

This is a note by D.Dai for PMATH 347, Spring 2019 with Prof. B.Madill at University of Waterloo.

No commercial uses please.

# Contents

<b>1</b>	<b>Intro</b>	<b>4</b>
1.1	Basic . . . . .	4
1.2	Cyclic Groups . . . . .	7
1.3	Symmetric Groups . . . . .	10
1.4	Dihedral Groups . . . . .	12
1.5	Quaternion Groups . . . . .	13
<b>2</b>	<b>Quotient Group</b>	<b>14</b>
2.1	Cosets . . . . .	14
2.2	Quotient Groups . . . . .	17
<b>3</b>	<b>Group Homomorphism</b>	<b>23</b>
3.1	Homomorphism . . . . .	23
3.2	First Isomorphism Theorem . . . . .	25
<b>4</b>	<b>Group Actions</b>	<b>32</b>
4.1	Intro . . . . .	32
4.2	Applications of Group Actions . . . . .	35
4.3	Finite Abelian Groups . . . . .	39
<b>5</b>	<b>Basic Ring</b>	<b>45</b>
5.1	Intro . . . . .	45
5.2	Integral Domain and Fields . . . . .	48

5.3	Homomorphism . . . . .	50
<b>6</b>	<b>Ideals</b>	<b>52</b>
6.1	Intro to Ideals and Quotient Rings . . . . .	52
6.2	First Isomorphism Theorem . . . . .	54
6.3	Maximal and Prime Ideals . . . . .	57
6.4	Zorn's Lemma and More on Maximal Ideals . . . . .	59
<b>7</b>	<b>Different Kinds of Domains</b>	<b>64</b>
7.1	Euclidean Domain . . . . .	64
7.2	Principal Ideal Domain . . . . .	67
7.3	Unique Factorization Domain . . . . .	70
<b>8</b>	<b>Final</b>	<b>74</b>

# Chapter 1

## Intro

### 1.1 Basic

**Definition 1.1.1.** Midterm, Tues, June 18, 6:30-7:50 PM. It will cover up to Theorem 4.1.15.

STC 0060

1. Basic Group Structure, 3 parts
2. Homomorphism and Isomorphism, 4 parts
3. Proofs, 2 parts
4. New assignment type question, part a would be quotient group and part b would be group action
5. 10 parts, examples and definitions (be careful with this one, it may be difficult).  
Example: Group with  $p^2$  elements are abelian.

Need to know assignment questions, it is very important.

**Definition 1.1.2.** A **binary operation**  $\star$  on a set  $G$  is a function  $\star : G \times G \rightarrow G$ . We say  $\star$  is commutative if for all  $x, y \in G$ , we have  $\star(x, y) = \star(y, x)$ .

**Definition 1.1.3.** A **group** is an ordered pair  $(G, \star)$  where  $G$  is a set and  $\star$  is a binary operation on  $G$  with the following axioms:

1.  $(a \star b) \star c = a \star (b \star c)$
2.  $\exists e \in G$ , such that  $e \star x = x \star e$  for all  $x \in G$
3.  $\forall a \in G, \exists b \in G$  such that  $a \star b = b \star a = e$ , we write  $b := a^{-1}$ , and call it the inverse of  $a$ .

**Definition 1.1.4.** We say  $(G, \star)$  is commutative or abelian if  $a \star b = b \star a$  for all  $a, b \in G$ .

**Remark 1.1.5.** We will omit the operation and write  $a \star b := ab$  most of the time. The operation normally will be clear from the context. We will say  $G$  is group without indicate the operation in general setting. We will normally write the identity to be  $e$  or  $e_G$ , sometimes 1, sometimes 0. It should be clear from the context as well.

**Proposition 1.1.6.** Let  $G$  be a group, then

1.  $e$  is unique,
2.  $a^{-1}$  is unique,
3.  $(a^{-1})^{-1} = a$  for all  $a \in G$ ,
4.  $(ab)^{-1} = b^{-1}a^{-1}$
5.  $a_1a_2\dots a_n$  is a valid expression.

**Proposition 1.1.7.** For  $a, b, u, v \in G$ , we have  $au = av \Rightarrow u = v$ ,  $ub = vb \Rightarrow u = v$ .

**Definition 1.1.8.** We write  $x^n := xxx\dots x$  where operation repeat  $n$  times.

**Definition 1.1.9.** The **order** of  $a \in G$  is the smallest positive integer  $n$  such that  $a^n = e$  and denote this as  $|a|$ . If  $a$  never equal  $e$ , we say  $|a| = \infty$ .

**Definition 1.1.10.** We say  $H$  is a **subgroup** of  $G$  and write  $H \leq G$ , when  $H$  is closed under product and inverse.

**Definition 1.1.11.** Let  $\mathbb{F}$  be a field.

$GL_n(\mathbb{F}) := \{A \in M_{n \times n}(\mathbb{F}) : \det(A) \neq 0_F\}$  is called the **general linear group** together with the matrix multiplication.

$SL_n(\mathbb{F}) := \{A \in M_{n \times n}(\mathbb{F}) : \det(A) = 1_F\}$  is the **special linear group**.

**Proposition 1.1.12.** Just few things about field  $\mathbb{F}$ ,

1. If  $|F| < \infty$  then  $|F| = p^m$  for some prime number  $p$  and positive integer  $m$ .
2. If  $|F| = q < \infty$ , then  $|GL_n(\mathbb{F})| = \prod_{i=0}^{n-1} (q^n - q^i)$

*Proof.* We will prove part two.

$A \in GL_n(F)$  if and only if the row vectors are linear independent. Thus, the first row of  $A$  has  $p^n - 1$  choices where the only vector we do not pick is the zero vector. The second row cannot be linear dependent to the first row, thus it must not be a scalar multiple of the first row. Hence, once the first row is fixed, the second row has  $p^n - p$  choices as it cannot be  $a \cdot \text{Row}_1(A)$  where  $a \in \mathbb{F}$ . The third row has  $p^n - p^2$  choices, as it cannot be a scalar multiple of the first and the second row, and the number of scalar multiples of the first row is  $p$ , the number of scalar multiple of the second row is  $p$  as well. Continue this argument, we obtained that the  $i$ th row has  $p^n - p^{i-1}$  choices where  $1 \leq i \leq n$ . This way we enumerated all the possible cases, and hence  $|GL_n(F)| = \prod_{i=1}^n (p^n - p^{i-1})$  as desired.  $\heartsuit$

**Proposition 1.1.13.** A subset  $H$  of  $G$  is subgroup if and only if

1.  $H \neq \emptyset$ , and
2.  $\forall x, y \in H, xy^{-1} \in H$

*Proof.* Say  $H \leq G$ , then we are done.

Conversely, let  $x \in H$ , and let  $y = x$ , we have  $xx^{-1} = e \in H$  so it contains the identity. Next, let  $x \in H$ , then  $ex^{-1} = x^{-1} \in H$ , and thus  $H$  is closed under taking inverse. Let  $x, y \in H$ , then  $x, y^{-1} \in H$  and note  $x(y^{-1})^{-1} = xy \in H$ . Hence  $H$  is a subgroup of  $G$ .  $\heartsuit$

**Definition 1.1.14.** Let  $H$  be a subgroup of  $G$  and fix  $g \in G$ , we call  $gHg^{-1} := \{ghg^{-1} : h \in H\}$  the conjugate of  $H$  in  $G$  by  $g$ .

**Example 1.1.15.**  $gHg^{-1} \leq G$

*Solution.* Note  $e \in gHg^{-1}$  as  $geg^{-1} = e$ . Next, let  $gxg^{-1}, gyg^{-1} \in gHg^{-1}$ , then we have  $(gxg^{-1})(gyg^{-1})^{-1} = gxyg^{-1}$ . Note  $xy \in H$  as  $H$  is a subgroup and thus  $gxyg^{-1} \in gHg^{-1}$ , so  $gHg^{-1}$  is a subgroup. ♠

**Example 1.1.16.**  $a^2 = e$  for all  $a \in G$  imply  $G$  is abelian

*Solution.* Suppose  $a^2 = e$  for all  $a \in G$ , then  $aa = e$  and  $a^{-1}aa = a^{-1}e$  so  $a = a^{-1}$  for all  $a \in G$ . Let  $x, y \in G$ , we have  $xy = x^{-1}y^{-1}$  since  $x, y \in G$ . Note  $(ab)^{-1} = b^{-1}a^{-1}$  for arbitrary group  $G$  and  $a, b \in G$  as  $abb^{-1}a^{-1} = b^{-1}a^{-1}ab = e$ , in particular, we must have  $(yx)^{-1} = x^{-1}y^{-1}$ . Hence  $xy = (yx)^{-1}$ . However,  $yx \in G$  so  $(yx)^{-1} \in G$  and we must have  $yx = (yx)^{-1}$  and hence  $xy = yx$  as desired for arbitrary  $x, y \in G$  hence it is abelian. ♠

**Definition 1.1.17.** The **center** of  $G$  is the set  $Z(G) := \{x \in G : \forall g \in G, xg = gx\}$ .

**Example 1.1.18.** Let  $G$  be a group, let  $\mathcal{H}$  be a non-empty collection of subgroups of  $G$ . Show that  $\bigcap_{H \in \mathcal{H}} H$  is a subgroup of  $G$ .

*Solution.* Let  $S = \bigcap_{H \in \mathcal{H}} H$ . Since every  $H \in \mathcal{H}$  is a subgroup of  $G$ , we have  $e \in S$  since  $e \in H$  for all  $H \in \mathcal{H}$ . Thus  $S$  is not empty. Now, let  $a, b \in S$ . We have  $ab^{-1} \in H$  for every  $H \in \mathcal{H}$  because  $S$  is the intersection of all  $H \in \mathcal{H}$  and therefore  $S \subseteq H$  for  $H \in \mathcal{H}$ . In particular,  $a, b^{-1} \in H$  for every  $H \in \mathcal{H}$  so that  $ab^{-1} \in H$  for every  $H \in \mathcal{H}$ . Hence  $ab^{-1} \in S$ . By subgroup test we are done. ♠

**Definition 1.1.19.** Let  $S$  be a subset of  $G$ , we define  $\langle S \rangle = \bigcap \{H \leq G : S \subseteq H\}$ . We say  $\langle S \rangle$  is the group generated by elements of  $S$ .

**Proposition 1.1.20.** Let  $S$  be a subset of  $G$ , then  $\langle S \rangle$  is the smallest subgroup of  $G$  which contains  $S$ .

*Proof.* We will show that if  $P \leq G$  is a subgroup such that  $S \subseteq P$ , we must have  $\langle S \rangle \subseteq P$ . Note we have  $\langle S \rangle$  is a subgroup of  $G$  as we showed in Example 1.1.18, by taking  $\mathcal{H} = \{H \leq G : S \subseteq H\}$ . If  $S \subseteq P$ , then  $P \in \mathcal{H}$ , hence  $\langle S \rangle \subseteq P$  as  $\langle S \rangle$  is the intersection of all such subgroups. Hence it is indeed the smallest subgroup which contains  $S$ . ♡

**Definition 1.1.21.** Let  $G$  be a group, and  $A \subseteq G$ . We define

$$\bar{A} := \left\{ \prod_{i=1}^n a_i^{b_i} : n \in \mathbb{Z}, n \geq 0, a_i \in A, b_i = \pm 1 \text{ for } 1 \leq i \leq n \right\}$$

In addition, if  $A = \emptyset$ , then we define  $\bar{A} = \{e\}$ .

**Theorem 1.1.22.** Let  $G$  be a group. Let  $A$  be a subset of  $G$ . Then,  $\bar{A} = \langle A \rangle$ .

*Proof.* To see  $\bar{A}$  is a subgroup, note  $\bar{A}$  is never empty even if  $A$  is. If  $a, b \in \bar{A}$  with  $a = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}$  and  $b = b_1^{q_1} b_2^{q_2} \dots b_m^{q_m}$ . We have

$$ab^{-1} = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} b_m^{-q_m} b_{m-1}^{-q_{m-1}} \dots b_2^{-q_2} b_1^{-q_1}$$

Thus  $ab^{-1} \in \bar{A}$  as  $(x^{\pm 1})^{-1} = x^{\mp 1}$  and  $a_1, \dots, a_n, b_1, \dots, b_m \in A$ . By subgroup test, it is a subgroup.

Since each  $a \in A$  can be written as  $a^1$ , we have  $A \subseteq \bar{A}$ . Hence  $\langle A \rangle \subseteq \bar{A}$  as  $\langle A \rangle$  is the smallest subgroup contains  $A$ . However,  $\langle A \rangle$  is a group, so it is closed under the group operation and the process of taking inverse. Namely,  $\langle A \rangle$  contains each element of the form  $a_1^{k_1} \dots a_n^{k_n}$  where  $a_1, \dots, a_n \in A$  and  $k_1, \dots, k_n = \pm 1$ . Hence  $\bar{A} \subseteq \langle A \rangle$ . Hence  $\langle A \rangle = \bar{A}$ .  $\heartsuit$

**Example 1.1.23.** Prove or disprove the following:

1. If every element of  $G$  has finite order then  $G$  is finite.
2. If  $G$  has finitely many subgroups then  $G$  is a finite group.

*Proof.* 1. No this is not true in general. Let  $G = (\mathbb{Z}_2[x], +)$  be the group of polynomials with coefficient from  $\mathbb{Z}_2$  under addition. Clearly it forms a group. Addition of polynomials is associative. We have the identity element, namely the zero polynomial, 0. In addition, every polynomial have an inverse, namely itself. Indeed, let  $r(x) = \sum_{i=0}^n a_i x^i$ , where  $a_i = 1$  or  $a_i = 0$ . We have  $r(x) + r(x) = 0$ . Hence, every element in  $G$  has order 2, but this group is infinite.

2. We will do proof by cases.

If at least one element of  $G$  has infinite order, say  $y \in G$ , then we have  $\langle y \rangle, \langle y^2 \rangle, \langle y^3 \rangle, \dots$  are all different subgroups of  $G$ , and it obviously form a bijection between  $\langle y \rangle, \langle y^2 \rangle, \langle y^3 \rangle, \dots$  and  $\mathbb{N}$ . Hence  $G$  does not have finitely many subgroups, a contradiction to our assumption.

Suppose all the elements in  $G$  have finite order. Then  $\bigcup_{x \in G} \langle x \rangle$  is finite. Indeed,  $\langle x \rangle$  is finite for all  $x \in G$  because their order are all finite. In addition, we have the number of subgroups is finite so the number of cyclic subgroups formed this way must be less than or equal to the number of subgroups in total. However, the set  $\bigcup_{x \in G} \langle x \rangle$  contains all elements in  $G$  (each cyclic subgroups contain at least one distinct  $x \in G$ ), so  $G \subseteq \bigcup_{x \in G} \langle x \rangle$ . Obviously, we have  $\bigcup_{x \in G} \langle x \rangle \subseteq G$  as it is the union of subgroups of  $G$ . Hence  $G = \bigcup_{x \in G} \langle x \rangle$  and  $G$  is finite.  $\heartsuit$

## 1.2 Cyclic Groups

**Definition 1.2.1.** We say a group  $G$  is **cyclic** if  $\exists g \in G$  such that  $G = \langle g \rangle$

**Example 1.2.2.**  $\mathbb{Z}_2 \times \mathbb{Z}_2$  is not cyclic

*Solution.* None of the elements in the group has order 4 =  $|\mathbb{Z}_2 \times \mathbb{Z}_2|$ , i.e. every element has order at most 2, so it cannot be cyclic. ♠

**Proposition 1.2.3.** Let  $G$  be a group and suppose  $x \in G$  and  $n, m \in \mathbb{Z}$  with  $nm \neq 0$ . If  $x^n = x^m = e$  and  $d = \gcd(m, n)$ , then  $x^d = e$ . In particular, if  $k \in \mathbb{Z}$  such that  $x^k = e$ , then  $|x|$  divides  $k$ .

*Proof.* There exists  $d = an + bm$ . So we have  $x^d = x^{an+bm} = (x^n)^a(x^m)^b = (e)(e) = e$ .

Suppose  $x^k = e$  and let  $d = \gcd(k, |x|)$ , then we have  $x^d = e$ . By minimality, we have  $|x| \leq d$ , while by definition, we also have  $d \leq |x|$ , so  $d = |x|$ . Hence  $d|k \Rightarrow |x| \mid k$  ♡

**Proposition 1.2.4.** Let  $G$  be a group and suppose  $x \in G$  and  $m \in \mathbb{Z} \setminus \{0\}$ .

1. If  $|x| = \infty$  then  $|x^m| = \infty$
2. If  $|x| = n < \infty$  then  $|x^m| = \frac{n}{\gcd(m, n)}$

*Proof.* 1. If  $|x^m| = k < \infty$  then  $x^{mk} = e$ , hence  $|x| < mk < \infty$   
 2. Suppose  $|x| = n < \infty$ , let  $d = \gcd(m, n)$  and  $x^m = y$ . Let  $m = da$  and  $n = db$  for  $a, b \in \mathbb{Z}$ . We must show  $|y| = b$ . Now  $y^b = x^{mb} = x^{dab} = (x^n)^a = e$ . So  $|y| \mid b$ . But  $y^{|y|} = e \Rightarrow x^{m|y|} = e \Rightarrow n \mid m|y| \Rightarrow db \mid da|y| \Rightarrow b \mid a|y|$ . However,  $\gcd(a, b) = \gcd(\frac{m}{d}, \frac{n}{d}) = 1$ , so  $b \mid |y|$  and  $b = |y|$

♡

**Proposition 1.2.5.** Let  $G = \langle x \rangle$  be a cyclic group.

1. If  $|x| = \infty$  then  $G = \langle x^m \rangle$  iff  $m = \pm 1$
2. If  $|x| = n < \infty$ , then  $G = \langle x^m \rangle$  iff  $\gcd(m, n) = 1$

*Proof.* 1. If  $m = \pm 1$  then we are done. Conversely, suppose  $\langle x^m \rangle = \langle x \rangle$ . Then we have  $x \in \langle x^m \rangle$  so  $x = x^{mk}$  for  $k \in \mathbb{Z}$ . Hence  $x^{mk-1} = e \Rightarrow mk = 1 \Rightarrow m = \pm 1$   
 2.

$$\begin{aligned} \langle x \rangle &= \langle x^m \rangle \\ \Leftrightarrow |x| &= |x^m| \\ \Leftrightarrow n &= \frac{n}{\gcd(m, n)} \\ \Leftrightarrow \gcd(n, m) &= 1 \end{aligned}$$

♡

**Example 1.2.6.** let  $G = \mathbb{Z}_{24}$ , we have  $|10| = |10 \cdot 1| = \frac{24}{\gcd(24, 10)} = \frac{24}{2} = 12$ .

**Example 1.2.7.** Let  $G = \mathbb{Z}_7^\times$ , find all generators.



*Solution.* First we have to show it is a cyclic group. Consider  $\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = G$ . Then the generators are  $3^m$ , where  $\gcd(m, 6) = 1$ , i.e.  $m = 1, 5$ . Hence the generators are 3 and  $3^5 = 5$ . ♠

**Proposition 1.2.8.** Say  $G = \langle x \rangle$  be cyclic.

1. Every subgroup of  $G$  is cyclic
2. If  $|G| = n < \infty$ , then for every positive  $d \in \mathbb{Z}$ , such that  $d|n$ , there is a unique subgroup of order  $d$ . Moreover, these are all of the subgroups.

*Proof.* 1. Suppose  $H \leq G$ . If  $H = \{e\} = \langle e \rangle$ , then we are done. Assume  $H \neq \{e\}$ . Let  $m \in \mathbb{N}$  be minimal such that  $x^m \in H$ . We claim  $H = \langle x^m \rangle$ . Clearly  $\langle x^m \rangle \subseteq H$ . Let  $x^k \in H$ , by the division algorithm,  $\exists q, r \in \mathbb{Z}$ , we have  $0 \leq r < m$  such that  $k = qm + r$ . Therefore,  $x^k = x^{mq}x^r$ , thus  $x^r = x^k x^{-mq}$ , and note  $x^k \in H$  and  $x^{-mq} \in H$ . Thus  $x^r \in H$ , however  $m$  is the minimal number makes  $x^m \in H$ , thus  $r$  must be zero as  $0 \leq r < m$ . Hence  $x^k = x^{mq} \in \langle x^m \rangle$ . Therefore  $H \subseteq \langle x^m \rangle$  and  $H = \langle x^m \rangle$ .

2. Let  $d \in \mathbb{N}$ ,  $d|n$ . Let  $m = n/d$ , and let  $H = \langle x^m \rangle$ . Thus

$$|H| = |x^m| = \frac{n}{\gcd(m, n)} = \frac{n}{\gcd(n/d, n)} = \frac{n}{n/d} = d$$

Now, let  $K$  be an arbitrary subgroup of order  $d$ , we are going to show  $K = H$ . Note  $K = \langle x^k \rangle$  where  $k \in \mathbb{N}$  is minimal such that  $x^k \in K$ . Note  $d = |K| = \frac{n}{\gcd(k, n)}$  which imply  $\gcd(k, n) = \frac{n}{d} = m$ . Hence  $m|k$ , and  $\langle x^k \rangle \leq \langle x^m \rangle$ . However, since they have the same order, we have  $K = H$ .

Now, let  $J \leq G$ , thus  $J = \langle x^j \rangle$ . Note  $\gcd(j, n)|j$ , therefore  $\langle x^j \rangle \leq \langle x^{\gcd(j, n)} \rangle$ . However,  $|J| = |x^j| = \frac{n}{\gcd(n, j)}$  and so  $\frac{n}{|J|} = \gcd(n, j)$  and  $|J| | n$ .

♡

**Example 1.2.9.** Let  $G$  be a group and  $a, b \in G$  with  $ab = ba$  and  $\gcd(|a|, |b|) = 1$ . Then  $|ab| = \text{lcm}(|a|, |b|)$ .

*Solution.* Let  $|a| = m$ ,  $|b| = n$ , let  $d = \gcd(n, m)$ . Then we have  $\text{lcm}(n, m) = nm/\gcd(m, n)$ . Hence, we first show  $ab^{\text{lcm}(n, m)} = e$ . We have  $ab^{\text{lcm}(n, m)} = ab^{nm} = (a^m)^n(b^n)^m = e$  as we have  $ab = ba$ . Next, suppose  $q = |ab|$  and  $q < \text{lcm}(n, m) = nm$ . Then, we have  $nm = kq + r$  where  $r < q$ . Hence,  $(ab)^{nm} = e = (ab)^{kq+r} = (a^{kq})(a^r)(b^{kq})(b^r) = ((ab)^q)^k(ab)^r = e(ab)^r$ . Thus  $(ab)^r = e$ , contradict to the fact that  $q$  is the smallest. Hence we must have  $q \geq nm$ , and thus  $q = nm$  as it is the smallest. ♠

**Example 1.2.10.** Let  $\gcd(n, m) \neq 1$ . Prove  $\mathbb{Z}_n \times \mathbb{Z}_m$  is not cyclic. In addition,  $\gcd(n, m) = 1$  then  $\mathbb{Z}_n \times \mathbb{Z}_m$  is cyclic.

*Solution.* Let  $d > 1$ ,  $d|n$  and  $d|m$ . Therefore, we have  $H_1 \leq \mathbb{Z}_n$  and  $H_2 \leq \mathbb{Z}_m$  where  $|H_1| = |H_2| = d$ . Now,  $H_1 \times \{0\}$  and  $\{0\} \times H_2$  are both groups of order  $d$ , and they are different. By Proposition 1.2.8, it is impossible to have two distinct subgroups with the same order in cyclic group.

Suppose  $\gcd(m, n) = 1$  and consider  $a = (1, 0)$  and  $b = (0, 1)$  in  $\mathbb{Z}_n \times \mathbb{Z}_m$ . Then,  $|a| = n$ ,  $|b| = m$ , and  $a + b = b + a$ . From Example 1.2.9, we have  $|a + b| = |(1, 1)| = nm = |\mathbb{Z}_n \times \mathbb{Z}_m|$  and hence  $\mathbb{Z}_n \times \mathbb{Z}_m = \langle (1, 1) \rangle$  is cyclic. ♠

## 1.3 Symmetric Groups

**Definition 1.3.1.** Let  $\emptyset \neq X$  be a set. Let  $S_X = \{f : X \rightarrow X : f \text{ is bijection}\}$ , then  $(S_X, \circ)$  is a group, where  $\circ$  is function composition. We denote its identity to be  $e$ . We call all such  $S_X$  to be **symmetric group**.

**Remark 1.3.2.** Note  $|S_n| = n!$ , where  $n = \{1, 2, 3, \dots, n\}$ .

**Example 1.3.3.** Let  $f, g \in S_5$  to be

$$f : 1 \mapsto 3, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 5, 5 \mapsto 2$$

and

$$g : 1 \mapsto 5, 2 \mapsto 4, 3 \mapsto 3, 4 \mapsto 1, 5 \mapsto 2$$

Determine  $f^2 \circ g$

*Solution.* We have  $f^2 \circ g : 1 \mapsto 4, 2 \mapsto 2, 3 \mapsto 3, 4 \mapsto 1, 5 \mapsto 5$  ♠

**Definition 1.3.4.** A ***m*-cycle** is a string of  $m$  distinct numbers from  $\{1, 2, 3, \dots, n\}$ . The  $m$ -cycle  $(a_1, a_2, \dots, a_m)$  denotes the permutation

$$a_i \mapsto a_{i+1}, a_{i+1} \mapsto a_{i+2}, \dots, a_m \mapsto a_1$$

**Remark 1.3.5.** Every  $\sigma \in S_n$  can be written as a product of disjoint cycles. We call this disjoint cycle form. Moreover, when write in cycle form, we omit elements that maps to itself. Thus,  $\sigma = (1, 2)(3)(4, 5) = (1, 2)(4, 5)$ .

**Example 1.3.6.** In the last example, we have  $f = (1, 3)(2, 4, 5)$  and  $g = (1, 5, 2, 4)$ . Therefore we have

$$f^2 \circ g = (13)(245)(13)(245)(1524) = (14)$$

**Example 1.3.7.** Let  $\alpha = (1, 2)(4, 5)$  and  $\beta = (16532)$ , then we have  $\alpha\beta = (16453)$

**Remark 1.3.8.** Disjoint cycles commute.

Moreover, the  $m$ -cycle  $\sigma = (a_1, \dots, a_m)$  has the inverse  $\sigma^{-1} = (a_m, a_{m-1}, \dots, a_1)$ . In general, we have  $\sigma = \sigma_1 \dots \sigma_l$  then  $\sigma = \sigma_l^{-1} \dots \sigma_1^{-1}$ .

**Proposition 1.3.9.** Let  $\sigma = \sigma_1 \dots \sigma_l \in S_n$  be in disjoint cycle form, then  $|\sigma| = \text{lcm}(|\sigma_1|, \dots, |\sigma_l|)$ .

*Proof.* Suppose  $\sigma = \sigma_1 \dots \sigma_m \in S_n$ , where the  $\sigma_i$ 's are disjoint cycles. For all  $i, j$ , we then have that  $\sigma_i \sigma_j = \sigma_j \sigma_i$ . Let  $r = |\sigma|$  so that  $e = \sigma^r = \sigma_1^r \sigma_2^r \dots \sigma_m^r$ . Since  $\sigma_i$ 's

are disjoint, we must have that each  $\sigma_i^r = e$ . Therefore,  $|a_i| \mid r$  for  $i = 1, 2, \dots, m$ . In particular,  $r$  is a common multiple of  $|\sigma_1|, \dots, |\sigma_m|$ , and so  $\text{lcm}(|\sigma_1|, \dots, |\sigma_m|) \leq r$ . Let  $d = \text{lcm}(|\sigma_1|, \dots, |\sigma_m|)$ , we also have that  $\sigma^d = e \cdot e \cdot e \dots \cdot e = e$  and thus  $r \leq d$  as well. So  $|\sigma| = d$  as desired.  $\heartsuit$

**Example 1.3.10.** Let  $\alpha = (12)(345)$  and  $\beta = (134)(25)$  then  $\alpha\beta = (14235)$ . Thus  $|\alpha\beta| = 5$  and  $|\alpha| = \text{lcm}(2, 3) = 6$ .

**Definition 1.3.11.** A 2-cycle in  $S_n$  is called a transposition. i.e.  $\tau = (a_1, a_2)$ .

**Proposition 1.3.12.** Every  $\sigma \in S_n$  can be written as a product of transposition. That is, if  $T$  is the set of transposition in  $S_n$  then  $\langle T \rangle = S_n$

*Proof.* It suffices to show any cycle in  $S_n$  is a product of transpositions. Consider  $\sigma = (a_1, \dots, a_m) \in S_m$ , then  $\sigma = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_3)(a_1 a_2)$   $\heartsuit$

**Definition 1.3.13.** Let  $\sigma \in S_n$ , we define the sign of  $\sigma$ , and write  $\text{sgn}(\sigma)$ , as the following: let  $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$  be the polynomial with  $n$  variables, then define

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}), \text{ then } \text{sgn}(\sigma) = \begin{cases} 1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta \end{cases}.$$

In addition, we say  $\sigma$  is even if and only if  $\text{sgn}(\sigma) = 1$ , otherwise, we say  $\sigma$  is odd.

**Definition 1.3.14.** We define the **alternating group of degree  $n$**  to be  $A_n := \{\sigma \in S_n : \text{sgn}(\sigma) = 1\}$

**Proposition 1.3.15.** We list some properties of  $\text{sgn}$ ,

1.  $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$
2. All transpositions are odd
3.  $\sigma$  is even if and only if  $\sigma$  can be written as a product of an even number of transpositions
4.  $A_n \leq S_n$

*Proof.* 1. Observe that

$$\begin{aligned} \sigma\tau(\Delta) &= \sigma(\text{sgn}(\tau)\Delta) = \text{sgn}(\tau)\sigma(\Delta) \\ &= \text{sgn}(\tau)\text{sgn}(\sigma)\Delta \\ &= \text{sgn}(\sigma\tau)\Delta \end{aligned}$$

and so  $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$ .

2. A transposition  $\tau = (p, q) \in S_n$  with  $p < q$ , will change the sign of the terms

$$(x_p - x_q), (x_{p+1} - x_q), \dots, (x_{q-1} - x_q)$$

$$(x_p - x_{q-1}), (x_p - x_{q-2}), \dots, (x_p - x_{p+1})$$

There are  $(q - 1 - p + 1) + (q - 1 - p) = 2(p - q) - 1$  such terms and thus  $\text{sgn}(\tau) = (-1)^{2(p-q)-1} = -1$ .

3. Let  $\sigma = \tau_1 \dots \tau_m \in S_n$  be written as a product of transposition. Then  $\sigma$  is even if and only if  $\text{sgn}(\tau_1) \dots \text{sgn}(\tau_m) = 1$  iff  $(-1)^m = 1$  if and only if  $m$  is even.

4. Let  $\alpha, \beta \in A_n$  so that  $\text{sgn}(\alpha) = \text{sgn}(\beta) = 1$ . Now,  $e = \beta\beta^{-1} \Rightarrow 1 = \text{sgn}(e) = \text{sgn}(\beta)\text{sgn}(\beta^{-1}) \Rightarrow \text{sgn}(\beta^{-1}) = 1$ . Thus  $\text{sgn}(\alpha\beta^{-1}) = 1 \cdot 1 = 1$  and so  $A_n \leq S_n$  by subgroup test.

Note, we can also prove all the above propositions by matrix correspondence between permutations and permutation matrices. ♥

**Example 1.3.16.**  $\sigma = (142)(2567) = (13)(14)(27)(26)(25)$

**Example 1.3.17.**  $S_n = \langle (1, 2), (1, 2, \dots, n) \rangle$

*Solution.* Let  $c = (1, 2, \dots, n)$ . Then

$$\begin{aligned} c(1, 2)c^{-1} &= (2, 3) \\ c(2, 3)c^{-1} &= (3, 4) \\ &\vdots \\ c(n-2, n-1)c^{-1} &= (n-1, n) \end{aligned}$$

Thus, we must have  $(i-1, i) \in \langle (1, 2), c \rangle$  for all  $1 \leq i \leq n$ . Moreover,

$$\begin{aligned} (2, 3)(1, 2)(2, 3)^{-1} &= (1, 3) \\ (3, 4)(1, 3)(3, 4)^{-1} &= (1, 4) \\ &\vdots \\ (n-1, n)(1, n-1)(n-1, n)^{-1} &= (1, n) \end{aligned}$$

Thus we have  $(1, i) \in \langle (1, 2), c \rangle$  for all  $1 \leq i \leq n$ . Next, for  $1 \leq i < j \leq n$ , we have  $(i, j) = (1, i)(1, j)(1, i)^{-1} \in \langle (1, 2), c \rangle$ , so all the transpositions are in  $\langle (1, 2), c \rangle$ . Hence, we must have  $S_n = \langle (1, 2), c \rangle$ . ♠

## 1.4 Dihedral Groups

**Definition 1.4.1.** For  $n > 1$ , let  $D_{2n}$  denote the group of symmetries of the regular  $n$ -gon (under composition).

**Remark 1.4.2.** We work with  $D_{2n}$  by realizing its elements as permutations in  $S_n$ , we do this by labelling the vertices with  $\{1, 2, 3, \dots, n\}$  and recording how the symmetries permute the vertices.

**Remark 1.4.3.** Some conventions.  $D_{2n}$  be regular  $n$ -gons centered at origin and we denote  $r$  to be the rotation (move every vertex to the next vertex clockwise) and  $s$  be the reflection over the line joining vertex 1 and the origin.

We have  $|r| = n$  and  $|s| = 2$ . Moreover,  $rs = sr^{-1} = sr^{n-1}$  and we have  $D_{2n} = \{e, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$ .

## 1.5 Quaternion Groups

**Definition 1.5.1.** The *Quaternion group* is defined as the set

$$Q = \{1, -1, i, -i, j, -j, k, -k\}$$

with the operation given in the following table:

	1	-1	$i$	$-i$	$j$	$-j$	$k$	$-k$
1	1	-1	$i$	$-i$	$j$	$-j$	$k$	$-k$
-1	-1	1	$-i$	$i$	$-j$	$j$	$-k$	$k$
$i$	$i$	$-i$	-1	1	$k$	$-k$	$-j$	$j$
$-i$	$-i$	$i$	1	-1	$-k$	$k$	$j$	$-j$
$j$	$j$	$-j$	$-k$	$k$	-1	1	$i$	$-i$
$-j$	$-j$	$j$	$k$	$-k$	1	-1	$-i$	$i$
$k$	$k$	$-k$	$j$	$-j$	$-i$	$i$	-1	1
$-k$	$-k$	$k$	$-j$	$j$	$i$	$-i$	1	-1

# Chapter 2

## Quotient Group

### 2.1 Cosets

**Definition 2.1.1.** Let  $G$  be a group and  $H \leq G$ . Let  $g \in G$ , we define the left (resp. right) coset of  $H$  in  $G$  containing  $g$  to be the set  $gH := \{gx : x \in H\}$  (resp.  $Hg := \{xg : x \in H\}$ ).

**Example 2.1.2.** Let  $G = \mathbb{Z}$ , and  $H = \langle 2 \rangle$ , then  $0 + H = \{0 + h : h \in H\} = H$ . Moreover,  $1 + H = \{1 + h : h \in H\} = \{1 + 2k : k \in \mathbb{Z}\}$ . Similarly, we find that  $3 + H = 1 + H$ .

**Example 2.1.3.** Let  $G = S_4$  and  $H = A_4$ . and say  $\sigma = (12)(14)(34)(23)(13)$  and  $\alpha = (14)(34)(23)(13)$ . Then, since  $\alpha \in H$ , we have  $\sigma H = (12)\alpha H = (12)H$ .

**Proposition 2.1.4.** Let  $G$  be a group and  $H \leq G$ .

1.  $eH = He = H$
2. We have  $gH = Hg = H$  iff  $g \in H$
3.  $aH = bH$  iff  $b^{-1}a \in H$  and  $Ha = Hb$  iff  $ba^{-1} \in H$
4.  $|gH| = |Hg| = |H|$

*Proof.*

1. Trivial
2. We will show  $gH = H$  iff  $g \in H$  as the other case is similar. Suppose  $gH = H$ . Then we have  $e \in H$  since it is a subgroup, and  $ge = g \in H$ . Conversely, suppose  $g \in H$ . Let  $x = gh \in gH$ , then  $g \in H$  and  $h \in H$  we have  $gh \in H$  thus  $x \in H$  so  $gH \subseteq H$ . Then, let  $h \in H$ , we have  $h = gg^{-1}h$  and  $g^{-1}h \in H$  so  $h \in gH$ . Therefore  $H \subseteq gH$  and the proof follows.
3. We will show  $aH = bH \iff b^{-1}a \in H$  and the other case is similar. Suppose  $aH = bH$ , then  $ae = bh$  for some  $h \in H$ . Thus,  $b^{-1}a = h \in H$ . Conversely, suppose  $b^{-1}a \in H$ , then we have  $b^{-1}aH = H$  by the last result. Then,  $\forall h_1 \in H$ , there exists  $h_2 \in H$ , so that  $b^{-1}ah_2 = h_1$ , and this happens if and only if  $ah_2 = bh_1$ . Hence, let  $bh_1 \in bH$ , then we can find  $h_2$  so that  $ah_2 \in aH$  which imply  $bH \subseteq aH$ . Next, for all  $b^{-1}ah_1 \in b^{-1}aH$ , we can find

$h_2$  so that  $b^{-1}ah_1 = h_2$ , which happens if and only if  $ah_1 = bh_2$ . Thus, for all  $ah_1 \in aH$ , we can find  $h_2$  so that  $ah_1 = bh_2$ . Hence,  $aH \subseteq bH$  and we are done.

4. Note  $\phi : H \rightarrow gH$  where  $h \mapsto gh$  is a bijection. Similarly,  $\Phi : H \rightarrow Hg$  where  $h \mapsto hg$  is a bijection. Hence, we are finished.

♡

**Proposition 2.1.5.** *Let  $G$  be a group and  $H \leq G$ .*

1. *If  $a, b \in G$  then  $aH \cap bH = \emptyset$  or  $aH = bH$ .*
2. *For all  $g \in G$ ,  $g \in gH$ , i.e. the distinct left coset of  $H$  in  $G$  partition  $G$ .*

*Proof.* We will show (1), as (2) is trivial. If  $aH \cap bH = \emptyset$  then we are done. Thus, suppose  $x \in aH \cap bH \neq \emptyset$ . Therefore,  $x = ah_1 = bh_2$  for some  $h_1, h_2 \in H$ . Thus,  $b^{-1}a = h_2h_1^{-1} \in H$ . However,  $b^{-1}a \in H$  imply  $aH = bH$  by the Proposition 2.1.4.(3). ♡

**Theorem 2.1.6.** *[Lagrange] If  $G$  is a finite group and  $H$  is a subgroup, then  $|H| \mid |G|$ . Moreover,  $|G|/|H|$  is the number of distinct left cosets of  $H$  in  $G$ .*

*Proof.* Let  $g_1H, g_2H, \dots, g_nH$  be the distinct left cosets of  $H$  in  $G$ . Since these cosets partition  $G$ , we have  $|G| = |g_1H| + |g_2H| + \dots + |g_nH| = n|H|$  since we know  $|gH| = |H|$ . Thus  $|G|/|H| = n$  as required. ♡

**Corollary 2.1.6.1.** *If  $G$  is finite group and  $g \in G$  then  $|g| \mid |G|$ .*

*Proof.* Note  $|g| = |\langle g \rangle|$  thus by Lagrange theorem we have  $|g| \mid |G|$  ♡

**Corollary 2.1.6.2.** *If  $|G| = p$  is a prime, then  $G$  is cyclic.*

*Proof.* Take  $e \neq g \in G$ , then  $|g| \mid p$ , so  $|g| = p$  as  $g$  is not the identity. Then  $|\langle g \rangle| = |G|$  so  $\langle g \rangle = G$ . ♡

**Corollary 2.1.6.3 (Euler's theorem).** *If  $\gcd(a, n) = 1$  then  $a^{\phi(n)} \equiv 1 \pmod{n}$*

*Proof.* Note  $a \in \mathbb{Z}_n^\times$  and  $|\mathbb{Z}_n^\times| = \phi(n)$  so  $|a| \mid \phi(n)$ . Say  $\phi(n) = |a|m$ , so  $a^{\phi(n)} = a^{|a|m} = 1 \in \mathbb{Z}_n^\times = U(n)$ . ♡

**Example 2.1.7.** We have  $G = A_4$  and  $|G| = \frac{4!}{2} = 12$ . We want to show that  $G$  has no subgroup of order 6. For contradiction, suppose there exists  $H \leq G$  with  $|H| = 6$ . Now, let  $\sigma \in G$  to be order 3. Now, by Lagrange, there are  $12/6 = 2$  distinct left cosets of  $H$  in  $G$ . Consider,  $H, \sigma H, \sigma^2 H$ . Since the distinct cosets are two, we must have two of the three are equal. Then we have three cases:

1. If  $\sigma H = H$ , then  $\sigma \in H$
2. If  $\sigma H = \sigma^2 H$ , then  $H = \sigma H$  and  $\sigma \in H$
3. If  $\sigma^2 H = H$ , then  $\sigma^2 \in H$  where  $\sigma^{-1} = \sigma^2$ . Thus  $\sigma \in H$  as  $H$  is a subgroup.

Thus, in any case,  $\sigma \in H$ . Therefore, all  $\sigma \in G$  with order 3 are in  $H$ , and we have at least seven 3-cycles in  $G$ , and therefore contradiction.

**Definition 2.1.8.** Let  $G$  be a group and  $H \leq G$ . We define the **index** of  $H$  in  $G$ ,  $[G : H]$ , to be the number of distinct left (or right) cosets of  $H$  in  $G$ . Moreover, we denote the set of left cosets of  $H$  in  $G$  by  $G/H$  and say  $G \bmod H$ .

**Remark 2.1.9.** If  $G$  is finite, then  $|G/H| = \frac{|G|}{|H|} = [G : H]$ .

**Example 2.1.10.** For each of the following groups  $G$  and  $H \leq G$ , list the distinct left cosets of  $H$  in  $G$  and compute  $[G : H]$ .

1.  $G = GL_n(\mathbb{Z}_p)$ ,  $H = SL_n(\mathbb{Z}_p)$  where  $p$  is prime
2.  $G = S_n$ ,  $H = \{\sigma \in S_n : \sigma(n) = n\}$
3.  $G = \mathbb{Z}_n \times \mathbb{Z}_n$ ,  $H = \{(x, x) : x \in \mathbb{Z}_n\}$

*Solution.*

1. Note  $aH = bH \iff b^{-1}a \in H \iff \det(b^{-1}a) = 1 \iff \det(a) = \det(b)$ . Thus  $G/H = \{a_1H, \dots, a_{p-1}H\}$  where  $\det(a_i) = i$  is any matrix with determinant equal  $i$ . In particular, we have  $[G : H] = p - 1$ .
2.  $\sigma H = \tau H \iff \tau^{-1}\sigma \in H \iff \tau^{-1}\sigma(n) = n \iff \sigma(n) = \tau(n)$ . Thus  $G/H = \{\sigma_1H, \dots, \sigma_nH\}$  where  $\sigma_i = (i, n)$  and  $\sigma_n = e$ . In particular,  $[G : H] = n$ .
3. Note  $(a, b) + H = (c, d) + H \iff (a - c, b - d) \in H \iff a - c = b - d$ . Thus,  $(0, 0), (1, 0), \dots, (n - 1, 0)$  are distinct cosets of  $H$  in  $G$ . Since  $[G : H] = |G|/|H| = n$ , this list is complete.



**Example 2.1.11.** Let  $G = D_8$ , we have  $Z(G) = \{e, r^2\}$ . However,  $G/Z(G)$  is abelian where  $G$  is not abelian.

**Example 2.1.12.**  $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle$ ,

$$\begin{aligned} a + n\mathbb{Z} = b + n\mathbb{Z} &\iff a - b \in n\mathbb{Z} \\ &\iff n|(a - b) \\ &\iff a \equiv b \pmod{n} \end{aligned}$$

Thus,  $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n - 1) + n\mathbb{Z}\}$

**Example 2.1.13.** Let  $G = S_4$  and  $H = A_4$ . We have

$$\begin{aligned} \sigma H = \tau H &\iff \tau^{-1}\sigma \in H \\ &\iff \text{sgn}(\tau^{-1}\sigma) = 1 \\ &\iff \text{sgn}(\tau^{-1})\text{sgn}(\sigma) = 1 \\ &\iff \text{sgn}(\tau)\text{sgn}(\sigma) = 1 \\ &\iff \text{sgn}(\tau) = \text{sgn}(\sigma) \end{aligned}$$

Therefore,  $G/H = \{H, (1, 2)H\}$ . Note:  $|G|/|H| = 2 \Rightarrow |H| = \frac{|G|}{2}$ .



**Example 2.1.14.** Let  $G = G_1 \times G_2$  and  $H = G_1 \times \{e\}$ . Then consider  $G/H$ , we have

$$\begin{aligned}(a, b)H = (c, d)H &\Leftrightarrow (c, d)^{-1}(a, b) \in H \\ &\Leftrightarrow (c^{-1}, d^{-1})(a, b) \in H \\ &\Leftrightarrow (c^{-1}a, d^{-1}b) \in H \\ &\Leftrightarrow d^{-1}b = e \\ &\Leftrightarrow d = b\end{aligned}$$

Thus, we have  $(x, y)H = (e, y)H$  and so  $G/H = \{(e, g)H : g \in G_2\}$ .

## 2.2 Quotient Groups

**Remark 2.2.1.** Now, we want to turn  $G/H$  into a group with the natural operation. Namely, we want  $(aH)(bH) = (ab)H$ . This operation have associativity, and we have  $eH = H$  to be the identity. Moreover, we have  $(gH)^{-1} = g^{-1}H$ . However, even it look satisfying every group axioms, this operation may not be well-defined.

**Example 2.2.2.** Say  $aH = \alpha H$  and  $bH = \beta H$ . Then

$$\begin{aligned}(aH)(bH) &= (\alpha H)(\beta H) \Rightarrow abH = \alpha\beta H \\ &\Rightarrow (ab)^{-1}(\alpha\beta) \in H \text{ with } \alpha = ah_1, \beta = bh_2, h_1, h_2 \in H \\ &\Rightarrow b^{-1}a^{-1}ah_1bh_2 \in H \\ &\Rightarrow b^{-1}h_1bh_2 \in H \\ &\Rightarrow b^{-1}h_1b \in H\end{aligned}$$

**Definition 2.2.3.** Let  $H \leq G$ , we say  $H$  is **normal** in  $G$  (or a **normal subgroup**) if for all  $g \in G$ , we have  $gHg^{-1} = H$ . If  $H$  is normal in  $G$ , we write  $H \trianglelefteq G$ .

**Remark 2.2.4.** We have  $gHg^{-1} = H$  iff  $gH = Hg$ .

**Example 2.2.5.** Let  $G = S_3$  and  $H = \langle (1, 2) \rangle = \{e, (1, 2)\}$ . Then we have  $H \not\trianglelefteq G$ .

**Example 2.2.6.** Show that  $H \leq G$  and  $[G : H] = 2$  imply  $H \trianglelefteq G$ .

*Solution.* If  $g \in H$  then  $gH = Hg = H$ . Next, suppose  $g \notin H$ . Then we have  $G = H \cup gH$  where we know  $H$  and  $gH$  are disjoint. However, we also have the right coset partition the group, thus  $G = H \cup Hg$ , hence we must have  $Hg = gH$  for all cases. ♠

**Remark 2.2.7.** By Example 2.2.6, we have  $A_n \trianglelefteq S_n$ .

**Example 2.2.8.** Recall the Quaternion group, show that every subgroup of  $Q$  is normal.

*Solution.* Note  $|Q| = 8$ , thus if  $H$  is a subgroup then  $|H|$  must divide 8. Thus  $|H| = 1, 2, 4, 8$ . If  $|H| = 8$  then  $H = Q$ . Clearly  $xGx^{-1} \subseteq G$  thus it is normal.

Say  $|H| = 1$  then  $H = \{1\}$  and  $g1g^{-1} = 1$  for all  $g \in Q$ , thus it is normal.

Only one subgroup  $H = \{-1, 1\}$  of  $Q$  can have order 2, because every element in  $Q$  other than  $-1$  and  $1$  has order 4 (we can read this from the table, for instance,  $i^1 = i, i^2 = -1, i^3 = -1 \cdot i = -i, i^4 = 1$ ), and if  $x \in G$  such that  $|x| = 4$  and  $x \in H$  where  $|H| = 2$ , then  $\langle x \rangle \subseteq H$ , hence we must have  $4|2$ , which is a contradiction. If  $H = \{1, -1\}$  then clearly for all  $x \in Q$  we have  $x1x^{-1} = xx^{-1} = 1$  since  $e = 1$  and  $x(-1)x^{-1} = x^{-1}x^{-1} = 1$ . Thus  $xHx^{-1} \subseteq H$  as desired.

If  $|H| = 4$ , then since  $[G : H] = 2$ , all of them must be normal by Example 2.2.6. ♠

**Example 2.2.9.** If  $G$  is abelian and  $H \leq G$ . Thus, for  $g \in G$ , we have  $gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg \Rightarrow H \trianglelefteq G$ . Moreover, we have  $Z(G) \trianglelefteq G$  by the definition of the center of the group.

**Proposition 2.2.10.** Let  $Z(G)$  be the center of  $G$ .  $G/Z(G)$  is cyclic then  $G$  is abelian. In addition, if  $p, q$  are primes and  $|G| = pq$ , then  $G$  is abelian or  $Z(G) = \{e\}$ .

*Proof.* Let  $H = Z(G)$ . If  $G/Z(G)$  is cyclic, then  $G/H = \langle \bar{g} \rangle$  where  $g \in G$ . Let  $x, y \in G$ , we have  $\bar{x} = \bar{g}^n$  and  $\bar{y} = \bar{g}^m$ , thus we have  $xH = g^nH \Rightarrow xh_1 = g^n h_2$  where  $h_1, h_2 \in H$ , therefore,  $x = g^n h_x$  where  $h_x = h_2 h_1^{-1} \in H$ . Similarly, we must have  $y = g^m h_y$  where  $h_y \in H$ .

Hence, we have

$$\begin{aligned} xy &= g^n h_x g^m h_y = g^n g^m h_x h_y \\ &= g^m g^n h_y h_x = g^m h_y g^n h_x = yx \end{aligned}$$

Therefore,  $G$  is abelian.

Next, let  $|G| = pq$ . Next, by Lagrange, we have  $H \leq G$  then  $|H| \mid |G|$ , thus all subgroups of  $G$  must have size  $|H| \in \{pq, p, q, 1\}$ . Suppose  $G$  is not abelian. Then  $H := Z(G) \leq G$  must be a proper subgroup (We know it must be a subgroup since it is not empty and if  $x, y \in H$  then  $y^{-1}x$  also commute with all elements of  $G$ ). Thus, we must have  $|H| = p, q$  or  $H = \{e\}$ . If  $H = \{e\}$  then we are done. If  $|H| = p$ , or  $q$ , then by Corollary 2.1.6.2, we have  $|G|$  is prime imply the group is cyclic, we have  $Z/H$  is cyclic (recall  $|Z/H| = |Z|/|H|$ , thus it will always be prime if  $|H| \in \{p, q\}$ ). Thus  $G$  is abelian, and thus we obtained a contradiction. Hence, it is impossible to have  $G$  is not abelian and  $|Z(G)| = p$  or  $q$ . Therefore, we can only have  $G$  is abelian or  $Z(G) = \{e\}$ . ♡

**Proposition 2.2.11.** Let  $H \leq G$ , then  $H \trianglelefteq G \iff \forall g \in G (gHg^{-1} \subseteq H)$

*Proof.* Note equal imply subset, thus  $H \trianglelefteq G$  imply  $gHg^{-1} \subseteq H$  as  $gHg^{-1} = H$ .

Now, suppose the converse, and let  $g \in G$ . We have  $gHg^{-1} \subseteq H$ , hence  $gH \subseteq Hg$ . Similarly, since we have the conclusion for all  $g$ , in particular, we have  $g^{-1} \in G$  holds. Thus,  $g^{-1}Hg \subseteq H$  and therefore,  $Hg \subseteq gH$ . Hence,  $Hg = gH$  for all  $g \in G$ . ♡

**Example 2.2.12.** Show that  $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

*Solution.* Let  $A \in GL_n(\mathbb{R})$  and  $B \in SL_n(\mathbb{R})$ . We must show that  $ABA^{-1} \in SL_n(\mathbb{R})$ . It is obvious as we have  $\det(ABA^{-1}) = \det(B) = 1$ . Thus by our proposition 2.2.11, we are done as  $A$  was arbitrary. ♠

**Definition 2.2.13.** Let  $H \leq G$ , the **normalizer** of  $H$  in  $G$ , we write as  $N_G(H)$ , is the set  $\{g \in G : gHg^{-1} = H\}$ .

**Proposition 2.2.14.**  $N_G(H)$  is the largest subgroup of  $G$  which contains  $H$  as a normal subgroup. That is, if  $N$  is a subgroup and  $H \trianglelefteq N$ , then  $N \subseteq N_G(H)$ ,

*Proof.* We first show  $N_G(H)$  is a subgroup. Note  $e \in N_G(H)$  as  $eHe = H$ , hence  $e \in N_G(H)$ . Let  $x, y \in N_G(H)$ , then

$$(xy^{-1})^{-1}Hxy^{-1} = yx^{-1}Hxy^{-1} = yHy^{-1} = H$$

Thus  $N_G(H)$  is indeed a subgroup of  $G$ .

Next, we show  $H \leq N_G(H)$ . Since  $xH = H$  if and only if  $x \in H$ , let  $x, x^{-1} \in H$  then we have  $xH = H = Hx^{-1}$  which imply  $(xH)x^{-1} = Hx^{-1} = H$ . Thus  $H \subseteq N_G(H)$  as for every element of  $H$  we have  $hHh^{-1} = H$ . In addition,  $H$  is not empty as it is a subgroup of  $G$ . Next, let  $x, y \in H$ , we have  $xy^{-1} \in H$  as it is a subgroup of  $G$ , thus it is indeed a subgroup of  $N_G(H)$ .

Next, we show  $H \trianglelefteq N_G(H)$ . It suffice to show  $\forall x \in N_G(H)$  we have  $xHx^{-1} \subseteq H$ . Let  $x \in N_G(H)$  then by definition, we have  $xHx^{-1} = H \subseteq H$ . Hence  $H \trianglelefteq N_G(H)$  as desired.

Let  $P$  be a subgroup of  $G$  that contains  $H$  as a normal subgroup. Then we must have  $\forall p \in P, pHp^{-1} = H$  by definition. Thus  $P \subseteq N_G(H)$  and indeed  $N_G(H)$  is the largest. ♥

**Definition 2.2.15.** Let  $G$  be group,  $H, K$  be subgroups of  $G$ , we define the set  $HK = \{ab : a \in H, b \in K\}$

**Proposition 2.2.16.** Let  $H, K \leq G$  be finite subgroups of  $G$ , then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

*Proof.* Note  $HK$  is a union of left cosets of  $K$ , namely

$$HK = \bigcup_{h \in H} hK$$

Since each coset of  $K$  has cardinality  $|K|$ , it suffices to find the number of distinct left cosets of the form  $hK, h \in H$ . However,  $h_1K = h_2K$  for  $h_1, h_2 \in H$  if and only if  $h_2^{-1}h_1 \in K$  and thus

$$h_1K = h_2K \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K)$$

Thus, the number of distinct cosets of the form  $hK$ , for  $h \in H$ , is the number of distinct cosets  $h(H \cap K)$ , for  $h \in H$ . The latter number, by Lagrange's Theorem, is equal to  $\frac{|H|}{|H \cap K|}$  as  $H \cap K \leq H$ . Thus, we have  $\frac{|H|}{|H \cap K|}$  distinct cosets of  $K$ , with each have  $|K|$  elements and so  $|HK| = \frac{|H||K|}{|H \cap K|}$  as desired.  $\heartsuit$

**Proposition 2.2.17.**

1.  $H \leq N_G(K)$  then  $HK \leq G$
2. If  $K \trianglelefteq G$  then  $HK \leq G$

*Proof.* 1. If  $H \leq N_G(K)$  then it is a subset of  $N_G(K)$ . Hence, for all  $h \in H$ , we have  $hKh^{-1} = K$  and thus  $hK = Kh$ . This means for all  $k_1 \in K$ , we have  $hk_1 = k_2h$  where  $k_2 \in K$ . Let  $x, y \in HK$  where  $x = h_1k_1$ ,  $y = h_2k_2$ , and  $h_1, h_2 \in H, k_1, k_2 \in K$ . We have

$$\begin{aligned} xy^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1k_1h_2^{-1}k_3 \text{ Since } h_2^{-1}K = Kh_2^{-1} \Rightarrow \exists k_3 \in K (k_2^{-1}h_2^{-1} = h_2^{-1}k_3) \\ &= h_1h_2^{-1}k_4k_3 \text{ As } Kh_2^{-1} = h_2^{-1}K \Rightarrow \exists k_4 \in K (k_1h_2^{-1} = h_2^{-1}k_4) \end{aligned}$$

Thus  $HK$  is indeed a subgroup.

2. Since  $K \trianglelefteq G$ , we have  $gKg^{-1} = K$  for all  $g \in G$ . That is,  $gK = Kg$  for all  $g \in G$ . Let  $x = h_1k_1 \in HK$  and  $y = h_2k_2 \in HK$ . Note  $h_1, h_2 \in G$ . Thus, let  $k_3$  be such that  $h_2k_2^{-1}h_2^{-1} = k_3$  and  $k_4$  be such that  $h_2k_1h_2^{-1} = k_4$ , then  $k_2^{-1}h_2^{-1} = h_2^{-1}k_3$  and  $k_1h_2^{-1} = h_2^{-1}k_4$ , we have

$$\begin{aligned} xy^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1k_1h_2^{-1}k_3 \\ &= h_1h_2^{-1}k_4k_3 \in HK \end{aligned}$$

Therefore,  $HK \leq G$ .  $\heartsuit$

**Example 2.2.18.**

1. We have  $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ .
2. We have  $S_n/A_n = \{\overline{e}, \overline{(1, 2)}\}$
3. Let  $Q/\langle i \rangle$  where  $Q$  is the quaternion group. We have  $\overline{i} = \overline{1}$ ,  $\overline{-1} = \overline{ii} = \overline{ii} = \overline{11} = \overline{1}$ ,  $\overline{ij} = \overline{k} \Rightarrow \overline{j} = \overline{k}$ . If we keep doing this, we obtain  $Q/\langle i \rangle = \{\overline{1}, \overline{j}\}$ .
4. Consider  $GL_2(\mathbb{R})/SL_2(\mathbb{R})$ .

$$\text{We have } \overline{\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}} = \overline{\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}} \cdot \overline{\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}} = \overline{\begin{bmatrix} 1 & 2 \\ 2 & 6 \end{bmatrix}}$$

**Example 2.2.19.** Let  $H \trianglelefteq G$  and  $[G : H] = n < \infty$ , Let  $g \in G$ , we have  $\overline{g} \in G/H$  then  $\overline{g}^n = \overline{e}$  by Lagrange. Indeed, the order of  $\langle \overline{g} \rangle$  must divide  $n$  as  $n = |G/H| = [G : H]$  by Lagrange. Hence, let  $|\overline{g}| = m$ , we have  $mk = n$  and thus  $\overline{g}^n = \overline{g}^{mk} = \overline{e}^k = \overline{e}$ . Thus  $g^n \in H$ .

**Theorem 2.2.20 (Cauchy's Theorem for Abelian Groups).** Let  $G$  be finite and abelian. If  $p$  is a prime, such that  $p|G$ , then  $G$  has an element of order  $p$ .

*Proof.* Let  $p \mid |G|$ , we proceed by induction on  $|G|$ . Namely, we assume the result holds for all groups with size less than  $G$ , then we conclude the claim holds for  $G$ .

If  $|G| = p$  then for all  $e \neq g \in G$ , we have  $G = \langle g \rangle$  and so  $|g| = |G| = p$  and we are done. Hence, we assume  $|G| > p$ .

Assume the result for all groups  $H$  such that  $|H| < |G|$  with  $p \mid |H|$ .

Take  $e \neq x \in G$ , and let  $N = \langle x \rangle$ . If  $G = N$  then we are done. Thus we can assume  $|N| < |G|$ .

Case 1: If  $p \mid |N|$  then there exists  $g \in N$  such that  $|g| = p$  by induction hypothesis.

Case 2: If  $p \nmid |N|$  then  $p \mid |G/N|$ . Since  $G$  is abelian, we have  $N \trianglelefteq G$  and so  $G/N$  is a group with  $|G/N| < |G|$ . By hypothesis,  $G/N$  has an element  $\bar{y} = yN$  such that  $|\bar{y}| = p$  in  $G/N$ . In particular,  $\bar{y} \neq \bar{e}$  as  $yN \neq eN = N$  and  $\bar{y}^p = \bar{e}$ . Thus  $y \notin N$  and  $y^p \in N$ . Let  $m = |y|$ , then  $|y^p| = \frac{m}{\gcd(m,p)} \in \{m/p, m\}$ .

However,  $\langle y^p \rangle \subseteq \langle y \rangle$  where  $\langle y^p \rangle \subseteq N$  and  $\langle y \rangle \not\subseteq N$ . Hence  $\langle y^p \rangle \neq \langle y \rangle$  and in particular  $|y^p| \neq |y| \Rightarrow |y^p| \neq m$ . Thus  $|y^p| = m/p$  which imply  $p \mid m$ . By case 1 with  $N = \langle y \rangle$ , we are done.  $\heartsuit$

**Example 2.2.21.** Let  $G = S_4$  and let  $V = \{e, (12)(34), (13)(24), (14)(23)\}$  and  $H = \{e, (12)(34)\}$ . Then we have  $H \trianglelefteq V \trianglelefteq G$  but  $H \not\trianglelefteq G$ .

**Proposition 2.2.22.** Let  $G$  be a group, let  $N \trianglelefteq G$  and let  $H \leq G$  such that  $N \leq H$ . We have  $N \trianglelefteq H$  and  $H/N \leq G/N$ .

*Proof.* Since  $N \trianglelefteq G$ , thus  $gNg^{-1} = N$  for all  $g \in G$ . Next, since  $N \leq H \leq G$ , we have  $H \subseteq G$ . For all  $h \in H$ , we have  $hNh^{-1} = N$  since  $x \in N$ , thus  $N \trianglelefteq H$ .

Next, let  $\bar{a}, \bar{b} \in H/N$ , since  $H \leq G$ , we have  $ab^{-1} \in H$ . Thus,  $\bar{a} \cdot \bar{b}^{-1} \in H/N$ . Thus  $H/N \leq G/N$ .  $\heartsuit$

**Theorem 2.2.23 (Correspondence Theorem).** Let  $G$  be a group and let  $N \trianglelefteq G$ . Every subgroup  $\bar{H}$  of  $G/N$  is of the form  $\bar{H} = H/N$ , for some subgroup  $H$  of  $G$  containing  $N$ .

*Proof.* Let  $\bar{H}$  be a subgroup of  $G/N$  (thus it is not empty). We define  $H := \{x \in G : \bar{x} = xN \in \bar{H}\}$ . Note we must have  $\bar{e} \in \bar{H}$  as it is a subgroup. Thus we claim  $N \subseteq H$ , as for every  $x \in N$ , we have  $\bar{x} = \bar{e} \Rightarrow \bar{x} \in \bar{H} \Rightarrow x \in H$ . Note this also ensure that  $H$  is not empty as  $e \in H$ .

Next, we note  $H \subseteq G$  and we claim  $H$  is a subgroup of  $G$ . To see this, let  $x, y \in H$ , we have  $x^{-1}y \in G$ . In addition, we have  $\bar{x} \in \bar{H}$  and  $\bar{y} \in \bar{H}$ . Since  $\bar{H}$  is a group, we have  $\bar{x}^{-1} = \overline{x^{-1}} \in \bar{H}$  and  $\bar{y}$  times anything in  $\bar{H}$  be still in  $\bar{H}$ . In particular, we have  $\bar{x}^{-1}\bar{y} = \overline{x^{-1}y} \in \bar{H}$  and hence  $x^{-1}y \in H$ . By construction, we have  $\bar{H} = H/N \leq G/N$ . Moreover, if  $g \in N$ , then  $\bar{g} \in \bar{H}$  so  $g \in H$  and hence  $N \subseteq H$ .

♡

**Corollary 2.2.23.1 (Normal Correspondence Theorem).** *Let  $G$  be a group and let  $N \trianglelefteq G$ . Every normal subgroup  $\overline{H}$  of  $G/N$  is of the form  $\overline{H} = H/N$ , for some  $H \trianglelefteq G$  containing  $N$ .*

*Proof.* Let  $\overline{H} \trianglelefteq G/N$ . Then, we have  $\overline{x} \cdot \overline{H} \cdot \overline{x}^{-1} = \overline{H}$ . Let  $H =: \{x \in G : \overline{x} \in \overline{H}\}$ . Then from the proof of the correspondence theorem, we see that  $\overline{H} = H/N$  and  $N \subseteq H$  since  $N \trianglelefteq G$  and  $\overline{H} \leq G/N$ . Hence, it suffice to show  $H$  is normal in  $G$ .

Let  $g \in G$ , then we have  $gHg^{-1} = \{ghg : h \in H\}$ . It suffice to show  $ghg^{-1} \in H$  for arbitrary  $h \in H$  as this imply  $gHg^{-1} \subseteq H$  and hence  $gHg^{-1} = H$ . Note  $\overline{ghg^{-1}} = \overline{g} \cdot \overline{h} \cdot \overline{g}^{-1}$  where  $\overline{h} \in \overline{H}$  and thus  $\overline{g} \cdot \overline{h} \cdot \overline{g}^{-1} \in \overline{H}$ . Hence  $ghg^{-1} \in H$  by the definition of  $H$ . ♡

**Definition 2.2.24.** Let  $a, b \in G$ , the **commutator** of  $a$  and  $b$  is defined to be the element  $[a, b] := aba^{-1}b^{-1}$ . The **commutator subgroup**  $[G, G]$  of  $G$  is the subgroup generated by all the commutators of  $G$ , that is,  $[G, G] = \langle [a, b] : a, b \in G \rangle$

**Proposition 2.2.25.**  $[G, G]$  is the smallest subgroup  $H$  of  $G$  such that  $G/H$  is abelian.

*Proof.* Let  $N := [G, G]$ .

We first show  $G/N$  is abelian. Let  $\overline{x}, \overline{y} \in G/N$ , then  $xyx^{-1}y^{-1} \in [G, G]$  and so  $\overline{xyx^{-1}y^{-1}} = \overline{e}$ . Hence  $\overline{xy} = \overline{yx}$ .

Next, we show if  $H \trianglelefteq G$  and  $G/H$  is abelian then  $N \subseteq H$ . Let  $x, y \in G$  so that  $xyx^{-1}y^{-1} \in N$ . Since  $G/H$  is abelian, we have  $\overline{xyx^{-1}y^{-1}} = \overline{e}$  and so  $xyx^{-1}y^{-1} \in H$ . Therefore, by minimality of groups generated by sets, we have  $N \subseteq H$  as required.

♡

# Chapter 3

## Group Homomorphism

### 3.1 Homomorphism

**Definition 3.1.1.** Let  $A, B$  be groups. A function  $\phi : A \rightarrow B$  is a **homomorphism** if for all  $x, y \in A$ , we have  $\phi(xy) = \phi(x)\phi(y)$ .

In addition, injective homomorphism from  $A$  to  $B$  is called an **embedding of  $A$  into  $B$** . Bijective homomorphism is called **isomorphism**. Moreover, if there exists an isomorphism between  $A$  and  $B$ , we say  $A$  and  $B$  is **isomorphic** and write  $A \cong B$ .

**Example 3.1.2.**

1. Let  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$  and  $\phi(a) = [a]$ . Then  $\phi(a+b) = [a+b] = [a] + [b] = \phi(a) + \phi(b)$ .
2. Let  $\phi : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$  and  $\phi(A) = \det(A)$ , we have  $\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$ .
3. Let  $\phi : (M_2(\mathbb{R}), +) \rightarrow \mathbb{R}$ . Then  $\phi(A) = \det(A)$  is not a homomorphism.  $\phi(A) = \text{tr}(A)$  is a homomorphism as we have  $\phi(A+B) = \text{tr}(A+B) = \text{tr}(A) + \text{tr}(B)$ .
4. Let  $\phi : S_n \rightarrow C_2$  where  $C_2 = (\{1, -1\}, \cdot)$ . Then  $\phi(\sigma) = \text{sgn}(\sigma)$  is a homomorphism by assignment two.
5. Let  $\phi : \mathbb{R}^\times \times \mathbb{R}^\times \rightarrow GL_2(\mathbb{R})$  where  $\phi(a, b) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$  is an embedding.
6. Let  $D := \{\text{diag}(a, b) \in M_2(\mathbb{R}) : a, b \neq 0\}$  be a group with matrix multiplication. Then  $\phi : \mathbb{R}^\times \times \mathbb{R}^\times \rightarrow D$  where  $\phi(a, b) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$  is an isomorphism.
7. Let  $\phi : \mathbb{Z}_2 \rightarrow C_2$  be  $\phi(0) = 1$  and  $\phi(1) = 0$ . We have  $\phi$  is an isomorphism.
8. Let  $V$  be  $n$  dimensional vector space over  $\mathbb{R}$  and let  $GL(V) := \{T : V \rightarrow V : T \text{ is invertible+linear}\}$  with composition as the operation. We have  $GL(V) \cong GL_n(\mathbb{R})$ . Indeed, let  $\phi : GL(V) \rightarrow GL_n(\mathbb{R})$  be  $\phi(T) = [T]_\beta$  where  $\beta$  is a fixed basis for  $V$ . Thus, for  $T, W \in GL(V)$ , we have  $\phi(T \circ W) = [T \circ W]_\beta = [T]_\beta[W]_\beta$ , thus  $\phi$  is homomorphism.

Next, we need to show it is an isomorphism. To show it is surjective, let  $A \in GL_n(\mathbb{R})$ , consider  $T : V \rightarrow V$  where  $T(v) := A[v]_\beta$ . Thus,  $\phi(T) = A$  and hence it is surjective. To show it is injective, let  $T, W \in GL(V)$  then

- $\phi(T) = \phi(W)$  imply  $[T]_\beta = [W]_\beta$  and hence  $[T]_\beta[x]_\beta = [W]_\beta[x]_\beta$  for all  $x \in V$ . Therefore,  $T(x) = W(x)$  for all  $x \in V$ . Hence it is isomorphism.
9. Let  $A, B$  be cyclic and  $|A| = |B| = n$ , then  $A$  and  $B$  is isomorphic. We have  $\phi(a^l) = b^l$  is an isomorphism (try to check). In particular, we also have  $A \cong B \cong \mathbb{Z}_n$ .
  10. Let  $V$  be a vector space, then  $T : (V, +) \rightarrow (V, +)$  is a homomorphism where  $T$  is linear.

**Definition 3.1.3.** Let  $\phi : A \rightarrow B$  be homomorphism,  $E \leq A$  and  $F \leq B$ . Then we have  $\phi(E) = \{\phi(x) : x \in E\}$  is the **the image of  $E$  under  $\phi$** . We have  $\phi^{-1}(F) = \{x \in A : \phi(x) \in F\} \leq A$  is the **pre-image of  $F$  under  $\phi$** . In addition, the **kernal** of  $\phi$  is  $Ker(\phi) = \{x \in A : \phi(x) = e_B\}$ .

**Proposition 3.1.4.** Let  $\phi : A \rightarrow B$  be homomorphism, then

1.  $\phi(e_A) = e_B$
2.  $\forall g \in A, \phi(g)^{-1} = \phi(g^{-1})$
3.  $H \leq A$ , then  $\phi(H) \leq B$ .
4.  $H \leq B$ , then  $\phi^{-1}(H) \leq A$ .
5.  $Ker(\phi) \trianglelefteq A$
6.  $\phi$  is an embedding iff  $Ker(\phi) = \{e_B\}$

*Proof.*

1.  $e_B = \phi(e_A)^{-1}\phi(e_A) = \phi(e_A)^{-1}\phi(e_A e_A) = \phi(e_A)^{-1}\phi(e_A)\phi(e_A) = \phi(e_A)$
2.  $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = e = \phi(g^{-1}g) = \phi(g^{-1})\phi(g)$
3. It suffice to show  $x, y \in \phi(H) \Rightarrow x^{-1}y \in \phi(H)$  as  $e_B \in \phi(H)$  so it is not empty. Note  $x, y \in \phi(H)$  so  $x = \phi(x')$  and  $y = \phi(y')$  where  $x', y' \in H$ . Thus, we have  $x^{-1} = \phi(x')^{-1} = \phi(x'^{-1})$  and so  $x^{-1}y = \phi(x'^{-1})\phi(y') = \phi(x'^{-1}y') \in \phi(H)$  as  $x', y' \in H$  and  $H$  is a subgroup.
4. It suffice to show  $x, y \in \phi^{-1}(H) \Rightarrow x^{-1}y \in \phi^{-1}(H)$  as  $\phi^{-1}(H)$  is not empty.  $x, y \in \phi^{-1}(H)$  imply  $x = \phi^{-1}(x')$  and  $y = \phi^{-1}(y')$  where  $x', y' \in H$ . Thus,  $x^{-1}y = \phi^{-1}(x'^{-1}y')$  and so  $x^{-1}y \in \phi^{-1}(H)$  as  $x'^{-1}y' \in H$ .
5. We first show  $Ker(\phi) \leq A$ . Let  $x, y \in Ker(\phi)$  then  $\phi(xy^{-1}) = ee^{-1} = e$  and  $xy^{-1} \in Ker(\phi)$  as desired. Next, let  $g \in A$  and  $h \in Ker(\phi)$ . Then  $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = e$ . Thus for all  $g \in A$ , we have  $gKer(\phi)g^{-1} \subseteq Ker(\phi)$  Hence  $Ker(\phi) \trianglelefteq A$ .
6. If  $\phi$  is an embedding. Let  $x \in Ker(\phi)$ , then we have  $\phi(x) = e = \phi(e)$ , thus  $x = e$ .

Suppose conversely, suppose  $Ker(\phi) = \{e\}$ . Then

$$\phi(x) = \phi(y) \Rightarrow \phi(x)\phi(y)^{-1} = e \Rightarrow \phi(xy^{-1}) = e \Rightarrow xy^{-1} = e \Rightarrow x = y$$

♡

**Remark 3.1.5.** Let  $\phi : A \rightarrow B$  be an embedding. Then  $A \cong \phi(A) \leq B$ . In addition,  $\phi : A \rightarrow B$  be an isomorphism, then we say  **$A$  is the same group as  $B$  up to isomorphism**

**Example 3.1.6.** Let  $\phi : A \rightarrow B$  be an embedding, then  $a^n = e$  if and only if  $\phi(a^n) = e$  if and only if  $|\phi(a)| = |\phi(a)|$ .



**Example 3.1.7.** Why are the following *not* isomorphic?

1.  $\mathbb{Z}$  and  $\mathbb{Z} \times \mathbb{Z}$
2.  $\mathbb{R}^\times$  and  $(0, \infty)$
3.  $\mathbb{R}^\times$  and  $\mathbb{C}^\times$

*Solution.*

1.  $\mathbb{Z} \times \mathbb{Z}$  is not cyclic (may be in the midterm) while  $\mathbb{Z}$  is cyclic.
2.  $-1 \in \mathbb{R}^\times$  has order 2, but no elements in  $(0, \infty)$  has order 2.
3.  $|i| = 4$ , but no elements in  $\mathbb{R}^\times$  has order 4.



## 3.2 First Isomorphism Theorem

**Example 3.2.1.**

1. Show there does not exist an embedding  $\phi : GL_2(\mathbb{R}) \rightarrow \mathbb{R}^\times$
2. Show  $\phi : \mathbb{Z}_3 \rightarrow \mathbb{Z}_6, \phi(a) = a$  is not a homomorphism
3. Show  $(\mathbb{R}, +) \cong (\mathbb{C}, +)$
4. Give an example of a group  $G$  with  $H < G$  ( $H \leq G$  and  $H \neq G$ ) such that  $H \cong G$

*Solution.*

1. Otherwise we will have  $GL_2(\mathbb{R}) \cong H \leq \mathbb{R}^\times$  where  $H$  is abelian and  $GL_2(\mathbb{R})$  is not.
2.  $\phi(1) = 1$  and  $\phi(4) = 4$  where  $1 \neq 4$  in  $\mathbb{Z}_6$ . Thus it is not well-defined.
3. We have  $\dim_{\mathbb{Q}}(\mathbb{R}) = \dim_{\mathbb{Q}}(\mathbb{C}) = 2^{\aleph}$ , thus  $\mathbb{R}$  and  $\mathbb{C}$  are isomorphic as vector spaces, and hence they are isomorphic as groups.
4. Take  $G = \prod_{i=1}^{\infty} \mathbb{Z} = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \dots$ , let  $H = \{0\} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \dots$ . Then we have  $H \cong G$  as we have  $\{e\} \times G \cong G$ .



**Example 3.2.2.**

1. Let  $G = D_8$ , and let  $H_1 = \langle r^2 \rangle, H_2 = \langle s \rangle$ . Note  $|H_1| = |H_2| = 2$ , thus  $H_1 \cong H_2$  as they are cyclic. Let's consider  $G/H_1 = \{\bar{e}, \bar{r}, \bar{s}, \bar{r}\bar{s}\}$ . Note  $\{\bar{r}, \bar{s}, \bar{r}\bar{s}\}$  are all order of 2. Next, we have  $G/H_2 = \{\bar{e}, \bar{r}, \bar{r}^2, \bar{r}^3\}$ , and notice  $\bar{r}$  has order 4. Thus, even  $H_1 \cong H_2$ , we still have  $G/H_1 \not\cong G/H_2$ .
2. Let  $G = \prod_{i=1}^{\infty} \mathbb{Z}$ , then we have  $H_1 = \mathbb{Z} \times \{0\} \times \{0\} \times \{0\} \dots$  and  $H_2 = \mathbb{Z} \times \mathbb{Z} \times \{0\} \times \{0\} \times \dots$ . However, we have  $G/H_1 \cong G \cong G/H_2$  and  $H_1 \not\cong H_2$ .

**Proposition 3.2.3.** Let  $G$  and  $H$  be groups and let  $N \trianglelefteq G$ . Suppose  $\phi : G \rightarrow H$  is homomorphism. Then  $\bar{\phi} : G/N \rightarrow H$  defined by  $\bar{\phi}(\bar{g}) = \phi(g)$  is well-defined homomorphism if and only if  $N \subseteq \text{Ker}\phi$ .

*Proof.* Suppose  $\bar{\phi} : G/N \rightarrow H$  defined by  $\bar{\phi}(\bar{g}) = \bar{\phi}(gN) = \phi(g)$  is well-defined. Then we have  $xN, yN \in G/N$  and  $xN = yN$  imply  $\bar{\phi}(xN) = \bar{\phi}(yN)$  and  $x^{-1}y \in N$ . Note  $\bar{\phi}(xN) = \phi(x)$  and  $\bar{\phi}(yN) = \phi(y)$ . Thus  $xN = yN$  imply  $\phi(x) = \phi(y)$ . Note  $\phi$  is homomorphism, thus  $\phi(x) = \phi(y) \Rightarrow \phi(x^{-1}y) = e_H \Rightarrow x^{-1}y \in \text{Ker}(\phi)$ . Hence  $N \subseteq \text{Ker}(\phi)$  as  $xN = yN \iff x^{-1}y \in N$  and we have  $xN = yN \Rightarrow \phi(x^{-1}y) = e_H$ .

Suppose, conversely that  $N \subseteq \text{Ker}(\phi)$ . Then, we need to show  $\bar{\phi}$  is well-defined, and it is homomorphism.

Let  $xN, yN \in G/N$  with  $xN = yN$  then  $x^{-1}y \in N$  and so  $\phi(x^{-1}y) = e_H \Rightarrow \phi(x) = \phi(y)$  where  $\bar{\phi}(xN) = \phi(x)$  and  $\bar{\phi}(yN) = \phi(y)$ . Hence  $\bar{\phi}(xN) = \bar{\phi}(yN)$  and it is indeed well-defined.

To show it is a homomorphism, let  $xN, yN \in G/N$ , then  $\bar{\phi}((xN)(yN)) = \bar{\phi}(xyN) = \phi(xy) = \phi(x)\phi(y) = \bar{\phi}(xN)\bar{\phi}(yN)$ . ♡

**Proposition 3.2.4.** *Let  $G$  be a group. Then  $H \trianglelefteq G$  if and only if  $\exists \phi : G \rightarrow G'$  such that  $H = \text{Ker}(\phi)$  where  $G'$  is arbitrary groups.*

*Proof.* ( $\Leftarrow$ ) Done by Proposition 3.1.4.

( $\Rightarrow$ ) Suppose  $H \trianglelefteq G$ . Consider the quotient homomorphism:  $q : G \rightarrow G/H$  where  $q(g) = \bar{g}$ . Note  $q(ab) = \overline{ab} = \bar{a}\bar{b} = q(a)q(b)$ . Moreover, we see that

$$g \in \text{Ker}(q) \iff q(g) = \bar{e} \iff \bar{g} = \bar{e} \iff g \in H$$

Thus we are finished. ♡

**Theorem 3.2.5 (First Isomorphism Theorem).** *Let  $\phi : G \rightarrow G'$  be homomorphism. Then  $G/\text{Ker}(\phi) \cong \phi(G)$  via the isomorphism  $\bar{g} \mapsto \phi(g)$ .*

*Proof.* Consider  $\psi : G/\text{Ker}(\phi) \rightarrow \phi(G)$  given by  $\psi(\bar{g}) = \phi(g)$ .

We first show it is well-defined. Suppose  $\bar{a} = \bar{b}$  in  $G/\text{Ker}(\phi)$ . Thus,

$$\begin{aligned} \overline{b^{-1}a} &= \bar{e} \\ \Rightarrow b^{-1}a &\in \text{Ker}(\phi) \\ \Rightarrow \phi(b^{-1}a) &= e \\ \Rightarrow \phi(b)^{-1}\phi(a) &= e \\ \Rightarrow \phi(a) &= \phi(b) \\ \Rightarrow \psi(\bar{a}) &= \psi(\bar{b}) \end{aligned}$$

We then check it is an homomorphism. Let  $\bar{a}, \bar{b} \in G/\text{Ker}(\phi)$ . Then  $\psi(\bar{a}\bar{b}) = \psi(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \psi(\bar{a})\psi(\bar{b})$ .

Next, by construction, we note  $\psi$  is surjective.

Then, we show it is injective. Let  $\bar{a} \in \text{Ker}(\psi)$ . Then,

$$\begin{aligned}\psi(\bar{a}) &= e \\ \Rightarrow \phi(a) &= e \\ \Rightarrow a &\in \text{Ker}(\phi) \\ \Rightarrow \bar{a} &= \bar{e}\end{aligned}$$

Thus  $\text{Ker}(\psi) = \{\bar{e}\}$  and so  $\psi$  is injective. ♡

**Remark 3.2.6.** If  $\phi$  is surjective, then  $G/\text{Ker}(\phi) \cong \phi(G) = G'$

**Example 3.2.7.**  $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$ . Consider  $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ . We know it is surjective homomorphism with  $\text{Ker}(\det) = SL_n(\mathbb{R})$ , and by the first isomorphism theorem, we have

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$$

**Example 3.2.8.** Consider  $S_n/A_n$ . Recall that  $\sigma A_n = \tau A_n \iff \tau^{-1}\sigma \in A_n \iff \text{sgn}(\sigma) = \text{sgn}(\tau)$ . Thus, we claim  $S_n/A_n \cong C_2 = \{-1, 1\}$ . Consider  $\text{sgn} : S_n \rightarrow C_2$ , we learned that  $\text{sgn}$  is a surjective homomorphism. Next, recall  $\text{Ker}(\text{sgn}) = A_n$ , thus we indeed have  $S_n/A_n \cong C_2$  by First Isomorphism Theorem.

**Example 3.2.9.** Let  $G = \mathbb{C}[x]$ .

1. Let  $H = \{f(x) \in G : f(0) = 0\}$ , show  $\mathbb{C}[x]/H \cong \mathbb{C}$ .
2. Let  $K = \{f(x) \in G : f(1) = f(0) = 0\}$ , show  $\mathbb{C}[x]/K \cong \mathbb{C}^2$ .

*Solution.* 1. Let  $G = \mathbb{C}[x]$ , let  $H = \{f(x) \in G : f(0) = 0\}$ . We claim  $G/H \cong \mathbb{C}$ . Note  $f(x) + H = g(x) + H \iff f(x) - g(x) \in H \iff f(0) - g(0) = 0 \iff f(0) = g(0)$ . Thus, let  $\phi : G \rightarrow \mathbb{C}$  be  $\phi(f(x)) = f(0)$ , then indeed we have  $\phi$  is surjective homomorphism. Next, we have  $\text{Ker}(\phi) = H$  and hence we have  $G/H \cong \mathbb{C}$  by First Isomorphism Theorem.

2. Define  $\phi : \mathbb{C}[x] \rightarrow \mathbb{C}^2$  to be  $\phi(f(x)) = (f(0), f(1))$ . We first note  $\text{Ker}(\phi) = K$ . Next, let  $f(x), g(x) \in \mathbb{C}[x]$ , then we have

$$\begin{aligned}\phi(f(x) + g(x)) &= ((f + g)(0), (f + g)(1)) = (f(0) + g(0), f(1) + g(1)) \\ &= (f(0), f(1)) + (g(0), g(1)) = \phi(f(x)) + \phi(g(x))\end{aligned}$$

Hence  $\phi$  is homomorphism. Let  $(a, b) \in \mathbb{C}^2$  be given, then  $f(x) = (b - a)x + a$  imply  $\phi(f(x)) = (a, b)$ . Thus it is surjective. Hence by first isomorphism theorem we have  $\mathbb{C}[x]/\text{Ker}(\phi) = \mathbb{C}[x]/K \cong \phi(\mathbb{C}[x]) = \mathbb{C}^2$



**Example 3.2.10.** Let  $G := \mathbb{R}$  and  $H := \mathbb{Z}$ . Then, consider  $G/H$ , we have  $a + H = b + H \iff a - b \in \mathbb{Z}$ . We claim that  $\mathbb{R}/\mathbb{Z} \cong S^1$ , where  $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ . Let  $\phi : \mathbb{R}/\mathbb{Z} \rightarrow S^1$  where  $\phi(\bar{t}) = e^{2\pi \cdot i \cdot t}$ , then we would have an isomorphism.

**Example 3.2.11.** Show the following are not isomorphic:

1.  $Q$  and  $D_8$

2.  $\mathbb{Z}_2 \times \mathbb{Z}_6$  and  $\mathbb{Z}_{12}$
3.  $S_4$  and  $D_8 \times \mathbb{Z}_3$
4.  $(\mathbb{Q}, +)$  and  $(\mathbb{Q}^\times, \cdot)$

*Solution.* 1. Note we have four elements of order 2 in  $D_8$ , namely  $sr, sr^2, sr^3, s$ . However, in  $Q$ , we have  $|i| = |j| = |k| = |-k| = 4$  and  $|1| = 1$ . Thus  $Q$  cannot have four elements with order 2 as it already have five elements with order not equal to 2.

2. Note  $\mathbb{Z}_{12}$  is cyclic and  $\mathbb{Z}_2 \times \mathbb{Z}_6$  is not as we showed in class.
3. Note all elements in  $S_4$  have order at most 4. Indeed, note we have  $|\sigma_1, \dots, \sigma_l| = \text{lcm}(|\sigma_1|, \dots, |\sigma_k|)$  and  $|\sigma_i| \in \{1, 2, 3, 4\}$ , where  $\sigma_i$  are all disjoint and  $1 \leq i \leq k$ . Note this means we must have  $\sum_{i=1}^k |\sigma_i| = 4$ . Then, we enumerate the interger partitions of 4, and get  $\{1, 1, 1, 1\}, \{1, 1, 2\}, \{2, 2\}, \{1, 3\}, \{4\}$  and we see the maximum for  $\text{lcm}(|\sigma_1|, \dots, |\sigma_k|)$  must be 4.

Then, note  $(1, r) \in D_8 \times \mathbb{Z}_3$ , we have  $|(1, r)| = 12$ . Therefore, they cannot be isomorphic.

4. Suppose the two groups are isomorphic. Then there exists isomorphism  $\phi : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}^\times, \cdot)$ . Hence, there exists  $x \in \mathbb{Q}$  so that  $-1 = \phi(x)$  as  $-1 \in \mathbb{Q}^\times$ . Note

$$\begin{aligned} -1 = \phi(x) &= \phi\left(\frac{x}{2} + \frac{x}{2}\right) = \left(\phi\left(\frac{x}{2}\right)\right)^2 \\ \Rightarrow \phi\left(\frac{x}{2}\right) &\in \mathbb{Q}^\times \text{ and } \phi\left(\frac{x}{2}\right)^2 = -1 \Rightarrow \phi\left(\frac{x}{2}\right) = i \notin \mathbb{Q}^\times \end{aligned}$$

This is impossible so there cannot be any isomorphisms.



**Example 3.2.12.** Find an isomorphic non-quotient group for the following quotient groups:

1.  $M_n(\mathbb{R})/T$  where  $T = \{A \in M_n(\mathbb{R}) : \text{Tr}(A) = 0\}$
2.  $\mathbb{R}^\times/P$  where  $P = (0, \infty)$

*Solution.* 1. Note we must be working with matrix addition, for if  $T$  is a group under matrix multiplication, then in particular,  $T$  would not be a group when

$$n = 2 \text{ and } A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in T, \text{ for } A^2 = I \notin T.$$

Thus, define  $\phi : M_n(\mathbb{R}) \rightarrow (\mathbb{R}, +)$  to be  $\phi(A) = \text{tr}(A)$ . We have  $\phi(A + B) = \phi(A) + \phi(B)$  and  $\text{Ker}(\phi) = T$ . Next, note  $\phi$  is surjective because for  $x \in \mathbb{R}$ , we have  $A_x = \text{diag}(x, 0, 0, \dots, 0) \in M_n(\mathbb{R})$  so that  $\phi(A_x) = x$ . Hence, we have  $M_n(\mathbb{R})/T \cong (\mathbb{R}, +)$  by first isomorphism theorem.

2. Note  $0 \notin \mathbb{R}^\times$ . Define  $\phi : \mathbb{R}^\times \rightarrow (\{-1, 1\}, \cdot) = (C_2, \cdot)$  to be  $\phi(x) = \frac{x}{|x|}$  where  $|x|$  is the absolute value function. Then, we have  $\phi(x) = 1$  if  $x > 0$  and  $\phi(x) = -1$  if  $x < 0$ . Let  $x, y \in \mathbb{R}^\times$  be given, then

$$\phi(xy) = \frac{xy}{|xy|} = \frac{xy}{|x||y|} = \frac{x}{|x|} \frac{y}{|y|} = \phi(x)\phi(y)$$

Thus  $\phi$  is homomorphism, and we note  $\text{Ker}(\phi) = P$  as  $x \in P \Rightarrow \phi(x) = 1$  is the identity in  $C_2$ . Next, let  $x \in C_2$  be given, we have  $\phi(1) = 1$  and  $\phi(-1) = -1$ , thus  $\phi$  is indeed a surjection and hence by first isomorphism theorem, we have  $\mathbb{R}^\times/P \cong (C_2, \cdot)$ .



**Example 3.2.13.** Find all homomorphisms  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ .

*Solution.* We first show that  $\phi$  is a homomorphism then  $\phi(x) = ax$  for some  $x \in \mathbb{Z}_m$ . Indeed, if  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$  is a homomorphism, then  $\phi(x + y) = \phi(x) + \phi(y)$ . In particular, we have  $\phi(x) = \phi(\sum_{i=1}^x 1) = \sum_{i=1}^x \phi(1) = x \cdot \phi(1)$ . Note  $\phi(1) \in \mathbb{Z}_m$  is fixed, so we have  $\phi(x) = ax$  where  $a = \phi(1) \in \mathbb{Z}_m$ .

Next, we show that  $\phi$  given by  $\phi(x) = ax$  is a homomorphism if and only if  $na \equiv 0 \pmod{m}$ .

If  $\phi(x) = ax$  is homomorphism, then we note  $\phi(n) = n\phi(1) = na$  where  $n = 0 \in \mathbb{Z}_n$  thus  $\phi(n) = 0 \in \mathbb{Z}_m$ . Hence  $na \equiv 0 \pmod{m}$  as  $na = 0 \in \mathbb{Z}_m$ .

Conversely, say  $na \equiv 0 \pmod{m}$ . Then define  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$  and  $\phi(x) = ax$ . We will show this is a homomorphism.

Let  $x, y \in \mathbb{Z}_n$ . Then, we must have  $k_1, k_2, k_3 \in \mathbb{Z}_{\geq 0} := \{z \in \mathbb{Z} : z \geq 0\}$  and  $r_1, r_2, r_3 \in \mathbb{Z}_{\geq 0}$  with  $r_1 < n$  and  $r_2, r_3 < m$  so that  $x+y = k_1n+r_1$ ,  $x = k_2m+r_2$ , and  $y = k_3m+r_3$ . Then, note  $x+y \in \mathbb{Z}_n$  is equal to  $r_1$ ,  $x \in \mathbb{Z}_m$  is equal to  $r_2$ , and  $y \in \mathbb{Z}_m$  is equal to  $r_3$ . Hence, we have  $\phi(x+y) \equiv ar_1 \pmod{m}$  and  $\phi(x) + \phi(y) \equiv ar_2 + ar_3 \pmod{m}$ . Next, note  $a(x+y) = k_1an + ar_1$ ,  $ax + ay = k_2am + ar_2 + k_3am + ar_3$  and we have

$$k_1an + ar_1 \equiv k_1(0) + ar_1 \equiv ar_1 \pmod{m}$$

and

$$k_2am + ar_2 + k_3am + ar_3 \equiv ar_2 + ar_3 \pmod{m}$$

Thus we indeed have  $ar_1 \equiv ar_2 + ar_3 \pmod{m}$  and hence  $\phi(x+y) = \phi(x) + \phi(y)$  as desired.

Then, we are looking for all  $a$  such that  $na \equiv 0 \pmod{m}$ .

Recall that, let  $d = \gcd(n, m)$ , then if  $u$  is a solution to  $nx \equiv 0 \pmod{m}$ , then the general set of solution is  $\{u + \frac{mk}{d} \in \mathbb{Z}_m : k = \{0, 1, \dots, d-1\}\}$ . Hence, we note  $n \cdot 0 \equiv 0 \pmod{m}$ , and thus  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$  with  $\phi(x) = ax$  is a homomorphism if and only if  $a = \frac{mk}{d}$  where  $k \in \mathbb{Z}_d$  and  $d = \gcd(n, m)$ . ♠

**Example 3.2.14.** Find all homomorphisms  $\phi : \mathbb{Z}_{20} \rightarrow \mathbb{Z}_{12}$ .

*Solution.* By the above example, we note  $d = \gcd(20, 12) = 4$ . Thus the solution set is  $\{0, 3, 6, 9\}$ .

Thus  $\phi_1(x) = 0x$ ,  $\phi_2(x) = 3x$ ,  $\phi_3(x) = 6x$  and  $\phi_4(x) = 9x$  are all the homomorphisms. ♠

**Proposition 3.2.15 (Second Isomorphism Theorem).** *Let  $G$  be a group and let  $A$  and  $B$  be subgroups of  $G$  such that  $A \leq N_G(B)$ . Then  $B \trianglelefteq AB$ ,  $A \cap B \trianglelefteq A$  and  $AB/B \cong A/(A \cap B)$*

*Proof.* Recall that  $N_G(B) = \{g \in G : gBg^{-1} = B\}$ . In addition, recall  $AB = \{ab \in G : a \in A, b \in B\}$ .

We first show that  $B \trianglelefteq AB$ . Clearly  $B \leq AB$ . Let  $ab \in AB$ , where  $a \in A$  and  $b \in B$ . For any  $x \in B$ , we have  $(ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} \in B$  as  $A \subseteq N_G(B)$ . Thus  $B \trianglelefteq AB$ .

Next, we show  $A \cap B \trianglelefteq A$ . Clearly  $A \cap B \leq A$ . Now, for  $x \in A \cap B$  and  $g \in A$ , we have  $gxg^{-1} \in A$  and  $gxg^{-1} \in B$  since  $A \subseteq N_G(B)$ . Thus,  $gxg^{-1} \in A \cap B$  as required.

Next, let  $\phi : A \rightarrow AB/B$  to be  $\phi(x) = xB$ , we have  $\phi(x) = xB$  where  $x \in A$ . Note  $x \in AB \iff x = ab, a \in A, b \in B$  and thus  $xB = abB = aB$ . Next, we have  $\text{Ker}(\phi) = A \cap B$ , this is because  $xB = B \iff x \in B$ , and hence all elements in the intersection of  $A$  and  $B$  must be in the kernel of  $\phi$ . Now we claim  $\phi$  is surjective homomorphism. Note this map is well-defined by coset properties. Let  $x, y \in A$ , then  $\phi(xy) = xyB = (xB)(yB) = \phi(x)\phi(y)$ . Thus it is homomorphism. Next, let  $xB \in AB/B$ , we have  $x \in AB$ , thus  $x = ab$  where  $a \in A, b \in B$  and hence  $xB = abB = aB$  and we have  $\phi(a) = xB$  as desired.

Thus by first isomorphism theorem, we have  $A/\text{Ker}(\phi) = A/(A \cap B) \cong AB/B \quad \heartsuit$

**Proposition 3.2.16 (Third Isomorphism Theorem).** *Let  $G$  be a group and let  $A$  and  $B$  be normal subgroups with  $A \leq B$ . Then  $B/A \trianglelefteq G/A$  and  $(G/A)/(B/A) \cong G/B$*

*Proof.* Recall  $A, B \trianglelefteq G$  then  $gAg^{-1} = A$  and  $gBg^{-1} = B$  for all  $g \in G$ . We first show  $B/A \trianglelefteq G/A$ . This follows from the Correspondence Theorem 2.2.23.

Next, we show  $(G/A)/(B/A) \cong G/B$ . Let  $\phi : G/A \rightarrow G/B$  be  $\phi(gA) = gB$ . We first note  $\phi(gA) = B$  if and only if  $g \in B$  and thus  $B/A = \{bA : b \in B\}$  is the kernel of  $\phi$ . It is easy to see this map is well-defined by coset properties. Next, note  $\phi(xAyA) = \phi(xyA) = xyB = xByB = \phi(xA)\phi(yA)$  and hence it is homomorphism. Let  $gB \in G/B$  be given, then  $\phi(gA) = gB$  so it is surjective. Hence by first isomorphism theorem, we have  $(G/A)/\text{Ker}(\phi) = (G/A)/(B/A) \cong G/B. \quad \heartsuit$

**Definition 3.2.17.** An isomorphism  $\phi : G \rightarrow G$  is called **automorphism**. We write the collection of all automorphisms of  $G$  to be  $\text{Aut}(G)$ .

In addition, for fixed  $g \in G$ , we have  $\phi_g : G \rightarrow G$ , where  $\phi_g(x) = gxg^{-1}$ , is an automorphism. We call this **conjugation by  $g$** . We write the collection of all conjugations to be  $\text{Inn}(G) = \{\phi_g : g \in G\}$ , and say it is the **inner automorphism**.

**Remark 3.2.18.** The collections of all automorphisms of  $G$ ,  $\text{Aut}(G)$ , is a group under composition.

$\text{Inn}(G)$  is a subgroup of  $\text{Aut}(G)$ . Moreover, we have  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ .

**Example 3.2.19.** We have  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ . Indeed, let  $f \in \text{Aut}(G)$  and  $\phi_g \in \text{Inn}(G)$ . Then,  $\forall x \in G$ , we have

$$\begin{aligned} f \circ \phi_g \circ f^{-1}(x) &= f(g(f^{-1}(x))g^{-1}) \\ &= f(g)xf(g)^{-1} = \phi_{f(g)}(x) \in \text{Inn}(G) \end{aligned}$$

Thus, we must have  $\forall f \in \text{Aut}(G)$ , that  $f(\text{Inn}(G))f^{-1} \subseteq \text{Inn}(G)$  and so  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$  as desired.

**Example 3.2.20.**  $G/Z(G) \cong \text{Inn}(G)$ .

*Solution.* Let  $\phi : G \rightarrow \text{Inn}(G)$  be  $\phi(g) = \phi_g$ . For  $g, h \in G$  be arbitrary, for all  $x \in G$ , we have  $(\phi(gh))(x) = \phi_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g\phi_h(x)g^{-1} = g((\phi(h))(x))g^{-1} = (\phi(g) \circ \phi(h))(x)$ . Thus  $\phi(gh) = \phi(g)\phi(h)$  for all  $g, h \in G$ .

For any  $\phi_g \in \text{Inn}(G)$ , we have  $\phi(g) = \phi_g$  and so  $\phi$  is surjective. Finally, let  $g \in \text{Ker}(\phi)$ , then we have  $\phi(g) = \text{id}$ . Thus, for all  $x \in G$ , we have  $\phi_g(x) = \text{id}(x) = x$ . Thus  $gxg^{-1} = x \iff gx = xg$ . Hence,  $g \in Z(G)$  and indeed we have  $\text{Ker}(\phi) = Z(G)$ . Thus, by the first isomorphism theorem, we have  $G/Z(G) \cong \text{Inn}(G)$ . ♠

# Chapter 4

## Group Actions

### 4.1 Intro

**Definition 4.1.1.** Let  $G$  be a group, and  $X$  is a set. A **group action** of  $G$  on  $X$  is a map such that

- It maps  $G \times X \rightarrow X$
- $\forall x \in X, ex = x$
- $\forall g, h \in G$ , we have  $\forall x \in X, (gh)x = g(hx)$

**Definition 4.1.2.** Let  $G$  acts on  $X$ . If  $x \in X$ , we define the **stabilizer** of  $x$  to be  $stab(x) = \{g \in G : gx = x\} \subseteq G$ .

Moreover, we define the **orbit** of  $x$  to be  $orb(x) = \{gx : g \in G\} \subseteq X$ , and call it the **orbit of  $x$** .

**Definition 4.1.3.** Let  $G$  acts on  $X$ .

We say the action is a **faithful** if for all  $e \neq g \in G$ , there exists  $x \in X$  such that  $gx \neq x$ .

We say the action is **transitive** if for all  $x, y \in X$ , there exists  $g \in G$  such that  $gx = y$ .

**Remark 4.1.4.** The motivation of faithful action is because sometimes we want only the identity action to be the identity action, and all other elements of  $G$  at least maps one  $x$  to be something else.

**Example 4.1.5.** Let  $G$  be a group and  $X = G$ . Then a action that  $G$  acts on itself can be defined as  $g \cdot x = gx$ .

Moreover, we can have  $G$  acts on itself by conjugation as define  $g \cdot x = gxg^{-1}$ .

**Remark 4.1.6.** Let  $G$  acts on  $X$ , then if  $x \in X$ , then we have  $stab(x) \leq G$ . Moreover, we also have  $orb(x) \subseteq X$ .

**Definition 4.1.7.** Let  $G$  be a group, the **centralizer** of  $x \in G$  is  $C(x) = \{g \in G : gx = xg\}$ .



**Example 4.1.8.**

1. Let  $G$  acts on  $X = G$  by left multiplication, then we have  $\text{stab}(x) = \{e\}$  and  $\text{orb}(x) = G$ .
2. Let  $G$  acts on  $X = G$  by conjugation, then  $\text{stab}(x) = \{g \in G : gx = xg\} = C(x)$ .
3. Let  $G = S_n$  and  $X = \{1, 2, 3, \dots, n\}$  and  $\sigma \cdot i = \sigma(i)$  is a group action. Moreover, let  $H \leq S_n$ , then  $H$  acts on  $\{1, 2, \dots, n\}$  in the same way.
4. Let  $H = \langle (1, 2) \rangle \leq S_3$ , the action that  $H$  acts on  $X = \{1, 2, 3\}$  is not transitive. Since there does not exists  $\sigma \in H$  such that  $\sigma(1) = 3$ .
5. Let  $G = S_n$  where  $n > 2$  and  $X = \{\Delta, -\Delta\}$ . We define  $\sigma \cdot X = \sigma(X)$ . Then  $\forall \sigma \in A_n, \sigma(\Delta) = \Delta$  and  $\sigma(-\Delta) = -\Delta$ . Thus this action is not faithful.
6. Let  $G = S_n$  and  $|X| = n$  where  $X = \{x_1, x_2, \dots, x_n\}$ , then  $\sigma \cdot x_i = x_{\sigma(i)}$  is a group action.
7. Let  $G = D_{2n}$  and  $X = \{\text{configurations of the labelled n-gon}\}$ , then  $G$  acts on  $X$  by rotation and reflection.
8. Let  $G = GL_n(\mathbb{R})$  and  $X = \mathbb{R}^n$ , then  $A \cdot x = Ax$  is a group action.
9. Let  $G = \text{Aut}(H)$  and  $X = H$ , we can define  $\phi \cdot h = \phi(h)$  where  $\phi \in \text{Aut}(H)$  and  $h \in H$ .
10. Let  $G$  be any group, and  $X = \{H \subseteq G : H \leq G\}$ . We can define the group action by conjugation as  $g \cdot H = gHg^{-1}$ . Fix  $H \in X$ , we have  $\text{stab}(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$ .
11. Let  $G$  be a group and  $H \leq G$ , and  $X = G/H$ . We can define the group action as  $g \cdot (aH) = gaH$  by left multiplication.

**Theorem 4.1.9 (Cayley's Theorem).** *Every finite group  $G$  is isomorphic to a subgroup of  $S_n$  where  $|G| = n$ .*

*Proof.* Say  $G = \{g_1, \dots, g_n\}$  where  $g_i \neq g_j$  for  $i \neq j$ . Take  $g \in G$ , note that  $gg_i = gg_j \iff g_i = g_j \iff i = j$ . Thus,  $(gg_1, gg_2, \dots, gg_n) = (g_{\sigma(1)}, g_{\sigma(2)}, \dots, g_{\sigma(n)})$  for some  $\sigma \in S_n$ .

We define  $\phi : G \rightarrow S_n$  by  $\phi(g) = \sigma$  as above.

We first claim  $\phi$  is homomorphism. Let  $a, b \in G$  such that  $\phi(a) = \alpha$  and  $\phi(b) = \beta$ . Then,  $(abg_1, \dots, abg_n) = (ag_{\beta(1)}, ag_{\beta(2)}, \dots, ag_{\beta(n)}) = (g_{\alpha(\beta(1))}, \dots, g_{\alpha(\beta(n))})$ , thus  $\phi(ab) = \alpha\beta = \phi(a)\phi(b)$ .

Next, we claim  $\phi$  is an embedding. Note  $g \in \text{Ker}(\phi)$  iff  $gg_i = g_i$  for all  $1 \leq i \leq n$ . In particular, we have  $ge = e$  and thus we must have  $g = e$ . Since the kernel is trivial, we have  $\phi$  is an embedding and hence we are done.  $\heartsuit$

**Example 4.1.10.** Let  $G$  be finite, suppose  $H \leq G$  and  $[G : H] = n$ . Show that there exists a homomorphism  $\phi : G \rightarrow S_n$  defined in terms of how  $g$  permutes the left cosets of  $H$  in  $G$  when  $G$  acts on  $G/H$  by left multiplication.

Then, let  $K$  be the kernel of the above homomorphism, show that  $K \subseteq H$  and  $G/K$  is isomorphic to a subgroup of  $S_n$ .

*Solution.* Note  $[G : H] = n$  and thus we have  $g_1, \dots, g_n \in G$  so that  $g_1H, g_2H, \dots, g_nH$  are all the distinct left cosets of  $H$  in  $G$ . Then, we define  $\phi(g) = \sigma$  where

$$(gg_1H, gg_2H, \dots, gg_nH) = (g_{\sigma(1)}H, g_{\sigma(2)}H, \dots, g_{\sigma(n)}H)$$

Note  $\sigma$  is indeed an element of  $S_n$ , as if  $gg_iH = gg_jH \iff g_j^{-1}g^{-1}gg_i = g_j^{-1}g_i \in H \iff g_jH = g_iH$ , which is contradictory. Thus,  $i \neq j \Rightarrow gg_iH \neq gg_jH$  and thus  $\sigma$  is indeed a permutation as claimed.

We need to show  $\phi$  is a homomorphism as  $\phi$  maps  $G$  to  $S_n$ . Let  $x, y \in G$  and  $\phi(x) = \sigma, \phi(y) = \tau$ , then

$$\begin{aligned} (xyg_1H, \dots, xyg_nH) &= (xg_{\tau(1)}H, \dots, xg_{\tau(n)}H) \\ &= (g_{\sigma(\tau(1))}H, \dots, xg_{\sigma(\tau(n))}H) \\ &= (g_{\sigma\tau(1)}H, \dots, xg_{\sigma\tau(n)}H) \end{aligned}$$

Thus, we have  $\phi(xy) = \sigma\tau = \phi(x)\phi(y)$  as desired. Therefore,  $\phi$  is a homomorphism as claimed.

To show the next claim, we note  $x \in \text{Ker}(\phi)$  imply

$$(xg_1H, \dots, xg_nH) = (g_1H, \dots, g_nH)$$

In particular, there exists  $1 \leq i \leq n$  so that  $g_iH = H$  and thus we have  $xg_iH = x(g_iH) = xH = g_iH = H$ , which imply  $x \in H$ . Therefore, we must have  $\text{Ker}(\phi) \subseteq H$ . Note, by the first isomorphism theorem, we have  $G/K \cong \phi(G)$ , where  $\phi(G)$  is a subgroup of  $S_n$  as desired. ♠

**Example 4.1.11.** Show that  $H \leq G$  and  $[G : H] = p$ , where  $p$  is the smallest prime dividing  $|G|$ , then  $H$  is normal in  $G$ .

*Solution.* Let  $\phi$  be defined as in Example 4.1.10 with  $H, G$  and  $[G : H] = p$ . Then, we have  $K = \text{Ker}(\phi) \trianglelefteq G$ ,  $K \subseteq H$  (note we also have  $K \leq H$ ), and  $G/K \cong S$  where  $S \leq S_p$ .

Let  $|H| = h$ ,  $|G| = n$ , and  $|K| = k$ . Since  $k|h$  by Lagrange, let  $h = ak$  where  $a > 0$  and  $a \in \mathbb{Z}$ . Note we have  $n/h = p$  and thus  $n = hp$ . In addition, we let  $n/k := s$  where  $s > 0$  and  $s \in \mathbb{Z}$ . Therefore, we have  $n = ks = hp$ , where  $h = ak$ , thus  $ks = akp \Rightarrow s = ap \Rightarrow p|s$  where  $s = n/k$ . Thus  $p \mid [G : K]$ .

Note  $[G : K] \mid |S_p|$  where  $|S_p| = p!$ . Thus  $[G : K] \mid p!$  and hence  $[G : K] \nmid p^i$  as it is impossible to prime factor  $i$  many  $p$ 's out of  $[G : K]$  when  $[G : K]$  divides  $p(p-1)(p-2)\dots 1$ . In addition, we also note, for all primes  $q$  where  $q > p$ , we have  $q$  is not a prime factor of  $[G : K]$ . Suppose, for a contradiction, we have  $[G : K] \neq p$ . Since  $p \mid [G : K]$ , we must have  $[G : K] > p$ . Then,  $[G : K] = p \cdot \prod_{i=1}^u p_i^{t_i}$  where each  $p_i < p$  and  $1 < p_i$ . However, this imply  $|G| = |K| \cdot p \cdot \prod_{i=1}^u p_i^{t_i}$ , and thus  $p$  would not be the smallest prime that divides  $|G|$ , and we have a contradiction.

If  $[G : K] = p$ , we have  $\frac{|G|}{|K|} = \frac{|G|}{|H|}$ , and thus  $|K| = |H|$  where  $K \subseteq H$ . Therefore,  $K = H$  and hence  $H \trianglelefteq G$ . ♠

## 4.2 Applications of Group Actions

**Theorem 4.2.1 (Orbit-stabilizer theorem).** *Let  $G$  be finite. Let  $G$  acts on  $X$ , for all  $x \in X$ , we have*

$$|G| = |\text{stab}(x)| \cdot |\text{orb}(x)|$$

*Proof.* Fix  $x \in G$ . Let  $S = \text{stab}(x)$ ,  $O = \text{orb}(x)$  and define  $\phi : G/S \rightarrow O$  by  $\phi(\bar{g}) = gx$ , we need to show this function is bijection.

First, we need to check this function is well-defined. Suppose  $\bar{a} = \bar{b} \in G/S$ . Hence,  $a = bs$  where  $s \in S$ . Then  $ax = b(sx) \Rightarrow ax = bx \Rightarrow \phi(\bar{a}) = \phi(\bar{b})$ .

Suppose  $\bar{a}, \bar{b} \in G/S$  such that  $\phi(\bar{a}) = \phi(\bar{b})$ . This means that

$$ax = bx \Rightarrow b^{-1}ax = x \Rightarrow b^{-1}a \in S \Rightarrow \bar{a} = \bar{b}$$

Thus  $\phi$  is injective.

Let  $y \in O$  so that  $y = gx, g \in G$ . Hence  $\phi(\bar{g}) = gx = y$  and so  $\phi$  is surjective.

Note in the proof we do not use the fact that  $G$  is finite so this bijection would work in general even  $G$  is infinite.

♡

**Example 4.2.2.** Let  $G$  be finite and let  $X = \{H : H \leq G\}$ . Let the action be conjugation, we fix  $H \in X$ , by the Orbit-stablizer theorem, we have  $|G| = |\text{stab}(H)| \cdot |\text{orb}(H)| = |N_G(H)| \cdot |\text{orb}(H)|$ . Hence,  $|\text{orb}(H)| = \frac{|G|}{|N_G(H)|} = [G : N_G(H)]$ .

**Example 4.2.3.** Let  $G$  be finite and  $H, K \leq G$ . Let  $X = HK = \{hk : h \in H, k \in K\}$  Then,

1. show  $H \times K$  acts on  $X$  via the action  $(x, y) \cdot hk = xhky^{-1}$ ,
2. compute the order of  $X$  using Orbit-Stablizer Theorem.

*Solution.* To show it is a group action, we need to check the group action axioms.

Let  $x \in H, y \in K$ , then for arbitrary  $t = hk \in X$ , we have  $(x, y)hk = xhky^{-1}$  where  $ky^{-1} \in K$  and  $xh \in H$ , thus  $(x, y)hk \in X$ , so this indeed maps  $(H \times K) \times X \rightarrow X$

Next, note  $e \in H \times K$  is the element  $(e, e)$  where  $e \in G$ , thus for arbitrary  $hk \in X$ , we have  $(e, e)hk = ehke^{-1} = hk$ .

Let  $(x, y) \in H \times K$  and  $(u, v) \in H \times K$ . Then, for arbitrary  $hk \in X$ , we have

$$\begin{aligned} ((x, y)(u, v)) \cdot hk &= (xu, yv)hk = xuhkv^{-1}y^{-1} \\ &= x((u, v) \cdot hk)y^{-1} \\ &= (x, y) \cdot ((u, v) \cdot hk) \end{aligned}$$

Thus,  $(x, y) \cdot hk = xhky^{-1}$  is indeed an action on  $X$  by  $H \times K$ .

Next, we note  $H \times K$  acts on  $X$ , thus we have  $|H \times K| = |H| \cdot |K| = |\text{stab}(x)| \cdot |\text{orb}(x)|$ . Then, note  $e \in HK$ , and thus we have  $|\text{stab}(e)| \cdot |\text{orb}(e)| = |H||K|$ . Let  $(x, y) \in H \times K$ , then  $(x, y)e = e \iff xy^{-1} = e \iff x = y$ . Thus  $\text{stab}(e) = H \cap K$ .

Next, we show the orbit of  $e$  is  $HK$ . Note  $t \in \text{orb}(e) \iff t = (x, y)e$  for some  $(x, y) \in H \times K$ . Thus,  $t = xy^{-1}$ , where  $x \in H$  and  $y^{-1} \in K$ , and hence  $\text{orb}(e) \subseteq HK = X$ . Next, let  $t \in HK$ , then  $t = hk$ , and in particular,  $t = h(k^{-1})^{-1}$ , and thus  $t \in \text{orb}(e)$ . In turn, we indeed have  $\text{orb}(e) = HK$ .

Thus, by Orbit-Stab Theorem, we have

$$|H| \cdot |K| = |H \cap K| \cdot |HK| \Rightarrow |X| = |HK| = \frac{|H||K|}{|H \cap K|}$$



**Remark 4.2.4.** We note Example 4.2.3.2 obtained the same result as Proposition 2.2.16.

**Lemma 4.2.5.** Let  $G$  act on  $X$ , then for  $x, y \in X$ , we have either  $\text{orb}(x) = \text{orb}(y)$  or  $\text{orb}(x) \cap \text{orb}(y) = \emptyset$ .

*Proof.* It suffice to show  $\neg(\text{orb}(x) \cap \text{orb}(y) = \emptyset) \rightarrow \text{orb}(x) = \text{orb}(y)$ .

Suppose  $\text{orb}(x) \cap \text{orb}(y) \neq \emptyset$  and  $z \in \text{orb}(x) \cap \text{orb}(y)$ . Thus, we have  $z = g_1x = g_2y$  where  $g_1, g_2 \in G$ . Thus,  $x = g_1^{-1}g_2y$  and hence  $\text{orb}(x) \subseteq \text{orb}(y)$ . Similarly, we must have  $y = g_2^{-1}g_1x$  and so we have  $\text{orb}(y) \subseteq \text{orb}(x)$  and we are done.  $\heartsuit$

**Theorem 4.2.6 (Class Equation).** Let  $C(b_i)$  be all the distinct centralizers of  $G$  where  $b_i \notin Z(G)$ , then we have

$$|G| = |Z(G)| + \sum \frac{|G|}{|C(b_i)|} = |Z(G)| + \sum [G : C(b_i)]$$

*Proof.* Note for any  $x \in X$ , we have  $x = ex \in \text{orb}(x)$ . With this observation and Lemma 4.2.5, we have  $X = \bigcup \text{orb}(a_i)$  where  $i \neq j \Rightarrow \text{orb}(a_i) \cap \text{orb}(a_j) = \emptyset$  is disjoint unions.

If  $X$  is finite and  $G$  is finite, then  $|X| = \sum |\text{orb}(a_i)|$ . We pull out all the orbits with cardinality one. To do this, we define  $X_G = \{x \in X : \forall g \in G, gx = x\}$  and we see this is the number of orbits of size one. Thus, we have  $|X| = |X_G| + \sum |\text{orb}(b_i)|$  where  $\text{orb}(b_i)$  are distinct representatives such that  $b_i \notin X_G$ .

Now, let  $G$  act on  $X = G$  by conjugation. Then,  $|G| = |Z(G)| + \sum |\text{orb}(b_i)|$  where  $\text{orb}(b_i)$  are represented by elements not in the center. By Orbit-stabilizer theorem,

we have

$$\begin{aligned}
|G| &= |Z(G)| + \sum |orb(b_i)| \\
&= |Z(G)| + \sum \frac{|G|}{|stab(b_i)|} \\
&= |Z(G)| + \sum \frac{|G|}{|C(b_i)|} \\
&= |Z(G)| + \sum [G : C(b_i)]
\end{aligned}$$

♡

**Example 4.2.7.** Let  $p$  be prime and  $|G| = p^n$ . Show  $Z(G) \neq \{e\}$ .

*Solution.* By the class equation, we have  $p^n = |Z(G)| + \sum [G : C(b_i)]$ . Suppose  $Z(G) = \{e\}$  then  $|Z(G)| = 1$ . Since  $b_i \notin Z(G)$  and so we have  $C(b_i) \subset G$  and so  $\frac{|G|}{|C(b_i)|} > 1$ . This imply  $\frac{|G|}{|C(b_i)|}$  is in the form of  $p^k$ . Thus  $\frac{|G|}{|C(b_i)|} \equiv 0 \pmod{p}$  and then, we would have  $0 \equiv 1 + 0 \pmod{p}$  as we mod both side of  $p^n = |Z(G)| + \sum [G : C(b_i)]$  by  $p$ . This is a contradiction and we are done. ♠

**Example 4.2.8.** Let  $p$  be prime, let  $G$  be non-abelian with  $|G| = p^3$ . Compute the number of conjugacy classes in  $G$ , i.e. the number of orbits when  $G$  acts on itself by conjugation.

*Solution.* By Class Equation, we have  $|G| = |Z(G)| + \sum [G : C(b_i)]$  where  $b_i$  are representatives of conjugacy classes in  $G$  such that  $b_i \notin Z(G)$ . Thus,  $p^3 = |Z(G)| + \sum [G : C(b_i)]$ , and note  $Z(G) \neq \{e\}$  and since  $|Z(G)| \mid |G|$ , we have  $|Z(G)| = p, p^2$  or  $p^3$ .

If  $|Z(G)| = p^3$ , then  $G$  is Abelian and thus a contradiction. Therefore, either  $|Z(G)| = p$  or  $|Z(G)| = p^2$ .

Suppose  $|Z(G)| = p^2$ , then  $|G/Z(G)| = p$  and thus  $G/Z(G)$  must be cyclic (Note we have  $|G| = p$  imply  $G$  is cyclic, as if  $x \neq e$  and  $x \in G$ , then  $|\langle x \rangle| \mid p$ , which imply  $\langle x \rangle = G$ ), which imply  $G$  is Abelian by Proposition 2.2.10, a contradiction.

Therefore, we must have  $|Z(G)| = p$ . Next, suppose there exists  $b_i \notin Z(G)$  so that  $[G : C(b_i)] = p^2$ . Then  $p^2 = \frac{|G|}{|C(b_i)|} \Rightarrow |C(b_i)| = p$  where  $C(b_i) = \{g \in G : gb_i = b_i g\}$ . However, note  $Z(G) \subseteq C(g)$  for all  $g \in G$ . Indeed, let  $x \in Z(G)$  then  $xg = gx$  and thus  $x \in C(g)$ , which imply  $Z(G) \subseteq C(g)$ . Therefore,  $|C(b_i)| = |Z(G)| = p$  imply  $Z(G) = C(b_i)$ , which imply  $b_i \in Z(G)$  and thus a contradiction.

Note  $C(g) \leq G$  (indeed, note  $e \in C(g)$  and thus  $C(g) \neq \emptyset$ . Next, let  $x, y \in C(g)$  then  $xy^{-1}g = xgy^{-1} = gxy^{-1}$  and  $C(g)$  is a subgroup). Therefore,  $|C(g)| \mid |G|$ , which imply  $|C(g)| \in \{1, p, p^2, p^3\}$ .

Hence, we must have  $[G : C(b_i)] = p$  as we showed  $[G : C(b_i)]$  cannot be  $p^2$  for all  $b_i$ , and it is certainly impossible to have  $|C(b_i)| = 1$  as this imply  $[G : C(b_i)] = p^3$

which contradicts the fact  $|Z(G)| \neq 0$ . Moreover, suppose  $C(b_i) = p^3$  then  $[G : C(b_i)] = 1$  then  $C(b_i) = G$ , and thus  $Z(G) \subseteq C(b_i)$  and thus  $Z(G) = G$ , which is a contradiction.

Therefore,  $|C(b_i)| = p$  and  $\sum [G : C(b_i)] = kp$  where  $k$  is the number of conjugacy classes such that  $b_i$  is not in the center as  $[G : C(b_i)] = \text{stab}(b_i)$  under the action of conjugation, where  $\text{stab}(b_i)$  is the conjugacy class of  $b_i$ . Thus, we have  $kp + p = p^3$  and hence  $k = p^2 - 1$ .

In total, we would have  $k + p$  many conjugacy classes,  $p$  many from  $Z(G)$  and  $k$  many from  $C(b_i)$  where  $b_i \notin Z(G)$ . Thus the total number is  $p^2 + p - 1$ .

♠

**Theorem 4.2.9.** [Cauchy's] If  $G$  is a finite group and  $p$  is a prime such that  $p \mid |G|$ , then we have an element  $y$  in  $G$  such that  $|y| = p$ .

*Proof.* Note we have  $|G| = |Z(G)| + \sum [G : C(b_i)]$ .

If  $p \mid |Z(G)|$ , then we are done by Cauchy's theorem for abelian finite groups.

If  $p \nmid |Z(G)|$ , thus there exists  $i$  such that  $p \nmid \frac{|G|}{|C(b_i)|}$  (indeed, if  $p \mid \frac{|G|}{|C(b_i)|}$  for all  $i$ , then we mod  $p$  by both side of  $|G| = |Z(G)| + \sum [G : C(b_i)]$ , which would lead to a contradiction) and hence  $p \mid |C(b_i)|$ , where  $|C(b_i)| \mid |G|$ . The result follows by induction. ♡

**Definition 4.2.10.** Let  $G$  be finite group and  $X$  be finite set. Let  $g \in G$ , we define  $\text{fix}(g) = \{x \in X : gx = x\} \subseteq X$ .

We define  $X \backslash G = \{\text{orbits of this action}\}$  be the set of all orbits.

**Remark 4.2.11.** Let's add up the size of fixs of  $G$ , i.e.  $\sum_{g \in G} |\text{fix}(g)|$ . Note we have

$$\begin{aligned} \sum_{g \in G} |\text{fix}(g)| &= |\{(g, x) \in G \times X : gx = x\}| \\ &= |\{(x, g) \in X \times G : gx = x\}| = \sum_{x \in X} |\text{stab}(x)| \\ &= \sum_{x \in X} \frac{|G|}{|\text{orb}(x)|} = |G| \sum_{x \in X} \frac{1}{|\text{orb}(x)|} \\ &= |G| \sum_{A \in X \backslash G} \sum_{x \in A} \frac{1}{|A|} = |G| \sum_{A \in X \backslash G} |A| \frac{1}{|A|} \\ &= |G| |X \backslash G| \end{aligned}$$

**Theorem 4.2.12 (Burnside's Lemma).** Let  $G$  be a finite group acting on a non-empty finite set  $X$ . Then,  $|X \backslash G| = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$

*Proof.* Immediately by Remark 4.2.11. ♡

**Example 4.2.13.** Say we have  $n$  colors and we want to color the four corner of a floor tile. How many different floor tiles could we make?

*Solution.* Let  $X$  be the set of all configurations of all possibilities include rotations. Note,  $x, y \in X$  are the same tile iff  $\exists g \in \langle r \rangle \leq D_8$  such that  $gx = y$  iff  $orb(x) = orb(y)$ . Thus, now we are looking for  $|X \backslash G|$ .

Let  $G = \langle r \rangle$ , we now count the size of fixes. We have  $|fix(e)| = n^4$ . We have  $|fix(r)| = n$ ,  $|fix(r^2)| = n^2$  and  $|fix(r^3)| = n$ .

Therefore,  $|X \backslash G| = \frac{n^4 + n^2 + 2n}{4}$  by Burnside's Lemma. ♠

**Example 4.2.14.** Compute how many ways can a 6-beaded necklace be made using 3 black beads and 3 white beads?

*Solution.* Let  $X$  be all the configurations of the necklace with 3 black beads and 3 white beads which include rotations. Let  $G = D_{12}$ , then  $x = y \iff \exists g \in G, gx = y$ . Thus,  $x = y$  if and only if  $orb(x) = orb(y)$ . Thus, we are looking for the number of orbits of this action.

Thus,  $|X \backslash G| = \frac{\sum |fix(g)|}{|G|}$  where  $g \in G$ . We calculate each  $fix(g)$  where  $g \in \{e, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$

$|fix(e)| = \frac{6!}{3!3!} = 20$ ,  $|fix(r)| = 0$ ,  $|fix(r^2)| = 2$ ,  $|fix(r^3)| = 0$ ,  $|fix(r^4)| = 2$ ,  $|fix(r^5)| = 0$ ,  $|fix(s)| = 4$ ,  $|fix(sr)| = 0$ ,  $|fix(sr^2)| = 4$ ,  $|fix(sr^3)| = 0$ ,  $|fix(sr^4)| = 4$ , and  $|fix(sr^5)| = 0$ .

Thus, we have  $|X \backslash G| = \frac{1}{12}(20 + 2 + 2 + 4 + 4 + 4) = 3$ . ♠

**Example 4.2.15.** How many different ways can the vertices of a cube be colored using  $n$  colors?

*Solution.* The answer is  $\frac{n^8 + 17n^4 + 6n^2}{24}$ . For detailed work, consider your own assignment solution. ♠

## 4.3 Finite Abelian Groups

**Remark 4.3.1.** Intuitively, if  $n = \prod_{i=1}^k p_i^{n_i}$  is the prime factorization of  $n$ , then  $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \dots \times \mathbb{Z}_{p_k^{n_k}}$ .

Thus, to classify finite Abelian groups by isomorphism, we want to decompose  $G$  into direct products of cyclic groups.

**Proposition 4.3.2.** Let  $G$  be a group,  $H \trianglelefteq G$ ,  $K \trianglelefteq G$ , and  $H \cap K = \{e\}$ , then we have  $HK \cong H \times K$ . In particular, we have  $|HK| = |H| \cdot |K|$ .



*Proof.* Since  $H, K$  are normal subgroups, for all  $h \in H$  and  $k \in K$ , we have  $h^{-1}k^{-1}h \in K$  and thus  $h^{-1}k^{-1}hk \in K$ . Also,  $k^{-1}hk \in H$  and thus  $h^{-1}k^{-1}hk \in H$ . Hence,  $h^{-1}k^{-1}hk \in H \cap K$  and thus  $h^{-1}k^{-1}hk = e$ . Therefore,  $hk = kh$  for all  $h \in H, k \in K$  and in particular,  $HK = KH$ .

Let  $\phi : H \times K \rightarrow HK$  where  $\phi(h, k) = hk$ , we show it is an isomorphism. First, note  $(h_1, k_1) = (h_2, k_2)$ , then  $h_1 = h_2, k_1 = k_2$ , and thus  $\phi(h_1, k_1) = \phi(h_2, k_2)$  and  $\phi$  is well-defined.

Next, let  $(h_1, k_1), (h_2, k_2) \in H \times K$ , then

$$\phi((h_1, k_1) \cdot (h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$$

Next, let  $x \in HK$ , then  $x = hk$  where  $h \in H, k \in K$ . Thus  $\phi(h, k) = x$  and so  $\phi$  is surjective.

Next, let  $g = (h, k) \in \text{Ker}(\phi)$ , then  $\phi(h, k) = hk = e$  and thus  $h = k^{-1}$  where  $h \in H$  and  $k^{-1} \in K$  and thus  $h \in H \cap K$ , so  $h = e$  and thus  $k^{-1} = k = e$  which imply  $g = (e, e) = e \in H \times K$ . Thus  $\phi$  is injective as the kernel is trivial.

Hence  $H \times K \cong HK$ . ♡

**Definition 4.3.3.** Let  $G$  be a group and  $H, K \trianglelefteq G$ , where  $H \cap K = \{e\}$ . We define the **internal direct product** of  $H$  and  $K$  to be  $HK$ , where  $HK := \{hk : h \in H, k \in K\}$ .

**Definition 4.3.4.** Let  $G$  be a group and let  $p$  be prime.

1. A group  $G$  is called a ***p*-group** if  $|G| = p^n$  for some  $n \in \mathbb{N}$ . Subgroups of  $G$  which are *p*-groups are called ***p*-subgroups**.
2. If  $G$  is a group of order  $p^n \cdot m$  where  $p \nmid m$ , then a subgroup  $H \leq G$  of order  $p^n$  is called a ***Sylow p*-subgroup** of  $G$ .
3. The set of ***Sylow p*-subgroups** of  $G$  is denoted as  $\text{Syl}_p(G)$  and the number of Sylow *p*-subgroups of  $G$  is denoted by  $n_p(G)$ .

**Lemma 4.3.5.** Let  $P \in \text{Syl}_p(G)$ . If  $Q$  is any *p*-subgroup of  $G$  then  $Q \cap N_G(P) = Q \cap P$ .

*Proof.* Let  $H = N_G(P) \cap Q$ . Since  $P \leq N_G(P)$ , it is clear that  $P \cap Q \leq H$ . It suffice to show  $H \leq P \cap Q$ . By definition, we have  $H \leq Q$ , it suffice to show  $H \leq P$ . We do this by showing  $PH$  is a *p*-subgroup of  $G$  containing both  $P$  and  $H$ , where  $P$  is a *p*-subgroup of  $G$  of largest possible order, so we must have  $PH = P$  and thus  $H \leq P$ .

Since  $H \leq N_G(P)$ , by Proposition 2.2.17.(2), we have  $PH$  is a subgroup. By Proposition 2.2.16, we have  $|PH| = \frac{|P||H|}{|P \cap H|}$ . Note  $|P|$  is the power of  $p$ ,  $H$  is a subgroup of  $Q$  which means  $|H|$  divides  $|Q|$  so  $|H|$  must be a power of  $p$  as well. In addition,  $P \cap H$  is a subgroup of  $P$ , which imply  $|P \cap H|$  divides the power of  $p$  and so it must be a power of  $p$ . Moreover,  $P$  is a subgroup of  $PH$  so the order of  $PH$  is divisible by  $p^n$ , the largest power of  $p$  which divides  $|G|$ . Thus, we must have  $|PH| = |P|$  and hence  $PH = P$  and so  $H \leq P$ . ♡



**Remark 4.3.6.** Sylow's first theorem for abelian groups is Theorem 4.3.7.(1).

**Theorem 4.3.7.** [Sylow's Theorem] Let  $G$  be a finite group of order  $p^n m$ , where  $p$  is prime and  $p \nmid m$ . Then,

1. Sylow  $p$ -subgroups of  $G$  exists, i.e.  $\text{Syl}_p(G) \neq \emptyset$ ,
2.  $P \in \text{Syl}_p(G)$  and  $Q$  is any  $p$ -subgroups of  $G$ , then there exists  $g \in G$  such that  $Q \leq gPg^{-1}$ , i.e.  $Q$  is contained in some conjugate of  $P$ . In particular, any two Sylow  $p$ -subgroups of  $G$  are conjugate in  $G$ .
3. The number of Sylow  $p$ -subgroups of  $G$  is of the form  $1 + kp$ , i.e.,

$$n_p(G) \equiv 1 \pmod{p}$$

In addition,  $n_p(G)$  is the index in  $G$  of the normalizer  $N_G(P)$  for any Sylow  $p$ -subgroup  $P$ , hence  $n_p(G) \mid m$ .

*Proof.* We prove part one first. We use induction on  $|G|$ . If  $|G| = 1$ , there is nothing to prove. Assume inductively the existence of Sylow  $p$ -subgroups for all groups of order less than  $|G|$ .

If  $p$  divides  $|Z(G)|$ , then by Cauchy's Theorem for Finite Abelian Groups,  $Z(G)$  has a subgroup  $N$  of order  $p$  (indeed, we have one element  $y \in Z(G)$  so that  $|y| = p$ , and we just let  $N = \langle y \rangle$ ). So, we have  $|G/N| = p^{n-1}m$ . By induction,  $G/N$  has a subgroup  $\overline{P}$  of order  $p^{n-1}$ . If we let  $P$  be the subgroup of  $G$  containing  $N$  such that  $P/N = \overline{P}$  (we know this by Correspondence Theorem 2.2.23), then  $|P/N| = p^{n-1}$  where  $|P/N| = |P|/|N|$  so  $|P| = p^n$ . Hence  $P$  is a Sylow  $p$ -subgroup of  $G$  and therefore, we can suppose  $p \nmid |Z(G)|$ .

Let  $g_1, \dots, g_r$  be representatives of the distinct centralizers where none of them are in the center of  $G$ . Then, by Class Equation, we have

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$$

If  $p \mid [G : C_G(g_i)]$  for all  $1 \leq i \leq r$ , then since  $p \mid |G|$ , we must have  $p \mid |Z(G)|$  which would be a contradiction. Therefore, there exists  $i$  so that  $p \nmid [G : C_G(g_i)]$ . Let  $H = C_G(g_i)$ , then since  $p \mid |G|$  and  $p \nmid [G : H]$ , we must have  $|H| = p^n k$  where  $p \nmid k$ .

Since  $g_i \notin Z(G)$ , we have  $|H| < |G|$ . By induction,  $H$  has a Sylow  $p$ -subgroup,  $P$ , which is a subgroup of  $G$  as well where  $|P| = p^n$ . Therefore,  $P$  is a Sylow  $p$ -subgroup of  $G$ . This finishes part one.

Before we proceed to part two and three, we make some calculations. By part 1, there exists a Sylow  $p$ -subgroup  $P$  of  $G$ .

Let  $\mathcal{S} = \{gPg^{-1} : g \in G\} = \{P_1, \dots, P_r\}$  be the set of all conjugates of  $P$ , let  $Q$  be any  $p$ -subgroup of  $G$ . By definition of  $\mathcal{S}$ , we have  $G$ , hence  $Q$ , acts by conjugation on  $\mathcal{S}$ . Write  $\mathcal{S}$  as a disjoint union of orbits under the action by  $Q$ , we have

$$\mathcal{S} = \mathcal{O}_1 \cup \dots \cup \mathcal{O}_s$$

where  $r := |\mathcal{S}| = \sum_{i=1}^s |\mathcal{O}_i|$ . Note that  $r$  does not depend on  $Q$ , but  $s$  does depend on  $Q$  (we also note definition,  $G$  has only one orbit on  $\mathcal{S}$  but a subgroup  $Q$  of  $G$  may have more than one orbit). Renumber the elements of  $\mathcal{S}$  if necessary so that the first  $s$  elements of  $\mathcal{S}$  are representatives of the  $Q$ -orbits:  $P_i \in \mathcal{O}_i$  for  $1 \leq i \leq s$ . It follows from Theorem 4.2.1, the orbit-stabilizer theorem, that, let  $o_i \in \mathcal{O}_i$  be a representative, then  $|\mathcal{O}_i| \cdot |\text{Stab}(o_i)| = Q$  where  $\text{Stab}(o_i) = N_Q(P_i)$  as we are acting by conjugation (recall Example 4.2.2). Thus, we have  $|\mathcal{O}_i| = |Q|/|N_Q(P_i)|$ . However, we note by definition,  $N_Q(P_i) = N_G(P_i) \cap Q$  and so by Lemma 4.3.5, we have  $N_G(P_i) \cap Q = P_i \cap Q$ . Hence, we get

$$|\mathcal{O}_i| = |Q|/|P_i \cap Q|, \quad 1 \leq i \leq s$$

Now, we prove  $r \equiv 1 \pmod{p}$ . Since  $Q$  was arbitrary, we may take  $Q = P_1$  above, so that we have  $|\mathcal{O}_1| = 1$ .

Now, for all  $i > 1$ , we have  $P_1 \neq P_i$ , so  $P_1 \cap P_i < P_1$  and we have

$$|\mathcal{O}_i| = |P_1|/|P_1 \cap P_i| > 1, \quad 2 \leq i \leq s$$

Since  $P_1$  is a  $p$ -group, we have  $|P_1|/|P_1 \cap P_i|$  must be a power of  $p$ , so that  $p \mid |\mathcal{O}_i|$  for  $2 \leq i \leq s$ . Thus, we have

$$r \equiv |\mathcal{O}_1| + \sum_{i=2}^s |\mathcal{O}_i| \equiv 1 \pmod{p}$$

We now prove part two. Let  $Q$  be any  $p$ -subgroup of  $G$ , suppose  $Q$  is not contained in  $P_i$  for any  $i \in \{1, 2, \dots, r\}$ , i.e.  $Q \not\leq gPg^{-1}$  for all  $g \in G$ . In this situation,  $Q \cap P_i < Q$  for all  $i$ , then we have

$$|\mathcal{O}_i| = |Q|/|Q \cap P_i| > 1, \quad 1 \leq i \leq s$$

Thus, we have  $p \mid |\mathcal{O}_i|$  for all  $i$  and so  $p$  divides  $r = \sum_{i=1}^s |\mathcal{O}_i|$ , this contradicts the fact that  $r \equiv 1 \pmod{p}$ . Hence, we have  $Q \leq gPg^{-1}$  for some  $g \in G$ . This establishes part two. In particular, let  $Q$  be any Sylow  $p$ -subgroup of  $G$ . By the preceding argument,  $Q \leq gPg^{-1}$  for some  $g \in G$ . Since  $|gPg^{-1}| = |Q| = p^n$ , we must have  $pGp^{-1} = Q$ .

Next, we show part three. By part two, we must have  $\mathcal{S} = \text{Syl}_p(G)$  since every Sylow  $p$ -subgroup of  $G$  is conjugate to  $P$ , and so  $n_p \equiv r \equiv 1 \pmod{p}$ , which is the first half of part three. Since all Sylow  $p$ -subgroups are conjugate, we have  $n_p(G) = |\mathcal{S}| = |G|/|\text{stab}(P)| = |G|/|N_G(P)|$  where the action is  $G$  acts on  $\mathcal{S}$  by conjugation and  $P \in \text{Syl}_p(G)$ .

♡

**Proposition 4.3.8.** *Let  $G$  be a group and  $H_1, \dots, H_k \leq G$ . If for every  $i$ , we have  $H_i \cap H_1 \dots H_{i-1} H_{i+1} \dots H_k = \{e\}$  then  $H_1 \dots H_k \leq G$  and  $H_1 H_2 \dots H_k \cong H_1 \times H_2 \times \dots \times H_k$ .*

**Theorem 4.3.9.** *Let  $G$  be a finite abelian group of order  $\prod_{i=1}^k p_i^{n_i}$  where  $p_i$  is prime and  $p_i \neq p_j$  for  $i \neq j$ . For each  $i$ ,  $G$  has a normal subgroup  $H_i$  such that  $|H_i| = p_i^{n_i}$ . Moreover,  $G = H_1 H_2 \dots H_k \cong H_1 \times H_2 \times \dots \times H_k$ .*

*Proof.* By Sylow, each  $H_i$  exists. For each  $i$ , if  $g \in H_i \cap H_1 \dots H_{i-1} H_{i+1} \dots H_k$ , then  $|g| \mid |H_i|$  and  $|g| \mid \prod_{j \neq i, 1 \leq j \leq k} p_j^{n_j}$  (indeed, as  $G$  is abelian). Thus  $|g| = 1$  and so  $g = e$ . Thus  $H_1 \dots H_k \cong H_1 \times \dots \times H_k$ . In particular,  $H_1 \dots H_k \leq G$  with  $|H_1 \dots H_k| = |G|$  and therefore,  $G = H_1 \dots H_k$ .  $\heartsuit$

**Lemma 4.3.10.** *Let  $|G| = p^n$  be abelian. If  $G$  has a unique subgroup of order  $p$  then  $G$  is cyclic.*

*Proof.* We proceed by induction on  $n$ . If  $|G| = p$  then we are done. Suppose it holds for all groups with  $|G| = p^i$  where  $1 \leq i \leq n-1$  where  $n \geq 2$ .

Assume  $|G| = p^n$ , where  $G$  is abelian and has a unique subgroup of order  $p$ . Let  $H$  be the unique subgroup of  $G$  with  $|H| = p$ . We note that  $H$  contains exactly  $e$  and the elements of  $G$  of order  $p$ . Consider the homomorphism  $\phi : G \rightarrow G$  given by  $\phi(x) = x^p$  and by construction we have  $\text{Ker}(\phi) = H$ . By the first isomorphism theorem, we have  $G/H \cong \phi(G) \leq G$ . Thus,  $G/H$  has a unique subgroup  $\bar{K} = K/H$  of order  $p$ . By the inductive hypothesis,  $G/H$  is cyclic. Say  $G/H = \langle gH \rangle$  where  $g \in G$ , thus  $G/H = \langle H, gH, g^2H, \dots, g^mH \rangle = \langle g \rangle/H$  for some  $m \in \mathbb{N}$ . This means  $\frac{|G|}{|H|} = \frac{|\langle g \rangle|}{|H|} \Rightarrow |G| = |\langle g \rangle|$  which imply  $G = \langle g \rangle$  and hence cyclic.  $\heartsuit$

**Lemma 4.3.11.** *Let  $|G| = p^n$  be abelian and let  $C \leq G$  be cyclic subgroup of maximal cardinality. Then, there exists  $H \leq G$  such that  $C \cap H = \{e\}$  and  $G = CH$ , in particular,  $G \cong C \times H$ .*

*Proof.* We proceed by induction on  $n$ . If  $n = 1$ , and  $|G| = p$ , then  $G$  is cyclic and  $C = G$  and thus  $H = \{e\}$  would do the job. Assume the result for  $1, 2, \dots, k$  for some  $k \in \mathbb{N}$ .


Suppose  $|G| = p^{k+1}$  where  $G$  is abelian. Let  $C \leq G$  be cyclic of maximal order. If  $G$  is cycli then we have  $C = G$  and we are done. Suppose  $G$  is not cyclic, and thus by the first lemma,  $G$  has at least 2 subgroups of order  $p$ . However,  $C$  has a unique subgroup of order  $p$  and thus there exists  $G \leq G$ , where  $|H| = p$  such that  $H \cap C = \{e\}$ .

Consider  $G/H$ . Let  $\bar{A}$  be a cyclic subgroup of  $G/H$ , where  $\bar{A} = A/H$  with  $A \leq G$  is cyclic. Therefore,  $|\bar{A}| = \frac{|A|}{|H|} \leq \frac{|C|}{|H|}$ . Now, we have  $CH/H$ , by the second isomorphism theorem, we have  $CH/H \cong C/(C \cap H) = C/\{e\} \cong C$ . Hence,  $HC/H$  is a maximal cyclic subgroup of  $G/H$ , and by induction, there exists  $K/H \leq G/H$ , where  $H \leq K \leq G$ , such that  $G/H = (GH/H)(K/H)$  and  $(CH/H) \cap (K/H) = \{H\}$ . This means  $G/H = CHK/H = CK/H$  and thus  $G = CK$ . Next, note  $CH \cap K \subseteq H$  and therefore,  $C \cap K \subseteq CH \cap K \subseteq C \cap H = \{e\}$  and thus we indeed have  $G = CK$  and  $C \cap K = \{e\}$ .  $\heartsuit$

**Proposition 4.3.12.** *Every finite abelian  $p$ -group is isomorphic to a direct product of cyclic group.*

*Proof.* Immediately by previous Lemmas. 

**Theorem 4.3.13 (Fundamental Theorem of Finite Abelian Groups).** *Every finite abelian group is isomorphic to a direct product of cyclic groups.*

*Proof.* By previous theorems, propositions and lemmas. 

**Example 4.3.14.** Find a complete, irredundant list of Abelian groups of order 1176, up to isomorphism. Note  $1176 = 2^3 \cdot 3 \cdot 7^2$ .

*Solution.*

1.  $\mathbb{Z}_{1176} \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{7^2}$
2.  $\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_{7^2}$
3.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{7^2}$
4.  $\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$
5.  $\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$
6.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$



**Example 4.3.15.** Find all Abelian groups of order  $108 = 2^2 \cdot 3^3$  that have exactly one subgroup of order 3.

*Solution.*

1.  $\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3}$
2.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^3}$



# Chapter 5

## Basic Ring

### 5.1 Intro

**Definition 5.1.1.** A **ring**  $R$  is a set together with two binary operation on  $R$ ,  $+$  and  $\times$ , satisfying the following axioms:

1.  $(R, +)$  is an abelian group,
2.  $\times$  is associative, namely, for all  $a, b, c \in R$ ,  $(a \times b) \times c = a \times (b \times c)$
3. the distributivity laws hold in  $R$ : for all  $a, b, c \in R$ , we have

$$(a + b) \times c = ac + bc \text{ and } a \times (b + c) = ab + ac$$

**Definition 5.1.2.** The ring  $R$  is **commutative** if multiplication is commutative.

**Remark 5.1.3.** We do not assume the existence of  $1 \in R$  such that  $1x = x1 = x$  for all  $x \in R$ . When  $R$  does have such an element  $1 \in R$ , we say  $R$  is unital and call  $1$  the unity.

**Definition 5.1.4.** Let  $R$  be unital and  $a \in R$  such that  $\exists b \in R$  with  $ab = ba = 1$ , then we say  $a$  is a **unit** or **invertible**. We call  $b$  the **multiplicative inverse** of  $a$  and write  $b = a^{-1}$ .

**Definition 5.1.5.** Let  $R$  be unital, the collection of units of  $R$ , denoted by  $R^\times$ , form a group under multiplication.

**Definition 5.1.6.** Let  $R$  be unital, then we denote  $\sum_{i=1}^n 1_R := n$ . Since there exists  $-1$ , the additive inverse of multiplicative inverse, we denote  $\sum_{i=1}^n (-1_R) := -n$ .

**Remark 5.1.7.** Let  $a, b \in R$ , then we define  $a - b := a + (-b)$ .

**Definition 5.1.8.** If  $R$  is a ring such that  $ab = ba$  for all  $a, b \in R$ , we say  $R$  is **commutative**.

**Example 5.1.9.**

1.  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  and  $\mathbb{Z}_n$  are rings.
2. Let  $R$  be a ring, then  $M_n(R)$  and  $R[x]$  are rings, where  $M_n(R)$  is the  $n \times n$  matrices, and  $R[x]$  is the collection of polynomials over  $R$ .
3.  $M_2(\mathbb{R})$  is non-commutative ring,  $2\mathbb{Z}$  is non-unital ring,  $M_3(\mathbb{Z}_5)$  is finite and

non-commutative ring, and  $\{0, 2, 4, 6\} \subseteq \mathbb{Z}_8$  is finite and non-unital.

4.  $\{0, 2, 4, 6, 8\} \subseteq \mathbb{Z}_{10}$  is unital with unity 6.

**Remark 5.1.10.** We note that in  $R[x]$ , it is not necessary true that  $\deg(fg) = \deg(f) + \deg(g)$ . Consider  $R = \mathbb{Z}_4$ , and  $f(x) = 2x + 1$ , then  $f(x)f(x) = 1$  and so  $\deg(ff) = 0$ , however,  $\deg(f) + \deg(f) = 2$ .

**Definition 5.1.11.** Let  $R, S$  be rings, we define the **direct sum** of  $R$  and  $S$ , and denote  $R \oplus S$ , to be the ring over the set  $\{(a, b) : a \in R, b \in S\}$  with  $(a, b) + (c, d) = (a + c, b + d)$  and  $(a, b)(c, d) = (ac, bd)$ .

**Example 5.1.12.** Let  $R = C(\mathbb{R})$  be the collection of continuous functions over  $\mathbb{R}$ , we define  $(f + g)(x) = f(x) + g(x)$  to be the addition and  $(fg)(x) = f(x)g(x)$  to be the multiplication, then  $R$  is a ring.

Note  $C(\mathbb{R})$  is not a ring with composition as multiplication. Let  $f(x) = x^2$  and  $g(x) = x, h(x) = 1$ . Then  $[f \circ (g + h)](x) = x^2 + 2x + 1$  and  $(fg + fh)(x) = x^2 + 1$ . Thus it does not have distributivity. However, if we consider  $V$  be a vector space and  $L(V)$  be the collection of linear operators, then  $(L(V), +, \circ)$  is a ring with  $\circ$  be composition.

**Proposition 5.1.13.** For all  $a, b, c \in R$ ,

1.  $a0 = 0a = 0$
2.  $a(-b) = (-a)b = -(ab)$
3.  $a(b - c) = ab - ac$ , and  $(b - c)a = ba - ca$

*Proof.*

1.  $a0 = a(0 + 0) = a0 + a0$  and thus  $a0 - a0 = a0 + a0 - a0$ , which imply  $0 = a0$ . Similarly, we have  $0a = 0$ .
2.  $a(-b) + ab = a(-b + b) = a(0) = 0$  and thus  $-(ab) = a(-b)$ . Similarly,  $-(ab) = (-a)b$ .
3.  $a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac$

♡

**Definition 5.1.14.** Let  $R$  be a ring, we say  $\emptyset \neq S \subseteq R$  is a **subring** of  $R$  if  $S$  forms a ring using the operations of  $R$ .

**Proposition 5.1.15 (Subring test).** Let  $R$  be a ring,  $\emptyset \neq S \subseteq R$ , then  $S$  is a subring of  $R$  iff for all  $a, b \in S$ , we have

1.  $a - b \in S$
2.  $ab \in S$

*Proof.* Immediately by subgroup test and definition of rings.

♡

**Remark 5.1.16.** Let  $S$  be a subring of  $R$ , then we may write  $S \leq R$ .

**Definition 5.1.17.** We define the **center** of  $R$  to be  $Z(R) = \{a \in R : \forall b \in R, ab = ba\}$ .

**Definition 5.1.18.** Let  $R$  be a ring and  $r \in R$ , then we say  $r$  is nilpotent if  $\exists n \in \mathbb{N}$  such that  $r^n = 0$ .

**Example 5.1.19.** Let  $R$  be a ring,

1.  $Z(R) \leq R$
2. We say  $d \in \mathbb{Z}$  is **square-free** when there does not exist prime  $p$  such that  $p^2 \mid d$ . Then, the ring of quadratic integers,  $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ , is a subring of  $\mathbb{C}$ .

We show this by subring test. Let  $a + b\sqrt{d}$  and  $a' + b'\sqrt{d}$ . Then, we have  $(a + b\sqrt{d}) - (a' + b'\sqrt{d}) = (a - a') + (b - b')\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ .

Next, we have  $(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + dbb') + (ab' + ba')\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ .

3. The ring of Gaussian integers is  $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
4. If  $R$  is commutative, then we have  $\text{Nil}(R) = \{r \in R : r \text{ is nilpotent}\}$  is a subring of  $R$ .

Indeed, if  $a^n = 0$  and  $b^m = 0$ , and let  $k = mn$ , we have  $a^k = b^k = 0$ . Then, we have  $(ab)^k = a^k b^k = 0$ , and thus  $ab \in \text{Nil}(R)$ .

Next, let  $p = 2k$ , then we have  $(a - b)^p = \sum_{i=0}^p \binom{p}{i} a^i (-b)^{p-i} = 0$ . Hence,  $a - b \in \text{Nil}(R)$ .

5. Let  $R = M_2(\mathbb{R})$ , and  $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ ,  $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ . Note  $A^2 = B^2 = 0$ , and  $A + B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ . Then,  $(A + B)^{2k} = I$  and  $(A + B)^{2k+1} = A + B$ .

**Definition 5.1.20.** Let  $R$  be unital, then the **characteristic** of  $R$  is the  $|1|$  in the underlying addition group, the order of unity in  $(R, +)$ . In addition, if  $|1| = \infty$  then we say  $R$  has **characteristic zero**.

**Example 5.1.21.** Let  $F(\mathbb{R})$  denote the set of functions from  $\mathbb{R} \rightarrow \mathbb{R}$ . Assume  $F(\mathbb{R})$  is a ring with  $(f + g)(x) = f(x) + g(x)$  and  $(fg)(x) = f(x)g(x)$ . Determine if the following are subrings of  $F(\mathbb{R})$ :

1.  $A = \{f \in F(\mathbb{R}) : f(1) = f(2)\}$
2.  $B = \{f \in F(\mathbb{R}) : f(x) \geq 0, \forall x \in \mathbb{R}\}$
3.  $C = \{f \in F(\mathbb{R}) : f(-x) = -f(x), \forall x \in \mathbb{R}\}$
4.  $D = \{f \in F(\mathbb{R}) : f \text{ has finitely many zero in } (0, 1)\} \cup \{0\}$
5.  $E = \{f \in F(\mathbb{R}) : f \text{ has infinitely many zero in } (0, 1)\}$

*Solution.* 1. It is. Let  $I(x) = 1$ , then  $I(1) = I(2)$  and  $I(x) \in A$  is the multiplicative identity of the ring. Hence  $A$  is not empty. Let  $f(x), g(x) \in A$ , then  $(f - g)(1) = f(1) - g(1) = f(2) - g(2) = (f - g)(2)$ . Moreover,  $(fg)(1) = f(1)g(1) = f(2)g(2) = (fg)(2)$ . Thus  $A \leq F(\mathbb{R})$ .

2. No, it is not. Consider  $f(x) = x^2$  and  $g(x) = x^4$ , then  $(f - g)(2) = -12 < 0$ . Thus it is not closed under addition (and taking inverse).

3. No. Consider  $f(x) = x^3$  and  $g(x) = x$ , then we have  $(fg)(x) = x^4$  and  $(fg)(-x) = fg(x)$ , thus  $fg \notin C$ .

4. Nope. The additive identity (the zero function) is not in  $D$ .

5. Nope. Consider

$$f(x) = \begin{cases} 0 & \text{if } x \in (0.1, 0.2) \\ 1 & \text{otherwise} \end{cases}, g(x) = \begin{cases} 0 & \text{if } x \in (0.4, 0.5) \\ 1 & \text{otherwise} \end{cases}$$

Both  $f(x)$  and  $g(x)$  have infinitely many zeros, but  $(f + g)(x) \geq 1$  for all  $x \in (0, 1)$ . Thus  $f + g$  is not in  $E$  and hence it is not closed under addition.



**Example 5.1.22.** Show the following results:

1. If  $R$  is a ring such that  $r^2 = r$  for all  $r \in R$  then  $R$  is commutative.
2. If  $S \leq R$  where  $R$  is finite ring, then  $|S| \mid |R|$ .
3. If  $R$  is commutative and unital ring with  $\text{char}(R) = p$ ,  $p$  is prime, then  $(a + b)^p = a^p + b^p$  for all  $a, b \in R$ .
4. If  $R$  is finite unital ring and  $R^\times$  is a group of odd order, then  $\text{char}(R) = 2$ .

*Solution.* 1. For all  $r \in R$ , we have  $2r = (2r)^2 = 4r^2 = 4r$  so that  $2r = r + r = 0$ . Thus  $r = -r$  for all  $r \in R$ . Then, for all  $a, b \in R$ , we have  $(a + b)^2 = (a + b)^2 = a^2 + b^2 + ab + ba = a + b + ab + ba$ . Thus, we have  $ab + ba = 0$  which imply  $ab = -ba = -(-b)a = ba$ . Thus  $R$  is commutative.

2. If  $S \leq R$  then  $(S, +) \leq (R, +)$  so by Lagrange, we have  $|S| \mid |R|$ .

3. Note for all  $1 \leq i < p$ , we have  $(p - i)!i! \nmid p!$  as  $p$  is a prime, thus  $\frac{p!}{(p-i)!i!}$  contains the term  $p$  (or we have  $p \mid \frac{p!}{(p-i)!i!}$ ) and so it must be zero as  $p = 0$  in  $R$  by the definition of  $\text{char}(R) = p$ . Thus, let  $x, y \in R$ ,

$$\begin{aligned} (x + y)^p &= \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} \\ &= \sum_{i=0}^p \frac{p!}{(p-i)!i!} x^i y^{p-i} \\ &= x^p + y^p \end{aligned}$$

4. Note if  $u$  is a unit then  $-u$  is a unit, therefore, if  $|R^\times|$  is odd, there must exists  $x \in R^\times$  such that  $x = -x$ . If all of  $x \in R^\times$ , we have  $x \neq -x$ , then  $|R^\times|$  must be even. Therefore, we have  $x + x = 0$  and  $(1 + 1)x = 0$ , which imply  $1 + 1 = 0$  as  $x \neq 0$  because  $x \in R^\times$ .



## 5.2 Integral Domain and Fields

**Definition 5.2.1.** Let  $R$  be a ring, we say  $0 \neq a \in R$  is a **left zero divisor** if  $\exists 0 \neq b \in R$  such that  $ab = 0$ . Similarly, we say  $0 \neq a \in R$  is a **right zero divisor** if there exists  $0 \neq b \in R$  such that  $ba = 0$ .



**Remark 5.2.2.** We say  $a \in R$  is a zero divisor if  $a$  is a left or right divisor.

Moreover, we insist that  $1 \neq 0$  in  $R$ , if  $R$  is unital.

**Definition 5.2.3.** We say a ring  $R$  is an *integral domain* if  $R$  is commutative, unital, and has no zero divisors.

**Definition 5.2.4.** A ring  $R$  is a field if  $R$  is commutative, unital, and every nonzero element is a unit.

**Example 5.2.5.** Let  $R$  be a ring,

1. if  $\forall a, b \in R$ , the multiplication is defined as  $ab = 0$ , then we say this is a trivial multiplication.
2.  $\{0\}$  is a trivial ring and not unital
3.  $\text{char}(\mathbb{Z}_n) = n$ ,  $\text{char}(\mathbb{Z}) = 0$ , and  $\text{char}(\mathbb{Z}_n \oplus \mathbb{Z}_m) = \text{lcm}(n, m)$ .
4.  $\mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}, \mathbb{Z}[\sqrt{d}]$  are all integral domain.
5. If  $R$  is integral domain, then  $R[x]$  is integral domain.
6.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \mathbb{Q}[\sqrt{2}]$  are fields.
7. Let  $F$  be a field, then  $F(x) = \{\frac{f(x)}{g(x)} : f, g \in F[x], g \neq 0\}$  is a field, called rational function field. In addition, note  $\mathbb{Z}_p(x) \supset \mathbb{Z}_p$  and  $\mathbb{Z}_p(x) \neq \mathbb{Z}_p$ .
8.  $\mathbb{Z}$  is a integral domain but not a field.
9. Let  $R$  be a integral domain then  $R \oplus R$  can never be a integral domain. Indeed,  $(0, 1) \times (1, 0) = (0, 0)$ , so the zero divisor exists.

**Proposition 5.2.6.** Let  $R$  be unital, if  $\text{char}(R) = n < \infty$ , then  $nr = 0$  for all  $r \in R$ .

*Proof.*  $nr = \sum_{i=1}^n r = (\sum_{i=1}^n 1)r = 0r = 0$

♡

**Proposition 5.2.7.** Let  $R$  be a ring, let  $a, b, c \in R$  such that  $a \neq 0$  and  $ab = ac$ , and  $a$  is not a left zero divisor, then  $b = c$ .

*Proof.*  $ab = ac \Rightarrow a(b - c) = 0$ , since  $a \neq 0$  and not a left zero divisor, we have  $b - c = 0$ , thus  $b = c$ .

♡

**Proposition 5.2.8.** Every field is an integral domain.

*Proof.* Note  $F$  is commutative and unital, thus it suffice to show we do not have left zero divisor.

Suppose  $0 \neq a \in F$ . Suppose  $ab = 0$ , then  $a^{-1}ab = 0$  and thus  $b = 0$ . Hence,  $F$  has no zero divisor.

♡

**Proposition 5.2.9.** Every finite integral domain is a field.

*Proof.* Suppose  $R = \{a_1, \dots, a_n\}$  is finite integral domain. Then  $R$  is commutative and unital. Let  $0 \neq a \in R$ . Then  $aa_i = aa_j$  if and only if  $a_i = a_j$ . In particular, note  $R = \{aa_1, \dots, aa_n\}$  and thus  $\exists i$  such that  $aa_i = 1$ .

♡

**Proposition 5.2.10.** *Let  $R$  be an integral domain, then  $\text{char}(R) = 0$  or  $\text{char}(R) = p$  where  $p$  is a prime.*

*Proof.* It suffice to show  $\text{char}(R) \neq 0 \Rightarrow \text{char}(R) = p$ .

Suppose  $\text{char}(R) = n > 0$ . Suppose  $n$  is not a prime for contradiction. Then  $n = ab$  where  $1 < a, b < n$ . Thus,  $ab = 0$  where  $a \neq 0$  and  $b \neq 0$ , contradicting the fact that  $R$  is integral domain.  $\heartsuit$

## 5.3 Homomorphism

**Definition 5.3.1.** let  $R, R'$  be a ring, we say  $\phi : R \rightarrow R'$  is a homomorphism if

1.  $\phi(a + b) = \phi(a) + \phi(b)$
2.  $\phi(ab) = \phi(a)\phi(b)$

**Remark 5.3.2.** Let  $\phi : S \rightarrow R$  be a homomorphism between two rings  $S$  and  $R$ , we have  $\phi_+ : (R, +) \rightarrow (S, +)$  is a group homomorphism.

**Example 5.3.3.**

1.  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$  given by  $\phi(n) = [n]$  is a homomorphism,
2.  $\phi : M_n(\mathbb{R}) \rightarrow \mathbb{R}$  given by  $\phi(A) = \det(A)$  is not a homomorphism,
3. let  $R$  be commutative,  $\phi : R[x] \rightarrow R$  given by  $\phi(f(x)) = f(a)$  is a homomorphism.
4. let  $R$  be commutative, unital and  $\text{char}(R) = p$  is a prime, then  $\phi(x) = x^p$  is a homomorphism from  $R$  to  $R$ .

**Example 5.3.4.** We find all the homomorphisms from  $\mathbb{Z} \oplus \mathbb{Z}$  to  $\mathbb{Z}$ .

Let  $\phi$  be a homomorphism. Suppose  $\phi(1, 0) = n$  and  $\phi(0, 1) = m$ . Then, for arbitrary  $(a, b) \in \mathbb{Z} \oplus \mathbb{Z}$ , we have

$$\begin{aligned}\phi(a, b) &= \phi(a(1, 0) + b(0, 1)) \\ &= an + bm\end{aligned}$$

.

Therefore,  $n$  and  $m$  completely determine  $\phi$ . Next, note  $(1, 0) \times (1, 0) = (1, 0)$ , thus  $\phi((1, 0) \times (1, 0)) = n \times n = \phi(1, 0) = n$ . Therefore,  $n^2 = n$  (and  $m^2 = m$ ) and so  $n, m \in \{0, 1\}$ .

If  $n = m = 0$  then  $\phi$  is the trivial mapping with  $\phi(a, b) = 0$  for all  $(a, b) \in \mathbb{Z} \oplus \mathbb{Z}$ .

If  $n = 0$  and  $m = 1$  then  $\phi(a, b) = b$  is the homomorphism. If  $n = 1, m = 0$  then  $\phi(a, b) = a$  is the homomorphism.

If  $n = m = 1$ , then  $\phi(a, b) = a + b$ . However, note  $(1, 1)^2 = (1, 1)$ , thus  $\phi(1, 1) = \phi(1, 1)\phi(1, 1)$  and thus  $(1 + 1) = 2 = (1 + 1)(1 + 1) = 4$ , and we have a contradiction.

**Definition 5.3.5.** Let  $R, S$  be rings and  $\phi : R \rightarrow S$  be homomorphism. Then

1. if  $\phi$  is injective, we say  $\phi$  is an *embedding*,
2. if  $\phi$  is bijective, we say  $\phi$  is an *isomorphism* and we say  $R$  and  $S$  are *isomorphic* and write  $R \cong S$ .

**Example 5.3.6.** Let  $V = \mathbb{R}^n$  and  $R = \{T : V \rightarrow V : T \text{ is linear}\}$ . Then  $R \cong M_n(\mathbb{R})$ . In particular, we have  $\phi(T) = [T]_\sigma$  where  $\sigma$  is the standard basis.

**Example 5.3.7.** Let  $F$  be a field, and let 1 be the multiplicative identity,

1. if  $\text{char}(F) = 0$ , then  $R = \{n1(m1)^{-1} : n, m \in \mathbb{Z}, m \neq 0\}$  is a subfield of  $F$ . Also, note  $R \cong \mathbb{Q}$ .
2. if  $\text{char}(F) = p$ , where  $p$  is a prime, then  $R = \{0, 1, \dots, p-1\}$  is a subfield of  $F$  with  $R \cong \mathbb{Z}_p$ .

In either case,  $R$  is called the *prime field* of  $F$ .

# Chapter 6

## Ideals

### 6.1 Intro to Ideals and Quotient Rings

**Remark 6.1.1.** Let  $R$  be a ring, and  $S \leq R$ , then  $(S, +) \leq (R, +)$ . Moreover,  $(R, +)$  is abelian and so  $(S, +) \trianglelefteq (R, +)$ .

Let  $R/S$  denote the set of cosets of  $(S, +)$  in  $(R, +)$ , i.e.  $R/S = \{a + S : a \in R\}$ . Since  $(S, +) \trianglelefteq (R, +)$ , we have  $(R/S, +)$  is an abelian group where  $(a + S) + (b + S) = (a + b) + S$ .

Now, we want to turn  $(R/S, +, \times)$  into a ring with  $(R/S, +)$  and multiplication defined as  $(a + S)(b + S) = ab + S$ . Note this multiplication is associative and distributive, hence we only need to check well-definedness.

**Definition 6.1.2.** We say  $S \leq R$  is a **left-ideal** if for all  $a \in S$  and  $r \in R$ , we have  $ra \in S$ . We say  $S$  is a **right-ideal** if for all  $a \in S$  and  $r \in R$ , we have  $ar \in S$ . We say  $S$  is an **ideal** of  $R$  if it is a left and right ideal.

**Theorem 6.1.3.** Let  $S \leq R$  then  $R/S$  is a ring with the well-defined operations  $(a + S) + (b + S) = (a + b) + S$  and  $(a + S)(b + S) = ab + S$  if and only if  $S$  is an ideal of  $R$ .

*Proof.* ( $\Leftarrow$ ) Homework.

( $\Rightarrow$ ) Suppose  $R/S$  is a ring with these well-defined operations. Take  $r \in R$  and  $a \in S$ . Then  $ra + S = (r + S)(a + S) = (r + S)(0 + S) = r0 + S = 0 + S$ . Thus  $ra \in S$ . Similarly,  $ar \in S$ .  $\heartsuit$

**Definition 6.1.4.** If  $I$  is an ideal of  $R$ , we will write  $I \trianglelefteq R$ .

**Proposition 6.1.5.** Let  $\emptyset \neq I \subseteq R$ , then  $I \trianglelefteq R$  if and only if,

1.  $\forall a, b \in I, a - b \in I$ ,
2.  $\forall a, b \in R, a \in I \vee b \in I \Rightarrow ab \in I$ .

**Example 6.1.6.** Let  $R$  be a ring and  $a \in R$ , then

1.  $Ra = \{ra : r \in R\}$  is the left ideal of  $R$  generated by  $a$ . Similarly, we have  $aR = \{ar : r \in R\}$  is the right ideal of  $R$  generated by  $a$ . Note they are the minimal left/right ideal containing  $a$  if  $R$  is unital.
2.  $\{rar' : r, r' \in R\}$  might not be a subring of  $R$  as it may not close under addition.
3.  $RaR = \langle a \rangle = \{\sum_{i=1}^n r_i a r'_i : r_i, r'_i \in R, n \in \mathbb{N}\}$  is the principal ideal of  $R$  generated by  $a$ . Note this is indeed closed in multiplication.

**Example 6.1.7.** Let  $R = M_2(\mathbb{R})$ ,  $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ , then  $RA = \left\{ \begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix} : x, y \in \mathbb{R} \right\}$  and  $AR = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in \mathbb{R} \right\}$ . Thus, note  $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin AR$  and thus  $AR$  is not a left ideal (but it is a right ideal).

**Example 6.1.8.** Let  $R$  be a commutative and unital ring, find all ideals of  $M_n(R)$ .

*Solution.* Let  $I \trianglelefteq R$ , we will show  $M_n(I) \trianglelefteq M_n(R)$ . Let  $A = (a_{ij}) \in M_n(I)$  and  $B = (b_{ij}) \in M_n(R)$ , then  $BA = \begin{bmatrix} \sum_{i=1}^n b_{1i}a_{i1} & \sum_{i=1}^n b_{1i}a_{i2} & \dots & \sum_{i=1}^n b_{1i}a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n b_{ni}a_{i1} & \sum_{i=1}^n b_{ni}a_{i2} & \dots & \sum_{i=1}^n b_{ni}a_{in} \end{bmatrix}$ . In particular, for all  $1 \leq k, l \leq n$ , we have  $\sum_{i=1}^n b_{ki}a_{il} \in I$  as  $a_{il} \in I \Rightarrow b_{ki}a_{il} \in I$  and  $I$  is a subring (hence closed under addition). Thus  $BA \in M_n(I)$ . Similarly, we see  $AB \in M_n(I)$  and so  $M_n(I)$  is an ideal of  $M_n(R)$ .

Conversely, suppose  $W \trianglelefteq M_n(R)$ , we show it is in the form of  $M_n(I)$  for some  $I \trianglelefteq R$ . In particular, define  $\Phi : M_n(R) \rightarrow \mathcal{P}(R)$  to be  $\Phi(A) = \bigcup_{1 \leq i, j \leq n} \{a_{ij}\}$  where  $\mathcal{P}(R)$  is the power set of  $R$  and  $a_{ij}$  is the  $(i, j)$  entry of  $A$ . Let  $I = \bigcup_{A \in W} \Phi(A)$ . We note we have  $W \subseteq M_n(I)$  by the way we defined  $I$ . Next, note  $a \in I$  if and only if  $a$  is an entry in an element of  $W$ . Say  $a$  is the  $(i, j)$  entry of  $A \in W$ . Then,  $E_{ii}AE_{jj} \in W$  where  $E_{kl}$  is the matrix such that the only non-zero entry with value  $1 \in R$  of  $E_{kl}$  is the  $(k, l)$  entry, i.e. the  $(i, j)$  entry of  $E_{kl}$  is 0 if  $(i, j) \neq (k, l)$  and the  $(k, l)$  entry of  $E_{kl}$  is 1. In particular, note  $E_{ii}AE_{jj} = aE_{ij}$  and hence  $aE_{ij} \in W$ . Since  $a$  was arbitrary, we have  $a \in I \Rightarrow \forall 1 \leq i, j \leq n, aE_{ij} \in W$ . Let  $A = (a_{ij}) \in M_n(I)$ , we have  $A = \sum_{i=1}^n \sum_{j=1}^n a_{ij}E_{ij}$  and since  $W$  is a subring of  $M_n(R)$ , the addition is closed and thus  $A \in W$ . Therefore,  $M_n(I) \subseteq W$  as  $A$  was arbitrary. Thus,  $M_n(I) = W$ . We will show  $I$  is an ideal of  $R$ . Let  $\phi : R \rightarrow M_n(R)/W$  to be  $\phi(x) = xE_{11} + W$ . We first note  $xE_{11} \in W = M_n(I)$  if and only if  $x \in I$ . Thus,  $\phi(x) = W$  if and only if  $x \in I$ . Therefore,  $\text{Ker}(\phi) = I$  and so  $I$  is an ideal of  $R$  as it is the kernel of  $\phi$ .

Thus, we have  $W$  is an ideal of  $M_n(R)$  if and only if there exists  $I \trianglelefteq R$  and  $W = M_n(I)$ . ♠

**Remark 6.1.9.** If  $R$  is commutative,  $I$  is left ideal iff  $I$  is right ideal iff  $I$  is ideal. Thus  $aR = Ra = \langle a \rangle$  if  $R$  is commutative.

**Example 6.1.10.** Let  $R$  be unital and  $u \in R^\times$ , then  $uR = R$  as  $uu^{-1} = u \in uR$ . In particular, if  $F$  is a field, then the ideals is equal  $F$  or  $\{0\} = \langle 0 \rangle$ .

**Example 6.1.11.** Let  $R$  be unital and non-commutative. Then  $1 \in Z(R)$  and

$Z(R) \neq R$ , in particular,  $Z(R)$  is not a left or right ideal as if  $Z(R)$  is a left or right ideal then  $Z(R) = R$ , which would be contradiction.

**Remark 6.1.12.** Note  $S \trianglelefteq R$  if and only if  $S = \text{Ker}(\phi)$  for some homomorphism  $\phi : R \rightarrow R'$  where  $R'$  is any ring.

**Example 6.1.13.**

1. Let  $R = \mathbb{Z} \oplus \mathbb{Z}$  and  $S = \{(a, a) : a \in \mathbb{Z}\}$ , then we have  $S \leq R$  but  $(1, 1)(1, 2) = (1, 2) \notin S$  and thus  $S$  is not normal in  $R$ .
2. Let  $R = \mathbb{Z}[x]$ , and  $I = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$ . We see that  $I = \langle x \rangle$ . Then,  $\overline{f(x)} = \overline{g(x)}$  iff  $f(x) - g(x) \in I$  iff  $f(0) - g(0) = 0$  iff  $f(0) = g(0)$ .
3. Let  $R = M_2(\mathbb{Z})$  and  $I = M_2(2\mathbb{Z})$ , we note  $I \trianglelefteq R$ . Then,  $A = (a_{ij})$  and  $B = (b_{ij})$  are equal in  $R/I$  if and only if  $A - B \in I$  iff  $a_{ij} \equiv b_{ij} \pmod{2}$ . In addition, we have  $|R/I| = 2^4$  and  $R/I \cong M_2(\mathbb{Z}_2)$ .

**Theorem 6.1.14 (Division Algorithm).** Let  $F$  be a field and let  $R = F[x]$ . For all  $f(x), g(x) \in R$ ,  $g(x) \neq 0$ , there exists unique  $q(x), r(x) \in R$ , such that  $f(x) = g(x)q(x) + r(x)$  where  $r(x) = 0$  or  $\deg(r) < \deg(g)$ .

*Proof.* Long division. ♡

**Proposition 6.1.15.** Let  $F$  be a field and  $R = F[x]$ , every ideal of  $R$  is principal.

*Proof.* Let  $I$  be an ideal of  $F[x]$ . If  $I = \{0\}$  then  $I = \langle 0 \rangle$ . Suppose  $I \neq \{0\}$ . Let  $g(x) \in I$  be non-zero polynomial of minimal degree in  $I$ .

We claim that  $I = \langle g(x) \rangle$ . Clearly  $\langle g(x) \rangle \subseteq I$ .

Let  $f(x) \in I$ , by division algorithm, there exists  $q(x), r(x)$  with  $r(x) = 0$  or  $\deg(r) < \deg(g)$  such that  $f(x) = g(x)q(x) + r(x)$ . But  $r(x) = f(x) - g(x)q(x)$  where  $f(x), g(x)q(x) \in I$ . Thus  $r(x) \in I$  and by minimality, we must have  $r(x) = 0$ . Thus  $f(x) = g(x)q(x) \in \langle g(x) \rangle$ . ♡

**Example 6.1.16.** Let  $F$  be a field and  $a \in F$ . Then  $I = \{f(x) \in F[x] : f(a) = 0\} \trianglelefteq F[x]$ . Note  $f(x) = x - a \in I$ , and thus if there exists  $0 \neq b \in F$  such that  $b \in I$ , then  $b$  is a unit and so  $I = F[x]$ , which is contradiction. Therefore,  $x - a$  is a polynomial of minimal degree in  $I$  and thus  $I = \langle x - a \rangle$ .

**Remark 6.1.17.** Note  $\mathbb{Z}$  has a division algorithm, and by the same argument, every ideal of  $\mathbb{Z}$  is principal and has the form  $\langle n \rangle = n\mathbb{Z}$ .

## 6.2 First Isomorphism Theorem

**Theorem 6.2.1 (First Isomorphism Theorem).** Let  $R, S$  be a ring and  $\phi : R \rightarrow S$  be homomorphism. Then  $R/\text{Ker}\phi \cong \phi(R)$  where  $\phi(R) \leq S$ . In particular, the isomorphism is  $\bar{a} \mapsto \phi(a)$ .

*Proof.* The proof is almost the same as the first isomorphism theorem for groups. ♡

**Example 6.2.2.**

1. Note  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$  with  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$  given by  $\phi(x) = [x]$  as we have  $\text{Ker}\phi = n\mathbb{Z}$ .
2. Consider  $R : \mathbb{Z}_3[x]/\langle x^2 + 2 \rangle$ . We have  $R \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$  as  $|R| = 3^2$  and  $\bar{0} = \overline{(x+1)(x+2)}$ . Next, we define  $\phi : \mathbb{Z}_3[x] \rightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_3$  by  $\phi(f(x)) = (f(1), f(2))$ , then check  $\text{Ker}\phi = \langle x^2 + 2 \rangle$  and  $\phi$  is surjective.
3. Consider  $C = \mathbb{R}/\langle x^2 + 1 \rangle$ , we remark that  $C \cong \mathbb{C}$ .

**Remark 6.2.3.** Let  $F$  be a field and  $f(x) \in F[x]$  with  $\deg(f) = n$ .

Then  $F[x]/\langle f(x) \rangle = \overline{\{\sum_{i=0}^{n-1} a_i x^i : a_i \in F\}}$ . If  $|F| = m$ , then  $|F[x]/\langle f(x) \rangle| = m^n$ .

**Definition 6.2.4.** Let  $R$  be a ring, if  $I, J \trianglelefteq R$ , then we define

$$IJ := \left\{ \sum_{i=1}^n a_i b_i : a_i \in I, b_i \in J, n \in \mathbb{N} \right\}, I + J := \{a + b : a \in I, b \in J\}$$

Moreover, we say  $I, J$  are **comaximal** if  $I + J = R$ .

**Theorem 6.2.5 (Chinese Remainder Theorem).** *Let  $R$  be commutative and unital, and  $I, J \trianglelefteq R$  and  $I, J$  are comaximal, then we have*

$$R/(IJ) \cong R/I \oplus R/J$$

*Proof.* Suppose  $I + J = R$ . Let  $x \in IJ$ , then  $x = \sum a_i b_i$  where  $a_i \in I$  and  $b_i \in J$ . Thus  $x \in I$  as  $I$  is an ideal and  $a_i b_i \in I$ . Similarly,  $x \in J$  as  $J$  is an ideal and  $a_i b_i \in J$ . Hence,  $IJ \subseteq I \cap J$ . Suppose  $x \in I \cap J$ , then  $x \in I$  and  $x \in J$ . Next, note there exists  $a \in I$  and  $b \in J$  so that  $a + b = 1$  as  $I + J = R$  and  $R$  is unital. Hence,  $x = 1x = (a + b)x = ax + bx = ax + xb$ , where  $a \in I$  and  $x \in J$  and  $x \in I$  and  $b \in J$ . Thus  $x \in IJ$  and so  $I \cap J \subseteq IJ$ . Hence  $I \cap J = IJ$ .

Since  $R = I + J$ , for all  $x \in R$ , we have  $x = x_i + x_j$  where  $x_i \in I$  and  $x_j \in J$ . Let  $\phi : R \rightarrow R/I \oplus R/J$  to be  $\phi(x) = (x + I, x + J) = (x_j + I, x_i + J)$ . We first note that if  $x = x_i + x_j = x'_i + x'_j$  with  $x_i, x'_i \in I, x_j, x'_j \in J$ , then  $\phi(x) = (x_j + I, x_i + J) = (x'_i + x'_j - x_i + I, x'_i + x'_j - x_j + J) = (x'_j + I, x'_i + J)$  as  $x'_i - x_i \in I$  and  $x'_j - x_j \in J$ . Hence  $\phi$  is well-defined function.

Note  $I + J = R$  so let  $(x + I, y + J) \in S := R/I \oplus R/J$  be arbitrary, we have  $x = x_i + x_j, y = y_i + y_j$  and thus  $x + I = x_j + I$  as  $x_i \in I, y + J = y_i + J$  as  $y_j \in J$ . In particular, this imply  $(x + I, y + J) = (x_j + I, y_i + J)$  and so  $z = y_i + x_j \in R$  would give us  $\phi(z) = (x_j + I, y_i + J) = (x + I, y + J)$ . Hence  $\phi$  is surjective.

Next, let  $x, y \in R$ , we have  $x = x_i + x_j$  and  $y = y_i + y_j$ , and thus  $\phi(x + y) = \phi(x_i + y_i + x_j + y_j) = (x_j + y_j + I, x_i + y_i + J) = (x_j + I, x_i + J) + (y_j + I, y_i + J) = \phi(x) + \phi(y)$ . Similarly, we see  $\phi(xy) = \phi(x_i y_i + x_i y_j + x_j y_i + x_j y_j) = (xy + I, xy + J) = (x_j y_j + I, x_i y_i + J)$  as  $x_i y_j, x_j y_i \in I \cap J$  so that  $x_i y_j + I = 0 + I = x_j y_i + I$  and  $x_i y_j + J = 0 + J = x_j y_i + J$ . However, we note  $\phi(x)\phi(y) = (x_j + I, x_i + J)(y_j + I, y_i + J) = (x_j y_j + I, x_i y_i + J) = \phi(xy)$ , and thus  $\phi$  is homomorphism. Next, if we

can show  $\text{Ker}(\phi) = I \cap J$ , then by first isomorphism theorem, we would have the desired result.

We claim  $\text{Ker}(\phi) = I \cap J = IJ$ . Let  $x \in I \cap J$ , we have  $x + I = 0 + I$  and  $x + J = 0 + J$ , thus  $I \cap J \subseteq \text{Ker}(\phi)$ . Conversely, suppose  $x \in \text{Ker}(\phi)$ , then  $\phi(x) = (x + I, x + J)$ . Note  $x + I = 0 + I$  iff  $x - 0 \in I$  and so  $x \in I$ . Similarly, we see  $x + J = 0 + J$  iff  $x \in J$ , and thus  $x \in I \cap J$ . Therefore,  $\text{Ker}(\phi) = IJ$  and so  $R/(I \cap J) = R/IJ \cong S = R/I \oplus R/J$ .  $\heartsuit$

**Lemma 6.2.6.** *Let  $R$  be commutative unital ring, then  $R[x]/\langle x - a \rangle \cong R$  for all  $a \in R$ .*

*Proof.* Let  $\phi : R[x] \rightarrow R$  be the mapping  $\phi(f(x)) = f(a)$ . First, note this is well-defined as  $\sum_{i=1}^n b_i a^i$  is unique (in the sense that in  $R$ , the addition and multiplication is well-defined function). Next, we note this is obviously homomorphism as  $\phi(kf(x) + g(x)) = k\phi(f(x)) + \phi(g(x))$  as  $\phi(kf(x) + g(x)) = kf(a) + g(a) = k\phi(f(x)) + \phi(g(x))$ . Thus, it suffice to show  $\langle x - a \rangle$  is the kernel of  $\phi$ . Note  $\langle x - a \rangle \subseteq \text{Ker}(\phi)$ . Next, suppose  $\phi(f(x)) = 0$ . Next, note  $f(x) = g(x)(x - a) + r(x)$  where  $g(x), r(x) \in R[x]$  and  $\deg(r) \leq \deg(x - a)$  as  $x - a$  is monic polynomial. Thus,  $r(x)$  must be zero as  $f(a) = 0 = g(a)0 + r(a) \Rightarrow r(a) = 0$  and so  $f(x) = g(x)(x - a)$ . Thus  $f(x) \in \langle x - a \rangle$  and  $\text{Ker}(\phi) = \langle x - a \rangle$ .  $\heartsuit$

**Example 6.2.7.** Show that

$$\mathbb{Z}_5[x]/\langle x^2 + 2x + 2 \rangle \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5$$

*Solution.* We note  $x^2 + 2x + 2 = x^2 - 3x + 2 = (x - 1)(x - 2)$ . Next, let  $I = \langle x - 1 \rangle$  and  $J = \langle x - 2 \rangle$ , we will show  $I + J = R := \mathbb{Z}_5[x]$  and then  $\langle x^2 + 2x + 2 \rangle = IJ$ .

Since  $f(x) = x - 1 \in I$  and  $g(x) = x - 2 \in J$ , we have  $f(x) - g(x) = x - 1 - x + 2 = 1 \in I + J$ . In particular, this imply  $I + J = R$  as  $I + J$  is an ideal<sup>1</sup> of  $R$ .

Next, note  $IJ \subseteq \langle x^2 + 2x + 2 \rangle$  as  $x^2 + 2x + 2 = (x - 1)(x - 2)$  and  $\langle x^2 + 2x + 2 \rangle \subseteq IJ$ . Thus  $IJ = \langle x^2 + 2x + 2 \rangle$  and so by Chinese Remainder Theorem,  $R/\langle x^2 + 2x + 2 \rangle = R/IJ$  where  $R/IJ \cong R/I \oplus R/J$  as  $I + J = R$ .

Then, we note by Lemma 6.2.6, we have  $R/\langle x - a \rangle \cong \mathbb{Z}_5$  for  $a \in \mathbb{Z}_5$ . Hence, we have  $R/IJ = \mathbb{Z}_5[x]/\langle x^2 + 2x + 2 \rangle \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5$  as  $R/I, R/J \cong \mathbb{Z}_5$ .  $\spadesuit$

**Remark 6.2.8.** When we see  $R = \mathbb{Z}_p[x]/\langle f(x) \rangle$ , where  $f(x)$  can be factored into two monic polynomial of degree one, we can conclude that  $R \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ .

---

<sup>1</sup>Indeed, let  $r \in I + J$ , we have  $r = r_i + r_j$  where  $r_i \in I$  and  $r_j \in J$ . Thus, let  $x \in R$  be arbitrary, we have  $rx = xr_i + xr_j \in I + J$  as  $xr_i \in I$  and  $xr_j \in J$ . Similarly, we see  $rx \in I + J$  and thus  $I + J$  is an ideal.



**Example 6.2.9.** Let  $a_1, a_2 \in \mathbb{Z}$  and let  $m, n \geq 2$  be positive integers such that  $\gcd(m, n) = 1$ . Show that the system of equations

$$\begin{cases} x \equiv a_1 \pmod{m} \\ x \equiv a_2 \pmod{n} \end{cases}$$

has precisely the solution  $\{x \in \mathbb{Z} : x \equiv a \pmod{mn}\}$  for some  $a \in \mathbb{Z}$ .

*Solution.* Let  $R = \mathbb{Z}$ ,  $I = n\mathbb{Z}$  and  $J = m\mathbb{Z}$ . Since  $\gcd(n, m) = 1$ , there exists  $a, b \in \mathbb{Z}$  such that  $an + bm = 1$ . In particular, note  $an \in I$  and  $bm \in J$  so that  $an + bm \in I + J$  and thus  $I + J = R$ . Next, we note  $IJ = nm\mathbb{Z}$ . Indeed, note  $IJ = I \cap J$ , and suppose  $x \in IJ$ , then  $n \mid x$  and  $m \mid x$  so  $nm \mid x \Rightarrow x \in nm\mathbb{Z}$ . Conversely,  $x \in nm\mathbb{Z}$  clearly imply  $x \in I \cap J$ . Hence  $IJ = nm\mathbb{Z}$ . Thus, we have  $R/IJ \cong R/I \oplus R/J = \mathbb{Z}_n \oplus \mathbb{Z}_m$  as  $I + J = R$  where  $R/IJ = \mathbb{Z}_{nm}$ .

Recall in (a), we defined  $\phi : R \rightarrow R/I \oplus R/J$  to be  $\phi(x) = (x + I, x + J)$ . In our particular case, we recognize that, for  $x \in R$ , we have  $x + I = x + \mathbb{Z}_n$  is the same as  $x \pmod{n}$  and  $x + J = x + \mathbb{Z}_m$  is the same as  $x \pmod{m}$ . Thus, by the first isomorphism theorem, we recall that the isomorphism  $\Phi$  we obtained for  $R/IJ$  to  $R/I \oplus R/J$  is defined to be  $\Phi(x + IJ) = \phi(x) = (x + I, x + J)$ .

Since  $\Phi$  is isomorphism, it is bijection. Thus, there exists a unique inverse of  $(a_2 + I, a_1 + J)$ , denote this element to be  $\alpha + IJ$ , i.e.  $\Phi(\alpha + IJ) = (a_2 + I, a_1 + J)$ . We will show that the solution set to

$$\begin{cases} x \equiv a_1 \pmod{m} \\ x \equiv a_2 \pmod{n} \end{cases}$$

is exactly the set  $\{x \in \mathbb{Z} : x \equiv \alpha \pmod{mn}\}$ .

Suppose  $x \equiv a_1 \pmod{m}$  and  $x \equiv a_2 \pmod{n}$ . Then, in particular, we have  $x + J = a_1 + J$  and  $x + I = a_2 + I$ . Thus  $\phi(x) = (a_2 + I, a_1 + J)$  and so  $\Phi(x + IJ) = (a_2 + I, a_1 + J)$ .

Since  $\Phi$  is bijection, we must have  $x + IJ = \alpha + IJ$  and so  $x \equiv \alpha \pmod{nm}$  as desired. Conversely, suppose  $x \equiv \alpha \pmod{mn}$ , then  $x + IJ = \alpha + IJ$  and so  $\Phi(x + IJ) = \phi(x) = (x + I, x + J)$  and  $\Phi(x + IJ) = \Phi(\alpha + IJ) = (a_2 + I, a_1 + J)$  so  $x + I = a_2 + I$  and  $x + J = a_1 + J$  and thus  $x$  is a solution. ♠

## 6.3 Maximal and Prime Ideals

**Definition 6.3.1.** Let  $R$  be unital and  $I \trianglelefteq R$  with  $I \neq R$ . We say  $I$  is **prime ideal** if whenever  $a, b \in R$  such that  $aRb = \{arb : r \in R\} \subseteq I$  then  $a \in I$  or  $b \in I$ .

**Definition 6.3.2.** Let  $R$  be unital and  $I \trianglelefteq R$  with  $I \neq R$ . We say  $I$  is **maximal** if whenever  $J \trianglelefteq R$  such that  $I \subseteq J \subseteq R$ , then either  $I = J$  or  $J = R$ .

**Remark 6.3.3.** Let  $R$  be commutative and unital, and  $I \subseteq R$  be proper. Then  $I$  is prime iff whenever  $a, b \in R$  such that  $ab \in I$  then  $a \in I$  or  $b \in I$ .

**Example 6.3.4.** Let  $\langle n \rangle \subseteq \mathbb{Z}$  with  $n > 1$ . Suppose  $n$  is prime, and let  $a, b \in \mathbb{Z}$  such that  $ab \in \langle n \rangle$ . Then  $ab \in \langle n \rangle \Rightarrow n|ab \Rightarrow n|a \vee n|b$ . Thus,  $a \in \langle n \rangle$  or  $b \in \langle n \rangle$  and hence  $\langle n \rangle$  is prime ideal.

Similarly, if  $\langle n \rangle$  is prime ideal, then  $n$  has to be prime.

**Example 6.3.5.** Let  $I = \{a + bi : a, b \in 2\mathbb{Z}\} \subseteq \mathbb{Z}[i]$ . Then  $(1 + i)(1 + i) = 2i \in I$  but  $(1 + i) \notin I$ . Thus,  $I$  is not prime.

**Example 6.3.6.** Let  $R = F(\mathbb{R})$ .  $I = \{f(x) : f(\pi) = 0\} \subseteq R$ . We claim  $I$  is maximal.

First, since  $f(x) = x \notin I$ ,  $I$  is proper. Next, let  $J \subseteq R$  such that  $I$  is proper set of  $J$ . We show  $J = R$ . Let  $0 \neq f(x) \in J$  such that  $f(x) \notin I$ . Thus,  $f(\pi) \neq 0$ . Let  $g(x) = f(x) - f(\pi)$ , then  $g(\pi) = 0$  and thus  $g(x) \in I$ .

Thus,  $f(x) \in J$  and  $g(x) \in I \subseteq J$  and so  $f(x) - g(x) \in J$  where  $f(x) - g(x) = f(\pi)$  is a constant function. However, since  $f(\pi) \neq 0$ , we have  $f(\pi)$  is a unit of  $R$ . Since  $J$  contains a unit, we have  $J = R$ .

**Example 6.3.7.** Let  $R = \mathbb{Z}[x]$ , and  $I = \langle x \rangle$ . Show  $I$  is prime and not maximal.

*Solution.* Since  $1 \notin I$ ,  $I \neq \mathbb{Z}[x]$ . Now suppose  $f(x), g(x) \in R$  such that  $fg \in I$ . Thus,  $f(0)g(0) = 0$ . Since  $\mathbb{Z}$  is an integral domain,  $f(0) = 0$  or  $g(0) = 0$ . Thus  $f(x) \in I$  or  $g(x) \in I$ .

$I$  is not maximal. Consider  $\langle x \rangle \subseteq \langle x, 2 \rangle \subseteq R$ . Since  $2 \notin \langle x \rangle$ , we have  $\langle x \rangle \neq \langle x, 2 \rangle$ . Suppose  $\langle x, 2 \rangle = \mathbb{Z}[x]$ . Thus  $\exists f, g \in R$  such that  $1 = f(x)x + g(x) \cdot 2$  which imply  $1 = 0 + g(0) \cdot 2$  and in turn imply 1 is even. A contradiction! ♠

**Proposition 6.3.8.**  $R$  be commutative and unital. Let  $I \subseteq R$ , then  $I$  is prime iff  $R/I$  is an integral domain.

*Proof.* ( $\Rightarrow$ ) Suppose  $I$  is prime. Since  $R$  is commutative,  $R/I$  is commutative. Since  $I \neq R$ , we have  $R/I$  is unital. Let  $\bar{a}, \bar{b} \in R/I$  such that  $\bar{a} \cdot \bar{b} = \bar{0}$ . This imply  $\overline{ab} = \bar{0}$  and thus  $ab \in I$ . Since  $I$  is prime, we have  $a \in I$  or  $b \in I$ . Thus,  $\bar{a} = \bar{0}$  or  $\bar{b} = \bar{0}$  and hence  $R/I$  is integral domain.

( $\Leftarrow$ ) Suppose  $R/I$  is an integral domain. Since  $R/I$  is unital, we have  $I \neq R$ . Let  $a, b \in R$  such that  $ab \in I$ . Thus,  $\overline{ab} = \bar{0}$  in  $R/I$  and so  $\bar{a} \cdot \bar{b} = \bar{0}$ . Since  $R/I$  is an integral domain, we have  $\bar{a} = \bar{0}$  or  $\bar{b} = \bar{0}$ . Thus,  $a \in I$  or  $b \in I$ . ♡

**Example 6.3.9.**

1. Since  $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$  and  $\mathbb{Z}$  is an integral domain, we have  $\langle x \rangle$  must be prime.
2.  $\mathbb{Z}[x]/\langle x, 4 \rangle \cong \mathbb{Z}_4$  and  $\mathbb{Z}_4$  is not an integral domain, thus  $\langle x, 4 \rangle$  is not prime.
3.  $\mathbb{Z}[x]/\langle x, p \rangle \cong \mathbb{Z}_p$  where  $p$  is prime, and  $\mathbb{Z}_p$  is integral domain and thus  $\langle x, p \rangle$  is prime.

## 6.4 Zorn's Lemma and More on Maximal Ideals

**Definition 6.4.1.** Let  $X$  be a set and a relation  $\preceq$  is a partial order on  $X$  if

1.  $\forall x \in X, x \preceq x$
2.  $\forall x, y \in X, x \preceq y \wedge y \preceq x \Rightarrow x = y$
3.  $\forall x, y, z \in X, x \preceq y, y \preceq z \Rightarrow x \preceq z$

**Definition 6.4.2.** If  $\preceq$  is a partial order on  $X$ , we call  $(X, \preceq)$  a **poset**.

**Example 6.4.3.**

1. Let  $X = P(\mathbb{N})$  be the power set of  $\mathbb{N}$ , then  $(X, \subseteq)$  is a poset.
2. Let  $X = \mathbb{R}$ , then  $\leq$  is a partial order.
3. Let  $X = \{(a_n)_{n=1}^{\infty} : a_i \in \mathbb{R}\}$ , the lexicographic ordering  $(a_n) \preceq (b_n)$  is defined as,  $(a_n)$  is less than  $(b_n)$  iff  $\exists N \in \mathbb{N}$  such that  $a_n = b_n$  for  $n < N$  and  $a_N < b_N$  and  $(a_n)$  equal  $(b_n)$  iff  $(a_n) = (b_n)$ .

**Remark 6.4.4.** Let  $(X, \preceq)$  be a poset. We do not insist that for every  $x, y \in X$ ,  $x \preceq y$  or  $y \preceq x$ .

**Definition 6.4.5.** A partial order  $\preceq$  on  $X$  is **total order** if  $x \leq y$  or  $y \leq x$  for all  $x, y \in X$ .

**Example 6.4.6.**  $(P(\mathbb{R}), \subseteq)$  is not a total order.

**Definition 6.4.7.** Let  $(X, \preceq)$  be a poset. If  $A \subseteq X$  and  $(A, \preceq)$  is a totally ordered poset, we call  $A$  a **totally ordered subset**. Some other books will call it a **chain**.

**Definition 6.4.8.** Let  $(X, \preceq)$  be a poset and  $A \subseteq X$ . An **upper bound** for  $A$  is a  $x \in X$  such that  $\forall a \in A, a \preceq x$ .

**Example 6.4.9.** Let  $X = \mathbb{R}$  and  $(X, \leq)$  be a poset. Let  $A = (0, 1)$ . Then 1 is an upper bound for  $A$ .

**Definition 6.4.10.** Let  $(X, \preceq)$  be a poset. We say  $x \in X$  is **maximal** if  $\nexists y \in X$  such that  $x \neq y$  and  $x \leq y$ .

**Theorem 6.4.11 (Zorn's lemma).** Let  $(X, \preceq)$  be a non-empty poset. If every totally ordered subset of  $X$  has an upper bound in  $X$ , then  $X$  has a maximal element.

**Proposition 6.4.12.** Let  $R$  be a unital ring. Every proper ideal  $I$  of  $R$  is contained in a maximal ideal. In particular, let  $I = \langle 0 \rangle$ ,  $R$  has a maximal ideal.

*Proof.* Let  $I$  be a proper ideal of  $R$ . Consider  $X = \{J \trianglelefteq R : I \subseteq J, J \neq R\}$ . Then  $(X, \subseteq)$  is a poset. Since  $I \in X$ ,  $X \neq \emptyset$ . Let  $Y$  be a totally ordered subset of  $X$ , let  $J = \bigcup_{A \in Y} A$ , then  $I \subseteq J$ . We claim that  $J$  is a proper ideal of  $R$ .

Let  $a, b \in J$ , let  $r \in R$ . Then  $a \in A$  and  $b \in B$  for some  $A, B \in Y$ . Since  $Y$  is totally ordered, we may assume  $A \subseteq B$ . Since  $B \trianglelefteq R$ ,  $a - b, ra, ar \in B$ . Then  $a - b, ra, ar \in J$  so  $J$  is an ideal of  $R$ . Suppose that  $J = R$ . Then  $1 \in J$  so  $1 \in A$  for some  $A \in Y$ , but  $A$  is a proper ideal, which is a contradiction. Thus  $J \neq R$  and so  $J \in X$ . In addition, for  $A \in Y$ ,  $A \subseteq J$  by construction, therefore  $J$  is an upper bound for  $Y$  in  $X$ . Since  $Y$  was arbitrary, it follows from Zorn's lemma that  $X$  has

a maximal element. ♡

**Lemma 6.4.13.** *Let  $R$  be unital ring, then  $P$  is a prime ideal of  $R$  if and only if for all  $A, B \trianglelefteq R$ , we have  $AB \subseteq P$  imply  $A \subseteq P$  or  $B \subseteq P$ .*

*Proof.* Suppose  $P$  is prime. Then, for all  $a, b \in R$ , we have  $aRb = \{arb : r \in R\} \subseteq P$  imply  $a \in P$  or  $b \in P$ . Thus, suppose  $A, B$  are two ideals such that  $AB \subseteq P$ . Suppose  $B \not\subseteq P$ , we will show  $A \subseteq P$ . Indeed, since  $B \not\subseteq P$ , there exists  $b \in B$  and  $b \notin P$ . However,  $ab \in AB$  for all  $a \in A$  and so  $a \in P$  as  $ab \in aRb$  where  $R$  is unital and  $b \notin P$ . Hence  $A \subseteq P$ .

Conversely, suppose for all  $A, B \trianglelefteq R$ , we have  $AB \subseteq P$  imply  $A \subseteq P$  or  $B \subseteq P$ . Suppose  $aRb \subseteq P$ . Suppose  $b \notin P$ , we will show  $a \in P$ . Since  $b \notin P$ , we have  $Rb$  is an ideal and  $Rb \not\subseteq P$  as  $1b = b \in Rb$ . Next, note  $aRb = aRRb$  as  $R = R^2$  since  $R$  is unital. Indeed, let  $x \in R$ , then  $x = 1x \in RR$  so  $R \subseteq RR$ . Let  $x \in RR$ , then  $x = \sum_{i=1}^n a_i b_i$  for  $a_i, b_i \in R$  and  $n \in \mathbb{N}$ . Thus  $x \in R$  as the operation on  $R$  is closed and so  $RR \subseteq R$  and  $RR = R$ . Thus, we have  $aRb = aRRb \subseteq P$  and since  $Rb \not\subseteq P$ , we must have  $aR \subseteq P$  and in particular, we have  $a1 \in P$  and so  $a \in P$ . ♡

**Example 6.4.14.** Let  $R$  be commutative and unital ring. Let

$$I = \bigcap \{P : P \trianglelefteq R \text{ is prime}\}$$

Show that every element of  $I$  is nilpotent.

*Solution.* It suffice to show  $x$  is not nilpotent imply there exists prime ideal  $P$  so that  $x \notin P$ .

Suppose  $x$  is not nilpotent. Let  $\mathfrak{S}$  be the set of ideals that does not contain  $x^n$  for all  $n \in \mathbb{N}$ . Namely,

$$\mathfrak{S} = \{P \trianglelefteq R : \forall n \in \mathbb{N}, x^n \notin P\}$$

Note  $(\mathfrak{S}, \subseteq)$  is a poset and  $\mathfrak{S}$  is not empty as  $x$  is not nilpotent and so  $\langle 0 \rangle \in \mathfrak{S}$  (indeed,  $x^n \neq 0$  for all  $n \in \mathbb{N}$ ). Let  $\mathfrak{A}$  be a arbitrary totally ordered subset of  $\mathfrak{S}$ , let  $T = \bigcup_{X \in \mathfrak{A}} X$ . First, note  $x^n \notin T$  for all  $n \in \mathbb{N}$  as every  $X$  does not contain the power of  $x$ . Let  $z, y \in T$ , then  $\exists Z, Y \in \mathfrak{A}$  and  $z \in Z, y \in Y$ . In particular, this imply  $Z \subseteq Y$  or  $Y \subseteq Z$ . Thus  $z, y$  are both in  $Z$  or  $Y$ , say  $z, y \in Z$  (without lose of generality), thus  $z - y \in X$  and so  $z - y \in T$ . Let  $z \in T$  and  $y \in R$  be arbitrary, thus  $z \in Z$  for some  $Z \in \mathfrak{A}$ , hence  $yz = zy \in Z$  and so  $yz = zy \in T$ . Hence,  $T$  is a ideal of  $R$  and  $x^n \notin T$  for all  $n \in \mathbb{N}$ . Next, note  $X \in \mathfrak{A}$  imply  $X \subseteq T$ . Thus, every totally ordered subset of  $\mathfrak{S}$  has a upper bound. Hence, there exists a maximal element  $M \in \mathfrak{S}$ .

Nest, we show  $M$  is a prime ideal. Let  $A, B \trianglelefteq R$ , suppose  $AB \subseteq M$ . Suppose  $A \not\subseteq P$  and  $B \not\subseteq P$  for a contradiction. Since  $A \not\subseteq M$ , we claim  $\exists n \in \mathbb{N}$  so  $x^n \in A$ . Indeed, if  $\forall n \in \mathbb{N}, x^n \notin A$ , we have  $A \in \mathfrak{S}$  and so  $A \subseteq M$  as  $M$  is the maximal element in  $\mathfrak{S}$ . Similarly, since  $B \not\subseteq M$ , there exists  $m \in \mathbb{N}$  so  $x^m \in B$ . In particular,

this imply  $x^{n+m} \in AB$  and thus  $x^{n+m} \in M$ , which is a contradiction. Hence, we must have  $A \subseteq P$  or  $B \subseteq M$  and so  $M$  is a prime ideal.

This imply  $I \subseteq M$  and thus  $I$  does not contain  $x$ . Thus, by contrapositive, we have every element of  $I$  is nilpotent. ♠

**Definition 6.4.15.** Let  $R$  be unital and let  $I$  be proper ideal of  $R$ .  $P \trianglelefteq R$  is called **minimal prime ideal over  $I$**  if  $I \subseteq P$  and whenever  $P'$  is a prime ideal of  $R$  such that  $I \subseteq P' \subseteq P$  then  $P' = P$ .

**Lemma 6.4.16.** Let  $A, B, C$  be ideals of unital ring  $R$ . If  $B + C = R$  then  $A(B + C) = AB + AC$ . Similarly, we have  $A + B = R$  then  $(A + B)C = AC + BC$ .

*Proof.* Let  $x \in A(B + C)$ , we have  $x = \sum_{i=1}^n a_i t_i$  for  $a_i \in A$  and  $t_i \in B + C$  and  $n \in \mathbb{N}$ . Thus, for each  $t_i$ , there exists  $b_i \in B, c_i \in C$  so  $t_i = b_i + c_i$ . Thus  $x = \sum_{i=1}^n a_i(b_i + c_i) = \sum_{i=1}^n a_i b_i + a_i c_i = \sum_{i=1}^n a_i b_i + \sum_{i=1}^n a_i c_i \in AB + AC$ .

Conversely, let  $x \in AB + AC$ , we have  $x = \sum_{i=1}^n a_i b_i + \sum_{i=1}^n \alpha_i c_i$  for  $a_i, \alpha_i \in A, b_i \in B, c_i \in C$ . In particular, since  $A$  is an ideal, we have  $a_i b_i = a'_i$  for some  $a'_i \in A$  for all  $1 \leq i \leq n$ . Similarly, we have  $\alpha_i c_i = \alpha'_i$  for some  $\alpha'_i \in A$  for all  $1 \leq i \leq n$ . Thus,  $x = \sum_{i=1}^n a'_i + \alpha'_i = \sum_{i=1}^n (a'_i + \alpha'_i)1$ , note  $1 = b + c$  for some  $b \in B$  and  $c \in C$  as  $B + C = R$ , so indeed, we have  $x = \sum_{i=1}^n t_i(b + c)$  where  $t_i \in A$  and  $b + c = 1 \in B + C$ . Thus  $A(B + C) = AB + AC$ .

A proof to show  $(A + B)C = AC + BC$  is almost identical. ♡

**Proposition 6.4.17.** In a unital ring  $R$ , every maximal ideal  $M$  is prime.

*Proof.* We will show  $A \not\subseteq M$  and  $B \not\subseteq M$  imply  $AB \not\subseteq M$ , then by contrapositive, we must have  $M$  is prime. First note  $R = R^2$ . Indeed, let  $x \in R$ , then  $x = 1x \in RR$  so  $R \subseteq RR$ . Let  $x \in RR$ , then  $x = \sum_{i=1}^n a_i b_i$  for  $a_i, b_i \in R$  and  $n \in \mathbb{N}$ . Thus  $x \in R$  as the operation on  $R$  is closed and so  $RR \subseteq R$  and  $RR = R$ .

Next, we note  $A + M = B + M = R$ . Indeed, note  $A + M$  is an ideal and  $M \subseteq A + M$ , thus  $A + M = R$  as  $A \not\subseteq M$  and so  $A \neq M$ . Similarly we would get  $B + M = R$ . Thus, note  $MB, AM, MM \subseteq M$  as  $M$  is an ideal, we have

$$\begin{aligned} R &= RR = (A + M)(B + M) \\ &= (A + M)B + (A + M)M \\ &= AB + MB + AM + MM \\ &\subseteq M + AB \\ &\subseteq R \end{aligned}$$

This imply  $R \subseteq M + AB$  and  $M + AB \subseteq R$  and so  $M + AB = R$ . In particular, note  $M \neq R$ , we must have  $AB \not\subseteq M$  (indeed, if  $AB \subseteq M$  then  $AB + M = M$  and so  $M = R$ , which would be a contradiction). Thus, by contrapositive, we have  $M$  is prime. ♡

**Example 6.4.18.** Let  $R = 2\mathbb{Z}$ , then we have  $I = 4\mathbb{Z}$  is maximal but not prime. First note  $4\mathbb{Z}$  is not prime as  $(2\mathbb{Z})(2\mathbb{Z}) \subseteq 4\mathbb{Z}$  but  $2\mathbb{Z} \not\subseteq 4\mathbb{Z}$ . Next, suppose  $I \subset J \subseteq R$ , we will show  $J = R$ . Then, there exists  $k \in \mathbb{Z}$  so that  $4k + 2 \in J$ , as if such  $k$  does not exist, we have  $J = I$ . Thus  $4k + 2 - 4k \in J$  as  $4k \in I$  and  $I \subset J$  and  $J$  is a ring. Hence  $J = R$  as  $R = \langle 2 \rangle$  and  $2 \in J$ .

**Proposition 6.4.19.** Let  $R$  be unital, then for every proper ideal  $I \subseteq R$ , the minimal prime ideal exists.

*Proof.* Let  $I$  be a proper ideal of  $R$ . Let  $\mathcal{S} = \{P \subseteq R : I \subseteq P, P \text{ is prime ideal}\}$ .

Note every proper ideal  $I$  of unital ring  $R$  is contained in a maximal ideal. In particular, since every maximal ideal is prime, we know  $\mathcal{S}$  is not empty.

We note  $\supseteq$  is a partial order on  $\mathcal{S}$ , so  $(\mathcal{S}, \supseteq)$  is a poset. Next, let  $\mathcal{T}$  be a totally ordered subset of  $\mathcal{S}$ , we let  $J = \bigcap_{A \in \mathcal{T}} A$ , we will show  $J \in \mathcal{S}$  and  $J$  is an upper bound for  $\mathcal{T}$ . Note  $A \in \mathcal{T}$  then  $A \supseteq J$  by the way we constructed it, thus, it suffice for us to show that  $J \in \mathcal{S}$ . That is, we need to show  $J \subseteq R$  and  $I \subseteq J$  and  $J$  is prime.

First, we note if  $A, B \subseteq R$  then  $A \cap B \subseteq R$  (Let  $x \in R$  and  $y \in A \cap B$  be arbitrary, then  $xy, yx \in A$  and  $xy, yx \in B$  as  $A, B$  are both ideals. Hence  $xy, yx \in A \cap B$ . Next, note  $x, y \in A \cap B$  then  $x - y \in A$  and  $x - y \in B$  so  $x - y \in A \cap B$ . Thus  $A \cap B$  is an ideal). Hence,  $J$  is indeed an ideal as it is the intersection of ideals. Next, since  $A \in \mathcal{T}$  then  $I \subseteq A$ , we have  $x \in I$  then  $x \in A$  for all  $A \in \mathcal{T}$ . Hence  $x \in J$ . Since  $x$  was arbitrary, we have  $I \subseteq J$ .

Next, we show  $J$  is prime ideal. Suppose  $a, b \in R$  and  $aRb \subseteq J$ . Suppose  $a \notin J$ , we will show  $b \in J$ . Note  $aRb \subseteq J$  then  $aRb \subseteq A$  for all  $A \in \mathcal{T} \subseteq \mathcal{S}$ . Hence  $A$  is prime ideal and note  $aRb \subseteq J \subseteq A$ . Thus  $a \in A$  or  $b \in A$  for all  $A \in \mathcal{T}$ . In particular, suppose  $a \in A$  for all  $A \in \mathcal{T}$ , then  $a \in J$ , which would be a contradiction and so there is at least one element  $A_b$  of  $\mathcal{T}$  that does not contain  $a$  and so  $b \in A_b$ . Then, suppose for a contradiction, that there exists  $A'_b \in \mathcal{T}$  such that  $b \notin A'_b$ . This would imply  $a \in A'_b$ . Since  $\mathcal{T}$  is a totally ordered subset of  $\mathcal{S}$ , we note  $A'_b$  must be a subset of some elements in  $\mathcal{T}$  and a supset of the rest of the elements in  $\mathcal{T}$ . In particular, we have either  $A_b \supseteq A'_b$  or  $A'_b \supseteq A_b$ . Note  $A_b \supseteq A'_b$  imply  $a \in A_b$ , which is a contradiction.  $A'_b \supseteq A_b$  would imply  $b \in A'_b$ , which is a contradiction. Thus, all elements of  $\mathcal{T}$  contains  $b$ . Thus  $b \in J$  and so  $J$  is a prime ideal. Therefore,  $J \in \mathcal{S}$  and hence  $\mathcal{T}$  has upper bound  $J$ . Since  $\mathcal{T}$  was arbitrary, by Zorn's lemma, there exists an element  $P \in \mathcal{S}$  such that for all  $X \in \mathcal{S}$ , we have  $X \supseteq P$ . Note  $P$  is an prime ideal containing  $I$  as  $P \in \mathcal{S}$ .

We claim  $P$  is the prime ideal we are looking for. Indeed, suppose we have  $P' \subseteq R$  such that  $I \subseteq P' \subseteq P$  and  $P'$  is prime ideal. Then  $P' \in \mathcal{S}$  and so  $P' \supseteq P$ . Thus  $P' = P$ . ♥

**Remark 6.4.20.** Let  $R$  be a ring, let  $I, J \subseteq R$ . Then  $I + J \subseteq R$ .

**Proposition 6.4.21.** Let  $R$  be a commutative unital ring. Let  $M \subseteq R$  be proper. Then  $R/M$  is a field if and only if  $M$  is maximal.

*Proof.* Suppose  $R/M$  is a field and let  $I$  be an ideal of  $R$  properly containing  $M$ . Let  $a \in I, a \notin M$ . Then  $a + M$  is not the zero element of  $R/M$ , and so  $(a + M)(b + M) = 1 + M$  for some  $b \in R$  as  $R/M$  is a field. Then  $ab - 1 \in M$ . Let  $m = ab - 1$ . Now we have  $1 = ab - m$  so  $1 \in I$  since  $a \in I$  and  $m \in I$ . It follows  $I = R$  and so  $M$  is a maximal ideal of  $R$ .

Suppose  $M$  is maximal. Then  $M \neq R$  and  $R/M$  is commutative and unital. Let  $0 + M \neq a + M \in R/M$ . Then  $a \notin M$ . Let  $J = M + \langle a \rangle \supset I$ . Since  $M$  is maximal,  $J = M + \langle a \rangle = R$ . Then  $1 \in J$  so there exists  $x \in M, b \in R$  such that  $1 = x + ab$ , which imply  $1 + M = (x + ab) + M$  and so  $1 + M = ab + M$  as desired. Since every  $a + M$  is invertible,  $R/M$  is a field.

♡

**Example 6.4.22.** Let  $1 \neq d \in \mathbb{Z}$  be square-free. Let  $\{0\} \neq P \leq \mathbb{Z}[\sqrt{d}]$  be a prime ideal. Show that  $P$  is maximal.

*Solution.* Let  $R = \mathbb{Z}[\sqrt{d}]$ . Let  $0 \neq a + d\sqrt{d} \in P$ . Then  $(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}$  and  $a^2 - db^2 \neq 0$ . Let  $a^2 - db^2 = N$ , then  $N \in P$ . Since  $R/P$  is an integral domain, we must have  $\overline{N} = \overline{0}$ . Then  $R/P \subseteq \{\overline{a} + \overline{b\sqrt{d}} : 0 \leq a, b < N\}$  is finite. Therefore it is a field and so  $P$  is maximal. ♠



# Chapter 7

## Different Kinds of Domains

### 7.1 Euclidean Domain

**Definition 7.1.1.** Let  $R$  be an integral domain, a **norm** on  $R$  is a function  $N : R \rightarrow \mathbb{N} \cup \{0\}$  such that  $N(0) = 0$ .

**Definition 7.1.2.** Let  $R$  be an integral domain, we say  $R$  is a **Euclidean domain** if there exists a norm  $N$  on  $R$  such that for all  $a, b \in R$  where  $b \neq 0$ , there exists  $q, r \in R$  such that  $a = bq + r$  with  $r = 0$  or  $N(r) < N(b)$ .

**Example 7.1.3.**

1. Let  $R = \mathbb{Z}$  and  $a, b \in \mathbb{Z}$  with  $b \neq 0$ . We have  $a = bq + r$  with  $0 \leq r < |b|$  with  $N(x) = |x|$ .
2. Let  $F$  be a field and  $R = F[x]$ . Then,  $R$  is a Euclidean domain with  $N(f(x)) = \deg(f(x))$ .
3. Let  $F$  be a field. Let  $a, b \in F$  with  $b \neq 0$ , then  $F$  is Euclidean domain with  $N(x) = 0$  is a norm. Indeed,  $a = b(b^{-1}a) + (0)$  for all  $a \in F$  and  $0 \neq b \in F$ .

**Example 7.1.4.** Show  $R = \mathbb{Z}[i]$  is a Euclidean domain with  $N(a + bi) = a^2 + b^2$ .

*Solution.* Let  $x = a + bi$  and  $y = c + di \in R$  with  $y \neq 0$ . Note  $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$  is a field. Then,  $xy^{-1} = \alpha + \beta i \in \mathbb{Q}(i)$  and let  $p + qi \in \mathbb{Z}[i]$  such that  $|p - \alpha| \leq \frac{1}{2}$  and  $|q - \beta| \leq \frac{1}{2}$ . Therefore, denote  $r := -y(p + qi) + x$ , we have  $x = y(p + qi) + r$ . Note  $r = x - y(p + qi) = y(\alpha + \beta i) - y(p + qi) = y((\alpha - p) + (\beta - q)i)$ , therefore,  $r = 0$  or  $N(r) = N(y)N((\alpha - p) + (\beta - q)i) = N(y)((\alpha - p)^2 + (\beta - q)^2) \leq \frac{1}{2}N(y) < N(y)$ . Thus,  $r = 0$  or  $N(r) < N(y)$  with  $x = y(p + qi) + r$ . ♠

**Proposition 7.1.5.** Let  $d \in \mathbb{Z}$  be square-free,  $d \neq 1$ . Let  $R = \mathbb{Z}[\sqrt{d}]$ , we have  $N(a + b\sqrt{d}) = |a^2 - db^2|$  is a norm of  $R$  with  $N(x) = 0$  if and only if  $x = 0$  and  $N(ab) = N(a)N(b)$ . Moreover,  $x \in R$  is a unit if and only if  $N(x) = 1$ .

*Proof.* We first show  $N(x) = 0$  if and only if  $x = 0$ . Suppose  $N(x) = 0$  where  $x = a + b\sqrt{d}$ . Suppose, for a contradiction, that  $a \neq 0$  or  $b \neq 0$ . Note if  $a \neq 0$



and  $b = 0$ , we must have  $N(x) = a^2$  which would not be 0, so impossible. If  $b \neq 0$  and  $a = 0$ , then we must have  $N(x) = db^2 > 0$ , so impossible. Therefore, we must have  $a \neq 0$  and  $b \neq 0$  as we assumed  $a \neq 0$  or  $b \neq 0$ . If  $a \neq 0$  and  $b \neq 0$ ,  $|a^2 - db^2| = 0 \Rightarrow a^2 - db^2 = 0 \Rightarrow a^2 = db^2 \Rightarrow d = (\frac{a}{b})^2$  (note it is still an integer as we assumed  $a^2 - db^2 = 0$  and it is well-defined). In particular, since  $\frac{a}{b}$  is a non-zero integer (as  $a \neq 0$ ) and  $d \neq 1$ , we have  $|\frac{a}{b}| > 1$  and so there exists a prime  $p$  such that  $p \mid |\frac{a}{b}|$ . Hence, this imply  $p^2 \mid d$ , which is a contradiction as  $d$  is square-free. Therefore, we must have  $a = b = 0$ .

Conversely, suppose  $x = 0$ , then  $N(x) = |0^2 - d \cdot 0^2| = 0$ .

Then, we show  $N(xy) = N(x)N(y)$ . Let  $x = a + b\sqrt{d}$  and  $y = \alpha + \beta\sqrt{d}$ . Then  $xy = (a\alpha + b\beta d) + (a\beta + b\alpha)\sqrt{d}$ . Thus,

$$\begin{aligned} N(xy) &= |(a\alpha + b\beta d)^2 - d(a\beta + b\alpha)^2| \\ &= |a^2\alpha^2 + b^2\beta^2d^2 - a^2\beta^2d - b^2\alpha^2d| \\ &= |a^2\alpha^2 - b^2\alpha^2d + b^2\beta^2d^2 - a^2\beta^2d| \\ &= |\alpha^2(a^2 - db^2) - \beta^2d(-b^2d + a^2)| \\ &= |(a^2 - db^2)(\alpha^2 - d\beta^2)| \\ &= |a^2 - db^2| \cdot |\alpha^2 - d\beta^2| = N(x)N(y) \end{aligned}$$

At last, suppose  $x = a + b\sqrt{d}$  is a unit, then  $\exists y \in R$  such that  $y = \alpha + \beta\sqrt{d}$  and  $xy = 1$ . In particular, we have  $N(xy) = 1 = N(x)N(y)$  where  $N(x), N(y) \in \mathbb{N} \cup \{0\}$ . Therefore,  $N(x) = N(y) = 1$ .

Conversely, suppose  $N(x) = 1$ , then  $|a^2 - db^2| = 1 \Rightarrow (a^2 - db^2 = 1) \vee (a^2 - db^2 = -1)$ . Suppose  $a^2 - db^2 = 1$ , then  $(a - b\sqrt{d})(a + b\sqrt{d}) = 1$  and so  $y = a - b\sqrt{d}$  would give us  $xy = 1$  and so  $x$  is a unit.

Suppose  $a^2 - db^2 = -1$ , then  $db^2 - a^2 = 1 \Rightarrow (b\sqrt{d} - a)(b\sqrt{d} + a) = 1$  and so  $y = -a + b\sqrt{d}$  would give us  $xy = 1$  and so  $x$  is a unit.  $\heartsuit$

**Proposition 7.1.6.** *If  $R$  is a Euclidean domain, then every ideal of  $R$  is principal.*

*Proof.* Let  $I \trianglelefteq R$ . If  $I = \langle 0 \rangle$  then we are done. Otherwise, take  $0 \neq x \in I$  to be the element with smallest norm. We claim  $I = \langle x \rangle$ . Clearly  $\langle x \rangle \subseteq I$ . Next, take  $y \in I$ , there exists  $q, r \in R$  such that  $y = qx + r$  with  $r = 0$  or  $N(r) < N(x)$ . Since  $r = y - qx \in I$ , we have  $r = 0$  as  $x$  has the smallest norm in  $I$ . Thus,  $I \subseteq \langle x \rangle$ .  $\heartsuit$

**Definition 7.1.7.** Let  $R$  be commutative and unital, let  $a, b \in R$  with  $b \neq 0$ . Then  $b$  is said to **divide**  $a$  or be a **divisor** of  $a$ , written  $b \mid a$ , if  $a = bx$  for some  $x \in R$ .

**Definition 7.1.8.** Let  $R$  be commutative and unital, let  $a, b \in R$ . Then a **greatest common divisor** (gcd) of  $a$  and  $b$  is a nonzero element  $d$  such that  $d \mid a$  and  $d \mid b$ , and for all  $z \in R$ , if  $z \mid a$  and  $z \mid b$  then  $z \mid d$ .

**Proposition 7.1.9.** *Let  $R$  be commutative and unital. Let  $a, b \in R$  be non-zero. If  $I = \langle a, b \rangle$  is principal, then  $I = \langle d \rangle$  for any gcd of  $a$  and  $b$ .*

*Proof.* Suppose  $I = \langle a, b \rangle = \langle d \rangle$ . Then,  $a, b \in \langle d \rangle$  and thus  $d$  is a common divisor of  $a$  and  $b$ . Let  $c \in R$  be a common divisor of  $a, b$ , thus  $a, b \in \langle c \rangle$  and so  $\langle a, b \rangle \subseteq \langle c \rangle$ . Thus,  $\langle d \rangle \subseteq \langle c \rangle \Rightarrow d \in \langle c \rangle$  and so  $c|d$  and thus  $d$  is a gcd of  $a$  and  $b$ .

Let  $d'$  also be a gcd of  $a, b$ , therefore,  $d'|d$  and  $d|d'$ . Thus  $\langle d \rangle \subseteq \langle d' \rangle$  and  $\langle d' \rangle \subseteq \langle d \rangle$  and so  $I = \langle d \rangle = \langle d' \rangle$ . ♡

**Definition 7.1.10.** Let  $R$  be commutative and unital. We say  $a, b \in R$  are **associates** if  $a = ub, u \in R^\times$ .

**Proposition 7.1.11.** Let  $R$  be integral domain. Let  $a, b \in R$ , then  $a, b$  are associates iff  $\langle a \rangle = \langle b \rangle$ . If  $a, b$  are non-zero and  $d, d'$  are gcd's of  $a, b$  then  $d$  and  $d'$  are associates.

*Proof.* Homework ♡

**Remark 7.1.12.** Let  $R$  be commutative and unital, let  $\langle a, b \rangle = \langle d \rangle$  where  $a, b$  are non-zero. Then,  $d = ax + by$ , where  $x, y \in R$ .

**Theorem 7.1.13 (Euclidean Algorithm).** Let  $R$  be an Euclidean domain, let  $a, b \in R$  and they are non-zero. If  $b | a$ , then  $\gcd(a, b) = b$ . If  $b \nmid a$ , then

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0q_1 + r_1 \\ r_0 &= r_1q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \text{ where } r_n \neq 0 \\ r_{n-1} &= r_nq_{n+1} + 0 \end{aligned}$$

and we have  $r_n$  is a gcd of  $a$  and  $b$ .

*Proof.* Indeed, note  $N(b) > N(r_0) > \dots \geq 0$ , thus the chain must stop at one point. ♡

**Example 7.1.14.** Let  $f(x) = x^5 + x^2 + x + 1$  and  $g(x) = x^3 + x^2 + x + 1$  in  $\mathbb{Z}_2[x]$ , compute  $\gcd(f(x), g(x))$ .

**Example 7.1.15.** Note  $f(x) = (x^2 - x)g(x) + (x^2 + 2x + 1) = (x^2 - x)g(x) + (x^2 + 1)$ . Let  $r_0(x) = x^2 + 1$ . Next, we have  $g(x) = (x + 1)r_0(x) + 0$ , thus  $x^2 + 1$  is a gcd.

**Example 7.1.16.** Show that  $\mathbb{Z}[-2]$  is Euclidean domain.

*Solution.* Let  $N(a + b\sqrt{-2}) = |a^2 + 2b^2|$ , we first note  $N : \mathbb{Z}[\sqrt{-2}] \rightarrow \mathbb{N} \cup \{0\}$  with  $N(0 + 0\sqrt{-2}) = 0$ . We show  $\mathbb{Z}[\sqrt{-2}]$  with  $N$  is Euclidean domain. First, we note  $N(ab) = N(a)N(b)$  for all  $a, b \in \mathbb{Z}[\sqrt{-2}]$  by Proposition 7.1.5.

Next, let  $a, b \in R := \mathbb{Z}[\sqrt{-2}]$ . Suppose  $a = x + y\sqrt{-2}$  and  $b = u + v\sqrt{-2}$ , where  $b \neq 0$ . Consider  $Q := \mathbb{Q}[\sqrt{-2}]$ , we have  $b' = \frac{u}{u^2+2v^2} - \frac{v}{u^2+2v^2}\sqrt{-2}$  and  $bb' = b'b = 1$ .

Thus  $b' = b^{-1}$ . Let  $ab^{-1} = \alpha + \beta\sqrt{-2} \in Q$ , let  $p, q \in \mathbb{Z}$  so that  $|p - \alpha| \leq \frac{1}{2}$  and  $|q - \beta| \leq \frac{1}{2}$ . Let  $r = a - b(p + q\sqrt{-2})$ , then we have

$$a = a - b(p + q\sqrt{-2}) + b(p + q\sqrt{-2}) = b(p + q\sqrt{-2}) + r$$

Next, note  $a = ab^{-1}b$ , so

$$\begin{aligned} r &= ab^{-1}b - b(p + q\sqrt{-2}) \\ &= b(\alpha + \beta\sqrt{-2}) - b(p + q\sqrt{-2}) \\ &= b(\alpha - p + (\beta - q)\sqrt{-2}) \end{aligned}$$

It suffice to show  $0 \leq N(r) \leq N(b)$ . Note

$$\begin{aligned} N(r) &= N(b(\alpha - p + (\beta - q)\sqrt{-2})) \\ &= N(b)N(\alpha - p + (\beta - q)\sqrt{-2}) \\ &= N(b)|(\alpha - p)^2 + 2(\beta - q)^2| \\ &\leq N(b) \cdot \left(\frac{1}{4} + \frac{1}{2}\right) = \frac{3}{4}N(b) \\ &< N(b) \end{aligned}$$

Thus,  $R$  is indeed Euclidean domain with our defined  $N(x)$ . ♠

## 7.2 Principal Ideal Domain

**Definition 7.2.1.** Let  $R$  be an integer domain, we say  $R$  is a **principal ideal domain**(PID), if every ideal of  $R$  is principal.

**Remark 7.2.2.** Let  $R$  be PID,  $0 \neq a, b \in R$ ,  $\langle a, b \rangle = \langle d \rangle$ , then  $d = \gcd(a, b)$  exists.

**Example 7.2.3.**

1. Euclidean domain imply PID
2. Consider  $\mathbb{Z}[x]$ . This is not a PID. Let  $I = \langle x, 2 \rangle$ , then  $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$ , thus  $I$  is maximal. Suppose  $I = \langle f(x) \rangle$ , then  $x = f(x)g(x)$  and  $2 = f(x)h(x)$ . Therefore, we must have  $\deg(f(x)) = 0$  and so  $f(x) \in \{\pm 1, \pm 2\}$ . Since  $I$  is proper,  $\langle I \rangle \neq \mathbb{Z}$  and so  $f(x) \neq \pm 1$ . Thus  $f(x) = \pm 2$ , and so  $x = \pm 2g(x)$ , which would be a contradiction.
3. Note PID does not imply Euclidean domain. Consider Dummit and Foote p.g. 277,281,282. Let  $R = \mathbb{Z}[(1 + \sqrt{-19})/2]$ , then  $R$  is PID but not Euclidean domain.

**Proposition 7.2.4.** Every nonzero prime ideal in a PID is maximal.

*Proof.* Let  $0 \neq P \subseteq R$  be prime ideal, where  $R$  is a PID. Say  $P = \langle a \rangle, a \in R$ . Let  $J \subseteq R$  such that  $P \subseteq J \subseteq R$ . Suppose  $J = \langle b \rangle, b \in R$ , thus  $a \in \langle b \rangle$ . Hence

$a = bx, x \in R$ . Since  $P$  is prime,  $b \in P$  or  $x \in P$ . If  $b \in P$ , then  $J = \langle b \rangle \subseteq P$  which imply  $P = J$ . If  $x \in P$ , then  $x = ay$  for some  $y \in R$ . Hence,  $a = bay = aby$ . Since  $a \neq 0$  as  $P \neq 0$ , and  $R$  is an integral domain, we have  $1 = by$ , which imply  $b \in R^\times$ , which in turn imply  $J = R$ .  $\heartsuit$

**Example 7.2.5.** Note  $\mathbb{Z}$  is a PID, and  $\langle 0 \rangle$  is prime but not maximal.

**Proposition 7.2.6.** Let  $R$  be a ring, then  $R[x]$  is a PID if and only if  $R$  is a field.

*Proof.* ( $\Leftarrow$ ) Done

( $\Rightarrow$ ) Suppose  $R[x]$  is a PID, then  $R$  is an integral domain. Thus,  $R[x]/\langle x \rangle \cong R$  which imply  $\langle x \rangle$  is prime. Therefore,  $\langle x \rangle$  is maximal as we are in a PID. Thus  $R$  is a field as  $R \cong R[x]/\langle x \rangle$ .  $\heartsuit$

**Definition 7.2.7.** Let  $R$  be an integral domain, let  $x \in R$  be non-zero and not a unit, then

1. we say  $x$  is **irreducible** if whenever  $x = ab$ ,  $a, b \in R$ , then  $a \in R^\times$  or  $b \in R^\times$ , otherwise, we say  $x$  is **reducible**,
2. we say  $x$  is **prime** if whenever  $x \mid ab$  then  $x \mid a$  or  $x \mid b$ .

**Example 7.2.8.**

1. In  $\mathbb{Z}$ , the primes are  $\pm p$ , where  $p$  is a prime number.
2.  $x$  is prime iff  $\langle x \rangle$  is prime and non-zero.

**Proposition 7.2.9.** Prime imply irreducible.

*Proof.* Let  $p \in R$  be prime,  $p \notin R^\times$ , and  $p \neq 0$ . Suppose  $p = ab$ , then we have  $p \mid ab$ , and so  $p \mid a$  or  $p \mid b$ .

Suppose, without loss of generality,  $p \mid a$ , we have  $a = px$ , thus  $p = ab = pxb$  and  $1 = xb$  and so  $b \in R^\times$ .  $\heartsuit$

**Proposition 7.2.10.** Let  $R$  be PID, then an element is prime if and only if irreducible.

*Proof.* It suffice to show irreducible imply prime.

Let  $p \in R$  be irreducible, then  $p \notin R^\times, p \neq 0$ . We show  $\langle p \rangle$  is prime. Let  $M$  be a maximal ideal of  $R$  which contains  $\langle p \rangle$ . Say  $M = \langle m \rangle$  where  $m \in R$ . In particular,  $p \in \langle m \rangle$  and so  $p = mx$  for some  $x \in R$ .

Note  $m \notin R^\times$  as that would make  $\langle m \rangle = R$ . Thus we have  $x \in R^\times$ , and  $p, m$  are associates. Thus  $\langle p \rangle = \langle m \rangle$  and so  $\langle p \rangle$  maximal and hence prime.  $\heartsuit$

**Proposition 7.2.11.** Let  $R$  be a PID, let  $x \in R$  be non-zero. Then  $\langle x \rangle$  is maximal if and only if  $x$  is irreducible.

*Proof.* ( $\Leftarrow$ ) Done by the last proof.

( $\Rightarrow$ )  $\langle x \rangle$  is maximal imply  $\langle x \rangle$  is prime imply  $x$  is prime and so  $x$  is irreducible.  $\heartsuit$

**Example 7.2.12.**

1. Let  $R = \mathbb{Z}[\sqrt{-5}]$ . Note  $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \times 3$ . Thus  $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ . Note there does not exist  $a, b \in \mathbb{Z}$  such that  $1 \pm \sqrt{-5} = 2(a + b\sqrt{-5})$ . Hence, 2 does not divide either one of  $1 \pm \sqrt{-5}$  and hence 2 is not a prime.
2. Let  $R = \mathbb{Z}[\sqrt{-5}]$ . We have 2 is irreducible. Indeed, note  $2 \neq 0$  and  $2 \notin R^\times$  as  $N(2) = 4 \neq 1$ . Suppose  $2 = xy$  where  $x, y \in R$ . Thus  $4 = N(x)N(y)$  and so  $N(x), N(y) \in \{1, 2, 4\}$ . Note  $N(a + b\sqrt{-5}) = a^2 + 5b^2$  and it does not have any integer solutions for  $a^2 + 5b^2 = 2$ , hence either  $N(x) = 1$  or  $N(y) = 1$ . Therefore,  $x \in R^\times$  or  $y \in R^\times$ , so we have 2 is irreducible.

**Example 7.2.13.** Let  $R = \mathbb{Z}[x, y]$  be the ring of integral polynomials in two variables  $x$  and  $y$ . Is  $R$  a PID? Is  $R$  a Euclidean domain?

*Solution.* We will show  $P = \langle 2, x \rangle$  is not principle. Suppose  $P$  is principle, then  $P = \langle f(x, y) \rangle$  where  $f(x, y) \in \mathbb{Z}[x, y]$ . Thus, we must have  $2 = g(x, y)f(x, y)$  and this happens if and only if  $g(x, y)$  and  $f(x, y)$  are both constant terms (indeed, first note  $\mathbb{Z}[x, y]$  is the same as  $(\mathbb{Z}[x])[y]$ , the polynomial ring with variable  $y$  of  $\mathbb{Z}[x]$ , in terms of the underlying set, operations, and properties. Thus, since  $\mathbb{Z}$  is integral domain, we have  $\mathbb{Z}[x]$  is integral domain, so  $\mathbb{Z}[x, y]$  is integral domain. Suppose  $f(x, y)g(x, y) = c$  where  $f, g$  are not constant, then  $f(x, y)g(x, y) - c = 0$  where  $h(x, y) = f(x, y)g(x, y) - c$  is not constant and hence not zero. A contradiction as we have  $h(x, y)x = 0$  but  $\mathbb{Z}[x, y]$  is integral domain.) Hence,  $f(x, y) = r$  where  $r \in \mathbb{Z}$ , thus  $r = \{\pm 1, \pm 2\}$ . Note  $r = \pm 1$  imply  $P = \mathbb{Z}[x, y]$ , which is obviously false. Thus  $f(x, y) = \pm 2$ . Thus  $x = \pm 2h(x, y)$  for some  $h(x, y) \in \mathbb{Z}[x, y]$ , a contradiction.

Next,  $R$  is not a Euclidean domain. Suppose for a contradiction, that  $R$  is, then  $R$  is PID, a contradiction. ♠

**Example 7.2.14.** Let  $R = \mathbb{Z}[x, y]$  be the ring of integral polynomials in two variables  $x$  and  $y$ . Let  $I = \langle x - 2y \rangle$ . Is  $I$  a prime ideal? Is  $I$  a maximal?

*Solution.*  $I = \langle x - 2y \rangle$  is prime but not maximal.

Note  $\mathbb{Z}[x, y] = (\mathbb{Z}[y])[x]$ , the polynomial ring with variable  $x$  and coefficients on  $\mathbb{Z}[y]$  (note this should be an isomorphism, if  $\mathbb{Z}[x, y]$  is defined alternatively. However, since we did not define  $\mathbb{Z}[x, y]$ , one definition of this  $\mathbb{Z}[x, y]$  is just  $\mathbb{Z}[x][y]$ ). Note  $\mathbb{Z}$  is commutative unital, we have  $\mathbb{Z}[y]$  is commutative unital. Thus, by the Lemma 6.2.6, we have  $\mathbb{Z}[x, y]/\langle x - 2y \rangle \cong \mathbb{Z}[y]$ , the underlying ring of  $(\mathbb{Z}[y])[x]$ . Since  $\mathbb{Z}[y]$  is integral domain but not a field, we have  $\langle x - 2y \rangle$  is prime but not maximal. ♠

## 7.3 Unique Factorization Domain

**Definition 7.3.1.** An integral domain  $R$  is a **unique factorization domain** (UFD) if every non-zero, non-unit can be uniquely written as a product of irreducibles in  $R$ , upto reordering and associates.

**Example 7.3.2.**

1. Let  $R = \mathbb{Z}$ , then  $30 = 2 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 2 = (-3) \cdot 5 \cdot (-2)$ .
2. Note field imply UFD.

**Proposition 7.3.3.** Let  $R$  be UFD, every irreducible is prime.

*Proof.* Let  $p \in R$  be irreducible, thus,  $0 \neq p$  and  $p \notin R^\times$ . Let  $x, y \in R$  such that  $p \mid xy$ . Thus,  $xy = pz$  for  $z \in R$ . By uniqueness in UFD,  $p$  must be an associate of an irreducible factor of  $x$  or  $y$ . Without loss of generality, say  $p = uq$  where  $u \in R^\times$  and  $q$  is an irreducible factor of  $x$ . Then  $u^{-1}p = q$  which imply  $p \mid q$  and since  $q \mid x$ , we have  $p \mid x$ .  $\heartsuit$

**Example 7.3.4.** Recall Example 7.1.16. Now, show that for  $n \geq 3$  where  $n$  is square-free, we have  $\mathbb{Z}[\sqrt{-n}]$  is not a UFD.

*Solution.* Since  $n$  is square-free, we have  $p^2 \nmid n$  for all prime  $p$ . Since  $n \in \mathbb{Z}$  and  $\mathbb{Z}$  is UFD, let  $n = \prod_{i=1}^k p_i$  where  $p_i$  are distinct primes. Note this is indeed the case as  $n$  is square-free (if it contains a prime with square, namely  $n = p^2 \prod p_i$ , then it would not be square-free).

Suppose  $2 \nmid n$ , then  $n$  is odd and so  $n+1$  is even. Therefore, we have  $n+1 = (1 + \sqrt{-n})(1 - \sqrt{-n}) = 2k$  where  $k = \frac{n}{2}$ . Clearly,  $2 \neq 1 + \sqrt{-n}$  and  $2 \neq 1 - \sqrt{-n}$ . Next, we claim  $(1 - \sqrt{-n})$  and  $(1 + \sqrt{-n})$  are irreducible. Suppose, for a contradiction,

$$1 + \sqrt{-n} = (a + b\sqrt{-n})(c + d\sqrt{-n})$$

with  $a + b\sqrt{-n}, c + d\sqrt{-n} \notin (\mathbb{Z}[\sqrt{-n}])^\times$ . Hence, we have  $a^2 + nb^2$  and  $c^2 + nd^2$  both greater than 1, and

$$\begin{aligned} N(1 + \sqrt{-n}) &= (a^2 + nb^2)(c^2 + nd^2) = n + 1 \\ \Rightarrow (ja^2 - 1) + (jb^2 - 1)n &= 0 \quad \text{with } j = c^2 + nd^2 \end{aligned}$$

Note  $j$  is greater than 1, and  $a^2, b^2$  are greater than or equal to 0. However, if  $a^2 = 0$ , then  $a = 0$  and so  $-1 + jnb^2 - n = 0$  and  $jb^2 = 1 + \frac{1}{n}$ , which is not an integer, so contradiction. If  $b^2 = 0$ , then  $b = 0$  and so  $1 + \sqrt{-n} = a(c + d\sqrt{-n}) = ac + ad\sqrt{-n}$ , by comparing coefficients, we must have  $ac \in \mathbb{Z}^\times$ , which imply  $N(a + b\sqrt{-n}) = 1$ , a contradiction. Thus,  $a^2 > 0$  and  $b^2 > 0$ . Hence, we have  $ja^2 - 1 > 0$  and  $jb^2 - 1 > 0$  as  $c + d\sqrt{-n}$  is not a unit and so  $N(c + d\sqrt{-n}) > 1$ , which imply  $(ja^2 - 1) + (jb^2 - 1)n \neq 0 \in \mathbb{Z}[\sqrt{-n}]$ , a contradiction. Thus  $1 + \sqrt{-n}$  is irreducible. Similarly, we have  $1 - \sqrt{-n}$  is irreducible. Thus,  $n+1 = (1 + \sqrt{-n})(1 - \sqrt{-n}) = 2k$  and if 2 is irreducible, we obtained a second way to factor  $n+1$ . Thus it is not UFD. Note 2 is indeed irreducible in  $\mathbb{Z}[\sqrt{-n}]$ . Suppose  $2 = (a + b\sqrt{-n})(c + d\sqrt{-n})$ ,

then  $4 = (a^2 + nb^2)(c^2 + nd^2)$ . Let  $j = c^2 + nd^2$ , then we have  $a^2 + nb^2 \mid 4$  and so  $a^2 + nb^2 = 1, 2$  or  $4$ . Note  $n \geq 3$ , so we must have  $a^2 + nb^2 = 4$ . Thus,  $a^2 = 4 - nb^2$ , which imply  $4 - nb^2$  is a positive integer and a square, and thus  $b$  must be zero or one ( $b > 1$  imply  $4 - nb^2 < 0$ ). If  $b = 0$  then  $a = \pm 1$  and so it is a unit. If  $b = \pm 1$ , then  $2 = \pm nd \pm c\sqrt{-n}$ , by comparing coefficient, we have  $\pm nd = 2$ , and this imply  $n \mid 2$ , a contradiction.

Suppose  $2 \mid n$ , then  $n$  is even. Consider  $n$ , we have  $n = -\sqrt{-n}\sqrt{-n} = 2k$  where  $2$  does not equal  $\sqrt{-n}$ , and both them are irreducibles. Indeed, we see  $2$  is irreducible, and to see  $\sqrt{-n}$  is irreducible, we have  $\sqrt{-n} = (a + b\sqrt{-n})(c + d\sqrt{-n})$  imply  $n = ja^2 + jb^2n$  where  $j = c^2 + nd^2$ . Suppose both of them are not units for contradiction. Note if  $b = 0$  then  $a \in \{1, -1\}$ , which would be a contradiction. Suppose  $b \geq 1$ , then  $ja^2 \geq 0$  and  $jb^2 - 1 > 0$  as  $j > 1$ , thus  $ja^2 + (jb^2 - 1)n = 0$  which imply  $n \neq 0$ , a contradiction. Thus  $\sqrt{-n}$  is irreducible. Thus we obtained two different factorizations (note  $2k$  is not the complete factorization, but it is enough for us to see they are different) of  $n$  and so it is not UFD. ♠

**Definition 7.3.5.** Let  $R$  be a ring, we say  $R$  is Noetherian if whenever  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$  is a chain of ideals of  $R$ , there exists  $N \in \mathbb{N}$  such that  $I_k = I_N$  for  $k \geq N$ .

**Example 7.3.6.** Consider the ring  $R = \mathbb{C}[x_1, x_2, x_3, \dots]$  be the collection of all finite polynomials with countable many variables. Then, we have  $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \dots$  and so  $R$  is not Noetherian.

**Lemma 7.3.7.** Every PID is Noetherian.

*Proof.* Suppose  $R$  is a PID, let  $I_1 \subseteq I_2 \subseteq \dots$  be a chain of ideals of  $R$ . Then,  $\bigcup_{i=1}^{\infty} I_i = I$  is an ideal of  $R$ . Say  $I = \langle a \rangle$  where  $a \in R$  as  $R$  is PID. Thus, there exists  $N \in \mathbb{N}$  such that  $a \in I_N$ , which imply  $I \subseteq I_N$ . Thus  $I_k = I_N = I$  for all  $k \geq N$ . ♥

**Theorem 7.3.8.** Every PID is UFD.

*Proof.* Let  $R$  be a PID. Let  $r \in R$  be non-zero such that  $p \notin R^\times$ .

We will show existence first. If  $r$  is irreducible then we are done. Otherwise,  $r = r_1 r_2$  where  $r_1, r_2 \notin R^\times$ . If  $r_1$  and  $r_2$  are irreducible, we are done. Otherwise, we have  $r_1$  or  $r_2$  is not irreducible. Without lose of generality,  $r_1$  is not irreducible. Thus  $r_1 = r_{11} r_{12}$  where  $r_{11}, r_{12} \notin R^\times$ . Continuing in this way,  $\langle r \rangle \subset \langle r_1 \rangle \subset \langle r_{11} \rangle \subset \dots$  Since  $R$  is Noetherian, this process must terminate. Hence, we indeed have a factorization of irreducibles of  $p$ .

We then show uniqueness. We proceed by induction on the number of irreducible factors of  $r$ , say induction on  $n$ . Say  $r = p_1 \dots p_n = q_1 \dots q_m$  where  $p_i, q_j$  are irreducibles. Since  $R$  is PID,  $p_1$  is irreducible if and only if  $p_1$  is prime. Thus  $p_1 \mid q_1 \dots q_m$ . Without lose of generality, suppose  $p_1 \mid q_1$ , and thus  $q_1 = p_1 u$  where  $u \in R$ . Since  $q_1$  is irreducible and  $p_1 \notin R^\times$ , we have  $u \in R^\times$ . Hence,  $r = p_1 \dots p_n = u p_1 q_2 q_3 \dots q_m$ . Inductively,  $p_2, \dots, p_n$  and  $q_2, \dots, q_m$  must be the same up to ordering and associates. Moreover, since  $p_1$  and  $q_1$  are associates, we are done. ♥



**Definition 7.3.9.** Let  $R$  be an integral domain, let  $X = \{(a, b) : a, b \in R, b \neq 0\}$ . Define a relation on  $X$  by  $(a, b) \sim (c, d)$  if and only if  $ad = bc$ . For each  $(a, b) \in X$ , let  $\frac{a}{b} := \{x \in X : x \sim (a, b)\}$ . Then let  $F$  denote the set of distinct sets of the form  $\frac{a}{b}$ , we obtained  $F$  is a field with the operation  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$  and  $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ , and is called **field of fractions of  $R$** .

**Theorem 7.3.10 (Gauss's lemma).** Let  $R$  be UFD, let  $F$  be the field of fractions of  $R$ . Let  $f(x) \in R[x]$ . If  $f(x) = A(x)B(x)$  for some non-constant  $A(x), B(x) \in F[x]$ , then there exists  $a(x), b(x) \in R[x]$  such that

1.  $\deg(A) = \deg(a), \deg(B) = \deg(b)$
2. and  $f(x) = a(x)b(x)$ .

*Proof.* Suppose  $f(x) = A(x)B(x)$  as in the theorem. Then, multiple through by a common denominator  $0 \neq d \in R$  for all the coefficients of  $A(x)$  and  $B(x)$ , we obtain  $df(x) = \alpha(x)\beta(x)$  where  $\alpha(x), \beta(x) \in R[x]$ . If  $d$  is a unit in  $R$ , we are done as  $a(x) = d^{-1}\alpha(x), b(x) = \beta(x)$  would be the claimed polynomials in  $R[x]$ . Thus, assume  $d \notin R^\times$ , then  $d = p_1 \dots p_n$  where  $1 \leq i \leq n$  and  $p_i$  is irreducible as  $R$  is UFD. Note in UFD, we have irreducible imply prime, so  $\langle p_i \rangle$  is prime ideal for  $1 \leq i \leq n$ . Thus,  $(R/\langle p_i \rangle)[x]$  is integral domain as  $R/\langle p_i \rangle$  is integral domain. Thus, mod  $df(x) = \alpha(x)\beta(x)$  by  $p_i$ , we have  $0 = \overline{\alpha(x)} \cdot \overline{\beta(x)}$  in  $(R/\langle p_i \rangle)[x]$ . Hence, we must have  $\overline{p_i} \mid \overline{\alpha(x)}$  or  $\overline{p_i} \mid \overline{\beta(x)}$  as  $(R/\langle p_i \rangle)[x]$  is integral domain and we must have either  $\overline{\alpha(x)} = 0$  or  $\overline{\beta(x)} = 0$ . Say  $p_i \mid \alpha(x)$ , then we can cancel  $p_i$  from both side of the equation  $df(x) = \alpha(x)\beta(x)$  in  $R[x]$ . Start with 1 and continue this process, we can cancel all of the factors of  $d$  on the left hand side of  $df(x) = \alpha(x)\beta(x)$  and so  $f(x) = a(x)b(x)$  as desired. In particular, we note  $a(x), b(x)$  are  $F$ -multiples of  $A(x), B(x)$ , respectively, i.e.  $\exists u, v \in F$  so  $a(x) = uA(x)$  and  $b(x) = vB(x)$ .  $\heartsuit$

**Corollary 7.3.10.1.** Let  $R$  be UFD and  $F$  be the field of fraction of  $R$ .

1. If  $f(x) \in R[x]$  is reducible over  $F$  then  $f(x)$  is reducible over  $R$ .
2. If  $f$  is irreducible and non-constant in  $R[x]$  then  $f(x)$  is irreducible in  $F[x]$ .

**Example 7.3.11.**

1.  $2 \in \mathbb{Z}[x]$  is irreducible, but  $2 \in \mathbb{C}[x]$  is not irreducible as it is a unit.
2.  $2x \in \mathbb{Z}[x]$  is reducible, but is not reducible in  $\mathbb{Q}[x]$ .

**Proposition 7.3.12.** Let  $R$  be UFD,  $F$  be field of fraction, and  $f(x) \in R[x]$ . Suppose a gcd of the coefficients of  $f(x)$  is 1. Then,  $f(x)$  is irreducible over  $R$  if and only if  $f(x)$  is irreducible over  $F$ .

*Proof.* ( $\Rightarrow$ ) By Gauss, corollary 2.

( $\Leftarrow$ ) Note  $f(x)$  is irreducible over  $F$ ,  $f(x) = g(x)h(x)$  in  $R[x]$ . Then,  $\deg(g) = 0$  or  $\deg(h) = 0$ . Without lose of generality, suppose  $g(x) = d \in R$ , then  $f(x) = dh(x)$ . Next, note 1 is a gcd of  $f(x)$ , so  $d$  divides every coefficients of  $f$ , thus  $d \mid 1$  and  $d \in R^\times$ .  $\heartsuit$

**Proposition 7.3.13.** Let  $R$  be UFD if and only if  $R[x]$  is UFD.



*Proof.* ( $\Leftarrow$ ) Clear.

( $\Rightarrow$ ) Suppose  $R$  is UFD. We will show existence first.

Let  $f(x) \in R[x]$  be non-zero and not a unit. If  $\deg(f) = 0$ , we are done. Assume  $\deg(f) > 0$ , let  $d$  be a gcd of the coefficients of  $f$ . Then,  $f(x) = dg(x)$  where  $g(x) \in R[x]$  and a gcd of the coefficients of  $g(x)$  is 1. Thus, it suffice to show  $g(x)$  can be factored into irreducibles, where the gcd of coefficients of  $g$  is 1.

Let  $F$  be the field of fractions of  $R$ . Then,  $F[x]$  is a UFD as  $F[x]$  is PID hence UFD. Then  $g(x) = Q_1(x) \dots Q_n(x)$  where each  $Q_i(x) \in F[x]$  is irreducible. Then,  $g(x) = p_1(x) \dots p_n(x)$  in  $R[x]$ , where  $p_i(x)$  is an F-multiple of  $Q_i(x)$ . Therefore,  $p_i(x)$  is irreducible in  $R[x]$  since a gcd of the coefficients of  $p_i(x)$  is 1. This is because a gcd of  $g(x)$  is 1. Hence,  $g(x)$  indeed can be written as a finite products of irreducibles in  $R[x]$ .

Next, we show uniqueness. Suppose  $g(x) = q_1(x) \dots q_r(x) = p_1(x) \dots p_n(x)$  in  $R[x]$  where  $q_i(x), p_j(x)$  are all irreducibles. Since the gcd of the coefficients of  $g(x)$  is 1, we have 1 is a gcd for each of the  $q_i$  and  $p_j$ . Thus,  $q_i, p_j$  are all irreducible in  $F[x]$ , and by unique factorization in  $F[x]$ , we must have  $r = n$ . Possibly after rearrangement, we have  $q_i = \frac{a_i}{b_i} p_i$ , where  $0 \neq a_i, b_i \in R$ . Thus,  $b_i q_i(x) = a_i p_i(x)$ . Since a gcd of the coefficients of  $b_i q_i(x)$  is  $b_i$  and a gcd of  $a_i p_i(x)$  is  $a_i$  and the gcds of the coefficients of a non-zero polynomial in UFD is unique up to units,  $a_i = u_i b_i$  for some unit  $u \in R$ . Thus  $q_i(x) = u_i p_i(x)$  as desired. This complete the proof.  $\heartsuit$

**Example 7.3.14.** Note  $\mathbb{Z}$  is UFD, so  $\mathbb{Z}[x]$  is UFD. Hence,  $\mathbb{Z}[x]$  is UFD but not PID.

Next,  $R$  is UFD, then  $R[x_1]$  is UFD. Thus,  $R[x_1][x_2] = R[x_1, x_2]$  is UFD and so on. Thus,  $R[x_1, \dots, x_n]$  is UFD.

# Chapter 8

## Final

**Remark 8.0.1.** Note the following inclusion:

Commutative ring  $\supset$  Integral domains  $\supset$  UFD  $\supset$  PID  $\supset$  ED  $\supset$  Fields  $\supset$  Fintie fields

**Definition 8.0.2.** We will have 7 questions.

- 4,3,3 Elementary ring theory
- 3,4,4 Prime v.s. maximal ideals
- 3,4,3 Group theory
- 2,5,3 Group actions/applications
- 3,3,4 Integral domains/ Fields
- 3,4,4 Divisibility in integral domain
- 10\*1 Gives an example.

Remember to study assignments as they will be covered in exam.