

# Artin's Algebra

Ashan Jayamal

2024-04-21



# Contents

<b>1 Matrices</b>	<b>5</b>
1.1 Basic Operations . . . . .	5
<b>2 Group Theory</b>	<b>9</b>
2.1 Laws of Compositions . . . . .	9
2.2 Groups and Subgroups . . . . .	10
2.3 Subgroups of the Additive Group of Integers . . . . .	12
2.4 Cyclic Groups . . . . .	13
2.5 Homomorphisms . . . . .	13
2.6 Isomorphisms . . . . .	14
2.7 Equivalence Relations and Partitions . . . . .	14
2.8 Cosets . . . . .	22
2.9 Modular Arithmetic . . . . .	22
2.10 The Correspondence Theorem . . . . .	22
2.11 Product Groups . . . . .	27
2.12 Quotient Groups . . . . .	33
<b>3 Vector Space</b>	<b>39</b>
3.1 Subspace of $\mathbb{R}^n$ . . . . .	39
3.2 Fields . . . . .	41
<b>4 Exercises</b>	<b>45</b>
4.1 Chapter 1 . . . . .	45
4.2 Chapter 2 . . . . .	45

<b>5 Tempoarray files for exercises</b>	<b>155</b>
5.1 Chapter 3 . . . . .	155
<b>6 Vector spaces.</b>	<b>185</b>

# Chapter 1

## Matrices

### 1.1 Basic Operations

Let  $m$  and  $n$  be positive integers. An  $m \times n$  matrix is a collection of  $mn$  numbers arranged in a rectangular array.

A handwritten diagram on a piece of paper defining an  $m \times n$  matrix. It shows a bracketed rectangular arrangement of elements  $a_{ij}$ . The top row is labeled  $a_{11} \dots a_{1n}$ , and the bottom row is labeled  $a_{m1} \dots a_{mn}$ . To the right of the matrix, the text "m rows" is written vertically. Below the matrix, the text "n columns" is written.

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

m rows

n columns

::: {.example #unnamed-chunk-1}

$$A := \begin{bmatrix} 8 & 0 & 3 \\ 78 & -5 & 2 \end{bmatrix}$$

$A$  is  $2 \times 3$  matrix.(two rows and three columns)

::: The numbers in a matrix are the matrix entries. They may be denoted by  $a_{ij}$ , where  $i$  and  $j$  are indices (integers) with  $1 < i < m$  and  $1 < j < n$ . The index  $i$  represents the row index, and  $j$  represents the column index. So  $a_{ij}$  is the entry that appears in the  $i$ th row and  $j$ th column of the matrix.

$$i \begin{bmatrix} & & j \\ & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{bmatrix}$$

Figure 1.1:

In the above example,  $a_{11} = 8$ ,  $a_{13} = 0$ , and  $a_{23} = -5$ .

We sometimes denote the matrix whose entries are  $a_{ij}$  by  $(a_{ij})$ .

### Definition 1.1.

- An  $n \times n$  matrix is called a **square matrix**. A  $1 \times 1$  matrix  $[a]$  contains a single number, and we do not distinguish such a matrix from its entry.
- A  $1 \times n$  matrix is an  $n$ -dimensional **row vector**. We drop the index  $i$  when  $m = 1$  and write a row vector as

$$[a_1 \dots a_n], \text{ or as } (a_1, \dots, a_n)$$

- . Commas in such a row vector are optional.
- Similarly, an  $m \times 1$  matrix is an  $m$ -dimensional **column vector**:

$$\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

In most of this book, we won't make a distinction between an  $n$ -dimensional column vector and the point of  $n$ -dimensional space with the same coordinates. In the few places where the distinction is useful, we will state this clearly.

**Definition 1.2** (Addition of matrices). Addition of matrices is defined in the same way as vector addition. Let  $A = (a_{ij})$  and  $B = (b_{ij})$  be two  $m \times n$  matrices. Their sum  $A + B$  is the  $m \times n$  matrix  $S = (s_{ij})$  defined by  $s_{ij} = a_{ij} + b_{ij}$ .

**Example 1.1.**

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 3 & 5 \\ 3 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 3 & 4 & 5 \\ 4 & 1 & 6 \end{bmatrix}$$

Addition is defined only when the matrices to be added have the same shape — when they are  $m \times n$  matrices with the same  $m$  and  $n$ .

**Example 1.2** (Non Example).

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 3 & 5 \\ 3 & 1 & 3 \\ 3 & 4 & 5 \end{bmatrix}$$

This two matrices can not be added.

**Definition 1.3** (Scalar Multiplication). Scalar multiplication of a matrix by a number is also defined as with vectors. The result of multiplying an  $m \times n$  matrix  $A$  by a number  $c$  is another  $m \times n$  matrix  $B = (b_{ij})$ , where  $b_{ij} = c \cdot a_{ij}$  for all  $i, j$ . Thus,

$$2 \cdot \begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix} = \begin{bmatrix} 4 & 2 & 0 \\ 2 & 6 & 10 \end{bmatrix}$$

Let's assume for now that the scalars are real numbers. In later chapters other scalars will appear. Just keep in mind that, except for occasional reference to the geometry of real two- or three-dimensional space, everything in this chapter continues to hold when the scalars are complex numbers.

**Definition 1.4** (Matrix Multiplication). The product of two matrices  $A = (a_{ij})$  and  $B = (b_{ij})$  is defined when the number of columns of  $A$  is equal to the number of rows of  $B$ . If  $A$  is an  $l \times m$  matrix and  $B$  is an  $m \times n$  matrix, then the product will be an  $l \times n$  matrix. Symbolically,

$$(l \times m) \cdot (m \times n) = (l \times n)$$

The entries of the product matrix are computed by multiplying all rows of  $A$  by all columns of  $B$ . If we denote the product matrix  $AB$  by  $P = (p_{ij})$ , then

$$p_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{im}b_{mj} \quad (1.1)$$

This is the product of the  $i$ th row of  $A$  and the  $j$ th column of  $B$ .

$$\begin{bmatrix} a_{i1} & \dots & a_{im} \end{bmatrix} \begin{bmatrix} b_{1j} \\ \vdots \\ b_{mj} \end{bmatrix} = p_{ij}$$

# Chapter 2

# Group Theory

## 2.1 Laws of Compositions

**Definition 2.1** (Law of Composition). A law of composition on a set  $S$  is any rule for combining pairs  $a, b$  of elements of  $S$  to get another element, say  $p$ , of  $S$ .

**Example 2.1.**

- Some models for this concept are addition and multiplication of real numbers.
- Matrix multiplication on the set of  $n \times n$  matrices is another example.

Formally, a law of composition is a function of two variables, or a map,

$$S \times S \rightarrow S$$

Here,  $S \times S$  denotes, as always, the product set, whose elements are pairs  $a, b$  of elements of  $S$ .

The element obtained by applying the law to a pair  $a, b$  is usually written using a notation resembling one used for multiplication or addition:

$$p = ab, a \times b, a \circ b, a + b$$

, or whatever, a choice being made for the particular law in question. The element  $p$  may be called the product or the sum of  $a$  and  $b$ , depending on the notation chosen.

## 2.2 Groups and Subgroups

**Definition 2.2** (Group). A group is a set  $G$  together with a law of composition that has the following properties:

- The law of composition is associative:  $(ab)c = a(bc)$  for all  $a, b, c$  in  $G$ .
- $G$  contains an identity element  $1$ , such that  $la = a$  and  $al = a$  for all  $a$  in  $G$ .
- Every element  $a$  of  $G$  has an inverse, an element  $b$  such that  $ab = 1$  and  $ba = 1$ .

**Notation:** If set  $G$  with composition  $\cdot$  is a group, then we denote it by  $(G, \cdot)$  :: { .definition #unnamed-chunk-11 name="Ableian Group"} Group G is called abelian if its law of composition is commutative. i.e.

$$\forall x \in G, xy = yx$$

:::

**Example 2.2.**

- $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$  is an abelian group under multiplication
- $GL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : A \text{ is invertible}\}$  with matrix multiplication is non-abelian group. This group is called *general linear group*.

**Definition 2.3** (Order of group). The order of a group  $G$  is the number of elements that it contains. We

$$|G| := \text{number of elements of } G = \text{the order of } G$$

If the order is finite,  $G$  is said to be a finite group. If not,  $G$  is an infinite group.

Here is our notation for some familiar infinite abelian groups:

**Example 2.3.**

- $(\mathbb{Z}, +)$  :The set of integers, with addition as its law of composition (the additive group of integers)
- $(\mathbb{R}, +)$  :The set of real numbers, with addition as its law of composition (the additive group of real numbers)
- $(\mathbb{R}^\times, \times)$  :The set of nonzero real numbers, with multiplication as its law of composition(the multiplicative group)  $(\mathbb{C}, +)$  :the set of complex numbers, with addition as its law of composition (the additive group of complex numbers)
- $(\mathbb{C}^\times, \times)$  :The set of nonzero complex numbers, with multiplication as its law of composition(the multiplicative group of complex numbers)

**Proposition 2.1** (Cancellation Law). *Let  $G$  be group and let  $a, b, c \in G$  whose law of composition is written multiplicatively.*

- If  $ab = ac$  or if  $ba = ca$ , then  $b = c$ .
- If  $ab = a$  or if  $ba = a$ , then  $b = 1$

*Proof.* Multiply both sides of  $ab = ac$  on the left by  $a^{-1}$  to obtain  $b = c$ . The other proofs are analogous.  $\square$

*Remark.* As you saw  $a^{-1}$  plays a major rule in above proof. So the cancellation rule does not hold when element  $a$  is not invertible.

**Example 2.4** (Example that not holding the cancellation law).

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$$

**Example 2.5.** Let  $T$  be a set and  $G := \{f : T \rightarrow T : f \text{ is a bijection}\}$ . Then  $G$  with composition is a group. We use notation  $\$sys(T)$  to denote the

**Example 2.6.** The group of permutations of the set of indices  $\{1, 2, \dots, n\}$  is called the *symmetric group*, and is denoted by  $S_n$ . Then  $|S_n| = n!$ . So,  $S_n$  is a finite group of order  $n!$ .

Let's discuss some individual cases for  $n$ .

- $n = 2$

The permutations of a set  $\{1, 2\}$  of two elements are the identity  $i$  and the transposition  $\tau = (12)$ .

$$S_2 := \{id, (12)\}$$

$$\begin{array}{ccc} \circ & id & (12) \\ \hline id & id & (12) \\ (12) & (12) & id \\ \hline \hline \end{array}$$

- $n = 3$

$S_3$  has order  $3! = 6$ .  $S_3$  serves as a convenient example because it is the smallest group whose law of composition isn't commutative. We will refer to it often. To describe it, we pick two particular permutations in terms of which we can write all others. We take the cyclic permutation  $(123)$ , and the transposition  $(12)$ , and label them as  $x$  and  $y$ , respectively. Then

$$x^3 = (123)^3 = (123)(123)(123) = (123)(132) = id \quad (2.1)$$

$$y^2 = (12)^2 = (12)(12) = id \quad (2.2)$$

$$yx = (12)(123) = (13) = (132)(12) = ((123)(123))(12) = (123)^2(123)$$

As a summary,

$$x^3 = 1, Y^2 = 1, yx = x^2y$$

## 2.3 Subgroups of the Additive Group of Integers

We review some elementary number theory here, in terms of subgroups of the additive group  $\mathbb{Z}^+$  of integers. To begin, we list the axioms for a subgroup when additive notation is used in the group: A subset  $S$  of a group  $G$  with law of composition written additively is a subgroup if it has these properties:

- *Closure* : If  $a$  and  $b$  are in  $S$ , then  $a + b$  is in  $S$ .
- *Identity* :  $0$  is in  $S$ .
- *Inverses* : If  $a$  is in  $S$  then  $-a$  is in  $S$ .

Let  $a$  be an integer different from  $0$ . We denote the subset of  $\mathbb{Z}$  that consists of all multiples of  $a$  by  $a\mathbb{Z}$ :

$$a\mathbb{Z} := \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \in \mathbb{Z}\}$$

This is a subgroup of  $\mathbb{Z}^+$ . Its elements can also be described as the integers divisible by  $a$ .

**Theorem 2.1.** *Let  $S$  be a subgroup of the additive group  $\mathbb{Z}^+$ . Either  $S$  is the trivial subgroup  $\{0\}$ , or else it has the form  $a\mathbb{Z}$ , where  $a$  is the smallest positive integer in  $S$ .*

*Proof.* Let  $S$  be a subgroup of  $\mathbb{Z}^+$ . Then  $0 \in S$ , and if  $0$  is the only element of  $S$  then  $S$  is the trivial subgroup. ie.:  $S = \{0\}$  So that case is settled.

Otherwise,  $S$  contains an integer  $n$  different from  $0$ , and either  $n$  or  $-n$  is positive. The third property of a subgroup tells us that  $-n$  is in  $S$ , so in either case,  $S$  contains a positive integer. We must show that  $S$  is equal to  $a\mathbb{Z}$ , when  $a$  is the smallest positive integer in  $S$ .

We first show that  $a\mathbb{Z}$  is a subset of  $S$ , in other words, that  $ka$  is in  $S$  for every integer  $k$ . If  $k$  is a positive integer, then  $ka = a + a + \dots + a$  ( $k$  terms). Since  $a$  is in  $S$ , closure and induction show that  $ka$  is in  $S$ . Since inverses are in  $S$ ,  $-ka$  is in  $S$ . Finally,  $0 = 0a$  is in  $S$ .

Next we show that  $S$  is a subset of  $Za$ , that is, every element  $n$  of  $S$  is an integer multiple of  $a$ . We use division with remainder to write  $n = qa + r$ , where  $q$  and  $r$  are integers and where the remainder  $r$  is in the range  $0 < r < a$ . Since  $Za$  is contained in  $S$ ,  $qa$  is in  $S$ , and of course  $n$  is in  $S$ . Since  $S$  is a subgroup,  $r = n - qa$  is in  $S$  too. Now by our choice,  $a$  is the smallest positive integer in  $S$ , while the remainder  $r$  is in the range  $0 < r < a$ . The only remainder that can be in  $S$  is  $0$ . So  $r = 0$  and  $n$  is the integer multiple  $qa$  of  $a$ .  $\square$

## 2.4 Cyclic Groups

## 2.5 Homomorphisms

**Definition 2.4.** Let  $(G, *)$  and  $(G', \odot)$  be groups. A **homomorphism**  $\phi : G \rightarrow G'$  is a map from  $G$  to  $G'$  such that for all  $a$  and  $b$  in  $G$ :

$$\phi(a * b) = \phi(a) \odot \phi(b). \quad (2.4)$$

### Examples of Homomorphisms

1. **Determinant Function:**  $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$
2. **Exponential Map:**  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^\times, \times)$  defined by  $x \mapsto e^x$
3. **Map**  $\phi : (\mathbb{Z}, +) \rightarrow G$  defined by  $\phi(n) = a^n$ , where  $a$  is a given element of  $G$
4. **Absolute Value Map:**  $|\cdot| : (\mathbb{C}^\times, \times) \rightarrow (\mathbb{R}^\times, \times)$

### Trivial Homomorphism

The trivial homomorphism  $\phi : G \rightarrow G'$  between any two groups maps every element of  $G$  to the identity in  $G'$ .

### Inclusion Map

If  $H$  is a subgroup of  $G$ , the inclusion map  $i : H \rightarrow G$  defined by  $i(x) = x$  for  $x$  in  $H$  is a homomorphism.

**Proposition 2.2.** Let  $\phi : G \rightarrow G'$  be a group homomorphism.

- (a) If  $a_1, \dots, a_k$  are elements of  $G$ , then  $\phi(a_1 \dots a_k) = \phi(a_1) \dots \phi(a_k)$ .
- (b)  $\phi$  maps the identity to the identity:  $\phi(1_G) = 1_{G'}$ .
- (c)  $\phi$  maps inverses to inverses:  $\phi(a^{-1}) = \phi(a)^{-1}$ .

**Proposition 2.3.** Let  $\phi : G \rightarrow G'$  be a homomorphism of groups, and let  $a, b \in G$ . Let  $K \ker(\phi)$ . Then following conditions are equivalent:

- $\phi(a) = \phi(b)$ ,
- $a^{-1}b$  is in  $K$ ,
- $b$  is in the coset  $aK$ ,
- The cosets  $bK$  and  $aK$  are equal.

*Proof.*

- (1)  $\Rightarrow$  (2). Suppose  $\phi(a) = \phi(b)$ . Now consider

$$\phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a^{-1})\phi(b) = 1$$

- Thus,  $a^{-1}b \in K$ .
- (2)  $\Rightarrow$  (1) If  $a^{-1}b \in K$

$$1 = \phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a^{-1})\phi(b)$$

- . Thus,  $\phi(a) = \phi(b)$ .
- Suppose  $b$  is in the coset  $aK$ . Then  $b = ak$  for some

□

## 2.6 Isomorphisms

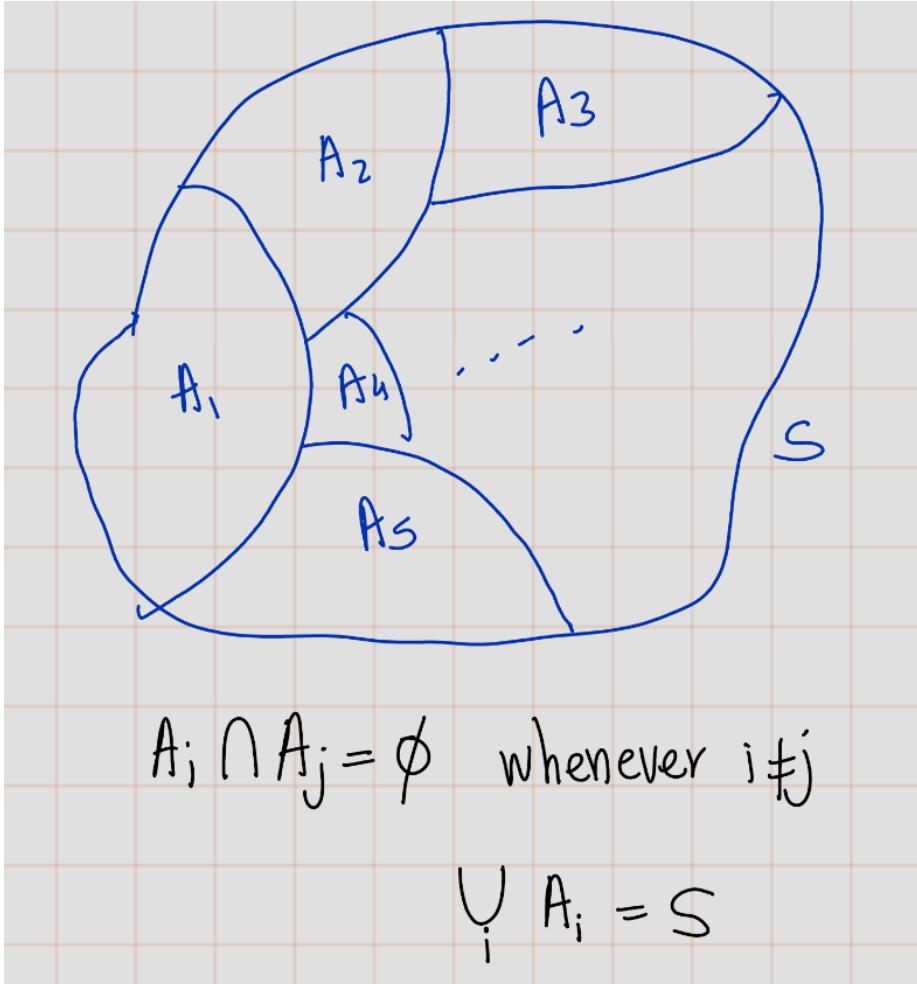
## 2.7 Equivalence Relations and Partitions

**Definition 2.5.** Sure, here is the LaTeX version of your statement:

A partition  $n$  of a set  $S$  is a subdivision of  $S$  into nonoverlapping, nonempty subsets:

$$S = \bigcup_i A_i$$

, where  $A_i$  are disjoint nonempty subsets of  $S$ .



**Example 2.7.** The two sets *Even* and *Odd* partition the set of integers.

**Example 2.8.** With the usual notation, the sets

$$\{1\}, \{y, xy, x^2y\}, \{x, x^2\}$$

form a partition of the symmetric group  $S_3$ .

**Definition 2.6.** An equivalence relation on a set  $S$  is a relation that holds between certain pairs of elements.

- Reflexive: For all  $a$ ,  $a \sim a$ .
- Symmetric: If  $a \sim b$ , then  $b \sim a$ .
- Transitive: If  $a \sim b$  and  $b \sim c$ , then  $a \sim c$ .

**Example 2.9.** Two triangles are said to be congruent if their sides have the same length and angles have same measure.

Congruence of triangles is an example of an equivalence relation on the set of triangles in the plane. If  $A, B$ , and  $C$  are triangles, and if  $A$  is congruent to  $B$  and  $B$  is congruent to  $C$ , then  $A$  is congruent to  $C$ . It is very easy to check three equivalence properties. I am not going to do this.

**Example 2.10.** Conjugacy is an equivalence relation on a group. Let  $G$  be a group. Two group elements are conjugate,  $a \sim b$ , if  $b = gag^{-1}$  for some  $g \in G$ .

- *Reflexive:* Observe that  $a = aaa^{-1}$  then,  $a \sim a$ .
- *Symmetric:* Suppose that  $a \sim b$ , then  $b = gag^{-1}$ . Thus,  $a = g^{-1}bg$ . Hence,  $b \sim a$ .
- *Transitive:* Suppose that  $a \sim b$  and  $b \sim c$ . This means that  $b = g_1ag_1^{-1}$  and  $c = g_2bg_2^{-1}$  for some group elements  $g_1$  and  $g_2$ . Then  $c = g_2(g_1ag_1^{-1})g_2^{-1} = (g_2g_1)a(g_2g_1)$ , so  $a \sim c$

**Proposition 2.4.** *An equivalence relation on a set  $S$  determines a partition of  $S$ , and conversely.*

*Proof.*

- ( $\Rightarrow$ ): Given a partition of  $S$ , the corresponding equivalence relation is defined by the rule that  $a \sim b$  if  $a$  and  $b$  lie in the same subset of the partition. The axioms for an equivalence relation are obviously satisfied.
- ( $\Rightarrow$ ): Given an equivalence relation ( $\sim$ ), one defines a partition this way: The subset that contains  $a$  is the set of all elements  $b$  such that  $a \sim b$ . This subset is called the **equivalence class** of  $a$ . We'll denote it by  $C_a$  here

$$C_a = \{b \in S | a \sim b\}$$

The next lemma completes the proof of the proposition

□

**Lemma 2.1.** *Given an equivalence relation on a set  $S$ , the subsets of  $S$  that are equivalence classes partition  $S$ .*

*Proof.* This is an important point, so we will check it carefully. We must remember that the notation  $C_a$  stands for a subset defined in a certain way. The partition consists of the subsets, and several notations may describe the same subset.

- *Non-emptiness:* The reflexive axiom tells us that  $a$  is in its equivalence class. Therefore, the class  $C_a$  is nonempty.

- *Union is whole set:* Since  $a$  can be any element, the union of the equivalence classes is the whole set  $S$ .
- *Disjoint property:* To show this, we prove following claim:
  - **Claim:** If  $C_a$  and  $C_b$  have an element in common, then  $C_a = C_b$ .  
Since we can interchange the roles of  $a$  and  $b$ , it will suffice to show that if  $C_a$  and  $C_b$  have an element, say  $d$ , in common, then  $C_b \subseteq C_a$ . Suppose that  $x$  is in  $C_b$ , then  $b \sim x$ . Since  $d$  is in both sets,  $a \sim d$  and  $b \sim d$ , and the symmetry property tells us that  $d \sim b$ . So we have  $a \sim d$ ,  $d \sim b$ , and  $b \sim x$ . Two applications of transitivity show that  $a \sim x$ , and therefore,  $x$  is in  $C_a$ .

□

**Example 2.11.** The relation on a group defined by  $a \sim b$  if  $a$  and  $b$  are elements of the same order is an equivalence relation. (Trivial.)

The corresponding partition for the symmetric group  $S_3$  are

$$\{1\}, \{y, xy, x^2y\}, \{x, x^2\}.$$

If a partition of a set  $S$  is given, we may construct a new set  $\bar{S}$  whose elements are the subsets. We imagine putting the subsets into separate piles, and we regard the piles as the elements of our new set  $\bar{S}$ . It seems advisable to have a notation to distinguish a subset from the element of the set  $S$  (the pile) that it represents. If  $U$  is a subset, we will denote by  $[U]$  the corresponding element of  $S$ .

**Example 2.12.** If  $S$  is the set of integers and if Even and Odd denote the subsets of even and odd integers, respectively, then  $\bar{S}$  contains the two elements [Even] and [Odd].

We will use this notation more generally. When we want to regard a subset  $U$  of  $S$  as an element of a set of subsets of  $S$ , we denote it by  $[U]$ .

When an equivalence relation on  $S$  is given, the equivalence classes form a partition, and we obtain a new set  $\bar{S}$  whose elements are the equivalence classes  $[C_a]$ . We can think of the elements of this new set in another way, as the set obtained by changing what we mean by equality among elements. If  $a$  and  $b$  are in  $S$ , we interpret  $a \sim b$  to mean that  $a$  and  $b$  become equal in  $\bar{S}$ , because  $C_a = C_b$ . With this way of looking at it, the difference between the two sets  $S$  and  $\bar{S}$  is that in  $\bar{S}$  more elements have been declared “equal,” i.e., equivalent. It seems to me that we often treat congruent triangles this way in school.

For any equivalence relation, there is a natural surjective map

$$\pi : S \rightarrow \bar{S} \tag{2.5}$$

that maps an element  $a$  of  $S$  to its equivalence class:  $\pi(a) = [C_a]$ . When we want to regard  $\bar{S}$  as the set obtained from  $S$  by changing the notion of equality, it will be convenient to denote the element  $[C_a]$  of  $\bar{S}$  by the symbol  $a$ . Then the map  $\pi$  becomes

$$\pi(a) = \bar{a} \quad (2.6)$$

We can work in  $\bar{S}$  with the symbols used for elements of  $S$ , but with bars over them to remind us of the new rule:

$$\text{If } a \text{ and } b \text{ are in } S, \text{ then } \bar{a} = \bar{b} \text{ means } a \sim b. \quad (2.7)$$

A disadvantage of this bar notation is that many symbols represent the same element of  $S$ . Sometimes this disadvantage can be overcome by choosing a particular element, a representative element, in each equivalence class. For example, the even and the odd integers are often represented by  $\bar{0}$  and  $\bar{1}$ :

$$\{\text{[Even]}, \text{[Odd]}\} = \{\bar{0}, \bar{1}\}. \quad (2.8)$$

Though the pile picture may be easier to grasp at first, the second way of viewing  $S$  is often better because the bar notation is easier to manipulate algebraically.

### 2.7.1 The Equivalence Relation Defined by a Map

Any map of sets  $f : S \rightarrow T$  gives us an equivalence relation on its domain  $S$ . It is defined by the rule:  $a \sim b$  if  $f(a) = f(b)$ .

**Definition 2.7** (Inverse Image and Fibers). The inverse image of an element  $t$  of  $T$  is the subset of  $S$  consisting of all elements  $s$  such that  $f(s) = t$ . It is denoted symbolically as

$$f^{-1}(t) = \{s \in S \mid f(s) = t\}. \quad (2.9)$$

The inverse images are also called the fibres of the map  $f$ , and the fibres that are not empty are the equivalence classes for the relation defined above.

*Remark.* This is symbolic notation. Please remember that **unless  $f$  is bijective,  $f^{-1}$  will not be a map**.

Here the set  $S$  of equivalence classes has another incarnation, as the image of the map. The elements of the image correspond bijectively to the nonempty fibres, which are the equivalence classes

**Example 2.13.** Let's consider the absolute value map from the complex numbers  $\mathbb{C}^\times$  to the positive real numbers  $\mathbb{R}^+$ :

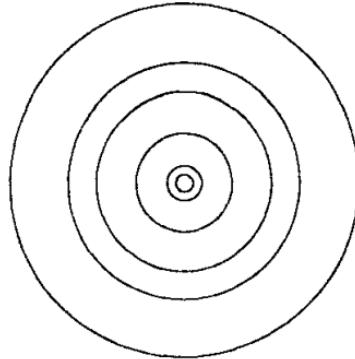
$$f : \mathbb{C}^\times \rightarrow \mathbb{R}^+, \quad f(z) = |z|$$

The fiber of an element  $t$  in  $\mathbb{R}^+$  is the subset of  $\mathbb{C}^\times$  consisting of all complex numbers  $z$  such that  $f(z) = |z| = t$ . Symbolically, we denote the fiber as:

$$f^{-1}(t) = \{z \in \mathbb{C}^\times : |z| = t\}$$

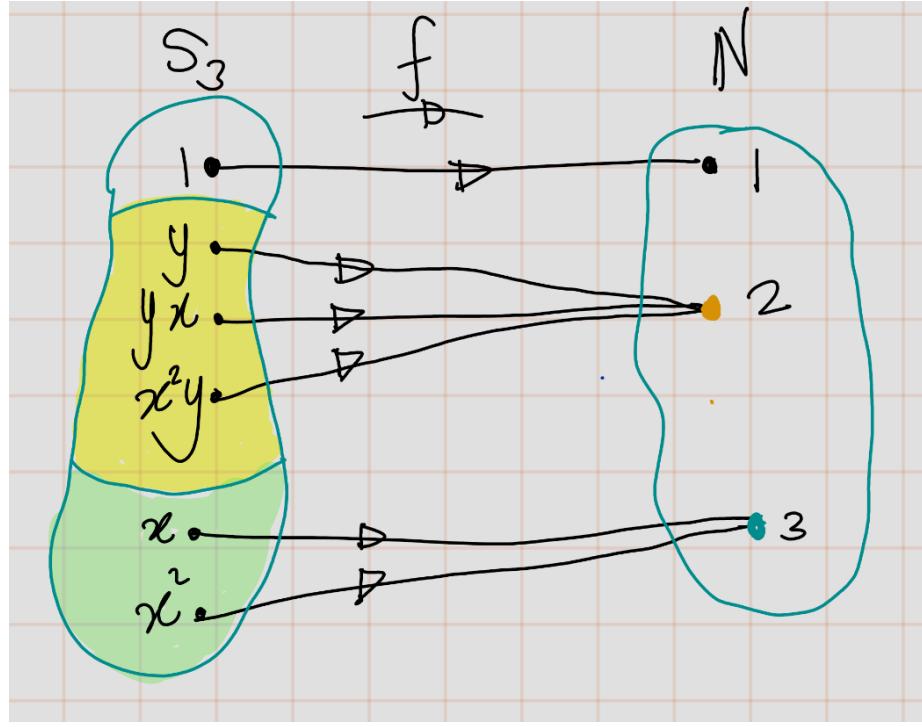
This fiber represents all complex numbers with the same absolute value  $t$ . Thus, fibers are circles in Complex plane.

Note that the absolute value map is surjective, so each positive real number  $t$  corresponds to a unique fiber in  $\mathbb{C}^\times$ .



Some Fibres of the Absolute Value Map  $\mathbb{C}^\times \rightarrow \mathbb{R}^\times$ .

**Example 2.14.** If  $G$  is a finite group, we can define a map  $f : G \rightarrow \mathbb{N}$  to the set  $\{1, 2, 3, \dots\}$  of natural numbers, letting  $f(a)$  be the order of the element  $a$  in  $G$ . The fibers of this map are the sets of elements with the same order (see example 2.11).

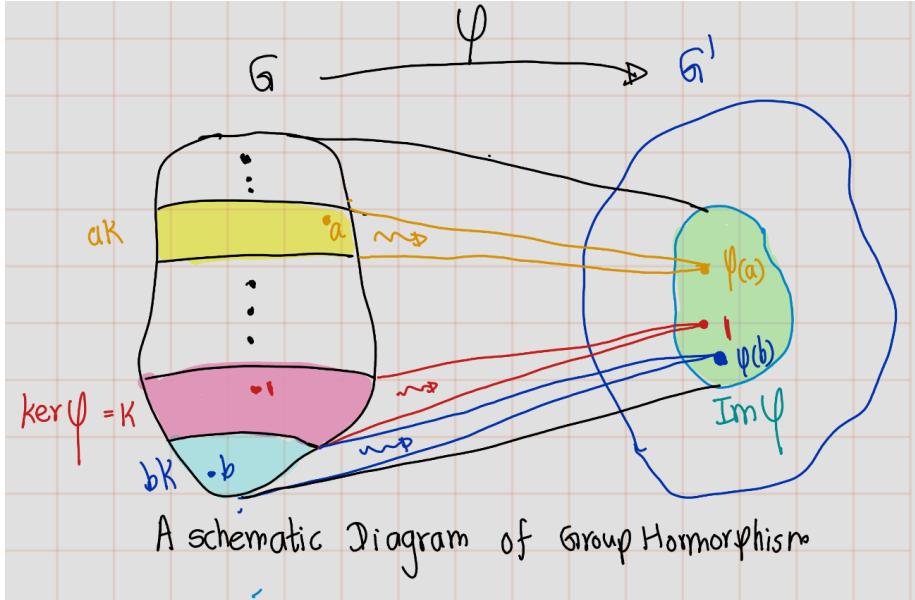


**Definition 2.8** (congruence). Let  $G, G'$  be groups and  $\phi : G \rightarrow G'$  be a group homomorphism. The equivalence relation on  $G$  defined by  $\phi$  is usually denoted by  $\equiv$ , rather than by  $\sim$ , and is referred to as congruence.

$$a \equiv b \text{ if } \phi(a) = \phi(b)$$

We have seen that elements  $a$  and  $b$  of  $G$  are congruent, i.e.,  $\phi(a) = \phi(b)$ , if and only if  $b$  is in the coset  $aK$  of the kernel  $K$  (See proposition 2.3)

**Proposition 2.5.** Let  $K$  be the kernel of a homomorphism  $\varphi : G \rightarrow G'$ . The fibre of that contains an element  $a$  of  $G$  is the coset  $aK$  of  $K$ . These cosets partition the group  $G$ , and they correspond to elements of the image of  $\varphi$ .



*Proof.* The fibre of  $\varphi$  over an element  $g' \in G'$  is the set of all elements  $a \in G$  such that  $\varphi(a) = g'$ . Let's denote this fibre as

$$F_{g'} = \{a \in G : \varphi(a) = g'\}$$

Now, let's take an arbitrary element  $a \in G$  and consider the left coset  $aK = \{ak : k \in K\}$ .

We know that  $K$  is the kernel of  $\varphi$ , so for any  $k \in K$ , we have  $\varphi(k) = 1_{G'}$  where  $1_{G'}$  is the identity element in  $G'$ .

- Claim 1:  $aK = F_{\varphi(a)}$ .

- sub claim 1.1:  $aK \subseteq F_{\varphi(a)}$ .

For any  $ak \in aK$ , we have  $\varphi(ak) = \varphi(a)\varphi(k) = \varphi(a)1_{G'} = \varphi(a)$ . This shows that every element in the coset  $aK$  is mapped to the same element under  $\varphi$  as  $a$  itself. Therefore, the coset  $aK$  is a subset of the fibre  $F_{\varphi(a)}$ .

- sub claim 1.2 :  $F_{\varphi(a)} \subseteq aK$ .

If  $a' \in F_{\varphi(a)}$ , then  $\varphi(a') = \varphi(a)$ , which implies that  $\varphi((a')^{-1}a) = 1_{G'}$ . This means that  $(a')^{-1}a \in K$ , or equivalently,  $a' \in aK$ . (by proposition 2.3)Therefore, the fibre  $F_{\varphi(a)}$  is a subset of the coset  $aK$ .

Since  $aK$  is a subset of  $F_{\varphi(a)}$  and  $F_{\varphi(a)}$  is a subset of  $aK$ , we conclude that  $aK = F_{\varphi(a)}$ . So, the fibre of  $\varphi$  that contains an element  $a$  of  $G$  is indeed the coset  $aK$  of  $K$ .

- Claim 2: The cosets of a subgroup  $K$  partition the group  $G$ .

A partition of a set is a collection of non-empty subsets such that every element in the set is in exactly one of these subsets.

To show that the cosets of  $K$  partition  $G$ , we need to show two things:

- sub claim 2.1: Every element of  $G$  is in at least one coset of  $K$ .  
Given any  $g \in G$ ,  $g$  is in the coset  $gK$ . So, every element of  $G$  is in at least one coset of  $K$ .
- sub claim 2.2: No element of  $G$  is in more than one coset of  $K$ .  
Suppose  $gK$  and  $hK$  are two cosets of  $K$  and there is some element  $x \in G$  that is in both  $gK$  and  $hK$ . This means that there exist  $k_1, k_2 \in K$  such that  $x = gk_1 = hk_2$  (by proposition 2.3). Then  $g = hk_2k_1^{-1}$ . Thus,  $g \in hK$ , which implies that  $gK = hK$ . So, no element of  $G$  is in more than one coset of  $K$ .

Therefore, the cosets of  $K$  partition the group  $G$ . □

## 2.8 Cosets

## 2.9 Modular Arithmetic

## 2.10 The Correspondence Theorem

**Definition 2.9.** Let  $\phi : G \rightarrow G'$  be a group homomorphism, and let  $H$  be a subgroup of  $G$ . We may restrict  $\phi$  to  $H$ , obtaining a homomorphism

$$\phi|_H : H \rightarrow G'$$

In other words, we take the same map but restrict its domain.

**Notation:** We use this notation for clarity  $[\phi|_H](h)$ .

Further, we can see that following observations.

- By definition,  $\forall h \in H, \phi|_H(h) = \phi(h)$
- The restriction  $\phi|_H$  is a homomorphism (Since  $\phi$  is homomorphism).
- The kernel of  $\phi|_H$  is the intersection of the kernel of  $\phi$  with  $H$ :

$$\ker(\phi|_H) = (\ker\phi) \cap H$$

There is no need to prove this. This is trivial by definition of kernel.

- Image of  $\phi|_H$  is the same as the image  $\phi(H)$  of  $H$  under the map  $\phi$ .

$$Im(\phi_H) = \phi(H)$$

- If  $|H|$  and  $|G'|$  have no common factor,  $\phi(H) = \{1\}$ , so  $H$  is contained in the kernel. (Since, by Artin's book corollary 2.8.13,

$$\begin{array}{c|c} |Im(\phi_H)| & |H| \\ \hline & \end{array} \quad (2.10)$$

$$\begin{array}{c|c} |Im(\phi_H)| & |G'| \\ \hline & \end{array} \quad (2.11)$$

, Thus, if  $|H|$  and  $|G'|$  have no common factors,  $|Im(\phi_H)| = |\phi(H)| = 1$ . So,  $Im(\phi_H) = \phi(H) = \{1\}$

Now let's see an example.

**Example 2.15.** Define sign homomorphism  $\sigma : S_n \rightarrow \{\pm 1\}$  by  $\sigma(x) = 1$  if  $x$  is even, and  $\sigma(x) = -1$  if  $x$  is odd. Then the image of the sign homomorphism is,

$$Im(\sigma) = \{\pm 1\}$$

it has order 2.

Let  $H = \{x \in S_n : \text{if } x \text{ has odd order}\}$ . Then  $H$  is a subgroup. So,  $H \subset \ker(\sigma)$  (We can easily verify this.)

Further, The sub group of  $S_n$  with even permutations is called *Alternating group* ( $A_n$ ).

### 2.10.1 PROBLEM

**Proposition 2.6.** Let  $\phi : G \rightarrow G'$  be a homomorphism with kernel  $K$ , and let  $H' \leq G'$ . Denote the inverse image  $\phi^{-1}(H')$  by  $H$ . i.e.:

$$H = \phi^{-1}(H') = \{x \in G : \phi(x) \in H'\}$$

Then,

- $\phi^{-1}(H')$  is a subgroup of  $G$  that contains  $K$ .
- If  $H$  is a normal subgroup of  $G'$ , then  $\phi^{-1}(H')$  is also a normal subgroup of  $G$ .
- If  $\phi$  is surjective and  $H$  is a normal subgroup of  $G$ , then  $\phi^{-1}(H')$  is a normal subgroup of  $G'$ .

*Remark.*  $\phi^{-1}$  is not a map.

*Proof.*

- **Claim 1:**  $K \subseteq \phi^{-1}(H') = H$   
Let  $x \in K$ . Then  $\phi(x) = 1_{G'}$ . Since  $1_{G'} \in H'$ . Thus,  $x \in \phi^{-1}(H') = H$ .  
Therefore,  $K \subseteq \phi^{-1}(H') = H$
- **Claim 2:**  $\phi^{-1}(H')$  is a subgroup of  $G$

- *Closure* : Suppose  $x, y \in H = \phi^{-1}(H')$ . Then  $\phi(x), \phi(y) \in \phi(H')$ . Since  $\phi$  is homomorphism  $\phi(x)\phi(y) = \phi(xy)$ . Since  $H' \leq G'$ , then  $\phi(xy) = \phi(x)\phi(y) \in H'$ . Thus,  $xy \in \phi^{-1}(H') = H$
- *Identity* : Since  $\phi(1_G) = 1_{G'}$ ,  $1_G \in \phi^{-1}(H') = H$
- *Inverse* : Let  $x \in \phi^{-1}(H') = H$ . Then  $\phi(x) \in H'$  and since  $H' \leq G'$ , then  $(\phi(x))^{-1} \in H'$ . Since  $\phi$  is a homomorphism,  $(\phi(x))^{-1} = \phi(x^{-1})$ . Thus  $(\phi(x))^{-1} = \phi(x^{-1}) \in H'$ . Hence,  $x^{-1} \in \phi^{-1}(H')$ .

- **Claim 3:** If  $H'$  is a normal subgroup of  $G'$ , then  $\phi^{-1}(H')$  is also a normal subgroup of  $G$ .

Now suppose that  $H'$  is a normal subgroup of  $G'$ . Let  $x \in H$  and  $g \in G$ . Then, since  $\phi$  is homomorphism,

$$\phi(-1) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(x)(\phi(g))^{-1}$$

So,  $\phi(gxg^{-1})$  is conjugate of  $\phi(x)$ . Since  $x \in H = \phi^{-1}(H')$ , the  $\phi(x) \in H'$ .  
Thus,  $\phi(gxg^{-1}) = \phi(g)\phi(x)(\phi(g))^{-1} \in H'$ . Hence,  $gxg^{-1} \in \phi^{-1}(H') = H$ .

- **Claim 4:** If  $\phi$  is surjective and  $H$  is a normal subgroup of  $G$ , then  $\phi^{-1}(H')$  is a normal subgroup of  $G'$ .

Suppose that  $\phi$  is surjective and  $H$  is a normal subgroup of  $G$ . Let  $a \in H'$  and  $b \in G'$ . Since  $\phi$  is surjective, There are elements  $x \in H$  and  $y \in G$  such that  $\phi(x) = a$  and  $\phi(y) = b$ . Since  $H$  is normal  $yxy^{-1} \in H$ , thus  $\phi(yxy^{-1}) = bab^{-1} \in H'$ .

□

**Example 2.16.** let denote the determinant homomorphism

$$\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$$

. Note that  $\mathbb{R}^+ \trianglelefteq \mathbb{R}^\times$ . (It is very clear that \$The set of positive real numbers is a subgroup of  $\mathbb{R}^\times$ , and since  $\mathbb{R}^\times$  is abelian,  $\mathbb{R}^+$  is normal.) Now consider the inverse image of  $\mathbb{R}^+$ ,

$$\det^{-1}(\mathbb{R}^+) = \{A \in GL_n(\mathbb{R}) : \det(A) \in \mathbb{R}^+\} = SL_n(\mathbb{R})$$

. By above proposition we can ge that  $SL_n(\mathbb{R})$  is normal subgroup. (Because  $\mathbb{R}^+ \trianglelefteq \mathbb{R}^\times$  and  $\det$  is surjective map.)

**Theorem 2.2** (Correspondence Theorem). *Let  $\phi : G \rightarrow G'$  be a surjective group homomorphism with kernel  $K$ . There is a bijective correspondence between subgroups of  $G'$  and subgroups of  $G$  that contain  $K$ :*

$$\{\text{subgroups of } G \text{ that contain } K\} \leftrightarrow \{\text{subgroups of } G'\}$$

This correspondence is defined as follows:

$$\begin{aligned} \text{a subgroup } H \text{ of } G \text{ that contains } K &\rightsquigarrow \text{its image } \phi(H) \in G', \\ \text{a subgroup } H' \text{ of } G' &\rightsquigarrow \text{its inverse image } \phi^{-1}(H') \text{ in } G. \end{aligned}$$

- If  $H$  and  $H'$  are corresponding subgroups, then  $H$  is normal in  $G$  if and only if  $H'$  is normal in  $G'$ .
- If  $H$  and  $H'$  are corresponding subgroups, then

$$|H| = |H'||K|$$

*Proof.* Let  $H$  be subgroup of  $G$  that contain  $K$ . Let  $H'$  be a subgroup of  $G'$ . Now we need to check folllwings,

- $\phi(H)$  is a subgroup of  $G'$ .
- $\phi^{-1}(H')$  is a subgroup of  $G$ , and it contains  $K$ .
- $H'$  is a normal subgroup of  $G'$  if and only if  $\phi^{-1}(H')$  is a normal subgroup of  $G$ .
- (bijectivity of the correspondence)  $\phi(\phi^{-1}(H')) = H'$  and  $\phi^{-1}(\phi(H)) = H$
- $|(\phi^{-1}(H'))| = |H'||K|$ .
- **Claim 1:**  $\phi(H)$  is a subgroup of  $G'$ .
  - *Closure:* Let  $x, y \in \phi(H)$ . Then there is  $a, b \in H$  such that  $\phi(a) = x$  and  $\phi(b) = y$ . Since  $\phi$  is homomorphism,  $xy = \phi(a)\phi(b) = \phi(ab)$ . Since  $H \leq G$ ,  $ab \in H$ ,  $xy = \phi(ab) \in \phi(H)$ .
  - *Identity:* Since  $1_G \in H$ ,  $\phi(1_G) = 1_{G'} \in \phi(H)$
  - *Inverse:* Let  $x \in \phi(H)$ . Then there exist  $a \in H$  such that  $\phi(a) = x$ . Since  $H \leq G$ ,  $a^{-1}$  exists in  $H$ .  $\phi(a^{-1}) = \phi(a)^{-1} = x^{-1} \in \phi(G)$ .
- **Claim 2:**  $\phi^{-1}(H')$  is a subgroup of  $G$ , and it contains  $K$ .  
This is true from proportion 2.6
- **Claim 3:**  $H'$  is a normal subgroup of  $G'$  if and only if  $\phi^{-1}(H')$  is a normal subgroup of  $G$ .  
Alreday this prooved in proportion 2.6
- **Claim 4.1:**  $\phi(\phi^{-1}(H')) = H'$

- $\phi(\phi^{-1}(H')) \subset H'$   
Lett  $x \in \phi(\phi^{-1}(H'))$ . Then there exist  $y \in \phi^{-1}(H')$  such that  $\phi(y) = x$ . Then by definiton of the pre image  $x = \phi(y) \in H'$ .
- $\phi(\phi^{-1}(H')) \supset H'$   
Let  $a \in H'$ . Since  $\phi$  is surjective, there exists  $b \in G$  such that  $\phi(b) = a \in H'$ . Thus  $b \in \phi^{-1}(H')$ . Hence  $a = \phi(b) = \phi(\phi^{-1}(H'))$ .

Therefore,  $\phi(\phi^{-1}(H')) = H'$ .

• **Claim 4.2:**  $\phi^{-1}(\phi(H)) = H$

- $\phi^{-1}(\phi(H)) \supset H$   
Let  $x \in H$ . Then  $\phi(x) \in \phi(H)$ . So,  $x \in \phi^{-1}(\phi(H))$ .
- $\phi^{-1}(\phi(H)) \subset H$   
Let  $y \in \phi^{-1}(\phi(H))$ . By definition of inverse image,  $\phi(y) \in \phi(H)$ . Then there exist  $z \in H$  such that  $\phi(y) = \phi(z)$ . Then  $z^{-1}y$  is in the kernal  $K$ . (by Artins book proposition 2.5.8). Since  $K \subset H$ ,  $z^{-1}y \in H$ . So,  $a \in H$  and  $a^{-1}z \in H$ . Thus,  $a(a^{-1}x) = x \in H$ . Hence  $\phi^{-1}(\phi(H)) \subset H$

Therefore,  $\phi^{-1}(\phi(H)) = H$  - **Claim 5** :  $|(\phi^{-1}(H'))| = |H'||K|$ .

□

### 2.10.2 Problem

**Example 2.17.** Recall

$$\begin{aligned} S_4 &= \{id, (12), (13), (14), (23), (24), (34), (123), (124), (132), (134), (142), (143), (234), (1234)\} \\ S_3 &= \{id, (12), (13), (23), (123), (132)\} \end{aligned}$$

There are 6 such subgroups of  $S_3$ ,

$$\langle (12) \rangle, \langle (13) \rangle, \langle (23) \rangle, \langle (123) \rangle = \langle (132) \rangle, S_3$$

. There is one proper subgroup of order 3. That is  $\langle (123) \rangle$ . There are 3 subgroups of order 2. They are  $\langle (12) \rangle, \langle (13) \rangle, \langle (23) \rangle$

The Correspondence Theorem tells us that there are four proper subgroups of  $S_4$  that contain  $K$ .

### 2.10.3 Problem

## 2.11 Product Groups

Let  $G, G'$  be two groups. The product set  $G \times G'$ , the set of pairs of elements  $(a, a')$  with  $a$  in  $G$  and  $a'$  in  $G'$ , can be made into a group by component-wise multiplication,

multiplication of pairs is defined by the rule,

$$(a, a') \cdot (b, b') = (ab, a'b') \quad \text{for } a, b \in G \text{ and for } a', b' \in G'$$

Let's prove that  $G \times G'$  is a group.

*Proof.* Let  $G, G'$  be two groups and let  $a, b, c \in G$  and  $a', b', c' \in G'$

- *Closure* :  $(a, a') \cdot (b, b') = (ab, a'b')$ . So, since  $a, b \in G$  and  $a', b' \in G'$  and  $G$  and  $G'$  be a group, then  $ab \in G$  and  $a'b' \in G$ . Thus,  $(a, a') \cdot (b, b') = (ab, a'b') \in G \times G'$ .
- *Asscitivity*: We can obtain following using asscitivity property of group  $G$  and  $G'$ .

$$((a, a') \cdot (b, b')) \cdot (c, c') = (ab, a'b') \cdot (c, c') = (abc, a'b'c') = (a, a') \cdot (bc, b'c') = (a, a') \cdot ((b, b') \cdot (c, c'))$$

- *identity*:  $(1_G, 1_{G'})$  is the identity

$$(1_G, 1_{G'}) \cdot (b, b') = (1_G b, 1_{G'} b') = (b, b') = (b 1_G, b' 1_{G'}) = (b, b') \cdot (1_G, 1_{G'})$$

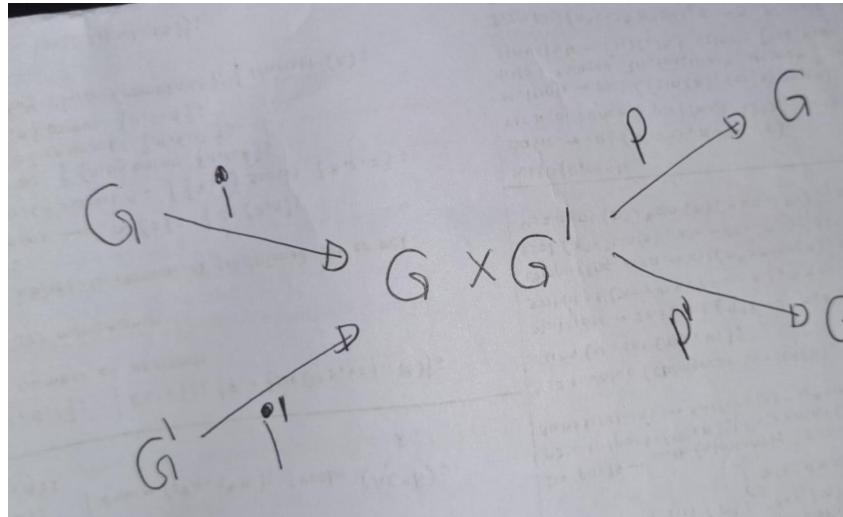
- *Inverse* : The inverse of  $(a, a')$  is  $(a^{-1}, (a')^{-1})$

$$(a, a') \cdot (a^{-1}, (a')^{-1}) = (aa^{-1}, a'(a')^{-1}) = (1_G, 1_{G'}) = (a^{-1}a, (a')^{-1}a') = (a^{-1}, (a')^{-1}) \cdot (a, a')$$

□

So, The group obtained in this way is called the product of  $G$  and  $G'$ .

It is related to the two factors  $G$  and  $G'$  in a simple way that we can sum up in



terms of some homomorphisms.

The homomorphisms are defined as follows,

$$i : G \rightarrow G \times G' \quad (2.12)$$

$$x \mapsto (x, 1) \quad (2.13)$$

(2.14)

$$i' : G' \rightarrow G \times G' \quad (2.15)$$

$$x \mapsto (x', 1) \quad (2.16)$$

(2.17)

$$p : G \times G' \rightarrow G' \quad (2.18)$$

$$(x, x') \mapsto x \quad (2.19)$$

(2.20)

$$p' : G' \times G' \rightarrow G' \quad (2.21)$$

$$(x, x') \mapsto x' \quad (2.22)$$

(2.23)

(2.24)

Observe that  $i$  and  $i'$  are injective and

$$Im(i) = G \times 1'_G \leq G \times G' \text{ and } Im(i') = 1_G \times G' \leq G \times G'$$

The maps  $p$  and  $p'$  are called projections and they are surjective.

$$\ker(p) = 1 \times G' \text{ and } \ker(p') = G \times 1_{G'}$$

It is obviously desirable to decompose a given group  $G$  as a product, that is, to find investigate groups  $H$  and  $H'$  such that  $G$  is isomorphic to the product  $H \times H'$ . The groups  $H$  and  $H'$  will be simpler, and the relation between  $H \times H'$  and its factors is easily understood. It is rare that a group is a product, but it does happen occasionally

**Example 2.18.** Consider a cyclic group of order 6 can be decomposed. It might be suprised you. A cyclic group  $C_6$  of order 6 is isomorphic to the product  $C_2 \times C_3$  of cyclic groups of orders 2 and 3.

$$C_6 \equiv C_2 \times C_3$$

Let say

$$C_2 = \langle y \rangle = \{1, y\}, \text{ with } y^2 = 1 \quad (2.25)$$

$$C_3 = \langle z \rangle = \{1, z, z^2\}, \text{ with } y^3 = 1 \quad (2.26)$$

Let  $x \in C_2 \times C_3$ . Then there exist  $p \in C_2$  and  $q \in C_3$  such that  $x = (p, q)$ . Let's find order of  $x$ , that is the smallest positive integer  $k$  such that  $x^k = (y^k, z^k)$  is the identity  $(1, 1)$ .

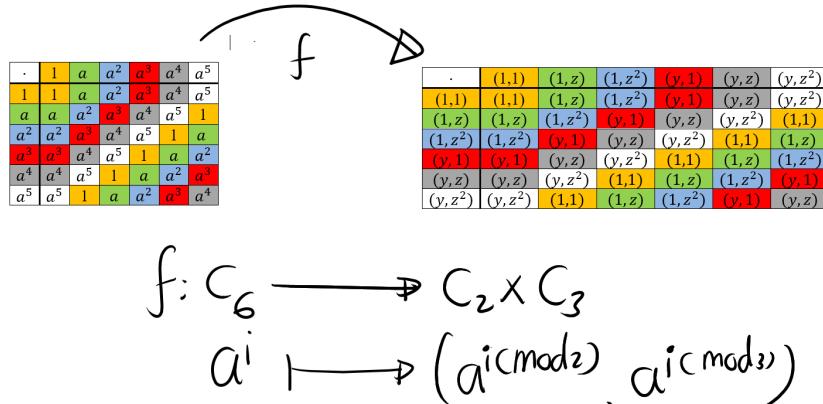
- Case-I:  $k = 1, x^1 = (y^1, z^1) = (y, z)$
- Case-II:  $k = 2, x^2 = (y^2, z^2) = (1, z^2)$
- Case-III:  $k = 3, x^3 = (y^3, z^3) = (y, 1)$
- Case-IV:  $k = 4, x^4 = (y^4, z^4) = (1, z)$
- Case-V:  $k = 5, x^5 = (y^5, z^5) = (1, z^2)$
- Case-VI:  $k = 6, x^6 = (y^6, z^6) = (1, 1)$

Thus, the smallest positive integer  $k$  such that  $x^k = (1, 1)$  is 6. So, order of  $x$  is 6. Since  $C_2 \times C_3$  has order 6. Furthur,

$$C_2 \times C_3 = \langle x \rangle$$

The powers of  $x$  are

$$(1, 1), (y, z), (1, z^2), (y, 1), (1, z), (y, z^2)$$



Here  $i = 0, 1, 2, \dots, 5$

So let's try to see above result more generally.

**Proposition 2.7.** *Let  $r$  and  $s$  be relatively prime integers. A cyclic group of order  $rs$  is isomorphic to the product of a cyclic group of order  $r$  and a cyclic group of order  $s$ .*

**Example 2.19 (s).** On the other hand, a cyclic group of order 4 is not isomorphic to a product of two cyclic groups of order 2.

$$C_4 \not\cong C_2 \times C_2$$

Because , every element of  $C_2 \times C_2$  has order 1 or 2, whereas a cyclic group of order 4 contains two elements of order 4.

The next proposition describes product groups.

**Proposition 2.8.** *Let  $G$  be a group and let  $H, K \leq G$ , and let  $f : H \times K \rightarrow G$  be the multiplication map, defined by  $f(h, k) = hk$ . Its image is the set  $HK = \{hk | h \in H, k \in K\}$ .*

- a.  *$f$  is injective if and only if  $H \cap K = \{1\}$ .*
- b.  *$f$  is a homomorphism from the product group  $H \times K$  to  $G$  if and only if elements of  $K$  commute with elements of  $H$ :  $hk = kh$ .*
- c. *If  $H$  is a normal subgroup of  $G$ , then  $HK$  is a subgroup of  $G$ .*
- d.  *$f$  is an isomorphism from the product group  $H \times K$  to  $G$  if and only if  $H \cap K = \{1\}$ ,  $HK = G$ , and also  $H$  and  $K$  are normal subgroups of  $G$ .*

*It is important to note that the multiplication map may be bijective though it isn't a group homomorphism. This happens, for instance, when  $G = S_3$ , and with the usual notation,  $H = \langle x \rangle$  and  $K = \langle y \rangle$ .*

*Proof.*

a.

- ( $\Rightarrow$ ) We are going to use proof by contrapositive. So, suppose that  $x \in H \cap K$  such that  $x \neq 1$ . Since  $x \in H$  then  $x^{-1} \in H$ .

$$f(x^{-1}, x) = x^{-1} \cdot x = 1 = 1 \cdot 1 = f(1, 1)$$

Thus,  $f$  is not injective. Thus, if  $f$  is injective then  $H \cap K = \{1\}$ . -( $\Leftarrow$ ) Now Suppose that  $H \cap K = \{1\}$ . Let  $(h_1, k_1), (h_2, k_2) \in H \times K$  such that  $h_1k_1 = h_2k_2$ . Now multiply both sides of this equation on the left by  $h_1^{-1}$  and on the right by  $k_2^{-1}$ ,

$$h_1k_1 = h_2k_2 \tag{2.27}$$

$$h_1^{-1}(h_1k_1)k_2^{-1} = h_1^{-1}(h_2k_2)k_2^{-1} \tag{2.28}$$

$$(h_1^{-1}h_1)k_1k_2^{-1} = h_1^{-1}h_2(k_2k_2^{-1}) \tag{2.29}$$

$$k_1k_2^{-1} = h_1^{-1}h_2 \tag{2.30}$$

Note that  $(k_1 k_2^{-1}) \in K$  and  $h_1^{-1} h_2 \in H$ . Since  $H \cap K = \{1\}$ ,

$$k_1 k_2^{-1} = h_1^{-1} h_2 = 1$$

. Then,

$$k_1 = k_2 \quad \text{and} \quad h_1 = h_2.$$

Then

$$(h_1, k_1) = (h_2, k_2)$$

b. Let  $(h_1, k_1), (h_2, k_2) \in H \times K$ . Now consider,

$$f((h_1, k_1) \cdot (h_2, k_2)) = f((h_1 h_2, k_1 k_2)) = h_1 h_2 k_1 k_2 \quad (2.31)$$

$$f((h_1, k_1)) \cdot f((h_2, k_2)) = (h_1 k_1) \cdot (h_2 k_2) = h_1 k_1 h_2 k_2 \quad (2.32)$$

$$f \text{ is homomorphism} \iff f((h_1, k_1) \cdot (h_2, k_2)) = f((h_1, k_1)) \cdot f((h_2, k_2)) \quad (2.33)$$

$$\iff h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 \quad (2.34)$$

$$\iff h_1^{-1} (h_1 h_2 k_1 k_2) k_2^{-1} = h_1^{-1} (h_1 k_1 h_2 k_2) k_2^{-1} \quad (2.35)$$

$$\iff (h_1^{-1} h_1) h_2 k_1 (k_2 k_2^{-1}) = (h_1^{-1} h_1) k_1 h_2 (k_2 k_2^{-1}) \quad (2.36)$$

$$\iff (h_1^{-1} h_1) h_2 k_1 (k_2 k_2^{-1}) = (h_1^{-1} h_1) k_1 h_2 (k_2 k_2^{-1}) \quad (2.37)$$

$$\iff h_2 k_1 = k_1 h_2 \quad (2.38)$$

c.

- Suppose that  $H$  is a normal sub group of  $G$ . Note that

$$KH = \bigcup_{k \in K} kH \quad \text{and} \quad HK = \bigcup_{k \in K} Hk$$

Since,  $H$  is normal,  $kH = Hk$  for all  $k \in K$ . So,  $HK = KH$ . We are going to use sub group test,

- *non-emptiness*: Clearly,  $1 = 1 \cdot 1 \in HK$  (because  $1 \in H$  and  $1 \in K$ )
- *closure*:

$$HKHK = HHKK = HK$$

Thus,  $HK$  is closed under multiplication.

- *closed under inverse*: Let  $hk \in HK$ . Then

$$(hk)^{-1} = k^{-1} \cdot h^{-1} \in KH = HK$$

This proves closure of  $HK$  under inverses.

d.

- ( $\Leftarrow$ ): Suppose that  $H \cap K = \{1\}$ ,  $HK = G$ , and also  $H, K \trianglelefteq G$ . According to the (b),  $f$  is a homomorphism from  $H \times K$  to  $G$  if and only if  $hk = kh$  for all  $h \in H$ . Consider,

$$(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}).$$

Note that, Since  $K \trianglelefteq G$ ,  $hkh^{-1} \in K$ . So,  $(hkh^{-1})k^{-1} \in K$ . Similary we can show that  $h(kh^{-1}k^{-1}) \in H$ . Thus,

$$(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K.$$

But from our hypothesis,  $H \cap K = \{1\}$ . Hence,

$$hkh^{-1}k^{-1} = 1 \quad (2.39)$$

$$hk = kh \quad (2.40)$$

Therefore, by (b) we can  $f$  is hormorphism. Now we have to proove bijectivity,  
- *Injectivity*: Already prooved in 2.8 (a) - *Surjectivity*: For any  $g \in G$ , we can write  $g = hk$  for some  $h \in H$  and  $k \in K$  (since  $Im(f) = HK = G$ ). Thus,  $f(h, k) = hk = g$ , so  $f$  is surjective.

Therefore  $f$  is an isomorphism.

- ( $\Rightarrow$ ) Now suppose that  $f$  is isomorphism.

- **Claim i:**  $H \cap K = \{1\}$ .

Suppose that  $x \in H \cap K$ . Then,

$$f(1, x) = x = f(x, 1)$$

Since  $f$  is an isomorphism (and hence injective), we must have  $x = 1$ .  
Therefore,  $H \cap K = \{1\}$ .

- **Claim ii :**  $HK = G$ .

Since  $f$  is surjective, for any  $g \in G$ , there exist  $h \in H$  and  $k \in K$  such that  $f(h, k) = hk = g$ . Therefore,  $HK = G$ .

- **Claim iii :**  $H$  and  $K$  are normal in  $G$ .

For any  $h \in H$  and  $g \in G$ , we can write  $g = hk$  for some  $k \in K$ .  
Then

$$ghg^{-1} = (hk)h(hk)^{-1} = hk(hh^{-1})k^{-1} = h(kk^{-1}) = h \in H.$$

Thus,  $H \trianglelefteq G$ . Similarly, we can show that  $K \trianglelefteq G$ .

□

**Proposition 2.9.** *There are two isomorphism classes of groups of order 4, the class of the cyclic group  $C_4$  of order 4 and the class of the Klein Four Group, which is isomorphic to the product  $C_2 \times C_2$  of two groups of order 2.*

*Proof.* Let  $G$  be a group of order 4. The order of any element  $x$  of  $G$  divides 4, so there are two cases to consider:

- Case 1:  $G$  contains an element of order 4 ( $|G| = 4$ ). Then  $G$  is a cyclic group of order 4.
- Case 2: Every element of  $G$  except the identity has order 2.

In this case,  $x = x^{-1}$  for every element  $x$  of  $G$ . Let  $x$  and  $y$  be two elements of  $G$ . Then  $xy$  has order 2, so  $(xy)(x^{-1}y^{-1}) = (xy)(xy) = 1$ . This shows that  $x$  and  $y$  commute,

$$xyx^{-1}y^{-1} = 1 \quad (2.41)$$

$$xyx^{-1}(y^{-1}y) = y \quad (2.42)$$

$$xyx^{-1} = y \quad (2.43)$$

$$xy(x^{-1}x) = yx \quad (2.44)$$

$$xy = yx \quad (2.45)$$

since  $x, y$  are arbitrary elements,  $G$  is abelian. So every subgroup is normal. We choose distinct elements  $x$  and  $y$  in  $G$ , and we let  $H$  and  $K$  be the cyclic groups of order 2 that they generate. Proposition 2.8 (d) shows that  $G$  is isomorphic to the product group  $H \times K$ .  $\square$

## 2.12 Quotient Groups

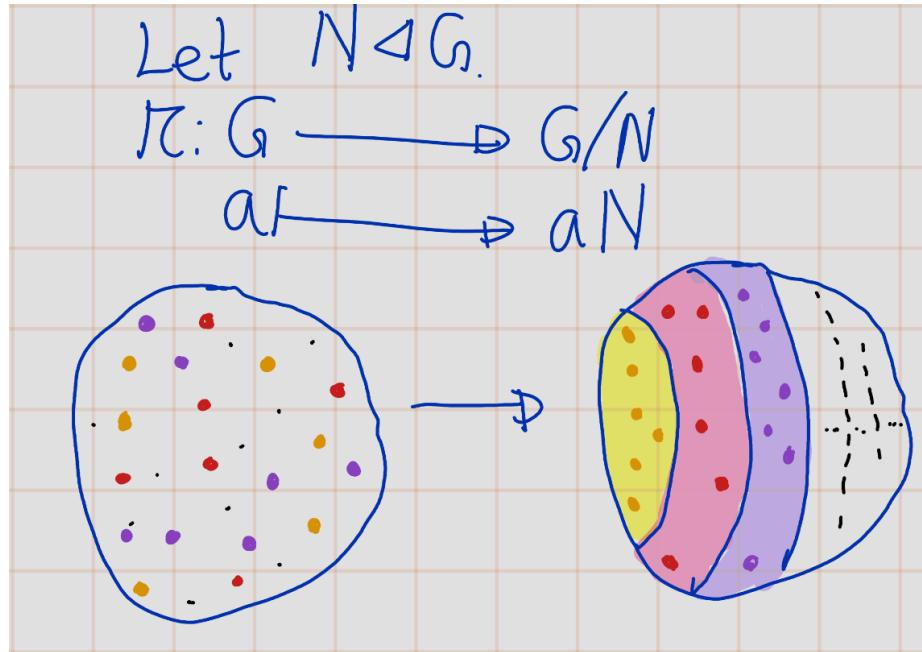
**Definition 2.10.** The set of cosets of a normal subgroup  $N$  of a group  $G$  is often denoted by  $G/N$ .

$G/N$  is the set of cosets of  $N$  in  $G$

**Notation:** When we regard a coset  $C$  as an element of the set of cosets, the bracket notation  $[C]$  may be used. If  $C = aN$ , we may also use the bar notation to denote the element  $[C]$  by  $\bar{a}$ , and then we would denote the set of cosets by  $\overline{G}$ :

$$\overline{G} = G/N$$

**Theorem 2.3.** Let  $N$  be a normal subgroup of a group  $G$ , and let  $\bar{G}$  denote the set of cosets of  $N$  in  $G$ . There is a law of composition on  $\bar{G}$  that makes this set into a group, such that the map  $\pi : G \rightarrow \bar{G}$  defined by  $\pi(a) = \bar{a}$  is a surjective homomorphism whose kernel is  $N$ .



*Remark.* The map is often referred to as the canonical map from  $G$  to  $\bar{G}$ . The word “canonical” indicates that this is the only map that we might reasonably be talking about

The next corollary is very simple, but it is important enough to single out:

**Corollary 2.1.** Let  $N \trianglelefteq G$ , and let  $\bar{G} = G/N$  be the canonical homomorphism. Let  $a_1, \dots, a_k \in G$  such that the product  $a_1 \cdots a_k \in N$ . Then  $\bar{a}_1 \cdots \bar{a}_k = \bar{1}$ .

*Proof.* Let  $p = a_1 \cdots a_k \in N$ . This implies  $\pi(p) = \bar{p} = \bar{1}$ .

Since  $\pi$  is a homomorphism,  $\pi(p) = \pi(a_1 \cdots a_k) = \pi(a_1) \cdots \pi(a_k) = \bar{a}_1 \cdots \bar{a}_k$   $\square$

*Proof of 2.3* There are several things to be done. We must

- define a law of composition on  $\bar{G}$ ,
- prove that the law makes  $\bar{G}$  into a group,
- prove that  $\pi$  is a surjective homomorphism, and
- prove that the kernel of  $\pi$  is  $N$ .

*Remark.* If  $A, B \subseteq G$  then  $AB$  denotes the set of products  $ab$ :

$$AB := \{x \in G : x = ab, a \in A, b \in B\}$$

- We will call this a product set, though in some other contexts the phrase “product set” refers to the set  $A \times B$  of pairs of elements

**Lemma 2.2.** *Let  $N$  be a normal subgroup of a group  $G$ , and let  $aN$  and  $bN$  be cosets of  $N$ . The product set  $(aN)(bN)$  is also a coset and*

$$(aN)(bN) = \{x \in G : x = anbm' \& n, n' \in N\} = abN$$

*Proof.* Since  $N$  is a subgroup,  $NN = N$ .

Since  $N$  is normal, left and right cosets are equal:  $Nb = bN$ .

$$(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN$$

□

- This lemma allows us to define multiplication on the set  $\overline{G} = G/N$ .
- Using the bracket notation, the definition is this: If  $C_1$  and  $C_2$  are cosets, then  $[C_1][C_2] = [C_1C_2]$ , Where  $C_1C_2$  is the product set.
- The lemma shows that this product set is another coset.
- To compute the product  $[C_1][C_2]$ , take any elements  $a \in C_1$  and  $b \in C_2$ . Then  $C_1 = aN$ ,  $C_2 = bN$ , and  $C_1C_2$  is the coset  $abN$  that contains  $ab$ . So,

$$[aN][bN] = [abN] \text{ or } \overline{ab} = \overline{ab}.$$

Then by definition of the map  $\pi$  in theorem 2.3,

$$\pi(ab) = \overline{ab} = \overline{ab} = \pi(a)\pi(b)$$

The fact that  $\pi$  is a homomorphism will follow, once we show that  $\overline{G}$  is a group. Since the canonical map  $\pi$  is surjective, the next lemma proves this

**Lemma 2.3.** *Let  $G$  be a group, and let  $Y$  be a set with a law of composition (both laws written with multiplicative notation). Consider a surjective map  $\varphi : G \rightarrow Y$  with the homomorphism property:  $\varphi(ab) = \varphi(a)\varphi(b)$  for all  $a$  and  $b$  in  $G$ . Then  $Y$  is a group, and  $\varphi$  is a homomorphism.*

*Proof.* The group axioms that are true in  $G$  are carried over to  $Y$  by the surjective map  $\varphi$ .

- **Closure** : Let  $y_1, y_2 \in Y$ . Since  $\varphi$  is surjective,  $y_1 = \varphi(x_1), y_2 = \varphi(x_2)$  for some  $x_1, x_2 \in G$ .

$$y_1 y_2 = \varphi(x_1) \varphi(x_2) = \varphi(x_1 x_2) \in Y$$

- **Associativity Property** :

Let  $y_1, y_2$ , and  $y_3$  be elements of  $Y$ . Since  $\varphi$  is surjective,  $y_i = \varphi(x_i)$  for some  $x_i$  in  $G$ . Then

$$(y_1 y_2) y_3 = (\varphi(x_1) \varphi(x_2)) \varphi(x_3) = \varphi(x_1 x_2) \varphi(x_3) = \varphi((x_1 x_2) x_3) \quad (2.46)$$

$$=^* \varphi(x_1 (x_2 x_3)) = \varphi(x_1) \varphi(x_2 x_3) = y_1 (y_2 y_3) \quad (2.47)$$

The equality marked with an asterisk ( $=^*$ ) is the associative law in  $G$ . The other equalities follow from the homomorphism property of  $\varphi$ .

- **Identity** Let  $y \in Y$ . Since  $\varphi$  is surjective, there exist  $x \in G$  such that  $y = \varphi(x)$ . Let  $1_G$  be identity of  $G$ . Then,

$$y \varphi(1_G) = \varphi(x) \varphi(1_G) = \varphi(x 1_G) = \varphi(x) = y = \varphi(1_G x) = \varphi(1_G) \varphi(x) = \varphi(1_G) y$$

Thus,  $\varphi(1_G)$  is the identity of  $Y$ .

- **Inverse** : Let  $y \in G$ . Since  $\varphi$  is surjective, there exist  $x \in G$  such that  $y = \varphi(x)$ ,

$$y \varphi(x^{-1}) = \varphi(x) \varphi(x^{-1}) = \varphi(x x^{-1}) = \varphi(1_G) = \varphi(x^{-1} x) = \varphi(x^{-1}) \varphi(x) = \varphi(x^{-1}) y$$

Thus,  $y^{-1} = \varphi(x)$

□

The only thing remaining to be verified is that the kernel of the homomorphism  $\pi$  is the subgroup  $N$ .

$$\pi(a) = \pi(1) \iff \bar{a} = \bar{1} \quad (2.48)$$

$$\iff [aN] = [1N] \quad (2.49)$$

$$\iff a \in N. \quad (2.50)$$

Thus,  $\ker(\pi) = N$

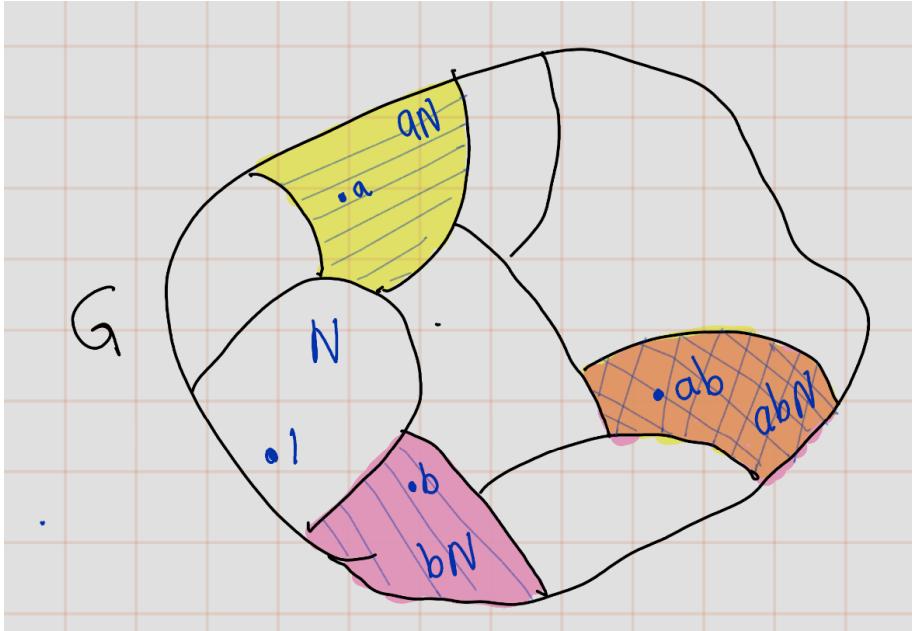


Figure 2.1: A Schematic Diagram of Coset Multiplication.

*Remark.* Our assumption that  $N$  is a **normal** subgroup of  $G$  is crucial to lemma 2.2. If  $H$  is **not** normal, there will be left cosets  $C_1$  and  $C_2$  of  $H$  in  $G$  such that the product set  $C_1C_2$  does not lie in a single left cosets.

Let's see an example for this. Going back once more to the subgroup  $H = \langle y \rangle$  of  $S_3$ . Note that the subgroup  $H$  is not normal.

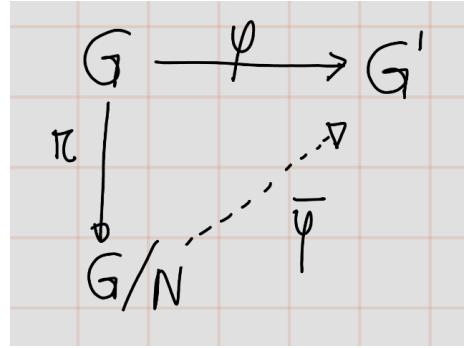
The product set  $(1H)(xH)$  contains four elements:

$$(1H)(xH) = \{1, y\}\{x, xy\} = \{x, xy, x^2y, x^2\}$$

. It is not a coset.

The next theorem relates the quotient group construction to a general group homomorphism, and it provides a fundamental method of identifying quotient groups.

**Theorem 2.4** (First Isomorphism Theorem). *Let  $\varphi : G \rightarrow G'$  be a surjective group homomorphism with kernel  $N$ . The quotient group  $\bar{G} = G/N$  is isomorphic to the image  $G'$ . To be precise, let  $\pi : G \rightarrow \bar{G} = G/N$  be the canonical map. There exists a unique isomorphism  $\bar{\varphi} : G/N \rightarrow G'$  such that  $\varphi = \psi \circ \pi$ .*



*Proof.* The elements of  $\overline{G} = G/N$  are the cosets of  $N$ , and they are also the fibres of the map  $\varphi$ . The map  $\bar{\varphi}$  referred to in the theorem is the one that sends a non-empty fibre to its image:  $\bar{\varphi}(\bar{x}) = \varphi(x)$ . For any surjective map of sets  $\varphi : G \rightarrow G'$ , one can form the set  $\overline{G}$  of fibres, and then one obtains a diagram as above, in which  $\bar{\varphi}$  is the bijective map that sends a fibre to its image. When  $\varphi$  is a group homomorphism,  $\bar{\varphi}$  is an isomorphism because

$$\bar{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(\overline{a})\bar{\varphi}(\overline{b}).$$

□

**Corollary 2.2.** *Let  $\varphi : G \rightarrow G'$  be a group homomorphism with kernel  $N$  and image  $H'$ . The quotient group  $\overline{G} = G/N$  is isomorphic to the image  $H'$ .*

# Chapter 3

## Vector Space

### 3.1 Subspace of $\mathbb{R}^n$

Vector spaces, which are the focus of this chapter, can be thought of as subsets within the realm of  $\mathbb{R}^n$ , where  $n$  represents the number of dimensions in real-numbered vector space. This topic is explored further in the current section, with a formal definition provided in Section 3.3.

While row vectors are more compact, column vectors are preferred due to their compatibility with matrix multiplication. For efficiency in written form, we often represent a column vector as  $(a_1, \dots, a_n)^t$  using the transpose operation. As established in Chapter 1, we treat a column vector and a point in  $\mathbb{R}^n$  with identical coordinates as equivalent. Typically, column vectors are indicated by lower-case letters like  $v$  or  $w$ . When  $v$  corresponds to  $(a_1, \dots, a_n)^t$ , this particular representation is referred to as the coordinate vector of  $v$ .

We consider two operations on vectors:

$$\begin{array}{lll} \text{vector addition:} & \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} & = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}, \\ \text{scalar multiplication:} & c \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} & = \begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix}. \end{array}$$

These operations make  $\mathbb{R}^n$  into a vector space.

**Definition 3.1** (Subspace). A subset  $W$  of  $\mathbb{R}^n$  is a subspace if it has these properties:

- a. If  $w$  and  $w'$  are in  $W$ , then  $w + w'$  is in  $W$ .

- b. If  $w$  is in  $W$  and  $c$  is in  $\mathbb{R}$ , then  $cw$  is in  $W$ .
- c. The zero vector is in  $W$ .

There is another way to state the conditions for a subspace,

Let  $W$  be a non-empty set. If  $w_1, w_2, \dots, w_n$  are elements of  $W$  and  $c_1, c_2, \dots, c_n$  are scalars, then the linear combination  $c_1w_1 + c_2w_2 + \dots + c_nw_n$  is also in  $W$ .

**Definition 3.2** (Nullspace). Given an  $m \times n$  matrix  $A$  with coefficients in  $\mathbb{R}$ , the set of vectors in  $\mathbb{R}^n$  whose coordinate vectors solve the homogeneous equation  $AX = 0$  is called the nullspace of  $A$ .

**Example 3.1.** (Example for subspaces) Systems of homogeneous linear equations.

Given an  $m \times n$  matrix  $A$  with coefficients in  $\mathbb{R}$ , the set of vectors in  $\mathbb{R}^n$  whose coordinate vectors solve the homogeneous equation  $AX = 0$  is a subspace, called the nullspace of  $A$ . Though this is very simple, we will check the conditions for a subspace:

- Suppose that  $X$  and  $Y$  be solutions of given homogenous sysmstem. Then  $AX = 0$  and  $AY = 0$ . Thus,

$$A(X + Y) = AX + AY = 0 + 0 = 0$$

Thus,  $(X + Y)$  is a solution.

- If  $X$  and  $Y$  be solutions of given homogenous sysmstem. Then  $AX = 0$ . Let  $c \in \mathbb{R}$ .

$$A(cX) = c(AX) = c \cdot 0 = 0$$

Thus,  $cX$  is a solution.

- $A0 = 0$ . Thus, the zero vector  $0$  is solution.

Therfore nullspace of  $A$  is a subspace.

**Example 3.2.** The zerospace  $W = \{0\}$  and the whole space  $W = \mathbb{R}^n$  are subspaces.

**Definition 3.3** (Proper Subspace). A subspace is called a proper subspace if it's not the entire space

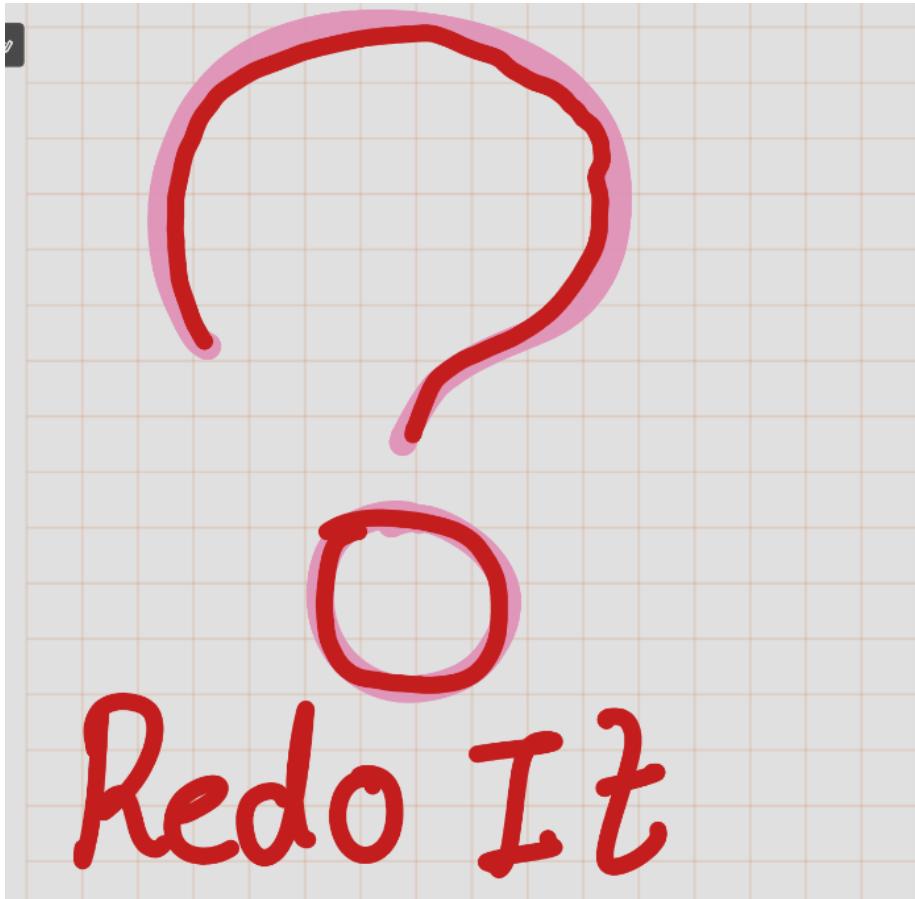
The next proposition describes the proper subspaces of  $\mathbb{R}^2$ .

**Proposition 3.1.** *Let  $W$  be a proper subspace of the space  $\mathbb{R}^2$ , and let  $w$  be a non-zero vector in  $W$ . Then  $W$  consists of the scalar multiples  $cw$  of  $w$ . Distinct proper subspaces have only the zero vector in common.*

**Definition 3.4.** The subspace consisting of the scalar multiples  $cw$  of a given nonzero vector  $w$  is called the subs pace **spanned by  $w$** .

Geometrically, it is a line through the origin in the plane  $\mathbb{R}^2$ .

*Proof.* (Proof of the proportion) Redo it.  $\square$



## 3.2 Fields

**Definition 3.5.** A field  $F$  is a set together with two laws of composition:

1. Addition:

$$+ : F \times F \rightarrow F \quad (3.1)$$

$$(a, b) \mapsto a + b \quad (3.2)$$

2. Multiplication

$$\times : F \times F \rightarrow F \quad (3.3)$$

$$(a, b) \mapsto ab \quad (3.4)$$

which satisfy these axioms:

- **(F1)** Addition makes  $F$  into an abelian group  $(F, +)$ ; its identity element is denoted by 0.
- **(F2)** Multiplication is commutative, and it makes the set of nonzero elements of  $F$  into an abelian group  $F^\times$ ; its identity element is denoted by 1.
- **(F3)** Distributive law:

$$\text{For all } a, b, \text{ and } c \in F, a(b + c) = ab + ac$$

The first two axioms describe properties of the two laws of composition, addition and multiplication, separately. The third axiom, the distributive law, relates the two laws.

We will be familiar with the fact that the real numbers satisfy these axioms, but the fact that they are the only ones needed for the usual algebraic operations can only be understood after some experience.

The next lemma explains how the zero element multiplies.

**Lemma 3.1.** *Let  $F$  be a field.*

- (a) *The elements 0 and 1 of  $F$  are distinct.*
- (b) *For all  $a$  in  $F$ ,  $a0 = 0$  and  $0a = 0$ .*
- (c) *Multiplication in  $F$  is associative, and 1 is an identity element.*

*Proof.*

- (a) Axiom (ii) implies that 1 is not equal to 0.
- (b) Since 0 is the identity for addition,  $0+0=0$ . Then  $a0+a0=a(0+0)=a0$ . Since  $(F, +)$  is a group, we can cancel  $a0$  to obtain  $a0=0$ , and then  $0a=0$  as well.
- (c) Since  $F \setminus \{0\}$  is an abelian group, multiplication is associative when restricted to this subset. We need to show that  $a(bc)=(ab)c$  when at least one of the elements is zero. In that case, (b) shows that the products in question are equal to zero. Finally, the element 1 is an identity on  $F \setminus \{0\}$ . Setting  $a=1$  in (b) shows that 1 is an identity on all of  $F$ .

□

**Example 3.3.**

- Real numbers ( $\mathbb{R}$ )  
Easy to verify
- Complex Numbers ( $\mathbb{C}$ )  
Easy to verify
- Prime field

$$\mathbb{F}_p := \overline{0}, \overline{1}, \dots, \overline{p-1} = \mathbb{Z}/p\mathbb{Z}$$

We saw in the previous chapter that the set  $\mathbb{Z}/n\mathbb{Z}$  of congruence classes modulo an integer  $n$  has laws of addition and multiplication derived from addition and multiplication of integers. All of the axioms for a field hold for the integers, except for the existence of multiplicative inverses. And as noted in previous chapters, such axioms carry over to addition and multiplication of congruence classes. But the integers are not closed under division, so there is no reason to suppose that congruence classes have multiplicative inverses. The class of 2, for example, has no multiplicative inverse modulo 6. It is somewhat surprising that when  $p$  is a prime integer, all nonzero congruence classes modulo  $p$  have inverses, and therefore the set  $\mathbb{Z}/p\mathbb{Z}$  is a field. In the next theorem, we prove the existence of multiplicative inverse of non-zero element in prime field.

**Theorem 3.1.** *Let  $p$  be a prime integer. Every nonzero congruence class modulo  $p$  has a multiplicative inverse, and therefore  $\mathbb{F}_p$  is a field of order  $p$ .*

We discuss the theorem before giving the proof.



# Chapter 4

## Exercises

### 4.1 Chapter 1

### 4.2 Chapter 2

#### 4.2.1 Laws of composition

**Exercise 4.1** (Artin 2.1.1). Let  $S$  be a set. Prove that the law of composition defined by  $ab = a$  for all  $a$  and  $b$  in  $S$  is associative? For which sets does this law have an identity?

**Solution:** Let  $a, b, c \in S$ . Now consider following

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

Thus, the given law of composition is associative.

If the given law of composition has an identity element whenever every element  $a \in S$  has a multiplicative inverse./ In other words, for every element  $a \in S$ , there exists an element  $e \in S$  such that

$$ae = ea = a.$$

Thus,  $ae = a = ea = e$ . So, the identity element is the same as every element in  $S$ , and the law has an identity for all sets  $S$ . Thus, only singletons sets have this given law of compositions have identity.

**Exercise 4.2** (Artin 2.1.2). Prove the properties of inverses that are listed near the end of the section.

- If an element  $a$  has both a left inverse  $l$  and a right inverse  $r$ , then  $r = l$ ,  $a$  is invertible and  $r$  is its inverse.

*Proof.* Since  $l$  is a left inverse for  $a$ , then  $la = 1$ . In the same way, since  $r$  is a right inverse for  $a$  the equality  $ar = 1$  holds. Let us now consider the expression  $lar$ . By associativity of the composition law in a group we have  $r = 1r = (la)r = lar = l(ar) = l1 = l$ . This implies that  $l = r$ . Since  $l = r$ , it holds also that  $ar = 1 = la = ra$  hence  $a$  is invertible and  $r$  is its inverse.  $\square$

- If  $a$  is invertible, its inverse is unique.

*Proof.* Let  $i_1$  and  $i_2$  be inverses of  $a$ . In particular  $i_1$  is a left inverse of  $a$  and  $i_2$  is a right inverse of  $a$ . By point (a)  $i_1 = i_2$ .  $\square$

- Inverses multiply in the opposite order: if  $a$  and  $b$  are invertible, then the product  $ab$  is invertible and  $(ab)^{-1} = b^{-1}a^{-1}$ .

*Proof.* In order to show that  $ab$  is invertible, it is enough to exhibit an element that is a right and a left inverse of  $ab$ . The element  $b^{-1}a^{-1}$  is a right inverse of  $ab$  since  $abb^{-1}a^{-1} = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$ . It is a left inverse since  $b^{-1}a^{-1}ab = b^{-1}(a^{-1}a)b = b^{-1}b = b^{-1}b = 1$ . This proves that  $ab$  is invertible and that  $b^{-1}a^{-1}$  is its inverse.  $\square$

### 4.2.2 Groups and Subgroups

**Exercise 4.3** (Artin 2.2.1). Make a multiplication table for the symmetric group  $S_3$ .

**Solution**

$\circ$	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(123)	(132)	(13)	(23)
(13)	(13)	(123)	e	(132)	(23)	(12)
(23)	(23)	(132)	(123)	e	(12)	(13)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

**Exercise 4.4** (Artin 2.2.2). Let  $S$  be a set with an associative law of composition and with an identity element. Prove that the subset consisting of the invertible elements in  $S$  is a group.

*Proof.* Let  $S^* \subseteq S$  with consisting of the invertible elements in  $S$ .

- *identity* : We are given identity element  $1 \in S$  and  $(1^{-1})(1) = 1 \implies 1 \in S^*$ .
- *Closure* : So let  $a, b \in S^*$ . Then  $a, b$  are invertible. Let  $a^{-1}, b^{-1} \in S^*$  be inverses of  $a$  and  $b$  respectively. Now we need to check  $ab \in S^*$ .

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e = aa^{-1} = a(bb^{-1})a^{-1} = (ab)(b^{-1}a^{-1})$$

□

Thus,  $(ab)^{-1} = b^{-1}a^{-1}$ . So,  $ab \in S^*$  Therefore,  $S^*$  is closed under the composition.

- *Associativity*: The associativity property inherit from the group  $S$ .

Therefore,  $S^*$  is a group.

**Exercise 4.5** (Artin 2.2.3). Let  $G$  be a group. Let  $x, y, z, w \in G$ .

- Solve for  $y$ , given that  $xyz^{-1}w = 1$ .
- Suppose that  $xyz = 1$ . Does it follow that  $yzx = 1$ ? Does it follow that  $yxz = 1$ ?

**Solution:**

a.

Let  $x, y, z, w \in \mathbb{N}$

$$x(yz)^{-1}w = 1$$

$$x^{-1}(x(yz)^{-1}w) = x^{-1}(x^{-1}) \quad (\text{Property of equality})$$

$$(x^{-1}x)(yz)^{-1}w = x^{-1} \quad (\text{Associativity})$$

$$1(yz)^{-1}w = x^{-1} \quad (\text{Identity } \rightarrow \text{Inverse})$$

$$yz^{-1}w = x^{-1} \quad (\text{Identity})$$

$$y(z^{-1}w) = x^{-1}w^{-1} \quad (\text{Property of equality})$$

$$y(z^{-1}w^{-1}) = x^{-1}w^{-1} \quad (\text{Associativity})$$

$$y(z^{-1})^{-1} = x^{-1}w^{-1} \quad (\text{Inverse})$$

$$y(z^{-1}) = x^{-1}w^{-1} \quad (\text{Identity})$$

$$y(z^{-1}z) = x^{-1}w^{-1}z \quad (\text{Property of equality})$$

$$y(z^{-1}z) = x^{-1}w^{-1}z \quad (\text{Associativity})$$

$$y_1 = x^{-1}w^{-1}z \quad (\text{inverse})$$

$$y = x^{-1}w^{-1}z \quad (\text{Identity})$$

b.

$xyz = 1$ $x^{-1}(xyz) = x^{-1}$ $(x^{-1}x)(yz) = x^{-1}$ $1(yz) = x^{-1}$	$yz = x^{-1}$ $(yz)x = x^{-1}x = 1$ $yzx = 1$
-------------------------------------------------------------------------------------	-----------------------------------------------------

- The given statement is false.

$$xyz = 1 \quad (4.1)$$

$$x^{-1}(xyz) = x^{-1} \cdot 1 \quad (4.2)$$

$$(x^{-1}x)(yz) = x^{-1} \quad (4.3)$$

$$1 \cdot (yz) = x^{-1} \quad (4.4)$$

$$(yz) = x^{-1} \quad (4.5)$$

$$(yz)z^{-1} = x^{-1}z^{-1} \quad (4.6)$$

$$y(zz^{-1}) = x^{-1}z^{-1} \quad (4.7)$$

$$y \cdot 1 = x^{-1}z^{-1} \quad (4.8)$$

$$yx = x^{-1}z^{-1}x \quad (4.9)$$

$$yxz = x^{-1}z^{-1}xz \quad (4.10)$$

$$(4.11)$$

If  $G$  is not abelian or  $z \neq x$ .  $xyz = 1 \Rightarrow yxz = 1$ .

**Exercise 4.6** (Artin 2.2.4). In which of the following cases is  $H$  a subgroup of  $G$ ?

(a)  $G = GL_n(\mathbb{C})$  and  $H = GL_n(\mathbb{R})$ .

(b)  $G = \mathbb{R}^\times$  and  $H = \{1, -1\}$ .

(c)  $G = \mathbb{Z}^+$  and  $H$  is the set of positive integers.

(d)  $G = \mathbb{R}^+$  and  $H$  is the set of positive reals.

(e)  $G = GL_2(\mathbb{R})$  and  $H$  is the set of matrices  $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$  with all entries equal to 0.

**Solution:**

(a)

- *Subset ?* : Since every matrix with real entries can be interpreted as a matrix with complex entries, we conclude that  $H \subset G$ .
- *Closure ?* : For every  $A, B \in GL_n(\mathbb{R})$  we have  $AB \in GL_n(\mathbb{R})$  since Product of invertible matrices is invertible. I proved this result in chapter 1.
- *Identity ?* : The identity in  $G$  is  $I_n$ , the identity  $n \times n$  matrix. Observe that  $I_n \in H = GL_n(\mathbb{R})$ . (Because every entry of  $I_n$  is 1 or 0)

- *Inverse ?*:  $GL_n(\mathbb{R})$  is the set of  $n \times n$  invertible matrices with real entries. So, all the elements in  $H$  is invertible.

Therefore,  $H \leq G$

(b)

- *Subset ?* : This is trivial  $\{-1, 1\} \subset \mathbb{R}^\times$
- *Closure ?* :

$$1 \times 1 = 1 \in H \quad (4.12)$$

$$(-1) \times 1 = (-1) \in H \quad (4.13)$$

$$1 \times (-1) = (-1) \in H \quad (4.14)$$

$$(-1) \times (-1) = -1 \in H \quad (4.15)$$

$$(4.16)$$

Thus,  $H$  is closed. - *Identity ?* : The identity in  $G$  is 1, which is also in  $H$ .

- *Inverse ?* :

$$1 \times 1 = 1 \implies (1)^{-1} = 1 \in H \quad (4.17)$$

$$(-1) \times (-1) = 1 \implies (-1)^{-1} = (-1) \in H \quad (4.18)$$

Therefore,  $H$  is sub group of  $G$ .

- (c) Note that  $2 \in H$ , but inverse of 2 in  $\mathbb{Z}^+$  is  $(-2) \notin H$ .  
Therefore,  $H$  is not a subgroup of  $G$ .

(d)

- *Subset ?* : This is trivial.  $H \subset \mathbb{R}^\times$
- *Closure ?* : Product of positive real number is positive. Thus,  $H$  is closed.
- *Identity ?* : 1 is the identity of  $G$ , which is in  $H$ .
- *Inverse ?* : Let  $a \in H$ . Then,

$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$$

So,  $\frac{1}{a} \in H$  is the inverse of  $a$ . Thus,  $H$  is closed under inverses.

- (e) Let  $A = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ . Then  $A \in H$ . But observe that  $\det(A) = 0 \implies A$  is not invertible. Thus,  $A \notin H$ . Thus, this  $H \not\subseteq G$ .

Therefore,  $H$  is not a subgroup of  $G$ .

**Exercise 4.7** (Artin 2.2.5). In the definition of a subgroup, the identity element in  $H$  is required to be the identity of  $G$ . One might require only that  $H$  have an identity element, not that it need be the same as the identity in  $G$ .

- Show that if  $H$  has an identity at all, then it is the identity in  $G$ .
- Show that the analogous statement is true for inverses.

Claim:  $H$  is a subgroup of group  $G$ . The identity element of  $H$  is equal to identity element of  $G$

Let  $G$  be group and  $H \leq G$ .

Let us assume that  $e_H$  and  $e_G$  be two identity in  $H$  and  $G$ . Let  $a \in H$ .

Since  $H \leq G$ ,  $a \in G$ .

Since  $e_H$  is the identity of  $H$

$$a * e_H = a = e_H * a \quad \textcircled{1}$$

Since  $e_G$  is the identity of  $G$ .

$$a * e_G = a = e_G * a \quad \textcircled{2}$$

Thus, by (1) and (2),

$$a * e_H = a * e_G$$

$$e_H = e_G \quad (\text{cancellation law})$$

Thus So,

~~Th~~ir claim:  $H$  is subgroup of group  $G$ . The inverse of any element in  $H$  equal to the inverse of same element.

Proof:

Let  $G$  be a group and  $H \leq G$ . Let  $a \in H$

Let  $b$  and  $c$  be two inverse elements of  $a$  in  $H$  and  $G$  respectively. ~~Let~~

Let Since  $b$  be the inverse element of  $a$ .

$$a * b = e = b * a \quad \text{--- (1)}$$

Since  $c$  is the inverse element of  $a$ .  
Further  $\overset{\text{since}}{H \leq G}$ , then  $a \in H \Rightarrow a \in G$ .

$$a * c = e = c * a \quad \text{--- (2)}$$

By (1) and (2)  $a * b = a * c$

Thus,  $b = c$  (By cancellation law)

**Exercise 4.8** (Artin 2.2.6). Let  $G$  be a group. We define an opposite group  $G^\circ$  with the law of composition  $a * b$  as follows: - The underlying set is the same as  $G$ , - but the law of composition is  $a * b = ba$ .

Prove that  $G^\circ$  is a group.

**Solution:**

Let  $G$  be a group. Define opposite group  $G^\circ$  with law of composition  $a * b$  as follows.

- The underline set is same as  $G$ .
- Law of composition  $a * b = ba$ .

Need to show  $a * b = ba \in G^\circ$  is a group.

Let  $a, b, c \in G^\circ$ . Then  $a, b, c \in G$ .

- Closure:  $a * b = ba \in G \Rightarrow a * b = ba \in G^\circ$ .  
Thus,  $\text{is closed under } *$
- Identity: Let  $e$  be the identity of  $G$ .  
Then  $e \in G^\circ$ .  
Claim: Observe following.

$$e * a = ae = a = ea = a * e$$

Thus,  $e \in G^\circ$  is the identity of  $G^\circ$ .

- Inverse: Since  $G$  is a group  
 $a^{-1} \in G$  exists. Then  $a^{-1} \in G^\circ$ . Observe  
 $a^{-1} * a = aa^{-1} = e = a^{-1}a = a * a^{-1}$   
Thus,  $a^{-1}$  is the inverse of  $a$  in  $G^\circ$ .
- Associativity:

$$\begin{aligned} (a * (b * c)) &= a * (cb) = (cb)a = c(cba) \quad (\text{since } G \text{ is a group}) \\ &= c(a * b) = (a * b) * c \end{aligned}$$

Thus associativity holds in  $G^\circ$ .

Therefore,  $G^\circ$  is a group.

### 4.2.3 Subgroups of the Additive Group of Integers

**Exercise 4.9** (Artin 2.3.1). Let  $a = 123$  and  $b = 321$ . Compute  $d = \gcd(a, b)$ , and express  $d$  as an integer combination  $ra + bs$ .

We use Euclidean Algorithm.

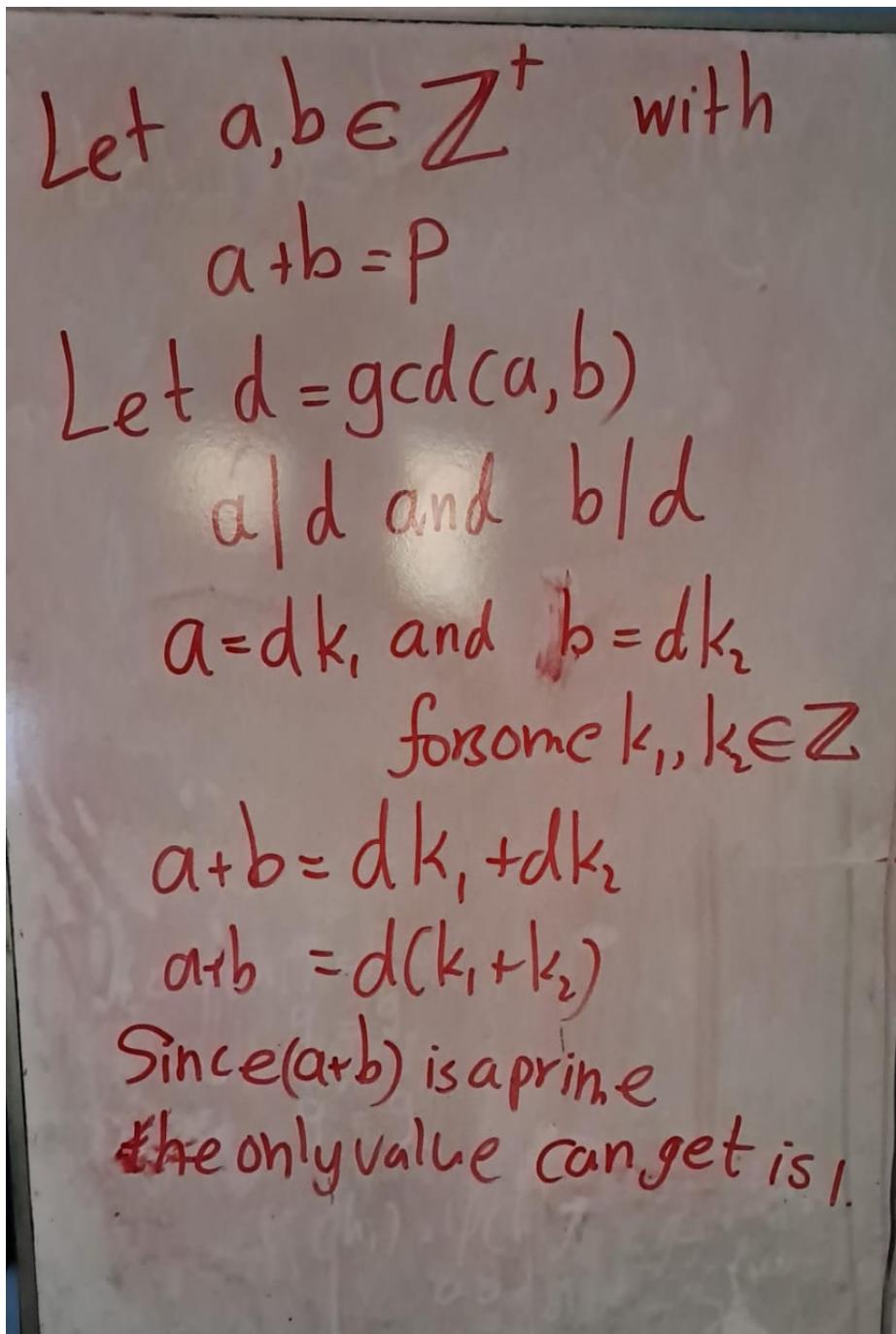
$$\begin{aligned}
 321 &= 2(123) + 75 \\
 123 &= 1(75) + 48 \\
 75 &= 1(48) + 27 \\
 48 &= 1(27) + 21 \\
 27 &= 1(21) + 6 \\
 21 &= 3(6) + 3 \\
 6 &= 3(2) + 0
 \end{aligned}$$

Thus  $\gcd(123, 321) = 3$ . Now let's back-substitute it.

$$\begin{aligned}
 3 &= 21 - 3(6) \\
 3 &= 1(21) - 3(27 - 1(21)) \\
 &= 1(21) - 3(27) + 3(21) \\
 &= 4(21) - 3(27) \\
 &= 4(48 - 1(27)) - 3(27) \\
 &= 4(48) - 7(27) \\
 &= 4(48) - 7(75 - 1(48)) \\
 &= 11(48) - 7(75) \\
 &= 11(123 - 1(75)) - 7(75) \\
 &= 11(123) - 18(75) \\
 &= 11(123) - 18(321 - 2(123)) \\
 &= 47(123) - 18(321)
 \end{aligned}$$

**Solution:**

**Exercise 4.10** (Artin 2.3.2). Prove that if  $a$  and  $b$  are positive integers whose sum is a prime  $p$ , their greatest common divisor is 1.



Solution:

Exercise 4.11 (Artin 2.3.3).

- Define the greatest common divisor of a set  $\{a_1, \dots, a_n\}$  of  $n$  integers. Prove that it exists, and that it is an integer combination of  $a_1, \dots, a_n$ .
- Prove that if the greatest common divisor of  $\{a_1, \dots, a_n\}$  is  $d$ , then the greatest common divisor of  $\{a_1/d, \dots, a_n/d\}$  is 1.

**Solution:**

a.

Let  $\{a_1, \dots, a_n\}$  be a set of integers.

Let  $S := a_1\mathbb{Z} + \dots + a_n\mathbb{Z} := \left\{ n \in \mathbb{Z} \mid n = r_1a_1 + r_2a_2 + \dots + r_na_n \text{ for some } r_1, \dots, r_n \in \mathbb{Z} \right\}$

claim:  $S \leq (\mathbb{Z}, +)$

• subset: clearly  $S \subseteq (\mathbb{Z}, +)$

• closure: let  $x, y \in S$ .

Then  $x = r_1a_1 + \dots + r_na_n$  for some  $r_1, \dots, r_n \in \mathbb{Z}$

and  $y = \tilde{r}_1a_1 + \dots + \tilde{r}_na_n$  for some  $\tilde{r}_1, \dots, \tilde{r}_n \in \mathbb{Z}$

$$x+y = r_1a_1 + \dots + r_na_n + \tilde{r}_1a_1 + \dots + \tilde{r}_na_n$$

$$= (r_1 + \tilde{r}_1)a_1 + \dots + (r_n + \tilde{r}_n)a_n \in S$$

Thus  $x+y \in S$

• Inverse: Let  $x \in S$ .

Then  $x = r_1a_1 + \dots + r_na_n$  for some  $r_1, \dots, r_n \in \mathbb{Z}$

claim: Inverse of  $x$  is  $y = (-r_1)a_1 + \dots + (-r_n)a_n$

$$x+y = r_1a_1 + \dots + r_na_n + (-r_1)a_1 + \dots + (-r_n)a_n$$

$$= (r_1 - r_1)a_1 + \dots + (r_n - r_n)a_n = 0a_1 + \dots + 0a_n = 0$$

$$y+x = (-r_1)a_1 + \dots + (-r_n)a_n + r_1a_1 + \dots + r_na_n$$

$$= (-r_1 + r_1)a_1 + \dots + (-r_n + r_n)a_n = 0a_1 + \dots + 0a_n = 0$$

Thus  $y$  is the inverse of  $x$  and since  $-r_1, \dots, -r_n \in \mathbb{Z}$ ,  $y \in S$ .

Therefore  $S$  is a subgroup of  $\mathbb{Z}$ .

By artins book thm 2.3.3 there exist a positive integer  $d$  such that

$$d\mathbb{Z} = a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$$

This  $d$  is define as  $\gcd(a_1, \dots, a_n)$

### Linear Combination

Note that  $d \in \mathbb{Z}$   $d = a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$

Thw, there exist  $r_1, \dots, r_n \in \mathbb{Z}$  such that

$$d = r_1a_1 + \dots + r_na_n$$

b.

b) Now suppose that  $d = \gcd(a_1, \dots, a_n)$

Now let  $e$  be an positive integer and common divisor of  $a_1/d, a_2/d, \dots, a_n/d$ . We know that exist, at least we can get  $e$  as,

Then  $\frac{a_i}{d} = ek_i$  for some  $k_i \in \mathbb{Z}$  for all  $i=1, 2, \dots, n$

$$a_i = (ed)k_i \text{ for all } i=1, 2, \dots, n$$

Thus  $ed | a_i$  for all  $i=1, 2, \dots, n$

By Artins Thm 223 c)  $ed | d$ .

Thus,  $ed \leq d$ ,

$$e \leq 1.$$

Since  $e$  is a positive integer,  $e=1$ .

#### 4.2.4 Cyclic group

**Exercise 4.12** (Artin 2.4.1). Let  $a$  and  $b$  be elements of a group  $G$ . Assume that  $a$  has order 7 and that  $a^3b = ba^3$ . Prove that  $ab = ba$ .

**Solution:**

Given that  $a^7 = 1$   
 $a(a^6) = 1 = (a^6)a$   
 Thus,  $a^{-1} = a^6$

$$\begin{aligned}
 ba^3 &= a^3 b \\
 (ba^3b^{-1})^2 &= a^3 \\
 (ba^3b^{-1})(ba^3b^{-1}) &= a^6 \\
 ba^3(b^{-1}b)a^3b^{-1} &= a^{-1} \\
 ba^6b^{-1} &= a^{-1} \\
 ba^6 &= a^{-1}b \\
 ba^{-1} &= a^{-1}b \\
 ab^{-1} &= b \\
 ab &= ba
 \end{aligned}$$

**Exercise 4.13** (Artin 2.4.2). An  $n$ th root of unity is a complex number  $z$  such that  $z^n = 1$ .

- (a) Prove that the  $n$ th roots of unity form a cyclic subgroup of  $\mathbb{C}^\times$  of order  $n$ .
- (b) Determine the product of all the  $n$ th roots of unity.

If  $z^n = 1$  then

$$z = \exp\left(\frac{2\pi i k}{n}\right), \quad k=0, 1, \dots, n-1$$

$$\begin{aligned} \text{Let } S &:= \left\{ e^{\frac{2\pi i k}{n}} \mid k=0, 1, 2, \dots, n-1 \right\} \\ &= \left\{ e^0, e^{\frac{2\pi i}{n}}, \dots, e^{\frac{2\pi i(n-1)}{n}} \right\} \end{aligned}$$

Solution: First let's check  $S$  is a subgroup of  $\mathbb{C}^\times$

• Subset : It is trivial that  $S \subseteq \mathbb{C}^\times$

• Closure : Let  $x, y \in S$ . Then

$$x = e^{\frac{2\pi i k_1}{n}} \text{ and}$$

$$y = e^{\frac{2\pi i k_2}{n}} \text{ for some } k_1, k_2 = 0, 1, \dots, n-1$$

$$\begin{aligned} \text{Then, } xy &= e^{\frac{(2\pi i k_1)}{n}} \cdot e^{\frac{(2\pi i k_2)}{n}} \\ &= e^{\frac{2\pi i (k_1 + k_2)}{n}} \end{aligned}$$

If  $(k_1+k_2) > n$ , we can find  $a, b \in \mathbb{N}$   
such that (by division algorithm)

$$k_1 + k_2 = an + b, \quad 0 \leq b < n$$

$$\begin{aligned} xy &= e^{\frac{2\pi i(k_1+k_2)}{n}} \\ &= e^{\frac{2\pi i}{n}(an+b)} \\ &= e^{2\pi i(a)} \cdot e^{\frac{2\pi i b}{n}} \\ &= 1 \times e^{\frac{2\pi i b}{n}} \\ &= e^{\frac{2\pi i b}{n}}, \text{ for some } b = 0, 1, 2, \dots, n-1 \end{aligned}$$

Thus,  $xy \in S$

- Inverse: Let  $x \in S$ .

◦ If  $x=1$ , then  $x^{-1}=1$ .

◦ If  $x \neq 1$ ,

Then  $x = e^{\exp(2\pi i k_1/n)}$  for some  $k_1 = 1, 2, \dots, n-1$   
choose  $y = e^{\exp(2\pi i (n-k_1)/n)}$

$$\begin{aligned} \text{Then, } xy &= e^{\frac{2\pi i k_1}{n}} \cdot e^{\frac{2\pi i (n-k_1)}{n}} = e^{\frac{2\pi i (k_1 + n - k_1)}{n}} \\ &= e^{\frac{2\pi i n}{n}} = e^{2\pi i} = 1 \end{aligned}$$

Thus,  $x^{-1} = y \in S$ .

By subgroup test  $S$  is a subgroup of  $G$ .

Now, we are done subgrouping. Now we have to look the cyclic property.

Observe that  $(e^{\frac{2\pi i}{n}})^k = e^{\frac{2\pi i k}{n}}, k=0, 1, \dots, n-1$

Therefore,  $S = \langle e^{\frac{2\pi i}{n}} \rangle$

$$\begin{aligned}
 b) \prod_{k=0}^{n-1} e^{\frac{2\pi i k}{n}} &= e^{\left(\sum_{k=0}^{n-1} \frac{2\pi i k}{n}\right)} \\
 &= e^{\frac{2\pi i}{n} \left(\sum_{k=0}^{n-1} k\right)} \\
 &= e^{\frac{2\pi i}{n} \left(\frac{n(n-1)}{2}\right)} \\
 &= e^{\pi i (n-1)} \\
 &= (e^{i\pi})^{n-1} \quad (\because e^{i\pi} = -1) \\
 &= (-1)^{n-1}
 \end{aligned}$$

**Exercise 4.14** (Artin 2.4.3). Let  $a$  and  $b$  be elements of a group  $G$ . Prove that  $ab$  and  $ba$  have the same order

*Proof.* Let  $a$  and  $b$  be elements in a group  $G$  with identity  $e$ .

Suppose that  $ab$  has finite order  $n$ . Then  $(ab)^n = e$  and  $n$  is the smallest positive integer for which this equation is true. We also have that

$$(ba)^{n+1} = (ba)(ba) \cdots (ba) = b \underbrace{(ab) \cdots (ab)}_{n \text{ times}} a = b(ab)^n a = a(ba)^m b = bea = ba.$$

Thus, since  $(ba)^{n+1} = (ba)^n(ba)$  we can conclude that  $(ba)^n(ba) = ba$  and then by the cancellation law, we have that  $(ba)^n = e$ .

Now, to show that the order of  $ba$  is  $n$ , we need to demonstrate that  $n$  is the smallest positive integer such that  $(ba)^n = e$ .

Suppose there exists a positive integer  $m < n$  such that  $(ba)^m = e$ . Then,

$$(ab)^{m+1} = (ab)(ab) \cdots (ab) = a \underbrace{(ba) \cdots (ba)}_{m \text{ times}} b = a(ba)^m b = aeb = ab.$$

Thus, since  $(ab)^{m+1} = (ab)^m(ab)$  we have that  $(ab)^m(ab) = ab$  and then by the cancellation law, we have that  $(ab)^m = e$  which contradicts the fact that  $n$  is the smallest positive integer such that  $(ab)^n = e$ .

Hence,  $n$  is the smallest positive integer such that  $(ba)^n = e$  and therefore  $(ba)$  has finite order  $n$ .  $\square$

**Exercise 4.15** (Artin 2.4.4). Describe all groups  $G$  that contain no proper subgroup

The easiest example is the trivial group.  $\{1\}$   
But we are not interested.

Let  $G$  be a non-trivial group no proper subgroup.

Claim:  $G$  is cyclic.

Assume that  $G$  is not cyclic.

Since  $G \neq \{1\}$ , there exist  $1 \neq a, b \in G$ , such that

$$b \notin \langle a \rangle$$

Thus  $\langle a \rangle$  is proper subgroup of  $G$ .

Since  $a \neq 1$ ,  $\langle a \rangle \neq \{1\}$ . This is  
contradict the choice of  $G$ .

Therefore  $G$  is cyclic.

Therefore there exist  $p \in G$  such that  
 $G = \langle p \rangle$  here  $p \neq 1$ .

Solution:

claim:  $G$  has a finite order.

Assume the contrary,  $G$  has infinite order.

Then consider,  $\bigvee H = \langle p^2 \rangle$

Note that  $H \leq G$ . Since  $p \notin \langle p^2 \rangle = H$ ,  $H$  is proper subgroup. This contradicts the choice of  $G$ . Therefore  $H$  has finite order.

So, let's say  $G$  has order  $n$ . (i.e.  $|G| = |\langle p \rangle| = n$ )

$$G = \langle p \rangle := \{1, p, p^2, \dots, p^{n-1}\}$$

So, let's investigate further,

Let's consider  $H' := \langle p^k \rangle$ , where  $k = 0, 1, \dots, n-1$

- if  $k=0$  then  $H' = \langle 1 \rangle = \{1\}$  trivial group that we are interested

- if  $k=1$  then  $H' = \langle p \rangle = H$ , this gives whole group.

- otherwise

Let  $d = \gcd(k, n)$ . By Artin's Thm 2.43, order of  $p^k$  is  $n/d$ . Thus  $|\langle p^k \rangle| = n/d$ .

if  $d \neq 1$ , then there might be a problem

if  $d \neq 1$ , then  $\langle p^k \rangle$  is proper subgroup. Because of the number of elements.

claim: Order of  $G$  is prime.

Assume the contrary that order of  $G = n$  is not prime

Previously, we saw that  $\langle p^k \rangle = H^1$  is proper subgroup  
So, it is contradiction. Thus  $G$  has prime order.

Therefore it is necessary for  $G$  to be prime order.

Is it sufficient?

Let  $G$  be a cyclic group of prime order.

Let  $G = \langle p \rangle$  and  $|G| = |\langle p \rangle| = n$ ;  $n$  is a prime number.

Then "Has  $G$  have prime order?"

Let  $H$  be a non-trivial subgroup of  $G$ .

Define,

$$S = \{ k \mid k \in \{1, 2, \dots, n\} \text{ and } p^k \in H \} \subseteq \{1, 2, \dots, n\}$$

Let  $k_0 = \min(S)$ . By well-ordering principle we know that  $\min(S)$  exists.

claim:  $H = \langle p^{k_0} \rangle$

subclaim<sub>1</sub>:  $\langle p^{k_0} \rangle \subseteq H$ .

Note that  $p^{k_0} \in H$ .

Let  $x \in \langle p^{k_0} \rangle$ . Then  $x = (p^{k_0})^m$  for some  $m \in \mathbb{Z}$

Thus  $x = \underbrace{p^{k_0} \cdot p^{k_0} \cdots p^{k_0}}_{m\text{-times}} \in H$  (Since  $H$  is a group.)

$\langle p^{k_0} \rangle \subseteq H$

subclaim<sub>2</sub>:  $\langle p^{k_0} \rangle \supseteq H$ .

Let  $y \in H$ . Since  $H$  is a subgroup of  $G$ ,  $y \in G$ .

Then,  $y = p^l$  for some  $l$ .

By division algorithm,  $l = qk_0 + r$ , where  $0 \leq r < k_0$

$$y = p^l = p^{(qk_0+r)} = (p^{k_0})^q \cdot p^r$$

claim:  $p^r \in H$

Note that  $p^l \in H$  and  $(p^{k_0})^q \in H$ . Thus,

$$p^r = p^{l-k_0q} = p^l \cdot (p^{k_0})^{q-1} \in H.$$

claim:  $r=0$

otherwise, if  $r > 0$ , since  $p^r \in H$ , then  $r \in S$ .

Since  $r < k_0$ . This is a contradiction because  $k_0$  is the  $\min(S)$ .

Thus  $r=0$ .

Therefore,  $y = p^l = p^{k_0} = (p^{k_0})^q \in \langle p^{k_0} \rangle$

Thus,  $\langle p^{k_0} \rangle \geq H$

By subclaim 1 and 2,  $\langle p^{k_0} \rangle = H$

Thus every subgroup of  $G$  in the form  $\langle p^s \rangle$ , where  $s=1, 2, \dots, n$

Since  $n$  is prime number,  $d = \gcd(s, n) = 1$  or  $n$

Observe that (order of  $p^s\right\rangle = |\langle p^s \rangle| = n/d$

$\rightarrow$  if  $d=1$  then  $|\langle p^s \rangle| = n/1 = n$ , then  $|\langle p^s \rangle| = n$

Thus,  $\langle p^s \rangle = G$ .

$\rightarrow$  if  $d=n$  then  $|\langle p^s \rangle| = n/n = 1$ , then  $|\langle p^s \rangle| = 1$

Thus,  $\langle p^s \rangle = \{1\}$  = trivial subgroup

Therefore, Every cyclic group  $G$  of prime order,  
 $G$  has no non-trivial subgroups.

Hence, Let  $G$  be a group

$G$  is cyclic group with prime order  $\iff G$  has no proper non-trivial subgroups.

**Exercise 4.16** (Artin 2.4.5). Prove that every subgroup of a cyclic group is cyclic. Do this by working with exponents, and use the description of the subgroups of  $(\mathbb{Z}, +)$ .

Let  $G$  be a cyclic group. Let  $G = \langle a \rangle$   
 Let  $H$  be a subgroup of  $G$  ( $H \leq G$ )

Define

$$S := \{k \in \mathbb{Z}, a^k \in H\}$$

claim:  $S \leq (\mathbb{Z}, +)$

- subset?: It is trivial  $S \subseteq (\mathbb{Z}, +)$
- closure?: Let  $k_1, k_2 \in S$ , Then  $a^{k_1}, a^{k_2} \in H$ . So,  

$$a^{(k_1+k_2)} = a^{k_1} \cdot a^{k_2} \in H \text{ (Since } H \text{ is subgroup)}$$

Thus,  $k_1 + k_2 \in S$ .

- Inverse?: Let  $k \in S$ . So,  $a^k \in H$ . Then  $\bar{a}^{k_1} = (a^k)^{-1} \in H$   
 $(\text{Because } H \text{ is subgroup})$   

$$\bar{a}^{k_1} \cdot a^{k_1} = a^{-k_1+k_1} = a^0 = 1 = a^0 = a^{k_1} \cdot \bar{a}^{k_1}$$

Thus,  $-k_1 + k_1 = 0 = k_1 - k$ , Thus, inverse of  $k_1$  is  $-k_1$ .

Therefore  $(S, +)$  is a subgroup of  $(\mathbb{Z}, +)$ .

i.e:  $(S, +) \leq (\mathbb{Z}, +)$

- If  $S = \{0\}$ , then  $H = \{1\}$  = trivial subgroup.
- If  $S$  is not trivial, by Artins Algebra book 2.33  
 $\exists b \in \mathbb{Z}$  such that  $S = b\mathbb{Z}$ .

$S_0$ ,

$$\begin{aligned} H &= \{a^k \mid k \in S\} = \{a^k \mid k \in b\mathbb{Z}\} \\ &= \{a^{ib} \mid i \in \mathbb{Z}\} = \langle a^b \rangle \end{aligned}$$

**Exercise 4.17** (Artin 2.4.6).

- (a) Let  $G$  be a cyclic group of order 6. How many of its elements generate  $G$ ?  
Answer the same question for cyclic groups of orders 5 and 8.
- (b) Describe the number of elements that generate a cyclic group of arbitrary order  $n$ .

**Solution:**

a)

CASE I: Order - 6

Let  $G$  be a cyclic group with order 6.

Let's say  $G = \langle a^7 \rangle$ ,

$$G := \{a^0=1, a^1, a^2, a^3, a^4, a^5\}$$

By Artin's book proposition 2.4.3,

$$|a^k| = |\langle a^k \rangle| = \frac{6}{\gcd(6, k)}, \text{ for all } k \in \{1, \dots, 5\}$$

$$\langle a^k \rangle = \langle a \rangle \iff |\langle a^k \rangle| = |\langle a \rangle|$$

$$\iff \frac{6}{\gcd(6, k)} = 6$$

$$\iff \gcd(6, k) = 1$$

$$\iff k = 1 \text{ or } k = 5$$

$$\langle a^1 \rangle = \langle a^5 \rangle = G$$

So,  $a, a^5$  generate  $G$ .

## CASE 2: order=5

Let  $G$  be a cyclic group with order 5.

Let's say  $G = \langle a^5 \rangle$

$$G := \{a^0, a^1, a^2, a^3, a^4\}$$

By Artin's book proposition 2.4.3,

$$|a^k| = |\langle a^k \rangle| = \frac{5}{\gcd(5, k)}, \text{ for all } k \in \{1, \dots, 5\}$$

$$\langle a^k \rangle = \langle a \rangle \iff |\langle a^k \rangle| = |\langle a \rangle|$$

$$\iff \frac{5}{\gcd(5, k)} = 5$$

$$\iff \gcd(5, k) = 1$$

$$\iff k = 1, 2, 3, 4$$

$$\langle a' \rangle = \langle a^2 \rangle = \langle a^3 \rangle = \langle a^4 \rangle = G.$$

$a', a^2, a^3, a^4$  generate  $G$ .

## CASE-III Order=8

Similar to above case, we can obtain that

$a', a^3, a^5, a^7$  generates  $G$ .

Let  $G$  be a group with order  $n$ .

By Artin's book proposition 2.4.3,  
 $|a^k| = |\langle a^k \rangle| = \frac{n}{\gcd(n, k)}$ , for all  $k \in \{1, \dots, n\}$

$$\begin{aligned} \langle a^k \rangle = \langle a \rangle &\iff |\langle a^k \rangle| = |\langle a \rangle| \\ &\iff \frac{n}{\gcd(n, k)} = k \\ &\iff \gcd(n, k) = 1 \end{aligned}$$

Thus  $a^k$  generates  $G \iff \gcd(n, k) = 1$   
Hence, number of generators of  $G = \left( \begin{array}{l} \text{number of integers} \\ 1 \leq k \leq n \text{ which are} \\ \text{relative prime } n \end{array} \right)$

b)

**Exercise 4.18** (Artin 2.4.7). Let  $x$  and  $y$  be elements of a group  $G$ . Assume that each of the elements  $x$ ,  $y$ , and  $xy$  has order 2. Prove that the set  $H = \{I, x, y, xy\}$  is a subgroup of  $G$ , and that it has order 4.

Let  $G$  be a group and  $x, y \in G$ . Suppose that

$$|x| = |y| = |xy| = 2$$

Let  $H = \{1, xy, xy\}$ .

claim:  $H \leq G$ .

- subset?:  $H \subseteq G$ . (It is trivial that  $1, xy \in G$  and since  $x, y \in G$ ,  $xy \in G\}$

- closure:

.	1	$x$	$y$	$xy$	
1	1	$x$	$y$	$xy$	By multiplication table, we can guarantee the closure.
$x$	$x$	1	$xy$	$y$	
$y$	$y$	$xy$	1	$xy = y^2 = x$	
$xy$	$xy$	$x$	$y$	1	

claim:  $xy = yx$

First of we have observe that

$$x^2 = y^2 = (xy)^2 = 1$$

Thus inverse of those elements are itself.

i.e:  $x^{-1} = x$ ,  $y^{-1} = y$ ,  $(xy)^{-1} = xy$  —  $\textcircled{*}$

$$\begin{aligned}
 (xy)^2 &= (xy)(xy) = 1 \\
 (xy) \bar{y}^1 &= \bar{y}^1 \\
 xyx &= \bar{y}^1 \\
 xyx\bar{x}^1 &= \bar{y}^1 \bar{x}^1 \\
 xy &= \bar{y}^1 \bar{x}^1 = yx \text{ (by *)}
 \end{aligned}$$

- Inverse:  $\bar{x}^1 = x, \bar{y}^1 = y, (xy)^{-1} = xy \in H$ .

Therefore,  $H$  is a subgroup of  $G$ .

Claim:  $|H| = 4$

- Since  $x, y, xy$  has order 2,  $H$  is not trivial.  
In other words,  $|H| \neq 1$ .

+ claim:  $x \neq y$

If  $x = y$ , then  $xy = x^2 = 1$ . This contradict the  $|xy| = 2$ .

+ claim:  $x \neq xy$

$$\begin{aligned}
 \text{if } x = xy \text{ then, } x &= xy \\
 x\bar{x} &= x\bar{y} \\
 x^2 &= x^1 y \\
 1 &= y.
 \end{aligned}$$

This contradict that  $|y| = 2$ .

+ claim  $y \neq xy$

If  $y = xy$  then

$$\begin{aligned} y &= xy \\ y^2 &= xxy \\ 1 &= x \end{aligned}$$

This contradicts that  $|x|=2$ .

Therefore,  $1 \neq x \neq y \neq xy$ . So every  $1, x, y, xy$  are distinct elements in  $H$ . Thus,  $|H|=4$

**Exercise 4.19** (Artin 2.4.8).

- a) Prove that the elementary matrices of the first and third types (1.2.4) generate  $GL_n(\mathbb{R})$ .
- b) Prove that the elementary matrices of the first type generate  $SL_n(K)$ . Do the  $2 \times 2$  case first.

Recall the types of elementary matrices,

(1.2.4)

*Type (i):*

$$i \begin{bmatrix} 1 & & i & j \\ & 1 & & \\ & & 1 & a \\ j & & & 1 \\ & & & 1 \end{bmatrix} \quad \text{or} \quad j \begin{bmatrix} 1 & & j & i \\ & 1 & & \\ & & 1 & 1 \\ i & & a & 1 \\ & & & 1 \end{bmatrix} \quad (i \neq j).$$

One nonzero off-diagonal entry is added to the identity matrix.

*Type (ii):*

$$i \begin{bmatrix} 1 & & i & j \\ & 0 & & \\ & & 1 & \\ j & & 1 & 0 \\ & & & 1 \end{bmatrix}$$

The  $i$ th and  $j$ th diagonal entries of the identity matrix are replaced by zero, and 1's are added in the  $(i, j)$  and  $(j, i)$  positions.*Type (iii):*

$$i \begin{bmatrix} 1 & & & i \\ & 1 & & \\ & & c & \\ & & & 1 \\ & & & 1 \end{bmatrix} \quad (c \neq 0).$$

One diagonal entry of the identity matrix is replaced by a nonzero scalar  $c$ .

**Exercise 4.20** (Artin 2.4.9). How many elements of order 2 does the symmetric group  $S_4$  contain?

- Elements in  $S_4$ , all the permutations  $\{1, 2, 3, 4\}$   
There are  $4! = 24$  elements in  $S_4$ .

clearly following elements are have order 2.

- |            |            |   |                                          |
|------------|------------|---|------------------------------------------|
| • $(1, 2)$ | • $(2, 3)$ | } | transpositions (2-cycle)<br>have order 2 |
| • $(1, 3)$ | • $(2, 4)$ |   |                                          |
| • $(1, 4)$ | • $(3, 4)$ |   |                                          |

\* 3-cycle have order 3, so, we ignore them

Further, following elements have order 2

- |                  |   |                |
|------------------|---|----------------|
| • $(1, 2)(3, 4)$ | } | disjoint cycle |
| • $(1, 3)(2, 4)$ |   |                |
| • $(1, 4)(2, 3)$ |   |                |

Therefore, there are 9-elements of order 2.

Additionally, I found this on the internet follow

There's not a simple formula known for this, and certain aspects of the question are the subject of ongoing research. For example, [this paper](#) summarizes some research that has been done on the maximum possible order for an element of  $S_n$ .

In general, the way to find the number of elements of order  $k$  in  $S_n$  is:

1. Determine all possible cycle types for an element of order  $k$ , and then
2. Determine the number of elements having each of these cycle types.

For step (1), you're just looking for all possible ways to partition  $n$  into cycles so that the least common multiple of the cycle lengths is  $k$ . For example, if permutation has order six, then all the cycles must have length 1, 2, 3, or 6, with either at least one 6-cycle or one cycle each of lengths 2 and 3. So if we want to count the number of permutations of order six in  $S_6$ , the possibilities are

$$\begin{aligned} 8 &= 1 \times 6 + 1 \times 2 \\ &= 1 \times 6 + 2 \times 1 \\ &= 2 \times 3 + 1 \times 2 \\ &= 1 \times 3 + 2 \times 2 + 1 \times 1 \\ &= 1 \times 3 + 1 \times 2 + 3 \times 1 \\ &= 2 \times 3 + 2 \times 1 \end{aligned}$$

- One 6-cycle, one 2-cycle,
- One 6-cycle, two 1-cycles,
- Two 3-cycles, one 2-cycle,
- One 3-cycle, two 2-cycles, and one 1-cycle, or
- One 3-cycle, one 2-cycle, and three 1-cycles.

Step (2) is easy once you figure out step (1). In particular, the number of permutations in  $S_n$  with a given cycle structure is

$$\frac{n!}{\prod_{d=1}^n (c_d)! d^{c_d}}$$

where  $c_d$  denotes the number of cycles of length  $d$ . For example, the number of elements of  $S_{20}$  having four 1-cycles, five 2-cycles, and two 3-cycles is

$$\frac{20!}{(4! \cdot 1^4)(5! \cdot 2^5)(2! \cdot 3^2)} = 1,496,593,128,000.$$

The following table shows the number of elements of each order in  $S_2$  through  $S_8$ .

	1	2	3	4	5	6	7	8	10	12	15
$S_2$	1	1	—	—	—	—	—	—	—	—	—
$S_3$	1	3	2	—	—	—	—	—	—	—	—
$S_4$	1	9	8	6	—	—	—	—	—	—	—
$S_5$	1	25	20	30	24	20	—	—	—	—	—
$S_6$	1	75	80	180	144	240	—	—	—	—	—
$S_7$	1	231	350	840	504	1470	720	—	504	420	—
$S_8$	1	763	1232	5460	1344	10640	5760	5040	4032	3360	2088

This table is entry [A05731](#) at OEIS.

We can use new method.

We need to find how many element have order 2 in  $S_4$

**Step 1:** Divisors of 2 := {1, 2}

Then ways of making 4

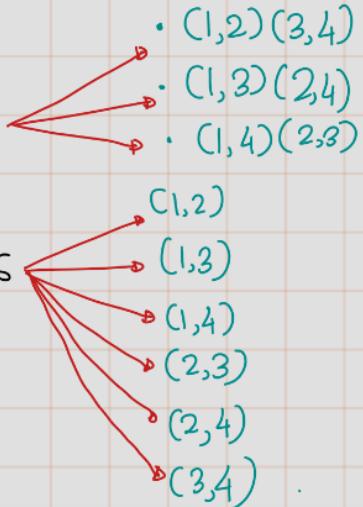
$$4 = 2 \times 2 \rightarrow \text{two 2-cycle}$$

$$4 = 1 \times 2 + 2 \times 1 \rightarrow \text{one 2-cycle \& two 1-cycle.}$$

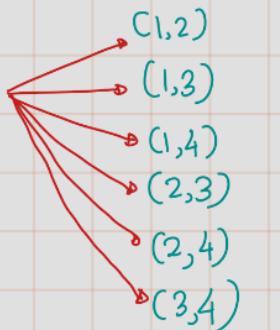
$$\cancel{4} = 4 \times 1 \rightarrow \text{this is not important. 1-cycle mean just 4-cycle.}$$

**Step 2:**

$$n_1 := \frac{4!}{(2! \cdot 1^2)} = 3$$



$$n_2 := \frac{4!}{(1! \cdot 2!) \cdot (2! \cdot 1^2)} = 6$$



**Exercise 4.21** (Artin 2.4.10). Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian?

Let  $A := \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$  and  $B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Note that

$$A^2 = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1+0 & -1+1 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$B^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1+0 & 0+0 \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus,  $|A|=|B|=2$

But,

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$(AB)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

By mathematical induction, we can prove that,

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Thus  $(AB)$  have infinite order

Let  $G$  be an abelian group.

Let  $x, y \in G$  such that  $|x| = n, |y| = m$ , where  $n, m \in \mathbb{Z}^+$   
Suppose that  $n, m$  are relative prime

Then show that order of  $xy$  is  $mn$ .

Let  $r$  be order of  $xy$

Now consider

$$(xy)^{nm} = \underbrace{(xy) \cdot (xy) \cdots (xy)}_{nm \text{ times}} = x^{nm} y^{nm} = (x^n)^m (y^m)^n = 1^m \cdot 1^n = 1.$$

(Since  $G$  is abelian)

Thus,  $r | mn$ . So,  $r \leq mn$  ————— (\*)

$$1 = 1^n = ((ab))^n = a^n b^n = (a^n)$$

Thus,  $m | r^n$ .

Since  $m$  and  $n$  are relative prime.

$$m | r \quad (\text{i})$$

Similarly we can show that  $n | r$  ————— (ii)

By (i) and (ii), since  $m, n$  are relative prime

$$mn | r. \text{ Thus } mn \leq r \quad (**)$$

$$\text{By } (*) \text{ and } (**) \quad r = mn$$

#### 4.2.5 Homomorphisms

**Exercise 4.22** (Artin 2.5.1). Let  $\varphi : G \rightarrow G'$  be a surjective homomorphism. Prove that if  $G$  is cyclic, then  $G'$  is cyclic, and if  $G$  is abelian, then  $G'$  is abelian.

Let  $\varphi: G \rightarrow G'$  is surjective homomorphism.

$\rightarrow$  If  $G$  is cyclic then  $G'$  is cyclic

Let  $G$  be a cyclic group. Let's say  $G = \langle a \rangle$ .

Let  $\varphi: G \rightarrow G'$  be a surjective homomorphism.

Let  $g' \in G'$ . Since  $\varphi$  is surjective,  $g \in G$  such that

$$\varphi(g) = g'$$

Since  $G$  is cyclic,  $g = a^k$  for some  $k \in \mathbb{Z}$

Since  $\varphi$  is homomorphism

$$g' = \varphi(g) = \varphi(a^k) = \varphi(a \cdot a \cdots a) = \varphi(a) \cdots \varphi(a) = [\varphi(a)]^k \in \langle \varphi(a) \rangle$$

Thus  $G' \subseteq \langle \varphi(a) \rangle$

(subgroup of cyclic is cyclic)

Perviously in Artin's exercise 2.4.5,  $G'$  is cyclic group. ■

$\rightarrow$  If  $G$  abliean then  $G'$  is abliean

Let  $g'_1, g'_2 \in G'$ . Since  $\varphi$  is surjective there exists

$g_1, g_2 \in G$  such that  $\varphi(g_1) = g'_1$  and  $\varphi(g_2) = g'_2$

Thus,  $g'_1 g'_2 = \varphi(g_1) \varphi(g_2)$

$$= \varphi(g_1 g_2) \quad (\text{since } \varphi \text{ is homom})$$

$$= \varphi(g_2 g_1) \quad (\text{since } G \text{ is cyclic})$$

$$= \varphi(g_2) \varphi(g_1) \quad (\because \varphi \text{ is homom})$$

$$= g'_2 g'_1$$

Thus  $G'$  is abliean. ■

**Exercise 4.23** (Artin 2.5.2). Prove that the intersection  $K \cap H$  of subgroups of a group  $G$  is a subgroup of  $H$ , and that if  $K$  is a normal subgroup of  $G$ , then  $K \cap H$  is a normal subgroup of  $H$ .

Let  $G$  be a group. Let  $H, K \leq G$ .

claim:  $K \cap H \leq H$ .

- subset: It is trivial  $K \cap H \subseteq H$ .

- closure: Let  $x, y \in K \cap H$ .

Then  $x, y \in K$

Since  $K$  is subgroup of  $G$

$$xy \in K \quad \text{--- (i)}$$

$x, y \in H$

Since  $H$  is subgroup of  $G$

$$xy \in H \quad \text{--- (ii)}$$

By (i) and (ii)  $xy \in K \cap H$ .

Thus closure property holds.

- Inverse: Let  $x \in K \cap H$ .

Then,  $x \in K \Rightarrow x^{-1} \in K$

$x \in H \Rightarrow x^{-1} \in H$

Since  $K, H \leq G$  Thus,  $K \cap H$  is subgroup of  $H$ .

If  $K \leq G$  then  $K \cap H \trianglelefteq H$

Let  $a \in K \cap H$  and  $b \in H$ . Now consider

Note that  $a \in H$  and  $b \in H \Rightarrow bab^{-1} \in H$ . --- (i)

Since,  $(a \in K \text{ and } b \in H)$  and  $K$  is normal

$$bab^{-1} \in K$$

By (i) and (ii)  $bab^{-1} \in K \cap H$ .

Thus,  $K \cap H \trianglelefteq H$ .

**Exercise 4.24** (Artin 2.5.3). Let  $U$  denote the group of invertible upper triangular  $2 \times 2$  matrices  $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ , and let  $\varphi : U \rightarrow \mathbb{R}^\times$  be the map that sends  $A$  to  $a^2$ . Prove that  $\varphi$  is a homomorphism, and determine its kernel and image.

Let  $A_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}$ ,  $A_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \in U$

$$A_1 A_2 = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{bmatrix}$$

$$\varphi(A_1 A_2) = \varphi\left(\begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{bmatrix}\right) = (a_1 a_2)^2$$

$$\varphi(A_1) \varphi(A_2) = \varphi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\right) \cdot \varphi\left(\begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}\right) = a_1^2 a_2^2 = (a_1 a_2)^2$$

Thus,  $\varphi(A_1 A_2) = \varphi(A_1) \varphi(A_2)$

Therefore  $\varphi$  is homomorphism.

$$\ker(\varphi) := \left\{ A \in U \mid \varphi(A) = 1 \right\}$$

$$= \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid \varphi\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\right) = a^2 = 1 \right\}$$

$$= \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a = \pm 1 \right\}$$

$$\begin{aligned}
 \text{Im}(\varphi) &= \varphi(U) := \left\{ \varphi(A) \mid A \in U \right\} \\
 &= \left\{ \varphi \left( \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \right) \mid \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in U \right\} \\
 &= \left\{ a^2 \mid \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in U \text{ and } a, b, d \in \mathbb{R} \right\} \\
 &= \left\{ x \in \mathbb{R} \mid x > 0 \right\} \\
 &= \mathbb{R}^+
 \end{aligned}$$

**Exercise 4.25** (Artin 2.5.4). Let  $f : (\mathbb{R}, +) \rightarrow (\mathbb{C}, \times)$  be the map  $f(x) = e^{ix}$ . Prove that  $f$  is a homomorphism, and determine its kernel and image.

claim:  $f$  is homomorphism

Let  $x, y \in \mathbb{R}, +$ .

$$f(x+y) = e^{i(x+y)} = e^{ix} \cdot e^{iy} = f(x) \cdot f(y)$$

Thus  $f$  is homomorphism.

kernel

$$\ker(\psi) := \{x \in \mathbb{R} \mid f(x) = 1\} = \{x \in \mathbb{R} \mid e^{ix} = 1+0i\}$$

$$= \{x \in \mathbb{R} \mid e^{ix} = \cos x + i \sin x = 1+0i\}$$

$$= \{x \in \mathbb{R} \mid \cos x = 1 \text{ and } \sin x = 0\}$$

$$= \{x \in \mathbb{R} \mid x = 2\pi k, k \in \mathbb{Z}\}$$

$$\cos(x) = 1 \text{ iff } x = 2\pi k, k \in \mathbb{Z}$$

$$\sin(x) = 0 \text{ iff } x = \pi k, k \in \mathbb{Z}$$

Thus,  $\cos(x) = 1 \& \sin(x) = 0 \text{ iff } x = 2\pi k, k \in \mathbb{Z}$

$$\operatorname{Im}(\psi) = \psi(\mathbb{R}) = \{\psi(x) \mid x \in \mathbb{R}\} = \{e^{ix} \mid x \in \mathbb{R}\}$$

$$|e^{ix}| = 1 \text{ iff } |z| = 1$$

Note that has points in  $e^{ix}$  located in the unit circle

$$\operatorname{Im}(\psi) = \{z \in \mathbb{C}^* \mid |z| = 1\}$$

**Exercise 4.26** (Artin 2.5.5). Prove that the  $n \times n$  matrices that have the block form  $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ , with  $A \in GL_r(\mathbb{R})$  and  $D \in GL_{n-r}(\mathbb{R})$ , form a subgroup  $H$  of  $GL_n(\mathbb{R})$ , and that the map  $H \rightarrow GL_r(\mathbb{R})$  that sends  $M \mapsto A$  is a homomorphism. What is its kernel?

**Exercise 4.27** (Artin 2.5.6). Determine the center of  $GL_n(\mathbb{R})$ .

*Hint:* You are asked to determine the invertible matrices  $A$  that commute with every invertible matrix  $B$ . Do not test with a general matrix  $B$ . Test with

elementary matrices.

#### 4.2.6 Isomorphisms

**Exercise 4.28** (Artin 2.6.1). Let  $G'$  be the group of real matrices of the form  $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ . Is the map  $\phi : (\mathbb{R}, +) \rightarrow G'$  that sends  $x$  to this matrix an isomorphism?

$\phi$  is homomorphism:

Let  $a, b \in (\mathbb{R}, +)$

$$(a+b) = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \phi(a) \cdot \phi(b)$$

Thus  $\phi$  is homomorphism.

$\phi$  is injective

Let  $x, y \in (\mathbb{R}, +)$ .

Suppose that  $\phi(x) = \phi(y)$

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$$

$$x = y$$

Thus  $\phi$  is injective.

$\phi$  is surjective

Let  $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in G'$ .

Then.  $f(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in A$ .

Thus  $\phi$  is surjective.

**Exercise 4.29** (Artin 2.6.2). Describe all homomorphisms  $\phi : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ .

Determine which are injective, which are surjective, and which are isomorphisms.

Let  $\psi: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$

**claim:**  $\psi(0) = 0$

$$\begin{aligned}\psi(1) &= \psi(1+0) = \psi(1) + \psi(0) \\ \psi(1) - \psi(1) &= \psi(1) + \psi(0) - \psi(1) \\ 0 &= \psi(0)\end{aligned}$$

**claim:**  $\psi(-1) = -\psi(1)$

$$\begin{aligned}0 &= \psi(0) \\ 0 &= \psi(1 + (-1)) \\ 0 &= \psi(1) + \psi(-1) \\ 0 - \psi(1) &= \psi(0) + \psi(-1) - \psi(1) \\ -\psi(1) &= \psi(-1)\end{aligned}$$

**claim:**  $\psi(n) = n\psi(1)$  for all  $n \in \mathbb{Z}^+$

$$\psi(n) = \psi(\underbrace{1 + \dots + 1}_{n\text{-times}}) = \underbrace{\psi(1) + \dots + \psi(1)}_{n\text{-times}} = n\psi(1)$$

**claim:**  $\psi(-m) = -m\psi(1)$  for all  $m \in \mathbb{Z}^+$

$$\psi(-m) = \psi(\underbrace{(-1) + \dots + (-1)}_{m\text{-times}}) = \underbrace{\psi(-1) + \dots + \psi(-1)}_{m\text{-times}} = m(-\psi(1)) = -m\psi(1)$$

### Injectivity

Claim: If  $\varphi(1) = 0$  then  $\varphi$  is not injective

Let  $\varphi(k) = \underbrace{\varphi(1) + \dots + \varphi(1)}_{k\text{-times}} = 0$  for all  $k \in \mathbb{Z}^+$ .

Thus  $\varphi$  is not injective.

Claim: If  $\varphi(1) \neq 0$ , then  $\varphi$  is injective

Let  $x, y \in \mathbb{Z}$ . Suppose that  $\varphi(x) = \varphi(y)$

$$\varphi(x) = \varphi(y)$$

$$x \varphi(1) = y \varphi(1)$$

$$(x-y) \varphi(1) = 0$$

Since  $\varphi(1) \neq 0$ , then  $x-y=0$ . Thus,  $x=y$ .

Therefore  $\varphi$  is injective.

### Surjectivity:

First observe the image set,

$$\begin{aligned} \text{Im}(\varphi) &:= \left\{ \varphi(x) \mid x \in \mathbb{Z} \right\} = \left\{ x \varphi(1) \mid x \in \mathbb{Z} \right\} \\ &= (\varphi(1))\mathbb{Z} \end{aligned}$$

So,  $\psi$  is surjective if  $\psi(1) = \pm 1$ .

$\psi: \mathbb{Z} \rightarrow \mathbb{Z}$  is isomorphism iff  $\psi(1) = \pm 1$

**Exercise 4.30** (Artin 2.6.3). Show that the functions  $f = \frac{1}{x}$ ,  $g = \frac{x-1}{x}$  generate a group of functions, the law of composition being composition of functions, that is isomorphic to the symmetric group  $S_3$ .

There are 6 elements in the  $S_3$ . Let  $G$  be the group that define in the question. First find the all 6 elements group. Let's do some rough works.

$$f(x) = \frac{1}{x}$$

$$g(x) = \frac{x-1}{x}$$

$$f \circ f(x) = \frac{1}{1/x} = x$$

$$g \circ g(x) = \frac{((x-1)/x) - 1}{(x-1)/x} = \frac{1}{x-1}$$

$$f \circ g(x) = \frac{x}{x-1}$$

$$g \circ f(x) = \frac{(1/x) - 1}{(1/x)} = 1 - x$$

Now let's define

$$f_1 = \frac{1}{x}, \quad f_2 = \frac{x-1}{x}, \quad f_3 = x, \quad f_4 = \frac{1}{x-1}, \quad f_5 = \frac{x}{x-1}, \quad f_6 = 1 - x$$

. Now let's construct multiplication table.

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_2$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$
$f_3$	$f_1$	$f_3$	$f_3$	$f_4$	$f_5$	$f_6$
$f_4$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_5$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_6$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$

This table proves the closure property. According to the table  $f_3$  is the identity. Further,

$$\begin{aligned} (f_1)^{-1} &= f_1 \\ (f_2)^{-1} &= f_4 \\ (f_3)^{-1} &= f_3 \\ (f_4)^{-1} &= f_2 \\ (f_5)^{-1} &= f_5 \\ (f_6)^{-1} &= f_6 \end{aligned}$$

The associativity property holds for the composition of rational functions are associative. To see the isomorphism let's rearrange rows and columns in this table.

$\circ$	$f_3$	$f_5$	$f_6$	$f_1$	$f_4$	$f_2$		$e$	(12)	(13)	(23)	(123)	(132)
$f_3$	$f_3$	$f_5$	$f_6$	$f_1$	$f_4$	$f_2$	$e$	(12)	(13)	(23)	(123)	(132)	
$f_5$	$f_5$	$f_3$	$f_2$	$f_4$	$f_1$	$f_6$	(12)	$e$	(132)	(123)	(23)	(13)	
$f_6$	$f_6$	$f_4$	$f_3$	$f_2$	$f_5$	$f_1$	(13)	(13)	(123)	$e$	(132)	(12)	(23)
$f_1$	$f_1$	$f_2$	$f_4$	$f_3$	$f_6$	$f_5$	(23)	(23)	(132)	(123)	$e$	(13)	(12)
$f_4$	$f_4$	$f_6$	$f_1$	$f_5$	$f_2$	$f_3$	(123)	(123)	(13)	(23)	(12)	(132)	$e$
$f_2$	$f_2$	$f_1$	$f_5$	$f_6$	$f_3$	$f_4$	(132)	(132)	(23)	(12)	(13)	$e$	(123)

By looking at the table we can tell that  $G \cong S_3$ .  $G$  is isomorphic to  $S_3$ .

Let  $\phi : G \rightarrow S_3$  ide defined by  $\phi(f) = (23)$  and  $\phi(g) = (132)$

**Exercise 4.31** (Artin 2.6.4). Prove that in a group, the products  $ab$  and  $ba$  are conjugate elements.

First observe that

$$b(ab)b^{-1} = ba$$

So, we have found  $g \in G$  such that

$$g(ab)g^{-1} = ba$$

Thus,  $ab$  and  $ba$  are conjugate

**Exercise 4.32** (Artin 2.6.5). Decide whether or not the two matrices  $A = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$  and  $B = \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix}$  are conjugate elements of the general linear group  $GL_2(\mathbb{R})$ .

Suppose that  $A$  and  $B$  are conjugate.  
Then there exist  $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$  such that,

$$AX = BX$$

$$\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} 3a & 2b \\ 3c & 2d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -2a+4c & -2b+4d \end{bmatrix}$$

$\begin{array}{l} 3a = a+c \\ 2a = c \end{array}$	$\begin{array}{l} 2b = b+d \\ b = d \end{array}$
$\begin{array}{l} 3c = -2a+4c \\ 2a = c \end{array}$	$\begin{array}{l} 2d = -2b+4d \\ d = b \end{array}$

We write  $X = \begin{pmatrix} a & b \\ 2a & b \end{pmatrix}$

Since  $X \in GL_2(\mathbb{R})$ ,  $\det(X) = ab - 2ab = -ab \neq 0$

So we can get  $a = b = c$ . Then  $X = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$

$$\text{Further: } XAX^{-1} = \left( \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \right) \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 6 & 2 \end{bmatrix} \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix} = B$$

Therefore  $A$  and  $B$  are conjugate elements

Suppose that  $A$  and  $B$  are conjugate.

Then there exist  $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$  such that,

$$AX = BX$$

$$\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} 3a & 2b \\ 3c & 2d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -2a+4c & -2b+4d \end{bmatrix}$$

$$\begin{array}{l|l} 3a = a+c & 2b = b+d \\ 2a = c & b = d \\ \hline 3c = -2a + 4c & 2d = -2b + 4d \\ 2a = c & d = b \end{array}$$

$$\text{We write } X = \begin{pmatrix} a & b \\ 2a & b \end{pmatrix}$$

Since  $X \in GL_2(\mathbb{R})$ ,  $\det(X) = ab - 2ab = -ab \neq 0$

So we can get  $a = b = c$ . Then  $X = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$

$$\begin{aligned} \text{Further, } XAX^{-1} &= \left( \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \right) \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 6 & 2 \end{bmatrix} \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix} = B \end{aligned}$$

Therefore  $A$  and  $B$  are conjugate elements

Suppose that  $A$  and  $B$  are conjugate.  
 Then there exist  $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$  such that,

$$AX = XB$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix} = \begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix}$$

$$\begin{array}{l|l} a+c = a+b & b+d = b \\ c = b & d = 0 \\ \hline c = c+d & d = d \\ d = 0 & \end{array}$$

$$\text{Then, } X = \begin{bmatrix} a & b \\ b & 0 \end{bmatrix}$$

Since  $X \in GL_2(\mathbb{R})$ ,  $\det(X) = -b^2 \neq 0$ .

Let  $X = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ . Now observe that,

$$XBX^{-1} = \left( \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right) \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = A.$$

Therefore,  $A$  and  $B$  are conjugate elements in  $GL_2(\mathbb{R})$

If  $\det(X) = -b^2 = 1 \Rightarrow b^2 = -1 \Rightarrow b = \pm i \notin \mathbb{R}$

So,  $A$  and  $B$  are not conjugate in  $SL_2(\mathbb{R})$

**Exercise 4.33** (Artin 2.6.7). Let  $H$  be a subgroup of  $G$ , and let  $g$  be a fixed element of  $G$ . The conjugate subgroup  $gHg^{-1}$  is defined to be the set of all conjugates  $ghg^{-1}$ , with  $h$  in  $H$ . Prove that  $gHg^{-1}$  is a subgroup of  $G$ .

Let  $G$  be a group and  $H \leq G$ . Fix  $g \in G$ .

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}$$

N.T.S:  $gHg^{-1} \leq G$ .

• subset?: Let  $x \in gHg^{-1}$ . Then  $x = ghg^{-1}$  for some  $h \in H$ .

Since  $g, h \in G$  then  $ghg^{-1} \in G$ . Thus  $gHg^{-1} \subseteq G$

• closure: Let  $x_1, x_2 \in gHg^{-1}$ . Then

$$x_1 = gh_1g^{-1} \text{ for some } h_1 \in H$$

$$x_2 = gh_2g^{-1} \text{ for some } h_2 \in H.$$

$$x_1 x_2 = (gh_1g^{-1})(gh_2g^{-1}) = gh_1(g^{-1}g)h_2g^{-1} = g(h_1 h_2)g^{-1}$$

Since  $H \leq G$ ,  $h_1, h_2 \in H$ . Then  $x_1 x_2 = g(h_1 h_2)g^{-1} \in gHg^{-1}$

• Inverse?: Let  $x \in gHg^{-1}$ . Then  $x = ghg^{-1}$  for some  $h \in H$ .

$$\text{claim: } x^{-1} = gh^{-1}g \in gHg^{-1}$$

$$x x^{-1} = (ghg^{-1})(gh^{-1}g) = gh(g^{-1}g)h^{-1}g = g(hh^{-1})g^{-1} = gg^{-1} = 1$$

$$x^{-1} x = (gh^{-1}g)(ghg^{-1}) = gh^{-1}(g^{-1}g)hg = g(hh^{-1})g^{-1} = gg^{-1} = 1$$

Note that  $gh^{-1}g \in gHg^{-1}$  ( $\because h \in H$  and  $H \leq G$ )

Therefore,  $gHg^{-1} \leq G$ .

**Exercise 4.34** (Artin 2.6.8). Prove that the map  $A \mapsto (A^t)^{-1}$  is an automorphism of  $GL_n(\mathbb{R})$ .

Let  $\phi: GL_n(\mathbb{R}) \rightarrow GL_n(\mathbb{R})$

$$\begin{array}{ccc} A & \longmapsto & (A^\top)^{-1} \end{array}$$

Let  $A, B \in GL_n(\mathbb{R})$ .

$$\phi(AB) = ((AB)^\top)^{-1} = (B^\top A^\top)^{-1} = (A^\top)^{-1} (B^\top)^{-1} = \phi(A) \cdot \phi(B)$$

Thus,  $\phi$  is bijective.

• Injective.

Suppose that  $\phi(A) = \phi(B)$

$$\left. \begin{array}{l} (A^\top)^{-1} = (B^\top)^{-1} \\ A^\top = B^\top \\ A = B. \end{array} \right\} \begin{array}{l} \text{• Surjective} \\ \text{Let } C \in GL_n(\mathbb{R}) \text{ and} \\ D = (C^\top)^\top \\ \phi(D) = (D^\top)^{-1} = ((C^\top)^\top)^{-1} \\ = (C^\top)^{-1} = C \end{array}$$

Thus  $\phi$  is injective

Hence  $\phi$  is bijective. Therefore  $\phi$  is isomorphism

**Exercise 4.35** (Artin 2.6.9). Prove that a group  $G$  and its opposite group  $G^o$  (Exercise 2.2.6) are isomorphic.

Let  $G$  be a group and  $G^\circ$  be the opposite group of  $G$ . Define,

$$\phi: G \longrightarrow G^\circ$$

$$x \longmapsto x'$$

for my simplicity,  $\phi: (G, *) \longrightarrow (G^\circ, \odot)$

Let  $x, y \in G$

$$\phi(x * y) = (x * y)^{-1} = y^{-1} * x^{-1} = x' \odot y' = \phi(x) \odot \phi(y)$$

Thus  $\phi$  is homomorphism.

- **Injective:** Suppose that  $\phi(x) = \phi(y)$

$$x' = y'$$

$$(x')^{-1} = x(y^{-1})y$$

$$y = x.$$

Thus  $\phi$  is injective.

- **Surjectivity**

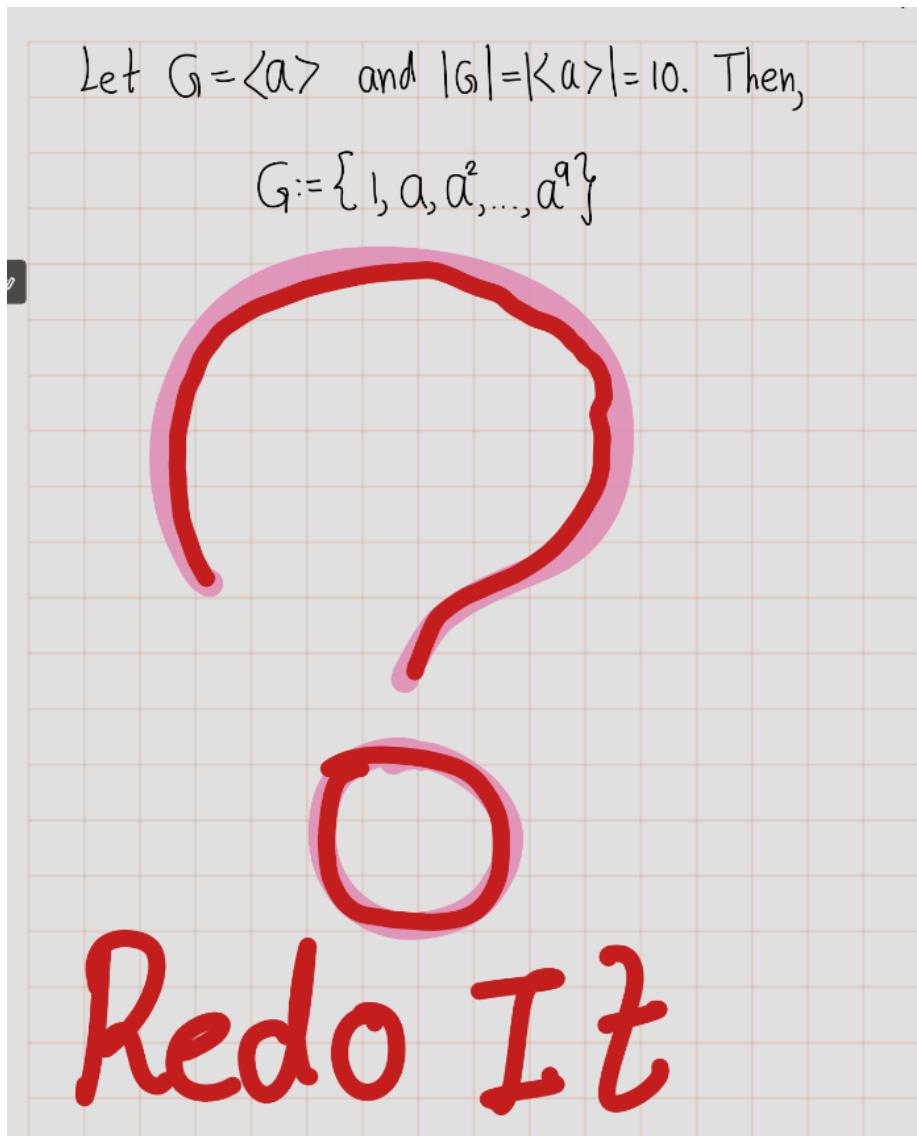
Since  $G$  is a group, then every element of  $G$  is invertible.

So,  $\phi$  is surjective.

Therefore  $\phi$  is isomorphism. Thus,  $G \xrightarrow{\text{iso}} G^\circ$

**Exercise 4.36** (Artin 2.6.10). Find all automorphisms of

- a cyclic group of order 10,
- the symmetric group  $S_3$ .



**Exercise 4.37** (Artin 2.6.11). Let  $a$  be an element of a group  $G$ . Prove that if the set  $\{1, a\}$  is a normal subgroup of  $G$ , then  $a$  is in the center of  $G$ .

Let  $a \in G$   
 Suppose that  $\{1, a\} \trianglelefteq G$ .  
 Since  $\{1, a\}$  is an normal subgroup,  
 $\forall g \in G, gag^{-1} \in \{1, a\}$

$\begin{aligned} &\text{If } gag^{-1} = 1 \\ &ga = g \\ &(g^{-1}g)a = g^{-1}g = 1 \\ &a = 1 \end{aligned}$ <p>But we know that  <math>a \neq 1</math>. This case    cannot happen.</p>	$\left. \begin{aligned} &\text{If } gag^{-1} = a \text{ for all } g \in G. \\ &ga(g^{-1}g) = ag \text{ for all } g \in G \\ &ga = ag \end{aligned} \right\} \text{Thus } a \in Z(G).$
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### 4.2.7 Equivalence Relations and Partitions

**Exercise 4.38** (Artin 2.7.1). Let  $G$  be a group. Prove that the relation  $a \sim b$  if  $b = gag^{-1}$  for some  $g$  in  $G$  is an equivalence relation on  $G$ .

Let  $G$  be a group. Define relation

$a \sim b$  iff  $b = gag^{-1}$  for some  $g \in G$ .

NTS:  $\sim$  is equivalence relation

Let  $a, b, c \in G$ .

• Reflexive: Note that  $a = 1 \cdot a \cdot 1 = 1 \cdot a \cdot (1)^{-1}$ . Since  $1 \in G$ , and  $a$ .

• Symmetric: Suppose that  $a \sim b$  then  $b = gag^{-1}$ .

Then,  $b = g^{-1}ag$

$$gb \in gg^{-1}ag = ag$$

$$gbg^{-1} = agg^{-1} = a$$

Since  $g, g^{-1} \in G$ ,  $b \sim a$ . Thus  $\sim$  is symmetric.

• Transitive: Suppose that  $a \sim b$  and  $b \sim c$ .

Then  $b = gag^{-1}$  for some  $g_1 \in G$  and

$c = g_2bg_2^{-1}$  for some  $g_2 \in G$ .

Then,  $c = g_2(g_1ag_1^{-1})g_2^{-1} = (g_2g_1)a(g_2g_1^{-1})$

Since  $g_2g_1 \in G$ ,  $c \sim a$ .

Thus,  $\sim$  is transitive.

Thus  $\sim$  is equivalence relation.

**Exercise 4.39** (Artin 2.7.2). An equivalence relation on  $S$  is determined by

the subset  $R$  of the set  $S \times S$  consisting of those pairs  $(a, b)$  such that  $a \sim b$ . Write the axioms for an equivalence relation in terms of the subset  $R$ .

Let  $\sim$  be an equivalence relation  $S$  is determined by  
Subset  $R \subseteq S \times S$ .

$a \sim b$  iff  $(a, b) \in R$ .

Axiom	General Notation	In terms of the subset $R$
Reflexive	$a \sim a$	$(a, a) \in R$
Symmetric	$a \sim b \Rightarrow b \sim a$	$(a, b) \in R \Rightarrow (b, a) \in R$
Transitive	$(a \sim b \text{ and } b \sim c) \Rightarrow a \sim c$	$(a, b) \in R \text{ and } (b, c) \in R \Rightarrow (a, c) \in R$

**Exercise 4.40** (Artin 2.7.3). With the notation of Exercise 2.7.2, is the intersection  $R \cap R'$  of two equivalence relations  $R$  and  $R'$  an equivalence relation? Is the union?

Let  $R, R'$  be the two equivalence relations on  $S$   
N.T.S:  $R \cap R'$  is an equivalence relation

Let  $a, b, c \in S$ .

• Reflexive

Since  $R$  and  $R'$  are reflexive

$$\begin{aligned} (a, a) \in R \\ (a, a) \in R' \end{aligned} \Rightarrow (a, a) \in R \cap R'$$

• Symmetric

Suppose  $(a, b) \in R \cap R'$

Since  $R$  and  $R'$  are symmetric,

$$\begin{aligned} (a, b) \in R \Rightarrow (b, a) \in R \\ (a, b) \in R' \Rightarrow (b, a) \in R' \end{aligned} \Rightarrow (b, a) \in R \cap R'$$

• Transitive

Suppose that  $(a, b) \in R \cap R'$  and  $(b, c) \in R'$

Since  $R$  and  $R'$  have transitivity property

$$\begin{aligned} (a, b) \in R \text{ and } (b, c) \in R \Rightarrow (a, c) \in R \\ (a, b) \in R' \text{ and } (b, c) \in R' \Rightarrow (a, c) \in R' \end{aligned} \Rightarrow (a, c) \in R \cap R'$$

Thus  $R \cap R'$  is an equivalence relation

Let's try for union.

• **Reflexive**:  $(a,a) \in R$  or  $(a,a) \in R' \Rightarrow (a,a) \in R \cup R'$

• **Symmetric**: Let  $(a,b) \in R \cup R'$

$$\begin{aligned} &\text{Then } (a,b) \in R \text{ or } (a,b) \in R' \\ &\Rightarrow (b,a) \in R \text{ or } (b,a) \in R' (\because R, R' \text{ are symmetric}) \\ &\Rightarrow (b,a) \in R \cup R' \end{aligned}$$

• **Transitivity?**  $\times$

But the problem rises with Transitivity Property.

Let's see following example.

$$S = \{a, b, c\}$$

$$R := \{(a,b), (b,c), (a,a), (b,b), (c,c)\}$$

$$R' := \{(b,c), (c,b), (a,a), (b,b), (c,c)\}$$

Note that  $R$  and  $R'$  are equivalence Relation.

$$R \cup R' := \{(a,b), (b,c), (c,b), (a,a), (b,b), (c,c)\}$$

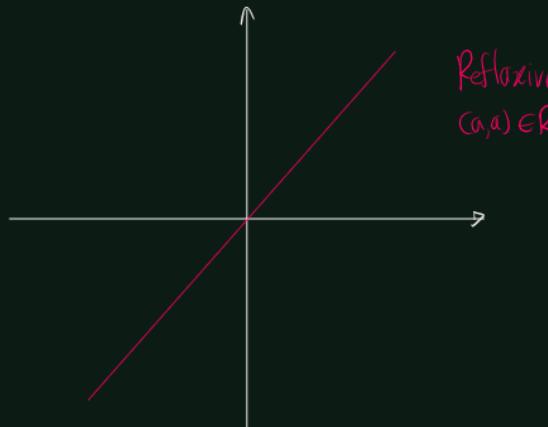
Note that  $(a,b) \in R \cup R'$  and  $(b,c) \in R \cup R'$

But  $(a,c) \notin R \cup R'$ .

Therefore,  $R \cup R'$  is NOT an equivalence relation.

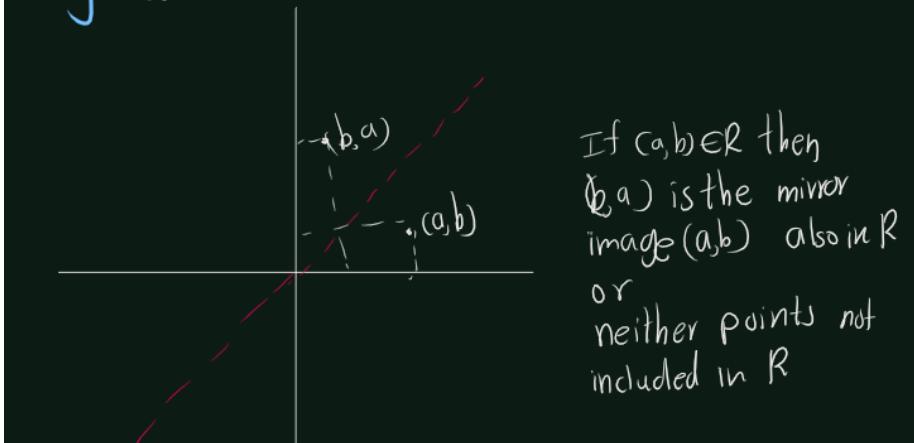
**Exercise 4.41** (Artin 2.7.4). A relation  $R$  on the set of real numbers can be thought of as a subset of the  $(x, y)$ -plane. With the notation of Exercise 7.2, explain the geometric meaning of the reflexive and symmetric properties.

• Reflexive



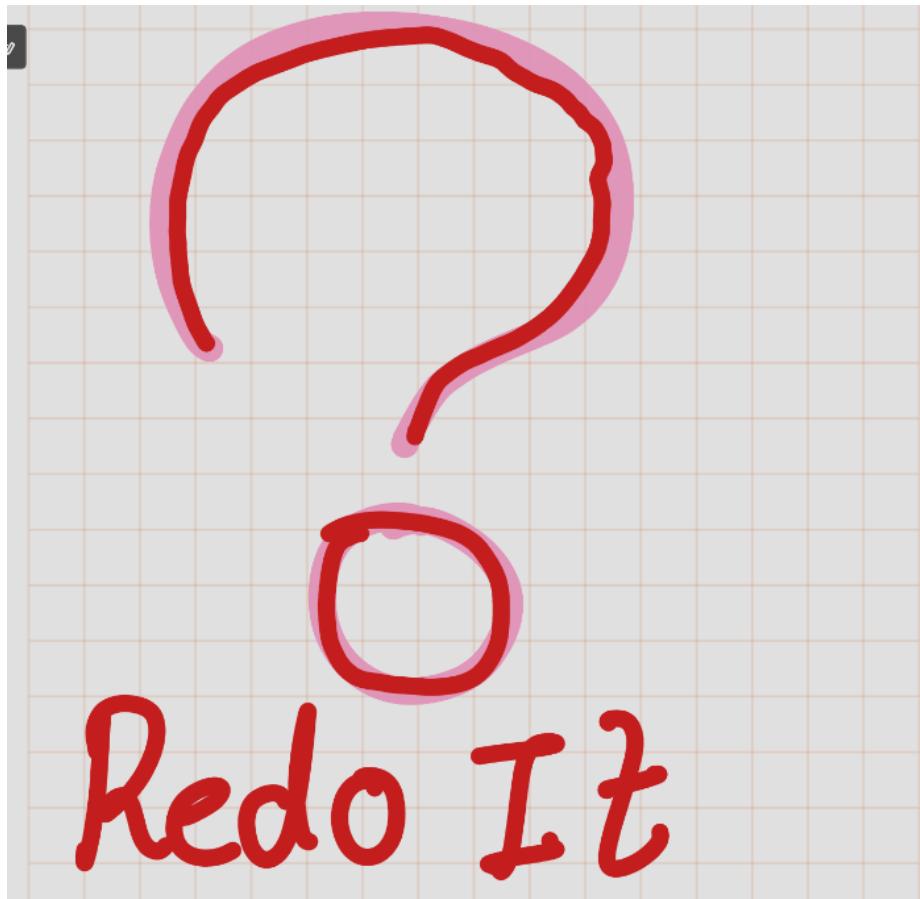
Reflexive means the points on  $y=x$  line.

• Symmetric



**Exercise 4.42** (Artin 2.7.5). With the notation of Exercise 7.2, each of the following subsets  $R$  of the  $(x, y)$ -plane defines a relation on the set  $\mathbb{R}$  of real numbers. Determine which of the axioms (2.7.3) are satisfied:

- (a) the set  $\{(s, s) | s \in \mathbb{R}\}$ ,
- (b) the empty set,
- (c) the locus  $\{xy + 1 = 0\}$ ,
- (d) the locus  $\{x^2y - xy^2 - x + y = 0\}$ .



**Exercise 4.43** (Artin 2.7.5). How many different equivalence relations can be defined on a set of five elements?

The question asks us to find

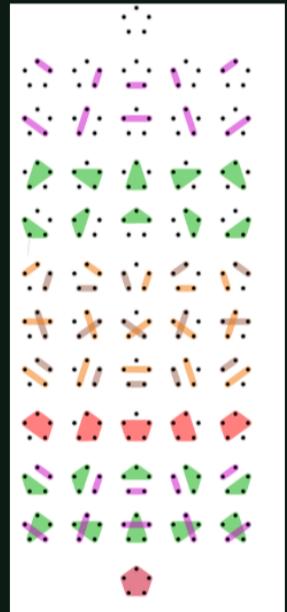
How many ways to define equivalence relations on set S?

So, we can rearrange the question as like this:

"How many ways to can we partition a set of 5?"

Let say set  $S := \{a, b, c, d, e\}$

Ways of partition	no of ways
$\{a\}, \{b\}, \{c\}, \{d\}, \{e\}$	${}_5C_0 = \frac{5!}{0!5!} = 1$
$\{a, b\}, \{c\}, \{d\}, \{e\}$	${}_5C_2 = \frac{5!}{2!3!} = 10$
$\{a, b, c\}, \{d\}, \{e\}$	${}_5C_3 = \frac{5!}{3!2!} = 10$
$\{a, b\}, \{c, d\}, \{e\}$	${}_5C_2 \times {}_2C_2 = \frac{10 \times 1}{2} = 15$
$\{a, b, c, d\}, \{e\}$	${}_5C_4 = \frac{5!}{4!1!} = 5$
$\{a, b, c\}, \{d, e\}$	${}_5C_3 \times {}_2C_2 = \frac{10 \times 1}{3!2!} = 10$
$\{a, b, c, d, e\}$	${}_5C_5 = 1$
Total	$1 + 10 + 10 + 15 + 5 + 10 + 1 = 52$



Now Let's see some details about the Bell Number. It is connected with this problem.

We are asked to find 5th Bell number  $B_5$ , this is 52.

Defn: Bell number

The Bell numbers count the all possible partition on a set.

Formula for find  $B_n$  ( $n$ th Bell number)

This formula is recursive one.

$$B_n = \sum_{k=0}^n {}^n C_k B_k$$

$$B_0 = 1$$

$$B_1 = 1$$

$$B_2 = {}^1 C_0 B_0 + {}^1 C_1 B_1 = 2$$

$$B_3 = {}^2 C_0 B_0 + {}^2 C_1 B_1 + {}^2 C_2 B_2$$

$$= 1 + 2 \times 1 + 1 \times 2$$

$$= 5$$

$$B_4 = {}^3 C_0 B_0 + {}^3 C_1 B_1 + {}^3 C_2 B_2 + {}^3 C_3 B_3$$

$$= 1 + 3 \times 1 + 3 \times 2 + 5$$

$$= 15$$

$$B_5 = {}^4 C_0 B_0 + {}^4 C_1 B_1 + {}^4 C_2 B_2 + {}^4 C_3 B_3 + {}^4 C_4 B_4$$

$$= 1 \times 1 + 4 \times 1 + 6 \times 2 + 4 \times 5 + 1 \times 15$$

$$= 52$$

### 4.2.8 Cosets

**Exercise 4.44** (Artin 2.8.1). Let  $H$  be the cyclic subgroup of the alternating group  $A_4$  generated by the permutation  $(123)$ . Exhibit the left and the right cosets of  $H$  explicitly.

First let's see the elements in the  $A_4$ . There are  $\frac{4!}{2} = \frac{1 \times 2 \times 3 \times 4}{2} = \frac{24}{2} = 12$  elements in the  $A_4$ .

$$A_4 = \{id, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$$

let  $H = \langle (123) \rangle = \{id, (123), (132)\}$  Let's find the left cosets, we apply the elements of  $A_4$  to  $H$ ,

- $id \cdot H = \{id \cdot id, id \cdot (123), id \cdot (132)\} = \{id, (123), (132)\} = H$
- $(12)(34)H = \{(12)(34) \cdot id, (12)(34) \cdot (123), (12)(34) \cdot (132)\} = \{(12)(34), (243), (143)\}$
- $(13)(24)H = \{(13)(24) \cdot id, (13)(24) \cdot (123), (13)(24) \cdot (132)\} = \{(13)(24), (142), (234)\}$
- $(14)(23)H = \{(14)(23) \cdot id, (14)(23) \cdot (123), (14)(23) \cdot (132)\} = \{(14)(23), (134), (124)\}$
- $(123)H = \{(123) \cdot id, (123) \cdot (123), (123) \cdot (132)\} = \{(123), (132), id\} = H$
- $(132)H = \{(132) \cdot id, (132) \cdot (123), (132) \cdot (132)\} = \{(132), id, (123)\} = H$
- $(124)H = \{(124) \cdot id, (124) \cdot (123), (124) \cdot (132)\} = \{(124), (14)(23), (134)\}$
- $(142)H = \{(142) \cdot id, (142) \cdot (123), (142) \cdot (132)\} = \{(142), (234), (13)(24)\}$
- $(134)H = \{(134) \cdot id, (134) \cdot (123), (134) \cdot (132)\} = \{(134), (124), (14)(23)\}$
- $(143)H = \{(143) \cdot id, (143) \cdot (123), (143) \cdot (132)\} = \{(143), (12)(34), (243)\}$
- $(234)H = \{(234) \cdot id, (234) \cdot (123), (234) \cdot (132)\} = \{(234), (13)(24), (142)\}$
- $(243)H = \{(243) \cdot id, (243) \cdot (123), (243) \cdot (132)\} = \{(243), (143), (12)(34)\}$

As a summary,

$$\begin{aligned} id \cdot H &= (123)H = (132)H = \{id, (123), (132)\} = H \\ (12)(34)H &= (243)H = (143)H = \{(12)(34), (243), (143)\} \\ (13)(24)H &= (142)H = (234)H = \{(13)(24), (142), (234)\} \\ (14)(23)H &= (134)H = (124)H = \{(14)(23), (134), (124)\} \end{aligned}$$

Futhur,  $A_4 = H \sqcup (12)(34)H \sqcup (13)(24)H \sqcup (14)(23)H$ . Similarly,

$$\begin{aligned} H \cdot id &= H(123) = H(132) = \{id, (123), (132)\} = H \\ H(12)(34) &= H(134) = H(234) = \{(12)(34), (134), (234)\} \\ H(13)(24) &= H(243) = H(124) = \{(13)(24), (243), (124)\} \\ H(14)(23) &= H(142) = H(143) = \{(14)(23), (142), (143)\} \end{aligned}$$

$A_4 = H \sqcup H(12)(34) \sqcup H(13)(24) \sqcup H(14)(23)$ . Further, note that  $(12)(34)H \neq H(12)(34)$

**Exercise 4.45** (Artin 2.8.2). In the additive group  $\mathbb{R}^m$  of vectors, let  $W$  be the set of solutions of a system of homogeneous linear equations  $AX = 0$ . Show that the set of solutions of an inhomogeneous system  $AX = B$  is either empty, or else it is an (additive) coset of  $W$ .

**Solution:**

Let  $W = \{\underline{x} \in \mathbb{R}^n : A\underline{x} = 0\}$  and  $W' = \{\underline{x} \in \mathbb{R}^n : A\underline{x} = B\} \setminus \text{Need to show:}$   
Either  $W' = \emptyset$  or  $W' = \underline{v}_0 + W$  for some  $\underline{v}_0 \in \mathbb{R}^n \setminus$  Suppose that  $W' \neq \emptyset$ .

Let  $\underline{x}_1 \in W'$ , then  $A\underline{x}_1 = B$ . Now consider following

$$\underline{x}_1 + W = \{\underline{x}_1 + \omega : \omega \in W\}$$

First of all, we are going to show that  $\underline{x}_1 + W \subseteq W'$ . Let  $\underline{x}_1 + \omega_1 \in \underline{x}_1 + W$ . Now consider

$$A(\underline{x}_1 + \omega_1) = A(\underline{x}_1) + A(\omega_1) = B + 0 = B$$

. Thus,  $\underline{x}_1 + \omega_1 \in W'$ . Therefore,  $\underline{x}_1 + W \subseteq W'$ . Now we need to show that reverse inclusion. Let  $\underline{y}_1 \in W'$ . Now let  $\underline{\omega}_2 = \underline{y}_1 - \underline{x}_1$ . Then  $A(\underline{\omega}_2) = A(\underline{y}_1 - \underline{x}_1) = A(\underline{y}_1) - A(\underline{x}_1) = B - B = 0$ . Hence  $\underline{\omega}_2 \in W$ .

$$\underline{x}_1 + \underline{\omega}_2 = \underline{x}_1 + (\underline{y}_1 - \underline{x}_1) = \underline{y}_1 \in \underline{x}_1 + W$$

Hence,  $W' \subseteq \underline{x}_1 + W$ . Therefore,  $W' = \underline{x}_1 + W$ .

**Exercise 4.46** (Artin 2.8.3). Does every group whose order is a power of a prime  $p$  contain an element of order  $p$ ?

**Yes.**

Let's prove following.

**Claim** : Every group whose order is a power of a prime  $p$  contain an element of order  $p$ .

*Proof.* (Prooo of Claim) Let  $G$  be group with  $|G| = p^k < \infty$  for some  $k \in \mathbb{Z}^+$ , where  $p$  is a prime number. Let  $e \neq x \in G$ . Then by Artin's book Corollary 2.8.10,  $Ord(x)|p^k$ . Thus,  $Ord(x) \cdot q = p^k$  forsome  $q \in \mathbb{Z}$ . Since  $p$  is a prime,  $Ord(x) = p^m$  for some  $1 \leq m \leq k$ . Choose  $y := x^{(p^{m-1})}$ . Now we are going to proove that  $Ord(y) = p$ .

$$y^p = (x^{(p^{m-1})})^p = x^{(p^{m-1}) \cdot p^1} = x^{p^m} = 1$$

If  $q \in \mathbb{Z}^+$  such that  $y^q = 1$ , then

$$1 = y^q = (x^{(p^{m-1})})^q = x^{(q \cdot p^{m-1})}$$

Since  $ord(x) = p^m$  then

$$\begin{aligned} q \cdot p^{(m-1)} &\geq p^m \\ q &\geq p \end{aligned}$$

Hence  $Ord(y) = p$ . The group  $G$  whose order is a power of a prime  $p$  contain an element of order  $p$ .  $\square$

**Exercise 4.47** (Artin 2.8.4). Does a group of order 35 contain an element of order 5? of order 7?

**Claim:** Let  $G$  be a group with order 35.  $G$  contains elements of order 5 & 7.

*Proof.* (proof of the claim.) Let  $x \in G$ . By Artin's book Corollary 2.8.10,  $Ord(x)$  should be a divisor of 35. In other words,  $Ord(x) \in \{1, 5, 7, 35\}$ .

- Case-I: Existence of group elements with order 5 We are going to use proof by contradiction method. Assume that there is no any element with order 5.
  - Sub claim: All non-identity elements have order 7. If  $e \neq p \in G$  with  $Ord(p) = 35$  then  $q = p^7$  has order 5 ( $: q^5 = (p^7)^5 = p^{35} = e$ ). This contradicts our hypothesis. Thus, in case-I all non-identity elements have order 7. Let  $h \in G$  with  $Ord(h) = 7$ . Now consider cyclic subgroup generated from  $\langle h \rangle = H$ . Then  $|H| = 7$ . Choose  $e \neq g \notin H$ . Then by above subclaim  $g$  has order 7. Now consider left cosets  $H, gH, g^2H, g^3H, g^4H, g^5H, g^6H$ . Note that those cosets are disjoint. Because if cosets are disjoint then there exist elements such as,  $g^a h^n = g^b h^m$  for some  $1 \leq a, b \leq 6$  and  $1 \leq n, m \leq 6$ . Then

$$\begin{aligned} g^a h^n &= g^b h^m \\ g^{a-b} &= h^{m-n} \end{aligned}$$

So, we can choose  $r \in \mathbb{Z}^+$  such that  $r(a - b) \equiv 1 \pmod{7}$ . Thus,

$$g = g^{r(a-b)} = h^{r(m-n)} \in H$$

This contradicts selection of  $g$ . Thus,  $H, gH, g^2H, g^3H, g^4H, g^5H, g^6H$  left cosets are disjoint. Recall the counting formula

$$\begin{aligned} (\text{order of } G) &= (\text{order of } H) \cdot (\text{number of cosets}) \\ |G| &= |H| \cdot [G : H] \end{aligned}$$

But observe that  $|G| = 35 \neq 49 = 7 \cdot 7 = |H| \cdot [G : H]$ . This contradicts our first hypothesis. Thus  $G$  contains an element of order 5.

- Case-II: Existence of group elements with order 7 This case is also similar to previous one. But I am going to do it. Now assume that there is no any element with order 7. It is very similar to previous case we can prove that all non-identity elements have order 5. Let  $h \in G$  with order 5. We can choose  $g$  very similar to previous case. Further we can consider left cosets  $H, gH, g^2H, g^3H, g^4H$ . So, we can prove that above cosets are disjoint. Then again we use counting formula,  $|G| = 35 \neq 25 = 5 \cdot 5 = |H| \cdot [G : H]$ . This is a contradiction. Thus  $G$  contains an element of order 7.

□

**Exercise 4.48** (Artin 2.8.5). A finite group contains an element  $x$  of order 10 and also an element  $y$  of order 6. What can be said about the order of  $G$ ?

Let  $G$  b group, with  $|G| < \infty$ . Let  $x, y \in G$  with  $|x| = 10$  and  $|y| = 6$ . By Artin's book Corollary 2.8.10 ,  $|x| \mid |G| = 10 \mid |G|$  and  $|y| \mid |G| = 6 \mid |G|$ . Hence,

$$LCM(|x|, |y|) \mid |G| = LCM(10, 6) \mid |G| = 30 \mid |G|$$

**Exercise 4.49** (Artin 2.8.6). Let  $\phi : G \rightarrow G'$  be a group homomorphism. Suppose that  $|G| = 18$ ,  $|G'| = 15$ , and that  $\phi$  is not the trivial homomorphism. What is the order of the kernel?

Then possibilities for  $Img(\phi)$  are as follows. We use Artin's Algbera book Corollary 2.8.13,

$$\begin{array}{lll} |img(\phi)| \mid |G| & \text{and} & |img(\phi)| \mid |G'| \\ |img(\phi)| \mid 18 & \text{and} & |img(\phi)| \mid 15 \\ |img(\phi)| = 1, 2, 3, 6, 9 \text{ or } 18 & \text{and} & |img(\phi)| = 1, 3, 5 \text{ or } 15. \end{array}$$

Thus,  $|img(\phi)| = 1, 3$ . But given that  $\phi$  is not the trivial homomorphism. Hence,  $|img(\phi)| \neq 1$ . Therefore,  $|img(\phi)| = 3$ .

Now let's find the order of the kernel. By Corollary 2.8.13,

$$\begin{aligned} |G| &= |\ker(\phi)| \cdot |im(\phi)| \\ 18 &= |\ker(\phi)| \cdot 3 \\ |\ker(\phi)| &= 6 \end{aligned}$$

**Exercise 4.50** (Artin 2.8.7). A group  $G$  of order 22 contains elements  $x$  and  $y$ , where  $x \neq 1$  and  $y$  is not a power of  $x$ . Prove that the subgroup generated by these elements is the whole group  $G$ .

*Proof.* Let  $G$  of order 22 contains elements  $x$  and  $y$ , where  $x \neq 1$  and  $y$  is not a power of  $x$ . Let  $G' = \langle x, y \rangle$ .

*Need to show:*  $|H| = 22$ .

By Largrage Therom,  $|G'| \mid |G| = |G'| \mid 22$ . So,  $|H| = 1, 2, 11, 22$ . Let's condier each and evrry cases.

- $|H| \neq 1$ . Beacuse  $1 \neq x \in H$ . So,  $H$  can not be happen trivial group.
- $|H| \neq 2$ . If  $|H| = 2$  then  $y = 1$  or  $y = x$ .  
But both cases can not happen. So,  $|H| \neq 2$ . Beacuse that contrduct that  $y$  is not a power of  $x$ .
- $|H| \neq 11$ . Beacuse if  $|H| = 11$  and 11 is prime, then  $H$  is cyclic. (By Corollary 2.8.11) Furthur,  $H = \langle x \rangle$ . Then  $y$  is a power of  $x$ , but it can not happen. So,  $|H| \neq 11$ .
- Therefore,  $|H| = |\langle x, y \rangle| = 22$ .

□

**Exercise 4.51** (Artin 2.8.8). Let  $G$  be a group of order 25. Prove that  $G$  has at least one subgroup of order 5, and that if it contains only one subgroup of order 5, then it is a cyclic group.

**Claim 1:** Let  $G$  be a group of order 25. Then  $G$  has at least one subgroup of order 5.

*Proof.* Let  $G$  be a group of order 25. Let  $1 \neq x \in G$ . By corollary 2.8.10,  $|x|$  divides  $|x| = |G'|$  which divides 25. So,  $|x| = 5, 25$ . Let's consider each and every case.

- If  $|x| = 5$  then  $H = \langle x \rangle$ . Then  $|H| = |\langle x \rangle| = 5$  (By corollary 2.8.11),  $G$  has at least one subgroup of order 5.
- Suppose that  $|x| = 25$ , let  $y = x^5$ .

*Subclaim:*  $|y| = 5$ .

$$y^5 = (x^5)^5 = x^{25} = 1.$$

Let  $m \in \mathbb{Z}$  such that  $y^m = 1$ . Then  $y^m = (x^5)^m = x^{5m}$ . Then  $25 \geq 5m \implies 5 \geq m$ . Thus,  $|y| = 5$ .

Hence  $\langle y \rangle = \langle x^5 \rangle$  is a subgroup of order 5. □

**Claim 2 :** If it contains only one subgroup of order 5, then it is a cyclic group.  
 :: {proof} Suppose that  $G$  contains only one subgroup of order 5. Let's call that subgroup  $G'$ . Let  $y \notin G'$  and  $1 \neq y \in G$ . By corollary 2.8.10,  $|y|$  divides  $|G| = |y|$  which divides 25. So,  $|y| = 5, 25$ .

- If  $|y| = 5$ , then  $|\langle y \rangle| = 5$ . But  $G'$  is the only one subgroup of order 5.  $G' = \langle y \rangle$ . But it contradicts the selection of  $y$ .
  - If  $|y| = 25$ , then  $|\langle y \rangle| = 25$ , so  $\langle y \rangle = G$ . Therefore,  $G = \langle x \rangle$  is cyclic.
- :::

**Exercise 4.52** (Artin 2.8.9). Let  $G$  be a finite group. Under what circumstances is the map  $f : G \rightarrow G$  defined by  $f(x) = x^2$  an automorphism of  $G$ ?

- **Claim 1:** The map  $f : G \rightarrow G$  is a homomorphism if and only if  $G$  is abelian.

*Proof.*  $f$  is a homomorphism if and only if for all  $x, y \in G$ ,  $f(xy) = f(x)f(y)$ . This is equivalent to for all  $x, y \in G$ ,  $(xy)^2 = (xy)(xy) = x^2y^2$ . This is equivalent to for all  $x, y \in G$ ,  $xyxy = xxyy$ . This is equivalent to for all  $x, y \in G$ ,  $xy = yx$ . This is equivalent to  $G$  is abelian.  $\square$

- **Claim 2:**  $f$  is injective if and only if no element in  $G$  has order 2. :::  
 {.proof}  $f$  is injective if and only if  $\ker(f) \neq \{1\}$ . This is equivalent to for all  $x \in G$  with  $1 \neq x$ ,  $f(x) = x^2 \neq 1$ . This is equivalent to no element having order 2. This is equivalent to all elements of  $G$  having odd order (By following sub claim).
  - *Sub Claim 2.1:* Group  $H$  has no element having order 2 is if and only if all elements of  $H$  having odd order.

First let's prove the backward direction. We use proof of contradiction. Assume the contrary. There are some elements of  $H$  having even order. So,  $|x| = 2k$  for some  $k \in \mathbb{Z}^+$ . Then  $|x^k| = 2$  has order 2. :::

**Exercise 4.53** (Artin 2.8.10). Prove that every subgroup of index 2 is a normal subgroup, and show by example that a subgroup of index 3 need not be normal.

*Proof.* Let  $G$  be a group and let  $H \leq G$  with  $[G : H] = 2$ . So,  $H$  has only two left cosets. Then left cosets are  $H$  and  $G \setminus H$  and the cosets partition  $G$ . Let  $x \in G$ .

- If  $x \in H$ , then  $gH = H = Hg$ .
- If  $x \notin H$ , then  $gH = G \setminus H$  and  $Hg = G \setminus H$ . Thus,  $gH = Hg$ .

Therefore,  $G$  is a normal subgroup.  $\square$

**Claim:** A subgroup of index 3 need not be normal.

**Example:** Consider  $S_3 = \{id, (12), (13), (23), (123), (132)\}$  and  $H = \langle (12) \rangle = \{id, (12)\} \leq S_3$ . Let's find the index using the counting formula

$$\begin{aligned}|G| &= |H| \cdot [G : H] \\6 &= 2 \cdot [G : H] \\[G : H] &= 3\end{aligned}$$

Let's take  $g = (13)$  and  $h = (12)$ , then  $ghg^{-1} = (13)(12)(13) = (23)$ . But  $(23) \notin H$ , so  $H$  is not a normal subgroup of  $S_3$ . Therefore, we have proven that  $H$  is not a normal subgroup of  $S_3$ . Thus,  $H$  is not a normal subgroup.

**Exercise 4.54** (Artin 2.8.11). Let  $G$  and  $H$  be the following subgroups of  $GL_2(\mathbb{R})$ :

$$G = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \right\}, H = \left\{ \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

with  $x$  and  $y$  real and  $x > 0$ . An element of  $G$  can be represented by a point in the right half plane. Make sketches showing the partitions of the half plane into left cosets and into right cosets of  $H$ .

**Exercise 4.55** (Artin 2.8.12). Let  $S$  be a subset of a group  $G$  that contains the identity element 1, and such that the left cosets  $aS$ , with  $a$  in  $G$ , partition  $G$ . Prove that  $S$  is a subgroup of  $G$ .

*Proof.* Let  $1 \in S \subseteq G$ , and such that  $\Pi = \{aS : a \in G\}$ , is a partition of  $G$ . -Subset : This is trivial.(Given in the problem in already.) - Identity :  $1 \in S$ . - Closure and Inversion : Let  $x, y \in S$ . Since  $\Pi$  is part of  $G$ , there exists  $g \in G$  such that  $xy^{-1} \in gS$ . So,  $xy^{-1} = gr$  for some  $r \in S$ . Then  $x = gry \in grS$  (since  $y \in S$ ). Thus,  $x \in S \cap grS$ . This implies  $S \cap grS \neq \emptyset$ . But  $\Pi$  is a partition of  $G$ . Thus,  $S = grS$ . Now observe that  $gr \in gS$  (since  $r \in S$ ) and  $gr \in grS$ . Hence  $gr \in gS \cap grS$ . Thus,  $gS = grS$ . Hence,  $xy^{-1} = S = gS = grS$ .

By the subgroup test,  $S$  is a subgroup of  $G$ .  $\square$

**Exercise 4.56** (Artin 2.8.13). Let  $S$  be a set with a law of composition: A partition  $\Pi_1 \cup \Pi_2 \cup \dots$  of  $S$  is compatible with the law of composition if for all  $i$  and  $j$ , the product

$$\Pi_i \Pi_j = \{xy : x \in \Pi_i, y \in \Pi_j\}$$

set is contained in a single subset  $\Pi_k$  of the partition.

- a) The set  $Z$  of integers can be partitioned into the three sets  $[\text{Pos}]$ ,  $[\text{Neg}]$ ,  $[\{0\}]$ . Discuss the extent to which the laws of composition  $+$  and  $\times$  are compatible with this partition.
- b) Describe all partitions of the integers that are compatible with the operation  $+$

### 4.2.9 Modular Arithmetic

**Exercise 4.57** (Artin 2.9.2). What are the possible values of  $a^2$  modulo 4? modulo 8?

**solution:**

- *In modulo 4*

$$\begin{aligned}\bar{0}^2 &\equiv 0 \pmod{4} \\ \bar{1}^2 &\equiv 1 \pmod{4} \\ \bar{2}^2 &\equiv 0 \pmod{4} \\ \bar{3}^2 &\equiv 1 \pmod{4}\end{aligned}$$

The possible values of  $a^2 \pmod{4}$  are 0 and 1.

- *In modulo 8*

$$\begin{aligned}\bar{0}^2 &\equiv 0 \pmod{8} \\ \bar{1}^2 &\equiv 1 \pmod{8} \\ \bar{2}^2 &\equiv 4 \pmod{8} \\ \bar{3}^2 &\equiv 1 \pmod{8} \\ \bar{4}^2 &\equiv 0 \pmod{8} \\ \bar{5}^2 &\equiv 1 \pmod{8} \\ \bar{6}^2 &\equiv 4 \pmod{8} \\ \bar{7}^2 &\equiv 1 \pmod{8}\end{aligned}$$

The possible values of  $a^2 \pmod{8}$  are 0,1 and 4.

**Exercise 4.58** (Artin 2.9.3). Prove that every integer  $a$  is congruent to the sum of its decimal digits modulo 9.

*Proof.* Let  $x \in \mathbb{Z}$ . Now we can represent  $x$  as follows

$$x = a_0 10^0 + a_1 10^1 + \cdots + a_n 10^n = \sum_{i=0}^n a_i 10^i \text{ forsome } n \in \mathbb{Z}, \text{ and } a_i \in \{0, 1, \dots, 9\}$$

We need to show  $x \equiv \sum_{i=0}^n a_i \pmod{9}$ . So, now consider,

$$x - \sum_{i=0}^n a_i = \sum_{i=0}^n a_i 10^i - \sum_{i=0}^n a_i \quad (4.19)$$

$$= \sum_{i=0}^n (a_i 10^i - a_i) \quad (4.20)$$

$$= \sum_{i=0}^n a_i (10^i - 1) \quad (4.21)$$

By following claim we can get that,

$$x - \sum_{i=0}^n a_i \equiv 0 \pmod{9} \quad (4.22)$$

$$x \equiv \sum_{i=0}^n a_i \pmod{9} \quad (4.23)$$

□

**Claim:**  $9|(10^k - 1)$  for any  $k \in \mathbb{N}$ .

*Proof.* We use mathematical induction.

$k = 1$

This case is trivial. Because  $9|10 - 1$ .

$k = n \in \mathbb{Z}$

Now assume when  $n = k, 9|(10^n - 1)$ .

$k = n + 1$

$$10^{n+1} - 1 = 10 \cdot 10^n - 1 = 9 \cdot 10^n + (10^n - 1)$$

Thus  $9|(10^{n+1} - 1)$ .

Therefore, by mathematical induction,  $9|(10^n - 1)$  for any  $n \in \mathbb{N}$ . □

**Exercise 4.59** (Artin 2.9.4). Solve the congruence  $2x \equiv 5 \pmod{9}$  and modulo 6.

$$2x \equiv 5 \pmod{9}$$

Note that  $2 \times 5 = 10 \equiv 1 \pmod{9}$

$$5 \times 2x \equiv 5 \times 5 \pmod{9}$$

$$x \equiv 25 \pmod{9}$$

$$x \equiv 7 \pmod{9}$$

$$2x \equiv 5 \pmod{6}$$

Note that  $\gcd(6, 2) = 2 \neq 1$

Thus There exist no solutions for  $x$  in  $\pmod{6}$ .

**Exercise 4.60** (Artin 2.9.5). Determine the integers  $n$  for which the pair of congruences  $2x - y \equiv 1$  and  $4x + 3y \equiv 2$  modulo  $n$  has a solution.

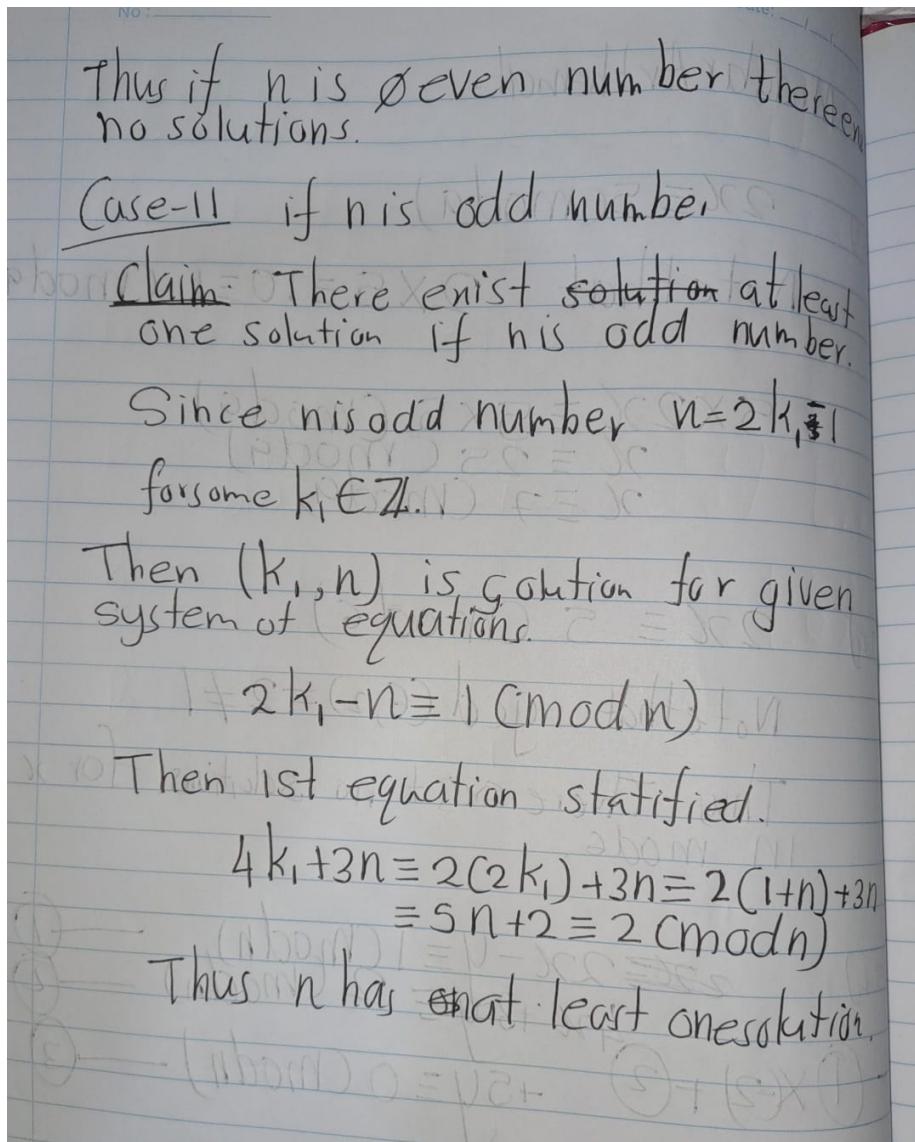
$$\begin{aligned} & \cancel{2x - y \equiv 1 \pmod{n}} \quad \text{--- (1)} \\ & 4x + 3y \equiv 2 \pmod{n} \quad \text{--- (2)} \\ \Rightarrow & (1) \times (-2) + (2) \quad +5y \equiv 0 \pmod{n} \quad \text{--- (3)} \end{aligned}$$

If  $n$  is an even number

Assume that (1), (2) eqn have solutions

(1) eqn gives  $y$  is odd  $\rightarrow$  This contradic

(3) eqn gives  $y$  is even  $\rightarrow$



**Exercise 4.61** (Artin 2.9.6). Prove the Chinese Remainder Theorem: Let  $a, b, u, v$  be integers, and assume that the greatest common divisor of  $a$  and  $b$  is 1. Then there is an integer  $x$  such that  $x \equiv u$  modulo  $a$  and  $X \equiv v$  modulo  $b$ .

Hint: Do the case  $u = 0$  and  $v = 1$  first.

**Exercise 4.62** (Artin 2.9.7). Determine the order of each of the matrices  $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$  when the matrix entries are interpreted modulo 3.

$$A := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, A^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$A^3 = A^2 \cdot A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

In modulo 3,  $A$  has order 3.

$$B := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$B^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

$$B^3 = B^2 \cdot B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}$$

$$B^4 = B^3 \cdot B = \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2I$$

$$B^5 = B^4 \cdot B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}$$

$$B^6 = B^5 \cdot B = \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}$$

$$B^7 = B^6 \cdot B = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$$

$$B^8 = B^7 \cdot B = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

In modulo 3, order of  $B$  is 8 ( $|B|=8$ )

#### 4.2.10 The Correspondence Theorem

**Exercise 4.63** (Artin 2.10.1). Describe how to tell from the cycle decomposition whether a permutation is odd or even.

**Exercise 4.64** (Artin 2.10.2). Let  $H$  and  $K$  be subgroups of a group  $G$ .

a) Prove that the intersection  $xH \cap yK$  of two cosets of  $H$  and  $K$  is either empty or else is a coset of the subgroup  $H \cap K$ . b) Prove that if  $H$  and  $K$  have finite index in  $G$  then  $H \cap K$  also has finite index in  $G$ .

**Exercise 4.65** (Artin 2.10.3). Let  $G$  and  $G'$  be cyclic groups of orders 12 and 6, generated by elements  $x$  and  $y$ , respectively, and let  $\phi : G \rightarrow G'$  be the map defined by  $\phi(x^i) = y^i$ . Exhibit the correspondence referred to in the Correspondence Theorem explicitly.

**Exercise 4.66** (Artin 2.10.4). With the notation of the Correspondence Theorem, let  $H$  and  $H'$  be corresponding subgroups. Prove that

$$[G : H] = [G' : H']$$

**Exercise 4.67** (Artin 2.10.5). With reference to the homomorphism  $S_4 \rightarrow S_3$  described in Example 2.5.13, determine the six subgroups of  $S_4$  that contain  $K$ .

#### 4.2.11 Product Group

**Exercise 4.68.** Let  $x$  be an element of order  $r$  of a group  $G$ , and let  $y$  be an element of  $G'$  of order  $s$ . What is the order of  $(x, y)$  in the product group  $G \times G'$ ?

**Solution:** The order of  $(x, y)$  in the product group  $G \times G'$  is  $\text{lcm}(r, s)$ . Let  $n \in \mathbb{Z}^+$  such that

$$(x, y)^n = (x^n, y^n) = (1_G, 1_{G'}).$$

This implies,  $x^n = 1_G$  and  $y^n = 1_{G'}$ . Since order of  $x$  and  $y$  are  $r$  and  $s$  respectively,

$$r|n \quad \text{and} \quad s|n$$

So, we know that the least positive integer such that above property holds is  $\text{lcm}(r, s)$ . Hence, the order of  $(x, y)$  in the product group  $G \times G'$  is  $\text{lcm}(r, s)$ .

**Exercise 4.69.** What does Proposition 2.8 tell us when, with the usual notation for the symmetric group  $S_3$ ,  $K$  and  $H$  are the subgroups  $\langle y \rangle$  and  $\langle x \rangle$ ?

Recall:  $y^2 = 1$  and  $x^3 = 1$ . Then

$$H = \langle x \rangle = \{1, x, x^2\} \quad \text{and} \quad K = \langle y \rangle = \{1, y\}$$

Let the multiplication map,  $f : H \times K \rightarrow S_3$  defined by  $f(h, k) = hk$ . Then,  $Im(f) = HK = \{hk : h \in \langle x \rangle, k \in \langle y \rangle\} = \{1, x, x^2, y, xy, x^2y\}$ .

**Claim 1:**  $f$  is injective.

Observe that  $H \cap K = \{1\}$ . by 2.8 a)  $f$  is injective.

**Claim 2:**  $f$  is surjective.

Observe that  $S_3 = HK = \{1, x, x^2, y, xy, x^2y\}$ . Thus,  $f$  is surjective.

**Claim 3 :**  $f$  is not homomorphism.

$$f((x, y) \cdot (x, 1)) = f(x^2, y^2) = f(x^2, 1) = x^2 \cdot 1 = x^2 \quad (4.24)$$

$$f(x, y) \cdot f(x, 1) = (x \cdot y) \cdot (x \cdot 1) = (xy) \cdot x = y \quad (4.25)$$

Thus,  $f$  is not a homomorphism.

**Exercise 4.70.** Prove that the product of two infinite cyclic groups is not infinite cyclic.

*Proof.*

- **Claim 1 :** Infinite cyclic groups are isomorphic to  $\mathbb{Z}$ .

Let  $G$  be a infinite cyclic group and  $\langle a \rangle = G$ . We can define a function  $f : \mathbb{Z} \rightarrow G$  by  $f(n) = a^n$  for all integers  $n$ . We need to show that  $f$  is an isomorphism, which means it is bijective.

- **Subclaim 1.1 :**  $f$  is a hormomorphism.

$$f(n + m) = a^{n+m} = a^n \cdot a^m = f(n) \cdot f(m)$$

Thus,  $f$  is a hormomorphism.

- **Subclaim 1.2 :**  $f$  is a injective

Suppose that  $f(n) = f(m)$

$$f(n) = f(m) \quad (4.26)$$

$$a^n = a^m \quad (4.27)$$

$$n = m \quad (\text{Since order is infinite}) \quad (4.28)$$

- **Subclaim 1.3 :**  $f$  is surjective.

Let  $x \in G = \langle a \rangle$ . Then,  $x = a^k$  for some  $k \in \mathbb{Z}$ . Then, observe that

$$f(k) = a^k = a$$

. Thus,  $f$  is surjective.

Therefore,  $f$  is an isomorphism. Thus, the infinite cyclic groups are isomorphic to  $\mathbb{Z}$ .

We can consider  $\mathbb{Z} \times \mathbb{Z}$ . Suppose that  $(a, b)$  generate the product group. But then, we see that  $(2a, b)$  cannot be obtained from adding  $(a, b)$  to itself, which implies that  $\mathbb{Z} \times \mathbb{Z}$  is not infinite cyclic.

□

**Exercise 4.71.** In each of the following cases, determine whether or not  $G$  is isomorphic to the product group  $H \times K$ .

- (a)  $G = \mathbb{R}^\times$ ,  $H = \{\pm 1\}$ ,  $K = \{\text{positive real numbers}\}$ .
- (b)  $G = \{\text{invertible upper triangular } 2 \times 2 \text{ matrices}\}$ ,  $H = \{\text{invertible diagonal matrices}\}$ ,  $K = \{\text{upper triangular matrices with diagonal entries 1}\}$ .
- (c)  $G = e^x$ ,  $H = \{\text{unit circle}\}$ ,  $K = \{\text{positive real numbers}\}$ .

**Solution:**

- (a) Observe that  $G = \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$  is abelian. Then  $H, K \trianglelefteq G$ . Further, observe that  $H \cap K = \{1\}$  and  $HK = \mathbb{R}^\times = G$ . Thus, by proposition 2.8  $G \cong H \times K$ .

(b)

- **Claim b.1:**  $K \trianglelefteq G$ .

Let  $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  be an arbitrary matrix in  $G$  and  $k = \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \in K$ . Then,

$$g^{-1} = \begin{bmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{bmatrix}$$

Then

$$\begin{aligned} gkg^{-1} &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a^{-1} & dc^{-1} - ba^{-1}c^{-1} \\ 0 & c^{-1} \end{bmatrix} = \begin{bmatrix} 1 & adc^{-1} \\ 0 & 1 \end{bmatrix} \in K \end{aligned}$$

Thus,  $H \trianglelefteq G$ .

- **Claim b.2 :**  $H = Z(G)$  ( $H$  is in the center of  $G$ ).

– *subclaim b.2.1 :  $H \subseteq Z(G)$ .*

Let  $h = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \in H$ . Then,

$$B = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} = x \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = BI$$

Then observe that, for any  $A \in G$ ,

$$BA = (xI)A = xA = Ax = A(xI) = AB$$

– *subclaim b.2.2 :  $H \supseteq Z(G)$ .*

Let  $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in Z(G)$ , then,

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \quad (4.29)$$

$$\begin{bmatrix} p & -q \\ r & -s \end{bmatrix} = \begin{bmatrix} p & q \\ -r & -s \end{bmatrix} \quad (4.30)$$

(4.31)

This yields  $-q = q$  and  $r = -r$  which imply  $q = r = 0$ . Now considering,

$$\begin{bmatrix} p & 0 \\ 0 & s \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} p & 0 \\ 0 & s \end{bmatrix} \quad (4.32)$$

$$\begin{bmatrix} 0 & p \\ q & 0 \end{bmatrix} = \begin{bmatrix} 0 & q \\ p & 0 \end{bmatrix} \quad (4.33)$$

(4.34)

This implies that  $a = d$  and since the matrix is invertible,  $a \neq 0$ . Thus,  $H \subseteq Z(G)$ .

Therefore,  $H = Z(G)$ . In other words,  $H$  is in the center of  $G$ .

- **Claim b.2 :**  $H \trianglelefteq G$ .

Since,  $H$  is in the center of  $G$ , then  $H$  is normal.

- **Claim b.3 :**  $H \cap K = \{I\}$ .

This is trivial.

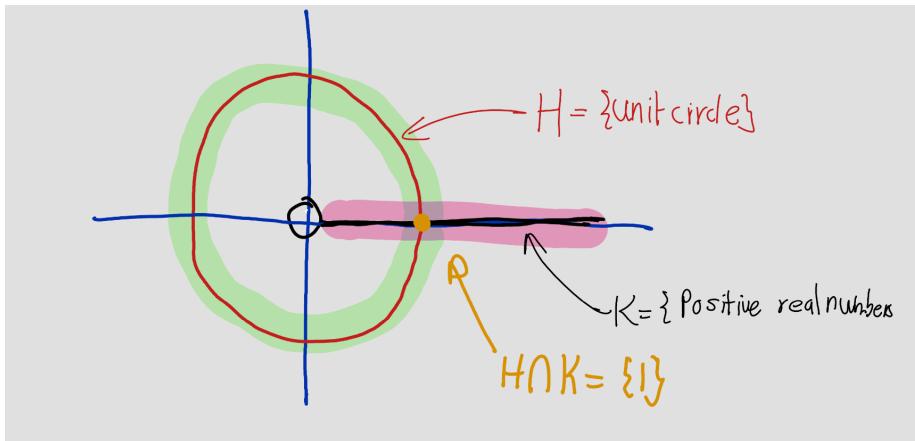
- **Claim b.4 :**  $HK = G$  Clearly,  $HK \subseteq G$ . Conversely, for any  $g \in G$ ,  $a \neq 0, b \neq 0$ ,

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a^{-1}b \\ 0 & 1 \end{bmatrix} \in HK$$

. Thus,  $HK = G$ .

Therefore, by proposition 2.8  $G \cong HK$

(c) Since  $C^\times$  is abelian, then  $H$  and  $K$  are normal. And,  $H \cap K = \{1\}$ .



Consider  $a + bi \in C^\times$ . Then

$$a + bi = \left( \frac{a}{\sqrt{a^2 + b^2}} + \frac{b}{\sqrt{a^2 + b^2}} i \right) \sqrt{a^2 + b^2} \in HK$$

So,  $HK = G$ . So, by proposition 2.8  $G \cong H \times K$ .

**Exercise 4.72.** Let  $G_1$  and  $G_2$  be groups, and let  $Z_i$  be the center of  $G_i$ . Prove that the center of the product group  $G_1 \times G_2$  is  $Z_1 \times Z_2$ .

Let  $Z_1 = Z(G_1) = \{x \in G_1 \mid xg = gx \ \forall g \in G_1\}$   
 and  $Z_2 = Z(G_2) = \{x \in G_2 \mid xg = gx \ \forall g \in G_2\}$

Need to show:  $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$

claim 1:  $Z(G_1) \times Z(G_2) \subseteq Z(G_1 \times G_2)$

Let  $(g_1, g_2) \in G_1 \times G_2$  and  $(z_1, z_2) \in Z(G_1) \times Z(G_2)$

$(z_1, z_2) \in Z(G_1) \times Z(G_2)$

$$(g_1, g_2) \cdot (z_1, z_2) = (g_1 z_1, g_2 z_2) \neq \cancel{(z_1, z_2)}$$

$$= (z_1 g_1, z_2 g_2) \quad (\text{Since } z_1 \in Z(G_1) \text{ and } z_2 \in Z(G_2))$$

$$= (z_1, z_2)(g_1, g_2).$$

Thus,  $Z(G_1) \times Z(G_2) \subseteq Z(G_1 \times G_2)$

claim 2:  $Z(G_1 \times G_2) \subseteq Z(G_1) \times Z(G_2)$

Let  $(x_1, x_2) \in Z(G_1 \times G_2)$

Then for all  $(a_1, a_2) \in G_1 \times G_2$

$$(a_1, a_2) \cdot (x_1, x_2) = (x_1, x_2) \cdot (a_1, a_2)$$

$$(a_1 x_1, a_2 x_2) = (x_1 a_1, x_2 a_2)$$

Thus,  $a_1 x_1 = x_1 a_1 \quad \forall a_1 \in G_1$  and  
 $a_2 x_2 = x_2 a_2 \quad \forall a_2 \in G_2$

Hence  $x_1 \in Z(G_1)$  and  $x_2 \in Z(G_2)$

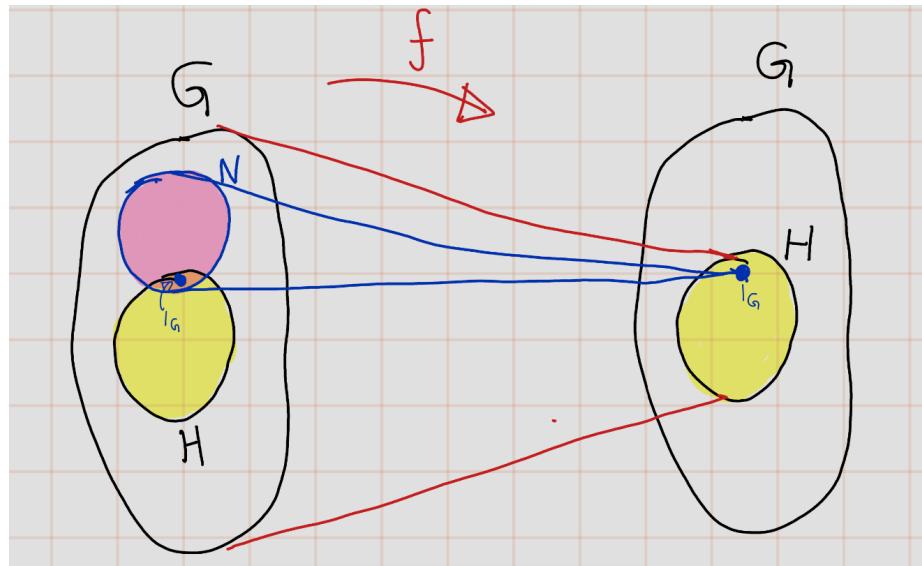
Therefore,  $(x_1, x_2) \in Z(G_1) \times Z(G_2)$

Thus,  $Z(G_1 \times G_2) \subseteq Z(G_1) \times Z(G_2)$

By claim 1 and 2,  $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$

**Exercise 4.73.** Let  $G$  be a group that contains normal subgroups of orders 3 and 5, respectively. Prove that  $G$  contains an element of order 15.

**Exercise 4.74.** Let  $H$  be a subgroup of a group  $G$ , let  $\phi : G \rightarrow H$  be a homomorphism whose restriction to  $H$  is the identity map, and let  $N$  be its kernel. What can one say about the product map  $H \times N \rightarrow G$ ?



Claim:  $f$  is injective.

Clearly  $l_G \in H \cap N$ .

Assume that  $l_G \neq x \in H \cap N$

$$x \in H \Rightarrow f(x) = x \neq l_G \quad \text{--- (1)}$$

$$x \in N \Rightarrow f(x) = l_G \quad \text{--- (2)}$$

(1) and (2) give contradiction,

Thus,  $H \cap N = \{l_G\}$

By proposition 2.4 (mg (Artins book) 2.11.4)

(a),  $f$  is injective.

Claim:  $f$  is surjective

This is trivial,  $\forall h \in H, h = f(h)$

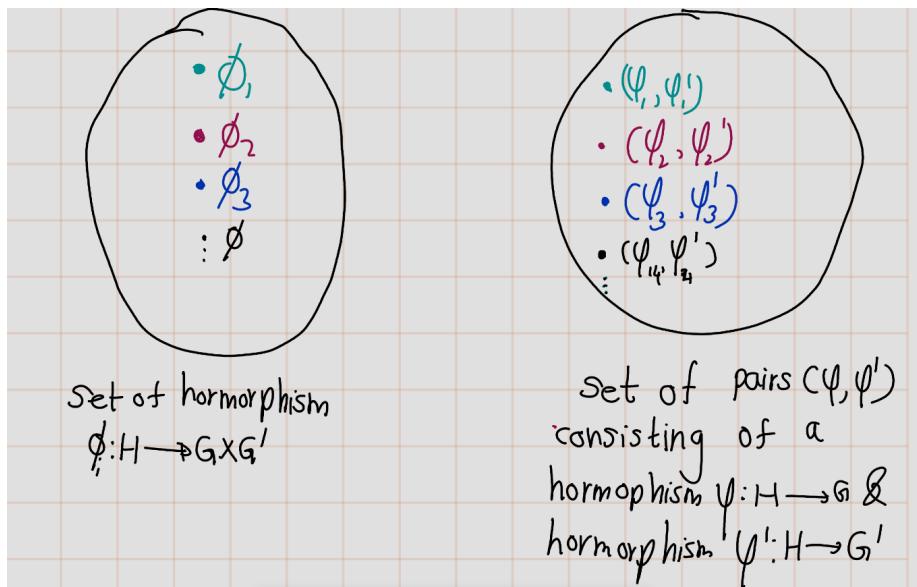
claim: If  $G$  is abelian then  $f$  is homomorphism

Suppose  $G$  is abelian then  $hn = nh$

$\forall h \in H \trianglelefteq G$  and  $\forall n \in N \trianglelefteq G$

Thus,  $\text{#}$  by artins book proposition 2.11.4  
part b)  $f$  is a homomorphism

**Exercise 4.75.** Let  $G$ ,  $G'$ , and  $H$  be groups. Establish a bijective correspondence between homomorphisms  $\phi : H \rightarrow G \times G'$  from  $H$  to the product group and pairs  $(\varphi, \varphi')$  consisting of a homomorphism  $\varphi : H \rightarrow G$  and a homomorphism  $\varphi' : H \rightarrow G'$ .



We have to define a map.

$$f: \left\{ \begin{array}{l} \text{homomorphisms} \\ \text{from } H \text{ to } G \times G' \end{array} \right\} \xrightarrow{\quad} \left\{ \begin{array}{l} \text{pairs of} \\ \text{homomorphisms} \\ (\psi, \psi') \end{array} \right\}$$

$$\underline{\Phi} \longmapsto (\pi \circ \underline{\Phi}, \pi' \circ \underline{\Phi})$$

where  $\pi, \pi'$  are projection maps,

$$\pi: G \times G' \longrightarrow G$$

$$(g, g') \longmapsto g$$

$$\text{and } \pi': G \times G' \longrightarrow G'$$

$$(g, g') \longmapsto g'$$

Now I am going to prove

1.  $f$  is well-defined

2.  $f$  is injective

3.  $f$  is surjective.

~~First let's check c1~~

First of all Let's denote

$$A := \left\{ \underline{\Phi}: H \rightarrow G \times G' \mid \underline{\Phi} \text{ is homomorphisms} \right\}$$

Let  $B := \{(\varphi, \psi) \mid \varphi: H \rightarrow G, \psi: H \rightarrow G' \text{ and } \varphi \text{ and } \psi \text{ are homomorphisms}\}$

Now let's start to check three conditions.

1  $\boxed{f(\phi) \in B \quad \forall \phi: H \rightarrow G \times G' \text{ be homomorph}}$

Let  $\phi: H \rightarrow G \times G'$  be a homomorphism

subclaim 1.1:  $\pi$  is homomorphism

Let  $(g_1, g'_1), (g_2, g'_2) \in G \times G'$

$$\begin{aligned} \pi((g_1, g'_1)(g_2, g'_2)) &= \pi(g_1 g_2, g'_1 g'_2) \\ &= (g_1 g_2) = \pi(g_1, g'_1) \pi(g_2, g'_2) \end{aligned}$$

Thus  $\pi$  is homomorphism  
Now we are done the subclaim

claim:  $\pi \circ \phi$  is homomorphism

Let  $h, h' \in H$

$$\begin{aligned} [\pi \circ \phi](hh') &= \pi(\phi(hh')) = \pi(\phi(h)\phi(h')) \\ &= \pi(\phi(h))\pi(\phi(h')) \\ &= \pi \circ \phi(h) \cdot \pi \circ \phi(h') \end{aligned}$$

Thus  $(\pi \circ \phi)$  is a homomorphism

Therefore  $f$  is well-defined ■

Claim:  $f$  is injective

Let  $\phi_1, \phi_2 \in A$  such that

$$\cancel{f(\phi_1)} = f(\phi_2)$$

$$(\pi \circ \phi_1, \pi' \circ \phi_1) = (\pi \circ \phi_2, \pi' \circ \phi_2)$$

Thus, for all  $h \in H$ ,

$$\pi \circ \phi_1(h) = \pi \circ \phi_2(h) \text{ and} \quad ①$$

$$\pi' \circ \phi_1(h) = \pi' \circ \phi_2(h) \quad ②$$

Let  $p$  be an arbitrary element in  $H$ ,

Then,

$$\cancel{\phi_1(p)} = \phi_1(p) = (g_1, g'_1) \text{ for some } g_1, g'_1 \in G'$$

$$\phi_2(p) = (g_2, g'_2) \text{ for some } g_2 \in G, g'_2 \in G'$$

By equation ①

$$\pi \circ \phi_1(p) = \pi \circ \phi_2(p)$$

$$\pi(g_1, g'_1) = \pi(g_2, g'_2)$$

$$\text{thus, } g_1 = g_2 \quad \cancel{g'_1 = g'_2} \quad ③$$

By equation ②

$$\pi_0^* \phi_1(p) = \pi_0^* \phi_2(p)$$

$$\pi^*(g_1, g_1') = \pi^*(g_2, g_2')$$

$$g_1' = g_2' \quad \text{--- ④}$$

By ③ and ④,

$$\phi_1(p) = \phi_2(p)$$

Since  $p$  is arbitrary,  $\phi_1 = \phi_2$

Therefore  $f$  is injective.

③  $f$  is surjective.

Let  $(\tilde{\psi}, \tilde{\psi}') \in B$

Define  $\tilde{\phi}: H \rightarrow G \times G'$   
 $q \mapsto (\tilde{\psi}(q), \tilde{\psi}'(q))$

sub claim 3.1:  $\tilde{\phi}$  is homomorphism

Let  $\tilde{h}_1, \tilde{h}_2 \in H$ .

$$\begin{aligned}\tilde{\phi}(h_1, h_2) &= (\tilde{\psi}(\tilde{h}_1, \tilde{h}_2), \tilde{\psi}'(\tilde{h}_1, \tilde{h}_2)) \\ &= (\tilde{\psi}(h_1)\tilde{\psi}(h_2), \tilde{\psi}'(h_1)\tilde{\psi}'(h_2)) \\ &= (\tilde{\psi}(h_1), \tilde{\psi}'(h_1))(\tilde{\psi}(h_2), \tilde{\psi}'(h_2)) \\ &= \underbrace{\tilde{\phi}(h_1)}_{\tilde{\phi}} \cdot \underbrace{\tilde{\phi}(h_2)}_{\tilde{\phi}}\end{aligned}$$

Thus  $\tilde{\phi}$  is homomorphism from  $H$  to  $G \times G'$

$$\tilde{\phi} \in A$$

~~$\tilde{\phi} = R \circ \tilde{\phi}, \tilde{\phi}' = R' \circ \tilde{\phi}$~~

Now we need to check

$$\tilde{\psi} = R \circ \tilde{\phi} \text{ and } \tilde{\psi}' = R' \circ \tilde{\phi}$$

~~$\tilde{\phi}(h)$~~  Let  $\forall h \in H$ ,  
 $(\pi \circ \tilde{\phi})(h) = \pi(\tilde{\phi}(h)) = \pi(\tilde{\phi}(ch), \tilde{\phi}'(ch)) = \tilde{\phi}(h)$   
 thus,  $\pi \circ \tilde{\phi} = \tilde{\phi}$   
 Similarly,  $\pi' \circ \tilde{\phi} = \tilde{\phi}'$

$f(\tilde{\phi}) = (\pi \circ \tilde{\phi}, \pi' \circ \tilde{\phi}) = (\phi, \phi')$

Thus  $f$  is surjective.

**Exercise 4.76.** Let  $H$  and  $K$  be subgroups of a group  $G$ . Prove that the product set  $HK$  is a subgroup of  $G$  if and only if  $HK = KH$ .

**Solution :**

*Proof.* Let  $G$  be group and  $H, K \leq G$ .

- ( $\Rightarrow$ ): **Claim** : if  $HK \leq G$  then  $HK = KH$ .

Suppose  $HK \leq G$ .

– **sub claim:** Let  $x \in KH$ . Then  $x = kh$  for some  $h \in H$  and  $k \in K$ ,

$$x = kh = 1kh1 = (1k)(h1) \in HK$$

(Since  $1 \in H$  and  $1 \in K$ ). Thus,  $KH \subseteq HK$ .

– **sub claim:**  $KH \supseteq HK$ .

We can not use previous method. Because we still do not know  $KH$  is sub group or not.

Let  $y \in HK$ . Since  $HK \leq G$ ,  $y^{-1} \in HK$ . Then  $y^{-1} = hk$  for some  $h_0 \in H$  and  $k_0 \in K$ .

$$y = (y^{-1})^{-1} = (h_0 k_0)^{-1} = k_0 h_0 \in KH$$

Thus,  $KH \supseteq HK$ .

Therefore,  $KH = HK$ .

- ( $\Leftarrow$ ): **Claim** : If  $HK = KH$  then  $HK \leq G$ .

Now suppose that  $HK = KH$ . Suppose that  $HK = KH$  is empty. Then,  $H, K$  is empty. Now we use sub group test.

- *Closure:* Let  $x, y \in HK$ . Then  $x = h_1k_1$  and  $y = h_2k_2$  for some  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ .

$$xy = (h_1k_1)(h_2k_2) \quad (4.35)$$

$$= h_1(k_1h_2)k_2 \quad (\text{By associativity property}) \quad (4.36)$$

$$= h_1(h_3k_3)k_2 \text{ for some } h_3 \in H \text{ and } k_3 \in K \text{ (Since } KH = HK \text{)} \quad (4.37)$$

$$= (h_1h_3)(k_3k_2) \in HK \quad (4.38)$$

- *Inverse:* Let  $x \in HK$ . Then  $x = h'k'$  for some  $h' \in H$  and  $k' \in K$ .

$$x^{-1} = (h'k')^{-1} = k'h' \in KH = HK$$

Thus,  $HK \leq G$ .

Therefore, the product set  $HK$  is a subgroup of  $G$  if and only if  $HK = KH$   $\square$

#### 4.2.12 Quotient Groups

**Exercise 4.77.** Show that if a subgroup  $H$  of a group  $G$  is not normal, there are left cosets  $aH$  and  $bH$  whose product is not a coset.

*Proof.* Suppose that  $H \leq G$  but  $H \not\trianglelefteq G$ . We are going to use indirect proof. So, assume that  $(aH)(bH)$  is a coset for all  $a, b \in G$ . Then,

$$aHbH = abH$$

then for all  $h_1, h_2, h_3 \in H$ , So,

$$ah_1bh_2 = abh_3$$

$$ah_1bh_2 = abh_3 \quad (4.39)$$

$$a^{-1}(ah_1bh_2) = a^{-1}(abh_3) \quad (4.40)$$

$$(a^{-1}a)(h_1bh_2) = (a^{-1}a)(bh_3) \quad (4.41)$$

$$h_1bh_2 = bh_3 \quad (4.42)$$

$$b^{-1}(h_1bh_2)h_2^{-1} = b^{-1}(bh_3)h_2^{-1} \quad (4.43)$$

$$b^{-1}h_1b(h_2h_2^{-1}) = (b^{-1}b)h_3h_2^{-1} \quad (4.44)$$

$$b^{-1}h_1b = h_3h_2^{-1} \in H \quad (4.45)$$

$$(4.46)$$

Thus,  $b^{-1}h_1b \in H$ . and since  $b \in G$  and  $h_1 \in H$  is arbitrary,  $H$  is normal subgroup, which contradict the our hypothesis. Thus, there exist left cosets  $aH$  and  $bH$  whose product is not a coset.  $\square$

**Exercise 4.78.** In the general linear group  $GL_3(\mathbb{R})$ , consider the subsets:

$$H = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \mid * \text{ represents an arbitrary real number} \right\}$$

and

$$K = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid * \text{ represents an arbitrary real number} \right\}$$

Show that  $H$  is a subgroup of  $GL_3$ , that  $K$  is a normal subgroup of  $H$ , and identify the quotient group  $H/K$ . Determine the center of  $H$ .

- **Claim 1:**  $H \leq G$ .

Certainly! Let's prove that the subset  $H$  is a subgroup of the general linear group  $GL_3(\mathbb{R})$ .

- *Non-emptiness:* We start by showing that  $H$  is non-empty. The identity matrix  $\mathbf{I}_3$  belongs to  $H$  since it satisfies the conditions for  $H$ :

$$\mathbf{I}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Therefore,  $H$  is non-empty.

- *Closure under matrix multiplication:* Let  $\mathbf{A}$  and  $\mathbf{B}$  be matrices in  $H$ . We need to show that their product  $\mathbf{AB}$  is also in  $H$ . Consider:

$$\mathbf{A} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

The product  $\mathbf{AB}$  is:

$$\mathbf{AB} = \begin{pmatrix} 1 & a+x & by+az+b \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$

“““ Since  $a+x$ ,  $y+az+b$ , and  $c+z$  are arbitrary real numbers,  $\mathbf{AB}$  satisfies the conditions for  $H$ . Hence,  $H$  is closed under matrix multiplication.

- *Closure under taking inverses:* Let  $\mathbf{A}$  be a matrix in  $H$ . We need to show that its inverse  $\mathbf{A}^{-1}$  is also in  $H$ . The inverse of  $\mathbf{A}$  is:

$$\mathbf{A}^{-1} = \begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

Again, since  $-a$ ,  $ac - b$ , and  $-c$  are arbitrary real numbers,  $\mathbf{A}^{-1}$  satisfies the conditions for  $H$ . Therefore,  $H$  is closed under taking inverses. Hence, we have shown that  $H$  is a subgroup of  $GL_3(\mathbb{R})$ .

- **Claim 2 :**  $K \leq H$ .

I am not going to prove that this case, because this is exhausting. This is very easy.

- **Claim 3 :**  $K$  is normal sub group of  $H$ .

Let  $A := \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in H$  and  $B := \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K$ , where  $a, b, c, d \in \mathbb{R}$ .

Then,

$$ABA^{-1} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \quad (4.47)$$

$$= \begin{bmatrix} 1 & a & d + b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \quad (4.48)$$

$$= \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K \quad (4.49)$$

Thus,  $K$  is normal sub group of  $H$ .

- **Quotient group  $H/K$  :**

Let  $h_1, h_2 \in H$  be such that

$$h_1 = \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } h_2 = \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}.$$

Suppose that  $h_1 K = h_2 K$ . By Artin's book 2.85,  $h_1^{-1} h_2 \in K$ .

$$h_1^{-1} h_2 = \begin{bmatrix} 1 & -a_1 & a_1 c_1 - b_1 \\ 0 & 1 & -c_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -a_1 + a_2 & b_2 - a_1 c_2 + a_1 c_1 - b_1 \\ 0 & 1 & -c_1 + c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

Since,

$$h_1 K = h_2 K \iff h_1^{-1} h_2 \in K \quad (4.50)$$

$$\iff -a_1 + a_2 = 0 \text{ and } -c_2 - c_1 \quad (4.51)$$

$$\iff a_1 = a_2 \text{ and } c_1 = c_2 \quad (4.52)$$

Thus,

$$H/K = \left\{ hK \mid \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, a, c \in \mathbb{R} \right\}$$

- **Center of Group H**

$$Z(H) = \left\{ A \in H \mid AX = XA \text{ for all } X \in H \right\}$$

Let's find center. We need to find  $a, b, c \in \mathbb{R}$  such that

$$\begin{aligned} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \text{ for all } x, y, z \in \mathbb{R} \\ \begin{bmatrix} 1 & a+x & b+y+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & a+x & b+y+xc \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix} \end{aligned} \quad (4.54)$$

By comparing  $1 \times 3$  index, we need to find that  $a, b, c \in \mathbb{R}$   $az = xc$  for all  $x, y, z \in \mathbb{R}$ . SO, the only possibility is  $a = c = 0$ . Thus,

$$Z(H) = \left\{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mid b \in \mathbb{R} \right\}$$

**Exercise 4.79.** Let  $P$  be a partition of a group  $G$  with the property that for any pair of elements  $A, B$  of the partition, the product set  $AB$  is contained entirely within another element  $C$  of the partition. Let  $N$  be the element of  $P$  that contains 1. Prove that  $N$  is a normal subgroup of  $G$  and that  $P$  is the set of its cosets.

*Proof.*

- **Claim 1:** The product set  $NN = N$ .

Let  $x \in N$ , Then  $x = x \cdot 1 \in NN$ . Thus,  $N \subseteq NN$ . We know that the product set  $NN$  is contained entirely within an element of partition, but  $N$  is a partition. The only way this happen  $N = NN$ .

- **Claim 2:**  $N \leq G$ .

- *Subset*: It is very clear that  $N \subseteq G$ .
- *Closure*: Let  $x, y \in N$ . Then  $(xy) \in NN = N$ . So,  $N$  is closed under composition.
- *Identity*: Given that  $1 \in N$ .
- *Inverse*: Let  $x \in N$ . We have to show that  $x^{-1}$  is contained in  $N$ . We use proof by contradiction. So, Assume contrary,  $x^{-1} \in M$ ,  $M$  is an element of partition  $P$  such that  $N \neq M$ .

$$xx^{-1} \in NM, xx^{-1} = 1 \in N$$

So, we would have  $NM \subseteq N$  (since the product set is contained entirely within one of the sets of partition). On the other hand,

$$1x^{-1} \in NM, 1x^{-1} = x^{-1} \in N$$

So,  $NM \subseteq N$  a contradiction.

Therefore, conclude that our assumption that  $x^{-1} \notin N$  was wrong, that we must have  $x^{-1} \in N$

- **Claim 3:**  $N \trianglelefteq$

Let  $a \in G$  and  $n \in N$ . Let  $a \in A$  and  $a^{-1} \in B$ , where  $A, B \in P$ .

$$ana^{-1} = ANB$$

, But also,  $1 \in N$ ,

$$g \cdot 1 \cdot g^{-1} = 1 \in ANB$$

Since  $P$  splits into disjoint subsets and the only one element of partition that contains 1 is  $N$ .

$$ANB = N$$

and but also  $gng^{-1} \in N$ . Therefore,  $N$  is normal subgroup.

**-Claim 4:**  $P$  is the set of its cosets.

Let  $A$  be some element of partition, and let  $a \in A$ .

Need to prove:  $A = aN$

- **Subclaim 4.1:**  $A \subseteq aN$ .

Let  $a \in A$ . Let  $b \in B$ , where  $B$  is element of partition. Then  $b^{-1}b \in BA$ ,  $b^{-1} = 1 \in N$  So,  $BA \subseteq N$ . Specially,

$$b^{-1}a \in N$$

So there exists some  $n \in N$  such that

$$b^{-1}a = n \iff a = bn \iff b = an^{-1}$$

Since  $N \leq G$ .  $n^{-1} \in N$ . Thus,  $b \in aN$ , so  $A \subset aN$ .

- Subclaim 4.2 :  $A \supseteq aN$ .
  - subclaim 4.2.1:  $AN \subseteq A$ ,

Note that  $a \in A$  and  $1 \in N$ . Thus,

$$a \cdot 1 \in AN, \quad a \cdot 1 = a \in A$$

Since, the product set is contained entirely in one element partition. Thus,  $AN \subseteq A$

Now,

$$aN = \{an | n \in N\} \subseteq \{an : a \in A, n \in N\} = AN \subseteq A$$

Thus,  $ax \in A$ , as required. Thus  $aN \subseteq A$

Hence, we can conclude that  $A = aN$ .

□

**Exercise 4.80.** Let  $H = \{\pm 1, \pm i\}$  be the subgroup of  $G = C^\times$  of fourth roots of unity. Describe the cosets of  $H$  in  $G$  explicitly. Is  $G/H$  isomorphic to  $G$ ?

Cosets are in the following form

$$ZH = \{zH, z^{-1}H\}, \text{ where } z \in \mathbb{C}^{\times}$$

We are going to use 1st isomorphism, we need to find a surjective homomorphism  $\varphi$  such that  $\ker(\varphi) = H$ .

Let  $\varphi: G \rightarrow G$  defined by

$$\begin{array}{ccc} & G & \longrightarrow G \\ z & \longmapsto & z^4 \end{array}$$

Claim 1:  $\varphi$  is homomorphism

Let  $a, b \in G$

$$\varphi(ab) = (ab)^4 = a^4 b^4 = \varphi(a) \varphi(b)$$

Thus,  $\varphi$  is homomorphism

Claim 2:  $\varphi$  is surjective.

Let  $c \in G$ . Then let  $d = \sqrt[4]{c}$ . We know that  $d$  exists. Because  $\mathbb{C}^{\times}$  have all  $n$ th roots every element of  $\mathbb{C}^{\times}$  (algebraically closed). Then,

$$\varphi(d) = c$$

Thus,  $\varphi$  is surjective.

claim 3:  $\ker(\psi) = H$

$$\begin{aligned}
 \ker(\psi) &= \{x \mid x^4 = 1\} \\
 &= \left\{ e^{\frac{2\pi i k}{4}} \mid k=0,1,2,3 \right\} \\
 &= \left\{ e^0, e^{\frac{2\pi i}{4}}, e^{\frac{4\pi i}{4}}, e^{\frac{6\pi i}{4}} \right\} \\
 &= \left\{ e^0, e^{\frac{\pi i}{2}}, e^{\pi i}, e^{\frac{3\pi i}{2}} \right\} \\
 &= \{1, i, -1, -i\} \\
 &= H
 \end{aligned}$$

claim 4:  $\text{Im}(\varphi) = G$

"We know that  $\text{Im}(\varphi) \subseteq G$   $\xrightarrow{*}$

Let  $x \in G - C^{\times}$ . Then  $x^{1/4}$  exists in  $C^{\times} - G$

$$\varphi(x^{1/4}) = x$$

Thus,  $\text{Im}(\varphi) \supseteq G$   $\xrightarrow{**}$

By  $*$  and  $**$   $\text{Im}(\varphi) = G$

claim:  $G/H \cong G$

By first theorem of isomorphism, we can conclude that,  $G/H \cong G$

**Exercise 4.81.** Let  $G$  be the group of upper triangular real matrices  $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$  with  $a$  and  $d$  different from zero. For each of the following subsets, determine whether or not  $S$  is a subgroup, and whether or not  $S$  is a normal subgroup. If  $S$  is a normal subgroup, identify the quotient group  $G/S$ .

1.  $S$  is the subset defined by  $b = 0$ .
2.  $S$  is the subset defined by  $d = 1$ .
3.  $S$  is the subset defined by  $a = d$ .

$$\textcircled{i} \quad S_i := \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, d \in \mathbb{R} \setminus \{0\} \right\}$$

Observe that  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$ . Thus,  $S \neq \emptyset$

Let  $A, B \in G$ . Then

$$A := \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \quad \text{for some } a_1, a_2 \in \mathbb{R} \setminus \{0\}$$

$$B := \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}$$

$$\text{Then } B^{-1} = \frac{1}{b_1 b_2} \begin{bmatrix} b_2 & 0 \\ 0 & b_1 \end{bmatrix} = \begin{bmatrix} 1/b_1 & 0 \\ 0 & 1/b_2 \end{bmatrix}$$

So,  $B^{-1} \in G$ . Thus,

$$\begin{aligned} AB^{-1} &= \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \begin{bmatrix} 1/b_1 & 0 \\ 0 & 1/b_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1/b_1 & 0 \\ 0 & a_2/b_2 \end{bmatrix} \end{aligned}$$

Since  $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{R} \setminus \{0\}$ , Thus  $AB^{-1} \in S$

Therefore,  $S$  is a subgroup.

Let's check  $S_3$  is normal or not

Claim:  $S_3$  is not normal

Let  $X := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in G$ . Then

$$X^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

Let  $Y = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in B$ . Then,

$$XYX^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & -1 \end{bmatrix}. \text{ But } XYX^{-1} \notin B$$

Therefore,  $B$  is NOT a Normal subgroup

$$\textcircled{2} \quad S'' := \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{R} \right\}$$

claim1:  $S'' \leq G$

Observe that  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S''$ . Thus  $S'' \neq \emptyset$ .

Let  $X'' = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \& Y'' = \begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} \in S''$

$$\begin{aligned} \text{Then } (Y'')^{-1} &:= \frac{1}{e} \begin{bmatrix} 1 & -f \\ 0 & e \end{bmatrix} \\ &= \begin{bmatrix} 1/e & -f/e \\ 0 & 1 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} (X'')(Y'')^{-1} &:= \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1/e & -f/e \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} ae & af+b \\ 0 & 1 \end{bmatrix} \in S'' \end{aligned}$$

Thus,  $S'' \leq G$

### Cosets

Let  $gS, hS \in G/S$ .

$$gS = hS \iff h^{-1}g \in S$$

$$\text{Let } g = \begin{bmatrix} g_1 & g_2 \\ 0 & g_3 \end{bmatrix}, h = \begin{bmatrix} h_1 & h_2 \\ 0 & h_3 \end{bmatrix}$$

where,  $g_1, g_2, g_3, h_1, h_2, h_3 \in \mathbb{R}$  and  $g_1, g_2, h_1, h_3 \neq 0$

$$\begin{aligned} \text{Then, } h^{-1}g &= \begin{bmatrix} 1/h_1 & -h_2/h_1h_3 \\ 0 & 1/h_3 \end{bmatrix} \begin{bmatrix} g_1 & g_2 \\ 0 & g_3 \end{bmatrix} \\ &= \begin{bmatrix} g_1/h_1 & g_2/h_1 - \frac{g_2h_2}{h_1h_3} \\ 0 & g_3/h_3 \end{bmatrix} \end{aligned}$$

$$\text{Thus } h^{-1}g \in S \iff \frac{g_3}{h_3} = 1 \iff g_3 = h_3$$

$$\text{Therefore, } gS \neq hS \iff g_3 \neq h_3$$

Note that  $g_1, g_2$  does not help to determine whether two cosets are equal.

Thus, we can fix  $a=1, b=0$ ,

$$G/S := \left\{ gS \mid g = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}, c \in \mathbb{R} \setminus \{0\} \right\}$$

$$(3) S''' := \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}$$

Observe that,  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S'''$ . Thus,  $S''' \neq \emptyset$

Let  $A := \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ ,  $B := \begin{bmatrix} e & f \\ 0 & e \end{bmatrix} \in S'''$ , where  $a, b, e, f \in \mathbb{R} \setminus \{0\}$

$$\text{Then } B' = \frac{1}{e^2} \begin{bmatrix} e & f \\ 0 & e \end{bmatrix} = \begin{bmatrix} 1/e & f/e \\ 0 & 1/e \end{bmatrix}$$

$$AB^{-1} = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \begin{bmatrix} 1/e & f/e \\ 0 & 1/e \end{bmatrix} = \begin{bmatrix} ae & af+be \\ 0 & ae \end{bmatrix} \in S'''$$

Thus,  $S''' \leq G$

$$\text{Let } A := \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in G. \text{ So, } A^{-1} := \begin{bmatrix} 1/a & -b/a \\ 0 & 1/c \end{bmatrix}$$

Let  $B := \begin{bmatrix} e & f \\ 0 & e \end{bmatrix} \in S'''$ . Then

$$ABA^{-1} = \begin{bmatrix} e & \cancel{(eb+af+be)} \\ 0 & e \end{bmatrix} \in S'''$$

Thus,  $S'''$  is normal.

So, we can fix that  $g_2=0$

$$G/S := \left\{ gS \mid g = \begin{bmatrix} g_1 & 0 \\ 0 & g_3 \end{bmatrix}, g_1, g_3 \in \mathbb{R} \right\}$$

#### 4.2.13 Miscellaneous Problems

**Exercise 4.82 (M1).** Describe the column vectors  $(a, c)^T$  that occur as the first column of an integer matrix  $A$  whose inverse is also an integer matrix.

$$\text{Let } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z})$$

$$A^{-1} \text{ exists} \iff \det(A) = ad - bc \neq 0$$

$$A^{-1} = \frac{1}{(ad - bc)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Lemma: Let  $A$  be matrix with integer entries.  
 $A^{-1}$  has integer entries  $\iff \det(A) = \pm 1$

We know that

$1 = \det(I) = \det(A^{-1}A) = \det(A^{-1})\det(A)$ . Thus,  
 $A$  and  $A^{-1}$  have integer entries  $\iff \det(A) = \pm 1$

Claim:  $a$  and  $c$  are relative prime

Assume that  $g = \gcd(a, c) > 1$ . Then

$$a = gk_1 \text{ and } c = gk_2 \text{ for some } k_1, k_2 \in \mathbb{Z}$$

$$\begin{aligned} \text{Thus, } \det(A) &= ad - bc = gk_1d - gk_2c \\ &= g(k_1d - k_2c) \end{aligned}$$

Thus  $g \mid \det(A)$

But  $\det(A) = \pm 1$ . So, it contradicts  $g > 1$ .

Hence,  $\gcd(a, c) = 1$

Therefore  $a$  and  $c$  must relative prime

#### Exercise 4.83 (M.2).

- (a) Prove that every group of even order contains an element of order 2.
- (b) Prove that every group of order 21 contains an element of order 3.

**Claim a :** Let  $G$  be a group whose identity is  $e$ . Let  $G$  be of even order. Then,  $\exists x \in G : |x| = 2$

*Proof.* (Claim a) In any group  $G$ , the identity element  $e$  is self-inverse with the property that the identity is the only group element of order 1, and is the only such element.

That leaves an odd number of elements.

Each element in  $x \in G : |x| > 2$  can be paired off with its inverse, as  $|x^{-1}| = |x| > 2$  (Since order of a group element equals the order of its inverse.)

Hence there must be at least one element which has not been paired off with any of the others which is therefore self-inverse. Let's say it, ' $y$ '.

$$y^{-1} = y \iff x \cdot y = e \quad (4.55)$$

$$\iff |y| = 2 \quad (4.56)$$

Thus, every group of even order contains an element of order 2.  $\square$

**Claim b:** Let  $G$  be a group whose identity is  $e$ . Let  $G$  be of order 21. ( $|G|=21|$ )  
Then,  $\exists x \in G : |x| = 3$

**Exercise 4.84** (Artin 2.M.9). (Double Cosets) Let  $H$  and  $K$  be subgroups of a group  $G$ , and let  $g$  be an element of  $G$ . The set  $HgK = \{x \in G | x = hgk \text{ for some } h \in H, k \in K\}$  is called a double coset. Do the double cosets partition  $G$ ?

They partition  $G$ . The proof is similar to the proof that left cosets of one subgroup partition  $G$ .

On  $G$ , define the relation  $\sim$  as

$$a \sim b \text{ iff } b = hak; \text{ for some } h \in H, k \in K$$

Let's prove that this is an equivalence relation. Let  $a, b, c \in G$ . - Reflexive?: Let  $g \in G$ . Then we can write

$$g = 1g1$$

Moreover,  $1 \in H$  and  $1 \in K$ , so  $g \sim g$ . Therefore, for every  $g \in G$  we have that  $g \sim g$ . so  $\sim$  is reflexive.

- Symmetric?: Suppose that  $a \sim b$ . Then  $b = hak$ , for some  $h \in H, k \in K$ . Multiplying by  $h^{-1}$  from the left and  $k^{-1}$  from the right we get

$$a = h^{-1}ak^{-1}$$

Since  $H$  is a subgroup of  $G$ ,  $h^{-1} \in H$ . Similarly,  $k^{-1} \in K$ . Thus,  $b \sim a$ . So, for every  $a, b \in G$  such that  $a \sim b \implies b \sim a$ . Thus,  $\sim$  is symmetric.

- Transitive?: Suppose that  $a \sim b$  and  $b \sim c$ . Then  $b = hak$  for some  $h \in H, k \in K$ , and  $c = h'b'k'$  for some  $h' \in H, k' \in K$ . Therefore,

$$c = h'hbk' = hhakk' = (hh')a(kk')$$

Thus,  $a \sim b$  and  $b \sim c$  then  $a \sim c$ . Therefore  $\sim$  is transitive.

By Artin's book Proposition 2.7.4, double cosets partition  $G$ ?

**Exercise 4.85** (Artin 2.M.10). Let  $H$  be a subgroup of a group  $G$ . Show that the double cosets (see Exercise M.9))

$$HgH = \{h_1gh_2 | h_1, h_2 \in H\}$$

are the left cosets  $gH$  if and only if  $H$  is normal.

*Proof.*

- ( $\implies$ ): Suppose that  $gH = HgH$ . Let  $g \in G$  and  $h \in H$ .  $ghg^{-1} \in H$ ?

$\square$

**4.2.14 Problem**

# Chapter 5

## Tempoarray files for exercises

### 5.1 Chapter 3

#### 5.1.1 Fields

**Exercise 5.1** (Artin 3.1.1). Prove that the numbers of the form  $a+b\sqrt{2}$ , where  $a$  and  $b$  are rational numbers, form a subfield of  $\mathbb{C}$

Let me introduce new notation for this set.

$$\mathbb{Q}[\sqrt{2}] := \{x \in \mathbb{C} \mid x = a + b\sqrt{2}, a, b \in \mathbb{Q}\}$$

claim:  $(\mathbb{Q}\sqrt{2}, +, \times)$  is a field

Note that addition (+) and multiplication ( $\times$ ) is used here is same as complex numbers. So it is well defined.

F1: claim.  $(\mathbb{Q}\sqrt{2}, +)$  is an abelian group

Closure? Let  $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

Identity:  $0 = 0 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$  is the identity of  $(\mathbb{Q}[\sqrt{2}], +)$

$$\begin{aligned} (a_1 + b_1\sqrt{2}) + (0 + 0\sqrt{2}) &= (a_1 + 0) + (b_1 + 0)\sqrt{2} \\ &= a_1 + b_1\sqrt{2} \end{aligned}$$

Similarly we can prove that  $(0 + 0\sqrt{2}) + (a_1 + b_1\sqrt{2})$ . Thus 0 is the identity of  $(\mathbb{Q}[\sqrt{2}], +)$ .

Inverse.

$$(a+b\sqrt{2}) + ((-a)+(-b)\sqrt{2}) = (a-a) + (b-b)\sqrt{2} = 0 + 0\sqrt{2} = 0$$

$$\text{Similarly, } ((-a)+(-b)\sqrt{2}) + (a+b\sqrt{2}) = 0 + 0\sqrt{2} = 0$$

Thus  $(-a)+(-b)\sqrt{2}$  is the inverse of  $a+b\sqrt{2}$ .

Commutative: As addition is commutative in  $\mathbb{C}$

it follows the restriction of commutative operator is

Commutative: Thus  $(\mathbb{Q}\sqrt{2}, +)$  is an abelian group

F2:  $(\mathbb{Q}\sqrt{2})^\times, \times$  is an abelian group

Closure

Let  $a_1+b_1\sqrt{2}, a_2+b_2\sqrt{2} \in \mathbb{Q}\sqrt{2}$

$$(a_1+b_1\sqrt{2}) \cdot (a_2+b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Q}\sqrt{2}$$

Identity

$$\begin{aligned} \overline{(a+b\sqrt{2})} \cdot (1+0\sqrt{2}) &= a \cdot 1 + 2 \cdot b \cdot 0 + (a \cdot 0 + b \cdot 1)\sqrt{2} \\ &= a + b\sqrt{2} \end{aligned}$$

Similarly,  $(1+0\sqrt{2}) \cdot (a+b\sqrt{2}) = a+b\sqrt{2}$

Thus  $(1+0\sqrt{2})$  is the identity on  $\times$  on  $(\mathbb{Q}\sqrt{2})^\times$ .

Inverse

$$\overline{(a+b\sqrt{2})} \times \frac{(a-b\sqrt{2})}{(a^2-b^2)} = 1 = 1+0\sqrt{2}$$

$$\frac{(a-b\sqrt{2})}{(a^2-b^2)} (a+b\sqrt{2}) = 1 = 1+0\sqrt{2}.$$

So,  $\frac{(a-b\sqrt{2})}{(a^2-b^2)}$  is the inverse of the  $a+b\sqrt{2}$ .

Commutative: As addition is commutative in  $\mathbb{C}$  it follows the restriction of commutative operator is commutative. Thus  $((\mathbb{Q}\sqrt{2})^\times, +)$  is an abelian group

F3 : Distributive

We have that Real Multiplication distributes Addition.

Therefore  $(\mathbb{Q}[\sqrt{2}], +, \times)$  is a field in  $\mathbb{C}$

**Exercise 5.2** (Artin 3.1.2). Find the inverse of 5 modulo  $p$ , for  $p = 7, 11, 13$ ,

and 17.

P=7

We use Euclidean Algorithm,

$$\begin{array}{l} 7 = 1(5) + 2 \quad | \Rightarrow 1 = 1(5) - 2(2) \\ 5 = 2(2) + 1 \quad | \quad 1 = 1(5) - 2(1(7) - 1(5)) \\ \quad \quad \quad \quad \quad \quad 1 = 1(5) - 2(7) + 2(5) \\ \quad \quad \quad \quad \quad \quad 1 = 3(5) - 2(7) \end{array}$$

Thus,  $3 \cdot 5 \equiv 1 \pmod{7}$ . Therefore  $5^{-1} = 3$  in mod 7

P=11

We use Euclidean Algorithm

$$11 = 2(5) + 1 \Rightarrow 1 = 11 - 2(5)$$

Thus,  $(-2) \cdot 5 \equiv 1 \pmod{11}$ . Therefore,  $5^{-1} = 9$  in modulo 11

P=13

$$\begin{array}{l} 13 = 2(5) + 3 \quad | \quad 1 = 1(3) - 1(2) \\ 5 = 1(3) + 2 \quad | \quad 1 = 1(3) - 1(1(5) - 1(3)) \\ 3 = 1(2) + 1 \quad | \quad 1 = 2(3) - 1(5) \\ \quad \quad \quad \quad \quad \quad 1 = 2(1(13) - 2(5)) - 1(5) \\ \quad \quad \quad \quad \quad \quad 1 = 2(13) - 5(5) \end{array}$$

Thus,  $(-5)5 \equiv 1 \pmod{13}$

$8 \cdot 5 \equiv 1 \pmod{13}$ . Therefore  $5^{-1} = 8$  in modulo 13

$p=7$ 

We use Euclidean Algorithm,

$$\begin{aligned} 7 &= 1(5) + 2 \quad | \quad 1 = 1(5) - 2(2) \\ 5 &= 2(2) + 1 \quad | \quad 1 = 1(5) - 2(1(7) - 1(5)) \\ &\quad \quad \quad 1 = 1(5) - 2(7) + 2(5) \\ &\quad \quad \quad 1 = 3(5) - 2(7) \end{aligned}$$

Thus,  $3 \cdot 5 \equiv 1 \pmod{7}$ . Therefore  $5^{-1} = 3$  in mod 7 $p=11$ 

We use Euclidean Algorithm

$$11 = 2(5) + 1 \Rightarrow 1 = 11 - 2(5)$$

Thus,  $(-2) \cdot 5 \equiv 1 \pmod{11}$   
 $9 \cdot 5 \equiv 1 \pmod{11}$ . Therefore,  $5^{-1} = 9$  in modulo 11 $p=13$ 

$$\begin{array}{l|l} 13 = 2(5) + 3 & 1 = 1(3) - 1(2) \\ 5 = 1(3) + 2 & 1 = 1(3) - 1(1(5) - 1(3)) \\ 3 = 1(2) + 1 & 1 = 2(3) - 1(5) \\ & 1 = 2(1(13) - 2(5)) - 1(5) \\ & 1 = 2(13) - 5(5) \end{array}$$

Thus,  $(-5) \cdot 5 \equiv 1 \pmod{13}$   
 $8 \cdot 5 \equiv 1 \pmod{13}$ . Therefore  $5^{-1} = 8$  in modulo 13

**Exercise 5.3** (Artin 3.1.3). Compute the product polynomial  $(x^3 + 3x^2 + 3x + 1)(x^4 + 4x^3 + 6x^2 + 4x + 1)$  when the coefficients are regarded as elements of the field  $\mathbb{F}_7$ . Explain your answer.

$$\begin{aligned}
 & (\chi^3 + 3\chi^2 + 3\chi + 1)(\chi^4 + 4\chi^3 + 6\chi^2 + 4\chi + 1) \\
 &= \chi^3(\chi^4 + 4\chi^3 + 6\chi^2 + 4\chi + 1) \\
 &\quad + 3\chi(\chi^4 + 4\chi^3 + 6\chi^2 + 4\chi + 1) \quad (\text{By distributive property}) \\
 &\quad + 3\chi(\chi^4 + 4\chi^3 + 6\chi^2 + 4\chi + 1) \\
 &\quad + 1(\chi^4 + 4\chi^3 + 6\chi^2 + 4\chi + 1) \\
 &= \chi^7 + 4\chi^6 - 6\chi^5 + 4\chi^4 + \chi^3 \\
 &\quad + 3\chi^6 + 12\chi^5 + 18\chi^4 + 12\chi^3 + 3\chi^2 \quad (\text{By distributive property}) \\
 &\quad + 3\chi^5 + 12\chi^4 + 18\chi^3 + 12\chi^2 + 3\chi \\
 &\quad + \chi^4 + 4\chi^3 + 6\chi^2 + 4\chi + 1 \\
 &= \chi^7 + 7\chi^6 + 21\chi^5 + 35\chi^4 + 35\chi^3 + 21\chi^2 + 7\chi + 1 \\
 &= \chi^7 + 1 \quad \left( \begin{array}{l} \text{Because } 7 \equiv 0 \pmod{7} \\ 21 \equiv 0 \pmod{7} \\ 35 \equiv 0 \pmod{7} \end{array} \right)
 \end{aligned}$$

**Exercise 5.4** (Artin 3.1.4). Consider the system of linear equations

$$\begin{bmatrix} 6 & -3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$$

- a. Solve the system in  $\mathbb{F}_p$  when  $p = 5, 11$ , and  $17$ .
- b. Determine the number of solutions when  $p = 7$ .

$$A = \begin{bmatrix} 6 & 3 \\ 2 & 6 \end{bmatrix} \quad B = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$$

$$\det(A) = 36 + 6 = 42$$

p=5 In modulo 5,  $\det(A)=2$  and  $2^{-1}=3$  in  $\mathbb{F}_5$

$$\text{Then } A^{-1} = 3 \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix} = 3 \begin{bmatrix} 1 & 3 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 9 \\ -6 & 3 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 4 & 3 \end{bmatrix}$$

$$\text{So, } X = A^{-1}B = \begin{bmatrix} 3 & 4 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} 9+4 \\ 12+3 \end{bmatrix} = \begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \end{bmatrix}$$

p=11

In modulo 11,  $\det(A)=42=9$ ,  $9^{-1}=5$

$$\text{Then, } A^{-1} = 5 \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix} = \begin{bmatrix} 30 & 15 \\ -10 & 30 \end{bmatrix} = \begin{bmatrix} 8 & 4 \\ 1 & 8 \end{bmatrix}$$

$$A^{-1}B = \begin{bmatrix} 8 & 4 \\ 1 & 8 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} 24+4 \\ 3+8 \end{bmatrix} = \begin{bmatrix} 28 \\ 11 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix}$$

p=17

In modulo 11,  $\det(A)=42=8$ ,

We have to find  $8^{-1}=15$

$$17 = 2(8) + 1$$

$$1 = 17 - 2(8)$$

$$\text{Thus } 8^{-1} \equiv (-2) \equiv 15 \pmod{17}$$

$$A^{-1} = 15 \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix} = \begin{bmatrix} 5 & 11 \\ 4 & 5 \end{bmatrix}. \text{ So, } A^{-1}B = \begin{bmatrix} 5 & 11 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} 15+11 \\ 12+5 \end{bmatrix} = \begin{bmatrix} 26 \\ 17 \end{bmatrix} = \begin{bmatrix} 9 \\ 0 \end{bmatrix}$$

b) If  $p=7$ ,

In modulo 7,  $\det(A)=42=0$

Therefore  $A^{-1}$  does not exist. Therefore, The system have no solution.

**Exercise 5.5** (Artin 3.1.5). Determine the primes  $p$  such that the

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & -1 \\ -2 & 0 & 2 \end{bmatrix}$$

is invertible, when its entries are considered to be in  $\mathbb{F}_p$ .

$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & -1 \\ -2 & 0 & 2 \end{bmatrix}$ . Let's find the

$$\det(A) := 1 \begin{vmatrix} 3 & 1 \\ 0 & 2 \end{vmatrix} - 2 \begin{vmatrix} 0 & -1 \\ 2 & 2 \end{vmatrix} + 0$$

$$= 1(6-0) - 2(0-2) = 6+4=10$$

$A$  is not invertible  $\iff \det(A)=10 \equiv 0 \pmod{p}$

$$\iff p|10$$

$$\iff p=2 \text{ or } p=5 \text{ (since } p \text{ is prime)}$$

Thus,  $A$  is invertible  $\iff p \neq 2$  and  $p \neq 5$

**Exercise 5.6** (Artin 3.1.5). Solve completely the systems of linear equations  $AX = 0$  and  $AX = B$ , where

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$$

- (a) in  $\mathbb{Q}$ ,
- (b) in  $\mathbb{F}_2$ ,
- (c) in  $\mathbb{F}_3$ ,
- (d) in  $\mathbb{F}_7$

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}$$

$$\begin{aligned} \det(A) &:= 1 \begin{vmatrix} 0 & 1 \\ -1 & -1 \end{vmatrix} - 1 \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} + 0 \\ &= 1(0+1) - 1(-1-1) \\ &= 1+2 = 3 \end{aligned}$$

Recall following Result from Linear Algebra

$A$  is invertible  $\Leftrightarrow$  null space = {0}

a) in  $\mathbb{Q}$

$$\det(A) = 3 \neq 0 \Rightarrow A \text{ is invertible} \Rightarrow \begin{matrix} \text{null space} = \{0\} \\ \downarrow \\ x=0 \end{matrix}$$

b) in  $\mathbb{F}_2$

$$\det(A) = 3 = 1 \neq 0 \Rightarrow A \text{ is invertible} \Rightarrow \begin{matrix} \text{null space} = \{0\} \\ \downarrow \\ x=0 \end{matrix}$$

c) in  $\mathbb{F}_3$

$$\det(A) = 3 = 0 \Rightarrow A \text{ is not invertible} \Rightarrow \text{null space} \neq \{0\}$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\left[ \begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & 1 & 0 \end{array} \right] \xrightarrow{R_3 \rightarrow R_3 + R_1} \left[ \begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & -1 & 0 \end{array} \right] \xrightarrow{R_3 \rightarrow R_3 + R_2} \left[ \begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right]$$

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \end{cases} \Rightarrow X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_1 \\ -x_1 \end{bmatrix} = \begin{bmatrix} 1 & x_1 \\ 2 & x_1 \\ 2 & x_1 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}$$

Nullspace contains all multiples of  $s = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}$

$$\text{Nullspace} = \left\{ 0 \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, 1 \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, 2 \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \right\} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ 4 \end{bmatrix} \right\}$$

d) In  $\mathbb{F}_7$

$$\det(A) = 3 \neq 0 \Rightarrow A \text{ is invertible} \Rightarrow \text{Nullspace} = \{0\}$$

$$\downarrow \\ X = 0$$

$$\text{Cofact}(A) = \begin{pmatrix} \begin{vmatrix} 0 & 1 \\ 1 & -1 \end{vmatrix} & -\begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 1 & -1 \end{vmatrix} \\ -\begin{vmatrix} 1 & 0 \\ 1 & -1 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 1 & -1 \end{vmatrix} & -\begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} \\ \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 0 \\ 1 & 0 \end{vmatrix} & \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} \end{pmatrix} = \begin{bmatrix} 1 & 2 & -1 \\ 1 & -1 & 2 \\ 1 & -1 & -1 \end{bmatrix}$$

$$\text{Adj}(A) = (\text{Cofact}(A))^T = \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix}$$

In  $\mathbb{Q}$   
Let's find  $\det(A)^{-1} = 3^{-1} = \frac{1}{3}$  in  $\mathbb{Q}$ . Then.

$$A^{-1} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix}$$

$$X = A^{-1}B = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1-1+1 \\ 2+1-1 \\ -1-2-1 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 \\ 2 \\ -4 \end{bmatrix}$$

$\xrightarrow{n \in \mathbb{F}_2}$   $\det(A) = 3 = 1$  and  $(\det(A))^{-1} = 1$

$$A^{-1} = (\det(A))^{-1} \text{adj}(A)$$

$$= 1 \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$A^{-1}B = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

in  $\mathbb{F}_3$

$$\left[ \begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{array} \right] \xrightarrow{R_3 \rightarrow R_3 + R_1} \left[ \begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 2 & 0 & -1 & 2 \end{array} \right]$$

" "

$$\left[ \begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array} \right] \xrightarrow{R_3 \rightarrow R_3 + R_2} \left[ \begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 2 \end{array} \right]$$

Therefore system have no solution.

in  $\mathbb{F}_7$

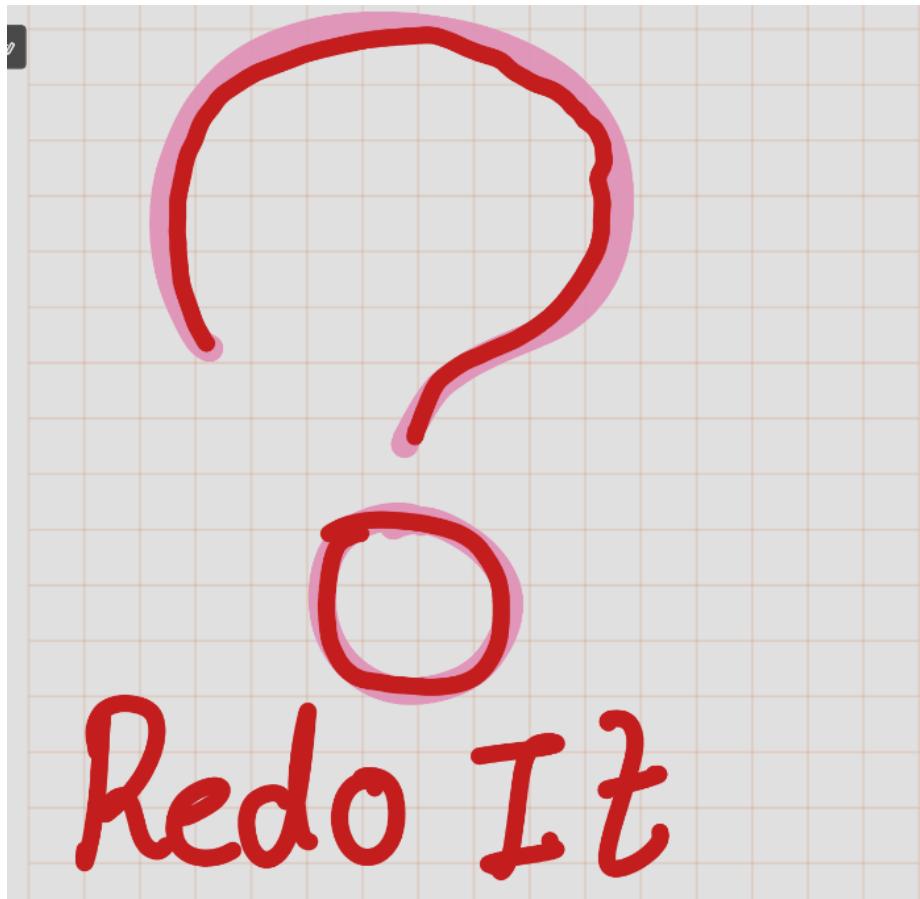
$$\det(A) = 3. \text{ So, } \det(A)^{-1} = 3^{-1} = 5$$

Then  $A^{-1} = (\det(A))^{-1} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} = 5 \begin{bmatrix} 1 & 1 & 1 \\ 2 & 6 & 6 \\ 6 & 2 & 6 \end{bmatrix}$

$$= \begin{bmatrix} 5 & 5 & 5 \\ 10 & 30 & 30 \\ 30 & 10 & 30 \end{bmatrix} = \begin{bmatrix} 5 & 5 & 5 \\ 3 & 2 & 2 \\ 2 & 3 & 2 \end{bmatrix}$$

$$X = A^{-1}B = \begin{bmatrix} 5 & 5 & 5 \\ 3 & 2 & 2 \\ 2 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 - 5 + 5 \\ 3 - 2 + 2 \\ 2 - 3 + 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \\ 1 \end{bmatrix}$$

**Exercise 5.7** (Artin 3.1.7). By finding primitive elements, verify that the multiplicative group  $\mathbb{F}_P^\times$  is cyclic for all primes  $p < 20$ .



**Exercise 5.8** (Artin 3.1.8). Let  $p$  be a prime integer. (a) Prove Fermat's Theorem: For every integer  $a$ ,  $a^p \equiv a \pmod{p}$ . (b) Prove Wilson's Theorem:  $(p - 1)! \equiv -1 \pmod{p}$ .

Let  $a \in \mathbb{Z}$  and  $p$  is a prime.  
 Proof of Fermat's Little Theorem.  
 first observe that

$$ar \equiv as \pmod{p} \iff r \equiv s \pmod{p}$$

Let's listing first  $p-1$  positive multiplies of  $a$

$$\{a, 2a, 3a, \dots, (p-1)a\}$$

$$\text{Then, } a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

$$a^{p-1} \equiv (p-1)! \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a \cdot a^{p-1} \equiv a \pmod{p}$$

$$a^p \equiv a \pmod{p}$$

Proof of Wilson's Theorem. Let  $p$  is prime and  $a \in \mathbb{Z}$

- If  $p=2$ , then it is trivially holds.

- If  $p \neq 2$ ,

Each  $k \in \{1, 2, \dots, p-1\}$  has an inverse

$k^{-1} \in \{1, 2, \dots, p-1\}$  in modulo  $p$  such that

$$k k^{-1} \equiv 1 \pmod{p}$$

This inverse is unique and  $(k^{-1})^{-1} = k$

If  $a = a^{-1}$  then  $1 \equiv a a^{-1} \equiv a^2 \pmod{p}$

$$\Rightarrow a^2 \equiv 1 \pmod{p}$$

$$\Rightarrow a \equiv \pm 1 \pmod{p}$$

Thus,  $a \equiv 1 \pmod{p}$  and  $a \equiv -1 \pmod{p}$

$a \equiv 1 \pmod{p}$  and  $a \equiv p-1 \pmod{p}$

In the  $\{1, 2, \dots, p-1\}$  has only two elements that are selfinverse. So we can pair elements with the inverse modulo  $p$ . Thus,

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv 1 \cdot 1 \cdot 1 \cdots (p-1) \equiv p-1 \equiv -1 \pmod{p}$$

$$(p-1)! \equiv -1 \pmod{p}$$

As an example: Let  $p=7$

$$\begin{aligned} 6! &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \\ &= 1 \times (\underbrace{2 \times 4}) \times (\underbrace{3 \times 5}) \times 6 \\ &\equiv 1 \times 1 \times 1 \times 6 \\ &\equiv 6 \equiv -1 \pmod{7} \end{aligned}$$

**Exercise 5.9** (Artin 3.1.9). Determine the orders of the matrices  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$  in the group  $GL_2(\mathbb{F}_7)$ .

First see following observations.

$$1) \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

$$2) \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 1 \end{pmatrix}$$

So, from first observation,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{we can easily prove this using mathematical induction}$$

for all  $n \in \mathbb{N}$ ,

Now let's go back to  $\mathbb{F}_7$ . Now,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^6 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^7 = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^4 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^5 = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} \quad \text{So, Order of } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ is } 7.$$

By 2nd observation,

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{array}{l} \text{(We can use mathematical)} \\ \text{induction to prove this)} \\ \text{it's trivial} \end{array}$$

Now in  $\mathbb{F}_3$

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Therefore, In  $\mathbb{F}_7$ , order of  $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$  is 3.

**Exercise 5.10** (Artin 3.1.10). Interpreting matrix entries in the field  $\mathbb{F}_2$ , prove that the four matrices

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

form a field.

Hint: You can cut the work down by using the fact that various laws are known to hold for addition and multiplication of matrices.

First Observe followings

- **Addition:**

+	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$

+	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\beginmath>\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$
$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

- *Closure ?*: By above table we can verify Closure.
- *Identity ?*: Identity element is  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ .
- *Inverse ?* : Inverse of each elements is itself.(We can verify it from the above table.)
- *Associativity ?*: Associativity property we can get from the matrix addition.
- *Commutative ?*: We can verify communicativeness of addition from the above table.

Thus, it makes abelian group under +.

- **Multiplication:**

*	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

- *Closure ?*: By above table we can verify Closure.
- *Identity ?*: Identity element is  $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ .
- *Inverse ?* : Inverse of each elements is itself.(We can verify it from the above table.)
- *Associativity ?*: Associativity property we can get from the matrix multiplication
- *Commutative ?*: We can verify communicativeness of addition from the above table.

Thus, the set of non-zero elements of given set is an abelian group.

**Distributive property:** Multiplications is distributive over addition.

Thus, The given set forms a field.

**Exercise 5.11** (Artin 3.1.9). Prove that the set of symbols  $\{a + bi \mid a, b \in \mathbb{F}_3\}$  forms a field with nine elements, if the laws of composition are made to mimic addition and multiplication of complex numbers. Will the same method work for  $\mathbb{F}_5$ ? For  $\mathbb{F}_7$ ? Explain.

$$\text{Let } S := \{a+bi \mid a, b \in \mathbb{F}_3\}$$

Then

$$S := \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+i, 2+2i\}$$

Associativity.

This derived from the fact the addition of Complex Numbers are associativity.

Identity:  $0 \in S$ , We can verify  $0$  is the identity from the complex number.

Inverse: Let  $a+bi \in S$ . Then we can find additive inverse of  $a$  and  $b$  in  $\mathbb{F}_3$ , (i.e:  $-a, -b \in \mathbb{F}_3$ )

Then

$$(a+bi)+(-a-bi) = (a-a)+i(b-b) = 0$$

Commutative: We can get it from the commutativeness property from the complex number.

Thus,  $(S, +)$  is an abelian group.

Let  $S^x := S \setminus \{0\}$

Associativity: We can get it from multiplication of complex numbers are associative.

Identity: Note that  $1 \in S^x$ . Since  $1$  is identity in  $(\mathbb{C}, \times)$ , we can tell that  $1$  is the identity of  $S^x$ .

Inverse: Let  $a+bi \in S^x$ . Then  $0 \neq a, b \in F_3$ . Then

Then  $a^2+b^2$  can be get only followings,

$$a^2+b^2 = 1, 2, 4, 5, 8, \text{ or } 0$$

In  $F_3$ ,  $a^2+b^2$  either  $1$  or  $2$

So,  $a^2+b^2 \neq 0$

$$\begin{aligned} 0^2+1^2 &= 1 = 1^2+0^2 \\ 0^2+2^2 &= 4 = 2^2+0^2 \\ 1^2+2^2 &= 5 = 2^2+1^2 \\ 1^2+1^2 &= 2 \\ 2^2+2^2 &= 8 \end{aligned}$$

Note that  $a^2+b^2 = 1$  or  $2$ . Thus inverse of  $(a^2+b^2)$  is itself. i.e.  $(a^2+b^2)^{-1} = (a^2+b^2)$

$$\begin{aligned} \text{Then } (a+bi) \cdot (a-bi) (a^2+b^2)^{-1} &= (a^2-b^2) \cdot (a^2+b^2)^{-1} \\ &= (a^2+b^2) (a^2+b^2)^{-1} \\ &= 1 \end{aligned}$$

Therefore  $(S^x, \times)$  is a group

\* Since multiplication on  $S$  is commutative (derived from the complex numbers)

\* Distributive property also holds.  $\rightarrow$  (Complex Number)

### 5.1.2 Vector Spaces

Exercise 5.12 (Artin 3.2.1).

2. (a) Prove that the scalar product of a vector with the zero element of the field  $F$  is the zero vector.

- (b) Prove that if  $w$  is an element of a subspace  $W$ , then  $-w$  is in  $W$  too.

Let  $V$  be an vector space of feild  $F$ .

Let  $\underline{0} \in V$  be the zero vector.

Let  $0 \in F$  be the zero element of  $F$ .

Let  $\underline{y} \in V$  be an vector.

$$0 \cdot \underline{y} = (0+0) \cdot \underline{y} \quad (\text{by feild axioms})$$

$$0 \cdot \underline{y} = 0 \cdot \underline{y} + 0 \cdot \underline{y} \quad (\text{distribution law})$$

$$\underbrace{0 \cdot \underline{y} + 0 \cdot \underline{y}}_{\underline{0}} = 0 \cdot \underline{y} + 0 \cdot \underline{y} + (-0) \cdot \underline{y}$$

$$\underline{0} = 0 \cdot \underline{y} + \underline{0}$$

$$\underline{0} = \underline{0}$$

b) Let  $W$  be subspace. Let  $\underline{w} \in W$ .  
 By def<sup>n</sup> of subspace  $c\underline{w} \in W$  for all  $c \in F$   
 Let  $c = -1$ . Then,

$$c\underline{w} = (-1)\underline{w} = -\underline{w} \in W$$

Here,  $-1$  represent the additive inverse of identity element in  $F$

**Exercise 5.13** (Artin 3.2.2). Which of the following subsets is a sub space of the vector space  $F^{n \times n}$  of  $n \times n$  matrices with coefficients in  $F$ ?

- (a) symmetric matrices ( $A = A^T$ ),
- (b) invertible matrices,
- (c) upper triangular matrices.

a) We have check two conditions:

Closed under addition

Let  $A, B$  two symmetric matrix,

$$A^T = A \text{ and } B^T = B$$

Let  $C = A + B$ , Now

$$C^T = (A + B)^T = A^T + B^T = (A + B) = C$$

Thus  $C$  is also symmetric.

Closed under scalar multiplication

Let  $A$  be a symmetric multiplication. Let  $D = cA$  where  $c$  is a scalar.

$$D^T = (cA)^T = cA^T = cA = D$$

Thus  $D$  is also symmetric.

Therefore: The set of symmetric is subset of

$$F^{n \times n}$$

b) Note that

$$\text{Let } A = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Note that  $A$  and  $B$  are invertible.

$$A+B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Note that  $(A+B)$  is not invertible.

Thus invertible matrices are not closed under addition,

Thus,  $F$  is not subspace of  $F^{n \times n}$

c) Addition

Let  $A, B$  be two upper triangle matrices.

$$a_{ij} = 0 \text{ for all } i > j$$

$$b_{ij} = 0 \text{ for all } i > j$$

$$\text{Let } C = A + B.$$

by def<sup>h</sup> of matrix additi

$$c_{ij} = a_{ij} + b_{ij}$$

Since  $a_{ij} = b_{ij} = 0$  for all  $i > j$

$$\text{Thus } c_{ij} = a_{ij} + b_{ij} = 0 \text{ for all } i > j$$

Thus  $C$  is upper triangle

Closed Under scalar multiplication

Let  $A$  be upper triangle matrix (i.e.  $a_{ij} \neq 0$  for  $i > j$ )

Let  $c$  be a scalar. Then by def<sup>b</sup>

$$ca_{ij} \neq 0 \text{ for } i > j$$

**Exercise 5.14** (Artin 3.3.1). Find a basis for the space of  $n \times n$  symmetric matrices ( $A^T = A$ ).

③ If  $n=2$ ,  $B_2 := \{E_{11}, E_{22}, E_{12} + E_{21}\}$

$$= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

If  $n=3$ ,  $B_3 := \{E_{11}, E_{22}, E_{33}, E_{12} + E_{21}, E_{21} + E_{31}, E_{13} + E_{32}\}$

$$= \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \right\}$$

So,  $B_n := \{E_{11}, E_{22}, \dots, E_{nn}, E_{12} + E_{21}, \dots, E_{(n-1)n} + E_{n(n-1)}\}$

Span

Let  $A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$  be a symmetric matrix. Then  $a_{12} = a_{21}, \dots, a_{(n-1)n} = a_{n(n-1)}$

Then  $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{12} & a_{22} & & & \vdots \\ a_{13} & & a_{33} & & a_{3(n-1)} \\ \vdots & \ddots & & a_{(n-1)(n-1)} & a_{nn} \end{bmatrix}$

So,  $A = a_{11}E_{11} + a_{22}E_{22} + \dots + a_{nn}E_{nn} + a_{12}(E_{12} + E_{21}) + a_{13}(E_{13} + E_{31}) + \dots + a_{1n}(E_{1n} + E_{n1}) + \dots + a_{(n-1)n}(E_{(n-1)n} + E_{n(n-1)})$

Therefore  $B_n$  spans the vector space of  $n \times n$  symmetric matrices.

---

• Linear independence

Suppose

$$a_{11}E_{11} + \dots + a_{nn}E_{nn} + a_{12}(E_{12} + E_{21}) + \dots + a_{(n-1)n}(E_{(n-1)n} + E_{n(n-1)}) = \underline{0}$$

$$a_{11}E_{11} + \dots + a_{nn}E_{nn} + a_{12}E_{12} + a_{21}E_{21} + \dots + a_{(n-1)n}E_{(n-1)n} + a_{n(n-1)}E_{n(n-1)} = \underline{0}$$

Since these matrices are elementary matrices,

$$a_{ij} = 0 \text{ for all } i, j \in \{1, 2, \dots, n\}$$

**Exercise 5.15** (Artin 3.3.2). Let  $W \subset \mathbb{R}^4$  be the space of solutions of the system of linear equations  $AX = 0$ , where  $A = \begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix}$ . Find a basis for  $W$ .

We have to find solution for following homogeneous system  
 $AX = 0$

$$\begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix} \xrightarrow{\substack{R_1 \rightarrow R_1 + (-R_2) \\ R_2 \rightarrow R_2 - R_1}} \begin{bmatrix} 1 & 0 & -1 & 3 \\ 0 & 1 & 4 & -3 \end{bmatrix}$$

$$x_1 - x_3 + 3x_4 = 0$$

$$x_2 + 4x_3 - 3x_4 = 0$$

Let  $x_3 = p$  and  $x_4 = q$  are parameters

$$\begin{aligned} \text{Then } x_1 &= p - 3q \\ x_2 &= -4p + 3q \end{aligned}$$

$$\begin{aligned}
 \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} &= \begin{bmatrix} p-3q \\ -4p+3q \\ p \\ q \end{bmatrix} = \begin{bmatrix} p \\ -4p \\ p \\ 0 \end{bmatrix} + \begin{bmatrix} -3q \\ 3q \\ 0 \\ q \end{bmatrix} \\
 &= p \begin{bmatrix} 1 \\ -4 \\ 1 \\ 0 \end{bmatrix} + q \begin{bmatrix} -3 \\ 3 \\ 0 \\ 1 \end{bmatrix} \\
 \text{So, } B &:= \left\{ \begin{bmatrix} 1 \\ -4 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 3 \\ 0 \\ 1 \end{bmatrix} \right\} \\
 \text{Thus, } B &\text{ is basis for space } W
 \end{aligned}$$

**Exercise 5.16** (Artin 3.3.3). Prove that the three functions  $x^2$ ,  $\cos(x)$ , and  $e^x$  are linearly independent.

*Proof.* Suppose that

$$\alpha x^2 + \beta \cos(x) + \gamma e^x = 0 \quad \text{for all } x \in \mathbb{R}$$

where  $\alpha, \beta, \gamma$  scalars.

1. The original equation, when substitute  $x = 0$  gives us  $b \cdot \cos(0) + c \cdot e^0 = 0$ , which simplifies to  $b + c = 0$ .
2. Differentiating once gives  $2a \cdot x - b \cdot \sin(x) + c \cdot e^x = 0$ . Substituting  $x = 0$  gives  $-b + c = 0$ .
3. Differentiating twice gives  $2a - b \cdot \cos(x) + c \cdot e^x = 0$ . Substituting  $x = 0$  gives  $2a + b + c = 0$ .

These equations show that the only solution is  $a = b = c = 0$ . Therefore, the functions  $x^2$ ,  $\cos(x)$ , and  $e^x$  are linearly independent.  $\square$

**Exercise 5.17** (Artin 3.3.4). Let  $A$  be an  $m \times n$  matrix, and let  $A'$  be the result of a sequence of elementary row operations on  $A$ . Prove that the rows of  $A$  span the same space as the rows of  $A'$ .



# Chapter 6

## Vector spaces.