

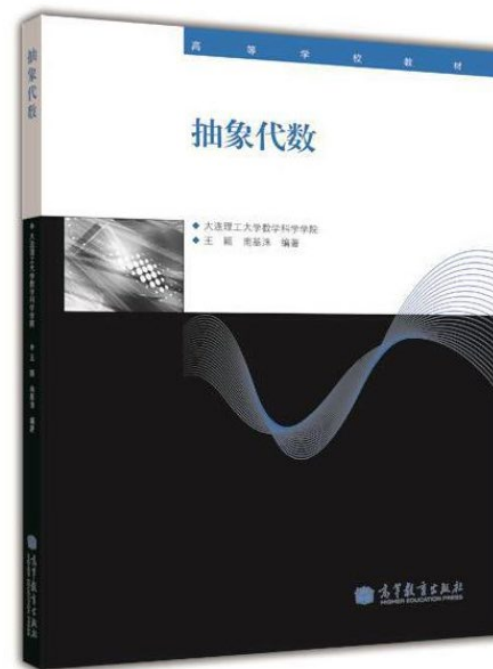
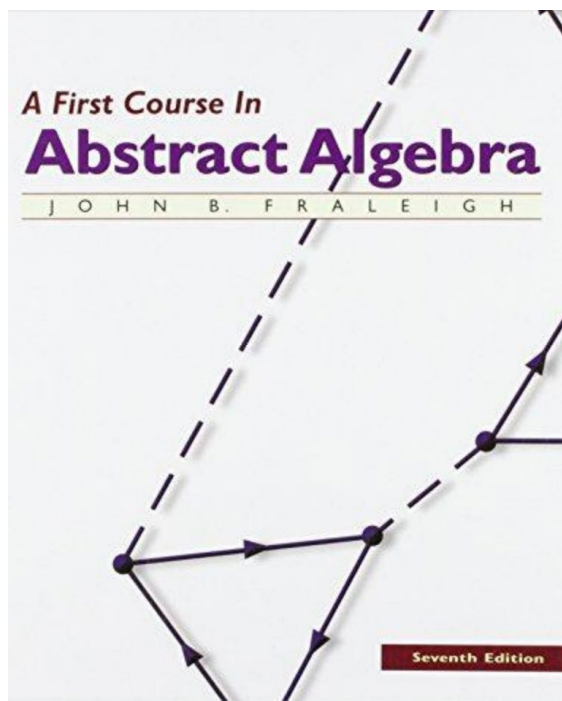


# Abstract Algebra

---

# Reference book

---



# Final score

---

Final test 50%

Homework 10%

Test in each lesson 10%

Chapter test  $10\% \times 3$

App score 10%

# SECTION 0: SETS AND RELATIONS

---

**Definition:** A **set** is a **well-defined** collection of objects.

$S$  is a **set** and  $a$  is some **object**, then either  $a$  is **definitely in**  $S$  (denoted by  $a \in S$ ), or  $a$  is **definitely not in**  $S$ , denoted by  $a \notin S$ .

the set  $S$  of some positive numbers.



the  $T$  of all prime positive integers.



# SECTION 0: SETS AND RELATIONS

---

**Definition:** A **set** is a **well-defined** collection of objects.

A **set**  $S$  is made up of **elements**, and if  $a$  is one of these elements, we shall denote this fact by  $a \in S$ .

There is exactly one set with no elements. It is the **empty set**, denoted by  $\emptyset$ .

# SECTION 0: SETS AND RELATIONS

---

2 ways:

listing elements separated by commas, in braces.

$\{2,4,6,8\}$ .

giving a characterizing property of the elements.  $\{x \mid P(x)\}$

$\{x \mid x \text{ is an even whole positive number } \leq 8\}$

$\{2x \mid x = 1, 2, 3, 4\}$

# SECTION 0: SETS AND RELATIONS

---

**0.1 Definition** A set  $B$  is a **subset** of a set  $A$ , denoted by  $B \subseteq A$  or  $A \supseteq B$ , if every element of  $B$  is in  $A$ .

The notations  $B \subset A$  or  $A \supset B$  will be used for  $B \subset A$  but  $B \neq A$ .

**Definition**  $A=B$  if  $A \supseteq B$  and  $B \supseteq A$ .

**Tips**  $A$  itself and  $\emptyset$  are both subsets of  $A$ .

**0.3 Example** Let  $S = \{1, 2, 3\}$ .

This set  $S$  has a total of eight subsets,

namely  $\emptyset$ ,  $\{1\}$ ,  $\{2\}$ ,  $\{3\}$ ,  $\{1, 2\}$ ,  $\{1, 3\}$ ,  $\{2, 3\}$ , and  $\{1, 2, 3\}$ .

# SECTION 0: SETS AND RELATIONS

---

**0.4 Definition** Let  $A$  and  $B$  be sets. The set  $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$  is the Cartesian product (卡尔积) of  $A$  and  $B$ .

**0.5 Example** If  $A = \{1, 2, 3\}$  and  $B = \{3, 4\}$ , then we have  $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$ .

**0.6 Example** The set  $R \times R$  is the familiar Euclidean plane.



# SECTION 0: SETS AND RELATIONS

---

## Notations

$\mathbb{Z}$  is the set of all integers (whole numbers: +, - and 0)

$\mathbb{Q}$  is the set of all rational numbers (that is, numbers that can be expressed as quotients  $m/n$  of integers, where  $n \neq 0$ ).

$\mathbb{R}$  is the set of all real numbers.

$\mathbb{C}$  is the set of all complex numbers.

$\mathbb{Z}^+$ ,  $\mathbb{Q}^+$ , and  $\mathbb{R}^+$  are the sets of positive members of  $\mathbb{Z}$ ,  $\mathbb{Q}$ , and  $\mathbb{R}$ , resp.

$\mathbb{Z}^*$ ,  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$  and  $\mathbb{C}^*$  are the sets of nonzero members of  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$ , resp.

# SECTION 0: SETS AND RELATIONS

---

**0.7 Definition** A relation between sets  $A$  and  $B$  is a subset  $R$  of  $A \times B$ . We read  $(a, b) \in R$  as  $a$  is related to  $b$  and write  $a R b$ .

**Definition** A relation on a set  $A$  is a subset  $R$  of  $A \times A$ .

**Example** bignees relation  $R$  on a  $R$

$$R = \{ (a, b) \mid a > b \text{ and } a, b \in R \}$$

$$">" = \{ (a, b) \mid a, b \in R \}$$

$$a R b$$

$$a > b$$

# SECTION 0: SETS AND RELATIONS

---

Example Equality Relation = on a set  $X$

$$“=” = \{ (a, b) \mid a=b \} = \{ (x, x) \mid x \in X \}$$

$$a = b$$

# SECTION 0: SETS AND RELATIONS

---

**0.9 Example** The graph of the function  $f$  where  $f(x)=x^3$  for all  $x\in R$ , is the subset  $\{(x, x^3) | x^3 \in R\}$  of  $R\times R$ . It is a relation on  $R$ .

# SECTION 0: SETS AND RELATIONS

---

**0.10 Definition** A **function**  $\phi$  mapping  $X$  into  $Y$  is a relation between  $X$  and  $Y$  with the property that each  $x \in X$  appears as the first member of exactly one ordered pair  $(x, y)$ . Such a function is also called a map or mapping of  $X$  into  $Y$ . We write  $\phi: X \rightarrow Y$  and express  $(x, y) \in \phi$  by  $\phi(x)=y$ .

The **domain** of  $\phi$  is the set  $X$  and the set  $Y$  is the codomain of  $\phi$ .

The **range** of  $\phi$  is  $\phi[X]=\{\phi(x) \mid x \in X\}$ .

# SECTION 0: SETS AND RELATIONS

---

**0.11 Example** We can view the addition of real numbers as a function  $+: (R \times R) \rightarrow R$ , that is, as a mapping of  $R \times R$  into  $R$ .

$+ \text{ on } (2, 3) \in R \times R$

$+((2, 3)) = 5.$

$((2, 3), 5) \in +.$

$2+3=5.$

# SECTION 0: SETS AND RELATIONS

---

**0.11 Definition** The number of elements in a set  $X$  is the cardinality of  $X$  and is often denoted by  $|X|$ .

$$|\{2,5,7\}|=3. \quad |R|=?$$

**0.11 Definition** Two sets  $X$  and  $Y$  have the **same cardinality**, if there exist a pairing of each  $x$  in  $X$  with only one  $y$  in  $Y$  in such a way that each element of  $Y$  is also used only once in this pairing.

$$X=\{2,5,7\} \text{ and } Y=\{?,!,\#\}$$

$$2 \leftrightarrow ?, \quad 5 \leftrightarrow !, \quad 7 \leftrightarrow \# \qquad \{(2,?), (5,!), (7,\#)\}$$

# SECTION 0: SETS AND RELATIONS

---

Example Shows that the sets  $\mathbb{Z}$  and  $\mathbb{Z}^+$  have the same cardinality.

1    2    3    4    5    6    7    8    9    10

0    -1    1    -2    2    -3    3    -4    4    -5

$\mathbb{Z}$  and  $\mathbb{Z}^+$  have the same cardinality.



# SECTION 0: SETS AND RELATIONS

---

**0.12 Definition** A function  $\phi : X \rightarrow Y$  is **one to one (injection, 单射)**.  
if  $\phi(x_1) = \phi(x_2)$  only when  $x_1 = x_2$

The function  $\phi$  is **onto (surjective, 满射)**  $Y$  if the range of  $\phi$  is  $Y$ .

A map that is both **injective** and **surjective** is a **bijection (双射, 一一映射)**.

# SECTION 0: SETS AND RELATIONS

---

**0.12 Definition** If a subset of  $X \times Y$  is a one-to-one function  $\phi$  mapping  $X$  onto  $Y$ . If we interchange the first and second members of all ordered pairs  $(x, y)$  in  $\phi$  to obtain a set of ordered pairs  $(y, x)$ . we get a subset of  $Y \times X$ , which gives a one-to-one function mapping  $Y$  onto  $X$ . This function is called the **inverse function** of  $\phi$ , and is denoted by  $\phi^{-1}$ .

**Summarizing** If  $\phi$  maps  $X$  one to one onto  $Y$  and  $\phi(x) = y$ , then  $\phi^{-1}$  maps  $Y$  one to one onto  $X$ , and  $\phi^{-1}(y) = x$ .

# SECTION 0: SETS AND RELATIONS

---

**0.13 Definition** Two sets  $X$  and  $Y$  have the **same cardinality** if there exists a one-to-one function mapping  $X$  onto  $Y$ , that is, if there exists a one-to-one correspondence between  $X$  and  $Y$ .

$$|Z| = |Z^+| = \mathbf{N_0}$$

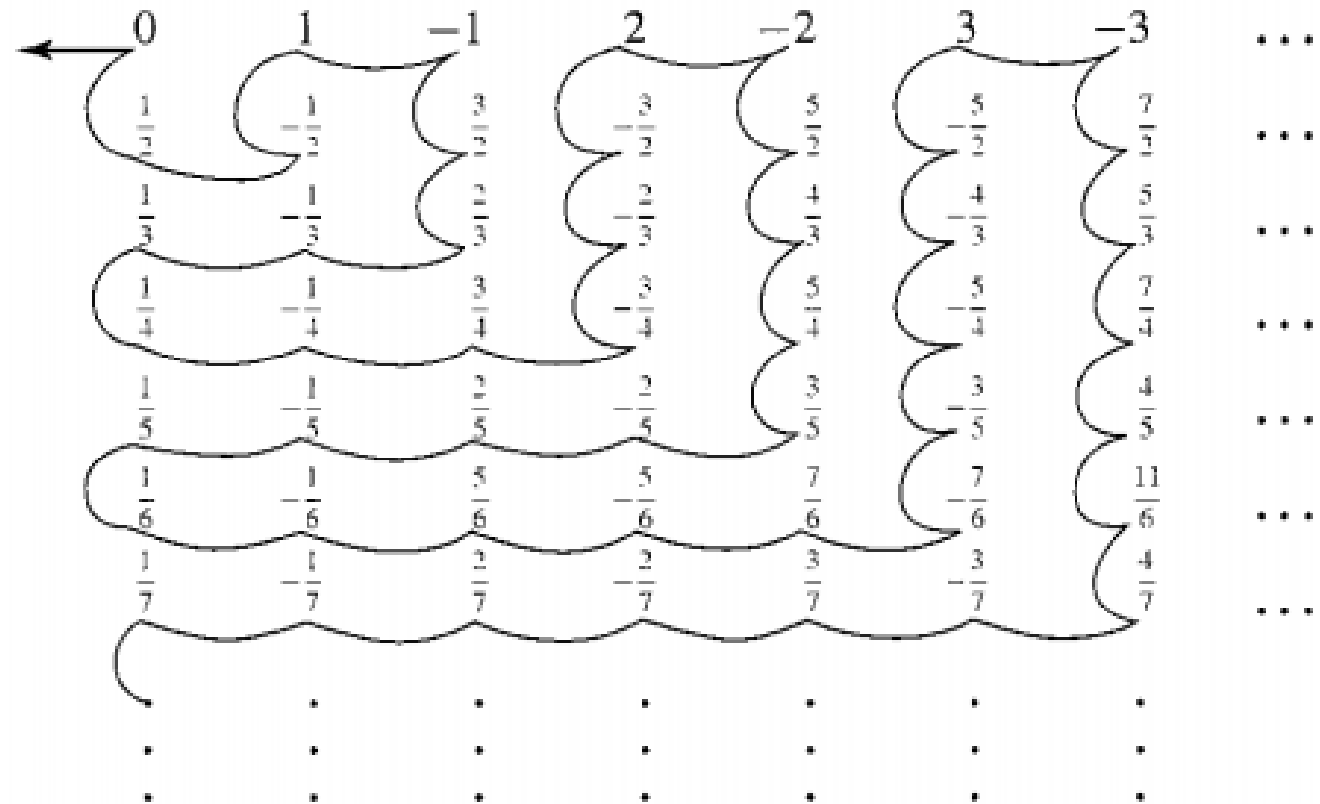
A set has cardinality  $\mathbf{N_0}$  if and only if all of its elements could be listed in an infinite row, so that we could "number them" using  $Z^+$ .

A set has cardinality  $\mathbf{N_0}$  if and only if all of its elements could be listed in an infinite row, so that we could "number them" using  $Z^+$ .

# SECTION 0: SETS AND RELATIONS

---

$$|Q| = N_0$$



# SECTION 0: SETS AND RELATIONS

---

$R$  has too many elements to be paired with those in  $\mathbb{Z}^+$ .

We just denote the cardinality of  $R$  by  $|R|$ .

There are infinitely many different cardinal numbers even greater than  $|R|$ .

# SECTION 0: SETS AND RELATIONS

---

**Definition** Sets are **disjoint** if no two of them have any element in common.

**0.16 Definition** A **partition**(分划, 划分) of a set  $S$  is a collection of nonempty subsets of  $S$  such that every element of  $S$  is in exactly one of the subsets. The subsets are the **cells** of the partition.

we denote by  $\bar{x}$  the cell containing the element  $x$  of  $S$ .

# SECTION 0: SETS AND RELATIONS

---

0.17 Example Splitting  $\mathbb{Z}^+$  into the subset of even positive integers and the subset of odd positive integers

$$\overline{1} = \{1, 3, 5, 7, \dots\}$$

$$\overline{14} = \{2, 3, 4, 6, \dots\}$$

# SECTION 0: SETS AND RELATIONS

---

**Example** We could also partition  $\mathbb{Z}^+$  into three cells. one consisting of the positive integers divisible by 3. Another containing all positive integers leaving a remainder of 1 when divided by 3. The last containing positive integers leaving a remainder of 2 when divided by 3.

$$\overline{3} = \{3, 6, 9, \dots\}$$

$$\overline{4} = \{1, 4, 7, 10, \dots\}$$

$$\overline{2} = \{2, 5, 8, 11, \dots\}$$



# SECTION 0: SETS AND RELATIONS

---

**0.18 Definition** An equivalence relation  $R$  on a set  $S$  is one that satisfies these three properties for all  $x, y, z \in S$ .

- 1.(Reflexive)(自反性)  $xRx$ .
- 2.(Symmetric)(对称性) If  $xRy$ , then  $yRx$ .
- 3.(Transitive)(传递性) If  $xRy$  and  $yRz$  then  $xRz$ .

# SECTION 0: SETS AND RELATIONS

---

0.19 Example For any nonempty set  $S$ , the equality relation  $=$  defined by the subset  $\{(x,x) \mid x \in S\}$  of  $S \times S$  is an equivalence relation.

# SECTION 0: SETS AND RELATIONS

---

**0.20 Example** (Congruence Modulo  $n$ ) Let  $n \in \mathbb{Z}^+$ . The equivalence relation on  $\mathbb{Z}^+$  corresponding to the partition of  $\mathbb{Z}^+$  into residue classes modulo  $n$ , discussed in Example 0.17, is congruence modulo  $n$ .

It is sometimes denoted by  $\equiv_n$ . Rather than write  $a \equiv_n b$ , we usually write  $a \equiv b \pmod{n}$ , read, "a is congruent to b modulo n."

$$15 \equiv 27 \pmod{4}$$

# SECTION 0: SETS AND RELATIONS

---

0.21 Example Let a relation  $R$  on the set  $Z$  be defined by  $nRm$  if and only if  $nm \geq 0$ . Is  $R$  an equivalence relation?

# SECTION 0: SETS AND RELATIONS

---

# SECTION 0: SETS AND RELATIONS

---

# SECTION 0: SETS AND RELATIONS

---



# Abstract Algebra

---



# SECTION 1–2: BINARY OPERATIONS

---

**2.1 Definition:** A binary operation  $*$  on a set  $S$  is a function mapping  $S \times S$  into  $S$ . For each  $(a, b) \in S \times S$ , we will denote the element  $*((a, b))$  of  $S$  by  $a * b$ .

**2.2 Example** Our usual addition  $+$  is a binary operation on the set  $\mathbb{R}$ . Our usual multiplication  $\cdot$  is a different binary operation on  $\mathbb{R}$ .

**Note** We require a binary operation on a set  $S$  to be defined for every ordered pair  $(a, b)$  of elements from  $S$ .

# SECTION 1–2: BINARY OPERATIONS

---

**2.1 Definition:** A binary operation  $*$  on a set  $S$  is a function mapping  $S \times S$  into  $S$ . For each  $(a, b) \in S \times S$ , we will denote the element  $*$  $((a, b))$  of  $S$  by  $a * b$ .

**2.3** Let  $M(R)$  be the set of all matrices with real entries. The usual matrix addition  $+$  is not a binary operation on this set since  $A+B$  is not defined for an ordered pair  $(A, B)$  of matrices having different numbers of rows or of columns.

**tip** Let  $M_n(R)$  be the set of all matrices of type  $n \times n$  with real entries. The usual matrix addition  $+$  is a binary operation.

# SECTION 1–2: BINARY OPERATIONS

---

**2.1 Definition:** Let  $*$  be a binary operation on  $S$  and let  $H$  be a subset of  $S$ . The subset  $H$  is **closed(封闭)** under  $*$  if for all  $a, b \in H$  we also have  $a*b \in H$ . In this case, the binary operation on  $H$  given by restricting  $*$  to  $H$  is the **induced operation** of  $*$  on  $H$ .

**Tip** By our very definition of a binary operation  $*$  on  $S$ , the set  $S$  is closed under  $*$

**2.5 Example** Our usual addition  $+$  on the set  $R$  of real numbers does not induce a binary operation on the set  $R^*$  of nonzero real numbers

$$2 + (-2) = 0$$

# SECTION 1-2: BINARY OPERATIONS

---

**2.1 Definition:** Let  $*$  be a binary operation on  $S$  and let  $H$  be a subset of  $S$ . The subset  $H$  is **closed(封闭)** under  $*$  if for all  $a, b \in H$  we also have  $a*b \in H$ . In this case, the binary operation on  $H$  given by restricting  $*$  to  $H$  is the **induced operation** of  $*$  on  $H$ .

**2.6 Example** Let  $+$  and  $\cdot$  be the usual binary operations of addition and multiplication on the set  $Z$ , and let  $H = \{n^2 \mid n \in Z^+\}$ . Determine whether  $H$  is closed under (a) addition and (b) multiplication.

# SECTION 1-2: BINARY OPERATIONS

---

**2.7 Example** Let  $F$  be the set of all **real-valued functions**  $f$  having as domain the set  $R$  of real numbers. We are familiar from calculus with the binary operations  $+$ ,  $-$ ,  $\cdot$  and  $\circ$  on  $F$ .

Namely, for each ordered pair  $(f,g)$  of functions in  $F$ , we define for each  $x \in H$

$f + g$  by  $(f+g)(x) = f(x) + g(x)$  **addition**,  
 $f - g$  by  $(f-g)(x) = f(x) - g(x)$  **subtraction**,  
 $f \cdot g$  by  $(f \cdot g)(x) = f(x)g(x)$  **multiplication**,  
 $f \circ g$  by  $(f \circ g)(x) = f(g(x))$  **composition**.

# SECTION 1-2: BINARY OPERATIONS

---

**2.8 Example** On  $Z^+$ , we define a binary operation  $*$  by  $a*b$  equals the smaller of  $a$  and  $b$ , or the common value if  $a=b$ .

$$2*11=2; \quad 15*10=10; \quad \text{and} \quad 3*3=3.$$

# SECTION 1-2: BINARY OPERATIONS

---

**2.10 Example** On  $\mathbb{Z}^+$ , we define a binary operation  $*$  by  $a * b = (a * b) + 2$ , where  $*$  is defined in Example 2.8.

$$4 * 7 =$$

$$25 * 9 =$$

$$6 * 6 =$$

# SECTION 1-2: BINARY OPERATIONS

---

2.9 Example On  $\mathbb{Z}^+$ , we define a binary operation  $*$ ' by  $a *' b = a$ .

$$2 *' 3 = 2$$

$$25 *' 10 = 25$$

$$5 *' 5 = 5$$



# SECTION 1–2: BINARY OPERATIONS

---

**2.11 Definition** A binary operation  $*$  on a set  $S$  is **commutative** if (and only if)  $a*b=b*a$  for all  $a,b \in S$ .

Are  $*$ ,  $*$ ' and  $*$ " commutative?

# SECTION 1-2: BINARY OPERATIONS

---

**2.11 Definition** A binary operation on a set  $S$  is **associative** if  $(a*b)*c=a*(b*c)$  for all  $a, b, c \in S$ .

Are  $*$ ,  $*$ ' and  $*$ " associative?

# SECTION 1-2: BINARY OPERATIONS

---

2.13 Theorem (Associativity of Composition) Let  $S$  be a set and let  $f, g$ , and  $h$  be functions mapping  $S$  into  $S$ . Then  $f \circ (g \circ h) = (f \circ g) \circ h$ .

# SECTION 1-2: BINARY OPERATIONS

---

2.14 Example Table 2.15 defines the binary operation  $*$  on  $S = \{a, b, c\}$  by the following rule:

**2.15 Table**

$*$	$a$	$b$	$c$
$a$	$b$	$c$	$b$
$b$	$a$	$c$	$b$
$c$	$c$	$b$	$a$

( $i$ th entry on the left)  $*$  ( $j$ th entry on the top)  
= (entry in the  $i$ th row and  $j$ th column of the table body)

# SECTION 1-2: BINARY OPERATIONS

---

2.16 Example Complete Table 2.17 so that  $*$  is a commutative binary operation on the set  $S=\{a,b,c,d\}$ .

**2.17 Table**

$*$	$a$	$b$	$c$	$d$
$a$	$b$			
$b$	$d$	$a$		
$c$	$a$	$c$	$d$	
$d$	$a$	$b$	$b$	$c$

# SECTION 1–2: BINARY OPERATIONS

---

1. Exactly **one** element is assigned to **each** possible ordered pair of elements of  $S$ ,
2. For each ordered pair of elements of  $S$ , the element assigned to it is **again** in

# SECTION 1-2: BINARY OPERATIONS

---

1. Exactly **one** element is assigned to **each** possible ordered pair of elements of  $S$ ,
2. For each ordered pair of elements of  $S$ , the element assigned to it is **again** in

**2.19 Example** On  $Q$ , let  $a*b = a/b$ . Here  $*$  is not everywhere defined on  $Q$ , for no rational number is assigned by this rule to the pair  $(2, 0)$ .

# SECTION 1–2: BINARY OPERATIONS

---

1. Exactly **one** element is assigned to **each** possible ordered pair of elements of  $S$ ,
2. For each ordered pair of elements of  $S$ , the element assigned to it is **again** in

**2.20 Example** On  $Q^+$ , let  $a*b=a/b$ . Here both Conditions 1 and 2 are satisfied, and  $*$  is a binary operation on  $Q^+$ .



# SECTION 1–2: BINARY OPERATIONS

---

1. Exactly **one** element is assigned to **each** possible ordered pair of elements of  $S$ ,
2. For each ordered pair of elements of  $S$ , the element assigned to it is **again** in

**2.21 Example** On  $Z^+$ , let  $a*b=a/b$ . Here both Conditions 1 and 2 are satisfied, and  $*$  is a binary operation on  $Z^+$ .

# SECTION 1–2: BINARY OPERATIONS

---

1. Exactly **one** element is assigned to **each** possible ordered pair of elements of  $S$ ,
2. For each ordered pair of elements of  $S$ , the element assigned to it is **again** in

**2.22 Example** Let  $F$  be the set of all real-valued functions with domain  $R$  as in Example 2.7. Suppose we define  $*$  to give the usual quotient of  $f$  by  $g$ , that is,  $f * g = h$ , where  $h(x) = f(x)/g(x)$ .

# SECTION 1–2: BINARY OPERATIONS

---

1. Exactly **one** element is assigned to **each** possible ordered pair of elements of  $S$ ,
2. For each ordered pair of elements of  $S$ , the element assigned to it is **again** in

**2.23 Example** Let  $F$  be the set of all real-valued functions with domain  $R$  as in Example 2.7. Suppose we define  $*$  to give the usual quotient of  $f$  by  $g$ , that is,  $f * g = h$ , where  $h(x) = f(x)/g(x)$ .



# Abstract Algebra

---

# SECTION 1-3: ISOMORPHIC BINARY STRUCTURES

---

**3.7 Definition:** Let  $(S, *)$  and  $(S', *')$  be binary algebraic structures. An isomorphism of  $S$  with  $S'$  is a one-to-one function  $\phi$  mapping  $S$  onto  $S'$  such that  $\phi(x * y) = \phi(x) *' \phi(y)$  for all  $x, y \in S$ .

If such a map  $\phi$  exists, then  $S$  and  $S'$  are **isomorphic binary structures**, which we denote by  $S \cong S'$ , omitting the  $*$  and  $*'$  from the notation.

# SECTION 1-3: ISOMORPHIC BINARY STRUCTURES

---

**Question** How to Show That Binary Structures Are Isomorphic

Step 1 **Define the function**  $\phi$  that gives the isomorphism of  $S$  with  $S'$ .

Step 2 Show that  $\phi$  is a **one-to-one function (injective)** (单设).

Step 3 Show that  $\phi$  is **onto (surjective)** (满射)  $S'$ .

Step 4 Show that  $\phi(x * y) = \phi(x) *' \phi(y)$

# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**3.8 Example** Let us show that the binary structure  $(\mathbb{R}, +)$  with operation the usual addition is isomorphic to the structure  $(\mathbb{R}^+, \cdot)$  where  $\cdot$  is the usual multiplication.

# SECTION 1-3: ISOMORPHIC BINARY STRUCTURES

---

**3.9 Example** Let  $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ , so that  $2\mathbb{Z}$  is the set of all even integers, positive, negative, and zero. We claim that  $(\mathbb{Z}, +)$  is isomorphic to  $(2\mathbb{Z}, +)$ , where  $+$  is the usual addition.



# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**Question** How to Show That Binary Structures Are Not Isomorphic

# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**3.10 Example** Example The binary structures  $(Q, +)$  and  $(R, +)$  are not isomorphic because  $Q$  has cardinality  $\aleph_0$  while  $|R| \neq \aleph_0$ .

# SECTION 1-3: ISOMORPHIC BINARY STRUCTURES

---

**3.11 Example** The sets  $Z$  and  $Z^+$  both have cardinality  $\aleph_0$ , and there are lots of one-to-one functions mapping  $Z$  and  $Z^+$ . However, the binary structures  $(Z, \cdot)$  and  $(Z^+, \cdot)$ , where  $\cdot$  is the usual multiplication, are not isomorphic.

In  $(Z, \cdot)$  there are two elements  $x$  such that  $x \cdot x = x$ , namely, 0 and 1. However, in  $(Z^+, \cdot)$ , there is only the single element 1.

# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**3.15 Example** We show that the binary structures  $(\mathbb{Q}, +)$  and  $(\mathbb{Z}, +)$  under the usual addition are not isomorphic.

The equation  $x+x=c$  has a solution  $x$  for all  $c \in \mathbb{Q}$ , but this is not the case in  $\mathbb{Z}$ . For example, the equation  $x+x=3$  has no solution in  $\mathbb{Z}$ .

# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**3.16 Example** The binary structures  $(C, \cdot)$  and  $(R, \cdot)$  under the usual multiplication are not isomorphic.

The equation  $x \cdot x = c$  has a solution  $x$  for all  $c \in C$ , but  $x \cdot x = -1$  has no solution in  $R$ .

A

# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**3.17 Example** The binary structure  $\langle M_2(R), \cdot \rangle$  of  $2 \times 2$  real matrices with the usual matrix multiplication is not isomorphic to  $(R, \cdot)$  with the usual number multiplication.

Multiplication of numbers is commutative, but multiplication of matrices is not.

# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**3.12 Definition** Let  $(S, *)$  be a binary structure. An element  $e$  of  $S$  is an **identity element**(单位元) for  $*$  if

$$e*s = s*e = s \text{ for all } s \in S.$$

**3.13 Theorem (Uniqueness of Identity Element)** A binary structure  $(S, *)$  has at most one identity element.

# SECTION 1–3: ISOMORPHIC BINARY STRUCTURES

---

**3.14 Theorem** Suppose  $(S, *)$  has an identity element  $e$  for  $*$ . If  $\phi : S \rightarrow S'$  is an isomorphism of  $(S, *)$  with  $(S', *')$ , then  $\phi(e)$  is an identity element for the binary operation  $*$ ' on  $S'$ .





# Abstract Algebra

---

# SECTION 4: GROUPS

---

Example:

$$(5 + x) = 2$$

$$-5 + (5 + x) = -5 + 2, \quad \text{adding } -5$$

$$(-5 + 5) + x = -5 + 2, \quad \text{associative law}$$

$$0 + x = -5 + 2, \quad \text{computing } -5 + 5$$

$$x = -5 + 2, \quad 0 \text{ is the identity element}$$

$$x = -3, \quad \text{computing } -5 + 2$$

# SECTION 4: GROUPS

---

**4.1 Definition** A **group**( $G, *$ )(群) is a set  $G$ , closed under a binary operation  $*$ , such that the following axioms are satisfied:

**R1:** For all  $a, b, c \in G$ , we have

$$(a*b)*c = a*(b*c) \quad \text{associativity(结合律) of } *$$

**R2:** There is an element  $e$  in  $G$  such that for all  $x \in G$ ,

$$e*x = x*e = x. \quad \text{identity element(单位元) } e \text{ for } *$$

**R3:** Corresponding to each  $a \in G$ , there is an element  $a'$  in  $G$  such that  $a*a' = a'*a = e$ . **inverse(逆元)**  $a'$  of  $a$ .

# SECTION 4: GROUPS

---

4.4 Example The set  $\mathbb{Z}^+$  under addition is not a group.

There is no identity element for  $+$  in  $\mathbb{Z}^+$ .

# SECTION 4: GROUPS

---

4.5 Example The set of all nonnegative integers (including 0) under addition is still not a group.

There is an identity element 0.

But it has no inverse for 2.

# SECTION 4: GROUPS

---

**4.6 Example** The familiar additive properties of integers and of rational, real, and complex numbers show that  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$  under addition are abelian groups.

**4.3 Definition** A group  $G$  is **abelian**(阿贝尔, 交换) if its binary operation is **commutative**.

# SECTION 4: GROUPS

---

4.7 Example The set  $\mathbb{Z}^+$  under multiplication is not a group.

There is an identity 1, but no inverse of 3.

# SECTION 4: GROUPS

---



# SECTION 4: GROUPS

---

4.9 Example. The set of all real-valued functions with domain  $\mathbb{R}$  under function addition is a group. This group is abelian.

# SECTION 4: GROUPS

---

4.10 Example. (Linear Algebra) Those who have studied vector spaces should note that the axioms for a vector space  $V$  pertaining just to vector addition can be summarized by asserting that  $V$  under vector addition is an abelian group.

# SECTION 4: GROUPS

---

**4.11 Example.** The set  $M_{m \times n}(R)$  of all  $m \times n$  matrices under matrix addition is a group.

The  $m \times n$  matrix with all entries 0 is the identity matrix. This group is abelian.

# SECTION 4: GROUPS

---

**4.12 Example.** The set  $M_n(R)$  of all  $n \times n$  matrices under matrix multiplication is not a group.

The  $n \times n$  matrix with all entries 0 has no inverse.

**4.13 Example.** Show that the subset  $S$  of  $M_n(R)$  consisting of all invertible  $n \times n$  matrices under matrix multiplication is a group.

# SECTION 4: GROUPS

---

4.14 Example. Let  $*$  be defined on  $Q^+$  by  $a*b=ab/2$ .

# SECTION 4: GROUPS

---

**4.15 Theorem** If  $G$  is a group with binary operation  $*$ , then the left and right cancellation laws hold in  $G$ , that is,  $a*b=a*c$  implies  $b=c$ , and  $b*a=c*a$  implies  $b=c$  for all  $a, b, c \in G$ .

# SECTION 4: GROUPS

---

**4.16 Theorem** If  $G$  is a group with binary operation  $*$ , and if  $a$  and  $b$  are any elements of  $G$ , then the linear equations  $a*x=b$  and  $y*a=b$  have unique solutions  $x$  and  $y$  in  $G$ .

# SECTION 4: GROUPS

---

**4.17 Theorem** In a group  $G$  with binary operation  $*$ , there is only one element  $e$  in  $G$  such that  $e*x=x*e=x$

for all  $x \in G$ . Likewise for each  $a \in G$ , there is only one element  $a'$  in  $G$  such that  $a' * a = a * a' = e$ .

The identity element and inverse of each element are unique in a group.

**4.18 Corollary** Let  $G$  be a group. For all  $a, b \in G$ , we have

$$(a * b)' = b' * a'.$$



# SECTION 4: GROUPS

---

## 4.17 Finite groups:

A minimal set that might give rise to a group is a one-element set  $\{e\}$ . The only possible binary operation  $*$  on  $\{e\}$  is defined by  $e*e=e$ .

# SECTION 4: GROUPS

---

**Question:** Is there a group structure on a set of two elements.

$*$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

$Z_2 = \{0,1\}$  under addition modulo 2  
is a group

# SECTION 4: GROUPS

---

**Question:** Is there a group structure on a set of three elements.

*	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

$Z_3 = \{0,1,2\}$  under addition modulo 3  
is a group

There is only one group of three elements,  
**up to isomorphism.**



# Abstract Algebra

---

# SECTION 5: SUBGROUPS

---

## Notation and Terminology:

For  $a*b$ ,

denoted it by  $a+b$  if  $*$  is commutative

$ab$  if  $*$  is not commutative or not determinate

For identity element  $e$ ,

denoted  $0$  if  $*$  is commutative

denoted  $1$  if  $*$  is not commutative or not determinate

# SECTION 5: SUBGROUPS

---

## Notation and Terminology:

For identity element  $e$ ,

denoted  $0$  if  $*$  is commutative

denoted  $1$  if  $*$  is not commutative or not determinate

$*$	$1$	$a$	$b$
$1$	$1$	$a$	$b$
$a$	$a$	$b$	$1$
$b$	$b$	$1$	$a$

# SECTION 5: SUBGROUPS

---

## Notation and Terminology:

For identity element  $e$ ,

denoted  $0$  if  $*$  is commutative

denoted  $1$  if  $*$  is not commutative or not determinate

$*$	$0$	$a$	$b$
$0$	$0$	$a$	$b$
$a$	$a$	$b$	$0$
$b$	$b$	$0$	$a$

# SECTION 5: SUBGROUPS

---

## Notation and Terminology:

For inverse of an element  $a$ ,

$-a$  in additive notation.

$a^{-1}$  in multiplicative notation

For identity element  $e$ ,

denoted  $0$  if  $*$  is commutative

denoted  $1$  if  $*$  is not commutative or not determinate



# SECTION 5: SUBGROUPS

---

## Notation and Terminology:

In multiplicative notation

denote the product  $aaa...a$  for  $n$  factors  $a$  by  $a^n$

denote the product  $a^{-1}a^{-1}a^{-1}...a^{-1}$  for  $n$  factors  $-a$  by  $a^{-n}$

In additive notation

denoted  $a+a+a+...+a$  for  $n$  summands by  $na$

denoted  $(-a)+(-a)+(-)+...+(-a)$  for  $n$  summands by  $-na$

# SECTION 5: SUBGROUPS

---

**5.3 Definition** If  $G$  is a group, then the order  $|G|$  of  $G$  is the number of elements in  $G$ .

# SECTION 5: SUBGROUPS

---

**5.4 Definition** If a subset  $H$  of a group  $G$  is closed under the binary operation of  $G$  and if  $H$  with the induced operation from  $G$  is itself a group, then  $H$  is a **subgroup (子群)** of  $G$ . We shall let  $H \leq G$  or  $G \geq H$  denote that  $H$  is a subgroup of  $G$ , and  $H < G$  or  $G > H$  shall mean  $H \leq G$  but  $H \neq G$ .

Thus  $(\mathbb{Z}, +) < (\mathbb{Q}, +)$

$(\mathbb{Q}, +)$  is not a subgroup of  $(\mathbb{R}, \cdot)$

# SECTION 5: SUBGROUPS

---

**5.5 Definition** If  $G$  is a group, then the subgroup consisting of  $G$  itself is the **improper subgroup** of  $G$ . All other subgroups are **proper subgroups**. The subgroup  $\{e\}$  is the trivial **subgroup** (平凡子群) of  $G$ . All other subgroups are nontrivial.

# SECTION 5: SUBGROUPS

---

**5.6 Example** Let  $R^n$  be the additive group of all  $n$ -component row vectors with real number entries.

The subset consisting of all of these vectors having 0 as entry in the first component is a subgroup of  $R^n$ .

$$R^n = \{(x_1, x_2, \dots, x_n) | x_1, x_2, \dots, x_n \in R\}$$

$$H = \{(0, x_2, \dots, x_n) | x_2, \dots, x_n \in R\}$$

# SECTION 5: SUBGROUPS

---

**5.13 Example**  $\mathcal{Q}^+$  under multiplication is a proper subgroup of  $\mathcal{R}^+$  under multiplication.

**5.8 Example** The  $n$ th roots of unity in  $\mathcal{C}$  form a subgroup  $U_n$  of the group  $\mathcal{C}^*$  of nonzero complex numbers under multiplication.

# SECTION 5: SUBGROUPS

---

**5.7 Example** There are two different types of group structures of order 4

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$V$ :  
Klein 4-group

*	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

# SECTION 5: SUBGROUPS

---

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The only nontrivial proper subgroup of  $\mathbb{Z}_4$  is  $\{0, 2\}$ .

$$\begin{array}{c} \mathbb{Z}_4 \\ | \\ \{0, 2\} \\ | \\ \{0\} \end{array}$$



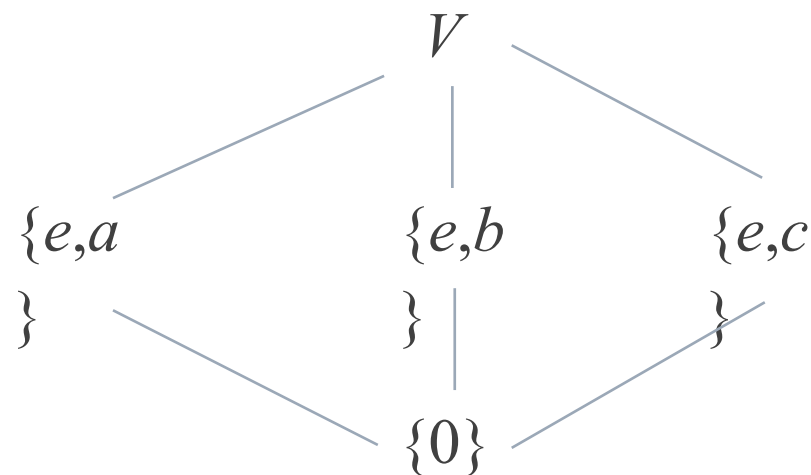
# SECTION 5: SUBGROUPS

---

$V$ :  
Klein 4-group

$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

$V$  has three nontrivial proper subgroups



# SECTION 5: SUBGROUPS

---

**5.13 Example** Let  $F$  be the group of all real-valued functions with domain  $R$  under addition. The subset of  $F$  consisting of those functions that are **continuous** is a subgroup of  $F$ .

# SECTION 5: SUBGROUPS

---

**5.14 Theorem** A subset  $H$  of a group  $G$  is a subgroup of  $G$  if and only if

1.  $H$  is closed under the binary operation of  $G$ ,
2. the identity element  $e$  of  $G$  is in  $H$ ,
3. for all  $a \in H$  it is true that  $a^{-1} \in H$  also.

# SECTION 5: SUBGROUPS

---

4.12 Example The set  $M_n(R)$  of all  $n \times n$  matrices under matrix multiplication is not a group.

4.13 Example Show that the subset  $S$  of  $M_n(R)$  consisting of all invertible  $n \times n$  matrices under matrix multiplication is a group.

5.16 Example Let  $T$  be the subset of  $G$  consisting of those matrices with determinant 1.

# SECTION 5: SUBGROUPS

---

5.17 Theorem Let  $G$  be a group and let  $a \in G$ . Then

$H = \{a^n \mid n \in \mathbb{Z}\}$  is a subgroup of  $G$  and is the smallest subgroup of  $G$  that contains  $a$ , that is, every subgroup containing  $a$  contains  $H$ .

# SECTION 5: SUBGROUPS

---

**5.17 Theorem** Let  $G$  be a group and let  $a \in G$ . Then

$H = \{a^n \mid n \in \mathbb{Z}\}$  is a subgroup of  $G$  and is the smallest subgroup of  $G$  that contains  $a$ , that is, every subgroup containing  $a$  contains  $H$ .

**5.18 Definition** Let  $G$  be a group and let  $a \in G$ . Then the subgroup  $\{a^n \mid n \in \mathbb{Z}\}$  of  $G$ , characterized in Theorem 5.17, is called the **cyclic subgroup (循环群)** of  $G$  **generated (生成)** by  $a$ , and denoted by  $\langle a \rangle$ .

# SECTION 5: SUBGROUPS

---

5.19 Definition An element  $a$  of a group  $G$  generates (生成)  $G$  and is a generator (生成元) for  $G$  if  $\langle a \rangle = G$ . A group  $G$  is cyclic if there is some element  $a$  in  $G$  that generates  $G$ .

## SECTION 5: SUBGROUPS

---

**5.20 Example** Let  $Z_4$  and  $V$  be the groups of Example 5.9. Then  $Z_4$  is cyclic and both 1 and 3 are generators, that is,  $\langle 1 \rangle = \langle 3 \rangle = Z_4$ . However,  $V$  is not cyclic, for  $\langle a \rangle$ ,  $\langle b \rangle$ , and  $\langle c \rangle$  are proper subgroups of two elements.



## SECTION 5: SUBGROUPS

---

**5.20 Example** Let  $Z_4$  and  $V$  be the groups of Example 5.9. Then  $Z_4$  is cyclic and both 1 and 3 are generators, that is,  $\langle 1 \rangle = \langle 3 \rangle = Z_4$ . However,  $V$  is not cyclic, for  $\langle a \rangle$ ,  $\langle b \rangle$ , and  $\langle c \rangle$  are proper subgroups of two elements.

$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

# SECTION 5: SUBGROUPS

---

**5.21 Example** The group  $\mathbb{Z}$  under addition is a cyclic group. Both 1 and  $-1$  are generators for this group, and they are the only generators. Also, for  $n \in \mathbb{Z}^+$ , the group  $\mathbb{Z}$ , under addition modulo  $n$  is cyclic. If  $n > 1$ , then both 1 and  $n-1$  are generators, but there may be others.

# SECTION 5: SUBGROUPS

---

**5.22 Example** Consider the group  $\mathbb{Z}$  under addition. Let us find  $\langle 3 \rangle$ . Here the notation is additive, and  $\langle 3 \rangle$  must contain

$$3, \quad 3+3=6, \quad 3+3+3=9, \quad 3+3+3+3=12, \quad \dots$$

$$0, \quad -3, \quad -6, \quad -9, \quad -12, \quad \dots$$

In other words, the cyclic subgroup generated by 3 consists of all multiples of 3, positive, negative, and zero. We denote this subgroup by  $3\mathbb{Z}$  as well as  $\langle 3 \rangle$ . In a similar way, we shall let  $n\mathbb{Z}$  be the cyclic subgroup  $\langle n \rangle$  of  $\mathbb{Z}$ . Note that  $6\mathbb{Z} \subset 3\mathbb{Z}$ .



# Abstract Algebra

---

# SECTION 6: CYCLIC GROUPS

---

**5.17 Theorem** Let  $G$  be a group and let  $a \in G$ . Then

$H = \{a^n \mid n \in \mathbb{Z}\}$  is a subgroup of  $G$  and is the smallest subgroup of  $G$  that contains  $a$ , that is, every subgroup containing  $a$  contains  $H$ .

**5.18 Definition** Let  $G$  be a group and let  $a \in G$ . Then the subgroup  $\{a^n \mid n \in \mathbb{Z}\}$  of  $G$ , characterized in Theorem 5.17, is called the **cyclic subgroup (循环群)** of  $G$  **generated (生成)** by  $a$ , and denoted by  $\langle a \rangle$ .

# SECTION 6: CYCLIC GROUPS

---

5.19 Definition An element  $a$  of a group  $G$  generates (生成)  $G$  and is a generator (生成元) for  $G$  if  $\langle a \rangle = G$ . A group  $G$  is cyclic if there is some element  $a$  in  $G$  that generates  $G$ .

# SECTION 6: CYCLIC GROUPS

---

6.1 Theorem Every cyclic group is abelian.

# SECTION 6: CYCLIC GROUPS

---

**Division Algorithm for  $\mathbb{Z}$**  If  $m$  is a positive integer and  $n$  is any integer, then there exist unique integers  $q$  and  $r$  such that.

$$n = mq + r$$



# SECTION 6: CYCLIC GROUPS

---

**6.4 Example** Find the quotient  $g$  and remainder  $r$  when 38 is divided by 7 according to the division

$$38=35+3=7(5)+3$$

# SECTION 6: CYCLIC GROUPS

---

**6.5 Example** Find the quotient  $g$  and remainder  $r$  when  $-38$  is divided by  $7$  according to the division algorithm.

$$38 = -42 + 4 = 7(-6) + 4$$

# SECTION 6: CYCLIC GROUPS

---

**6.6 Theorem** A subgroup of a cyclic group is cyclic.

# SECTION 6: CYCLIC GROUPS

---

**6.7 Corollary** The subgroups of  $\mathbb{Z}$  under addition are precisely the groups  $n\mathbb{Z}$  under addition for  $n \in \mathbb{Z}$ .

# SECTION 6: CYCLIC GROUPS

---

**6.8 Definition** Let  $r$  and  $s$  be two positive integers. The positive generator  $d$  of the cyclic group  $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$  under addition is the **greatest common divisor** (abbreviated **gcd**, 最大公约数) of  $r$  and  $s$ . We write  $d = \gcd(r, s)$ .

# SECTION 6: CYCLIC GROUPS

---

**6.9 Example** Find the gcd of 42 and 72.

# SECTION 6: CYCLIC GROUPS

---

**Definition** Two positive integers are **relatively prime** (互素) if their gcd is 1

# SECTION 6: CYCLIC GROUPS

---

**Result** If  $r$  and  $s$  are relatively prime and if  $r$  divides  $sm$ , then  $r$  must divide  $m$ .



# SECTION 6: CYCLIC GROUPS

---

**6.10 Theorem** Let  $G$  be a cyclic group with generator  $a$ . If the order of  $G$  is infinite, then  $G$  is isomorphic to  $\langle \mathbb{Z}, + \rangle$ . If  $G$  has finite order  $n$ , then  $G$  is isomorphic to  $\langle \mathbb{Z}_n, +_n \rangle$ .

# SECTION 6: CYCLIC GROUPS

---

**6.13 Example** Motivated by our work with  $U_n$ , it is nice to visualize the elements  $e = a^0, a^1, a^2, \dots, a^{n-1}$  of a cyclic group of order  $n$  as being distributed evenly on a circle (see Fig. 6.11).

# SECTION 6: CYCLIC GROUPS

---

**6.14 Theorem** Let  $G$  be a cyclic group with  $n$  elements and generated by  $a$ . Let  $b \in G$  and let  $b = a^s$ . Then  $b$  generates a cyclic subgroup  $H$  of  $G$  containing  $n/d$  elements, where  $d$  is the greatest common divisor of  $n$  and  $s$ . Also,  $\langle a^s \rangle = \langle a^t \rangle$  if and only if  $\gcd(s, n) = \gcd(t, n)$ .

# SECTION 6: CYCLIC GROUPS

---

**6.15 Example** For an example using additive notation, consider  $Z_{12}$ , with the generator  $a=1$ . Since the greatest common divisor of 3 and 12 is 3,  $3=3 \cdot 1$  generates a subgroup of  $12/3=4$  elements, namely

$$\langle 3 \rangle = \{0, 3, 6, 9\}$$

# SECTION 6: CYCLIC GROUPS

---

**6.16 Corollary** If  $a$  is a generator of a finite cyclic group  $G$  of order  $n$ , then the other generators of  $G$  are the elements of the form  $a^r$ , where  $r$  is relatively prime to  $n$ .

# SECTION 6: CYCLIC GROUPS

---

**6.17 Example** Let us find all subgroups of  $Z_{18}$  and give their subgroup diagram.



# Abstract Algebra

---

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

**5.17 Theorem** Let  $G$  be a group and let  $a \in G$ . Then

$H = \{a^n \mid n \in \mathbb{Z}\}$  is a subgroup of  $G$  and is the smallest subgroup of  $G$  that contains  $a$ , that is, every subgroup containing  $a$  contains  $H$ .

**5.18 Definition** Let  $G$  be a group and let  $a \in G$ . Then the subgroup  $\{a^n \mid n \in \mathbb{Z}\}$  of  $G$ , characterized in Theorem 5.17, is called the **cyclic subgroup (循环群)** of  $G$  **generated (生成)** by  $a$ , and denoted by  $\langle a \rangle$ .



# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

The smallest subgroup of  $G$  that contains both  $a$  and  $b$ .

$$a^2b^4a^{-3}b^2a^5$$

$$a^{-5}b^{-2}a^3b^{-4}a^{-2}$$

We call  $a$  and  $b$  **generators (生成元)** of this subgroup.

If this subgroup should be all of  $G$ , then we say that  $\{a,b\}$  **generates (生成)**  $G$ .

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

7.1 Example The Klein 4-group  $V=\{e,a,b,c\}$  of Example 5.9.

$V$  is generated by  $\{a,b\}$ .

$V$  is also generated by  $\{a,c\},\{b,c\},\{a,b,c\}$

$V$  is not generated by  $\{e,a\}$

$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

7.2 Example The group  $Z_6$ .

It is generated by  $\{1\}, \{5\}$ .

It is generated by  $\{2, 3\}$ .

It is also generated by  $\{3, 4\}, \{1, 3, 4\}, \{1, 3\}, \{3, 5\}$ .

But it is not generated by  $\{2, 4\}$ .

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

**7.3 Definition** Let  $\{S_i | i \in I\}$  be a collection of sets. Here  $I$  may be any set of indices. The intersection  $\bigcap_{i \in I} S_i$  of the sets  $S_i$  is the set of all elements that are in all the sets  $S_i$ , that is

$$\bigcap_{i \in I} S_i = \{x | x \in S_i \text{ for all } i \in I\}.$$

If  $I$  is finite,  $I = \{1, 2, \dots, n\}$ , we may denote  $\bigcap_{i \in I} S_i$  by  $S_1 \cap S_2 \dots \cap S_n$

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

**7.4 Theorem** The intersection of some subgroups  $H_i$  of a group  $G$  for  $i \in I$  is again a subgroup of  $G$ .

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

**7.5 Definition** Let  $G$  be a group and let  $a_i \in G$  for  $i \in I$ . The smallest subgroup of  $G$  containing  $\{a_i \mid i \in I\}$  is the subgroup **generated (生成)** by  $\{a_i \mid i \in I\}$ . If this subgroup is all of  $G$ , then  $\{a_i \mid i \in I\}$  generates  $G$  and the  $a_i$  are **generators (生成元)** of  $G$ . If there is a finite set  $\{a_i \mid i \in I\}$  that generates  $G$ , then  $G$  is **finitely generated (有限生成)**.

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

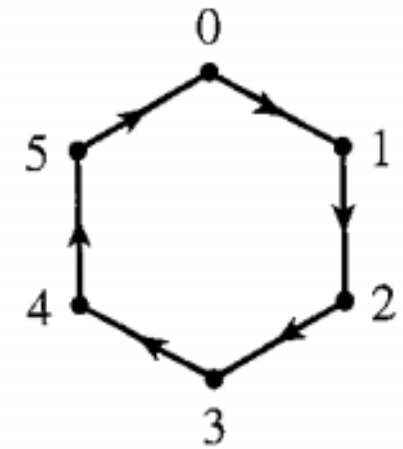
---

**7.6 Theorem** If  $G$  is a group and  $a_i \in I$  for  $i \in I$ , then the subgroup  $H$  of  $G$  generated by  $\{a_i \mid i \in I\}$  has as elements precisely those elements of  $G$  that are finite products of integral powers of the  $a_i$ , where powers of a fixed  $a_i$  may occur several times in the product.

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

Each element is represented by a dot,  
Each generator is represented by one type of arc.  
 $x \rightarrow y$  means that  $xa = y$ .

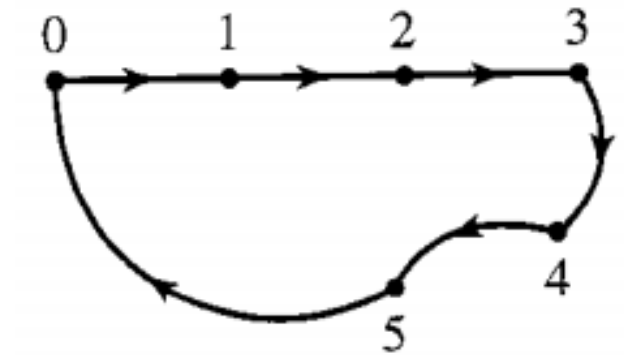


$\{1\}$  using  $\longrightarrow$



# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

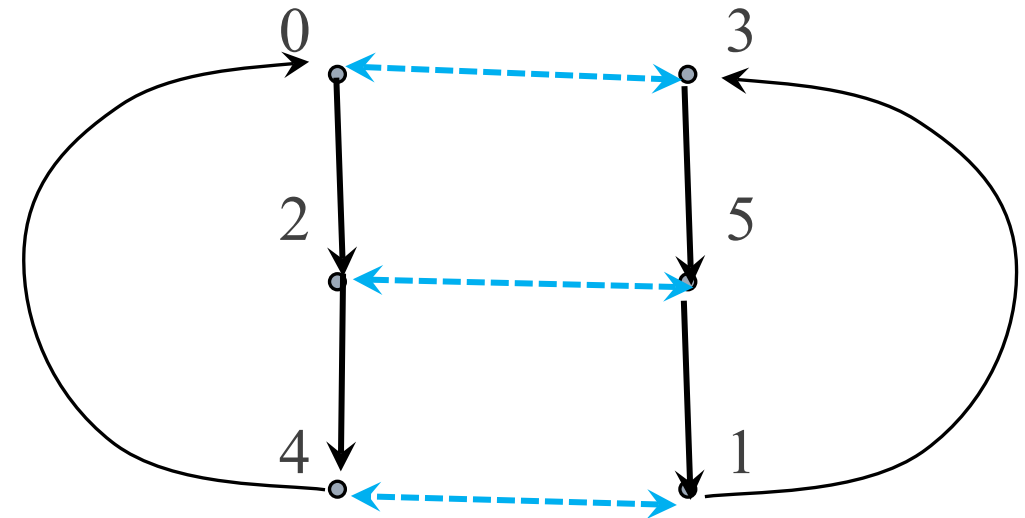
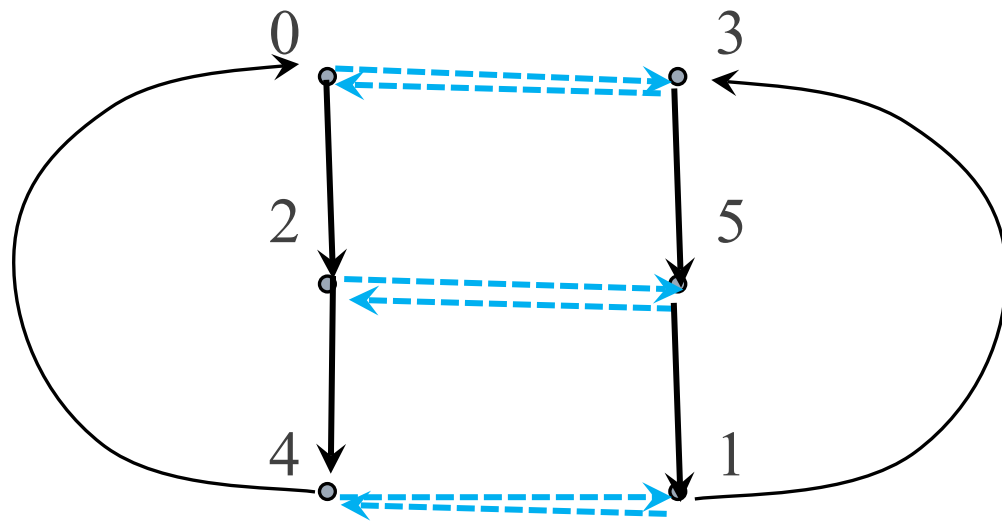
---



$\{1\}$  using  $\longrightarrow$

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

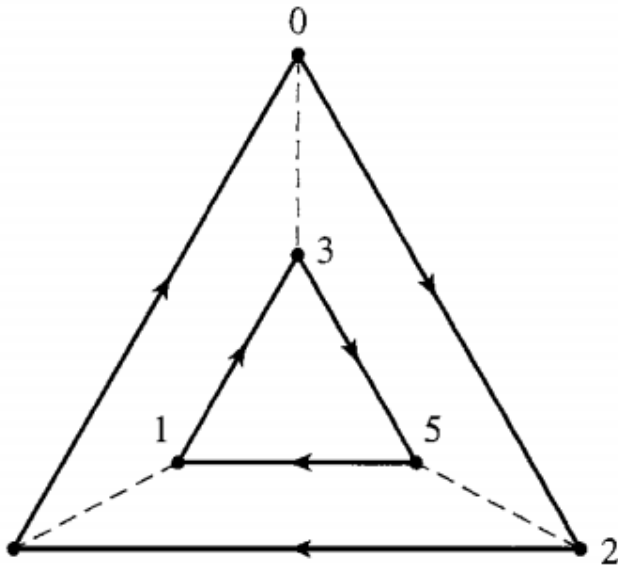
---



$\{2, 3\}$  using  $\longrightarrow$  and  $\dashrightarrow$

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---



$\{2,3\}$  using  $\longrightarrow$  and  $\dashrightarrow$

1. The digraph is connected.

$gx=h$  has a solution

2. At most one arc goes from a vertex  $g$  to a vertex  $h$ .

$ga=h$  and  $gb=h \Rightarrow a=b$

3. Each vertex  $g$  has exactly one arc of each type

4. sequences of arc from  $g$  to  $h$

$gq=h$  and  $gr=h \Rightarrow$

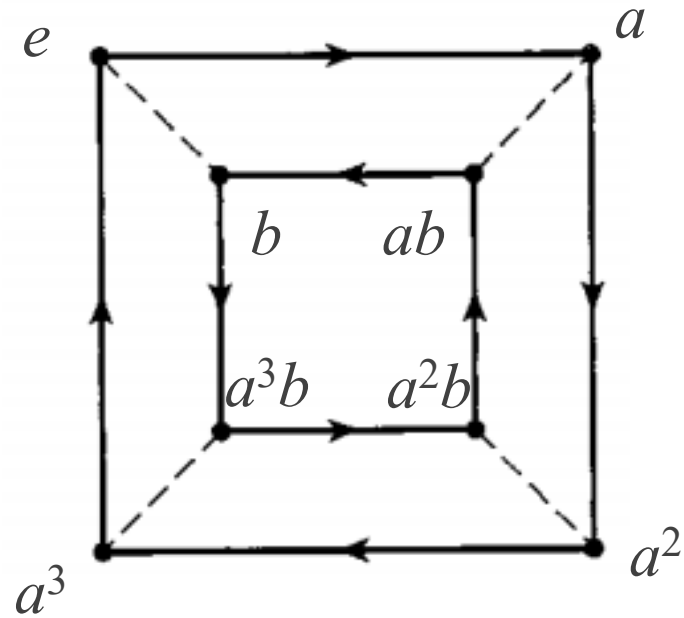
$\Rightarrow$  sequences of arc from  $u$  to  $v$

$uq=v$  and  $ur=v$

# SECTION 7: GENERATING SETS AND CAYLEY DIGRAPHS

---

## 7.12 Example



$\xrightarrow{\quad} a$  and  $----- b -----$ ,



# Abstract Algebra

---

# SECTION 8: GROUPS OF PERMUTATIONS

---

8.3 Theorem A **permutation**(轮换, 置换, 变换) of a set  $A$  is a function  $\phi : A \rightarrow A$  that is both one to one and onto.

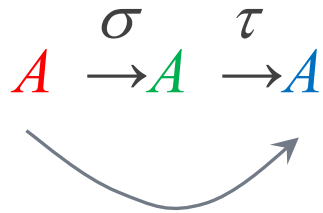
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

# SECTION 8: GROUPS OF PERMUTATIONS

---

**Result** Function composition  $\circ$  is a **binary operation** on the **collection of all permutations** of a set  $A$ .



$$\sigma \circ \tau: A \rightarrow A \quad (\sigma\tau(a_1) = \sigma(\tau(a_1)))$$

$\sigma\tau$  is one to one and onto.

# SECTION 8: GROUPS OF PERMUTATIONS

---

8.4 Example Suppose that  $A=\{1,2,3,4,5\}$ .

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

---

8.4 Example Suppose that  $A=\{1,2,3,4,5\}$ .

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

# SECTION 8: GROUPS OF PERMUTATIONS

---

**8.5 Example** Let  $A$  be a nonempty set, and let  $S_A$  be the collection of all permutations of  $A$ . Then  $S_A$  is a group under permutation multiplication.

# SECTION 8: GROUPS OF PERMUTATIONS

---

**8.5 Example** Let  $A$  be a nonempty set, and let  $S_A$  be the collection of all permutations of  $A$ . Then  $S_A$  is a group under permutation multiplication.

**8.6 Definition** Let  $A$  be the finite set  $\{1, 2, \dots, n\}$ . The group of all permutations of  $A$  is the **symmetric group(对称群)** on  $n$  letters, and is denoted by  $S_n$ . Note that  $S_n$  has  $n!$  elements, where  $n! = n(n-1)(n-2)\dots(3)(2)(1)$ .

# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

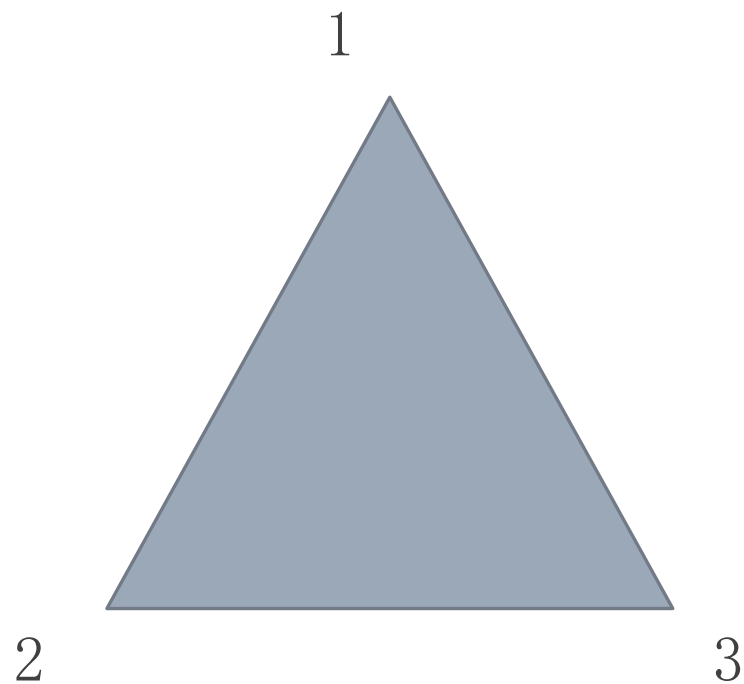
# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



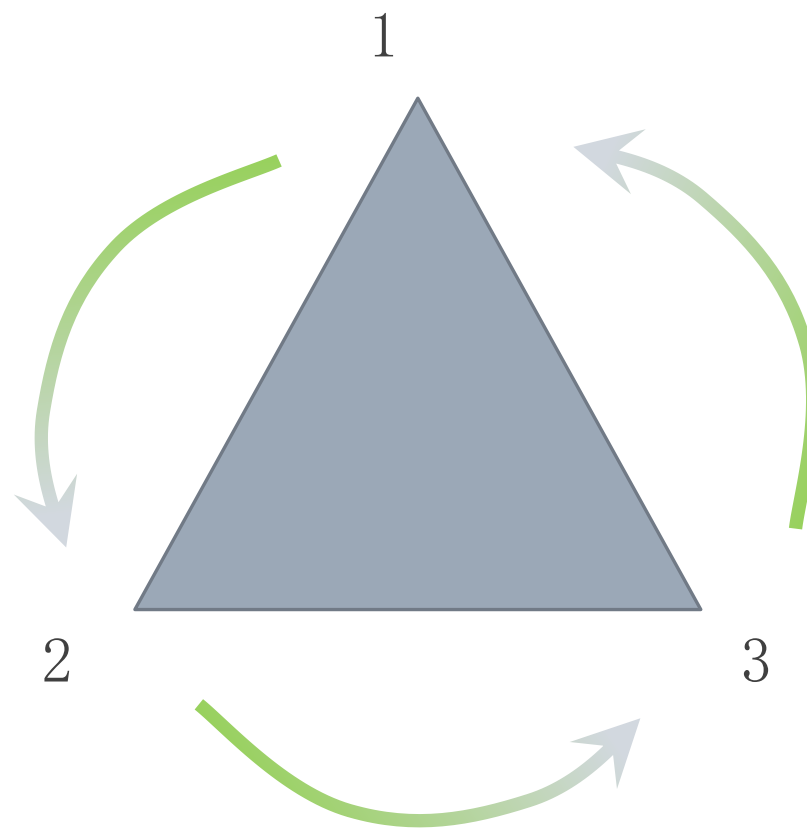
# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



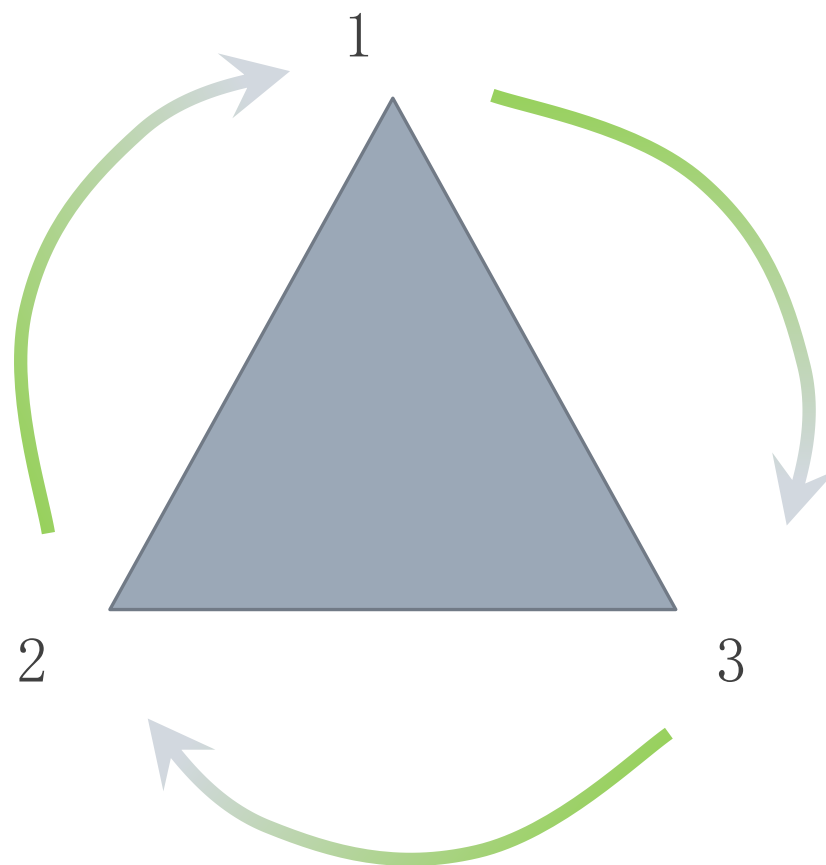
# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



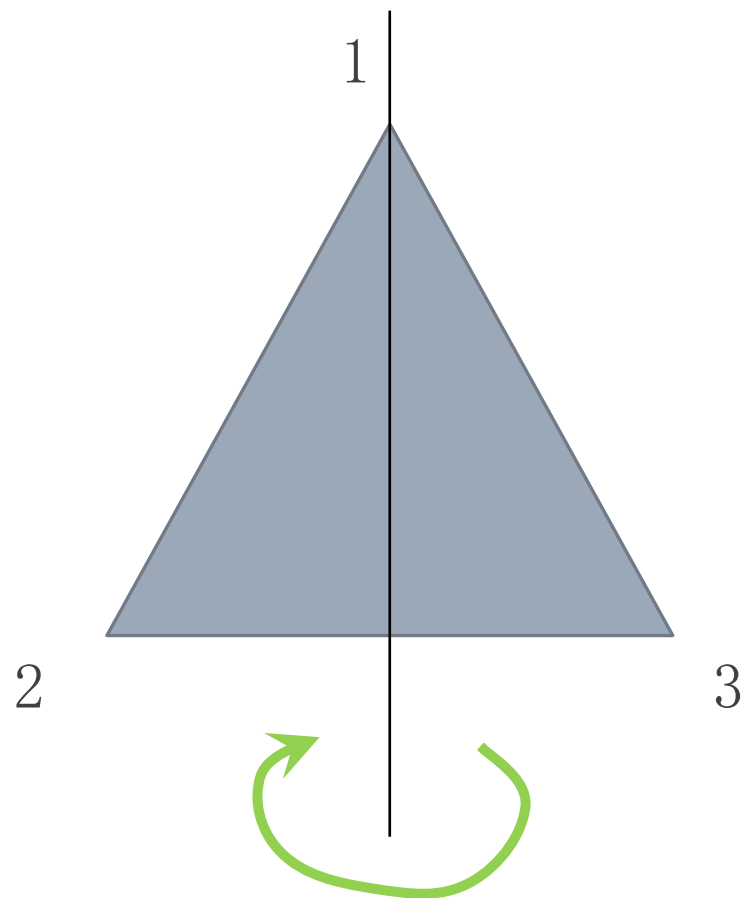
# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$





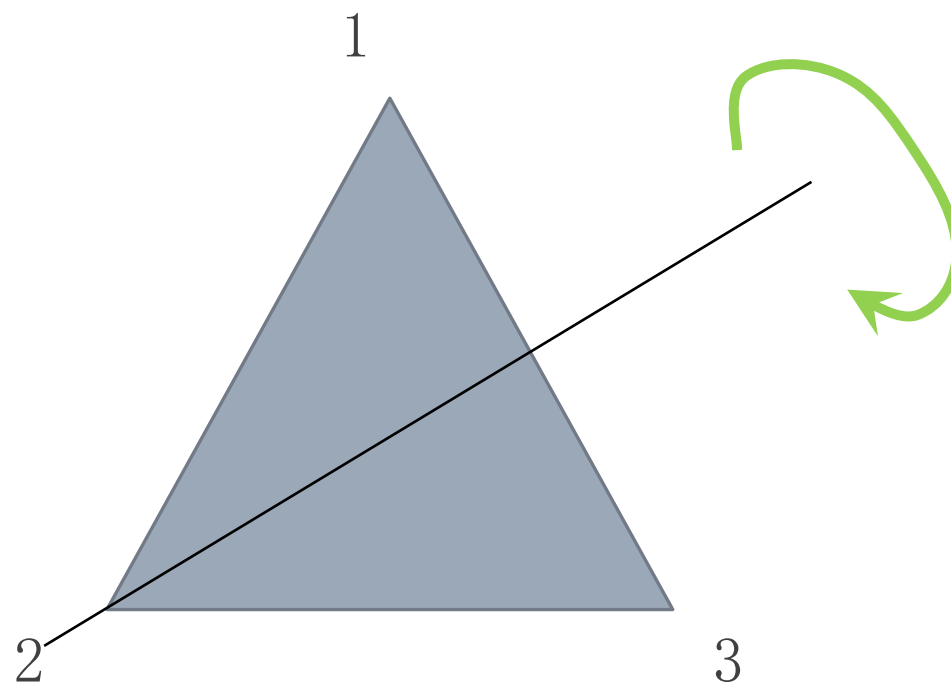
# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



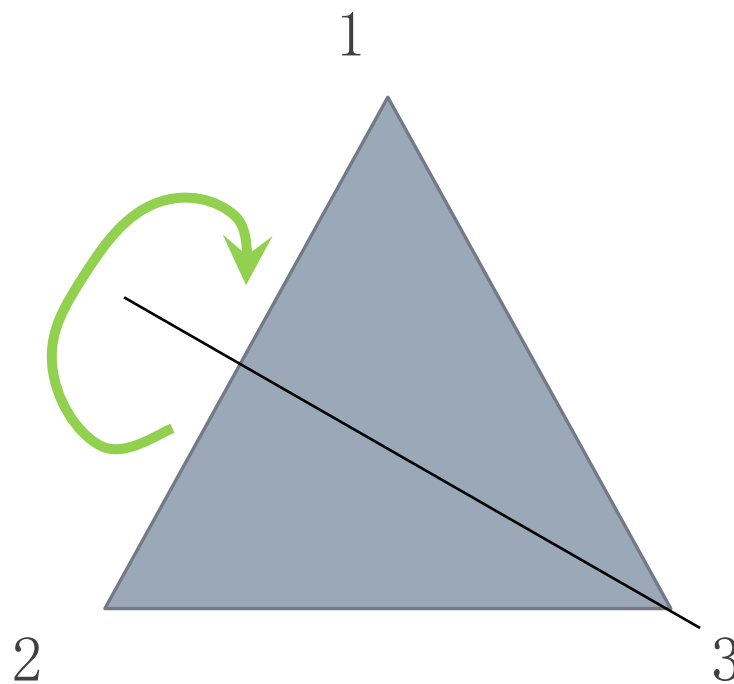
# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_0$	$\mu_3$	$\mu_1$	$\mu_2$
$\rho_2$	$\rho_2$	$\rho_0$	$\rho_1$	$\mu_2$	$\mu_3$	$\mu_1$
$\mu_1$	$\mu_1$	$\mu_2$	$\mu_3$	$\rho_0$	$\rho_1$	$\rho_2$
$\mu_2$	$\mu_2$	$\mu_3$	$\mu_1$	$\rho_2$	$\rho_0$	$\rho_1$
$\mu_3$	$\mu_3$	$\mu_1$	$\mu_2$	$\rho_1$	$\rho_2$	$\rho_0$

# SECTION 8: GROUPS OF PERMUTATIONS

---

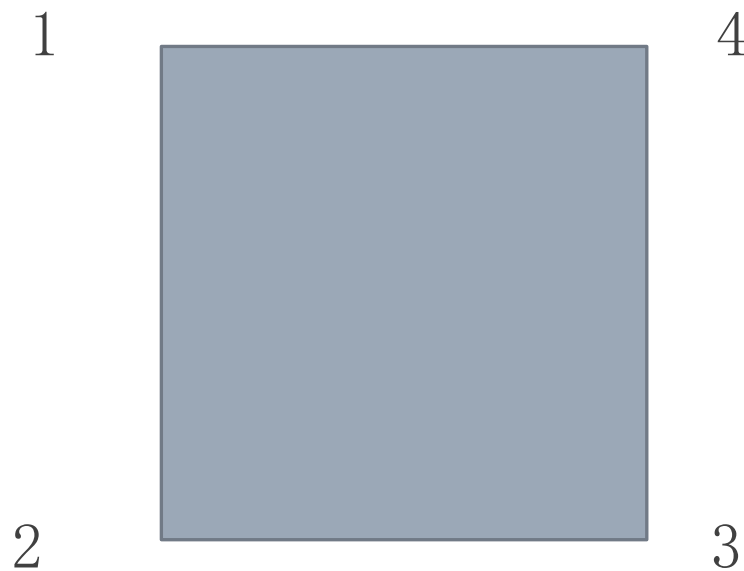
The notation  $D_3$  stands for the third dihedral group. The  $n$ th dihedral group  $D_n$  is the group of symmetries of the regular  $n$ -gon.

$D_4$  will then be the group of symmetries of the square. It is also called the **octic group**.

# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

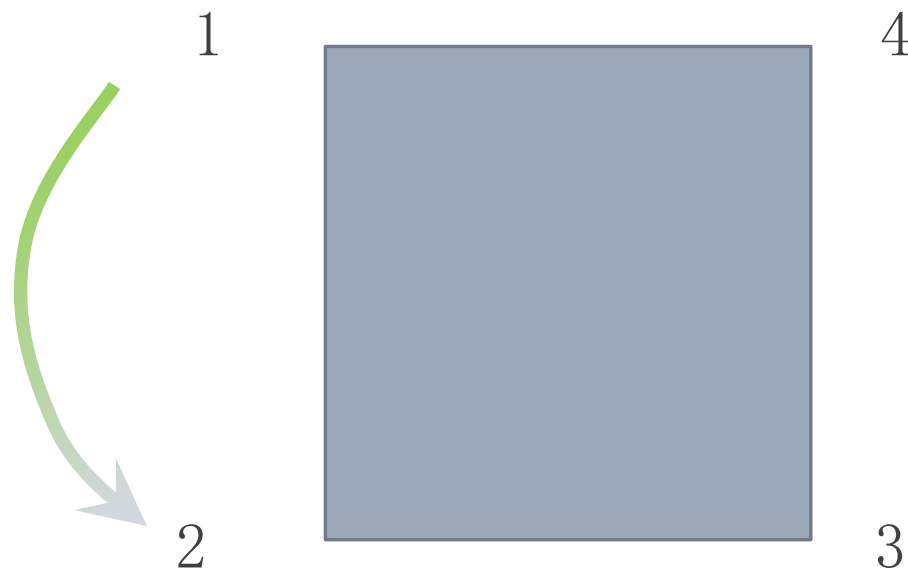


# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$



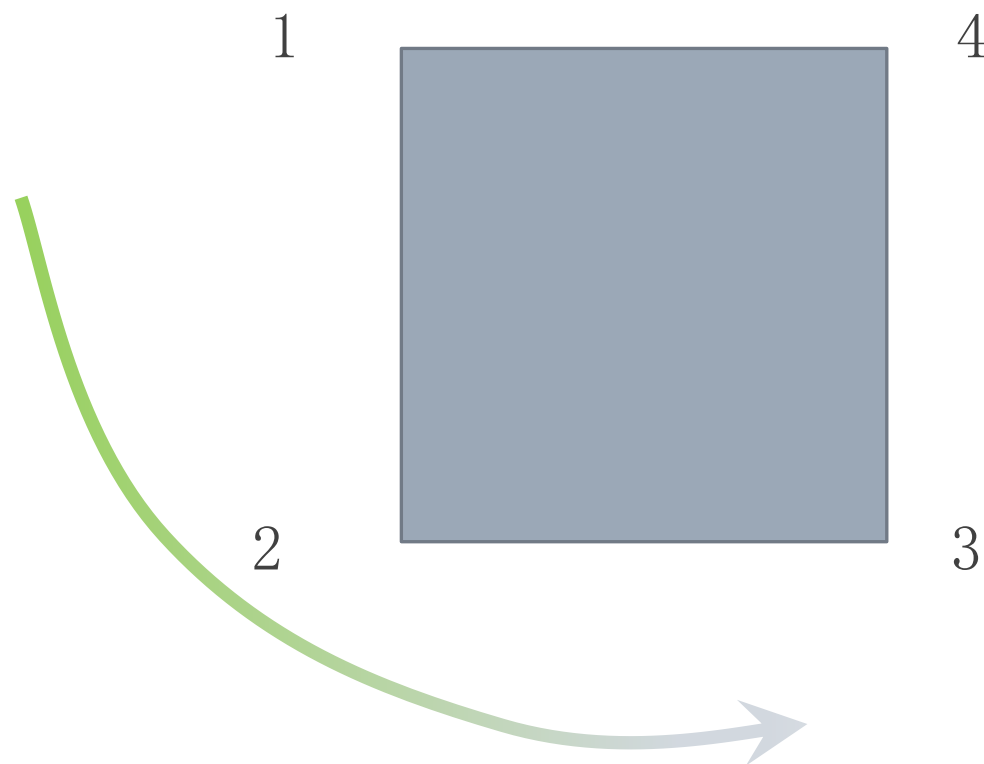
# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

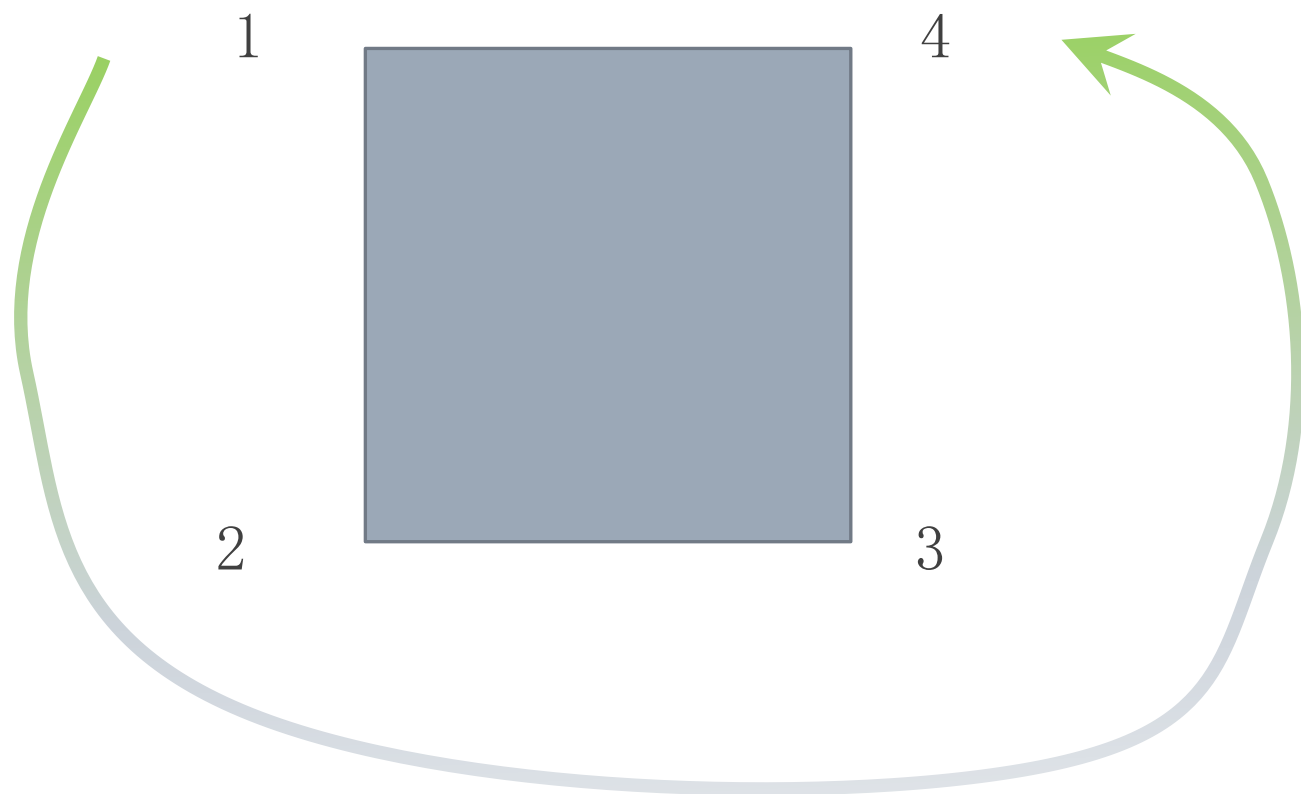
---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$





# SECTION 8: GROUPS OF PERMUTATIONS

---

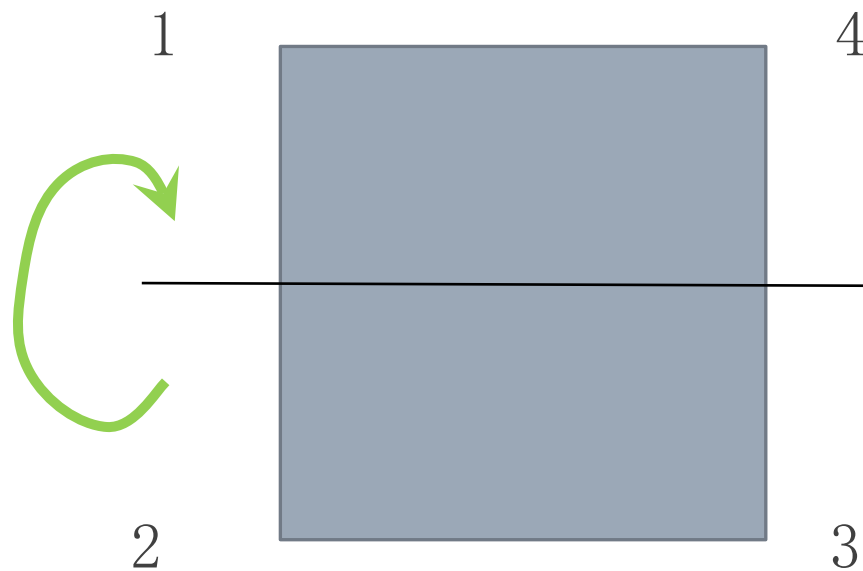
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

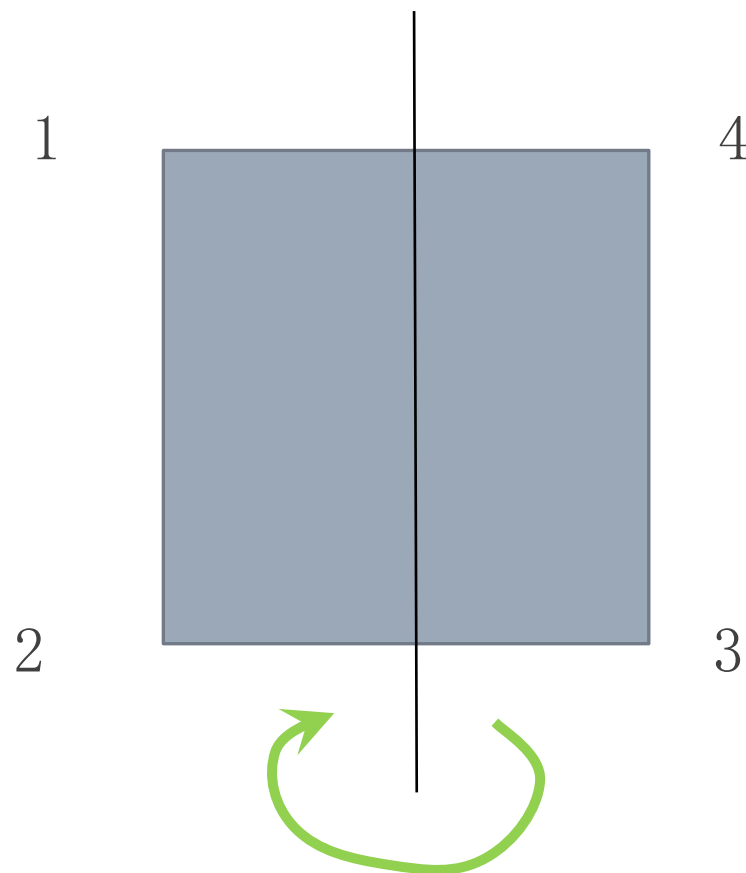
$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

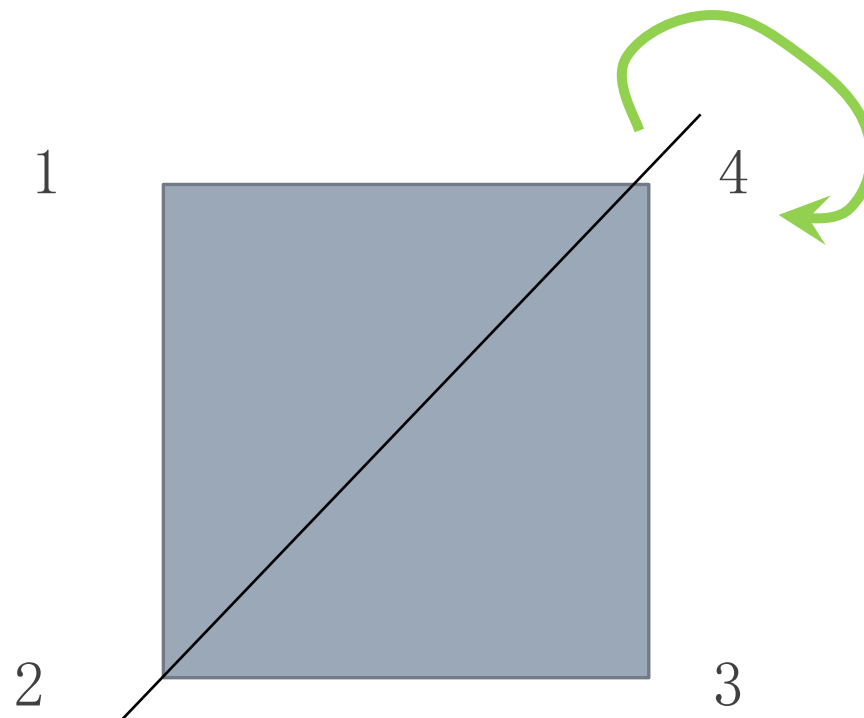
$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

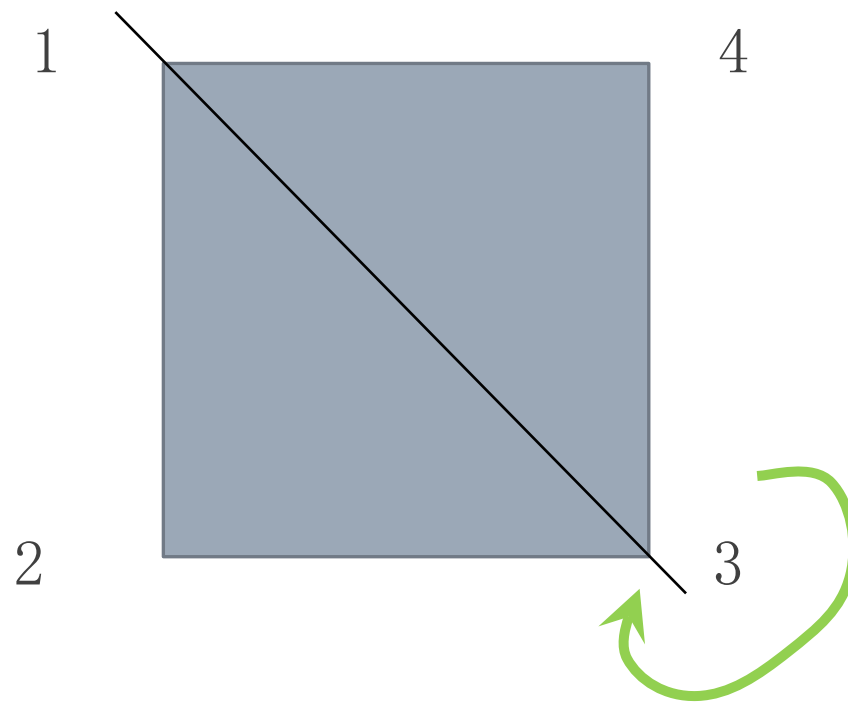
$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\mu_1$	$\mu_2$	$\delta_1$	$\delta_2$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\mu_1$	$\mu_2$	$\delta_1$	$\delta_2$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_3$	$\rho_0$	$\delta_1$	$\delta_2$	$\mu_2$	$\mu_1$
$\rho_2$	$\rho_2$	$\rho_3$	$\rho_0$	$\rho_1$	$\mu_2$	$\mu_1$	$\delta_2$	$\delta_1$
$\rho_3$	$\rho_3$	$\rho_0$	$\rho_1$	$\rho_2$	$\delta_2$	$\delta_1$	$\mu_1$	$\mu_2$
$\mu_1$	$\mu_1$	$\delta_2$	$\mu_2$	$\delta_1$	$\rho_0$	$\rho_2$	$\rho_3$	$\rho_1$
$\mu_2$	$\mu_2$	$\delta_1$	$\mu_1$	$\delta_2$	$\rho_2$	$\rho_0$	$\rho_1$	$\rho_3$
$\delta_1$	$\delta_1$	$\mu_1$	$\delta_2$	$\mu_2$	$\rho_1$	$\rho_3$	$\rho_0$	$\rho_2$
$\delta_2$	$\delta_2$	$\mu_2$	$\delta_1$	$\mu_1$	$\rho_3$	$\rho_1$	$\rho_2$	$\rho_0$

# SECTION 8: GROUPS OF PERMUTATIONS

---

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

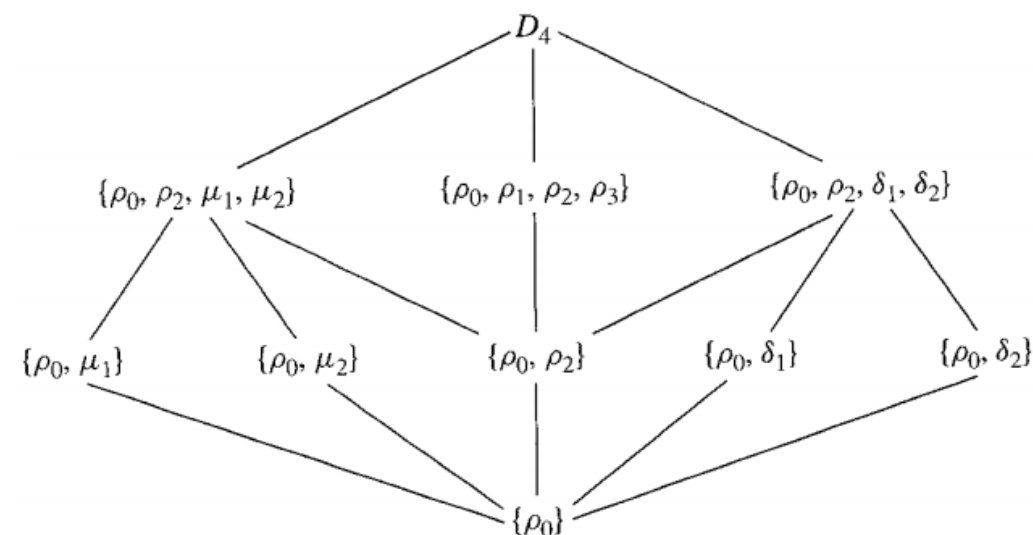
$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

---

**8.14 Definition** Let  $f:A \rightarrow B$  be a function and let  $H$  be a subset of  $A$ . The image of  $H$  under  $f$  is  $\{f(h) \mid h \in H\}$  and is denoted by  $f[H]$ .

**8.15 Lemma** Let  $G$  and  $G'$  be groups and let  $\varphi:G \rightarrow G'$  be a one-to-one function such that  $\varphi(xy)=\varphi(x)\varphi(y)$  for all  $x,y \in G$ . Then  $\varphi[G]$  is a subgroup of  $G'$  and  $\varphi$  provides an isomorphism of  $G$  with  $\varphi[G]$ .

# SECTION 8: GROUPS OF PERMUTATIONS

---

**8.15 Lemma** Let  $G$  and  $G'$  be groups and let  $\varphi: G \rightarrow G'$  be a one-to-one function such that  $\varphi(xy) = \varphi(x)\varphi(y)$  for all  $x, y \in G$ . Then  $\varphi[G]$  is a subgroup of  $G'$  and  $\varphi$  provides an isomorphism of  $G$  with  $\varphi[G]$ .



# SECTION 8: GROUPS OF PERMUTATIONS

---

8.16 Theorem (Cayley's Theorem) Every group is isomorphic to a group of permutations.

For  $x \in G$  let  $\lambda_x : G \rightarrow G$  be defined by  $\lambda_x(g) = xg$  for all  $g \in G$ .

$$\phi : G \rightarrow S_G$$

$$\phi : x \rightarrow \lambda_x$$

# SECTION 8: GROUPS OF PERMUTATIONS

---

8.16 Theorem (Cayley's Theorem) Every group is isomorphic to a group of permutations.

For  $x \in G$  let  $\lambda_x : G \rightarrow G$  be defined by  $\lambda_x(g) = xg$  for all  $g \in G$ .

$\phi : G \rightarrow S_G$        $\phi : x \rightarrow \lambda_x$        $\phi$  is the **left regular representation** of  $G$

For  $x \in G$  let  $\rho_x : G \rightarrow G$  be defined by  $\rho_x(g) = gx$  for all  $g \in G$ .

$\mu : G \rightarrow S_G$        $\mu : x \rightarrow \rho_x^{-1}$        $\mu$  is the **right regular representation** of  $G$

# SECTION 8: GROUPS OF PERMUTATIONS

---

8.18 Example Let us compute the left regular representation of the group given by the group table.

	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$



# Abstract Algebra

---

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**Fact** Each permutation  $\sigma$  of a set  $A$  determines a natural partition.

Each permutation  $\sigma$  of a set  $A$  determines an equivalence relation.

For  $a, b \in A$ , let  $a \sim b$  if and only if  $b = \sigma^n(a)$  for some  $n \in \mathbb{Z}$ . (1)

**Reflexive** Clearly  $a \sim b$  since  $a = \iota(a) = \sigma^0(a)$ .

**Symmetric** If  $a \sim b$ , then  $b = \sigma^n(a)$  for some  $n \in \mathbb{Z}$ . But then  $a = \sigma^{-n}(b)$

**Transitive** Suppose  $a \sim b$  and  $b \sim c$ , then  $b = \sigma^n(a)$  and  $c = \sigma^m(b)$ .

we find that  $c = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a)$ .

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**9.1 Definition** Let  $\sigma$  be a permutation of a set  $A$ . The equivalence classes in  $A$  determined by the equivalence relation (1) are the **orbits**(轨道) of  $\sigma$ .

**9.2 Example** Since the identity permutation of  $A$  leaves each element of  $A$  fixed, the orbits of  $\iota$  are the one-element subsets of  $A$ .

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

9.3 Example Find the orbits of the permutation  $\sigma$  in  $S_8$ .

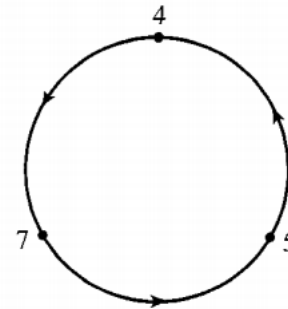
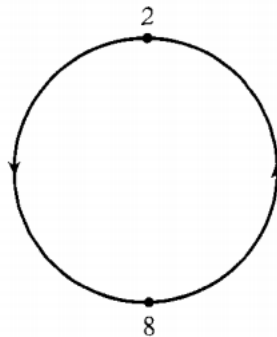
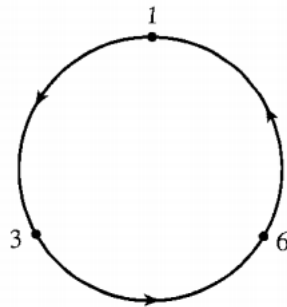
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

9.3 Example Find the orbits of the permutation  $\sigma$  in  $S_8$ .

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$





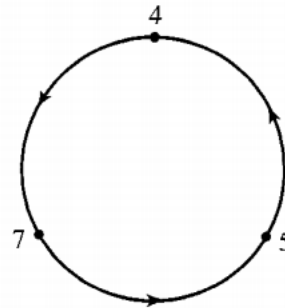
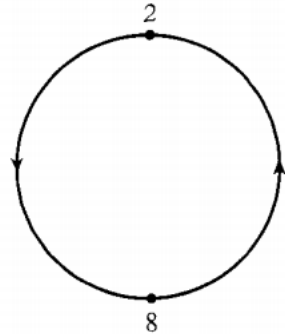
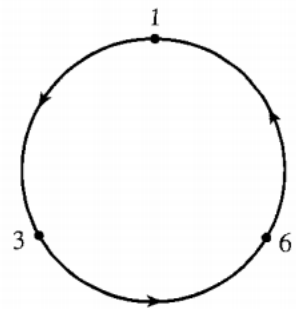
# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**Fact** Each individual circle also defines, by itself, a permutation in  $S_n$ .

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

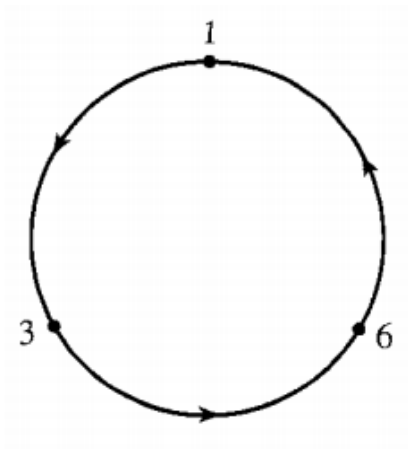
$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}$$



# SECTION 8: GROUPS OF PERMUTATIONS

---

**9.6 Definition** A permutation  $\sigma \in S_n$ , is a **cycle (轮换)** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit.



• • • • •

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}$$

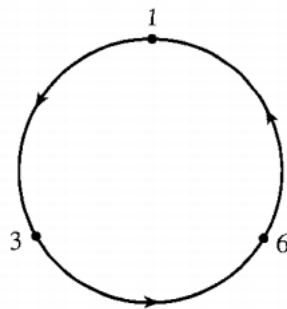
$$=(1,3,6)$$

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

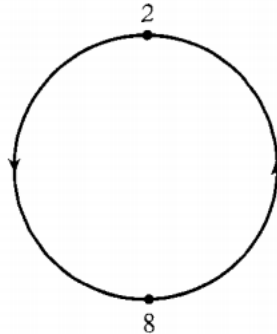
---

9.3 Example Find the orbits of the permutation  $\sigma$  in  $S_8$ .

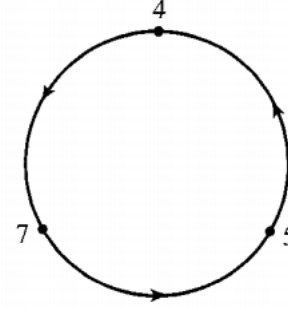
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$



$=(1,3,6)$



$=(2,8)$



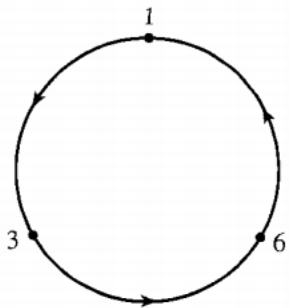
$=(4,7,5)$

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

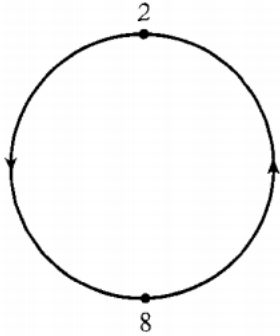
---

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

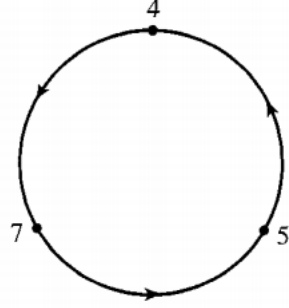
$$=(1,3,6) \ (2,8) \ (4,7,5)$$



$$=(1,3,6)$$



$$=(2,8)$$



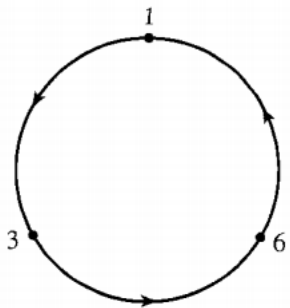
$$=(4,7,5)$$

**9.8 Theorem** Every permutation  $\sigma$  of a finite set is a product of disjoint cycles.

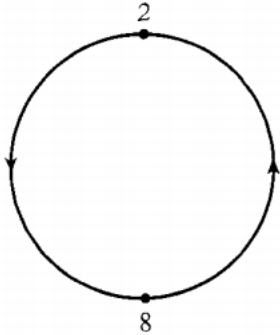
# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

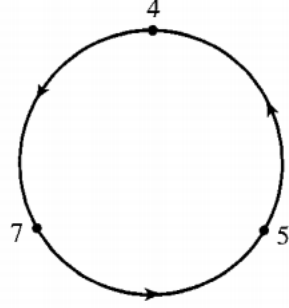
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$
$$=(1,3,6) \ (2,8) \ (4,7,5)$$



$=(1,3,6)$



$=(2,8)$



$=(4,7,5)$

**9.8 Theorem** Every permutation  $\sigma$  of a finite set is a product of disjoint cycles.

**Note** These cycles are disjoint.  
Any integer is in at most one of these cycles.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

9.9 Example Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$$

and write it as a product of disjoint cycles.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**9.10 Example** Consider the cycles  $(1, 4, 5, 6)$  and  $(2, 1, 5)$  in  $S_6$ . Give the product of them.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

9.11 Definition A cycle of length 2 is a **transposition**(对换).

$$(a_1, a_2, \dots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \dots (a_1, a_3)(a_1, a_2).$$

$$(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 4 & * & * & * & * \end{pmatrix}$$

$$(1,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & * & * & * & * \end{pmatrix}$$

$$(1,2,3,4) = (1,4)(1,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & * & * & * & * \end{pmatrix}$$



# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**9.12 Corollary** Any permutation of a finite set of at least two elements is a product of transpositions.

**9.13 Example**  $(1, 6)(2, 5, 3)$  is the product  $(1, 6)(2, 3)(2, 5)$  of transpositions.

**9.14 Example** In  $S_n$ , for  $n \geq 2$ , the identity permutation  $(1)$  is the product  $(1, 2)(1, 2)$  of transpositions.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**9.15 Theorem** No permutation in  $S_n$ , can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

**Proof** From the cycles.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**9.15 Theorem** No permutation in  $S_n$ , can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

**Proof** From linear algebra.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**9.15 Theorem** No permutation in  $S_n$ , can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

**Proof** Let  $\sigma \in S_n$ , and let  $\tau = (i, j)$  be a transposition in  $S_n$ . We claim that the number of orbits of  $\sigma$  and of  $\tau\sigma$  differ by 1.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

9.19 Example The identity permutation in  $S_n$ , is an even permutation.  
the permutation  $(1, 4, 5, 6)(2, 1, 5)$  in  $S_6$  is an odd permutation.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

Let  $\tau$  be any fixed transposition in  $S_n$  ( it exists since  $n \geq 2$ ).

$\lambda_\tau$  is one to one and onto.

# SECTION 9: ORBITS, CYCLES, AND THE ALTERNATING GROUPS

---

**9.20 Theorem** If  $n \geq 2$ , then the collection of all even permutations of  $\{1, 2, 3, \dots, n\}$  forms a subgroup of order  $n!/2$  of the symmetric group  $S_n$ :

**9.21 Definition** The subgroup of  $S_n$ , consisting of the even permutations of  $n$  letters is the **alternating group (交错群)**  $A_n$ , on  $n$  letters.





# Abstract Algebra

---

---

**Observation** The order of a subgroup  $H$  of a finite group  $G$  seems always to be a divisor of the order of  $G$ .

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.1 Theorem** Let  $H$  be a subgroup of  $G$ . Let the relation  $\sim_L$  be defined on  $G$  by  $a \sim_L b$  if and only if  $a^{-1}b \in H$ . Let the relation  $\sim_R$  be defined on  $G$  by  $a \sim_R b$  if and only if  $ab^{-1} \in H$ . Then  $\sim_L$  and  $\sim_R$  are equivalence relations on  $G$ .

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.1 Theorem** Let  $H$  be a subgroup of  $G$ . Let the relation  $\sim_L$  be defined on  $G$  by  $a \sim_L b$  if and only if  $a^{-1}b \in H$ . Then  $\sim_L$  is an equivalence relation on  $G$ .

**Proof**

Symmetric

Transitive

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.2 Definition** Let  $H$  be a subgroup of a group  $G$ . The subset  $aH = \{ah \mid h \in H\}$  of  $G$  is the **left coset (左陪集)** of  $G$  containing  $a$ , while the subset  $Ha = \{ha \mid h \in H\}$  is the **right coset (右陪集)** of  $H$  containing  $a$ .

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.2 Definition** Let  $H$  be a subgroup of a group  $G$ . The subset  $aH = \{ah \mid h \in H\}$  of  $G$  is the **left coset (左陪集)** of  $G$  containing  $a$ , while the subset  $Ha = \{ha \mid h \in H\}$  is the **right coset (右陪集)** of  $H$  containing  $a$ .

**Fact**  $aH$  is the cell of  $\sim_L$  containing  $a$ .

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.2 Definition** Let  $H$  be a subgroup of a group  $G$ . The subset  $aH = \{ah \mid h \in H\}$  of  $G$  is the **left coset (左陪集)** of  $G$  containing  $a$ , while the subset  $Ha = \{ha \mid h \in H\}$  is the **right coset (右陪集)** of  $H$  containing  $a$ .

**10.3 Example** Exhibit the left cosets and the right cosets of the subgroup  $3\mathbb{Z}$  of  $\mathbb{Z}$ .

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.2 Definition** Let  $H$  be a subgroup of a group  $G$ . The subset  $aH = \{ah \mid h \in H\}$  of  $G$  is the **left coset (左陪集)** of  $G$  containing  $a$ , while the subset  $Ha = \{ha \mid h \in H\}$  is the **right coset (右陪集)** of  $H$  containing  $a$ .

**10.3 Example** Exhibit the left cosets and the right cosets of the subgroup  $3\mathbb{Z}$  of  $\mathbb{Z}$ .



# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

10.4 Example The group  $Z_6$  is abelian. Find the partition of  $Z_6$  into cosets of the subgroup  $H=\{0,3\}$ .

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.4 Example** The group  $Z_6$  is abelian. Find the partition of  $Z_6$  into cosets of the subgroup  $H=\{0,3\}$ .

$+_6$	0	3	1	4	2	5
0						
3						
1						
4						
2						
5						

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.4 Example** The group  $Z_6$  is abelian. Find the partition of  $Z_6$  into cosets of the subgroup  $H=\{0,3\}$ .

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

10.4 Example The group  $Z_6$  is abelian. Find the partition of  $Z_6$  into cosets of the subgroup  $H=\{0,3\}$ .

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

$+_6$	0	3	1	4	2	5
0						
3						
1						
4						
2						
5						

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.7 Example** Let  $H$  be the subgroup  $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$  of  $S_3$ . Find the partitions of  $S_3$  into left cosets of  $H$ , and the partition into right cosets of  $H$ .

left cosets  $H = \{\rho_0, \mu_1\}$

$$\rho_1 H = \{\rho_1 \rho_0, \rho_1 \mu_1\} = \{ \quad \}$$

$$\rho_2 H = \{\rho_2 \rho_0, \rho_2 \mu_1\} = \{ \quad \}$$

right cosets  $H = \{\rho_0, \mu_1\}$

$$H \rho_1 = \{\rho_0 \rho_1, \mu_1 \rho_1\} = \{ \quad \}$$

$$H \rho_2 = \{\rho_0 \rho_2, \mu_1 \rho_2\} = \{ \quad \}$$

	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_0$	$\mu_3$	$\mu_1$	$\mu_2$
$\rho_2$	$\rho_2$	$\rho_0$	$\rho_1$	$\mu_2$	$\mu_3$	$\mu_1$
$\mu_1$	$\mu_1$	$\mu_2$	$\mu_3$	$\rho_0$	$\rho_1$	$\rho_2$
$\mu_2$	$\mu_2$	$\mu_3$	$\mu_1$	$\rho_2$	$\rho_0$	$\rho_1$
$\mu_3$	$\mu_3$	$\mu_1$	$\mu_2$	$\rho_1$	$\rho_2$	$\rho_0$

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.7 Example** Let  $H$  be the subgroup  $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$  of  $S_3$ . Find the partitions of  $S_3$  into left cosets of  $H$ , and the partition into right cosets of  $H$ .

left cosets  $H = \{\rho_0, \mu_1\}$

$$\rho_1 H = \{\rho_1 \rho_0, \rho_1 \mu_1\} = \{\rho_1, \mu_3\}$$

$$\rho_2 H = \{\rho_2 \rho_0, \rho_2 \mu_1\} = \{\rho_2, \mu_2\}$$

right cosets  $H = \{\rho_0, \mu_1\}$

$$H \rho_1 = \{\rho_0 \rho_1, \mu_1 \rho_1\} = \{\rho_1, \mu_2\}$$

$$H \rho_2 = \{\rho_0 \rho_2, \mu_1 \rho_2\} = \{\rho_2, \mu_3\}$$

	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_0$	$\mu_3$	$\mu_1$	$\mu_2$
$\rho_2$	$\rho_2$	$\rho_0$	$\rho_1$	$\mu_2$	$\mu_3$	$\mu_1$
$\mu_1$	$\mu_1$	$\mu_2$	$\mu_3$	$\rho_0$	$\rho_1$	$\rho_2$
$\mu_2$	$\mu_2$	$\mu_3$	$\mu_1$	$\rho_2$	$\rho_0$	$\rho_1$
$\mu_3$	$\mu_3$	$\mu_1$	$\mu_2$	$\rho_1$	$\rho_2$	$\rho_0$

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**Claim** Every left coset and every right coset of  $H$  have the same number of elements as  $H$ .

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

10.10 Theorem(Theorem of Lagrange) Let  $H$  be a subgroup of a finite group  $G$ . Then the order of  $H$  is a divisor of the order of  $G$ .

10.11 Corollary Every group of prime order is cyclic.



# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**Definition** The **order** (阶) of an element is the same as the order of the cyclic subgroup generated by the element.

# SECTION 10: COSETS AND THE THEOREM OF LAGRANGE

---

**10.13 Definition** Let  $H$  be a subgroup of a group  $G$ . The number of left cosets of  $H$  in  $G$  is the index  $(G:H)$  of  $H$  in  $G$ .

**Fact**  $(G:H)=|G|/|H|$  if  $|G|$  is finite.

**10.14 Theorem** Suppose  $H$  and  $K$  are subgroups of a group  $G$  such that  $K \leq H \leq G$ , and suppose  $(H:K)$  and  $(G:H)$  are both finite. Then  $(G:K)$  is finite, and  $(G:K)=(G:H)(H:K)$ .



# Abstract Algebra

---

---

**11.1 Definition** The Cartesian product of sets  $S_1, S_2, \dots, S_n$ , is the set of all ordered  $n$ -tuples  $(a_1, a_2, \dots, a_n)$ , where  $a_i \in S_i$  for  $i = 1, 2, \dots, n$ . The Cartesian product is denoted by either

$$S_1 \times S_2 \times \dots \times S_n$$

or by

$$\prod_{i=1}^n S_i$$

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.2 Theorem** Let  $G_1, G_2, \dots, G_n$  be groups. For  $(a_1, a_2, \dots, a_n)$  and  $(b_1, b_2, \dots, b_n)$  in  $\Pi_1^n G_i$ , define  $(a_1, a_2, \dots, a_n) (b_1, b_2, \dots, b_n)$  to be the element  $(a_1 b_1, a_2 b_2, \dots, a_n b_n)$ . Then  $\Pi_1^n G_i$  is a group, **the direct product (直积)** of the groups  $G_i$ , under this binary operation.

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

11.3 Example Consider the group  $\mathbb{Z}_2 \times \mathbb{Z}_3$ . It is a cyclic group.

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

11.4 Example Consider the group  $\mathbb{Z}_3 \times \mathbb{Z}_3$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.5 Theorem** The group  $Z_m \times Z_n$  is **cyclic** and is **isomorphic to  $Z_{mn}$**  if and only if  $m$  and  $n$  are relatively prime, that is, the gcd of  $m$  and  $n$  is 1.



# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

11.6 Corollary The group  $\Pi_1^n Z_{m_i}$  is cyclic and isomorphic to  $Z_{m_1 m_2 \dots m_n}$ , if and only if the numbers  $m_i$  for  $i=1, \dots, n$  are such that the gcd of any two of them is 1.

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.7 Example** The preceding corollary shows that if  $n$  is written as a product of powers of distinct prime numbers, as in

$$n = (p_1)^{n_1}(p_2)^{n_2}\dots(p_r)^{n_r},$$

then  $Z_n$  is isomorphic to  $Z_{p_1}^{n_1} \times Z_{p_2}^{n_2} \times \dots \times Z_{p_r}^{n_r}$ .

**Example**  $Z_{72}$  is isomorphic to  $Z_8 \times Z_9$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.8 Definition** Let  $r_1, r_2, \dots, r_n$  be positive integers. Their **least common multiple (abbreviated lcm 最小公倍数)** is the positive generator of the cyclic group of all common multiples of the  $r_i$ , that is, the cyclic group of all integers divisible by each  $r_i$ ; for  $i=1, 2, \dots, n$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.9 Theorem** Let  $(a_1, a_2, \dots, a_n) \in \Pi_1^n G_i$ . If  $a_i$  is of finite order  $r_i$  in  $G_i$ , then the order of  $(a_1, a_2, \dots, a_n)$  in  $\Pi_1^n G_i$  is equal to the least common multiple of all the  $r_i$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

11.10 Example Find the order of  $(8,4,10)$  in the group  $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.11 Example** The group  $\mathbb{Z} \times \mathbb{Z}_2$  is generated by the elements  $(1, 0)$  and  $(0, 1)$ . More generally, the direct product of  $n$  cyclic groups, each of which is either  $\mathbb{Z}$  or  $\mathbb{Z}_m$  for some positive integer  $m$ , is generated by the  $n$   $n$ -tuples

$(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), (0, 0, 1, \dots, 0), \dots, (0, 0, 0, \dots, n).$

**Note** Such a direct product might also be generated by fewer elements. For example,  $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{35}$  is generated by the single element  $(1, 1, 1)$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**Note** If  $\Pi_1^n G_i$  is the direct product of groups  $G_i$ , the subset

$$\bar{G}_i = \{(e_1, e_2, \dots, a_i, \dots, e_n) \mid a_i \in G_i\}.$$

is a subgroup of  $\Pi_1^n G_i$ .

It is also clear that this subgroup  $\bar{G}_i$  is naturally isomorphic to  $G_i$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

11.12 Theorem (Fundamental Theorem of Finitely Generated Abelian Groups) Every finitely generated abelian group  $G$  is isomorphic to a direct product of cyclic groups in the form

$$Z_{p_1}^{n_1} \times Z_{p_2}^{n_2} \times \dots \times Z_{p_r}^{n_r} \times Z \times Z \times \dots \times Z$$

where the  $p_i$  are primes, not necessarily distinct, and the  $r_i$  are positive integers.



# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.13 Example** Find all abelian groups, up to isomorphism, of order 360.

**Solution**  $360=2^3 \times 3^2 \times 5$ .

1.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

2.  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

3.  $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

4.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

5.  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

6.  $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.14 Definition** A group  $G$  is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise  $G$  is **indecomposable**.

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.15 Theorem** The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---

**11.16 Theorem** If  $m$  divides the order of a finite abelian group  $G$ , then  $G$  has a subgroup of order  $m$ .

# SECTION 11: DIRECT PRODUCTS AND FINITELY GENERATED ABELIAN GROUPS

---



# Abstract Algebra

---

---

13.1 Definition A map  $\varphi$  of a group  $G$  into a group  $G'$  is a **homomorphism(同态)** if the **homomorphismproperty**

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

holds for all  $a,b\in G$ .

$$\varphi(a *_1 b)=\varphi(a) *_2 \varphi(b)$$

---

13.2 Example Let  $\varphi: G \rightarrow G'$  be a group homomorphism of  $G$  onto  $G'$ . We claim that if  $G$  is abelian, then  $G'$  must be abelian.



---

13.3 Example Let  $S_n$  be the symmetric group on  $n$  letters, and let

$\varphi: S_n \rightarrow Z_2$  be defined by

$$\varphi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation} \\ 1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Show that  $\varphi$  is a homomorphism.

---

13.4 Example (Evaluation Homomorphism求值同态) Let  $F$  be the additive group of all functions mapping  $R$  into  $R$ , let  $R$  be the additive group of real numbers, and let  $c$  be any real number. Let  $\varphi_c: F \rightarrow R$  be the **evaluation homomorphism** defined by

$$\varphi_c(f) = f(c) \text{ for } f \in F.$$

---

**13.5 Example** Let  $R^n$  be the additive group of column vectors with  $n$  real-number components. Let  $A$  be an  $m \times n$  matrix of real numbers. Let  $\varphi: R^n \rightarrow R^n$  be defined by  $\varphi(v) = Av$  for each column vector  $v \in R^n$ . Then  $\varphi$  is a homomorphism.

---

**13.6 Example** Let  $GL(n, R)$  be the multiplicative group of all invertible  $n \times n$  matrices. Recall that a matrix  $A$  is invertible if and only if its determinant,  $\det(A)$ , is nonzero. Recall also that for matrices  $A, B \in GL(n, R)$  we have  $\det(AB) = \det(A)\det(B)$ .

This means that  $\det$  is a homomorphism mapping  $GL(n, R)$  into the multiplicative group  $R^*$  of nonzero real numbers.

---

**13.7 Example** Let  $r \in Z$  and let  $\lambda_r: Z \rightarrow Z$  be defined by  $\lambda_r(n) = rn$  for all  $n \in Z$ . Then  $\lambda_r$  is a homomorphism.

Note that  $\lambda_0$  is the trivial homomorphism.

$\lambda_1$  is the identity map, and  $\lambda_{-1}$  maps  $Z$  onto  $Z$ .

For all other  $r$  in  $Z$ , the map  $\lambda_r$  is not onto  $Z$ .

---

13.8 Example Let  $G = G_1 \times G_2 \times \dots \times G_n$ , be a direct product of groups. The **projection map**(投射)  $\pi_i: G \rightarrow G_i$  where  $\pi_i(g_1, g_2, \dots, g_n) = g_i$  is a homomorphism for each  $i = 1, 2, \dots, n$ .

---

13.9 Example Let  $F$  be the additive group of continuous functions with domain  $[0, 1]$  and let  $R$  be the additive group of real numbers. The map  $\sigma: F \rightarrow R$  defined by  $\sigma(f) = \int_0^1 f(x) dx$  for  $f \in F$  is a homomorphism.

---

13.10 Example (Reduction Modulo  $n$ ) Let  $\gamma$  be the natural map of  $\mathbb{Z}$  into  $\mathbb{Z}_n$ , given by  $\gamma(m)=r$ , where  $r$  is the remainder given by the division algorithm when  $m$  is divided by  $n$ . Then  $\gamma$  is a homomorphism.



---

**13.11 Definition** Let  $\varphi$  be a mapping of a set  $X$  into a set  $Y$ , and let  $A \subseteq X$  and  $B \subseteq Y$ . The **image**  $\varphi[A]$  of  $A$  in  $Y$  under  $\varphi$  is  $\{\varphi(a) \mid a \in A\}$ . The set  $\varphi[X]$  is the **range** of  $\varphi$ . The **inverse image**  $\varphi^{-1}[B]$  of  $B$  in  $X$  is  $\{x \in X \mid \varphi(x) \in B\}$ .

---

13.12 Theorem Let  $\varphi$  be a homomorphism of a group  $G$  into a group  $G'$ .

1. If  $e$  is the identity element in  $G$ , then  $\varphi(e)$  is the identity element  $e'$  in  $G'$ .
2. If  $a \in G$ , then  $\varphi(a^{-1}) = \varphi(a)^{-1}$ .
3. If  $H$  is a subgroup of  $G$ , then  $\varphi[H]$  is a subgroup of  $G'$ .
4. If  $K'$  is a subgroup of  $G'$ , then  $\varphi^{-1}[K']$  is a subgroup of  $G$ .

Tip  $\varphi$  preserves the identity element, inverses, and subgroups.

---

**13.13 Definition** Let  $\varphi: G \rightarrow G'$  be a homomorphism of groups. The subgroup  $\varphi^{-1}[\{e'\}] = \{x \in G \mid \varphi(x) = e'\}$  is the **kernel (核)** of  $\varphi$ , denoted by  $\text{Ker}(\varphi)$ .

---

**13.15 Theorem** Let  $\varphi: G \rightarrow G'$  be a group homomorphism, and let  $H = \text{Ker}(\varphi)$ . Let  $a \in G$ . Then the set

$$\varphi^{-1}[\varphi(a)] = \{x \in G \mid \varphi(x) = \varphi(a)\}$$

is the left coset  $aH$  of  $H$ , and is also the right coset  $Ha$  of  $H$ . Consequently, the two partitions of  $G$  into left cosets and into right cosets of  $H$  are the same.

---

**13.16 Example** The absolute value function  $| \cdot |$  is a homomorphism of the group  $\mathbf{C}^*$  of nonzero complex numbers under multiplication onto the group  $\mathbf{R}^+$  of positive real numbers under multiplication.

---

13.17 Example Let  $D$  be the additive group of all differentiable functions mapping  $R$  into  $R$ , and let  $F$  be the additive group of all functions mapping  $R$  into  $R$ . Then differentiation gives us a map  $\varphi: D \rightarrow F$ , where  $\varphi(f) = f'$  for  $f \in D$ . We easily see that  $\varphi$  is a homomorphism.

---

13.18 Corollary A group homomorphism  $\varphi: G \rightarrow G'$  is a one-to-one map if and only if  $\text{Ker}(\varphi) = \{e\}$ .

---

**13.18 Corollary** A group homomorphism  $\varphi: G \rightarrow G'$  is a one-to-one map if and only if  $\text{Ker}(\varphi) = \{e\}$ .

**Corollary** To Show  $\varphi: G \rightarrow G'$  is an isomorphism.

Step 1 Show  $\varphi$  is a homomorphism.

Step 2 Show  $\text{Ker}(\varphi) = \{e\}$ .

Step 3 Show  $\varphi$  maps  $G$  onto  $G'$ .





# Abstract Algebra

---

---

**14.1 Theorem** Let  $\varphi: G \rightarrow G'$  be a group homomorphism with kernel  $H$ . Then the cosets of  $H$  form a **factor group**,  $G/H$ , where  $(aH)(bH) = (ab)H$ . Also, the map  $\mu: G/H \rightarrow \varphi[G]$  defined by  $\mu(aH) = \varphi(a)$  is an isomorphism. Both coset multiplication and  $\mu$  are well defined, independent of the choices  $a$  and  $b$  from the cosets.

---

14.2 Example The map  $\gamma: \mathbb{Z} \rightarrow \mathbb{Z}_n$ , where  $\gamma(m)$  is the remainder when  $m$  is divided by  $n$  in accordance with the division algorithm is a homomorphism. Of course,  $\text{Ker}(\gamma) = n\mathbb{Z}$ , the factor group  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to  $\mathbb{Z}_n$ .

---

**Definition** A subgroup  $H$  of a group  $G$  is **normal (正规)** if  $aH=Ha$  for any  $a \in G$ .

---

---

---

**14.7 Example** Since  $Z$  is an abelian group,  $nZ$  is a normal subgroup. Corollary 14.5 allows us to construct the factor group  $Z/nZ$  with no reference to a homomorphism. As we observed in Example 14.2,  $Z/nZ$  is isomorphic to  $Z_n$ .

---

14.8 Example Consider the abelian group  $R$  under addition, and let  $c \in R^+$ .  $R/\langle c \rangle$  is then also isomorphic to the circle group  $U$  of complex numbers of magnitude 1 under multiplication.



---

14.9 Theorem Let  $H$  be a normal subgroup of  $G$ . Then  $\gamma: G \rightarrow G/H$  given by  $\gamma(x) = xH$  is a homomorphism with kernel  $H$ .

---

14.11 Theorem (The Fundamental Homomorphism Theorem) Let  $\phi: G \rightarrow G'$  be a group homomorphism with kernel  $H$ . Then  $\phi[G]$  is a group, and  $\mu: G/H \rightarrow \phi[G]$  given by  $\mu(gH) = \phi[g]$  is an isomorphism. If  $\gamma: G \rightarrow G/H$  is the homomorphism given by  $\gamma(g) = gH$ , then  $\phi(g) = \mu\gamma(g)$  for each  $g \in G$ .

---

14.12 Example Classify the group  $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2)$  according to the fundamental theorem of finitely generated abelian groups (Theorem 11.12).

---

**14.13 Theorem** The following are three equivalent conditions for a subgroup  $H$  of a group  $G$  to be a normal subgroup of  $G$ .

1.  $ghg^{-1} \in H$  for all  $g \in G$  and  $h \in H$ .
2.  $gHg^{-1} = H$  for all  $g \in G$ .
3.  $gH = Hg$  for all  $g \in G$ .

---

14.14 Example Every subgroup  $H$  of an abelian group  $G$  is normal.



# Abstract Algebra

---

---

15.2 Example The trivial subgroup  $N=\{0\}$  of  $Z$  is, of course, a normal subgroup. Compute  $Z/\{0\}$ .

---

15.3 Example Let  $n$  be a positive integer. The set  $nR = \{nr \mid r \in R\}$  is a subgroup of  $R$  under addition, and it is normal since  $R$  is abelian. Compute  $R/nR$ .



---

## 15.4 Example $S_n/A_n$ .

	$A_n$	$\sigma A_n$
$A_n$	$A_n$	$\sigma A_n$
$\sigma A_n$	$\sigma A_n$	$A_n$

---

## 15.4 Example $S_n/A_n$ .

	<i>even</i>	<i>odd</i>
<i>even</i>	<i>even</i>	<i>odd</i>
<i>odd</i>	<i>odd</i>	<i>even</i>

---

### 15.5 Example (Falsity of the Converse of the Theorem of Lagrange)

$A_4$ , which has order 12, contains no subgroup of order 6.

---

15.7 Example  $(\mathbb{Z}_4 \times \mathbb{Z}_6) / \langle (0,1) \rangle$ .

---

**15.8 Theorem** Let  $G=H\times K$  be the direct product of groups  $H$  and  $K$ . Then  $\bar{H}=\{(h,e) \mid h \in H\}$  is a normal subgroup of  $G$ . Also  $G/\bar{H}$  is isomorphic to  $K$  in a natural way. Similarly,  $G/\bar{K} \simeq H$  in a natural way.

---

15.9 Theorem A factor group of a cyclic group is cyclic.

---

15.10 Example  $(\mathbb{Z}_4 \times \mathbb{Z}_6) / \langle (0,2) \rangle$ .

---

15.11 Example  $(\mathbb{Z}_4 \times \mathbb{Z}_6) / \langle (2,3) \rangle$ .



---

15.12 Example Let us compute (that is, classify as in Theorem 11.12 the group  $(\mathbb{Z} \times \mathbb{Z}) / \langle (1, 1) \rangle$ ).

---

**15.14 Definition** A group is simple if it is nontrivial and has no proper nontrivial normal subgroups.

---

15.15 Definition The alternating group  $A_n$ , is simple for  $n \geq 5$ .

---

**15.16 Theorem** Let  $\varphi: G \rightarrow G'$  be a group homomorphism. If  $N$  is a normal subgroup of  $G$ , then  $\varphi[N]$  is a normal subgroup of  $\varphi[G]$ . Also, if  $N'$  is a normal subgroup of  $\varphi[G]$ , then  $\varphi^{-1}[N']$  is a normal subgroup of  $G$ .

---

**15.17 Definition** A maximal normal subgroup of a group  $G$  is a normal subgroup  $M$  not equal to  $G$  such that there is no proper normal subgroup  $N$  of  $G$  properly containing  $M$ .

---

15.18 Theorem  $M$  is a maximal normal subgroup of  $G$  if and only if  $G/M$  is simple.

---

**Definition** The **center(中心)**  $Z(G)$  is defined by  $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$ .

---

15.19 Example The center of a group  $G$  always contains the identity element. It may be that  $Z(G) = \{e\}$ , in which case we say that the center of  $G$  is trivial.

$$Z(S_3) = \{\rho_0\}$$

	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_0$	$\mu_3$	$\mu_1$	$\mu_2$
$\rho_2$	$\rho_2$	$\rho_0$	$\rho_1$	$\mu_2$	$\mu_3$	$\mu_1$
$\mu_1$	$\mu_1$	$\mu_2$	$\mu_3$	$\rho_0$	$\rho_1$	$\rho_2$
$\mu_2$	$\mu_2$	$\mu_3$	$\mu_1$	$\rho_2$	$\rho_0$	$\rho_1$
$\mu_3$	$\mu_3$	$\mu_1$	$\mu_2$	$\rho_1$	$\rho_2$	$\rho_0$



---

**15.19 Example** The center of a group  $G$  always contains the identity element. It may be that  $Z(G) = \{e\}$ , in which case we say that the **center of  $G$  is trivial**.

$$Z(S_3) = \{\rho_0\}$$

The center of every nonabelian group of order  $pq$  for primes  $p$  and  $q$  is trivial.

The center of  $S_3 \times Z_5$  must be  $\{\rho_0\} \times Z_5$ , which is isomorphic to  $Z_5$ .

---

**Definition** An element  $aba^{-1}b^{-1}$  in a group is a commutator of the group.

**15.20 Theorem** The set of all commutators  $aba^{-1}b^{-1}$  for  $a, b \in G$  generates a subgroup  $C$  (the commutator subgroup) of  $G$ . This subgroup  $C$  is a normal subgroup of  $G$ . Furthermore, if  $N$  is a normal subgroup of  $G$ , then  $G/N$  is abelian if and only if  $C \leq N$ .

---

15.20 Theorem The set of all commutators  $aba^{-1}b^{-1}$  for  $a, b \in G$  generates a subgroup  $C$  (the commutator subgroup) of  $G$ . This subgroup  $C$  is a normal subgroup of  $G$ . Furthermore, if  $N$  is a normal subgroup of  $G$ , then  $G/N$  is abelian if and only if  $C \leq N$ .

---

15.21 Example The commutator subgroup of  $C_3$  is  $A_3$ .

	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\mu_1$	$\mu_2$	$\mu_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_0$	$\mu_3$	$\mu_1$	$\mu_2$
$\rho_2$	$\rho_2$	$\rho_0$	$\rho_1$	$\mu_2$	$\mu_3$	$\mu_1$
$\mu_1$	$\mu_1$	$\mu_2$	$\mu_3$	$\rho_0$	$\rho_1$	$\rho_2$
$\mu_2$	$\mu_2$	$\mu_3$	$\mu_1$	$\rho_2$	$\rho_0$	$\rho_1$
$\mu_3$	$\mu_3$	$\mu_1$	$\mu_2$	$\rho_1$	$\rho_2$	$\rho_0$



# Abstract Algebra

---

---

18.1 Definition A **ring(环)**  $\langle R, +, \cdot \rangle$  is a set  $R$  together with two binary operations  $+$  and  $\cdot$ , which we call addition and multiplication, defined on  $R$  such that the following axioms are satisfied:

**R1.**  $(R, +)$  is an abelian group.

**R2.** Multiplication is associative.

**R3.** For all  $a, b, c \in R$ , the left distributive law,  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  and the right distributive law  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$  hold.

---

18.2 Example  $\langle \mathbb{Z}, +, \cdot \rangle$ ,  $\langle \mathbb{Q}, +, \cdot \rangle$ ,  $\langle \mathbb{R}, +, \cdot \rangle$ , and  $\langle \mathbb{C}, +, \cdot \rangle$  are rings.

---

18.3 Example Let  $R$  be any ring and let  $M_n(R)$  be the collection of all  $n \times n$  matrices having elements of  $R$  as entries.



---

18.4 Example Let  $F$  be the set of all functions  $f:R \rightarrow R$ . We know that  $(F, +)$  is an abelian group under the usual function addition,  $(f + g)(x) = f(x) + g(x)$ .

We define multiplication on  $F$  by  $(f \cdot g)(x) = f(x)g(x)$ .

Then  $\langle F, +, \cdot \rangle$  is a ring.

---

18.5 Example  $\langle n\mathbb{Z}, +, \cdot \rangle$  is a ring.

---

18.6 Example  $\langle \mathbb{Z}_n, +, \cdot \rangle$  is a ring.

---

**18.7 Example** If  $R_1, R_2, \dots, R_n$ , are rings, we can form the set  $R_1 \times R_2 \times \dots \times R_n$ , of all ordered  $n$ -tuples  $(r_1, r_2, \dots, r_n)$ , where  $r_i \in R_i$ . Defining addition and multiplication of  $n$ -tuples by components (just as for groups), we see at once from the ring axioms in each component that the set of all these  $n$ -tuples forms a ring under addition and multiplication by components. The ring  $R_1 \times R_2 \times \dots \times R_n$  is the direct product of the rings  $R_i$ .

---

18.8 Theorem If  $R$  is a ring with additive identity  $0$ , then for any  $a, b \in R$  we have

1.  $0a = a0 = 0$ ,

2.  $a(-b) = (-a)b = -(ab)$ ,

3.  $(-a)(-b) = ab$ .

---

18.9 Definition For rings  $R$  and  $R'$ , a map  $\varphi: R \rightarrow R'$  is a homomorphism if the following two conditions are satisfied for all  $a, b \in R$ :

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

---

18.10 Example For each  $a \in R$ , we have the evaluation homomorphism  $\varphi_a: F \rightarrow R$ , where  $\varphi_a(f) = f(a)$   $f \in F$ .

---

18.11 Example The map  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ , where  $\varphi(a)$  is the remainder of  $a$  modulo  $n$  is a ring homomorphism for each positive integer  $n$ .



---

18.12 Definition An isomorphism  $\varphi: R \rightarrow R'$  from a ring  $R$  to a ring  $R'$  is a that is one to one and onto  $R'$ . The rings  $R$  and  $R'$  are then isomorphic (同构).

---

18.13 Example As abelian groups  $\langle \mathbb{Z}, + \rangle$  and  $\langle 2\mathbb{Z}, + \rangle$  are isomorphic under the map  $\varphi: \mathbb{Z} \rightarrow 2\mathbb{Z}$ , with  $\varphi(x) = 2x$  for  $x \in \mathbb{Z}$ .

But  $\varphi$  is not a ring isomorphism, for  $\varphi(xy) = 2xy$  while  $\varphi(x) \varphi(y) = 2x2y = 4xy$ .

---

18.14 Definition A ring in which the multiplication is **commutative**(交换) is a commutative ring. A ring with a multiplicative identity element is a ring with **unity**(有一的环, 幺环); the multiplicative identity element 1 is called **unity**(幺元, 单位元).

$$(1+1+\cdots+1)(1+1+\cdots+1)=1+1+\cdots+1$$

$$(n \cdot 1)(m \cdot 1) = (nm) \cdot 1$$

---

**18.15 Example** We claim that for integers  $r$  and  $s$  where  $\gcd(r,s)=1$ , the rings  $Z_{rs}$  and  $Z_r \times Z_s$  are isomorphic. Additively, they are both cyclic abelian groups of order  $rs$  with generators 1 and  $(1, 2)$  respectively. Thus  $\varphi: Z_{rs} \rightarrow Z_r \times Z_s$ , defined by  $\varphi: (n \cdot 1) = n(1, 1)$  is an ring isomorphism.

$$\varphi: (nm) = (nm) (1, 1) = [n(1, 1)] [m(1, 1)] = \varphi(n) \varphi(m)$$

---

**Note** In a ring  $R$  with unity  $1 \neq 0$ , the set  $R^*$  of nonzero elements, if closed under the ring multiplication, will be a multiplicative group if multiplicative inverses exist.

A **multiplicative inverse** of an element  $a$  in a ring  $R$  with unity  $1 \neq 0$  is an element  $a^{-1} \in R$  such that  $aa^{-1} = a^{-1}a = 1$ .

---

**18.16 Definition** Let  $R$  be a ring with unity  $1 \neq 0$ . An element  $u$  in  $R$  is a unit of  $R$  if it has a multiplicative inverse in  $R$ . If every non zero element of  $R$  is a unit, then  $R$  is a division **ring (除环 or skew field)**. A **field(域)** is a commutative division ring. A noncommutative division ring is called a **strictly skew field**.

---

18.17 Example Let us find the units in  $Z_{14}$ . Of course, 1 and  $-1=13$  are units. Since  $(3)(5)=1$  we see that 3 and 5 are units; therefore  $-3=11$  and  $-5=9$  are also units.

None of the remaining elements of  $Z_{14}$  can be units, since no multiple of 2, 4, 6, 7, 8, or 10 can be one more than a multiple of 14.

---

18.18 Example  $\mathbb{Z}$  is not a field, because 2, for example, has no multiplicative inverse, so 2 is not a unit.

However,  $\mathbb{Q}$  and  $\mathbb{R}$  are fields.



---

**Definition** A **subring**(子环) of a ring is a subset of the ring that is a ring under induced operations from the whole ring; a **subfield** (子域) is defined similarly for a subset of a field.



# Abstract Algebra

---

---

---

---

---

---

---



---

19.7 Example  $\mathbb{Z}$  and  $\mathbb{Z}_p$ , for any prime  $p$  are integral domains.

$\mathbb{Z}_p$ , is not an integral domain if  $p$  is not prime.

The direct product  $R \times S$  of two nonzero rings  $R$  and  $S$  is not an integral domain. (for  $r \in R$  and  $s \in S$  both nonzero, we have  $(r,0)(0,s)=(0,0)$ . )

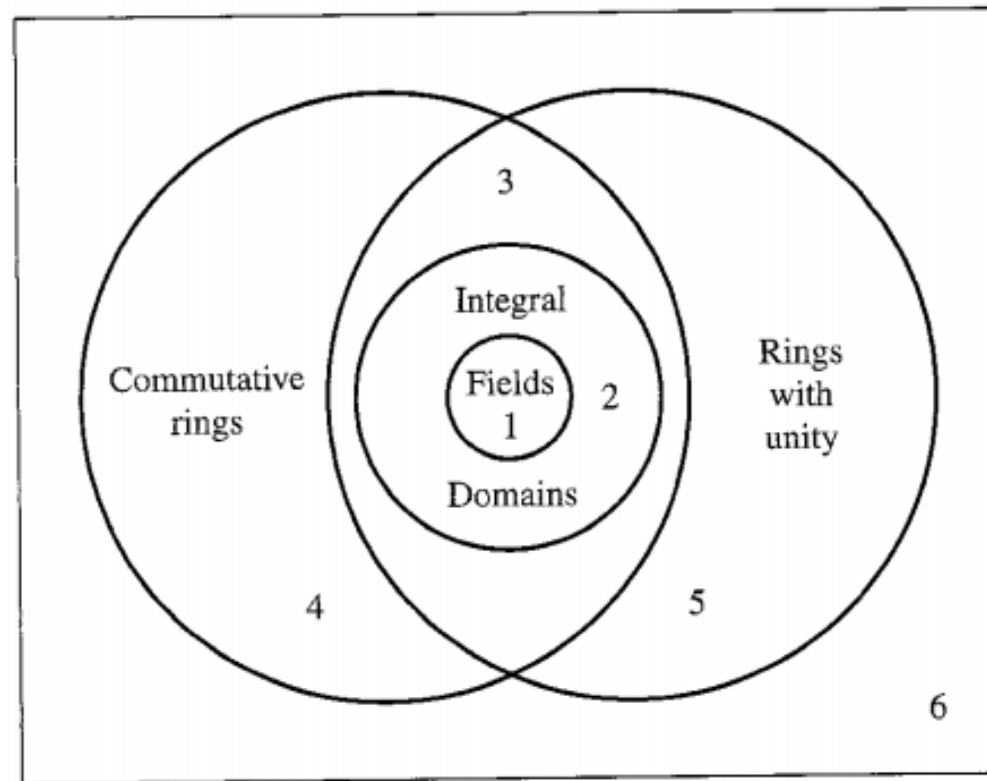
---

19.8 Example Show that although  $Z_2$  is an integral domain, the matrix ring  $M_2(Z_2)$  has divisors of zero.

---

19.9 Theorem Every field  $F$  is an integral domain.

Venn diagram



**19.10 Figure** A collection of rings.

---

19.11 Theorem Every finite integral domain is a field.

---

19.12 Corollary If  $p$  is a prime, then  $Z_p$  is a field..

---

**19.13 Definition** If for a ring  $R$  a positive integer  $n$  exists such that  $n \cdot a = 0$  for all  $a \in R$ , then the least such positive integer is the characteristic of the ring  $R$ . If no such positive integer exists, then  $R$  is of characteristic 0. ( $n \cdot a = a + a + \dots + a$ )

**19.14 Example** The ring  $Z_n$  is of characteristic  $n$ , while  $Z, Q, R$  and  $C$  all have characteristic 0.

---

**19.15 Theorem** Let  $R$  be a ring with unity. If  $n \cdot 1 \neq 0$  for all  $n \in \mathbb{Z}^+$ , then  $R$  has characteristic 0. If  $n \cdot 1 = 0$  for some  $n \in \mathbb{Z}^+$ , then the smallest such integer  $n$  is the characteristic of  $R$ .





# Abstract Algebra

---

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**Lemma** For any field, the nonzero elements form a group under the field multiplication.

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.1 Theorem (Little Theorem of Fermat)** If  $a \in \mathbb{Z}$  and  $p$  is a prime not dividing  $a$ , then  $p$  divides  $a^{p-1}-1$ , that is,  $a^{p-1} \equiv 1 \pmod{p}$  for  $a \not\equiv 0 \pmod{p}$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

20.2 Corollary If  $a \in \mathbb{Z}$ , then  $a^p \equiv a \pmod{p}$  for any prime  $p$ .

---

**20.3 Example** Let us compute the remainder of  $8^{103}$  when divided by 13.

**Solution** Using Fermat's theorem, we have

$$\begin{aligned} 8^{103} &\equiv (8^{12})^8 (8^7) \equiv (1^8) (8^7) \equiv 8^7 \equiv (-5)^7 \equiv ((-5)^2)^3 (-5) \\ &\equiv (25)^3 (-5) \equiv (-1)^3 (-5) \equiv 5 \equiv (\text{mod } 13). \end{aligned}$$

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**Solution** By Fermat's theorem,

$$2^{10} \equiv 1 \pmod{11},$$

$$\text{so } 2^{11213}-1 \equiv [(2^{10})^{1121} \cdot 2^3]-1 \equiv [1^{1121} \cdot 2^3]-1 \equiv 2^3-1 \equiv 8-1 \equiv 7 \pmod{11}.$$

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.5 Example** Show that for every integer  $n$ , the number  $n^{33}-n$  is divisible by 15.

**Solution** Note that  $n^{33}-n = n(n^{32}-1)$ .

If 3 divides  $n$ , then surely 3 divides  $n(n^{32}-1)$ . If 3 does not divide  $n$ , then by Fermat's theorem,  $n^2 \equiv 1 \pmod{3}$  so

$$n^{32}-1 \equiv (n^2)^{16}-1 \equiv 1^{16}-1 \equiv 0 \pmod{3},$$

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.5 Example** Show that for every integer  $n$ , the number  $n^{33}-n$  is divisible by 15.

**Solution** Note that  $n^{33}-n = n(n^{32}-1)$ .

If 5 divides  $n$ , then surely 5 divides  $n(n^{32}-1)$ . If 5 does not divide  $n$ , then by Fermat's theorem,  $n^4 \equiv 1 \pmod{5}$  so

$$n^{32}-1 \equiv (n^4)^8-1 \equiv 1^8-1 \equiv 0 \pmod{5},$$



# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**Lemma** For any field, the nonzero elements form a group under the field multiplication.

**20.6 Theorem** The set  $G$ , of nonzero elements of  $\mathbb{Z}_p$  that are not 0 divisors forms a group under multiplication modulo  $n$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**Definition** Let  $\varphi(n)$  be defined as the number of positive integers less than or equal to  $n$  and relatively prime to  $n$ . This function  $\varphi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  is the **Euler phi-function**.

Note that  $\varphi(1)=1$ .

**20.7 Example** Let  $n = 12$ . The positive integers less than or equal to 12 and relatively prime to 12 are 1, 5, 7 and 11,  $\varphi(12)=4$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

20.8 Theorem (Euler's Theorem) If  $a$  is an integer relatively prime to  $n$ , then  $a^{\varphi(n)} - 1$  is divisible by  $n$ , that is,  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

20.8 Theorem (Euler's Theorem) If  $a$  is an integer relatively prime to  $n$ , then  $a^{\varphi(n)} \equiv 1 \pmod{n}$ , that is,  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .  
应该是  $a^{\varphi(n)} \equiv 1 \pmod{n}$

20.1 Theorem (Little Theorem of Fermat) If  $a \in \mathbb{Z}$  and  $p$  is a prime not dividing  $a$ , then  $p$  divides  $a^{p-1} - 1$ , that is,  $a^{p-1} \equiv 1 \pmod{p}$  for  $a \not\equiv 0 \pmod{p}$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.9 Example** If  $a$  is relatively prime to 12, then  $a^4 \equiv 1 \pmod{12}$ .  
For example, with  $a=7$ , we have  $7^4 \equiv 1 \pmod{12}$

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.10 Theorem** Let  $m$  be a positive integer and let  $a \in \mathbb{Z}_m$  be relatively prime to  $m$ . For each  $b \in \mathbb{Z}_m$ , the equation  $ax=b$  has a unique solution in  $\mathbb{Z}_m$ .

**20.11 Corollary** If  $a$  and  $m$  are relatively prime integers, then for any integer  $b$ , the congruence  $ax \equiv b \pmod{m}$  has as solutions all integers in precisely one residue class modulo  $m$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.12 Theorem** Let  $m$  be a positive integer and let  $a, b \in \mathbb{Z}_m$ . Let  $d$  be the gcd of  $a$  and  $m$ . The equation  $ax=b$  has a solution in  $\mathbb{Z}_m$  if and only if  $d$  divides  $b$ . When  $d$  divides  $b$ , the equation has exactly  $d$  solutions in  $\mathbb{Z}_m$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.13 Corollary** Let  $d$  be the gcd of positive integers  $a$  and  $m$ . The congruence  $ax \equiv b \pmod{m}$  has a solution if and only if  $d$  divides  $b$ . When this is the case, the solutions are the integers in exactly  $d$  distinct residue classes modulo  $m$ .



# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

**20.13 Corollary** Let  $d$  be the gcd of positive integers  $a$  and  $m$ . The congruence  $ax \equiv b \pmod{m}$  has a solution if and only if  $d$  divides  $b$ . When this is the case, the solutions are the integers in exactly  $d$  distinct residue classes modulo  $m$ .

**20.11 Corollary** If  $a$  and  $m$  are relatively prime integers, then for any integer  $b$ , the congruence  $ax \equiv b \pmod{m}$  has as solutions all integers in precisely one residue class modulo  $m$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

20.14 Example Find all solutions of the congruence  $12x \equiv 27 \pmod{18}$ .

# SECTION 20: FERMAT'S AND EULER'S THEOREMS

---

20.15 Example Find all solutions of the congruence  $15x \equiv 27 \pmod{18}$ .



# Abstract Algebra

---

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

Let  $D$  be an integral domain that we desire to enlarge to a field of quotients  $F$ .

1. Define what the elements of  $F$  are to be.
2. Define the binary operations of addition and multiplication on  $F$ .
3. Check all the field axioms to show that  $F$  is a field under these operations.
4. Show that  $F$  can be viewed as containing  $D$  as an integral subdomain.

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**Step 1** Let  $D$  be a given integral domain, and form the Cartesian product  $D \times D = \{(a, b) | a, b \in D\}$ .

Let  $S$  be the subset of  $D \times D$  given by  $S = \{(a, b) | a, b \in D, b \neq 0\}$ .

**21.1 Definition** Two elements  $(a, b)$  and  $(c, d)$  in  $S$  are equivalent, denoted by  $(a, b) \sim (c, d)$ , if and only if  $ad = bc$ .

**21.2 Lemma** The relation  $\sim$  between elements of the set  $S$  as just described is an equivalence relation.

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**21.2 Lemma** The relation  $\sim$  between elements of the set  $S$  as just described is an equivalence relation.

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**21.2 Lemma** The relation  $\sim$  between elements of the set  $S$  as just described is an equivalence relation.

Define  $F$  to be the set of all equivalence classes  $[(a,b)]$  for  $(a,b) \in S$ .



# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**Step 2** Define operations of addition and multiplication on  $F$ .

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$

$$\text{and } [(a,b)][(c,d)] = [(ac, bd)]$$

**21.3 Lemma** The operations is well-defined operations of addition and multiplication on  $F$ .

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**21.3 Lemma** The operations is well-defined operations of addition and multiplication on  $F$ .

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$

$$\text{and } [(a,b)][(c,d)] = [(ac, bd)]$$

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**Step 3**  $F$  is a field.

1. Addition in  $F$  is commutative.
2. Addition is associative.
3.  $[(0,1)]$  is an identity element for addition in  $F$ .
4.  $[(-a,b)]$  is an additive inverse for  $[(a,b)]$  in  $F$ .

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**Step 3**  $F$  is a field.

5. Multiplication in  $F$  is associative.
6. Multiplication in  $F$  is commutative.
7. The distributive laws hold in  $F$ .
8.  $[(1,1)]$  is a multiplicative identity element in  $F$ .
9. If  $[(a,b)] \in F$  is not the additive identity element, then  $a \neq 0$  in  $D$  and  $[(b,a)]$  is a multiplicative inverse for  $[(a,b)]$ .

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**21.4 Lemma** The map  $i:D\rightarrow F$  given by  $i(a)=[(a,1)]$  is an isomorphism of  $D$  with a subring of  $F$ .

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**21.5 Theorem** Any integral domain  $D$  can be enlarged to (or embedded in) a field  $F$  such that every element of  $F$  can be expressed as a quotient of two elements of  $D$ . (Such a field  $F$  is a **field of quotients of (分式域)**  $D$ .)

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**21.6 Theorem** Let  $F$  be a field of quotients of  $D$  and let  $L$  be any field containing  $D$ . Then there exists a map  $\psi: F \rightarrow L$  that gives an isomorphism of  $F$  with a subfield of  $L$  such that  $\psi(a) = a$  for  $a \in D$ .

# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---

**21.8 Corollary** Every field  $L$  containing an integral domain  $D$  contains a field of quotients of  $D$ .



# SECTION 21: THE FIELD OF QUOTIENTS OF AN INTEGRAL DOMAIN

---



# Abstract Algebra

---

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.1 Definition** Let  $R$  be a ring. A polynomial  $f(x)$  with coefficients in  $R$  is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \dots + a_n x^n + \dots$$

where  $a \in R$  and  $a_i = 0$  for all but a finite number of values of  $i$ .

The  $a_i$  are **coefficients** of  $f(x)$ . If for some  $i \geq 0$  it is true that  $a_i \neq 0$ , the largest such value of  $i$  is the **degree** of  $f(x)$ . If all  $a_i = 0$ , then the degree of  $f(x)$  is undefined.

# SECTION 22: RINGS OF POLYNOMIALS

---

Let  $f(x)=a_0+a_1x+\cdots+a_nx^n+\cdots$

and  $g(x)=b_0+b_1x+\cdots+b_nx^n+\cdots$ .

## Addition

$f(x)+g(x)=c_0+c_1x+\cdots+c_nx^n+\cdots$ , where  $c_n=a_n+b_n$ .

## Multiplication

$f(x)g(x)=d_0+d_1x+\cdots+d_nx^n+\cdots$ , where  $d_n=\sum_{i=0}^n a_ib_{n-i}$ .

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.2 Theorem** The set  $R[x]$  of all polynomials in an indeterminate  $x$  with coefficients in a ring  $R$  is a ring under polynomial addition and multiplication. If  $R$  is commutative, then so is  $R[x]$ , and if  $R$  has unity  $1 \neq 0$ , then  $1$  is also unity for  $R[x]$ .

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.3 Example** In  $Z_2[x]$ , we have

$$(x + 1)^2 = (x + 1)(x + 1) = x^2 + (1+1)x + 1 = x^2 + 1.$$

Still working in  $Z_2[x]$ , we obtain

$$(x + 1) + (x + 1) = (x + 1)x + (1 + 1) = 0x + 0 = 0.$$

# SECTION 22: RINGS OF POLYNOMIALS

---

**Definition** Let  $R[x,y]=R[x][y]$  the ring of polynomials in two indeterminates  $x$  and  $y$  with coefficients in  $R$ . The ring  $R[x_1, x_2, \dots, x_n]$  of polynomials in the  $n$  indeterminates  $x_i$  with coefficients in  $R$  is similarly defined.

## SECTION 22: RINGS OF POLYNOMIALS

---

**Fact** If  $D$  is an integral domain then so is  $D[x]$ . In particular, if  $F$  is a field, then  $F[x]$  is an integral domain **but not** a field.

We similarly define  $F(x_1, x_2, \dots, x_n)$  to be the field of quotients of  $F[x_1, x_2, \dots, x_n]$ . This field  $F(x_1, x_2, \dots, x_n)$  is the field of **rational functions** in  $n$  indeterminates over  $F$ .



# SECTION 22: RINGS OF POLYNOMIALS

---

**22.4 Theorem** (The Evaluation Homomorphisms for Field Theory) Let  $F$  be a subfield of a field  $E$ , let  $\alpha$  be any element of  $E$ , and let  $x$  be an indeterminate. The map  $\phi_\alpha: F[x] \rightarrow E$  defined by

$\phi_\alpha(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ , for  $(a_0 + a_1x + \cdots + a_nx^n) \in F[x]$  is a homomorphism of  $F[x]$  into  $E$ .

Also,  $\phi_\alpha(x) = \alpha$ , and  $\phi_\alpha(a) = a$ .

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.6 Example** Let  $F$  be  $Q$  and  $E$  be  $R$  in Theorem 22.4, and consider the evaluation homomorphism

$$\phi_0: Q[x] \rightarrow R.$$

Here

$$\phi_0(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\mathbf{0} + \cdots + a_n\mathbf{0}^n = a_0.$$

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.7 Example** Let  $F$  be  $Q$  and  $E$  be  $R$  in Theorem 22.4, and consider the evaluation homomorphism

$$\phi_2: Q[x] \rightarrow R.$$

Here

$$\phi_2(x^2+x-6) = 2^2+2-6=0.$$

Thus  $x^2+x-6$  is in the kernel of  $\phi_2$ .

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.8 Example** Let  $F$  be  $\mathcal{Q}$  and  $E$  be  $\mathcal{C}$  in Theorem 22.4, and consider the evaluation homomorphism

$$\phi_i: \mathcal{Q}[x] \rightarrow \mathcal{C}.$$

Here

$$\phi_i(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1i + \cdots + a_ni^n.$$

$$\phi_i(x) = i.$$

$$\phi_i(x^2 + 1) = i^2 + 1 = 0,$$

so  $x^2 + 1$  is in the kernel  $\phi_i$ .

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.9 Example** Let  $F$  be  $Q$  and  $E$  be  $R$  in Theorem 22.4, and consider the evaluation homomorphism

$$\phi_\pi: Q[x] \rightarrow R.$$

Here

$$\phi_\pi(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\pi + \cdots + a_n\pi^n.$$

It can be proved that  $a_0 + a_1\pi + \cdots + a_n\pi^n = 0$  if and only if  $a_i = 0$  for  $i = 0, 1, \dots, n$ . Thus the kernel of  $\phi_\pi$  is  $\{0\}$ , and  $\phi_\pi$  is a one-to-one map. so  $x^2+1$  is in the kernel  $\phi_i$ .

## SECTION 22: RINGS OF POLYNOMIALS

---

**22.10 Definition** Let  $f(x)=a_0+a_1x+\cdots+a_nx^n$  be in  $F[x]$ , and let  $\phi_\alpha:F[x]\rightarrow E$  be the evaluation homomorphism of Theorem 22.4. Let  $f(\alpha)$  denote

$$\phi_\alpha(f(x))=a_0+a_1\alpha+\cdots+a_n\alpha^n.$$

If  $f(\alpha)=0$ , then  $\alpha$  is a **zero** of  $f(x)$ .

# SECTION 22: RINGS OF POLYNOMIALS

---

**22.11 Theorem** The polynomial  $x^2-2$  has no zeros in the rational numbers. Thus  $\sqrt{2}$  is not a rational number.



# Abstract Algebra

---



# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.1 Definition (Division Algorithm for  $F[x]$ )** Let  $R$  be a ring. A polynomial  $f(x)$  with coefficients in  $R$  is an infinite formal sum  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$  and  $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$  be two elements of  $F[x]$ , with  $a_n$  and  $b_m$  both nonzero elements of  $F$  and  $m > 0$ . Then there are unique polynomials  $q(x)$  and  $r(x)$  in  $F[x]$  such that  $f(x) = g(x)q(x) + r(x)$ , where either  $r(x) = 0$  or the degree of  $r(x)$  is less than the degree  $m$  of  $g(x)$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.2 Example** Let us work with polynomials in  $Z_5[x]$  and divide  $f(x)=x^4-3x^3+2x^2+4x-1$  by  $g(x)=x^2-2x+3$  to find  $q(x)$  and  $r(x)$  of Theorem 23.1.

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.3 Corollary (Factor Theorem)** An element  $a \in F$  is a zero of  $f(x) \in F[x]$  if and only if  $x-a$  is a factor of  $f(x)$  in  $F[x]$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.4 Example** Working again in  $Z_5[x]$ , note that 1 is a zero of  $f(x)=x^4+3x^3+2x+4$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.5 Corollary** A nonzero polynomial  $f(x) \in F[x]$  of degree  $n$  can have at most  $n$  zeros in a field  $F$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.6 Corollary** If  $G$  is a finite subgroup of the multiplicative group  $\langle F^*, \cdot \rangle$  of a field  $F$ , then  $G$  is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.7 Definition** A nonconstant polynomial  $f(x) \in F[x]$  is irreducible over  $F$  or is an **irreducible polynomial** in  $F[x]$  if  $f(x)$  cannot be expressed as a product  $g(x)h(x)$  of two polynomials  $g(x)$  and  $h(x)$  in  $F[x]$  both of lower degree than the degree of  $f(x)$ . If  $f(x) \in F[x]$  is a nonconstant polynomial that is not irreducible over  $F$ , then  $f(x)$  is **reducible** over  $F$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.8 Example** Theorem 22.11 shows that  $x^2-2$  viewed in  $Q[x]$  has no zeros in  $Q$ . This shows that  $x^2-2$  is irreducible over  $Q$ . However,  $x^2-2$  viewed in  $R[x]$  is not irreducible over  $R$ .



# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

23.9 Example  $f(x)=x^3+3x+2$  viewed in  $Z_5[x]$  is irreducible over  $Z_5$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.10 Theorem** Let  $f(x) \in F[x]$ , and let  $f(x)$  be of degree 2 or 3. Then  $f(x)$  is reducible over  $F$  if and only if it has a zero in  $F$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.11 Theorem** If  $f(x) \in \mathbb{Z}[x]$ , then  $f(x)$  factors into a product of two polynomials of lower degrees  $r$  and  $s$  in  $\mathbb{Q}[x]$  if and only if it has such a factorization with polynomials of the same degrees  $r$  and  $s$  in  $\mathbb{Z}[x]$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.11 Theorem** If  $f(x) \in Z[x]$ , then  $f(x)$  factors into a product of two polynomials of lower degrees  $r$  and  $s$  in  $Q[x]$  if and only if it has such a factorization with polynomials of the same degrees  $r$  and  $s$  in  $Z[x]$ .

**23.12 Corollary** If  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  is in  $Z[x]$  with  $a_0 \neq 0$ , and if  $f(x)$  has a zero in  $Q$ , then it has a zero  $m$  in  $Z$ , and  $m$  must divide  $a_0$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.13 Example** Corollary 23.12 gives us another proof of the irreducibility of  $x^2-2$  over  $\mathbb{Q}$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

23.14 Example Let us use Theorem 23.11 to show that

$f(x) = x^4 - 2x^2 + 8x + 1$  viewed in  $\mathbb{Q}[x]$  is irreducible over  $\mathbb{Q}$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.15 Theorem (Eisenstein Criterion)** Let  $p \in \mathbb{Z}$  be a prime. Suppose that  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$  is in  $\mathbb{Z}[x]$ , and  $a_n \not\equiv 0 \pmod{p}$ , but  $a_i \equiv 0 \pmod{p}$  for all  $i < n$ , with  $a_0 \not\equiv 0 \pmod{p^2}$ . Then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.16 Example** Taking  $p=3$ , we see by Theorem 23.15 that  $25x^5-9x^4-3x^2-12$  is irreducible over  $\mathbb{Q}$ .

**23.15 Theorem (Eisenstein Criterion)** Let  $p \in \mathbb{Z}$  be a prime. Suppose that  $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$  is in  $\mathbb{Z}[x]$ , and  $a_n \not\equiv 0 \pmod{p}$ , but  $a_i \equiv 0 \pmod{p}$  for all  $i < n$ , with  $a_0 \not\equiv 0 \pmod{p^2}$ . Then  $f(x)$  is irreducible over  $\mathbb{Q}$ .



# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

23.17 Corollary The polynomial

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over  $\mathbb{Q}$  for any prime  $p$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.18 Theorem** Let  $p(x)$  be an irreducible polynomial in  $F[x]$ . If  $p(x)$  divides  $r(x)s(x)$  for  $r(x), s(x) \in F[x]$ , then either  $p(x)$  divides  $r(x)$  or  $p(x)$  divides  $s(x)$ .

**23.19 Corollary** If  $p(x)$  is irreducible in  $F[x]$  and  $p(x)$  divides the product  $r_1(x)r_2(x) \dots r_n(x)$  for  $r_i(x) \in F[x]$ , then  $p(x)$  divides  $r_i(x)$  for at least one  $i$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

**23.20 Theorem** If  $F$  is a field, then every nonconstant polynomial  $f(x) \in F[x]$  can be factored in  $F[x]$  into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit (that is, nonzero constant) factors in  $F$ .

# SECTION 23: FACTORIZATION OF POLYNOMIALS OVER A FIELD

---

23.21 Example A factorization of  $x^4+3x^3+2x+4$  in  $Z_5[x]$  is  $(x-1)^3(x+1)$ .

$$(x-1)^3(x+1)=(x-1)^2(2x-2)(3x+3).$$



# Abstract Algebra

---

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.1 Definition** A map  $\phi$  of a ring  $R$  into a ring  $R'$  is a **homomorphism (同态)** if

$$\phi(a+b) = \phi(a) + \phi(b)$$

and

$$\phi(ab) = \phi(a) \phi(b)$$

for all elements  $a$  and  $b$  in  $R$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.2 Example (Projection Homomorphisms)** Let  $R_1, R_2, \dots, R_n$  be rings. For each  $i$ , the map  $\pi_i: R_1 \times R_2 \times \dots \times R_n \rightarrow R_i$  defined by  $\pi_i(r_1, r_2, \dots, r_n) = r_i$  is a homomorphism, projection onto the  $i$ th component.

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.3 Theorem (Analogue of Theorem 13.12)** Let  $\phi$  be a homomorphism of a ring  $R$  into a ring  $R'$ . If  $0$  is the additive identity in  $R$ , then  $\phi(0)=0'$  is the additive identity in  $R'$ , and if  $a \in R$ , then  $\phi(-a)=-\phi(a)$ . If  $S$  is a subring of  $R$ , then  $\phi[S]$  is a subring of  $R'$ . Going the other way, if  $S'$  is a subring of  $R'$ , then  $\phi^{-1}[S']$  is a subring of  $R$ . Finally, if  $R$  has unity  $1$ , then  $\phi(1)$  is unity for  $\phi[R]$ . Loosely speaking, subrings correspond to subrings, and rings with unity correspond to rings with unity under a ring homomorphism.



# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.4 Definition** Let a map  $\phi: R \rightarrow R'$  be a homomorphism of rings. The subring  $\phi^{-1}[0] = \{r \in R \mid \phi(r) = 0\}$  is the **kernel (核)** of  $\phi$ , denoted by  $\text{Ker}(\phi)$

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.5 Theorem (Analogue of Theorem 13.15)** Let a map  $\phi: R \rightarrow R'$  be a homomorphism of rings, and let  $H = \text{Ker}(\phi)$ . Then  $\phi^{-1}[\phi[a]] = a + H = H + a$ , where  $a + H = H + a$  is the coset containing  $a$  of the commutative additive group  $\langle H, + \rangle$ .

**13.15 Theorem** Let  $\phi: G \rightarrow G'$  be a group homomorphism, and let  $H = \text{Ker}(\phi)$ . Let  $a \in G$ . Then the set

$$\phi^{-1}[\phi(a)] = \{x \in G \mid \phi(x) = \phi(a)\}$$

is the left coset  $aH$  of  $H$ , and is also the right coset  $Ha$  of  $H$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

26.6 Corollary (Analogue of Corollary 13.18) A ring homomorphism  $\phi: R \rightarrow R'$  is a one-to-one map if and only if  $\text{Ker}(\phi) = \{0\}$ .

13.18 Corollary A group homomorphism  $\phi: G \rightarrow G'$  is a one-to-one map if and only if  $\text{Ker}(\phi) = \{e\}$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.7 Theorem (Analogue of Theorem 14.1)** Let  $\phi: R \rightarrow R'$  be a ring homomorphism with kernel  $H$ . Then the additive cosets of  $H$  form a ring  $R/H$  whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by

$$(a+H)+(b+H)=(a+b)$$

and the product of the cosets is defined by

$$(a+H)(b+H)=(ab)+H.$$

Also, the map  $\mu: R/H \rightarrow \phi[R]$  defined by  $\mu(a+H)=\phi(a)$  is an isomorphism.

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**14.1 Theorem** Let  $\varphi: G \rightarrow G'$  be a group homomorphism with kernel  $H$ . Then the cosets of  $H$  form a **factor group**,  $G/H$ , where  $(aH)(bH) = (ab)H$ . Also the map  $\mu: G/H \rightarrow \varphi[G]$  defined by  $\mu(aH) = \varphi(a)$  is an isomorphism. Both coset multiplication and  $\mu$  are well defined, independent of the choices  $a$  and  $b$  from the cosets.

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.8 Example** The map  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$  defined by  $\phi(m)=r$ , where  $r$  is the remainder of  $m$  when divided by  $n$ , is a homomorphism. Since  $\text{Ker}(\phi) = n\mathbb{Z}$ . Theorem 26.7 shows that  $\mathbb{Z}/n\mathbb{Z}$  is a ring where operations on residue classes can be computed by choosing representatives and performing the corresponding operation in  $\mathbb{Z}$ . The theorem also shows that this ring  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to  $\mathbb{Z}_n$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

26.9 Theorem (Analogue of Theorem 14.4) Let  $H$  be a subring of the ring  $R$ . Multiplication of additive cosets of  $H$  is well defined by the equation  $(a+H)(b+H)=(ab)+H$ .

if and only if  $ah \in H$  and  $hb \in H$  for all  $a, b \in R$  and  $h \in H$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.10 Definition** An additive subgroup  $N$  of a ring  $R$  satisfying the properties

$$aN \in N \text{ and } Nb \in N \text{ for all } a, b \in R$$

is an **ideal (理想)**.



# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.11 Example** We see that  $nZ$  is an ideal in the ring  $Z$  since we know it is a subring, and  $s(nm)=(nm)s = n(ms) \in nZ$  for all  $s \in Z$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.12 Example** Let  $F$  be the ring of all functions mapping  $R$  into  $R$ , and let  $C$  be the subring of  $F$  consisting of all the constant functions in  $F$ . Is  $C$  an ideal in  $F$  or Why?

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.13 Example** Let  $F$  be the ring of all functions mapping  $R$  into  $R$ , and let  $N$  be the subring of all functions  $f$  such that  $f(2)=0$ . Is  $N$  an ideal in  $F$ ? Why or why not?

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

**26.14 Corollary** (Analogue of Corollary 14.5) Let  $N$  be an ideal of a ring  $R$ . Then the additive cosets of  $N$  form a ring  $R/N$  with the binary operations defined by

$$(a + N) + (b + N) = (a + b) + N$$

and

$$(a + N)(b + N) = ab + N.$$

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

26.15 Definition The ring  $R/N$  in the preceding corollary is the **factor ring** (or **quotient ring**, 商环) of  $R$  by  $N$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

26.16 Theorem (Analogue of Theorem 14.9) Let  $N$  be an ideal of a ring  $R$ . Then  $\gamma: R \rightarrow R/N$  given by  $\gamma(x) = x + N$  is a ring homomorphism with kernel  $N$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

26.17 Theorem (Fundamental Homomorphism Theorem; Analogue of Theorem 14.11) Let  $\phi: R \rightarrow R'$  be a ring homomorphism with kernel  $N$ . Then  $\phi[R]$  is a ring, and the map  $\mu: R/N \rightarrow \phi[R]$  given by  $\mu(x+N) = \phi(x)$  is an isomorphism. If  $\gamma: R \rightarrow R/N$  is the homomorphism given by  $\gamma(x) = x+N$ , then for each  $x \in R$ , we have  $\phi(x) = \mu\gamma(x)$ .

# SECTION 26: HOMOMORPHISMS AND FACTOR RINGS

---

26.19 Example If  $\mu: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$  is an isomorphism.





# Abstract Algebra

---

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

27.1 Example A factor ring of an integral domain may be a field.

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p.$$

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.2 Example** A factor ring of a ring may be an integral domain, even though the original ring is not.  $(\mathbb{Z} \times \mathbb{Z})/N$ , where  $N = \{(0, n) | n \in \mathbb{Z}\}$

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.3 Example** If  $R$  is not even an integral domain, that is, if  $R$  has zero divisors, it is still possible for  $R/N$  to be a field.  $\mathbb{Z}_6/N$ , where  $N = \{0, 3\}$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

27.4 Example The structure of a factor ring may seem worse than that of the original ring.  $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.5 Theorem** If  $R$  is a ring with unity, and  $N$  is an ideal of  $R$  containing a unit, then  $N=R$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

27.6 Corollary A field contains no proper nontrivial ideals.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.7 Definition** A **maximal ideal**(极大理想) of a ring  $R$  is an ideal  $M$  different from  $R$  such that there is no proper ideal  $N$  of  $R$  properly containing  $M$ .



# SECTION 27: PRIME AND MAXIMAL IDEALS

---

27.8 Example If  $p$  is prime,  $pZ$  is a maximal ideal of  $Z$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.9 Theorem**(Analogue of Theorem 15.18) Let  $R$  be a commutative ring with unity. Then  $M$  is a maximal ideal of  $R$  if and only if  $R/M$  is a field.

**15.18 Theorem**  $M$  is a maximal normal subgroup of  $G$  if and only if  $G/M$  is simple.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.10 Example** Since  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to  $\mathbb{Z}_n$ , and  $\mathbb{Z}_n$  is a field if and only if  $n$  is a prime, we see that the maximal ideals of  $\mathbb{Z}$  are precisely the ideals  $p\mathbb{Z}$  for prime positive integers  $p$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.11 Corollary** A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.13 Definition** An ideal  $N \neq R$  in a commutative ring  $R$  is a prime ideal if  $ab \in N$  implies that either  $a \in N$  or  $b \in N$  for  $a, b \in R$ .

**Note**  $\{0\}$  is a prime ideal in  $\mathbb{Z}$ , and indeed, in any integral domain.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

27.14 Example  $\mathbb{Z} \times \{0\}$  is a prime ideal of  $\mathbb{Z} \times \mathbb{Z}$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.15 Theorem** Let  $R$  be a commutative ring with unity, and let  $N \neq R$  be an ideal in  $R$ . Then  $R/N$  is an integral domain if and only if  $N$  is a prime ideal in  $R$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.16 Corollary** Every maximal ideal in a commutative ring  $R$  with unity is a prime ideal.



# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.17 Theorem** If  $R$  is a ring with unity  $1$ , then the map  $\phi: \mathbb{Z} \rightarrow R$  given by  $\phi(n) = n \cdot 1$  for  $n \in \mathbb{Z}$  is a homomorphism of  $\mathbb{Z}$  into  $R$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.18 Corollary** If  $R$  is a ring with unity and characteristic  $n > 1$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}_n$ . If  $R$  has characteristic 0, then  $R$  contains a subring isomorphic to  $\mathbb{Z}$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.19 Theorem** A field  $F$  is either of prime characteristic  $p$  and contains a subfield isomorphic to  $\mathbb{Z}_p$  or of characteristic 0 and contains a subfield isomorphic to  $\mathbb{Q}$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

27.20 Definition The fields  $\mathbb{Z}_p$  and  $\mathbb{Q}$  are prime fields.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.21 Definition** If  $R$  is a commutative ring with unity and  $a \in R$ , the ideal  $\{ra \mid r \in R\}$  of all multiples of  $a$  is the **principal ideal generated** by  $a$  and is denoted by  $\langle a \rangle$ . An ideal  $N$  of  $R$  is a **principal ideal (主理想)** if  $N = \langle a \rangle$  for some  $a \in R$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.22 Example** Every ideal of the ring  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$ , which is generated by  $n$ , so every ideal of  $\mathbb{Z}$  is a principal ideal.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.23 Example** The ideal  $\langle x \rangle$  in  $F[x]$  consists of all polynomials in  $F[x]$  having zero constant term.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

27.24 Theorem If  $F$  is a field, every ideal in  $F[x]$  is principal.



# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.25 Theorem** An ideal  $\langle p(x) \rangle \neq \{0\}$  of  $F[x]$  is maximal if and only if  $p(x)$  is irreducible over  $F$ .

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.26 Example** Example 23.9 shows that  $x^3+3x+2$  is irreducible in  $Z_5[x]$ , so  $Z_5[x]/\langle x^3+3x+2 \rangle$  is a field. Similarly, Theorem 22.11 shows that  $x^2-2$  is irreducible in  $Q[x]$ , so  $Q[x]/\langle x^2-2 \rangle$  is a field. We shall examine such fields in more detail later.

# SECTION 27: PRIME AND MAXIMAL IDEALS

---

**27.27 Theorem** Let  $p(x)$  be an irreducible polynomial in  $F[x]$ . If  $p(x)$  divides  $r(x)s(x)$  for  $r(x), s(x) \in F[x]$ , then either  $p(x)$  divides  $r(x)$  or  $p(x)$  divides  $s(x)$ .



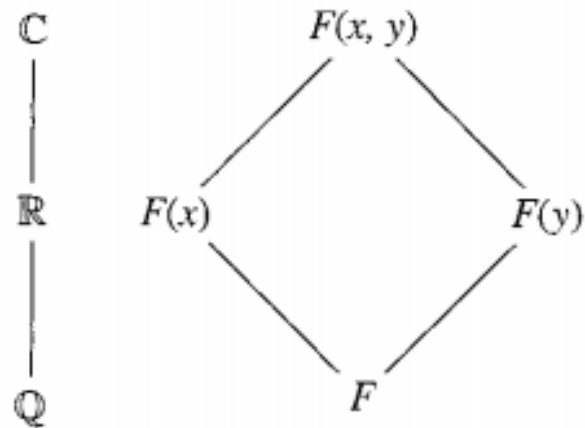
# Abstract Algebra

---

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.1 Definition** A field  $E$  is an extension field of a field  $F$  if  $F \leq E$ .



# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

29.3 Theorem (Kronecker's Theorem) (Basic Goal) Let  $F$  be a field and let  $f(x)$  be a nonconstant polynomial in  $F[x]$ . Then there exists an extension field  $E$  of  $F$  and an  $\alpha \in E$  such that  $f(\alpha)=0$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.4 Example** Let  $F=R$ , and let  $f(x)=x^2+1$ , which is well known to have no zeros in  $R$  and thus is irreducible over  $R$  by Theorem 23.10. Then  $\langle x^2+1 \rangle$  is a maximal ideal in  $R[x]$ , so  $R[x]/\langle x^2+1 \rangle$  is a field. Identifying  $r \in R$  with  $r + \langle x^2+1 \rangle$  in  $R[x]/\langle x^2+1 \rangle$ , we can view  $R$  as a subfield of  $E=R[x]/\langle x^2+1 \rangle$ . Let  $a=x+\langle x^2+1 \rangle$ .

Thus  $\alpha$  is a zero of  $x^2+1$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.5 Example** Let  $F=Q$ , and consider  $f(x)=x^4-5x^2+6$ . This time  $f(x)$  factors in  $Q[x]$  into  $(x^2-2)(x^2-3)$ , both factors being irreducible over  $Q$ , as we have seen. We can start with  $x^2-2$  and construct an extension field  $E$  of  $Q$  containing  $\alpha$  such that  $\alpha^2-2=0$ , or we can construct an extension field  $K$  of  $Q$  containing an element  $\beta$  such that  $\beta^2-3=0$ . The construction in either case is just as in Example 29.4.



# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.6 Definition** An element  $\alpha$  of an extension field  $E$  of a field  $F$  is algebraic over  $F$  if  $f(\alpha)=0$  for some nonzero  $f(x)\in F[x]$ . If  $\alpha$  is not algebraic over  $F$ , then  $\alpha$  is transcendental over  $F$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.7 Example**  $C$  is an extension field of  $Q$ . Since  $\sqrt{2}$  is a zero of  $x^2-2$ , we see that  $\sqrt{2}$  is an algebraic element over  $Q$ .

Also,  $i$  is an algebraic element over  $Q$ , being a zero of  $x^2+1$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.8 Example** It is well known (but not easy to prove) that the real numbers  $\pi$  and  $e$  are transcendental over  $\mathbb{Q}$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.9 Example** The real number  $\pi$  is transcendental over  $\mathbb{Q}$ , as we stated in Example 29.8. However,  $\pi$  is algebraic over  $\mathbb{R}$ , for it is a zero of  $(x - \pi) \in \mathbb{R}[x]$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.10 Example** It is easy to see that the real number  $\sqrt{1+\sqrt{3}}$  is algebraic over  $\mathbb{Q}$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.11 Definition** An element of  $C$  that is algebraic over  $Q$  is an **algebraic number**. A **transcendental number** is an element of  $C$  that is transcendental over  $Q$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.12 Theorem** Let  $E$  be an extension field of a field  $F$  and let  $\alpha \in E$ . Let  $\phi_\alpha: F[x] \rightarrow E$  be the evaluation homomorphism of  $F[x]$  into  $E$  such that  $\phi_\alpha(a) = a$  for  $a \in F$  and  $\phi_\alpha(x) = \alpha$ . Then  $\alpha$  is transcendental over  $F$  if and only if  $\phi_\alpha$  gives an isomorphism of  $F[x]$  with a subdomain of  $E$ , that is, if and only if  $\phi_\alpha$  is a one-to-one map.

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.13 Theorem** Let  $E$  be an extension field of a field  $F$ , and let  $\alpha \in E$ , where  $\alpha$  is algebraic over  $F$ . Then there is an irreducible polynomial  $p(x) \in F[x]$  such that  $p(\alpha) = 0$ . This irreducible polynomial  $p(x)$  is uniquely determined up to a constant factor in  $F$  and is a polynomial of minimal degree  $\geq 1$  in  $F[x]$  having  $\alpha$  as a zero. If  $f(\alpha) = 0$  for  $f(x) \in F[x]$ , with  $f(x) \neq 0$ , then  $p(x)$  divides  $f(x)$ .



# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.14 Definition** Let  $E$  be an extension field of a field  $F$ , and let  $\alpha \in E$ , where  $\alpha$  is algebraic over  $F$ . The unique monic polynomial  $p(x)$  having the property described in Theorem 29.13 is the irreducible polynomial for  $\alpha$  over  $F$  and will be denoted by  $\text{irr}(\alpha, F)$ . The degree of  $\text{irr}(\alpha, F)$  is the degree of  $\alpha$  over  $F$ , denoted by  $\deg(\alpha, F)$ .

**Definition** A polynomial having 1 as the coefficient of the highest power of  $x$  appearing is a **monic polynomial**.

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.15 Example** We know that  $\text{irr}(\sqrt{2}, Q) = x^2 - 2$ . Referring to Example 29.10, we see that for  $\alpha = \sqrt{1+\sqrt{3}}$  in  $R$ ,  $\alpha$  is a zero of  $x^4 - 2x^2 - 2$ , which is in  $Q[x]$ . Since  $x^4 - 2x^2 - 2$  is irreducible over  $Q$ , we see that  $\text{irr}(\sqrt{1+\sqrt{3}}, Q) = x^4 - 2x^2 - 2$ .

Thus  $\sqrt{1+\sqrt{3}}$  is algebraic of degree 4 over  $Q$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

Let  $E$  be an extension field of a field  $F$ , and let  $\alpha \in E$ . Let  $\phi_\alpha$  be the evaluation homomorphism of  $F[x]$  into  $E$  with  $\phi_\alpha(a) = a$  for  $a \in F$  and  $\phi_\alpha(x) = \alpha$ , as in Theorem 22.4. We consider two cases.

**Case I** Suppose  $\alpha$  is algebraic over  $F$ . Then as in Theorem 29.13, the kernel of  $\phi_\alpha$  is  $\langle \text{irr}(\alpha, F) \rangle$  and by Theorem 27.25,  $\langle \text{irr}(\alpha, F) \rangle$  is a maximal ideal of  $F[x]$ . Therefore,  $F[x]/\langle \text{irr}(\alpha, F) \rangle$  is a field and is isomorphic to the image  $\phi_\alpha[F[x]]$  in  $E$ . This subfield  $\phi_\alpha[F[x]]$  of  $E$  is then the smallest subfield of  $E$  containing  $F$  and  $\alpha$ . We shall denote this field by  $F(\alpha)$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

Let  $E$  be an extension field of a field  $F$ , and let  $\alpha \in E$ . Let  $\phi_\alpha$  be the evaluation homomorphism of  $F[x]$  into  $E$  with  $\phi_\alpha(a) = a$  for  $a \in F$  and  $\phi_\alpha(x) = \alpha$ , as in Theorem 22.4. We consider two cases.

**Case II** Suppose  $\alpha$  is transcendental over  $F$ . Then by Theorem 29.12,  $\phi_\alpha$  gives an isomorphism of  $F[x]$  with a subdomain of  $E$ . Thus in this case  $\phi_\alpha[F[x]]$  is not a field but an integral domain that we shall denote by  $F[\alpha]$ . By Corollary 21.8,  $E$  contains a field of quotients of  $F[\alpha]$ , which is thus the smallest subfield of  $E$  containing  $F$  and  $\alpha$ . As in Case I, we denote this field by  $F(\alpha)$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.16 Example** Since  $\pi$  is transcendental over  $\mathbb{Q}$ , the field  $\mathbb{Q}(\pi)$  is isomorphic to the field  $\mathbb{Q}(x)$  of rational functions over  $\mathbb{Q}$  in the indeterminate  $x$ .

Thus from a structural viewpoint, an element that is transcendental over a field  $F$  behaves as though it were an indeterminate over  $F$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.17 Definition** An extension field  $E$  of a field  $F$  is a **simple extension** of  $F$  if  $E=F(\alpha)$  for some  $\alpha \in E$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.18 Theorem** Let  $E$  be a simple extension  $F(\alpha)$  of a field  $F$ , and let  $\alpha$  be algebraic over  $F$ . Let the degree of  $\text{irr}(\alpha, F)$  be  $n \geq 1$ . Then every element  $\beta$  of  $E = F(\alpha)$  can be uniquely expressed in the form

$$\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1},$$

where the  $b_i$  are in  $F$ .

# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**29.19 Example** The polynomial  $p(x)=x^2+x+1$  in  $\mathbb{Z}_2[x]$  is irreducible over  $\mathbb{Z}_2$ . An extension field  $E$  of  $\mathbb{Z}_2$  containing a zero  $\alpha$  of  $x^2+x+1$ . By Theorem 29.18,  $\mathbb{Z}_2(\alpha)$  has as elements  $0+0\alpha, 1+0\alpha, 0+1\alpha$ , and  $1+1\alpha$ , that is,  $0, 1, \alpha$  and  $1+\alpha$ . This gives us a new finite field, of four elements! The addition and multiplication tables for this field are shown in Tables.

+	0	1	$\alpha$	$1+\alpha$
0	0	1	$\alpha$	$1+\alpha$
1	1	0	$1+\alpha$	$\alpha$
$\alpha$	$\alpha$	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	$\alpha$	1	0

	0	1	$\alpha$	$1+\alpha$
0	0	0	0	0
1	0	1	$\alpha$	$1+\alpha$
$\alpha$	0	$\alpha$	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	$\alpha$



# SECTION 29: INTRODUCTION TO EXTENSION FIELDS

---

**Example** Finally, we can use Theorem 29.18 to fulfill our promise of Example 29.4 and show that  $R[x]/\langle x^2+1 \rangle$  is isomorphic to the field  $C$  of complex numbers. We saw in Example 29.4 that we can view  $R[x]/\langle x^2+1 \rangle$  as an extension field of  $R$ . Let  $\alpha = x + \langle x^2+1 \rangle$ .

Then  $R[x]/\langle x^2+1 \rangle$  consists of all elements of the form  $a+b\alpha$  for  $a,b \in R$ , by Theorem 29.18. Thus  $R(\alpha) \approx C$ .



# Abstract Algebra

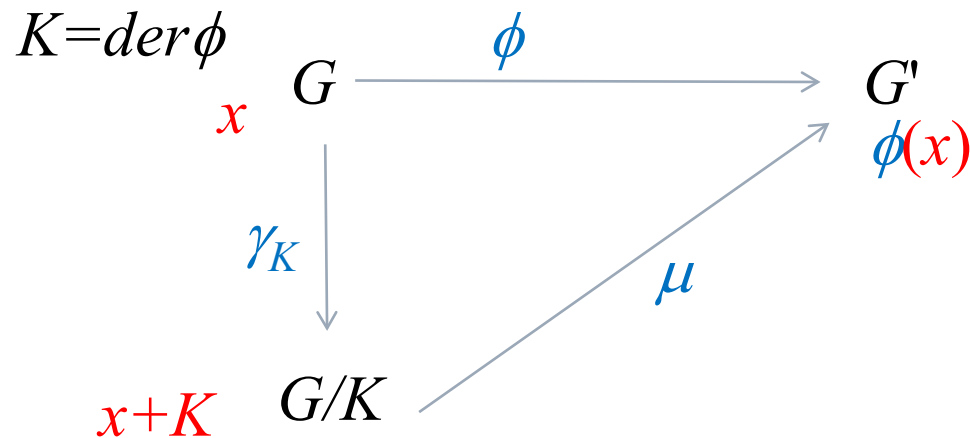
---

# SECTION 34: ISOMORPHISM THEOREMS

---

**34.2 Theorem (First Isomorphism Theorem)** Let  $\phi: G \rightarrow G'$  be a homomorphism with kernel  $K$ , and let  $\gamma_K: G \rightarrow G/K$  be the canonical homomorphism. There is a unique isomorphism  $\mu: G/K \rightarrow \phi[G]$  such that  $\phi(x) = \mu(\gamma_K(x))$  for each  $x \in G$ .

an extension field of a field  $F$  if  $F \leq E$ .



# SECTION 34: ISOMORPHISM THEOREMS

---

**34.3 Lemma** Let  $N$  be a normal subgroup of a group  $G$  and let  $\gamma: G \rightarrow G/N$  be the canonical homomorphism. Then the map  $\phi$  from the set of normal subgroups of  $G$  containing  $N$  to the set of normal subgroups of  $G/N$  given by  $\phi(L) = \gamma[L]$  is one to one and onto.

# SECTION 34: ISOMORPHISM THEOREMS

---

**Definition** If  $H$  and  $N$  are subgroups of a group  $G$ , then we let

$$HN = \{hn \mid h \in H, n \in N\}.$$

**Definition** We define the join  $H \vee N$  of  $H$  and  $N$  as the intersection of all subgroups of  $G$  that contain  $HN$ ; thus  $H \vee N$  is the smallest subgroup of  $G$  containing  $HN$ . Of course  $H \vee N$  is also the smallest subgroup of  $G$  containing both  $H$  and  $N$ , since any such subgroup must contain  $HN$ .

**Note** In general,  $HN$  need not be a subgroup of  $G$ . However, we have the following lemma.

# SECTION 34: ISOMORPHISM THEOREMS

---

**34.4 Lemma** If  $N$  is a normal subgroup of  $G$ , and if  $H$  is any subgroup of  $G$ , then  $HVN=HN=NH$ . Furthermore, if  $H$  is also normal in  $G$ , then  $HN$  is normal in  $G$ .

# SECTION 34: ISOMORPHISM THEOREMS

---

34.5 Theorem (Second Isomorphism Theorem) Let  $H$  be a subgroup of  $G$  and let  $N$  be a normal subgroup of  $G$ . Then  $(HN)/N \approx H/(H \cap N)$ .

## SECTION 34: ISOMORPHISM THEOREMS

---

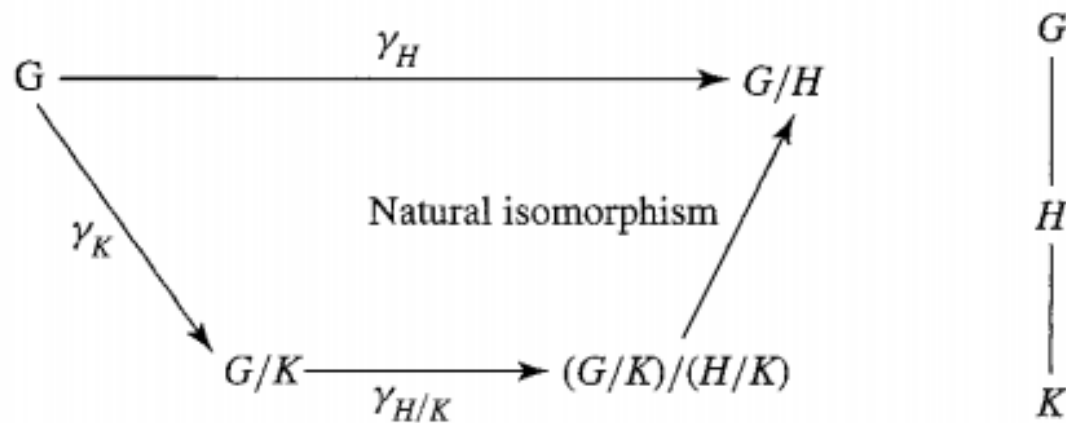
**34.6 Example** Let  $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ ,  $H = \mathbb{Z} \times \mathbb{Z} \times \{0\}$ , and  $N = \{0\} \times \mathbb{Z} \times \mathbb{Z}$ . Then clearly  $HN = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  and  $H \cap N = \{0\} \times \mathbb{Z} \times \{0\}$ . We have  $(HN)/N \approx \mathbb{Z}$  and we also have  $H/(H \cap N) \approx \mathbb{Z}$ .



# SECTION 34: ISOMORPHISM THEOREMS

---

34.7 Theorem (Third Isomorphism Theorem) Let  $H$  and  $K$  be normal subgroups of a group  $G$  with  $K < H$ . Then  $G/H \approx (G/K)/(H/K)$ .





# Abstract Algebra

---

# SECTION 36: SYLOW THEOREMS

---

**36.2 Definition** Let  $p$  be a prime. A group  $G$  is a  $p$ -group if every element in  $G$  has order a power of the prime  $p$ . A subgroup of a group  $G$  is a  $p$ -subgroup of  $G$  if the subgroup is itself a  $p$ -group.

# SECTION 36: SYLOW THEOREMS

---

**36.3 Theorem (Cauchy's Theorem)** Let  $p$  be a prime. Let  $G$  be a finite group and let  $p$  divide  $|G|$ . Then  $G$  has an element of order  $p$  and, consequently, a subgroup of order  $p$ .

# SECTION 36: SYLOW THEOREMS

---

**36.8 (First Sylow Theorem)** Let  $G$  be a finite group and let  $|G| = p^n m$  where  $n \geq 1$  and where  $p$  does not divide  $m$ . Then

1.  $G$  contains a subgroup of order  $p^i$  for each  $i$  where  $1 \leq i \leq n$ ,
2. Every subgroup  $H$  of  $G$  of order  $p^i$  is a normal subgroup of a subgroup of order  $p^{i+1}$  for  $1 \leq i \leq n$ .

# SECTION 36: SYLOW THEOREMS

---

**36.9 Definition** A Sylow  $p$ -subgroup  $P$  of a group  $G$  is a maximal  $p$ -subgroup of  $G$ , that is, a  $p$ -subgroup contained in no larger  $p$ -subgroup.

# SECTION 36: SYLOW THEOREMS

---

**36.10 Theorem (Second Sylow Theorem)** Let  $P_1$  and  $P_2$  be Sylow  $p$ -subgroups of a finite group  $G$ . Then  $P_1$  and  $P_2$  are conjugate subgroups of  $G$ .

# SECTION 36: SYLOW THEOREMS

---

**36.11 Theorem (Third Sylow Theorem)** If  $G$  is a finite group and  $p$  divides  $|G|$ , then the number of Sylow  $p$ -subgroups is congruent to 1 modulo  $p$  and divides  $|G|$ .



# SECTION 36: SYLOW THEOREMS

---

**36.12 Example** The Sylow 2-subgroups of  $S_3$  have order 2.

The subgroups of order 2 in  $S_3$  in Example 8.7

are  $\{\rho_0, \mu_1\}$ ,  $\{\rho_0, \mu_2\}$ ,  $\{\rho_0, \mu_3\}$

# SECTION 36: SYLOW THEOREMS

---

36.12 Example No group of order 15 is simple.