiplicative, and $(+)$ if its additive.

Proposition 1.0.1 : *Let $(G, \cdot)$ be a group. then:*

1. *The Neutral Element is uniuqe.*
2. *The inverse is unique*
3.

$$\forall x, y \in G : \quad (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$$

4.

$$\forall x, y, z \in G : \begin{cases} xy = xz \\ yx = zx \end{cases} \implies \begin{cases} y = z \\ y = z \end{cases}$$

Proof. 1. Let $e_1, e_2 \in G$ be a Neutral Element, then:

$$e_1 = e_1 \cdot e_2 = e_2$$

2. let $x \in G$ and $x_1, x_2 \in G$ be its inverses, then:

$$x_1 = x_1 \cdot e = x_1 \cdot (x \cdot x_2) = (x_1 \cdot x) \cdot x_2 = e \cdot x_2 = x_2$$

3. Let $x, y' \in G$. then:

$$\begin{aligned}(x \cdot y) \cdot (x \cdot y)^{-1} = e &\implies y \cdot (x \cdot y)^{-1} = x^{-1} \\ &\implies (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}\end{aligned}$$

$\square$

Exercise

Let $(G, \cdot)$ be a group and $x_1, x_2, \ldots, x_n \in G$. then:

- $(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1}$
- $(x_1^{-1})^{-1} = x_1$

Definition 1.0.2 : *Let $(G, \cdot)$ be a group, $n \in \mathbb{Z}$ and $x \in G$, define*

$$x^n = \begin{cases} x \cdot x \cdots x \\ e \\ x^{-1} \cdot x^{-1} \cdots x^{-1} \end{cases} \implies \begin{cases} \text{if } n \geq 1 \\ \text{if } n = 0 \\ \text{if } n \leq -1 \end{cases}$$

Example:

1. $(Z, +), (\mathbb{Q}^*, \cdot), (\mathbb{R}, +), (\mathbb{C}^*, \cdot)$
2. *The set $\mathcal{F}(\mathbb{R}, \mathbb{R})$ with addition of maps is an Abelian Group, with the null map as Neutral Element*
3. *The set S_n of all bijection of $\{1, \ldots, n\}$ with composition of maps is a group*

Definition 1.0.3 (Sub Group) : *Let $(G, \cdot)$ be a group and $H \subset G$ we say that H is a Subgroup of G if $(H, \cdot)$ is a gorup*

Proposition 1.0.2 :

Let $(G, \cdot)$ a group and $H \subset G$. then H is a Subgroup of G if and only if:

1. $H \neq \emptyset$
2. $\forall x, y \in H : \quad x \cdot y \in H$
3. $\forall x \in H : \quad x^{-1} \in H$

<u>*Remark*</u>: The conditions (2) and (3) are equivalent to:

$$\forall x, y \in H : \quad x^{-1} \cdot y \in H$$

Proof.

$$\forall x, y \in H : \quad x^{-1} \cdot y \in H \implies \begin{cases} \forall x, y \in H : \quad x \cdot y \in H \\ \forall x \in H : \quad x^{-1} \in H \end{cases}$$

□

<u>*Notation*</u>: if H is a Subgroup of G, we denote

$$H \leq G$$

if $H \leq G$ with $H \neq G$, we call H a proper Subgroup of G and we write $H < G$

Exercise

Let $(G, \cdot)$ be a group, then the set:

$$Z(G) = \{x \in G : \quad gx = xg, \forall g \in G\}$$

1. Prove that $Z(G) = G \iff G$ is an abelian group.

Proof. 1.

$$(\implies)$$

Suppose that G is an Abelian Group.

Let $x \in G$ and let $g \in G$, since G is an Abelian group, then $gx = xg$. then $x \in Z(G)$, then $Z(G) = G$

$$(\impliedby)$$

Suppose that $Z(G) = G$, let $x, y \in G$. then $x, y \in Z(G)$. so $\forall g \in G$:

$$\begin{cases} xg = gx \\ yg = gy \end{cases}$$

so for $g = y$, we get $xy = yx$ so G is an abelian group

2. Let $G \leq (\mathbb{Z}, +)$.

   - if $G = \{0\}$. then $G = 0\mathbb{Z}$.
   - if $G \neq \{0\}$, then $\exists m \in G$ with $m \neq 0$, without loss of generality. suppose $m > 0$, so $G \cap \mathbb{N} \neq \emptyset$, so $n = \min G \cap \mathbb{N}$, let $x \in n\mathbb{Z}$. then $x = kn, k \in \mathbb{Z}$, so $x \in G$. hence $n\mathbb{Z} \subset G$. Let $x \in G$, so $\exists q, r \in \mathbb{Z}$, $0 \leq r \leq n - 1$ such that $x = qn + r$. so $r = x - qn \in G$, if $r \neq 0$ then :

     $$\begin{cases} r < n \\ r = G \cap \mathbb{N} \end{cases} \implies \begin{cases} r < n \\ n = \min G \cap \mathbb{N} \leq r, & \text{is a contradiction} \end{cases}$$

     so $x = qn \in n\mathbb{Z}$, so $G \subset n\mathbb{Z}$

$\square$

Proposition 1.0.3 : *Let $H, K \leq G$, with G is a group. then:*

$$H \cap K \leq G$$

Proof. Since $e \in H$ and $e \in K$, then $e \in H \cap K \neq \emptyset$.
Let $x, y \in H \cap K$, then :

$$\begin{cases} x, y \in H \\ x, y \in K \end{cases} \implies \begin{cases} x^{-1}, y \in H \\ x^{-1}, y \in K \end{cases} \implies \begin{cases} x^{-1} \cdot y \in H \\ x^{-1} \cdot y \in K \end{cases} \implies x^{-1} \cdot y \in H \cap K$$

$\square$

Proposition 1.0.4 : *Let $\{H_i\}_{i \in I}$ be a family of Subgroup of a group G, then :*

$$\bigcap_{i \in I} H_i \leq G$$

<u>*Remark*</u>: $H \cup K$ is not always a Subgroup of G.

Proposition 1.0.5 : *Let $H, K \leq G$, Then $H \cup K \leq G \iff \begin{cases} H \subset K \\ K \subset H \end{cases}$*

Lecture 2

08:17 AM Thu, Oct 02 2025

Definition 1.0.4 : *Let G be a group and $A \subset G$, The group spanned by A is the intersection of all SG of G containing A, i.e.:*

$$\langle A \rangle = \bigcap_{H \leq G, A \subset H} H$$

Proposition 1.0.6 : *$\langle A \rangle$ is the smallest SG of G containing A*

Proof. $\langle A \rangle \leq G$

$$\begin{cases} e \in H, \forall H \leq G \implies \bigcap_{H \leq G} H \neq \emptyset \\ \forall x, y \in \langle A \rangle : \quad x, y \in H, \forall H \leq G \text{ and } A \subset H \end{cases}$$

so $xy^{-1} \in H, \forall H \leq G$ and $A \subset H$

so $xy^{-1} \in \bigcap_{H \leq G, A \subset H} H$

Let $B \leq G$ such that $A \subset B$.

since

$$\bigcap_{H \leq G, A \subset G} H \subset B, \quad \text{so } \langle A \rangle \subset B$$

so $\langle A \rangle$ is the smallest SG of G containing A □

Proposition 1.0.7 : *Let G be a group and $A \subset G$ such that $A \neq \emptyset$. Then:*

$$\langle A \rangle := \left\{ x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} : \quad n \in \mathbb{N}, x_i \in A, k_i = \pm 1, i \in \{1, \dots, n\} \right\}$$

In particular if $A = \{a\}$. then by definition:

$$\langle A \rangle = \langle a \rangle = \left\{ a^k : \quad k \in \mathbb{Z} \right\}$$

Definition 1.0.5 : *Let G be a group and $A \subset G$, we say:*

1. *A span G if $G = \langle A \rangle$*
2. *G is of finite type if $G = \langle A \rangle$ and A is finite.*
3. *G is cyclic if $G = \langle a \rangle, a \in G$*
4. *G is a finite group if $|G| < \infty$, in this case we call $|G|$ the order of G.*
5. *The order of $x \in G$ is $|\langle x \rangle|$*

Example:

1. *$(\mathbb{Z}, +)$ is cyclic. Indeed, $\mathbb{Z} = \langle 1 \rangle = \{n \cdot 1 : \quad n \in \mathbb{Z}\}$ or with -1.*
2. *$(n\mathbb{Z}, +)$ is cyclic. Since $n\mathbb{Z} = \langle n \rangle = \{k \cdot n : \quad k \in \mathbb{Z}\}$*
3. *$\left(\frac{\mathbb{Z}}{6\mathbb{Z}}, +\right)$ is cyclic. Since*

$$\begin{aligned}\frac{\mathbb{Z}}{6\mathbb{Z}} &= \langle \bar{1} \rangle = \{n \cdot \bar{1} : \quad n \in \{0, 1, \dots, 5\}\} \\ &= \langle \bar{5} \rangle = \{n \cdot \bar{5} : \quad n \in \{0, 1, \dots, 5\}\}\end{aligned}$$

Proposition 1.0.8 : *Any cylic group is Abelian.*

Proof. Let $G = \langle a \rangle = \left\{a^k : \quad k \in \mathbb{Z}\right\}$, we define:

$$HK = \{hk : \quad h \in H, k \in K\}$$

□

PRODUCT OF SG:

Let G be a group and $H, K \leq G$, we define

$$HK = \{hk : \quad h \in H, k \in K\}$$

Remark: $H, K \subset HK$

Proposition 1.0.9 :

$$HK \leq G \implies HK = KH$$

Proof. ($\implies$) since $HK \leq G$, then $HK \neq \emptyset$, let $x \in HK$. So $x = hk$ where $h, k \in H, K$. since it's a subgroup then, $x^{-1} = k^{-1}h^{-1} \in HK$, so $HK \subset KH$, let $x \in KH$. then $x = kh$ where $k, h \in K, H$ so $x^{-1} = h^{-1}k^{-1} \in HK$. Since $HK \leq G$ then $x \in HK$ so:

$$KH \subset HK$$

□

Proposition 1.0.10 : *if $HK \leq G$, then HK is the smallest SG of G containing H and K thats so:*

$$HK = \langle H \cup K \rangle$$

Proof. Set

$$\begin{aligned} L &= \left\{ x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} : \quad n \in \mathbb{N}, x_i \in H \cup K, k_i = \pm 1 \right\} \\ &= \langle H \cup K \rangle \end{aligned}$$

Let $x \in HK$, then $x = hk \in L$. so $HK \subset L$, since $H, K \subset HK$. then $H \cup K \subset HK$, since $HK \leq G$, then $\langle H \cup K \rangle \subset HK$ (see definition):

$$HK = \langle H \cup K \rangle$$

□

1.1 Quotient Group

Exercise

Let $H \leq G$, G is a group and let $x, y \in G$. Show that:

1. $xH = H \iff x \in H$
2. $x^{-1}y \in H \iff y \in xH$
3. $H^{-1} = H$ with $H^{-1} = \left\{ h^{-1} : \quad h \in H \right\}$

Proof.

$$x \in H \implies H \subset xH$$
$$h \in H \implies h = xx^{-1}h = x(x^{-1}h) \in xH$$

$\square$

- Let $H \leq G$, define on G the binary operations R_g and R_d by:

$$\forall x, y \in G : \begin{cases} x\mathcal{R}_g y \iff x^{-1}y \in H \\ x\mathcal{R}_d y \iff yx^{-1} \in H \end{cases}$$

we can show that $\mathcal{R}_g$ and $\mathcal{R}_d$ are equivallence relations, (reflexive, symmetric, transition) let $x \in G$. that left class of x by $\mathcal{R}_g$ is:

$$\begin{aligned} \overline{x} &= \{y \in G : \quad x\mathcal{R}_g y\} \\ &= \left\{y \in G : \quad x^{-1}y \in H\right\} = \{y \in G : \quad y \in xH\} = xH \end{aligned}$$

Similarly, the right class of x is:

$$\overline{x}^d = \{y \in G : \quad x\mathcal{R}_d y\} = Hx$$

Quotient of G by $\mathcal{R}_g$ and $\mathcal{R}_d$:

By definition:

$$\frac{G}{\mathcal{R}_y} = \left\{\overline{x}^2 : \quad x \in G\right\} = \{xH : x \in G\} \overset{\text{def}}{=} \left(\frac{G}{H}\right)_g$$

where:

$$\frac{G}{\mathcal{R}_d} = \left\{\overline{x}^d : x \in G\right\} = \{Hx : \quad x \in G\} \overset{\text{def}}{=} \left(\frac{G}{H}\right)_d$$

Proposition 1.1.1 : *$\left(\frac{G}{H}\right)_g$ and $\left(\frac{G}{H}\right)_d$ are partition of G.*

Proof.

$$xH \neq \emptyset \quad (x = x \cdot e \in xH)$$
$$\bigcup_{x \in G} xH = G$$
$$xH \cap yH \neq \emptyset \implies xH = yH$$

$\square$

Proposition 1.1.2 :

1. $\left(\frac{G}{H}\right)_g$ *and* $\left(\frac{G}{H}\right)_d$ *are equipotent.*

2. $\forall x \in G :\quad xH$ *and* Hx *are equipotent (in bijection).*

Proof. 1. Let

$$\begin{array}{rccc} f: & \left(\frac{G}{H}\right)_g & \longrightarrow & \left(\frac{G}{H}\right)_d \\ & \overline{x} = xH & \longmapsto & f(xH) = (xH)^{-1} = Hx^{-1} \end{array}$$

f is well defined:

$$\overline{x} = \overline{y} \implies f(\overline{x}) = f(\overline{y})$$

$$\begin{aligned} \overline{x} = \overline{y} &\implies xH = yH \\ &\iff x^{-1}yH = H \\ &\implies Hy^{-1}x = H \\ &\implies Hy^{-1} = Hx^{-1} \implies f(\overline{x}) = f(\overline{y}) \end{aligned}$$

□

Lecture 3 08:14 AM Thu, Oct 09 2025

Proposition 1.1.3 :

- $(\frac{G}{H})_d$ *and* $\left(\frac{G}{H}\right)_d$ *are equipotent.*
- *and for all* $x \in G :\quad xH$ *and* Hx *are equipotent.*

Proof.

$$\begin{array}{rccc} f: & (\frac{G}{H}))_g & \longrightarrow & \left(\frac{G}{H}\right)_d \\ & xH & \longmapsto & Hx^{-1} \end{array}$$

we have for all $x, y \in G$:

$$xH = yH \implies Hx^{-1} = Hy^{-1} \implies f(xH) = f(yH)$$

so f is well defined.

$$f(xH) = f(yH) \iff Hx^{-1} = Hy^{-1} \implies xH = yH \implies \text{ f injective}$$

Let $Hy \in \left(\frac{G}{H}\right)_d$ then:

$$f(y^{-1}H) = Hy \text{ with } y^{-1}H \in \left(\frac{G}{H}\right)_g$$

hence f is surjective, thus f is bijective. Let

$$\begin{aligned} f: \quad xH &\longrightarrow Hx \\ xh &\longmapsto hx \end{aligned}$$

we have that f is bijective. □

Theorem 1.1.4 (Lagrange Theorem) : *Let G be a finite group and let $H \leq G$, then $|H| \, / \, |G|$*

Proof. Let $H \leq G$. then $\left(\frac{G}{H}\right)_g$ is a partition of G, Let $\left(\frac{G}{H}\right) g = \{x_1 H, \ldots, x_n H\}$ for some $n \in \mathbb{N}$, so $G = \bigcup_{i=1}^{n} x_i H$. Since $\left(\frac{G}{H}\right)_g$ is a partition of G, then:

$$|G| = \left| \bigcup x_i H \right| = \sum_{i=1}^{n} |x_i H|$$

we have H and $x_i H$ are equipotent for all $i \in \{1, \ldots, n\}$, take

$$\begin{aligned} f: \quad H &\longrightarrow x_i H \\ h &\longmapsto x_i h \end{aligned}$$

so

$$|G| = \sum_{i=1}^{n} |H| = n \, |H|$$

hence $|H| \;\; |G|$ □

☞Notation:

$n = [G : H]$ called the index of H in G. if $|G| < +\infty$, then

$$[G : H] = \frac{|G|}{|H|}$$

For $G = (\mathbb{Z}, +)$ and $H = n\mathbb{Z}$ where $n \in \mathbb{N}$, we have:

$$[G : H] = \left| \left(\frac{G}{H}\right) \right| = n$$

Corollary 1.1.5 : *Every finite group G of prime order is cyclic spanned any element $x \in G \backslash \{e\}$*

Proof. Let $x \in G\setminus\{e\}$. By lagrange theorem we have $|\langle x\rangle| \setminus |G| = p$. so $\langle x\rangle = \{e\}$ or $G = \langle x\rangle$. since $x \neq e$, then $\langle x\rangle \neq \{e\}$. So $G = \langle x\rangle$ □

✎Remark:

The reciprical of this result is not true. we can have a cyclic group with a non prime order,

$$\frac{\mathbb{Z}}{6\mathbb{Z}} = \langle\overline{1}\rangle = \langle\overline{5}\rangle$$

is cyclic and $\left|\frac{\mathbb{Z}}{6\mathbb{Z}}\right| = 6$ not prime.

1.1.1 Normal Subgroups

Definition 1.1.1 : *Let $H \leq G$. we say that H is a normal group of G if:*

$$\forall x \in G: \quad xH = Hx \qquad \textit{(denoted } H \lhd G\textit{)}$$

✎Remark:

If G is abelian, then any subgroup of G is normal

Proposition 1.1.6 : *Let $H \leq G$. then the following statments are equivallent:*

① $\forall x \in G: \quad xHx^{-1} = H$

② $\forall x \in G: \quad xHx^{-1} \subset H$

Proof. Exercise □

Let G be a group and $(H \lhd G)$. then:

$$\left(\frac{G}{H}\right)_g = \left(\frac{G}{H}\right)_d \overset{\text{def}}{=} \frac{G}{H}$$

we equip $\frac{G}{H}$ by the binary operation, defined:

$$\forall x, y \in G: \quad (xH)\cdot(yH) = \overline{x}\cdot\overline{y} = \overline{xy} = (xy)\cdot H$$

Theorem 1.1.7 : $(\frac{G}{H}, \cdot)$ *is a group called the quotient group of G by H*

Proof.
- Associativity
- The neutral element of $\left(\frac{G}{H}\right)$ is $H = \overline{e} = eH$
- for all $\overline{x} \in \frac{G}{H}$: $\quad \overline{x}^{-1} = \overline{x^{-1}} = (xH)^{-1}$

□

1.2 Group Morphism

Definition 1.2.1 : *Let $(G, \cdot)$ and $(G', \mathcal{T})$ be two groups. A map $f : G \longrightarrow G'$ is a group morphism if for all $x, y \in G$ we have:*

$$f(x \cdot y) = f(x)\mathcal{T}f(y)$$

Proposition 1.2.1 : *Let $f : G \longrightarrow G'$ a Group morphism, and e, e' are the neutral elements of G and G' resp. Then:*

① $f(e) = e'$

② $\forall x \in G : \quad f(x^{-1}) = [f(x)]^{-1}$

③ $\forall x \in G, \quad \forall n \in \mathbb{Z} : \quad f(x^n) = [f(x)]^n$

Proof. $\boxed{1}$ ➽ $x = y = e \implies f(e) = f(e)f(e)$

$\boxed{2}$ ➽ $y = x^{-1} \implies e' = f(x)f(x^{-1})$

$\boxed{3}$ ➽ use induction

□

Example: *Let $H \lhd G$, then:*

$$\begin{array}{rccc} i: & H & \longrightarrow & G \\ & h & \longmapsto & h \end{array}$$

and

$$\begin{array}{rccc} s: & G & \longrightarrow & \frac{G}{H} \\ & x & \longmapsto & \overline{x} = xH \end{array}$$

are group morphism called injective and surjective, resp.

1.2.1 Kernel-Image

Let $f : G \longrightarrow G'$, The kernel of f is:

$$\boxed{\operatorname{Ker}(f) = \{x \in G : \quad f(x) = e'\} = f^{-1}(\{e'\})}$$

The image of f is:

$$\boxed{\operatorname{Im}(f) = \{f(x) : \quad x \in G\} = f(G)}$$

Proposition 1.2.2 : *Let $f : G \longrightarrow G'$ be a Group morphish, then:*

① *If $H \leq G$, then $f(H) \leq G'$*

② *$H' \leq G'$, then $f^{-1}(H') \leq G$*

so

$$Im(f) = f(G) \leq G'$$

and

$$f^{-1}(\{e'\}) = Ker(f) \leq G$$

Proposition 1.2.3 : *Let $f : G \longrightarrow G'$ be a group morphism, then:*

① *f injective $\iff$ $Ker(f) = \{e\}$*

② *f surjective $\iff$ $Im(f) = G'$*

Proof. Exercise `(you know it won't happen)` ✌ □

Proposition 1.2.4 : *Let $H \leq G$, then:*

$$H \lhd G \iff \exists G' \text{ a group and GM } f : G \longrightarrow G' \text{ such that: } H = Ker(f)$$

Proof.

$$(\Longleftarrow)$$

suppose that $\exists G'$ a group, and $f : G \longrightarrow G'$ a group morphism such that $H = \text{Ker}(f)$ Let $x \in G$, and let $y = xgx^{-1} \in x\text{Ker}(f)x^{-1}$, hence:

$$\begin{aligned} f(y) &= f(x)f(g)(x^{-1}) \\ &= f(x)f(x^{-1}) \\ &= e' \end{aligned}$$

so $y \in \text{Ker}(f)$. look at the hand below

$$☞\ x\text{Ker}(f)x^{-1} \subset \text{Ker}(f)$$

Therefore $H = \text{Ker}(f) \lhd G$.

$$(\Longrightarrow)$$

Let $H \lhd G$, and let

$$\begin{array}{rccc} f: & G & \longrightarrow & \frac{G}{H} \\ & x & \longmapsto & \overline{x} = xH \end{array}$$

we have f is a group morphism, and $\mathrm{Ker}(f) = H$ □

Theorem 1.2.5 (First Theorem of Isomorphism) : *Let $f : G \longrightarrow G'$ be a group morphism, then $\frac{G}{Ker(f)} \sim Im(f)$*

Proof. ✍ Let

$$\begin{array}{rccc} \widetilde{f}: & \frac{G}{\mathrm{Ker}(f)} & \longrightarrow & \mathrm{Im}(f) \\ & \overline{x} & \longmapsto & \widetilde{f}(\overline{x}) = f(x) \end{array}$$

Let $\overline{x}, \overline{y} \in \frac{G}{\mathrm{Ker}(f)}$ such that $\overline{x} = \overline{y}$, then $x\mathrm{Ker}(f) = y\mathrm{Ker}(f)$, therefore $x^{-1}y \in \mathrm{Ker}(f)$, hence we can deduce

$$\begin{aligned} f(x^{-1}y) = e &\iff f(x) = f(y) \\ &\iff \widetilde{f}(\overline{x}) = \widetilde{f}(\overline{y}) \end{aligned}$$

so f is well defined and injective. f is surjective by construction □