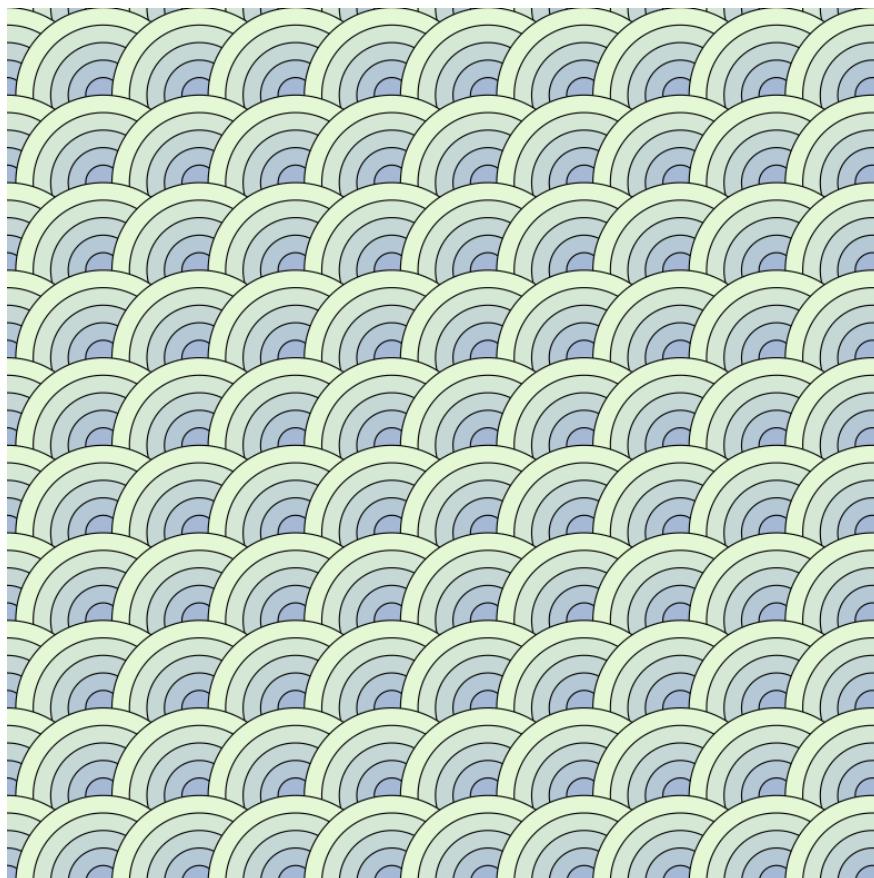


Abstract Algebra

2nd. EDITION

pehcy (MurphyShark) <https://github.com/pehcy>



Based on lectures UECM 3363 Abstract Algebra in Universiti Tunku Abdul Rahman in 2020
Notes taken by MurphyShark.

1

Groups

Definition 1.1 Closure

Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G . This condition is called **closure**.

The most familiar binary operations are ordinary addition, subtraction and multiplication of integers. However, the division of integers is not a binary operation on the integers.

Definition 1.2 Binary operation

Let G be a group. A **binary operation** is a map of sets:

$$*: G \times G \rightarrow G.$$

For ease of notation we write $*(a, b) = a * b \quad \forall a, b \in G$. Any binary operation on G gives a way of combining elements. As we have seen, if $G = \mathbb{Z}$ then $+$ and \times are natural examples of binary operations.

Additive Group	Multiplicative Group
Let G be a set, and $+$ be an operation, then $(G, +)$ is an additive group provided	Let G be a set, and \circ be an operation, then (G, \circ) is an multiplicative group provided
1. $\forall a, b \in G, a + b \in G$	6. $\forall a, b \in G, a \circ b \in G$
2. $\forall a, b, c \in G, a + (b + c) = (a + b) + c$	7. $\forall a, b, c \in G, a \circ (b \circ c) = (a \circ b) \circ c$
3. $\forall a \in G, \exists 0 \in G$ (identity) s.t. $a + 0 = a = 0 + a$	8. $\forall a \in G, \exists 1 \in G$ (unity) s.t. $a \circ 1 = a = 1 \circ a$
4. $\forall a \in G, \exists -a \in G$ (additive inverse) s.t. $a + (-a) = 0 = (-a) + a$	9. $\forall a \in G, \exists a^{-1} \in G$ (unity) s.t. $a \circ a^{-1} = 1 = a^{-1} \circ a$
5. (Commutative) $\forall a, b \in G, a + b = b + a$	10. (Commutative) $\forall a, b \in G, a \circ b = b \circ a$

Joining additive and multiplicative groups together, we form a ring with **distributive laws**

$$11. \quad \forall a, b, c \in G, (a + b) \circ c = (a \circ c) + (b \circ c)$$

$$12. \quad \forall a, b, c \in G, c \circ (a + b) = (c \circ a) + (c \circ b)$$

- Abelian group: (1-5) or (6-10)
- Associative Ring: 1-6, with 11 and 12
- Semigroup: 1, 2 only
- Monoid (Semigroup with identity): 1, 2, 3 only
- Commutative ring: 1-5, 6, 10, 11, and 12
- Ring: 1-5, with 11 and 12
- Ring with unity: 1-6, with 8, 11, and 12
- Field: 1-12

Axiom 1.1 Groups

Let G be a set together with a *binary operation* that assigns to each ordered pair (a, b) of elements of G an element in G denoted by $a * b$. We say that $(G, *)$ is a group under this operation if the following properties are satisfied.

1. **(Closure)** $\forall a, b \in G, a * b \in G$.
2. **(Associativity)** $\forall a, b, c \in G, a * (b * c) = (a * b) * c \in G$.
3. **(Existence of Identity)** $\forall a \in G, \exists e \in G$ s.t. $a * e = a = e * a \in G$.
4. **(Existence of Inverse)** $\forall a \in G, \exists a^{-1} \in G$ s.t. $a * a^{-1} = e = a^{-1} * a \in G$.

☞ **Example 1.0.1.** The set of integers \mathbb{Z} , the set of rational numbers \mathbb{Q} and the set of real numbers \mathbb{R} are all groups under normal addition.

☞ **Example 1.0.2.** The set

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

is a non-abelian group under matrix multiplication.

☞ **Solution** Check if $GL(2, \mathbb{R})$ is closure, associative, has identity and has inverse.

1. (Closureness) For all $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ in $GL(2, \mathbb{R})$, with $a_1d_1 - b_1c_1 \neq 0$ and $a_2d_2 - b_2c_2 \neq 0$.

$$\begin{aligned} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} &= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_1 & c_1b_2 + d_1d_2 \end{bmatrix} \in GL(2, \mathbb{R}) \\ &= (a_1a_2 + b_1c_2)(c_1b_2 + d_1d_2) - (a_1b_2 + b_1d_2)(c_1a_2 + d_1c_1) \\ &= a_1a_2c_1b_2 + a_1a_2d_1d_2 + b_1b_2c_1c_2 + b_1c_2d_1d_2 \\ &\quad - a_1a_2b_2c_1 - a_2b_2c_2d_1 - a_2b_1c_1d_2 - b_1c_2d_1d_2 \\ &= (a_1d_1 - b_1c_1)(a_2d_2 - c_2b_2) \neq 0 \in GL(2, \mathbb{R}). \end{aligned}$$

Matrix multiplication is closed under $GL(2, \mathbb{R})$.

2. (Associativity) For all $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$ in $GL(2, \mathbb{R})$, we have

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right) = \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}.$$

Matrix multiplication in $GL(2, \mathbb{R})$ is associative.

3. (Existence of identity) $\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{R}), \exists \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{R})$ s.t.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

4. (Existence of inverse) $\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{R}), \exists \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in GL(2, \mathbb{R})$ s.t.

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} &= \frac{1}{ad - bc} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \\ &= \frac{1}{ad - bc} \begin{bmatrix} ad - bc & -ab + ba \\ cd - cd & -bc + ad \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Similarly, we can verify that

$$\frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in GL(2, \mathbb{R})$$

since

$$\frac{1}{ad - bc} \det \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} (da - bc) = 1 \neq 0.$$

The inverse does exists whenever a, b, c, d in \mathbb{R} .



Example 1.0.3 (Non-example). The set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is not a group under multiplication modulo 4.

☞ **Solution** Because $\gcd(2, 4) = 2 \neq 1$, which means 2^{-1} does not exist in \mathbb{Z}_4 . Each elements in the group should have its unique inverse. Thus (\mathbb{Z}_4, \cdot) is not a group. ◀

☞ **Example 1.0.4 (Non-example).** The set of integers under subtraction is not a group.

☞ **Solution** For all $a, b, c \in \mathbb{Z}$,

$$a - (b - c) = a - b + c \neq (a - b) - c.$$

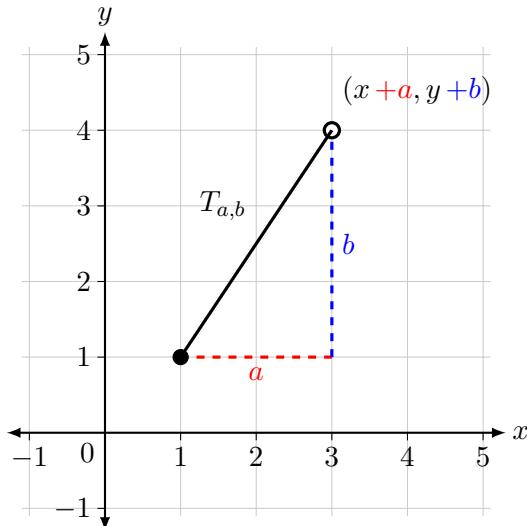
Which violates the associative property. So the subtraction in the set of integers is not a group. ◀

☞ **Example 1.0.5.** The set \mathbb{Q}^+ of positive rationals is a group under ordinary multiplication.

☞ **Example 1.0.6.** For a fixed point (x, y) in 2-dimensional cartesian plane \mathbb{R}^2 , we define the geometrical translation $T_{a,b} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by

$$T_{a,b}(x, y) = (x + a, y + b).$$

The set $G = \{T_{a,b} \mid a, b \in \mathbb{R}\}$ is a group under function composition.



☞ **Solution** 1. (Closureness) We want to show:

$$\forall T_{a,b}, T_{c,d} \in G, \quad T_{a,b} \circ T_{c,d} \in G$$

We compute the composition

$$\begin{aligned} (T_{a,b} \circ T_{c,d})(x, y) &= T_{a,b}(T_{c,d}(x, y)) \\ &= T_{a,b}(x + c, y + d) \\ &= (x + a + c, y + b + d) \\ &= (x + (a + c), y + (b + d)) \quad \text{associativity of ordinary addition} \\ &= T_{a+c, b+d}(x, y) \end{aligned}$$

which closed under G .

2. (Associativity) For all $T_{a,b}, T_{c,d}, T_{g,h} \in G$, we have

$$\begin{aligned} T_{a,b} \circ (T_{c,d} \circ T_{g,h}) &= T_{a,b} \circ T_{c+g,d+h} \\ &= T_{a+(c+g),b+(d+h)} \\ &= T_{(a+c)+g,(b+d)+h} \\ &= T_{a+c,b+d} \circ T_{g,h} \\ &= (T_{a,b} \circ T_{c,d}) \circ T_{g,h} \end{aligned}$$

so the translation closed under the function composition.

3. (Existence of identity) $\forall T_{a,b} \in G, \exists T_{e_1,e_2} \in G$ such that

$$T_{a,b} \circ T_{e_1,e_2} = T_{a,b} = T_{e_1,e_2} \circ T_{a,b}.$$

We need to find the value of e_1 and e_2 .

$$\begin{aligned} T_{a,b} \circ T_{e_1,e_2} = T_{a,b} &\Rightarrow T_{a+e_1,b+e_2} = T_{a,b} \\ &\Rightarrow a + e_1 = a \quad \text{and} \quad b + e_2 = b \end{aligned}$$

On solving, we have $e_1 = e_2 = 0$. Thus $T_{0,0} \in G$ is the identity.

4. (Existence of inverse) $\forall T_{a,b} \in G, \exists T_{\alpha,\beta} \in G$ such that

$$T_{a,b} \circ T_{\alpha,\beta} = T_{0,0} = T_{\alpha,\beta} \circ T_{a,b}.$$

Compute

$$\begin{aligned} T_{a,b} \circ T_{\alpha,\beta} = T_{0,0} &\Rightarrow T_{a+\alpha,b+\beta} = T_{0,0} \\ &\Rightarrow a + \alpha = 0 \quad \text{and} \quad b + \beta = 0 \end{aligned}$$

solving equations give us $\alpha = -a$ and $\beta = -b$. The inverse of $T_{a,b}$ in G is $T_{-a,-b}$.



Definition 1.3 Multiplicative group modulo n

The multiplicative group of integers modulo n , denoted \mathbb{Z}_n^* or $U(n)$, is the group

$$U(n) := \{k \in \mathbb{Z}_n \mid \gcd(n, k) = 1\}$$

where the binary operation is multiplication, modulo n .

Example 1.0.7. The set

$$U(n) = \{x \in \mathbb{Z}^+ \mid x < n, \gcd(x, n) = 1\}$$

is a group under multiplication modulo n .

Solution 1. (Closureness) For all $x, y \in U(n)$, where $x, y < n$ and $\gcd(x, n) = \gcd(y, n) = 1$, then $xy \in U(n)$ since $\gcd(xy, n) = \gcd(x, n) \cdot \gcd(y, n) = 1$.

2. (Associativity) Associative holds since $x(yz) = (xy)z$ whenever x, y, z in $U(n)$.

3. (Existence of identity) $\forall x \in U(n), \exists 1 \in U(n)$ s.t. $x \cdot 1 = x = 1 \cdot x$.

4. (Existence of inverse) For all $x \in U(n)$, since $\gcd(x, n) = 1$. Then by *extended Euclidean algorithm* we have

$$ax + bn = 1 \quad \text{for some } a, b \in U(n) \quad (\heartsuit)$$

taking modulo n on (\heartsuit) yields $ax = 1 \implies x^{-1} = a$. Thus the inverse of x does exists. \blacktriangleleft

Example 1.0.8. Draw a cayley table for $U(10)$.

Solution $U(10)$ contains all the integers that are coprime to 10. That is,

$$U(10) = \{1, 3, 7, 9\}.$$

$U(10)$ is a group under multiplication modulo 10.

\cdot_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Lemma 1.1 Uniqueness of group identity

In a group G , there is one and only one identity element e .

Proof. For the sake of contradiction. Suppose not, Suppose that e and e' are both identity elements of group G . Since e is an identity element of G , then $e \in G$ and

$$ea = a = ae \quad \forall a \in G. \quad (\heartsuit)$$

Since e' is also an identity element of G . we said that $e' \in G$ and

$$e'a = a = ae' \quad \forall a \in G. \quad (\clubsuit)$$

From (\heartsuit) , if we take $a = e'$, then $e \cdot e' = e'$.

From (\clubsuit) , if we take $a = e$, then $e = e \cdot e'$.

Combining the results we have $e = e \cdot e' = e'$, and so $e = e'$. There is only one identity element in G . We proved the uniqueness of identity. \square

Lemma 1.2 Cancellation rule

In a group G , $ba = ca$ implies $b = c$; and $ab = ac$ implies $b = c$.

Proof. Consider G is a group, then

$$\forall a \in G, \exists a' \in G \quad \text{s.t.} \quad aa' = e = a'a.$$

To show the right cancellation works, we further consider $ba = ca$. Multiplying a' on both sides of the previous equation on right, we obtained

$$(ba)a' = (ca)a'$$

Then, $b(aa') = c(aa')$ and so $be = ce \Rightarrow [b = c]$. The proof is now complete. \square

Theorem 1.1 Socks-shoes property

$$(\textcolor{red}{a} \circ \textcolor{orange}{b})^{-1} = \textcolor{orange}{b}^{-1} \circ \textcolor{red}{a}^{-1} \quad (1.1)$$

Proof. Since we know that G is a group, then $ab \in G$ for all $a, b \in G$ since G is closure. Next, we consider the following equation

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} && G \text{ is associative} \\ &= aea^{-1} \\ &= aa^{-1} \\ &= [\textcolor{black}{e}] && \text{cancellation rule returns identity} \end{aligned}$$

this equation states that

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

now we cancel off ab from both sides of the equations, we now arrive at

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

and we have done the proof. \square

Remark. In abstract algebra, the position of inputs in binary operator is very important! The commutative property no necessary hold. $\textcolor{red}{a} \circ \textcolor{orange}{b} \neq \textcolor{orange}{b} \circ \textcolor{red}{a}$. E.g. matrix multiplication $AB \neq BA$.

☞ **Example 1.0.9 (Tutorial).** Show that every group with identity e and $x * x = x$ for all $x \in G$ is abelian.

☞ **Solution** Given $(G, *)$ is a group, there is an identity $e \in G$ and for all $x \in G$, $x * x = x$. We want to show G is abelian.

$\forall a, b \in G, a * a = a$ and $b * b = b$. Since G is a group, so $a * b \in G$. Observe that

$$\begin{aligned} (a * b) * (a * b) &= a * b \Rightarrow a * (b * a) * b = (a * a) * (b * b) \\ &\Rightarrow a * (b * a) * b = a * a * b * b \\ &\Rightarrow a * (b * a) * b = a * (a * b) * b \\ &\Rightarrow \cancel{a} * (b * a) * \cancel{b} = \cancel{a} * (a * b) * \cancel{b} \\ &\Rightarrow [\textcolor{black}{b * a = a * b}]. \end{aligned}$$

Thus $*$ commute and G is an abelian group. \blacktriangleleft

1.1 Finite groups and Subgroups

Definition 1.4 Order of group

The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of G .

The order of an element g in G is the **smallest positive integer** n such that $g^n = e$ (In additive notation, this would be $ng = 0$). If no such integer exists, we said that g has infinite order. The order of an element $g \in G$ is denoted by $\text{ord}(g)$.

Example 1.1.1. $(\mathbb{Z}_5, +) = \{0, 1, 2, 3, 4\}$ is a group. The order of G is 5. We can write $|G| = 5$.

Take an element, said 2 in \mathbb{Z}_5 . The order of 2 is $\text{ord}(2) = 5$ since

$$2 + 2 + 2 + 2 + 2 = 10 \equiv 0 \pmod{5}.$$

It takes five iterations on the same operation to return back to the identity 0.

The order of 0 is infinity, $\text{ord}(0) = \infty$. No matter how many times you add on the zero, it is still zero and it is identity in \mathbb{Z}_5 .

Example 1.1.2. Take an element in $U(6)$, said 5. $\text{ord}(5) = 2$ because

$$5 \cdot 5 = 5^2 = 1 \pmod{6}.$$

Definition 1.5 Subgroups

If a subset H of a group G is itself a group under the same operation of G , we say that H is a subgroup of G .

Remark. We use the notation $H \leq G$ to mean that H is a subgroup of G . We use the notation $H < G$ to denote that H is a proper subgroup of G .

The subgroup $\{e\}$ is called the trivial subgroup of G ; a subgroup that is not $\{e\}$ is called a nontrivial subgroup of G .

1.1.1 Subgroup tests

Theorem 1.2 One step subgroup test

Suppose G is a multiplicative group and $H \subseteq G$. If

1. $H \neq \emptyset$,
2. $\forall a, b \in H, ab^{-1} \in H$

then H is a subgroup of G .

Proof. Given that G is a group and $\emptyset \neq H \subseteq G$ such that for any a, b in subgroup H , we have

$$ab^{-1} \in H \quad (\heartsuit)$$

Then, what we need to do is to show that $H \leq G$, which is equivalent to show that H itself is a group, and H definitely inherits the operation of G . So H is closed under the same operation of G .

(Closure) Take $a = x$ and $b = y^{-1}$ into (♥), which for all $x, y \in H$. We have

$$x(y^{-1})^{-1} = xy \in H$$

which is closed under H .

(Associativity) Since associative law holds in G , so as H , since both G and H are sharing the same operation.

(Existence of identity) Since H is nonempty, then we can randomly pick an element $x \in H$. If we replace a and b in the hypothesis (♥) with $a = b = x$, then we have

$$\forall x \in H, \quad xx^{-1} = e \in H$$

(Existence of inverse) Replacing $a = e$ and $b = x$ in (♥), we have

$$ex^{-1} = x^{-1} \in H \quad \forall x \in H$$

□

☞ **Example 1.1.3.** Let G be an abelian group with identity e . Then

$$H = \{x \in G \mid x^2 = e\}$$

is a subgroup of G .

☞ **Solution** We can use one-step subgroup test to check:

1. Since G is a group, then $e \in G$ and so $e = e^2 \in H \neq \emptyset$.
2. For all $a, b \in H$, we see that $a^2 = e$ and $b^2 = e$. Next, we compute

$$\begin{aligned} (ab^{-1})^2 &= (ab^{-1})(ab^{-1}) \\ &= a^2(b^{-1})^2 \\ &= a^2(b^2)^{-1} \\ &= ee^{-1} \\ &= e \end{aligned}$$

implies ab^{-1} is in H . Thus $H \leq G$.

◀

Theorem 1.3 Two-step subgroup test

Suppose G is a multiplicative group and $H \subseteq G$. H is a subgroup of G provided

1. $H \neq \emptyset$,
2. For any $a, b \in H$, $ab \in H$,
3. For all $a \in H$, $a^{-1} \in H$

Proof. Given that $a, b \in H$ and that b^{-1} is in H . We have $ab^{-1} \in H$ and so the One-step subgroup test is satisfied. \square

Theorem 1.4 Finite subgroup test

Suppose G is a multiplicative group and $H \subseteq G$. H is a subgroup of G provided

1. $|H| < \infty$
2. For all $a, b \in H$, $ab \in H$. (which means H closed under the same operation of G)

Proof. We need to show that a^{-1} is in H , and then using the Two-step subgroup test to verify.

For an $a \in H$, if $a = e$ then $a^{-1} = e^{-1} = e$ and we are done. However, if $a \neq e$, consider another subgroup $A = \{a, a^2, a^3, \dots\} \subseteq H$ by closure. Since H is finite, two of these must be identical, say

$$a^j = a^k \quad \text{for } 1 \leq j < k.$$

Now cancelling a^j on both sides, we get

$$\begin{aligned} e = a^{k-j} &\implies ea^{-1} = a^{k-j}a^{-1} \\ &\implies a^{-1} = a^{k-j-1} \in A. \end{aligned}$$

Hence a^{k-j-1} is the inverse of a and is an element of A , which also in H . By Two-step subgroup test, the finite subgroup test is valid. \square

☞ **Example 1.1.4.** Let G be an abelian group under multiplication with identity e . Then

$$H = \{x^2 \mid x \in G\}$$

is a subgroup of G .

☞ **Solution**

Since G is a group, then $e^2 = e \in G$ and G is nonempty.

For all $a, b \in H$, we see that $a = x^2$ and $b = y^2 \quad \forall x, y \in G$. Next, we compute

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

implies $ab^{-1} = (xy^{-1})^2$ is in H . Thus $H \leq G$. \blacktriangleleft

☞ **Example 1.1.5.** Let $G = \mathbb{R}^* \setminus \{0\}$, (G, \cdot) is a multiplicative group. And

$$H = \{x \in G \mid x = 1 \text{ or } x \text{ is irrational}\}$$

is not a subgroup of G .

☞ **Solution** With two-step subgroup test, step 2 is wrong.
(Counterexample) $\sqrt{2} \in H$, but $\sqrt{2}\sqrt{2} = 2 \notin H$. \blacktriangleleft

☞ **Example 1.1.6.** Let $G = \mathbb{R}^* \setminus \{0\}$, (G, \cdot) is a multiplicative group. And

$$K = \{x \in G \mid x \geq 1\}$$

is not a subgroup of G .

☞ **Solution** With two-step subgroup test, step 3 is wrong.

(Counterexample) Take $2 \in K$, but $2^{-1} = \frac{1}{2} \notin K$. ◀

1.2 Cyclic groups

Cyclic groups are groups in which every element is a power of some fixed element. In additive group, then every element is a multiple of some fixed element. For instance,

$$\underbrace{a + a + \cdots + a}_{n \text{ times}} = na, \quad n \text{ is integer}$$

Definition 1.6 Generating subgroup

If G is a multiplicative group and $g \in G$, then the subgroup generated by element g is

$$\langle g \rangle = \{ \underbrace{a \cdot a \cdots \cdot a}_{n \text{ times}} \mid n \in \mathbb{Z} \} = \{a^n \mid n \in \mathbb{Z}\} \quad (1.2)$$

If the group is abelian and is additive, then

$$\langle g \rangle = \{ \underbrace{a + a + \cdots + a}_{n \text{ times}} \mid n \in \mathbb{Z} \} = \{na \mid n \in \mathbb{Z}\} \quad (1.3)$$

Remark. $\langle g \rangle$ is called a **cyclic subgroup** generated by g in group G . When $G = \langle g \rangle$, then G is called a **cyclic group**.

Definition 1.7 Cyclic group

A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$. g is a **generator** of $\langle g \rangle$.

Lemma 1.3

$\langle g \rangle$ is a subgroup of G .

Proof. We can use 2-step subgroup test to verify $\langle g \rangle \leq G$:

1. Since $g \in \langle g \rangle \neq \emptyset$.
2. For all $g_1, g_2 \in \langle g \rangle$, we have

$$g_1 = g^{n_1}, \quad g_2 = g^{n_2}$$

where n_1 and n_2 are integers. And since

$$g_1 g_2 = g^{n_1} g^{n_2} = g^{n_1+n_2}$$

and $n_1+n_2 \in \mathbb{Z}$ implies that $g_1 g_2 \in \langle g \rangle$.

3. For all $g_1 \in \langle g \rangle$, we have $g_1 = g^k$, where k is integer. We compute the inverse

$$g_1^{-1} = (g^k)^{-1} = g^{-k}, \quad -k \in \mathbb{Z}$$

which tells us that $g_1^{-1} \in \langle g \rangle$.

Therefore, by 2-step subgroup test, $\langle g \rangle$ is a subgroup of G . \square

Lemma 1.4

If G is a cyclic group, then G is abelian.

Proof. Consider a cyclic group G . We want to show G is also an abelian group.

Since G is a group, we say

$$\forall g_1, g_2 \in G, \quad g_1 = g^{n_1}, \quad g_2 = g^{n_2}$$

where n_1 and n_2 are integers. In order to show that G is abelian, we need to show that the commutative law applied in group G .

now compute

$$\begin{aligned} g_1 g_2 &= a^{n_1} a^{n_2} \\ &= g^{n_1+n_2} \\ &= g^{n_2+n_1} \quad \text{commutative in normal addition} \\ &= g^{n_2} g^{n_1} = [g_2 g_1] \end{aligned}$$

thus G is an abelian group. \square

Definition 1.8 Center of group

The **center**, $Z(G)$ ¹, of a group G is a subset of elements in G that commute with every element of G , that is,

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}. \quad (1.4)$$

¹The Z stands for “Zentrum”, a German word for “Center”

Lemma 1.5

The center of a group G is also a subgroup of G .

Proof. We use one-step subgroup test to verify:

1. Since we know that G is a group, certainly the identity $e \in G$ and

$$ex = x = xe \quad \forall x \in G.$$

implies that $e \in Z(G)$ and $Z(G)$ is nonempty.

2. For any a_1, a_2 in $Z(G)$, we need to show

$$a_1 a_2^{-1} \in Z(G).$$

Since $Z(G)$ is the center, we have $a_1 x = xa_1$ and $a_2 x = xa_2$ for all $x \in G$. Proving $a_1 a_2^{-1} \in Z(G)$ is equivalent to show

$$a_1 a_2^{-1} x = xa_1 a_2^{-1} \quad \forall x \in G$$

compute

$$\begin{aligned} a_1 a_2^{-1} x &= a_1(a_2^{-1} x) && \text{Associativity of } Z(G) \\ &= a_1(xa_2^{-1}) && \text{Since } a_2^{-1} x = xa_2^{-1} \\ &= (a_1 x)a_2^{-1} && \text{Associativity of } Z(G) \\ &= (xa_1)a_2^{-1} && \text{Since } a_1 x = xa_1 \\ &= \boxed{xa_1 a_2^{-1}} \end{aligned}$$

which is what we desired.

Therefore the center $Z(G)$ is a subgroup of G by one-step subgroup test. \square

Definition 1.9 Group centralizer

Let a be a **fixed** element of a group G . The centralizer of a in G is

$$C(a) = \{g \in G \mid ga = ag\}. \quad (1.5)$$

Theorem 1.5

Let a be a **fixed** element in group G . If a has infinite order, then $a^i = a^j$ if and only if $i = j$. However, if a has finite order, said, n , then

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\} \quad (1.6)$$

and $a^i = a^j$ if and only if $n|i - j$.

Proof. Consider a group G , and take an a from G . If a has infinite order, say, $\text{ord}(a) = \infty$, then there is no nonzero integer n such that $a^n = e$. We assume an equation $a^i = a^j$ for some $i, j \in \mathbb{Z}$, we have

$$a^{i-j} = e \Rightarrow i - j = 0 \Rightarrow \boxed{i = j}.$$

and we are done.

On the other hand, if a has finite order, just say $\text{ord}(a) = n$. We want to show

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}.$$

Apparently, $e, a, a^2, \dots, a^{n-1}$ are all belongs to $\langle a \rangle$, so as the list $\{e, a, a^2, \dots, a^{n-1}\} \subseteq \langle a \rangle$. Now we continue to check if $\{e, a, a^2, \dots, a^{n-1}\} \supseteq \langle a \rangle$.

By *division algorithm*, there exists some integers q and r such that

$$k = nq + r, \quad 0 \leq r < n$$

compute

$$a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$$

this implies $a^k = a^r \in \{e, a, a^2, \dots, a^{n-1}\}$. Thus we have

$$\{e, a, a^2, \dots, a^{n-1}\} \supseteq \langle a \rangle.$$

Now the final part is to show $\alpha^i = \alpha^j$ iff $n|i - j$, we are going to proof on two directions.

(\Rightarrow) If $\alpha^i = \alpha^j$, we need to show that n is divisible by $i - j$. Again we applying the *division algorithm*,

$$i - j = nq + r, \quad 0 \leq r < n$$

which q is quotient and r is remainder.

compute

$$\begin{aligned} \alpha^{i-j} = e &\Rightarrow \alpha^{nq+r} = e && \text{division algorithm} \\ &\Rightarrow \alpha^{nq} \alpha^r = e \\ &\Rightarrow (\alpha^n)^q \alpha^r = e \\ &\Rightarrow e^q \alpha^r = e && \text{since } \alpha^n = e \\ &\Rightarrow e \alpha^r = e \\ &\Rightarrow \alpha^r = e \end{aligned}$$

but n is the least integer such that $\alpha^n = e$ and so the condition $0 \leq r < n$ implies $r = 0$. Now we continue on the opposite side of the statement.

(\Leftarrow) This part is more straightforward. Conversely, if $n|i - j$, then

$$\begin{aligned} \alpha^{i-j} &= \alpha^{nq+r} && \text{division algorithm} \\ &= \alpha^{nq} && \text{remainder } r \text{ is zero} \\ &= (\alpha^n)^q \\ &= e^q && \text{since } \alpha^n = e \\ &= e \end{aligned}$$

and we are done. □

Corollary 1.1

For any group element α , $\text{ord}(\alpha) = |\langle \alpha \rangle|$.

Proof. By previous theorem, $\langle \alpha \rangle = \{e, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ has n elements. Thus $|\langle \alpha \rangle| = \text{ord}(\alpha) = n$. □

Theorem 1.6

Let α be an element of order n in a group and let k be a positive integer. Then

$$\langle \alpha^k \rangle = \langle \alpha^{\gcd(n,k)} \rangle$$

and

$$\text{ord}(\alpha) = \frac{n}{\gcd(n, k)}.$$

Proof. 1. To show that $\langle \alpha^k \rangle = \langle \alpha^{\gcd(n,k)} \rangle$ is equivalent of showing $\langle \alpha^k \rangle \subseteq \langle \alpha^{\gcd(n,k)} \rangle$.

Consider $\alpha^k \in \langle \alpha^k \rangle$, and let $d = \gcd(n, k)$. This implies that d divide k and $k = dr$ for some integer r . Thus

$$\alpha^k = \alpha^{dr} = (\alpha^d)^r \in \langle \alpha^d \rangle = \langle \alpha^{\gcd(n,k)} \rangle.$$

On the other hand, we want to show $\langle \alpha^k \rangle \supseteq \langle \alpha^{\gcd(n,k)} \rangle$, which is equivalent to show $\langle \alpha^d \rangle \subseteq \langle \alpha^k \rangle$. Consider $\alpha^d \in \langle \alpha^d \rangle$. By extended Euclidean algorithm,

$$\begin{aligned}\alpha^d &= \alpha^{\gcd(n,k)} \\ &= \alpha^{nt+ks} && \text{for some integers } k, s \\ &= (\alpha^n)^t(\alpha^k)^s \\ &= e^t(\alpha^k)^s \\ &= (\alpha^k)^s \in \langle \alpha^k \rangle.\end{aligned}$$

2. Certainly,

$$\begin{aligned}\text{ord}(\alpha^k) &= |\langle \alpha^k \rangle| \\ &= |\langle \alpha^d \rangle| \\ &= \text{ord}(\alpha^d) \\ &= \frac{n}{d} \\ &= \frac{n}{\gcd(n, k)}.\end{aligned}$$

□

Theorem 1.7 Fundamental theorem of cyclic groups

Suppose $G = \langle g \rangle$ is cyclic.

1. Every subgroup of G is cyclic.
2. If $|G| = n$, then the order of any subgroup of G divides n .
3. If $|G| = n$, then for any positive integer k, n the subgroup $\langle g^{n/k} \rangle$ is the unique subgroup of order k .

Proof. 1. Let H is a subgroup of G , if $H = \{e\}$ then we are done.

Assume that $H \neq \{e\}$, choose $g^m \in H$ with minimal $m \in \mathbb{Z}^+$ by well-ordering. Clearly $\langle g^m \rangle \subseteq H$. If some $g^k \in H$ then by *division algorithm* we have

$$k = qm + r \implies r = k - qm \quad 0 \leq r < m$$

and then $g^r = g^k (g^m)^{-q} \in H$ and so $r = 0$ by minimality of m and so $g^k = (g^m)^q$ and hence $g^k \in \langle g^m \rangle$.

2. Take a subgroup $H \leq G$. From (1) we know H is cyclic and $H = \langle g^m \rangle$ with minimal positive integer m . Again we apply *division algorithm* and write

$$n = qm + r \implies r = n - qm \quad 0 \leq r < m$$

and $g^r = g^n (g^m)^{-q} \in H$ and so $r = 0$, and then

$$|H| = |\langle g^m \rangle| = \text{ord}(g^m) = \frac{n}{\gcd(n, m)} = \frac{n}{m}$$

and thus $m|H| = n$ and $|H|$ divide n .

3. Observe first that $k|n$ we have

$$|\langle g^{n/k} \rangle| = |g^{n/k}| = \frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k.$$

Thus certainly $\langle g^{n/k} \rangle$ is a subgroup of order k . We must show that it is unique. Let H be a subgroup of G such that $|H| = k|n$. Since $H \leq G$ by (1) and (2) we have $H = \langle g^m \rangle$ with $m|n$. Then we have

$$k = |H| = |\langle g^m \rangle| = \text{ord}(g^m) = \frac{n}{\gcd(n, m)} = \frac{n}{m}$$

Thus $m = \frac{n}{k}$ and so $H = \langle g^m \rangle = \boxed{\langle g^{n/k} \rangle}$.

□

 **Example 1.2.1.** In $\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$ the complete list of generators is $U(12) = \{1, 5, 7, 11\}$. So for example

$$\begin{aligned} \langle 5 \rangle &= \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\} \pmod{12} \\ &= \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} \end{aligned}$$

 **Example 1.2.2.** Consider $U(50)$: its order is $\phi(50) = 20$, and its elements are

$$\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49\}.$$

Given that $U(50) = \langle 3 \rangle$. Find all generators of $U(50)$.

 **Solution** Since $\langle 3^k \rangle = \langle 3 \rangle \Leftrightarrow \gcd(20, k) = 1 \Leftrightarrow k \in U(20)$. Since

$$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\},$$

the generators of $U(50)$ are

$$\{3, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}\} \text{ or } \{3, 27, 37, 33, 47, 23, 13, 17\}.$$

◀

 **Example 1.2.3.** Find all the subgroups of \mathbb{Z}_{42} .

 **Solution** Listed out all the possible divisors of 42 we have

k	$42/k$	subgroup order k , $\langle (42/k) \rangle$ with $k 42$.
1	42	$\langle 42 \rangle = \{0\}$
2	21	$\langle 21 \rangle = \{0, 21\}$
3	14	$\langle 14 \rangle = \{0, 14, 18\}$
6	7	$\langle 7 \rangle = \{0, 7, 14, 21, 28, 35\}$
7	6	$\langle 6 \rangle = \{0, 6, 12, 18, 24, 30, 36\}$
14	3	$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39\}$
21	2	$\langle 2 \rangle$ is set of all even numbers in \mathbb{Z}_{42}
42	1	$\langle 1 \rangle = \mathbb{Z}_{42}$

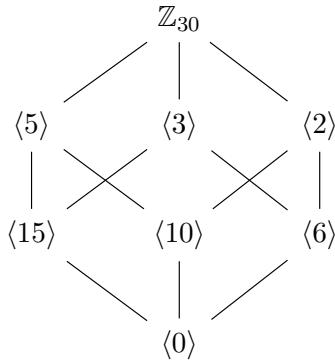
◀

Example 1.2.4. Draw a subgroup lattice of \mathbb{Z}_{30} .

Solution By prime factorizing $30 = 2 \cdot 3 \cdot 5$. The factors of 30 are

$$1, 2, 3, 5, 6, 10, 15, 30$$

The lattice diagram is



1.3 Permutation

Definition 1.10

A permutation of a set \mathcal{A} is a function from \mathcal{A} to \mathcal{A} that is both one-to one and onto. A permutation group of a set \mathcal{A} is the set of permutations of \mathcal{A} that forms a group under function composition

Example 1.3.1. Let S_3 denote the set of all one-to-one functions from $\{1, 2, 3\}$ to itself. The S_3 under function composition, is a group with six elements.

$$\begin{aligned} S_3 &= \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \\ &= \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 3)(1\ 2), (1\ 2)(1\ 3)\} \end{aligned}$$

Example 1.3.2. Let $A = \{1, 2, 3, 4\}$, and

$$S_4 = \{\sigma \mid \sigma : A \rightarrow A \text{ is a permutation from } A \text{ onto } A\}.$$

We defined σ as follow:

$$\sigma(1) \mapsto 2, \quad \sigma(2) \mapsto 3, \quad \sigma(3) \mapsto 4, \quad \sigma(4) \mapsto 1.$$

Now we can express σ as a permutation such that

$$\sigma = (1\ \sigma(1)\ \sigma^2(1)\ \sigma^3(1)) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

where

$$\begin{aligned}\sigma(1) &= 2 \\ \sigma^2(1) &= \sigma(\sigma(1)) = \sigma(2) = 3 \\ \sigma^3(1) &= \sigma(\sigma(\sigma(1))) = \sigma(\sigma(2)) = \sigma(3) = 4 \\ \sigma^4(1) &= \sigma(\sigma(\sigma(\sigma(1)))) = \sigma(\sigma(\sigma(2))) = \sigma(\sigma(3)) = \sigma(4) = 1\end{aligned}$$

 **Example 1.3.3.** Given $\alpha = (2\ 3\ 1\ 5\ 4)$ and $\beta = (2\ 1\ 3\ 4)$ in S_5 . Compute $\alpha\beta$, and β^{-1} .

 **Solution** Compute

$$\begin{aligned}\alpha\beta &= (2\ 3\ 1\ 5\ 4)(2\ 1\ 3\ 4) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix} \\ &= (1)(2\ 5\ 4\ 3) \\ &= (2\ 5\ 4\ 3)\end{aligned}$$

and

$$\begin{aligned}\beta^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} \\ &= (1\ 2\ 4\ 3)(5) \\ &= (1\ 2\ 4\ 3).\end{aligned}$$



Lemma 1.6

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem 1.8

If the pair of cycles $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_m)$ have no entries in common, then $\alpha\beta = \beta\alpha$. In other words, any two disjoint cycles commute.

Proof. Let $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_m)$ be two disjoint cycles. These cycles are defined on the set

$$\mathcal{A} = \{a_1, a_2, \dots, a_t, b_1, b_2, \dots, b_s, \underbrace{c_1, c_2, \dots, c_r}_{\text{Fixed points}}\}.$$

and so $\alpha, \beta \in S_{t+s+r}$. We want to show that $\alpha \circ \beta = \beta \circ \alpha$ is equivalent to show

$$(\alpha \circ \beta)(x) = (\beta \circ \alpha)(x) \quad \forall x \in \mathcal{A}.$$

We are considering three possible cases:

Case 1: Suppose that $x = a_i$, where $1 \leq i \leq t$. On LHS

$$\begin{aligned}(\alpha \circ \beta)(a_i) &= \alpha(\beta(a_i)) \\&= \alpha(a_i) \\&= a_{i+1}.\end{aligned}$$

and on RHS

$$\begin{aligned}(\beta \circ \alpha)(a_i) &= \beta(\alpha(a_i)) \\&= \beta(a_{i+1}) \\&= a_{i+1}.\end{aligned}$$

Thus, LHS = RHS for first case.

Case 2: Suppose that $x = b_j$, where $1 \leq j \leq s$. On LHS

$$\begin{aligned}(\alpha \circ \beta)(b_j) &= \alpha(\beta(b_j)) \\&= \alpha(b_{j+1}) \\&= b_{j+1}.\end{aligned}$$

and on RHS

$$\begin{aligned}(\beta \circ \alpha)(a_i) &= \beta(\alpha(b_j)) \\&= \beta(b_{j+1}) \\&= b_{j+1}.\end{aligned}$$

Thus, LHS = RHS for second case.

Case 3: At last, suppose that $x = c_k$, where $1 \leq k \leq r$. Each c_k are fixed points and they always stay in the same value whenever any cycles.

$$(\alpha \circ \beta)(c_k) = c_k = (\beta \circ \alpha)(c_k).$$

Hence, we conclude that any disjoint cycles are commute. \square

Definition 1.11

A permutation that can be expressed as a product of an even (or odd) number of 2-cycles is called an even (or odd) permutation.

 **Example 1.3.4.** Write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 2 & 5 & 8 & 6 \end{pmatrix} \in S_8$$

into the product of 2-cycles.

☞ **Solution** We can express σ as

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



☞ **Example 1.3.5.** Find the order of $\beta = (1\ 2\ 3\ 4)(5\ 6\ 7)$ in S_7 .

☞ **Solution** The order of a disjoint cycle is the LCM of the order of each disjoint cycles. Namely,

$$\begin{aligned}\text{ord}(\beta) &= \text{LCM}(\text{ord}(1\ 2\ 3\ 4), \text{ord}(5\ 6\ 7)) \\ &= \text{LCM}(4, 3) \\ &= \frac{4 \times 3}{\text{gcd}(4, 3)} \\ &= 12.\end{aligned}$$



Definition 1.12 Alternating group

The group of even permutations of n symbols is denoted by A_n and is called the **alternating group** of degree n .

Theorem 1.9

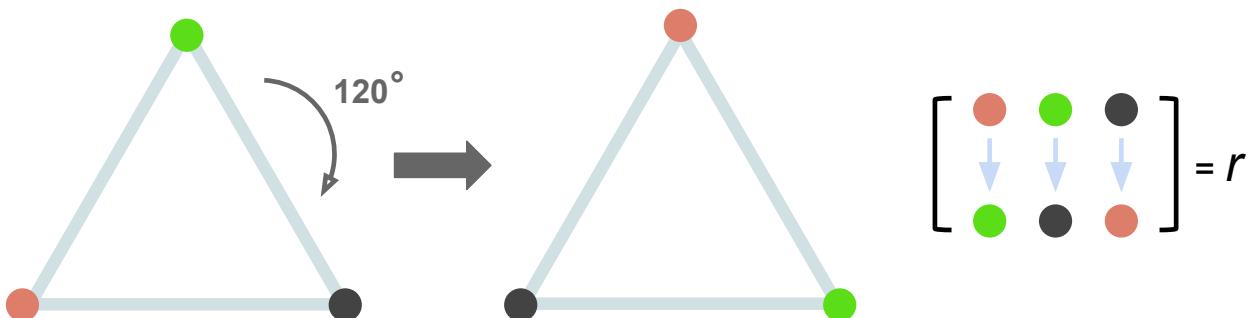
For $n > 1$, A_n has order $n!/2$.

1.4 Dihedral Group

Dihedral groups are an essential class in group theory that arise naturally in geometry and other areas of mathematics.

For $n \geq 3$, the dihedral group D_{2n} is described as the rigid motions taking a regular n -gon back to itself, with the operations

We could said that the rotational symmetry group of an equilateral triangle, C_3 , is isomorphic to \mathbb{Z}_3 . We can combine the horizontal reflection and rotations and form another reflection lines, which these reflection lines runs from one of the vertices to the center of the opposing side.



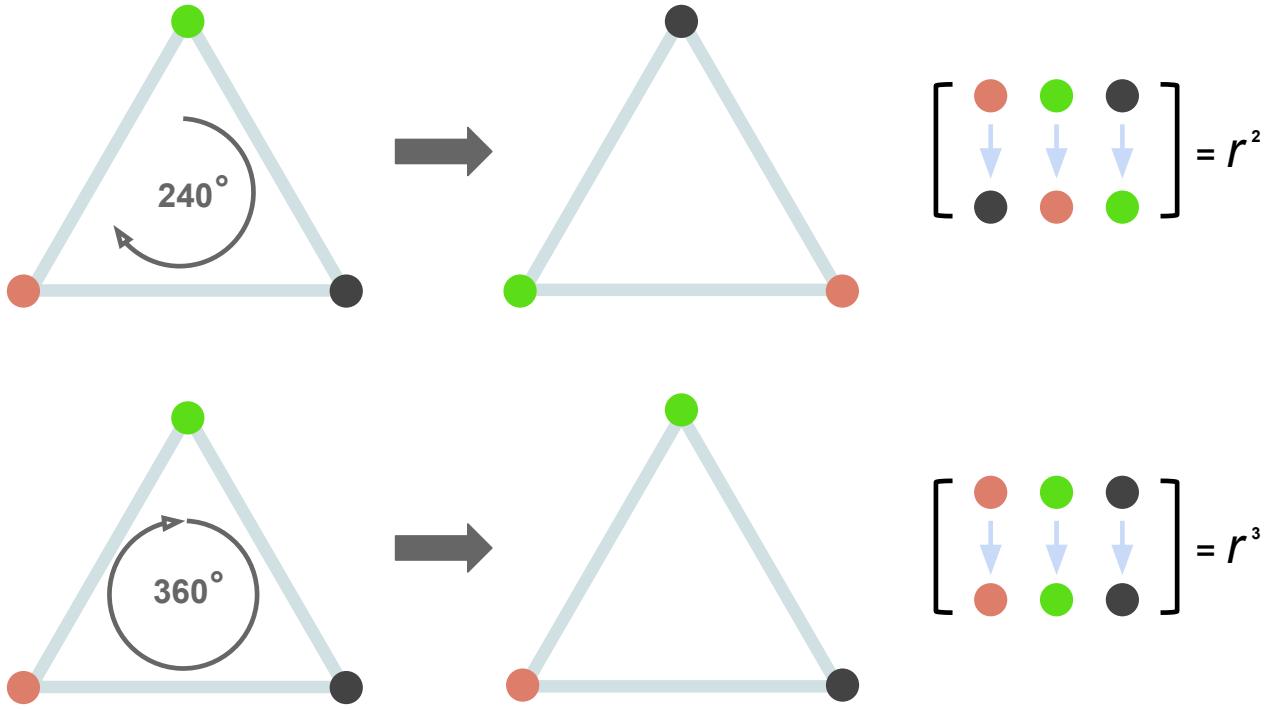


Figure 1.1: The rotation r on dihedral group D_6 with order 6. r in D_6 is described as rotating equilateral triangle 120 degree.

Theorem 1.10

Let the $2n$ -degree dihedral group

$$D_{2n} = \langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \rangle.$$

Then

1. $r^k s = sr^{-k}$.
2. The order of r^k is $\frac{n}{\gcd(n, k)}$.

Proof. 1. Compute

$$\begin{aligned} r^k s &= er^k s \\ &= s^2 r^k s \\ &= ssr^k s \\ &= \boxed{sr^{-k}}. \end{aligned}$$

and we are done.

2. We will first show that $r^k = e$ if and only if $n|k$.

(\Rightarrow) Consider $e = r^k$, then by *division algorithm* we have

$$k = na + b \quad \text{where } 0 \leq b < n.$$

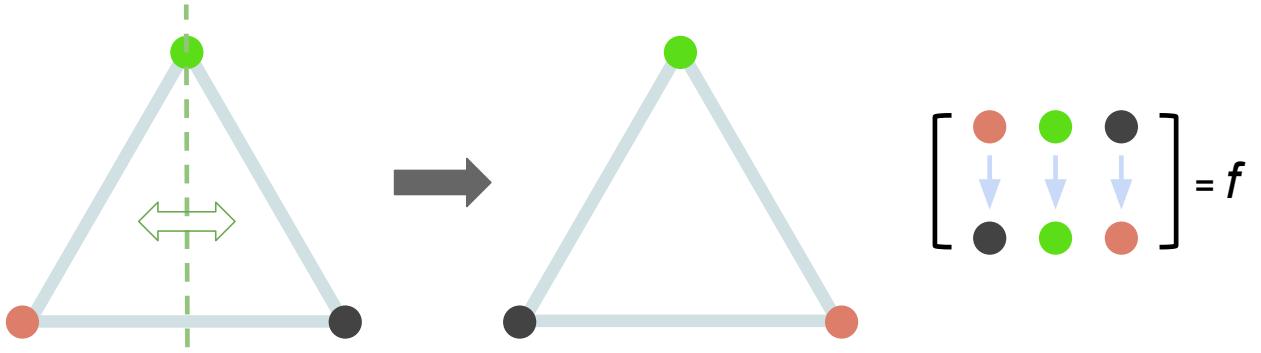


Figure 1.2: The group action f on dihedral group D_6 with order 6. f is a horizontal flip.

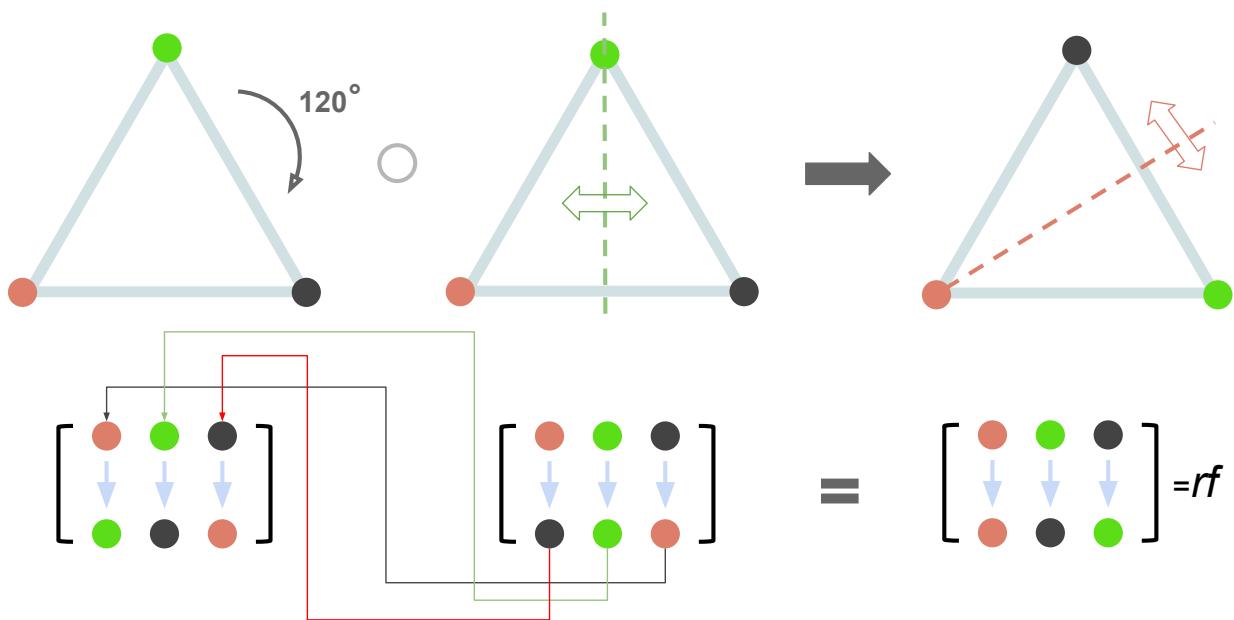


Figure 1.3: The composition of 120 deg rotation with horizontal reflection form another reflection line at vertice.

Thus

$$e = r^k = r^{na+b} = (r^n)^a r^b = e^a r^b = r^b.$$

Since the smallest possible integer m by well-ordering, such that $r^m = e$, is $n, b = 0$.

(\Leftarrow) Conversely, if n divide k , then $k = ns$ for some integer s . Hence

$$r^k = r^{ns} = (r^n)^s = e^s = e.$$

Thus $r^k = e \iff n|k$.

Now let $b = r^k \in D_n$, since r is a generator of D_n . We shall show that the smallest integer m such that $r^k = e$ is n/k . Let $d = \gcd(n, k)$. Consider

$$e = b^m = r^{km}.$$

Since this is the smallest integer m such that $n|km$. Thus $\frac{n}{d}$ divide $\frac{mk}{d}$. Because d is the greatest

common divisor of n and k , implies $\frac{n}{d}$ and $\frac{k}{d}$ are relatively prime. Hence

$$\frac{n}{d} \left| \frac{mk}{d} \right. \Rightarrow \frac{n}{d} \left| m \right.$$

The smallest such m is $\frac{n}{d}$. Thus

$$\text{ord}(r^k) = \frac{n}{\gcd(n, k)}.$$

□

 **Example 1.4.1.** In dihedral group order 7, simplify $r^2sr^6sr^3$ and $sr^4sr^3sr^2$.

 **Solution** In D_7 , compute

$$\begin{aligned} r^2sr^6sr^3 &= r^2(sr^6)sr^3 && \text{Associativity} \\ &= r^2(r^{-6}s)sr^3 && \text{Since } sr^6 = r^{-6}s \\ &= r^2r^{-6}ssr^3 \\ &= r^{-4}r^3 && s^2 = e, \text{ flip two time horizontally will back to original.} \\ &= r^{-1} && \text{Simplifying} \\ &= r^6 && 1 \text{ anticlockwise rotation} = 6 \text{ counterclockwise rotation.} \end{aligned}$$

On the other hand,

$$\begin{aligned} sr^4sr^3sr^2 &= s(r^4s)r^3(sr^2) && \text{Associativity} \\ &= s(sr^{-4})r^3(r^{-2}s) && \text{Since } r^4s = sr^{-4}, sr^2 = r^{-2}s \\ &= ssr^{-4}r^3r^{-2}s \\ &= r^{-3}s && s^2 = e, \text{ flip two time horizontally will back to original.} \\ &= r^4s && 3 \text{ anticlockwise rotation} = 4 \text{ counterclockwise rotation.} \end{aligned}$$

◀

 **Example 1.4.2.** Let

$$G = SL_2(\mathbb{Z}_3) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc = 1; a, b, c, d \in \mathbb{Z}_3 \right\}.$$

Show that $|G| = 48$.

 **Solution** From the first row, for all $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \setminus \{(0, 0)\}$. There are $({}^3P_1 \times {}^3P_1) - 1 = 8$ possibilities.

For the second row, for all $(c, d) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \setminus (a\mathbb{Z}_3, b\mathbb{Z}_3)$. There are $({}^3P_1 \times {}^3P_1) - 3 = 6$ possibilities.

Thus the order of group G is the product of the number of possibilities of these two rows.
 $|G| = 8 \times 6 = 48$. ◀

1.5 Normal subgroups, Quotient groups

1.5.1 Cosets

Definition 1.13 Cosets

Let G be a group and let H be a subset of G . For any $a \in G$, the set

$$aH := \{ah \mid h \in H\}$$

is called the **left coset** of H in G containing element a .

Analogously, the set

$$Ha := \{ha \mid h \in H\}$$

is called the **right coset** of H in G containing element a . In this case, the element a is called the **coset representative** of aH (or Ha).

We use $|aH|$ (or $|Ha|$) to be the number of elements in the left (or right) coset.

 **Example 1.5.1.** Consider $G = \mathbb{Z}_9 = \{0, 1, 2, \dots, 8\}(\text{mod } 9)$. We take a cyclic subgroup

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

which came from $(G, +_9)$. All **left cosets** of G with respect to H are $\{H, 1+_9H, 2+_9H\}$ where

$$0 + H = \{0 + 0, 0 + 3, 0 + 6\} (\text{mod } 9) = \{0, 3, 6\} = H$$

$$1 + H = \{1 + 0, 1 + 3, 1 + 6\} (\text{mod } 9) = \{1, 4, 7\}$$

$$2 + H = \{2 + 0, 2 + 3, 2 + 6\} (\text{mod } 9) = \{2, 5, 8\}$$

$$3 + H = \{3 + 0, 3 + 3, 3 + 6\} (\text{mod } 9) = \{3, 6, 0\} = H$$

As for the right cosets of G with respect to H are $\{H, H +_9 1, H +_9 2\}$. Pay attention that now the element of coset are being added to right-hand side instead of from left side.

$$H + 0 = \{0 + 0, 0 + 3, 0 + 6\} (\text{mod } 9) = \{0, 3, 6\} = H$$

$$H + 1 = \{0 + 1, 3 + 1, 6 + 1\} (\text{mod } 9) = \{1, 4, 7\}$$

$$H + 2 = \{0 + 2, 3 + 2, 6 + 2\} (\text{mod } 9) = \{2, 5, 8\}$$

$$H + 3 = \{0 + 3, 3 + 3, 6 + 3\} (\text{mod } 9) = \{3, 6, 0\} = H$$

Also, we can draw multiplication table of the cosets.

	H	$1 + H$	$2 + H$
H	H	$1 + H$	$2 + H$
$1 + H$	$1 + H$	$2 + H$	H
$2 + H$	$2 + H$	H	$1 + H$

Two cosets can also be multiply together. For instance,

$$(1 + H) \cdot (2 + H) = (1 + 2) + H = 0 + H = H$$

and

$$(2 + H) \cdot (2 + H) = (2 + 2) + H = 4 + H = 1 + H.$$

 **Example 1.5.2.** The reals under addition $(\mathbb{R}, +)$, the subgroup $(\mathbb{Z}, +)$ of integers. Now

$$\mathbb{R}/\mathbb{Z} = \{r + \mathbb{Z} \mid r \in \mathbb{R}\}.$$

The cosets are $r + \mathbb{Z}$ with $r \in [0, 1)$. \mathbb{R}/\mathbb{Z} is isomorphic to the circle group \mathbb{S}^1 of complex numbers of absolute value 1. The isomorphism is

$$\phi[(r + \mathbb{Z})] = e^{i2\pi r}.$$

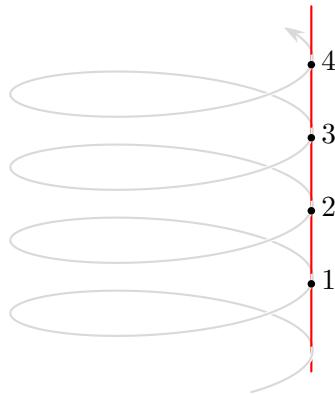


Figure 1.4: The abelian group \mathbb{R}/\mathbb{Z} can be generated by $e^{i2\pi r}$.

1.5.2 Normal subgroups

Definition 1.14 Normal subgroups

A subgroup H of (G, \cdot) is called a normal subgroup if for all $g \in G$ we have

$$gH = Hg. \quad (1.7)$$

We shall denote that H is a subgroup of G by $H < G$, and that H is a normal subgroup of G by $H \triangleleft G$.

If H is a normal subgroup of G , and the order of H is equal to the order of G , we call H the proper normal subgroup, write as $H \trianglelefteq G$.

You should be very careful here. The equality $gH = Hg$ is a set equality. They are not constants or numbers! It says that a right coset is equal to left a coset, it is not an equality elementwise.

 **Example 1.5.3.** Let $\mathbb{R}[x]$ denote the group of all polynomial with real coefficients under normal addition.

For any f in $\mathbb{R}[x]$, let f' denote the derivative of f . Then the mapping $f \rightarrow f'$ is a homomorphism from $\mathbb{R}[x]$ to itself. The kernel of the derivative mapping is the set of all constant polynomials $f(x) = c$.

Now suppose we have a group (G, \cdot) , and H is a normal subgroup of G , just said $H \triangleleft G$. The

set G/H is defined by

$$G/H = \{gH \mid g \in G\}.$$

G/H is known as a **quotient group**.

☞ **Example 1.5.4.** Show that if H and K are normal subgroups of a group G such that $H \cap K = \{e\}$, then $hk = kh$ for all $h \in H$ and $k \in K$.

☞ **Solution** We knew that $H \trianglelefteq G$ and $K \trianglelefteq G$, these conditions imply

$$gHg^{-1} \subseteq H, \quad gKg^{-1} \subseteq K \quad \forall g \in G.$$

Since $khk^{-1} \in kHk^{-1} \subseteq kHk^{-1} \subseteq H$. We want to show $hk = kh$ for all $h \in H$ and $k \in K$. Compute

$$\begin{aligned} h(kh^{-1}k^{-1}) &= e \Rightarrow hkh^{-1}k^{-1} = e \\ &\Rightarrow hkh^{-1} = ke \\ &\Rightarrow hkh^{-1} = khk^{-1} \\ &\Rightarrow hk = kh. \end{aligned}$$



☞ **Example 1.5.5.** Prove that if G is abelian, then every subgroup H is normal.

☞ **Solution** Taking arbitrary $g \in G$. If G is abelian, then

$$gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = HG.$$

Thus H is normal.



1.5.3 Quotient group

Definition 1.15 Quotient group

Let G be a group, with H a subgroup such that $gH = Hg$ for any $g \in G$. The set

$$G/H = \{gH \mid g \in G\}$$

of cosets of H in G is called a **quotient group**.

We can check that G/H is indeed a group:

- Because $gH = Hg \implies gHg' = gg'H$ and G/H is closed under the same binary operator.
- Binary operation $\circ : G/H \times G/H, (gH, g'H) \mapsto gHg'H$ is associative.
- The identity element is H since $H(gH) = gH$ for any g in G .

- The inverse of gH is $g^{-1}H$, since

$$\begin{aligned}(gH)(g^{-1}H) &= (g^{-1}H)(gH) \\ &= (gg^{-1})H \\ &= eH \\ &= H.\end{aligned}$$

1.6 Group homomorphisms

Definition 1.16 Group homomorphisms

A group homomorphism is a map $f : (G, \diamond_G) \rightarrow (H, \bullet_H)$ that respects binary operations:

$$f(a) \bullet_H f(b) = f(a \diamond_G b) \quad \forall a, b \in G \tag{1.8}$$

Theorem 1.11 Properties of homomorphism

Let ϕ be a homomorphism from a group G to a group G' and let g be an element of G . Then

1. ϕ carries the identity of G to the identity of G' .
2. $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{Z}$.
3. If $\text{ord}(g)$ is finite, then $\text{ord}(\phi(g))$ divides $\text{ord}(g)$.
4. $\ker(\phi)$ is a subgroup of G .
5. $\phi(a) = \phi(b)$ if and only if $a \ker(\phi) = b \ker(\phi)$.
6. If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g \ker(\phi)$.

 **Example 1.6.1.** Let G be any group and let a be any element of G . Let $\phi : \mathbb{Z} \rightarrow G$ be defined by

$$\phi(n) = a^n$$

Show that ϕ is a homomorphism. Find the kernel of ϕ .

 **Solution** For all n_1, n_2 in \mathbb{Z} , we want to show

$$\phi(n_1 + n_2) = \phi(n_1) \phi(n_2).$$

In fact,

$$\phi(n_1 + n_2) = a^{n_1+n_2} = a^{n_1} a^{n_2} = \phi(n_1) \phi(n_2).$$

which means ϕ preserves the group operation of G . Again we want to show ϕ is both *one-to-one* and *onto*.

1. (One-to-one) For all $x, y \in \mathbb{Z}$,

$$\begin{aligned}\phi(x) = y &\Rightarrow a^x = y \\ &\Rightarrow x = \frac{\log y}{\log a}, \quad a > 0\end{aligned}$$

2. (Onto) For all $x, y \in \mathbb{Z}$,

$$\phi(x) = \phi(y) \Rightarrow a^x = a^y \Rightarrow x = y.$$

Hence, we compute the kernel of ϕ ,

$$\begin{aligned} Ker(\phi) &= \{n \in \mathbb{Z} \mid \phi(n) = 1\} \\ &= \{n \in \mathbb{Z} \mid a^n = 1\} \\ &= \{n \in \mathbb{Z} \mid a^n = a^0\} \\ &= \{n \in \mathbb{Z} \mid n = 0\} \\ &= \{0\}. \end{aligned}$$



1.7 Isomorphism

Definition 1.17 Group isomorphisms

An isomorphism ϕ from a group G to a group G' is a one-to-one mapping from G onto G' that preserves the group operation. That is,

$$\phi(a) \bullet_G \phi(b) = \phi(a \diamond_{G'} b)$$

for all $a, b \in G$. If there is an isomorphism from $G \rightarrow G'$, we say that G and G' are isomorphic and write as $G \cong G'$.

There are four separate steps involved in proving that a group G is isomorphic to another group G' .

1. Define a candidate for the isomorphism; that is, assume that $\phi(a) = \phi(b)$ and hence prove that $a = b$.
2. Prove that ϕ is one-to-one; that is, assume that $\phi(a) = \phi(b)$ and hence prove that $a = b$.
3. Prove that ϕ is onto; that is, for any element $g' \in G'$, find an element $g \in G$ such that $\phi(g) = g'$.
4. Prove that ϕ is operation-preserving; that is, show that

$$\phi(a) \bullet_G \phi(b) = \phi(a \diamond_{G'} b)$$

for all $a, b \in G$.

 **Example 1.7.1.** Let G be the real numbers under addition and G' be the positive real numbers under multiplication. G and G' are isomorphic under the mapping

$$\phi(x) = 2^x.$$

 **Solution** Define the mapping $\phi : (G = \mathbb{R}, +) \rightarrow (G' = \mathbb{R}^+, \cdot)$. For all x, y in G , we want to show

$$\phi(x + y) = \phi(x) \phi(y).$$

In fact,

$$\phi(x + y) = 2^{x+y} = 2^x 2^y = \phi(x) \phi(y).$$

which means ϕ is homomorphism. Again we want to show ϕ is both *one-to-one* and *onto*.

1. (One-to-one) For all $x, y \in G$,

$$\begin{aligned}\phi(x) = y &\Rightarrow 2^x = y \\ &\Rightarrow x = \log_2 y, \quad y > 0\end{aligned}$$

2. (Onto) For all $x, y \in G$,

$$\phi(x) = \phi(y) \Rightarrow 2^x = 2^y \Rightarrow x = y.$$

Hence, we compute the kernel of ϕ ,

$$\begin{aligned}Ker(\phi) &= \{x \in \mathbb{R} \mid \phi(x) = 1\} \\ &= \{x \in \mathbb{R} \mid 2^x = 1\} \\ &= \{x \in \mathbb{R} \mid x = 0\} \\ &= \{0\}.\end{aligned}$$

◀

 **Example 1.7.2.** Let $G = SL(2, \mathbb{R})$, the group of 2×2 real matrices with determinant 1. Let M be any 2×2 matrix with determinant 1. The mapping ϕ_M from $G \rightarrow G$ defined by

$$\phi_M(A) = MAM^{-1}$$

is an isomorphism.

 **Solution** 1. First we are going to show that ϕ_M is one-to-one; that is, for any $A_1, A_2 \in G$, if $\phi_M(A_1) = \phi_M(A_2)$, then $A_1 = A_2$.

$$\begin{aligned}\phi_M(A_1) = \phi_M(A_2) &\Rightarrow MA_1M^{-1} = MA_2M^{-1} \\ &\Rightarrow \cancel{M^{-1}}MA_1\cancel{M^{-1}} = \cancel{M^{-1}}MA_2\cancel{M^{-1}} \\ &\Rightarrow IA_1I = IA_2I \\ &\Rightarrow A_1 = A_2.\end{aligned}$$

2. Show ϕ_M is onto. For all $A_2 \in G$, we need to find $A_1 \in G$ such that

$$\phi_M(A_1) = A_2.$$

We find an equation for A_1 ,

$$\begin{aligned}\phi_M(A_1) = A_2 &\Rightarrow MA_1M^{-1} = A_2 \\ &\Rightarrow A_1 = M^{-1}A_2M\end{aligned}$$

Now we verify that $\phi_M(A_1) = A_2$. Compute

$$\begin{aligned}\phi_M(A_1) &= \phi_M(M^{-1}A_2M) \\ &= M(M^{-1}A_2M)M^{-1} \\ &= IA_2I \\ &= A_2.\end{aligned}$$

3. At last we are going to show ϕ_M is a homomorphism. That is,

$$\forall A_1, A_2 \in G, \quad \phi_M(A_1 A_2) = \phi_M(A_1) \phi_M(A_2).$$

We start from LHS,

$$\begin{aligned} \phi_M(A_1 A_2) &\Rightarrow MA_1 A_2 M^{-1} \\ &\Rightarrow MA_1 \textcolor{red}{I} A_2 M^{-1} \\ &\Rightarrow MA_1 (\textcolor{red}{M}^{-1} \textcolor{red}{M}) A_2 M^{-1} \\ &\Rightarrow (MA_1 \textcolor{red}{M}^{-1})(\textcolor{red}{M} A_2 M^{-1}) \\ &\Rightarrow \phi_M(A_1) \phi_M(A_2). \end{aligned}$$

Therefore ϕ_M is an isomorphism. ◀

 **Example 1.7.3.** The group $U(10)$ is not isomorphic to $U(12)$.

Theorem 1.12 Cayley's theorem

Every group is isomorphic to a group of permutation.

Proof. Let G be a multiplication group. From group G , we need to construct a permutation group \bar{G} that is isomorphic to G .

Step 1: construct permutation group \bar{G}

Given G , for all $g \in G$. We define a map $T_g : G \rightarrow G$ such that

$$T_g(x) = gx.$$

Let $\bar{G} = \{T_g \mid g \in G\}$. We need to show that \bar{G} under function composition is a group.

1. (Closureness) For all $T_g, T_h \in \bar{G}$, we want to show $T_g \circ T_h \in \bar{G}$.

$$\begin{aligned} T_g \circ T_h &= T_g(T_h(x)) \\ &= T_g(hx) \\ &= g(hx) \\ &= (gh)x \\ &= T_{gh}(x) \in \bar{G}. \end{aligned}$$

2. (Associativity) For all $T_g, T_h, T_k \in \bar{G}$, we have

$$T_g \circ (T_h \circ T_k) = T_{g(hk)} = T_{(gh)k} = (T_g \circ T_h) \circ T_k.$$

The associativity holds in \bar{G} .

3. (Existence of identity) For all $T_g \in \bar{G}$, there exists an $T_{g'} \in \bar{G}$ such that

$$\begin{aligned} T_g \circ T_{g'} &= T_g \Rightarrow T_{gg'} = T_g \\ &\Rightarrow gg' = g \\ &\Rightarrow g' = 1 \end{aligned}$$

so that $g'(x) = 1 \cdot x = x$.

4. (Existence of inverse) For all $T_g \in \bar{G}$, the inverse of T_g is

$$T_{g^{-1}}(x) = g^{-1}x \quad \forall g \in G.$$

Therefore \bar{G} is a group under function composition. In the next step we are going to prove that the mapping from G to \bar{G} is an isomorphism.

Step 2: show that $\phi : G \rightarrow \bar{G}$ is isomorphism

We now define a mapping $\phi : G \rightarrow \bar{G}$, where

$$\phi(g) = T_g(x) = gx \quad \forall g \in G.$$

We perform the 3 steps to check $\phi(g)$ is an isomorphism.

1. (ϕ is one-to-one) For all $g, h \in G$,

$$\begin{aligned} \phi(g) = \phi(h) &\Rightarrow T_g = T_h \\ &\Rightarrow T_g(x) = T_h(x) \quad \forall x \in G \\ &\Rightarrow gx = hx \quad \forall x \in G \\ &\Rightarrow g = h. \end{aligned}$$

2. (ϕ is onto) For all $T_{g'} \in \bar{G}$, we need to find an $g \in G$ such that $\phi(g) = T_{g'}$.

$$\begin{aligned} \phi(g) = T_{g'} &\Rightarrow T_g(x) = T_{g'}(x) \\ &\Rightarrow gx = g'x \\ &\Rightarrow g = g'. \end{aligned}$$

3. (ϕ is homomorphism) To show that ϕ is homomorphism, it is equivalent to show that

$$\phi(g \circ h) = \phi(g) \phi(h).$$

From LHS,

$$\begin{aligned} \phi(g \circ h) &= T_{gh} = T_{gh}(x) \\ &= (g \circ h)x \\ &= gx \cdot hx \\ &= \phi(g) \phi(h). \end{aligned}$$

□

Definition 1.18 Group stabilizer

If G is a group of permutations on the set S and $s \in S$ then we define the **stabilizer** of s to be the set

$$\text{Stab}_G(s) = \{\phi \in G \mid \phi(s) = s\}.$$

Lemma 1.7

If G is a group of permutations of the set S and $s \in S$. Then $\text{Stab}_G(s)$ is a subgroup of G .

Proof. Using two-step subgroup test to verify:

1. $\exists \phi : S \rightarrow S \in \text{Stab}_G(s)$ s.t. $\phi(x) = x$. Thus $\text{Stab}_G(s) \neq \emptyset$.

2. For all $\phi_1, \phi_2 \in \text{Stab}_G(s)$, we have

$$(\phi_1 \circ \phi_2)(s) = \phi_1(\phi_2(s)) = \phi_1(s) = s \in S$$

Therefore $\phi_1 \circ \phi_2 \in \text{Stab}_G(s)$.

3. For all $\phi \in \text{Stab}_G(s)$,

$$\begin{aligned} \phi(s) = s &\Rightarrow \phi^{-1}(\phi(s)) = \phi^{-1}(s) \\ &\Rightarrow \phi^{-1}(s) = s \in S \end{aligned}$$

So ϕ^{-1} is also in $\text{Stab}_G(s)$.

Therefore $\text{Stab}_G(s)$ is a subgroup of G . □

Definition 1.19 Group orbit

If G is a group of permutations of the set S and $s \in S$. We define the **orbit** to be the set

$$\text{Orbit}_G(s) = \{\phi(s) \mid \phi \in G\}.$$

Theorem 1.13 Orbit-Stabilizer theorem

For any group action $\phi : G \rightarrow \text{Permutation}(S)$, and for any $s \in S$,

$$|\text{Orbit}_G(s)| \cdot |\text{Stab}_G(s)| = |G|. \quad (1.9)$$

Proof. We define a mapping $f : G / \text{Stab}_G(s) \rightarrow \text{Orbit}_G(s)$ such that

$$f(\phi \text{Stab}_G(s)) = \phi(s).$$

f is a homomorphism, and we want to show f is one-to-one and onto.

1. (One-to-one) For all $\phi_1, \phi_2 \in \text{Stab}_G(s)$, we have

$$\begin{aligned}\phi_1 \text{Stab}_G(s) = \phi_2 \text{Stab}_G(s) &\Rightarrow (\phi_1^{-1} \circ \phi_2) \in \text{Stab}_G(s) \\ &\Rightarrow (\phi_1^{-1} \circ \phi_2)(s) = s \\ &\Rightarrow \phi_1^{-1}(\phi_2(s)) = s \\ &\Rightarrow \phi_2(s) = \phi_1(s)\end{aligned}$$

2. (Onto) We again want to show f is onto. For all $\phi \in \text{Orbit}_G(s)$, we have

$$f(\phi \text{Stab}_G(s)) = \phi(s).$$

So f is both one-to-one and onto. Which means

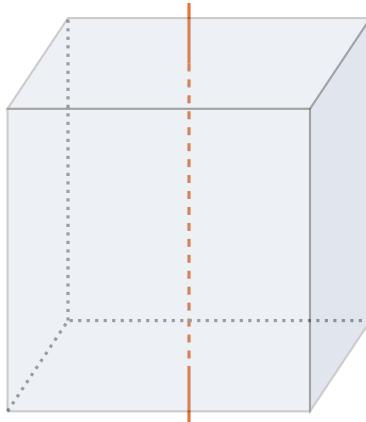
$$\begin{aligned}|G/\text{Stab}_G(s)| = |\text{Orbit}_G(s)| &\implies \frac{|G|}{|\text{Stab}_G(s)|} = |\text{Orbit}_G(s)| \\ &\implies |\text{Orbit}_G(s)| \cdot |\text{Stab}_G(s)| = |G|.\end{aligned}$$

□

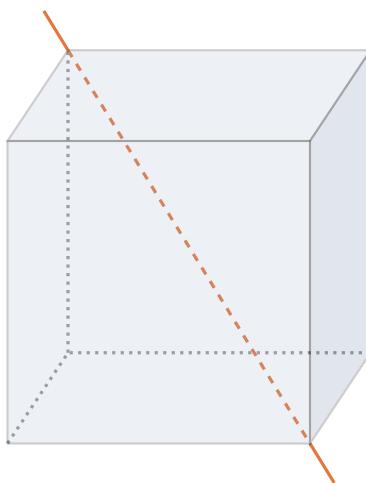
Theorem 1.14

The group of rotations of a cube is isomorphic to S_4 .

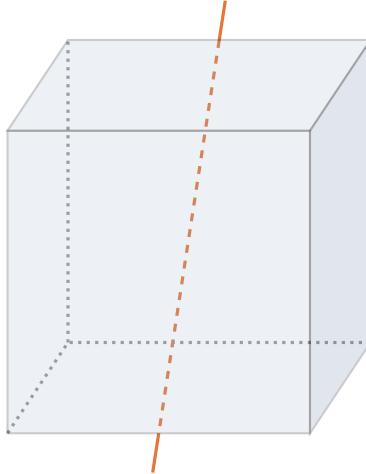
Proof. We can proof it by visualizing the rigid motions of a cube rotated along the possible axes.



One of three possible axes of rotation through the centers of opposite faces. Each rotation could be 0° , 90° , 180° , or 270° , for a total of $3 \times 4 = 12$ rotations of this type. But three in this count are the trivial identity rotation, which we only count once, so there are really 10 unique rotations along these axes.



One of four possible axes of rotation through opposite vertices. Each could be either 120° or 240° , so there are $4 \times 2 = 8$ rotations of this type.



One of six possible axes of rotation through the centers of opposite edges. Only a 180° rotation around these axes would preserve the shape, so we have only 6 rotations possible.

There are $10 + 8 + 6 = 24$ possible ways to rotate a cube, this is equal to the order of S_4 . The order of S_4 is

$$|S_4| = 4! = 4 \times 3 \times 2 \times 1 = 24.$$

□

Theorem 1.15 Properties of isomorphisms

Suppose that ϕ is an isomorphism from a group G onto a group G' . Then

1. ϕ carries the identity of G to the identity of G' .
 2. For every integer n and for every group element a in G ,
- $$\phi(a^n) = \phi(a)^n.$$
3. For any elements a and b of G , a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
 4. $G = \langle a \rangle$ if and only if $G' = \langle \phi(a) \rangle$.
 5. $\text{ord}(a) = \text{ord}(\phi(a))$ for all $a \in G$.
 6. For a fixed integer k and fixed group element $b \in G$, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b) \in G'$.
 7. If G is finite, then G and G' have exactly the same number of elements of every order.

Proof. 1. Work with G , we know $e = g^n g^{-n}$, so

$$\begin{aligned} \phi(e) &= \phi(g^n g^{-n}) \Rightarrow e' = \phi(g^n) \phi(g^{-n}) \\ &\Rightarrow e' = \underbrace{\phi(g * g * \dots * g)}_{n \text{ times}} \underbrace{\phi(g^{-1} * g^{-1} * \dots * g^{-1})}_{n \text{ times}} \\ &\Rightarrow e' = \underbrace{\phi(g) * \phi(g) * \dots * \phi(g)}_{n \text{ times}} \underbrace{\phi(g^{-1}) * \phi(g^{-1}) * \dots * \phi(g^{-1})}_{n \text{ times}} \end{aligned}$$

2. Using the similar technique, we have

$$\phi(g^n) = \underbrace{\phi(g * g * \cdots * g)}_{n \text{ times}} = \underbrace{\phi(g) * \phi(g) * \cdots * \phi(g)}_{n \text{ times}} = \phi(g)^n.$$

3. For all $a, b \in G$, a and b commute if and only if

$$\begin{aligned} ab &= ba \iff \phi(ab) = \phi(ba) \\ &\iff \phi(a)\phi(b) = \phi(b)\phi(a) \\ &\iff \phi(a) \text{ and } \phi(b) \text{ commute} \\ &\iff G' \text{ is abelian.} \end{aligned}$$

4. For all $a \in G$,

$$\begin{aligned} G = \langle a \rangle &\iff \phi(a^n) = \phi(e) \\ &\iff \phi(a^n) = e' \\ &\iff \phi(a)^n = e' \\ &\iff G' = \langle \phi(a) \rangle. \end{aligned}$$

(5, 6, 7) leave as tutorial. □

Theorem 1.16

Suppose that ϕ is an isomorphism from a group G onto a group G' . Then

1. ϕ^{-1} is an isomorphism from G' onto G .
2. G is abelian if and only if G' is abelian.
3. G is cyclic if and only if G' is cyclic.
4. If K is a subgroup of G , then

$$\phi(K) = \{\phi(k) \mid k \in K\}$$

is a subgroup of G' .

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \downarrow \leq & & \downarrow \leq \\ K & \xrightarrow{\phi} & \phi(K) \end{array}$$

Proof. 1. Given that ϕ is a homomorphism, then for all $a, b \in G$ we have

$$\phi(ab) = \phi(a)\phi(b).$$

We need to prove that ϕ^{-1} is also a homomorphism, that is,

$$\forall a', b' \in G' \quad \phi^{-1}(a'b') = \phi^{-1}(a')\phi^{-1}(b').$$

Certainly

$$\begin{cases} \phi(a) = a' \\ \phi(b) = b' \end{cases} \implies \begin{cases} \phi^{-1}(a') = a \\ \phi^{-1}(b') = b \end{cases}$$

Since ϕ is homomorphism,

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) \Rightarrow \phi(ab) = a'b' \\ &\Rightarrow ab = \phi^{-1}(a'b') \\ &\Rightarrow \phi^{-1}(a')\phi^{-1}(b') = \phi^{-1}(a'b') \end{aligned}$$

2. Refer to property (3) of previous theorem.

3. Refer to property (4) of previous theorem.

4. Given K is a subgroup of G , we want to show that $\phi(K) \leq G'$. The main idea is to use one-step subgroup test:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \downarrow \leq & & \downarrow \leq \\ \phi^{-1}(N) & \xleftarrow{\phi^{-1}} & N \end{array}$$

- Clearly, $e' = \phi(e) \in \phi(K)$. Thus $\phi(K)$ is nonempty. (Since $e \in K \neq \emptyset$ as $K \leq G$).
- For all $x, y \in \phi(K)$,

$$x \in \phi(K) \Rightarrow x = \phi(\alpha_1)$$

and

$$y \in \phi(K) \Rightarrow y = \phi(\alpha_2)$$

where $\alpha_1, \alpha_2 \in K$. Compute

$$\begin{aligned} xy^{-1} &= \phi(\alpha_1)\phi(\alpha_2)^{-1} \\ &= \phi(\alpha_1)\phi(\alpha_2^{-1}) \\ &= \phi(\alpha_1\alpha_2^{-1}) \end{aligned}$$

Since $\alpha_1\alpha_2^{-1} \in K$, thus $\phi(\alpha_1\alpha_2^{-1})$ in $\phi(K) \implies xy^{-1} \in \phi(K)$.

□

Theorem 1.17 Sylow's theorem

Let G be a finite group such that p^n divides $|G|$, where p is prime. Then there exists a subgroup of order p^n .

Proof. Assume that $|G| = p^n m$, where $m = p^r k$ with $\gcd(p, k) = 1$. Our central strategy is to consider a cleverly chosen group action of G and prove one of the stabilizer subgroups has order p^n . We will need to heavily exploit the orbit-stabilizer theorem.

Let S be the set of all subsets of G of order p^n . An element of S is an unordered n -tuple of distinct elements in G . There is a natural action of G on S by term-by-term composition on the left.

Consider $\sigma \in S$. If we fix an ordering $\sigma = \{\sigma_1, \sigma_2, \dots, \sigma_{p^n}\} \in S$, then

$$g(\sigma) := \{g * \sigma_1, g * \sigma_2, \dots, g * \sigma_{p^n}\}.$$

We first claim that $|\text{Stab}(\sigma)| \leq p^n$. To see this we define the function

$$f : \text{Stab}(\sigma) \rightarrow \sigma$$

$$g \mapsto g * \sigma_1$$

By the cancellation property for groups this is an injective map. Hence

$$|\text{Stab}(\sigma)| \leq |\sigma| = p^n.$$

On the other hand, observe that

$$|S| = \binom{p^n m}{p^n} = \frac{p^n m!}{(p^n)! (p^n m - p^n)!} = \prod_{j=0}^{p^n-1} \frac{p^n m - j}{p^n - j} = m \prod_{j=1}^{p^n-1} \frac{p^n m - j}{p^n - j}.$$

If $1 \leq j \leq p^n - 1$ then j is divisible by p at most $n - 1$ times. This means that $p^n m - j$ and $p^n - j$ have the same number of p factors, namely the number of p factor of j . This means that

$$\prod_{j=1}^{p^n-1} \frac{p^n m - j}{p^n - j}$$

has no p factors. Hence $p^r u$, where $\gcd(p, u) = 1$.

Now recall that S is the disjoint union of the orbits of our action of G on S . Hence there must be an $\sigma \in S$ such that

$$|\text{Orbit}(\sigma)| = p^s t$$

where $s \leq r$ and $\gcd(p, t) = 1$. By the *orbit-stabilizer theorem* we know that

$$|\text{Stab}(\sigma)| = \frac{p^{n+r-s} u}{t}$$

Because $|\text{Stab}(\sigma)| \in \mathbb{N}$ and u, t are coprime to p , we deduce that u/t is natural number. Hence $|\text{Stab}(\sigma)| \geq p^n$.

For this choice of $\sigma \in S$, $\text{Stab}(\sigma)$ is thus a subgroup of size p^n . □

Historically this is a slight extension of what is called Sylow's First Theorem. There are two more which describe the properties of such subgroups in greater depth.

1.8 Automorphisms

Definition 1.20 Automorphisms

An isomorphism from a group G onto itself is called an automorphism.

Example 1.8.1. Let the 2-dimensional cartesian plane

$$\mathbb{R}^2 = \{(a, b) | a, b \in \mathbb{R}\}.$$

Then

$$\phi(a, b) = (b, a)$$

is an automorphism of the group \mathbb{R}^2 under componentwise addition.

Example 1.8.2. Compute $\text{Aut}(\mathbb{Z}_{10})$.

Solution For any $\alpha \in \text{Aut}(\mathbb{Z}_{10})$ and for any $k \in \mathbb{Z}_{10}$. We define $k \mapsto k\alpha(1)$ such that

$$1 \mapsto \alpha_1 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_1(x) = x$$

$$3 \mapsto \alpha_3 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_3(x) = 3x$$

$$7 \mapsto \alpha_7 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_7(x) = 7x$$

$$9 \mapsto \alpha_9 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_9(x) = 9x$$

In fact, $\text{Aut}(\mathbb{Z}_{10})$ is isomorphic to $U(10) = \{1, 3, 7, 9\}$. $\text{Aut}(\mathbb{Z}_{10})$ is defined as

$$\text{Aut}(\mathbb{Z}_{10}) = \{\alpha : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10} \mid \alpha \text{ is an automorphism}\}.$$

\cdot_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

\circ	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

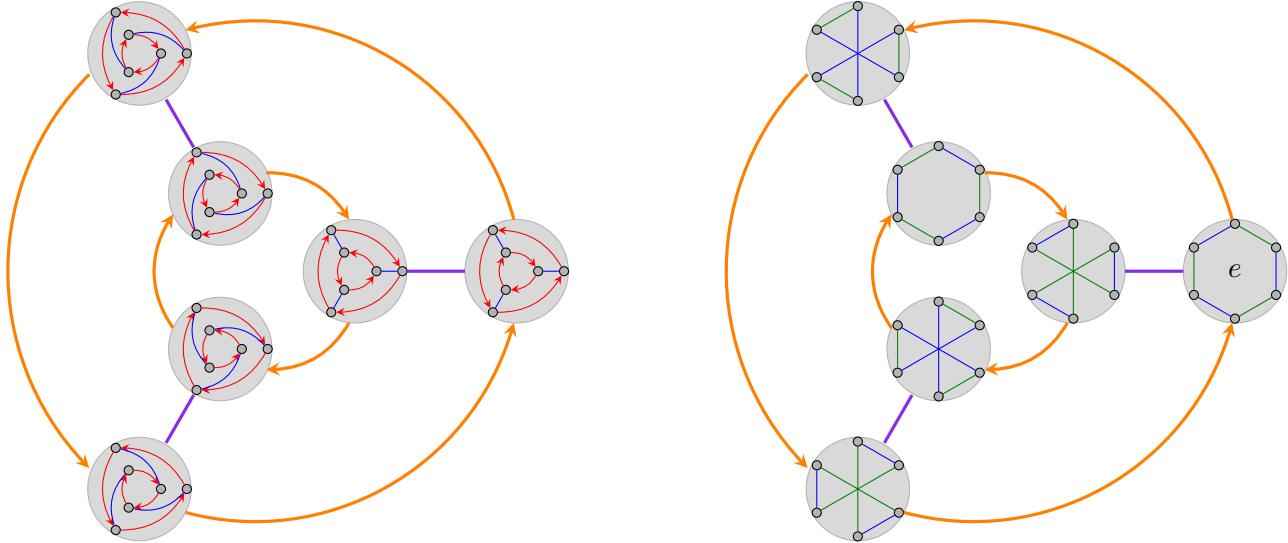
Theorem 1.18

For every positive integer n , $\text{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$.

Example 1.8.3. The automorphisms of D_3 is $\text{Aut}(D_3) = \langle \alpha, \beta \rangle \cong D_3$, where

$$\begin{cases} \alpha(r) = r \\ \alpha(f) = rf \end{cases} \quad \begin{cases} \beta(r) = r^2 \\ \beta(f) = f \end{cases}$$

All of these automorphisms are *inner* (of the form $f_x : g \mapsto x^{-1}gx$). Two Cayley diagrams for $\text{Aut}(D_3)$ are shown below.



Definition 1.21 Inner automorphisms

Let G be a group, and let $a \in G$. The function ϕ_a defined by

$$\phi_a(x) = axa^{-1} \quad \text{for all } x \in G$$

is called the inner automorphism of G included by a .

When G is a group, we use $\text{Aut}(G)$ to denote the set of all automorphisms of G and $\text{Inn}(G)$ to denote the set of all inner automorphisms of G .

Theorem 1.19

The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

Proof. The set of inner automorphisms of G included by a is

$$\text{Inn}(G) = \{\phi_a | \phi_a \text{ is an inner automorphism}\}.$$

Then satisfied the group properties:

1. We want to show $\forall \phi_a, \phi_b \in \text{Inn}(G), \quad \phi_a \circ \phi_b \in \text{Inn}(G)$.

Compute $(\phi_a \circ \phi_b)(g)$ for all g in G ,

$$\begin{aligned}
 (\phi_a \circ \phi_b)(g) &= \phi_a(\phi_b(g)) \\
 &= \phi_a(bgb^{-1}) && \text{(Defn. of inner automorphism)} \\
 &= a(bgb^{-1})a^{-1} \\
 &= (ab)g(b^{-1}a^{-1}) \\
 &= (ab)g(ab)^{-1} && \text{(Socks-shoes property)} \\
 &= \phi_{ab}(g) \in \text{Inn}(G)
 \end{aligned}$$

Thus $\text{Inn}(G)$ is closed under function composition.

2. Next we want to show the associativity in $\text{Inn}(G)$, that is,

$$\forall \phi_a, \phi_b, \phi_c \in \text{Inn}(G), \quad \phi_a \circ (\phi_b \circ \phi_c) = (\phi_a \circ \phi_b) \circ \phi_c$$

we compute $\phi_a \circ (\phi_b \circ \phi_c)$.

$$\begin{aligned} [\phi_a \circ (\phi_b \circ \phi_c)](g) &= a(bc)g(bc)^{-1}a^{-1} \\ &= (ab)cg\,c^{-1}\,b^{-1}\,a^{-1} \\ &= \color{blue}{(ab)}\color{red}{c}\color{red}{g}\color{red}{c^{-1}}\color{blue}{(ab)^{-1}} \\ &= [(\phi_a \circ \phi_b) \circ \phi_c](g) \end{aligned}$$

3. Suppose e is the identity element of G , then $\phi_e(g) = ege^{-1} = g \in \text{Inn}(G)$. ϕ_e is the identity of $\text{Inn}(G)$.

4. For all $\phi_a \in \text{Inn}(G)$, there exists $\phi_{a^{-1}} \in \text{Inn}(G)$ such that

$$\begin{aligned} \phi_a \circ \phi_{a^{-1}} &= a(ag^{-1}a^{-1})a^{-1} \\ &= (a\,a^{-1})g^{-1}(a\,a^{-1}) \\ &= g^{-1} \end{aligned}$$

We have shown that the inner automorphisms are group. Is $\text{Inn}(G)$ a subgroup of $\text{Aut}(G)$? Of course it is. We are going to use one-step subgroup test to find out.

One-step subgroup test:

1. First of all, we want to show

$$\forall \phi_a, \phi_b \in \text{Inn}(G), \phi_a \circ \phi_{b^{-1}} \in \text{Inn}(G).$$

we compute

$$\begin{aligned} (\phi_a \circ \phi_{b^{-1}})(g) &= \phi_a(bg^{-1}b^{-1}) \\ &= a(bg^{-1}b^{-1})a^{-1} \\ &= (ab)g^{-1}(ab)^{-1} \\ &= \phi_{(ab)^{-1}} \in \text{Inn}(G) \end{aligned}$$

□

1.8.1 Isomorphism theorems

Theorem 1.20 First Isomorphism theorem

Let $f : G \rightarrow H$ be a homomorphism of groups with kernel K . Then the quotient group G/K is isomorphic to $\text{Im } f$.

Proof. Step 1: Check if $\text{Ker}(f)$ is a subgroup of G .

The main idea is to use one-step subgroup test to check if $\text{Ker}(f) \leq G$:

1. Since ϕ is a homomorphism, then $\phi(e) = e$; and so

$$e \in \text{Ker}(\phi) \neq \emptyset.$$

So $\text{Ker}(\phi)$ is nonempty.

2. For all $g, h \in \text{Ker}(\phi)$, we need to show that

$$gh^{-1} \in \text{Ker}(\phi).$$

Given that $g \in \text{Ker}(\phi)$, then $\phi(g) = e$. Also, $h \in \text{Ker}(\phi)$, then $\phi(h) = e$. Now compute

$$\begin{aligned}\phi(gh^{-1}) &= \phi(g)\phi(h^{-1}) \\ &= \phi(g)\phi(h)^{-1} \\ &= ee^{-1} \\ &= e \in \text{Ker}(\phi).\end{aligned}$$

Since $gh^{-1} \in \text{Ker}(\phi)$, thus $\text{Ker}(\phi) \leq G$.

Step 2: Check if $\text{Ker}(\phi) \trianglelefteq G$

We want to show $a\text{Ker}(\phi)a^{-1} \subseteq \text{Ker}(\phi)$ for all $a \in G$. This is equivalent to show if $y \in a\text{Ker}(\phi)a^{-1}$, then y is in $\text{Ker}(\phi)$. Using normal subgroup test and check:

$$\begin{aligned}y \in a\text{Ker}(\phi)a^{-1} &\Rightarrow a^{-1}ya \in \text{Ker}(\phi) \\ &\Rightarrow \phi(a^{-1}ya) = e \\ &\Rightarrow \phi(a^{-1})\phi(y)\phi(a) = e \\ &\Rightarrow \phi(y) = \phi(a)\phi(e)\phi(a)^{-1} \\ &\Rightarrow \phi(y) = \phi(a)\phi(e)\phi(a^{-1}) \\ &\Rightarrow \phi(y) = \phi(aea^{-1}) = \phi(aa^{-1}) = \phi(e) = e\end{aligned}$$

Thus y is in $\text{Ker}(\phi)$. So $\text{Ker}(\phi) \trianglelefteq G$.

$$\begin{array}{ccc}G & \xrightarrow{\phi} & G' \\ \text{Ker}(\phi) & \lhd \downarrow & \downarrow \leq \\ G/\text{Ker}(\phi) & \xrightarrow{\cong} & \phi(G)\end{array}$$

Moreover, we still need to show $\phi(G) \leq G'$. $\phi(G)$ is the image of G that is define as

$$\phi(G) = \{\phi(g) \mid g \in G\}.$$

Again we use one-step subgroup test to check. For all $x, y \in \phi(G)$, we want to show xy^{-1} is in $\phi(G)$.

Let $x = \phi(g_1)$, and $y = \phi(g_2)$ where $g_1, g_2 \in G$. Compute

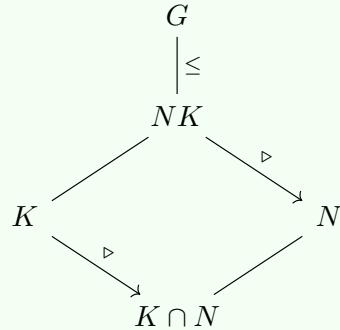
$$\begin{aligned} xy^{-1} &= \phi(g_1) \phi(g_2^{-1}) \\ &= \phi(g_1 g_2^{-1}) \in \phi(G) \end{aligned}$$

The map $T : G/\text{Ker}(\phi) \rightarrow \phi(G)$ (where $T(g\text{Ker}(\phi)) = \phi(g)$) is one-to-one and onto. So T is an isomorphism. \square

Theorem 1.21 Second Isomorphism Theorem

Let K be a proper subgroup of G , and $N \triangleleft G$. Then

1. $NK = \{nk \mid n \in N, k \in K\}$ is a proper subgroup of G , write $NK < G$.
2. $N \triangleleft NK$ and $K \cap N \triangleleft K$.
3. $K/(K \cap N)$ is isomorphism to NK/N .



Proof. 1. Clearly $NK \subset G$. By using two-step subgroup test. For all $nk, n'k' \in NK$

$$nkn'k' = (nn')(kk') \in NK.$$

and

$$nk = e \implies nkk^{-1}n^{-1} = e \implies (nk)^{-1} = k^{-1}n^{-1} \in NK.$$

Thus $NK < G$.

2. Clearly $N \triangleleft NK < G$, since $aN = Na$ whenever a in NK . $N \triangleleft G$ implies that the mapping $\pi : G \rightarrow G/N$ that maps $a \rightarrow Na$ is a surjective homomorphism. We define $f : K \rightarrow G/N$ which $k \mapsto Nk$ whenever k in K . Apparently f is also homomorphism.

The kernel of f is

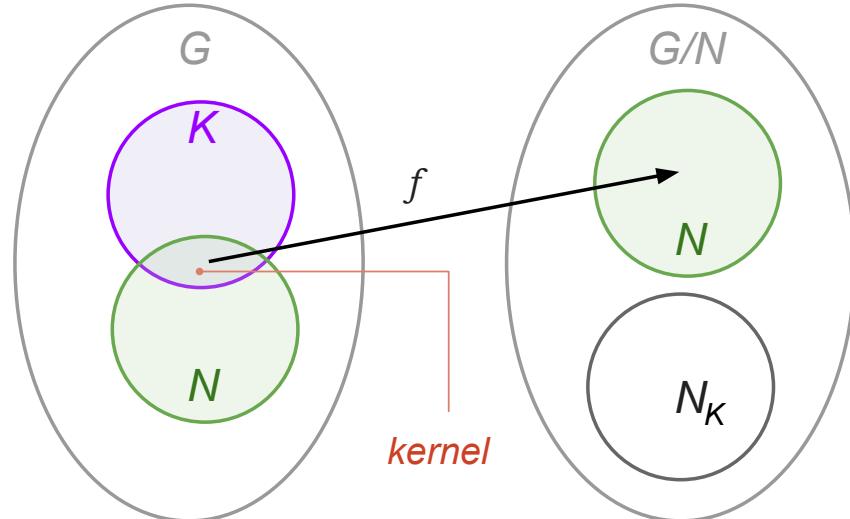
$$\begin{aligned} \ker f &= \{k \in K \mid f(k) = Ne\} \\ &= \{k \in K \mid Nk = Ne\} \\ &= \{k \in K \mid k \in N\} \\ &= K \cap N. \end{aligned}$$

Thus $K \cap N \triangleleft K$.

3. Find the image of f ,

$$\begin{aligned}\text{Im } f &= \{Nk \in G/N \mid k \in K\} \\ &= \{Nnk \in G/N \mid n \in N, k \in K\} \\ &= \{Nnk \in G/N \mid nk \in NK\} \\ &= NK/N.\end{aligned}$$

By First Isomorphism Theorem, we now have $K/(K \cap N)$ is isomorphism to NK/N .



□

Theorem 1.22 Subgroup of the quotient group G/N

Let $N \triangleleft G$, and let $N \subset K < G$. Then K/N is a proper subset of G/N .

Proof. Clearly if $N \triangleleft K$, then

$$K/N = \{N_k \mid k \in K\} \subset G/N = \{N_g \mid g \in G\}.$$

Thus $K/N < G/N$. □

1.9 Lagrange Theorem

Theorem 1.23 Lagrange theorem

If G is a finite group and H is a subgroup of G , then $|H|$ divides $|G|$.

Proof. Let a_1H, a_2H, \dots, a_rH denote the distinct left cosets and right cosets of H in G . For all $a \in G$, $\exists i$ s.t. $aH = a_iH$ and $a \subseteq aH$. Thus we can say that each members in G belongs to the one of the cosets of a_iH . Since $|a_iH| = |H|$, so

$$G = \bigcup_{k=1}^r a_kH \implies |G| = \sum_{k=1}^r |a_kH| = \sum_{k=1}^r |H| = r(|H|).$$

Thus $|H|$ divides $|G|$

□

☞ **Example 1.9.1.** Given G is a group of order 6. Find all possible subgroups of G .

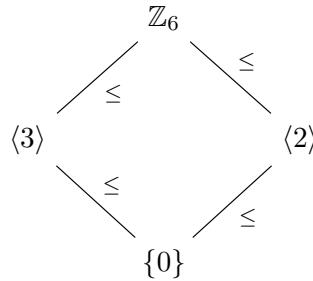
☞ **Solution** Suppose H is a subgroup of G , $H \leq G$, and so by Lagrange's theorem we have

$$|H| \mid |G| = 6$$

which implies $|H| \in \{1, 2, 3, 6\}$.

If the order of H is one, then $H = \langle e \rangle = \{e\}$.

On the other hand, when $|H| = 6$ which means $|H| = |G| = 6$ and $H = G$; that is, H is trivial subgroup.



◀

Theorem 1.24

If G is a group of order p , where p is a prime. Then G is cyclic.

Proof. Suppose H is a subgroup of G and we apply Lagrange's theorem, which we have

$$|H| \mid |G| = p.$$

Assume $H \neq \{e\}$ and the order of H is greater than one, implies $|H| = p$ and so $|G| = |H| = p$.

Hence, since $H \neq \{e\}$, then there exists $a \neq e$ and $a \in H$. So using a to generate we obtained

$$H = G = \langle a \rangle$$

implies that H and G are both cyclic.

□

☞ **Example 1.9.2 (Tutorial).** Draw a subgroup lattice of \mathbb{Z}_{60} .

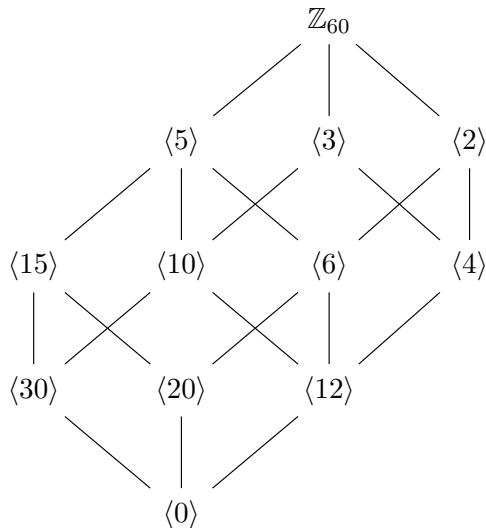
☞ **Solution** Suppose H is a subgroup of \mathbb{Z}_{60} . By Lagrange theorem,

$$|H| \mid 60 = 2^2 \cdot 3 \cdot 5.$$

Thus,

$$|H| \in \{1, 2, 4, 3, 6, 12, 5, 10, 20, 15, 30, 60\}.$$

The lattice diagram is as follow:



1.10 External Direct Product

Definition 1.22 External direct product

Given groups $(G, *)$ and $(H, +)$, the external direct product of G, H written as $G \oplus H$, is the set of all ordered pairs (g, h) for which the binary operation on $G \oplus H$ is defined component-wise:

$$(g_1, h_1) \oplus (g_2, h_2) = (g_1 * g_2, h_1 + h_2).$$

The resulting algebraic object satisfies the axioms for a group. Specifically:

- **Associativity**, the binary operation on $G \times H$ is indeed associative.
- **Existence of identity**, the direct product has an identity element, namely (e_1, e_2) , where e_1 is the identity element of G and e_2 is the identity element of H .
- **Existence of inverses**, the inverse of an element (g, h) of $G \times H$ is the pair (g^{-1}, h^{-1}) , where g^{-1} is the inverse of $g \in G$, and h^{-1} is the inverse of $h \in H$.

Example 1.10.1. Find $U(8) \oplus U(10)$.

Solution We have $U(8) = \{1, 3, 5, 7\}$ and $U(10) = \{1, 3, 7, 9\}$. Then $U(8) \oplus U(10)$ is the cartesian product of each element.

	1	3	7	9
1	(1, 1)	(1, 3)	(1, 7)	(1, 9)
3	(3, 1)	(3, 3)	(3, 7)	(3, 9)
5	(5, 1)	(5, 3)	(5, 7)	(5, 9)
7	(7, 1)	(7, 3)	(7, 7)	(7, 9)

Theorem 1.25

The order of an element in a direct product of a finite number of finite groups is the *least common multiple* of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \dots, g_n)| = \text{LCM}(\text{ord}(g_1), \text{ord}(g_2), \dots, \text{ord}(g_n)).$$

Proof. First we consider the case where the direct product has two components.

Consider $(g_1, g_2) \in G_1 \oplus G_2$. Let $s = \text{LCM}(\text{ord}(g_1), \text{ord}(g_2))$ and $t = |(g_1, g_2)|$. Then

$$(g_1, g_2)^s = (g_1^s, g_2^s) = (e, e) \implies t|s.$$

Thus $t \leq s$. But

$$(g_1^t, g_2^t) = (g_1, g_2)^t = (e, e) \implies g_1|t \text{ and } g_2|t.$$

Thus t is a common multiple of $\text{ord}(g_1)$ and $\text{ord}(g_2)$, which means $s \leq t$ since

$$s = \text{LCM}(\text{ord}(g_1), \text{ord}(g_2)).$$

Hence $s = t$ and $|\text{ord}(g_1, g_2)| = \text{LCM}(\text{ord}(g_1), \text{ord}(g_2))$.

For the general case, suppose the result holds for

$$G_1 \oplus G_2 \oplus \dots \oplus G_{n-1}.$$

But $G_1 \oplus G_2 \oplus \dots \oplus G_n = (G_1 \oplus G_2 \oplus \dots \oplus G_{n-1}) \oplus G_n$. So applying the previous argument, the result holds for

$$G_1 \oplus G_2 \oplus \dots \oplus G_n$$

by induction. □

Theorem 1.26

Let G_1 and G_2 be two groups. Let H_1 and H_2 be normal subgroups of G_1 and G_2 respectively then

$$H_1 \oplus H_2 \trianglelefteq G_1 \oplus G_2.$$

Proof. Since H_1 is a subgroup of G_1 and H_2 is a subgroup of G_2 , therefore $H_1 \oplus H_2$ is subgroup of $G_1 \oplus G_2$.

Now let $(h_1, h_2) \in H_1 \oplus H_2$ and $(g_1, g_2) \in G_1 \oplus G_2$, then

$$\begin{aligned} (g_1, g_2)(h_1, h_2)(g_1, g_2)^{-1} &= (g_1 h_1, g_2 h_2)(g_1^{-1}, g_2^{-1}) \\ &= (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}) \in H_1 \oplus H_2. \end{aligned}$$

$g_1 h_1 g_1^{-1} \in H_1$ and $g_2 h_2 g_2^{-1} \in H_2$ because $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$. Thus $H_1 \oplus H_2 \trianglelefteq G_1 \oplus G_2$. □

1.11 Internal Direct Product

Definition 1.23

Let $(G, *)$ be a group and let $(H, *)$ and $(K, *)$ be two subgroups of G . Then G is said to be the internal direct product of H and K (write $G = H \times K$) if:

1. $G = \{h * k \mid h \in H, k \in K\}$.
2. $H \cap K = \{e\}$ where e is the identity in G .
3. $h * k = k * h$ for all $h \in H$ and for all $k \in K$.

Remark. If $H, K \triangleleft G$, then

$$H \times K \cong H \oplus K.$$

☞ **Example 1.11.1.** Consider $H = \{0, 2, 4\}$ and $K = \{0, 3\}$, show that $G = \mathbb{Z}_6$ is the internal direct product of H and K .

☞ **Solution** 1. We check $G = H \times K$, compute

$$\begin{aligned} G &= H \times K \\ &= \{0, 2, 4\} \times \{0, 3\} \\ &= \{0 +_6 0, 0 +_6 3, 2 +_6 0, 2 +_6 3, 4 +_6 0, 4 +_6 3\} \\ &= \{0, 3, 2, 5, 4, 1\} = \mathbb{Z}_6. \end{aligned}$$

2. $H \cap K = \{0\}$, 0 is identity of \mathbb{Z}_6 .

3. $\forall a \in H, b \in K, a +_6 b = b +_6 a$.

H and K are subgroups of $G = \mathbb{Z}_6$. Thus G is the internal direct product of H and K . ◀

☞ **Example 1.11.2.** \mathbb{Z}_6 is internal direct product of \mathbb{Z}_2 and \mathbb{Z}_3 .

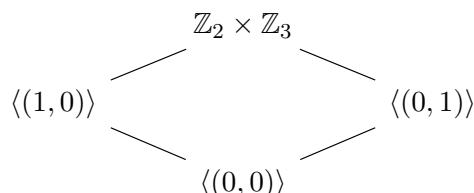
☞ **Solution** The direct product of \mathbb{Z}_2 and \mathbb{Z}_3 form a tuple,

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_3 &= \{(x, y) \mid x \in \mathbb{Z}_2 \text{ and } y \in \mathbb{Z}_3\} \\ &= \{(0, 0), (0, 1), (0, 2) \\ &\quad (1, 0), (1, 1), (1, 2)\} \end{aligned}$$

For all $(a_1, b_1), (a_2, b_2)$, we define the product as

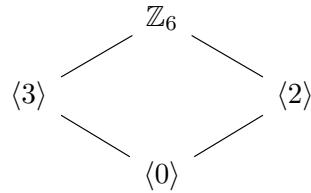
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 +_2 a_2, b_1 +_3 b_2).$$

For example, $(1, 0) \cdot (1, 2) = (1 + 0 \bmod 2, 1 + 2 \bmod 3) = (1, 0)$. Compute the Cayley table for all elements in $\mathbb{Z}_2 \times \mathbb{Z}_3$ (it is actually a 6×6 **Latin square**)



.	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 1)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)
(0, 2)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 1)	(1, 1)	(1, 2)	(1, 0)	(0, 1)	(0, 2)	(0, 0)
(1, 2)	(1, 2)	(1, 0)	(1, 1)	(0, 2)	(0, 0)	(0, 1)

Which is quite matches with the Cayley table of \mathbb{Z}_6 .



.	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

In fact, $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to \mathbb{Z}_6 . ◀

1.12 Finite Abelian groups

Theorem 1.27 Fundamental theorem of Finite Abelian groups

Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Since a cyclic group of order n is isomorphic to \mathbb{Z}_n . Then every finite Abelian group G is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where i 's are not necessarily distinct primes and the prime powers $p_1^{n_1}, p_2^{n_2}, \dots, p_k^{n_k}$ are uniquely determined by G .

Look at groups whose orders have the form p^k , where p is prime and $j \leq 4$. There is one group of order p^k for each set of positive integers whose sum is k (such a set is called a partition of k); that is, if k can be written as $k = n_1 + n_2 + \cdots + n_t$, where each n_i is a positive integer, then $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$ is an Abelian group of order p^k .

Order of G	Partitions of k	Possible direct products of G
p	1	\mathbb{Z}_p
p^2	2	\mathbb{Z}_{p^2}
	1 + 1	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	\mathbb{Z}_{p^3}
	1 + 2	$\mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$
	1 + 1 + 1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
p^4	4	\mathbb{Z}_{p^4}
	1 + 3	$\mathbb{Z}_p \oplus \mathbb{Z}_{p^3}$
	2 + 2	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
	1 + 1 + 2	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$
	1 + 1 + 1 + 1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

1.12.1 Greedy algorithm for an Abelian group of order p^n

Here are the procedure to find all the possible abelian group of order p^n . Note that p is prime.

1. Compute the orders of the elements of the group G .
2. Select an a_1 of maximum order and define $G_1 = \langle a_1 \rangle$. Set $i = 1$.
3. If $|G| = |G_i|$, stop. Otherwise, replace i by $i + 1$.
4. Select an element a_i of maximum order p^k such that

$$p^k \leq |G|/|G_{i-1}|$$

and none of $a_i, a_i^{p^1}, a_i^{p^2}, \dots, a_i^{p^{k-1}}$ is in G_{i-1} , and define $G_i = G_{i-1} \times \langle a_i \rangle$.

5. Return to step 3.

In the general case where $|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, we simply use the algorithm to build up a direct product of order $p_1^{n_1}$, then another of order $p_2^{n_2}$, and so on. The direct product of all these pieces is the desired factorization of G .

☞ **Example 1.12.1.** Let $G = \{1, 8, 12, 14, 18, 21, 31, 34, 38, 44, 47, 51, 52, 57, 64\}$ under multiplication modulo 65. Show that G is isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

☞ **Solution** Since G has order 16, we have

$$\begin{aligned} G &\cong \mathbb{Z}_{16} \\ &\cong \mathbb{Z}_2^4 && \text{take } p = 2, k = 4 \\ &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3} && \text{Partitions of } k = 1 + 3 \\ &\cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} && \text{Partitions of } k = 2 + 2 \\ &\cong \mathbb{Z}_4 \oplus \mathbb{Z}_4 \end{aligned}$$



Pseudocode 1: Greedy algorithm for an Abelian group of order p^n

```

// Main body of greedy algorithm for finding Abelian group of order  $p^k$ .
1 function Main_greedy_algorithm( $G$ : FiniteGroup) → Product of CyclicGroups
2    $\bar{a} \leftarrow \text{find\_element\_with\_max\_order}(G)$ 
   // Generated subgroup with first element  $\bar{a}_1$  from  $\bar{a}$ .
3    $H \leftarrow \langle \bar{a}_1 \rangle$ 
4    $i \leftarrow 1$ 
5   while  $|H| \neq |G|$  do                                ▷ Greedy search for all cyclic groups
6      $\text{max\_cyclic\_order} = |G|/|H|$ 
7      $\langle a_i \rangle = []$ 
8     while  $p^k \leq \text{max\_cyclic\_order}$  do          ▷ Check if  $\bar{a}_i^{p^{k-1}}$  already in previous  $H$ 
9       if  $\bar{a}_i^{p^{k-1}} \notin H$  then
10         $\langle a_i \rangle.\text{push}(\bar{a}_i^{p^{k-1}})$ 
11      else
12        continue
13       $k \leftarrow k + 1$ 
14       $H \leftarrow H \times \langle a_i \rangle$ 
15       $i \leftarrow i + 1$ 
16   return  $H$ 

// Compute the orders for all elements in group  $G$ .
17 function compute_orders( $G$ : FiniteGroup) → orders
18    $orders = []$ 
19   for  $a_i \in G$  do                                ▷ elements in  $G$ 
20     if  $a_i == \text{identity}(G)$  then
21       return 1                                     ▷ The order of identity element is one.
22     else
23        $j \leftarrow 1$ 
24       while  $a_i^j \neq e$  do                  ▷ Find the order of each element.
25          $j \leftarrow j + 1$ 
26        $orders.\text{push}(j)$ 
27   return  $orders$ 

// Filter out  $a_i$  with maximum order, return a list of tuple  $(a_i, |\langle a_i \rangle|)$ .
28 function find_element_with_max_order( $G$ : FiniteGroup) → Array<tuple(element, order)>
29    $orders \leftarrow \text{compute\_orders}(G)$ 
30   return  $\text{zip}(G, orders).\text{filter}((_, o) \rightarrow o == \text{Max}(orders))$ 

```

Example 1.12.2. Let $G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$ under multiplication modulo 135. Show that G is isomorphic to $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$.

Solution Since G has order 24, and the prime factorization of $24 = 3 \cdot 2^3$. We have

$$\begin{aligned}
G &\cong \mathbb{Z}_{24} \\
&\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{2^3} \\
&\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \\
&\cong \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \\
&\cong \mathbb{Z}_{3 \times 4} \oplus \mathbb{Z}_2 && \text{Since } \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq} \\
&\cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2
\end{aligned}$$

Tutorials

Exercise 1.12.1 Prove whether the following group G together with operation $*$ is a group.

1. Let $*$ defined on $G = \mathbb{R}$ by letting $a * b = ab \quad \forall a, b \in \mathbb{R}$.
2. Let $*$ defined on $G = 2\mathbb{Z}$ by letting $a * b = a + b \quad \forall a, b \in 2\mathbb{Z}$.
3. Let $*$ defined on $G = \mathbb{R}^*$ by letting $a * b = \sqrt{ab} \quad \forall a, b \in \mathbb{R}^*$.
4. Let $*$ defined on $G = \mathbb{Z}$ by letting $a * b = \max\{a, b\} \quad \forall a, b \in \mathbb{Z}$.

Exercise 1.12.2 Determine whether the given set of matrices under the specified operation, matrix addition or multiplication, is a group.

1. All 2×2 diagonal matrices under matrix addition.
2. All 2×2 diagonal matrices under matrix multiplication.
3. All 2×2 diagonal matrices with no zero diagonal entry under matrix multiplication.
4. All 2×2 diagonal matrices with all diagonal entries either 1 or -1 under matrix multiplication.
5. All 2×2 upper-triangular matrices under matrix multiplication.
6. All 2×2 upper-triangular matrices under matrix addition.
7. All 2×2 upper-triangular matrices with determinant 1 under matrix multiplication.
8. All 2×2 upper-triangular matrices with determinant either 1 or -1 under matrix multiplication.

Exercise 1.12.3 Prove whether

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0, a, b, c, d \in \mathbb{Z} \right\}$$

is a group under matrix multiplication.

Exercise 1.12.4 Prove whether

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid ad \neq 0, a, b, d \in \mathbb{Z} \right\}$$

is a non-abelian group under matrix multiplication.

Exercise 1.12.5 Prove whether

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \mid a \neq 0, a, b \in \mathbb{Z} \right\}$$

is an abelian group under matrix multiplication.

Exercise 1.12.6 Let $(G, *)$ be a group and suppose that

$$a * b * c = e \quad \forall a, b, c \in G.$$

Show that $b * c * a = e$.

Exercise 1.12.7 Show that if every element of the group G is its own inverse, then G is abelian.

Exercise 1.12.8 Show that every group with identity e and $x \cdot x = x$ for all $x \in G$ is abelian.

Exercise 1.12.9 Show that if G is a finite group with identity e and with even number of elements, then there is an $a \neq e$ in G such that $a * a = e$.

Exercise 1.12.10 Suppose G is a group such that

$$(ab)^2 = a^2 b^2 \quad \forall a, b \in G.$$

Show that G is abelian.

Exercise 1.12.11 Which of the following groups are cyclic? List all the generators of the group.

1. $G_1 = \{6^n \mid n \in \mathbb{Z}\}$ under multiplication.
2. $G_2 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ under addition.

Exercise 1.12.12 Find the order of the following cyclic groups.

1. The subgroup of $U(6)$ generated by $\cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$.
2. The subgroup of $U(5)$ generated by $\cos\left(\frac{4\pi}{3}\right) + i \sin\left(\frac{4\pi}{3}\right)$.
3. The subgroup of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ generated by $(1, 5)$.

Exercise 1.12.13 Let a and b be elements of a group G . Show that if ab has finite order n , then ba also has order n .

Exercise 1.12.14 Let G be a group and $a \in G$ generates a cyclic group of order 2 and is the unique such element. Show that $ax = xa$ for all $x \in G$.

Exercise 1.12.15 Show that a group with no proper nontrivial subgroup is cyclic.

Exercise 1.12.16 Show that \mathbb{Z}_p has no proper nontrivial subgroup if p is prime.

Exercise 1.12.17 Let G be an abelian group and H and K are finite subgroups of G such that $|H| = r$ and $|K| = s$. Show that if $\gcd(r, s) = 1$, then G contains a cyclic subgroup of order rs .

Exercise 1.12.18 Let G be a group and $a \in G$. Show that the centralizer of a in G ,

$$C(a) = \{x \in G \mid xa = ax\},$$

is a subgroup of G .

Exercise 1.12.19 Let G be a nonabelian group with center $Z(G)$. Show that there exists an abelian subgroup H of G such that $Z(G) \subset H$ but $Z(G) \neq H$.

Exercise 1.12.20 Find all subgroups of the following groups and draw the subgroups diagram for the subgroups. Hence, list all orders of the subgroups of the given groups.

1. \mathbb{Z}_{36}
2. \mathbb{Z}_{60}

Exercise 1.12.21

1. Find all the proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
2. Find all the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4$ of order 4.

Exercise 1.12.22

1. Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic?
2. Are the groups $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ and $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$ isomorphic?

Exercise 1.12.23 Show that a group that has only finite number of subgroups must be a finite group.

Exercise 1.12.24 Find all cosets of the subgroup $\langle 3 \rangle$ of \mathbb{Z}_{24} .

Exercise 1.12.25 Compute the quotient group $\mathbb{Z}_{12}/\langle 2 \rangle$.

Exercise 1.12.26 Let $\phi : G \rightarrow G$ be a mapping defined by

$$\phi(x) = x^3 \quad \forall x \in G$$

where $G = \mathbb{R} \setminus \{0\}$ is a group defined under usual multiplication. Show that ϕ is a homomorphism, and hence find $\ker(\phi)$.

Exercise 1.12.27 Let $\phi : G \rightarrow G$ be a mapping defined by

$$\phi(x) = 5^x \quad \forall x \in G$$

where $G = \mathbb{R} \setminus \{0\}$ is a group defined under usual multiplication. Show that ϕ is a homomorphism, and hence find $\ker(\phi)$.

Exercise 1.12.28 Let $\phi : G \rightarrow G$ be a mapping defined by

$$\phi(x) = 7x \quad \forall x \in G$$

where $G = \mathbb{Z}$ is a group defined under usual addition. Show that ϕ is a homomorphism, and hence find $\ker(\phi)$.

Exercise 1.12.29 Let G be a group and g an element in G . Consider the mapping $\phi : G \rightarrow G$ defined as $\phi(x) = gxg^{-1}$. Show that ϕ is an isomorphism.

Exercise 1.12.30 Let $\phi : G \rightarrow G'$ be a group homomorphism and let $N \triangleleft G$. Show that $\phi(N) \triangleleft \phi(G)$.

Exercise 1.12.31 Let $\phi : G \rightarrow G'$ be a group homomorphism and let $N' \triangleleft G'$. Show that $\phi^{-1}(N') \triangleleft G$.

Exercise 1.12.32 Find $\ker(\phi)$ for map $\phi : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{20}$ such that $\phi(1) = 8$.

Exercise 1.12.33 Find $\ker(\phi)$ for map $\phi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ such that $\phi(1, 0) = (2, -3)$ and $\phi(0, 1) = (-1, 5)$.

Exercise 1.12.34 Let $\phi : G \rightarrow H$ be a group homomorphism. Show that $\phi(G)$ is abelian if and only if

$$xyx^{-1}y^{-1} \in \ker(\phi) \quad \forall x, y \in G.$$

Exercise 1.12.35 Consider A the set of affine maps of \mathbb{R} , that is

$$A = \{f : x \mapsto ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}$$

1. Show that A is a group with respect to the composition of map.
2. Let

$$N = \{g : x \mapsto x + b, b \in \mathbb{R}\}$$

Show that $N \triangleleft A$.

3. Show that the quotient group A/N is isomorphic to \mathbb{R}^* .

Exercise 1.12.36 Find the conjugacy classes of dihedral group order 8.

Exercise 1.12.37 Let $G = S_4$ and let the Klein-four group

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

1. Show that H is a normal subgroup of G .
2. Let $\bar{H} = \{\sigma \in S_4 \mid \sigma(4) = 4\}$. Define $\sigma : \bar{H} \rightarrow \text{Aut}(H)$ by $\sigma(\tau) = \sigma\tau\sigma^{-1}$ for $\sigma \in \bar{H}$. Prove that

$$\bar{H} \ltimes_{\sigma} H \cong S_4.$$

Exercise 1.12.38 Find (up to isomorphism) all abelian groups of order 45.

Exercise 1.12.39 Show that any group of order p^2 is abelian.

Exercise 1.12.40 Let G be a group of order pq , where p and q are prime numbers. Show that every proper subgroup of G is cyclic.

Exercise 1.12.41 If $H \leq G$ such that the product of two right cosets of H is always a right coset of H in G , prove that $H \triangleleft G$.

Exercise 1.12.42 Show that if H is a subgroup of index 2 in a finite group G , then every left coset of H is also a right coset of H .

Exercise 1.12.43 If $H, K \leq G$, show that $H \cap K \leq G$.

Exercise 1.12.44 If $N \triangleleft G$ and $H \leq G$, show that $NH \leq G$.

Exercise 1.12.45 If $N_1, N_2 \triangleleft G$, show that $N_1 \cap N_2 \triangleleft G$.

Exercise 1.12.46 If $N \triangleleft G$ and $H \leq G$, show that $H \cap N \triangleleft G$.

This page intentionally left blank.

Rings

Ring is an algebraic structure which is a set of elements with two operations: addition and multiplication.

Axiom 2.1 Rings

A ring R is a set with two binary operation, addition (usually denoted by $+$) and multiplication (usually denoted by ab), such that for all $a, b, c \in R$.

1. Addition is commutative, $a + b = b + a$.
2. Associativity holds in addition, $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0_R . That is, there is an element $0_R \in R$ such that

$$a + 0_R = a = 0_R + a$$

for all $a \in R$.

4. There is an additive inverse $-a \in R$ such that

$$a + (-a) = 0_R = -a + a.$$

5. Associativity holds in multiplication, $a(bc) = (ab)c$.
6. Distributive law holds in R ,

$$a(b + c) = ab + ac$$

and

$$(b + c)a = ba + ca.$$

Here are a few things you should take notes:

1. A ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition.
2. Note that multiplication need not be commutative. When it is, we say that the ring is commutative.
3. A ring need not have an identity under multiplication. A unity (or identity) in a ring is a nonzero element that is an identity under multiplication.
4. A nonzero element of a commutative ring with unity need not have multiplicative inverse. When it does, we say that it is a unit of the ring. Thus, x is a unit if x^{-1} exists.
5. We follow the following terminology and notation. If x and y belong to a commutative ring R and x is nonzero, we say that x divides y and write $x|y$, if there exists an element c in R such that $y = xc$.

6. If x is an element from a group under the operation of addition and n is a positive integer, nx means $\underbrace{x + x + \cdots + x}_{n \text{ times}}$, where there are n summands.

 **Example 2.0.1.** The set \mathbb{Z} of integers under ordinary addition and multiplication is a commutative ring with unity 1. The units of \mathbb{Z} are 1 and -1 .

 **Example 2.0.2.** The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries is a noncommutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

 **Example 2.0.3.** The set of all continuous real-valued functions of a real variable whose graphs pass through the point $(1, 0)$ is a commutative ring without unity under the operations of pointwise addition and multiplication, that is,

$$(f + g)(x) = f(x) + g(x)$$

and

$$(fg)(x) = f(x)g(x).$$

Theorem 2.1

Let a, b and c belong to a ring R . Then

1. $a0 = 0a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.
5. Furthermore, if R has a unity element 1, then $(-1)a = -a$.
6. $(-1)(-1) = (-1)^2 = 1$.

Proof. We are going to prove each of them:

1.

$$\begin{aligned} a(0 + 0) &= a0 \Rightarrow a0 + a0 = a0 \\ &\Rightarrow (-a0) + a0 + a0 = (-a0) + a0 \\ &\Rightarrow 0 + a0 = 0 \\ &\Rightarrow a0 = 0. \end{aligned}$$

2.

$$\begin{aligned} a0 = 0 &\Rightarrow a(b + (-b)) = 0 \\ &\Rightarrow ab + a(-b) = 0 \\ &\Rightarrow - (ab) + ab + a(-b) = - (ab) + 0 \\ &\Rightarrow a(-b) = -(ab). \end{aligned}$$

3.

$$\begin{aligned}(-a)(-b) &= -(a(-b)) \\&= -(a(-b)) \\&= -(-(ab)) \\&= ab.\end{aligned}$$

4.

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac.$$

5.

$$\begin{aligned}0a = 0 &\Rightarrow (1 + (-1))a = 0 \\&\Rightarrow 1a + (-1)a = 0 \\&\Rightarrow a + (-1)a = 0 \\&\Rightarrow \color{red}{(-a)} + a + (-1)a = \color{red}{(-a)} + 0 \\&\Rightarrow 0 + (-1)a = \color{red}{(-a)} \\&\Rightarrow (-1)a = -a.\end{aligned}$$

6.

$$(-1)(-1) = -(1(-1)) = -(-(1 \cdot 1)) = 1.$$

□

Lemma 2.1

If a ring has a unity, it is unique.

Proof. Suppose 1_R and $1'_R$ are both unity of ring R . Then For all $a \in R$, we must have

$$a \cdot 1_R = a = 1_R \cdot a$$

and

$$a \cdot 1'_R = a = 1'_R \cdot a.$$

Thus, we say that $a \cdot 1_R = a = a \cdot 1'_R$. By cancellation law this yields

$$1_R = 1'_R.$$

So ring R has unique unity. □

2.1 subrings

Theorem 2.2 Subring test

A nonempty subset S of the ring R is a subring if S is closed under subtraction and multiplication, that is,

1. $S \neq \emptyset$.
2. $a - b \in S \quad \forall a, b \in S$.
3. $ab \in S \quad \forall a, b \in S$.

Proof. Since addition in R is commutative and S closed under subtraction, we know that by the one-step subgroup test that S is an Abelian group under addition.

Also, since multiplication in R is associative as well as distributive over addition, the same is true for multiplication in S .

Therefore, the only condition remaining to be checked is that multiplication is a binary operation on S . But this is exactly what closure means. \square

☞ **Example 2.1.1.** $S = \{0, 2, 4\}$ is a subring of \mathbb{Z}_6 .

☞ **Solution** Using subring test, the subtraction is closed and the multiplication form a group in S .

-	0	2	4
0	0	4	2
2	2	0	4
4	4	2	0

.	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

Thus $S \leq \mathbb{Z}_6$. \blacktriangleleft

2.2 Quotient rings, Ideals

2.2.1 Ideals

Definition 2.1 Ideals

A subring A of a ring R is called an ideal if for every $r \in R$ and every $a \in A$ both ra and ar are in A .

So, a subring A of a ring R is an ideal of R if

$$rA = \{ra \mid a \in A\} \subseteq A$$

and

$$Ar = \{ar \mid a \in A\} \subseteq A$$

for all $r \in R$. An ideal A of R is called a **proper ideal** of R if A is a proper subset of R .

Lemma 2.2

Let I be a subring of a ring R . Then I is an ideal in R if and only if multiplication

$$(a + I)(b + I) = (ab + I)$$

is a well-defined operation on the cosets of I in R .

Proof. (\Rightarrow) Assume that I is an ideal in R , and suppose that $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$. This implies that $a_1 = a_2 + k$ and $b_1 = b_2 + j$ for some $i, j \in I$. Then we have

$$a_1 b_1 = a_2 b_2 + a_2 j + k b_2 + k j.$$

Since I is a subring of R , and therefore it closed under multiplication, as well as addition, and $kj \in I$. Since I is an ideal, $a_2 j \in I$ and $k b_2 \in I$, and so $a_2 j + k b_2 + kj \in I$.

Therefore, $a_1 b_1 \in a_2 b_2 + I$ and $a_1 b_1 + I = a_2 b_2 + I$. Thus, the multiplication on the set of cosets of I is well-defined.

(\Leftarrow) Assume that the indicated operation is well-defined. We need to show that for all $r \in R$, and for all $x \in I$, we have $rx \in I$ and $xr \in I$. So we have $x + I = 0 + I = I$. Hence

$$rx + I = (r + I)(x + I) = (r + I)(0 + I) = 0 + I = I.$$

Again we have $xr \in I$. Thus I is an ideal in R . \square

Theorem 2.3 Ideal test

A nonempty subset A of a ring R is an ideal of R provided

1. $A \neq \emptyset$.
2. $a - b \in A$ whenever $a, b \in A$.
3. ra and ar are in A for all $a \in A$ and $r \in R$.

☞ **Example 2.2.1.** For any ring R , $\{0\}$ and R are ideals of R . The ideal $\{0\}$ is called the trivial ideal.

☞ **Example 2.2.2.** For any positive integer n , the set

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

is an ideal of \mathbb{Z} .

☞ **Solution** We can show $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ using ideal test.

1. Since $0 \in \mathbb{Z}$, then $n \cdot 0 = 0 \in n\mathbb{Z} \neq \emptyset$.
2. For all $a, b \in n\mathbb{Z}$, we let $a = nt_1$ and $b = nt_2$ for $t_1, t_2 \in \mathbb{Z}$. We have

$$a - b = nt_1 - nt_2 = n(t_1 - t_2) \in n\mathbb{Z}$$

since $t_1 - t_2$ is also an integer.

3. Whenever $a \in A$ and $r \in R$, let $a = nt'$, $t' \in \mathbb{Z}$. We have

$$ar = (nt')r = n(t'r) \in n\mathbb{Z}, \quad t'r \in \mathbb{Z}.$$

and

$$ra = r(nt') = nrt' = n(rt') = n(t'r) = ar \in n\mathbb{Z}.$$

Therefore $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.



Example 2.2.3. Let R be a commutative ring with unity and let $a \in R$. The set

$$\langle a \rangle = \{ra \mid r \in R\}$$

is an ideal of R called the **principal ideal** generated by a .

Solution Using ideal test to check

1. Since R is a ring, then $0_R \in R$ and so $0_R = 0_R \cdot a \in \langle a \rangle \neq \emptyset$.
2. For all $b, c \in \langle a \rangle$, let $b = r_1a$, $c = r_2a$, where $r_1, r_2 \in R$. Then

$$b - c = r_1a - r_2a = (r_1 - r_2)a \in \langle a \rangle.$$

and $r_1 - r_2$ is in R .

3. For all $\bar{a} \in \langle a \rangle$, $r \in R$, we let $\bar{a} = r'a$ and

$$\bar{a}r = (r'a)r = a(r'r) \in \langle a \rangle.$$

where $r'r \in R$.

On the other hand,

$$r\bar{a} = r(r'a) = a(rr') = a(r'r) = \bar{a}r \in \langle a \rangle.$$

Therefore $\langle a \rangle$ is a subring of R .



2.2.2 Quotient Rings

Theorem 2.4

Let R be a ring and let A be a subring of R . The set of cosets

$$R/A = \{r + A \mid r \in A\}$$

is a ring under the operations

- $(s + A) + (t + A) = s + t + A$
- $(s + A)(t + A) = st + A$

if and only if A is an ideal of R .

Proof. Let R to be a ring, and let $A \trianglelefteq R$. For all $s + A, t + A$ in R/A we define addition as

$$\boxplus(s + A, t + A) := (s + A) \boxplus (t + A) = s + t + A$$

and multiplication as

$$\odot(s + A, t + A) := (s + A) \odot (t + A) = st + A.$$

We want to show $(R/A, \boxplus, \odot)$ is a ring.

1. (Closureness) Suppose that $s + A = s' + A$ and $t + A = t' + A$ for all $s, s', t, t' \in \mathbb{R}$. First we need to show

$$(s + t) + A = (s' + t') + A.$$

We are going to express s, t in term of s', t' respectively.

$$\begin{aligned} s + A = s' + A &\Rightarrow s - s' \in A \\ &\Rightarrow s - s' = a_1 \in A \\ &\Rightarrow \boxed{s = a_1 + s'}, \quad a_1 \in A. \end{aligned} \tag{\heartsuit}$$

and

$$\begin{aligned} t + A = t' + A &\Rightarrow t - t' \in A \\ &\Rightarrow t - t' = a_2 \in A \\ &\Rightarrow \boxed{t = a_2 + t'}, \quad a_2 \in A. \end{aligned} \tag{\clubsuit}$$

Summing up (\heartsuit) together with (\clubsuit) we have

$$s + t = (a_1 + s') + (a_2 + t') = a_1 + a_2 + s' + t', \quad a_1 + a_2 \in A.$$

Subtracting $s' + t'$ on both side of the equation yields

$$s + t - (s' + t') = a_1 + a_2 \implies s + t - (s' + t') \in A.$$

We have shown R/A closed under addition \boxplus , we continue to proof

$$st + A = s't' + A.$$

Which is equivalent to show R/A closed under the multiplication \odot . Applying the results that we found from $(\heartsuit), (\clubsuit)$ we have

$$st - s't' = a_1 a_2 + a_1 t' + s' a_2$$

Is $a_1 t'$ in A ? Of course, since $a_1 \in A, t' \in R \implies a_1 t' \in A \triangleleft R$. So as $s' a_2 \in A \triangleleft R$.

2. (Existence of additive identity) For all $s + A \in R/A$, there exists $e + A \in R/A$ such that

$$\begin{aligned} (s + A) \boxplus (e + A) = s + A &\Rightarrow (s + e) + A = 0 + s + A \\ &\Rightarrow s + e = s \\ &\Rightarrow e = 0_A. \end{aligned}$$

Thus the additive identity is $0_A + A$.

3. (Existence of additive inverse) For all $s + A \in R/A$, there exists $r + A \in R/A$ such that

$$\begin{aligned}(s + A) \boxplus (r + A) &= 0 + A \Rightarrow (s + r) + A = 0 + A \\ &\Rightarrow s + r = 0 \\ &\Rightarrow r = -s.\end{aligned}$$

Thus the additive inverse of $s + A$ is $-s + A$ in R/A .

4. (Associativity of multiplication) For all $s + A, t + A, u + A$ in R/A , compute

$$\begin{aligned}(s + A) \odot [(t + A) \odot (u + A)] &= (s + A) \odot (tu + A) \\ &= s(tu) + A \\ &= (st)u + A \\ &= [(st) + A] \odot (u + A) \\ &= [(s + A) \odot (t + A)] \odot (u + A).\end{aligned}$$

Associativity in \odot holds.

5. (Existence of unity) For all $s + A \in R/A$, there exists $e' + A \in R/A$ such that

$$\begin{aligned}(s + A) \odot (e' + A) &= s + A \Rightarrow se' + A = s + A \\ &\Rightarrow se' = s \\ &\Rightarrow e' = 1_A \in R.\end{aligned}$$

The multiplicative identity is $1_A + A$ in R/A .

6. (Existence of multiplicative inverse) For all $s + A \in R/A$, there exists $r + A \in R/A$ such that

$$\begin{aligned}(s + A) \odot (r + A) &= 1_A + A \Rightarrow sr + A = 1_A + A \\ &\Rightarrow sr = 1_A \\ &\Rightarrow r = s^{-1}.\end{aligned}$$

The multiplicative inverse of $s + A$ is $s^{-1} + A$ in R/A , provided s^{-1} exists in R .

7. (Distributive Law) For all $s + A, t + A, u + A$ in R/A , compute

$$\begin{aligned}(s + A) \odot [(t + A) \boxplus (u + A)] &= (s + A) \odot [(t + u) + A] \\ &= s(t + u) + A \\ &= st + su + A \\ &= (st + A) + (su + A) \\ &= (st + A) \boxplus (su + A) \\ &= (s + A) \odot (t + A) \boxplus (s + A) \odot (u + A)\end{aligned}$$

Distributive law holds in $(R/A, \boxplus, \odot)$.

Therefore $(R/A, \boxplus, \odot)$ is a ring. □

 **Example 2.2.4.** $\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$

 **Solution** The integers with multiple of 4 is

$$4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, 12, \dots\}.$$

The left ideals are

$$\begin{aligned}1 +_4 4\mathbb{Z} &= \{\dots, -7, -3, 1, 5, 9, 13, \dots\} \\2 +_4 4\mathbb{Z} &= \{\dots, -6, -2, 2, 6, 10, 14, \dots\} \\3 +_4 4\mathbb{Z} &= \{\dots, -5, -1, 3, 7, 11, 15, \dots\} \\4 +_4 4\mathbb{Z} &= \{\dots, -4, 0, 4, 8, 12, 16, \dots\} = 4\mathbb{Z}\end{aligned}$$



Definition 2.2 characteristic of ring

The characteristic of a ring R is the least positive integer n such that $nx = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\text{char}(R)$.

Example 2.2.5. The characteristic of ring \mathbb{Z}_7 is 7.

Example 2.2.6. Find the characteristic of $R = \mathbb{Z}[i]/\langle 2 - i \rangle$.

Solution Given that

$$R = \mathbb{Z}[i]/\langle 2 - i \rangle = \{a + bi + \langle 2 - i \rangle\}.$$

Observe that

$$2 - i + \langle 2 - i \rangle = 0 + \langle 2 - i \rangle$$

and so we treat $2 - i$ as zero, and $i = 2$ and so

$$-1 = i^2 = 4 \implies 5 = 0 \in R.$$

Thus $R = \{0 + \langle 2 - i \rangle, 1 + \langle 2 - i \rangle, 2 + \langle 2 - i \rangle, 3 + \langle 2 - i \rangle, 4 + \langle 2 - i \rangle\}$. So $\text{Char}(R) = 5$.



Definition 2.3 Prime ideal

An ideal I in a commutative ring R is said to be prime if $I \neq R$ and whenever $ab \in I$, then either $a \in I$ or $b \in I$.

Lemma 2.3

Let R be a commutative ring with unity, and I be an ideal in R . Then I is a prime ideal in R if and only if R/I is an integral domain.

Proof. R/I will therefore be an integral domain if and only if it has no zero divisors. This condition is equivalent to the condition that

$$(a + I)(b + I) = I \iff a + I = I \text{ or } b + I = I.$$

Thus R/I is an integral domain if and only if $ab + I = I$ implies that $a + I = I$ or $b + I = I$ or, in other words, if and only if $ab \in I$ implies that $a \in I$ or $b \in I$, which is to say that I is a prime ideal in R . \square

Definition 2.4 Maximal ideal

An ideal I in a ring R is said to be maximal if $I \neq R$ and whenever J is an ideal such that

$$I \subset J \subset R$$

then $I = J$ or $J = R$.

Lemma 2.4

Consider R is a ring with nonzero unity, and M is an ideal such that $M \neq R$. If R/M is a division ring, then M is a maximal ideal.

Proof. Suppose I is an ideal such that $M \subsetneq I \subseteq R$. Then $\exists a \in I$ s.t. $a \notin M$. Then $a + M \neq 0 + M$ and there exists $b + M \in R/M$ such that

$$(a + M)(b + M) = 1_R + M \implies (1_R - ab) \in M \implies ab + m = 1_R$$

for some $m \in M$. Since $ab \in I$ and $m \in M \subset I$. Also $1_R \in I \implies I = R$. Thus M is a maximal ideal. \square

Theorem 2.5

Let M be an ideal in a commutative ring R with identity. Then M is a maximal ideal if and only if the quotient ring R/M is a field.

Proof. (\Leftarrow) If R/M is a field, then M is a maximal ideal by previous lemma.

(\Rightarrow) Since $M \neq R$, R/I is a commutative ring with $1_R + R \neq 0_R + M$. Take any nonzero $a + M \in R/M$, $a \notin M$ and put

$$N := Ra + M = \{ra + m \mid r \in R, m \in M\}.$$

Note that Ra is an ideal and M is also an ideal ($Ra = \langle a \rangle$). Thus $Ra + M$ is ideal that include M .

Since M is maximal, this implies that $N = R \implies 1_R \in N$. $ra + m = 1_R$ for some $r \in R, m \in M$. Compute

$$\begin{aligned} ra + m = 1_R &\Rightarrow ra + M = 1_R + M && \text{Since } (ra - 1_R) \in M \\ &\Rightarrow (a + M)(r + M) = 1_R + M. \end{aligned}$$

We can now see that $a + M$ is actually a unit in R/M . Hence R/M is a field. \square

Corollary 2.1

In a commutative ring R with unity, every maximal ideal is a prime ideal.

Proof. If I is a maximal ideal in R , then R/I is a field. Every field is an integral domain, so R/I is also an integral domain, and I is a prime ideal. \square

Example 2.2.7. The ideal $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$.

⇒ Solution Suppose that A is an ideal of $\mathbb{R}[x]$ that properly contains $\langle x^2 + 1 \rangle$. We will prove that $A = \mathbb{R}[x]$ by showing that A contains some nonzero real number c . Then

$$1 = \frac{1}{c}c \in A$$

and therefore $A = \mathbb{R}[x]$.

Let a polynomial $f(x) \in A$, but $f(x) \notin \langle x^2 + 1 \rangle$. Then

$$f(x) = q(x)(x^2 + 1) + r(x),$$

where $r(x) = ax + b$, where a, b both are nonzero, and hence

$$a^2x^2 - b^2 = (ax + b)(ax - b) \in A \text{ and } a^2(x^2 + 1) \in A.$$

So that

$$0 \neq a^2 + b^2 = (a^2x^2 + a^2) - (a^2x^2 - b^2) \in A.$$



Example 2.2.8. The ideal $\langle x^2 + 1 \rangle$ is not prime in $\mathbb{Z}_2[x]$.

⇒ Solution (Counterexample) Take

$$(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1 \in \langle x^2 + 1 \rangle$$

but $1 + x \notin \langle x^2 + 1 \rangle$.



2.3 Ring homomorphism

Definition 2.5 Ring homomorphism

A ring homomorphism f from a ring (R, \oplus, \odot) to a ring (S, \boxplus, \boxdot) is a mapping from R to S that preserves the ring additions (\oplus, \boxplus) and multiplications (\odot, \boxdot) ; that is,

$$f(a \oplus b) = f(a) \boxplus f(b)$$

and

$$f(a \odot b) = f(a) \boxdot f(b)$$

A ring homomorphism that is one-to-one and onto is called the **ring isomorphism**.

Example 2.3.1. The map $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_3$ defined by

$$\phi(x) = x \pmod{3} \quad \forall x \in \mathbb{Z}$$

is a ring homomorphism.

⇒ Solution Clearly, for all $x, y \in \mathbb{Z}$

$$\begin{aligned} \phi(x + y) &= (x + y) \pmod{3} = (x \pmod{3}) + (y \pmod{3}) \\ &= \phi(x) +_3 \phi(y) \end{aligned}$$

and

$$\begin{aligned}\phi(xy) &= (xy) \pmod{3} = (x \pmod{3}) \cdot (y \pmod{3}) \\ &= \phi(x) \cdot_3 \phi(y)\end{aligned}$$

This is an example of a map that respects both operations. ◀

 **Example 2.3.2.** Consider the map $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_6$, $\phi(x) = 3x$ for all x in \mathbb{Z}_4 . ϕ is a ring homomorphism.

 **Solution** For all $x, y \in \mathbb{Z}$, we check that

$$\begin{aligned}\phi(x+y) &= 3(x+y) \pmod{6} = (3x \pmod{6}) + (3y \pmod{6}) \\ &= \phi(x) +_6 \phi(y)\end{aligned}$$

and

$$\begin{aligned}\phi(xy) &= 3(xy) \pmod{6} = 9(xy) \pmod{6} = (3x \pmod{6}) \cdot (3y \pmod{6}) \\ &= \phi(x) \cdot_6 \phi(y)\end{aligned}$$

this map preserves both operations. So ϕ is a ring homomorphism.

In our calculation, we can have used the fact that $3 = 9 \pmod{6}$. The jump from 3 to 9 modulo 6 can be better seem in

$$3 \pmod{6} = \phi(1) = \phi(1 \cdot 1) = \phi(1) \phi(1) = 3 \cdot 3 = 9 \pmod{6}. \quad \blacktriangleleft$$

 **Example 2.3.3.** For $a, b \in \mathbb{R}$, let $A(a, b) = M_2(\mathbb{R})$ be defined by

$$A(a, b) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

Let $R = \{A(a, b) \mid a, b \in \mathbb{R}\} \subseteq M_2(\mathbb{R})$. Then $R \cong \mathbb{C}$.

 **Solution** Let $\phi : R \rightarrow \mathbb{C}$ be defined by

$$\phi(A(a, b)) = a + bi \in \mathbb{C}.$$

We show firstly that ϕ is a ring homomorphism.

For addition, we have

$$\begin{aligned}\phi(A(a, b) + A(c, d)) &= \phi(A(a+c, b+d)) \\ &= (a+c) + (b+d)i \\ &= (a+bi) + (c+di) \\ &= \phi(A(a, b)) + \phi(A(c, d)).\end{aligned}$$

For multiplication, we have

$$\begin{aligned}
\phi(A(a, b) + A(c, d)) &= \phi \left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \right) \\
&= \phi \left(\begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix} \right) \\
&= \phi(A(ac - bd, ad + bc)) \\
&= (a + bi)(c + di) \\
&= \phi(A(a, b)) \phi(A(c, d)).
\end{aligned}$$

Now, ϕ is one-to-one and onto since $\phi(A(a, b)) = a + bi = 0$ if and only if $a = b = 0$, and $\text{Ker } \phi = \{A(0, 0)\}$ is trivial. \blacktriangleleft

Example 2.3.4. Show that the equation $2x^3 - 5x^2 + 7x - 8 = 0$ has no solutions in \mathbb{Z} .

Solution Let $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_3$ be the natural homomorphism $\phi(x) = x \bmod 3$. Suppose that there is an integer $a \in \mathbb{Z}$ such that

$$2a^3 - 5a^2 + 7a - 8 = 0.$$

Then

$$0 = \phi(0) = \phi(2a^3 - 5a^2 + 7a - 8) = 2\phi(a)^3 - 5\phi(a)^2 + 7\phi(a) - 8.$$

Since $-5 = 7 = -8 = 1 \pmod{3}$ in \mathbb{Z}_3 , we have

$$2\phi(a)^3 - 5\phi(a)^2 + 7\phi(a) - 8 = 2\phi(a)^3 + \phi(a)^2 + \phi(a) + 1$$

and thus $2b^3 + b^2 + b + 1 = 0$, where $b = \phi(a)$ in \mathbb{Z}_3 .

However, one can easily check that no element $b \in \{0, 1, 2\}$ in \mathbb{Z}_3 is a solution to this equation. Therefore there is no such integer $a \in \mathbb{Z}$ to the original equation. \blacktriangleleft

Example 2.3.5 (Tutorial). Show that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Solution Assume the contrary and let $\phi : 2\mathbb{Z} \rightarrow 3\mathbb{Z}$ to be an isomorphism. Let us examine $\phi(2)$. Note that for some $k \in \mathbb{Z}$, $\phi(2) = 3k$. Since ϕ is a homomorphism,

$$\phi(k) = \phi(2+2) = \phi(2) + \phi(2) = 3k + 3k = 6k.$$

But ϕ is a ring homomorphism and

$$\phi(k) = \phi(2 \cdot 2) = \phi(2)\phi(2) = (3k)(3k) = 9k^2.$$

This implies that $6k = 9k^2 \implies k = 0$ or $k = \frac{2}{3}$.

For $k = 0 \implies \phi(x) = 0$ is not one-to-one and not onto. Also, $k = \frac{2}{3} \notin \mathbb{Z}$, and thus ϕ cannot be an isomorphism. \blacktriangleleft

Example 2.3.6. Determine all ring homomorphism from \mathbb{Z} to \mathbb{Z}_6 .

Solution Since \mathbb{Z} is generated from 1 by addition and subtraction, if a ring homomorphism $f : \mathbb{Z} \rightarrow \mathbb{Z}_6$, then for any $a \in \mathbb{Z}$, we have

$$f(a) = am$$

where $m = f(1)$. Then f is linear, so

$$f(a) + f(b) = am + bm = (a + b)m = f(a + b) \quad \forall a, b \in \mathbb{Z}.$$

So f is a ring homomorphism if and only if

$$0 = f(ab) - f(a)f(b) = abm - (am)(bm) = ab(m - m^2)$$

for any $a, b \in \mathbb{Z}$.

In particular, taking $a = b = 1$, we need to find m such that $0 = m - m^2 \pmod{6}$. Working modulo 6 one by one

$$\begin{array}{ll} 0 - 0^2 = 0 - 0 = 0, & 1 - 1^2 = 1 - 1 = 0, \\ 3 - 3^2 = 3 - 9 = -6 = 0, & 4 - 4^2 = 4 - 16 = 0, \\ 5 - 5^2 = 5 - 25 = 2 \neq 0 & \end{array}$$

The possible values of m are 0, 1, 3 and 4. So the homomorphisms are as follow

- $f(a) = 0 \pmod{6}, \quad \forall a \in \mathbb{Z}$.
- $f(a) = a \pmod{6}, \quad \forall a \in \mathbb{Z}$.
- $f(a) = 3a \pmod{6}, \quad \forall a \in \mathbb{Z}$.
- $f(a) = 4a \pmod{6}, \quad \forall a \in \mathbb{Z}$.



Theorem 2.6 The first isomorphism for rings

Let f be a ring homomorphism from ring R to S . Then the mapping from $R/\ker(f)$ to $f(R)$, given by

$$r + \ker(f) \rightarrow f(r)$$

is an isomorphism. In symbols, $R/\ker(f) \cong f(R)$.

Proof. Define a map $\bar{f} : R/K \rightarrow \text{Im } \bar{f}$ by

$$\bar{f}(a + K) = \bar{f}(a) \quad \forall a \in R, a + K \in R/K.$$

1. Since \bar{f} is well defined, so

$$\begin{aligned} a + K = b + K &\Rightarrow a - b \in K \\ &\Rightarrow \bar{f}(a - b) = 0_S \\ &\Rightarrow \bar{f}(a) - \bar{f}(b) = 0_S \\ &\Rightarrow \bar{f}(a) = \bar{f}(b) \end{aligned}$$

2. \bar{f} is injective since

$$\begin{aligned} \bar{f}(a + K) = \bar{f}(b + K) &\Rightarrow \bar{f}(a) = \bar{f}(b) \\ &\Rightarrow \bar{f}(a - b) = 0_S \\ &\Rightarrow a - b \in K \\ &\Rightarrow a + K = b + K. \end{aligned}$$

3. f is surjective. For all $f(a) \in \text{Im } \bar{f}$, $\exists a + K \in R/K$ such that $\bar{f}(a + K) = f(a)$.

4. f is homomorphism,

$$\begin{aligned} f(a + K + b + K) &\Rightarrow f((a + b) + K) \\ &\Rightarrow \bar{f}(a + b) \\ &\Rightarrow \bar{f}(a) + \bar{f}(b) \\ &\Rightarrow f(a + K) + f(b + K). \end{aligned}$$

$$\begin{aligned} f(a + K) \cdot f(b + K) &\Rightarrow f(ab + K) \\ &\Rightarrow \bar{f}(ab) \\ &\Rightarrow \bar{f}(a) \cdot \bar{f}(b) \\ &\Rightarrow f(a + K) \cdot f(b + K). \end{aligned}$$

Thus $f : R/K \cong \text{Im } f$ as rings. \square

 **Example 2.3.7.** Let $\phi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_3$ be the ring homomorphism defined by

$$\phi((a, b)) = b \bmod 3.$$

Then $\ker(\phi) = \mathbb{Z} \times 3\mathbb{Z}$ and $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times 3\mathbb{Z})$ is isomorphic to \mathbb{Z}_3 , which is a field. Thus $\mathbb{Z} \times 3\mathbb{Z}$ is a maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.

Definition 2.6

If I and J are ideals of a ring R , then we can define the following ideals of them:

1. The **sum** $I + J$ is

$$I + J = \{i + j \mid i \in I, j \in J\}. \quad (2.1)$$

If $I + J = R$ then we say that I and J are **coprime**.

2. The **intersect** of two ideals is

$$I \cap J = \{r \mid r \in I \text{ and } r \in J\}. \quad (2.2)$$

3. The **product** of two ideals equals

$$IJ = \left\{ \sum_{k=1}^n i_k j_k \mid i_k \in I, j_k \in J \right\}. \quad (2.3)$$

2.4 Polynomial rings

Definition 2.7

Let R be a commutative ring. We define

$$R[x] = \{r_n x^n + r_{n-1} x^{n-1} + \cdots + r_1 x + r_0 \mid r_i \in R\}. \quad (2.4)$$

The letter x here can be thought of a variable or just a placeholder. Either way the familiar

structure allows us to add, subtract and multiply these as we do traditional polynomials even if the ring were some strange abstract entity.

2.5 Factorization of polynomials

Theorem 2.7 Division algorithm

Let R be a ring with identity and $f(x), g(x) \in R[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ in $R[x]$ such that

$$f(x) = q(x)g(x) + r(x) \quad (2.5)$$

and $\deg(r) < \deg(g)$. $r(x) = 0$ if there is no remainder.

Proof. The basic idea is to formalize the process of long division in an inductive sense. We omit the details here. They're boring here. \square

Example 2.5.1. In \mathbb{Z}_3 we can divide $2x^2 + 1$ into $x^4 + 2x^3 + 2x + 1$. Then we have

$$x^4 + 2x^3 + 2x + 1 = (2x^2 + 1)(2x^2 + x + 2)$$

Theorem 2.8 Factor theorem

Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then a is a **root** (or **zero**) of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Proof. (\Rightarrow) Assume that $a \in F$ is a zero of $f(x) \in F[x]$. We wish to show that $x - a$ is a factor of $f(x)$. To do so, apply the division algorithm. By division algorithm, \exists unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = (x - a)q(x) + r(x)$$

and the $\deg(r) < \deg(x - a) = 1$, so $r(x) = c \in F$, where c is a constant. Also, the fact that a is a zero of $f(x)$ implies $f(a) = 0_F$. So

$$f(x) = (x - a)q(x) + c \implies 0_F = f(a) = (a - a)q(a) + c.$$

Thus $c = 0$, and $x - a$ is a factor of $f(x)$.

(\Leftarrow) On the other way, we want to show that if $x - a$ is a factor of $f(x)$, then a is a zero of $f(x)$. If $x - a$ is a factor of $f(x)$, then $\exists q(x) \in F[x]$ such that

$$f(x) = (x - a)q(x).$$

Evaluating at $x = a$, we have

$$f(a) = (a - a)q(a) = 0_F q(a) = 0_F.$$

Thus a is a zero of $f(x)$. \square

Definition 2.8 Algebraically closed

Given F a field, we call F **algebraically closed** if every $f \in F[x]$ such that $\deg(f) > 0$ has a root in F .

☞ **Example 2.5.2.** Show that $x^2 + 3x - 4 \in \mathbb{Z}_{12}[x]$ has 4 roots.

☞ **Solution** We list down all the values of $f(x) = x^2 + 3x - 4$ for $x = 0, 1, \dots, 11$.

x	0	1	2	3	4	5	6	7	8	9	10	11
$x^2 + 3x - 4 \pmod{12}$	8	0	6	2	0	0	2	6	0	8	6	6

which now we can see: $x^2 + 3x - 4$ has 4 zeros in $\mathbb{Z}_{12}[x]$. Thus, a polynomial of degree n can have more than n roots in a ring. The problem is that \mathbb{Z}_{12} is not a domain: $(x+4)(x-1) = 0$ does not imply one of the factors must be zero. ◀

☞ **Example 2.5.3.** Show that the polynomial $2x^3 + 3x^2 - 7x - 5$ can be factored into linear factors in $\mathbb{Z}_{11}[x]$.

☞ **Solution** We can use synthetic division,

$$\begin{array}{r|rrrr}
2 & 3 & -8 & -7 & 4 & 6 \\
& -2 & & -10 & -6 & \\
\hline
2 & -10 & 1 & -6 & & \\
& -4 & & 6 & & \\
\hline
2 & -3 & & & &
\end{array} \quad -1 \quad -2$$

Thus, $2x^3 + 3x^2 - 7x - 5 = (x+1)(x+2)(2x-3)$ in $\mathbb{Z}_{11}[x]$. ◀

2.5.1 Irreducibility tests

There are various methods to check if a polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$.

Theorem 2.9 Rational root test

Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (\star)$$

be a polynomial with integers coefficients. If $r \neq 0$ and the rational number r/s (in lowest terms) is a root of $f(x)$, then $r|a_0$ and $s|a_n$.

Proof. Plug $x = r/s$ into (\star) and equating with zero. The equation is now

$$a_n \left(\frac{r}{s}\right)^n + a_{n-1} \left(\frac{r}{s}\right)^{n-1} + \dots + a_1 \left(\frac{r}{s}\right) + a_0 = 0.$$

Again multiplying s^n on both sides

$$a_n r^n + a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} x + a_0 s^n = 0.$$

Factoring r out and moving $a_0 s^n$ to the right-hand side. We obtained

$$r(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1} x) = -a_0 s^n.$$

Since $\gcd(r, s) = 1$, thus $r|a_0$ and similarly $s|a_n$. □

Example 2.5.4. The polynomial $f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12$ is reducible in $\mathbb{Q}[x]$.

Solution If r/s is a root of $f(x)$, where $r|12$ and $s|2$. Thus the possible roots are

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}.$$

In fact, $f(x) = (x + 3)(x - \frac{1}{2})(2x^2 - 4x - 8) \in \mathbb{Q}[x]$. ◀

Example 2.5.5. The polynomial $g(x) = x^3 + 4x^2 + x - 1$ is irreducible in $\mathbb{Q}[x]$.

Solution The possible roots are $\{-1, 1\}$. However

$$g(1) = 1 + 4 + 1 - 1 = 5 \quad \text{and} \quad g(-1) = -1 + 4 - 1 - 1 = 1$$

So $g(x)$ has no root and $\deg g(x) = 3$. Thus $g(x)$ is irreducible over $\mathbb{Q}[x]$. ◀

Theorem 2.10 Mod p Irreducibility test

Let p be a prime and let $f(x) \in \mathbb{Z}[x]$ with degree 1 or greater. Let $\bar{f} \in \mathbb{Z}_p[x]$ obtained by reducing all of $f(x)$'s coefficients mod p . Then if

$$\deg(\bar{f}) = \deg(f) \tag{2.6}$$

and \bar{f} is irreducible over \mathbb{Z}_p then $f(x)$ is irreducible over \mathbb{Q} .

Proof. Assume that $f(x) = p(x)q(x)$ in $\mathbb{Z}[x]$. Since $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ defined by $\phi f(x) = \bar{f}(x)$ is a ring homomorphism. So

$$\bar{f}(x) = \overline{p(x)q(x)} = \bar{p}(x)\bar{q}(x).$$

If $p \nmid a_k$, then p does not divide the leading coefficients of $p(x)$ and $q(x)$. Thus $\deg \bar{p}(x) = \deg p(x)$ and $\deg \bar{q}(x) = \deg q(x)$. □

Example 2.5.6. The polynomial $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ is irreducible in \mathbb{Q} .

Solution We define

$$\bar{f}(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x].$$

By rational root test, the only possible root is 0.1 from \mathbb{R} but it is not an integer. There are several quadratic polynomials in $\mathbb{Z}_2[x]$ such as

$$x^2 + x + 1, \quad x^2 + 1, \quad x^2 + x, \quad x^2.$$

Since $x^2 + 1, x^2 + x, x^2$ both have roots, they cannot be factor of \bar{f} . The only possible factor of \bar{f} is $x^2 + x + 1$. Thus

$$x^5 + x^2 + 1 = (x^2 + x + 1)(x^3 + ax^2 + bx + c).$$

Equating coefficients of both sides, we have

$$\begin{cases} 1 + a = 0 \\ 1 + a + b = 0 \\ a + b + c = 0 \\ b + c = 0 \\ c = 1 \end{cases} .$$

On solving yields $a = -1 = 1(\text{mod } 2)$, $b = 0$ and $c = 1$ but $b + c \neq 0$ and is contradiction. So $f(x)$ does not has a quadratic factor. It means that $f(x)$ is irreducible in both $\mathbb{Z}_2[x]$ and \mathbb{Z} . So $f(x)$ is also irreducible in $\mathbb{Q}[x]$. \blacktriangleleft

Theorem 2.11 Eisenstein's criterion

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x] \setminus \{0\}$. If there is a prime number p such that $p \nmid a_n$, but $p|a_{n-1}, \dots, p|a_2$ and $p^2|a_0$. Then $f(x)$ is irreducible over \mathbb{Q} .

Proof. Suppose that $f(x)$ is reducible over \mathbb{Q} then

$$f(x) = g(x)h(x)$$

and $g(x), h(x)$ are nonconstant polynomials.

Let

$$\begin{aligned} f(x) &= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \\ g(x) &= b_rx^r + b_{r-1}x^{r-1} + \cdots + b_1x + b_0, \\ h(x) &= c_sx^s + c_{s-1}x^{s-1} + \cdots + c_1x + c_0. \end{aligned}$$

Since $p|a_0 = b_0c_0 \implies p|b_0$ or $p|c_0$, and $p^2 \nmid a_0$. This implies that p divides only one of them. Assume that $p|b_0$ and $p \nmid c_0$, then

$$p|a_0 = b_0c_1 + b_1c_0.$$

Since $p|b_0c_1$ and $p \nmid c_0 \implies p|b_1$. Assume that $p|b_i \forall 0 \leq i < m$ for some $m \leq r$. Then

$$p|a_m = \sum_{\substack{i+j=m \\ j \leq s}} b_i c_j \implies p|b_m c_0 \implies p|b_m.$$

By mathematical induction, $p|b_r$. Thus $p|a_n = b_r c_s$. This contradicting the fact that $f(x)$ is reducible. \square

Example 2.5.7. $x^9 + 5$ is irreducible in $\mathbb{Q}[x]$ with $p = 5$.

Example 2.5.8. $x^{17} + 6x^{13} - 15x^4 + 3x^2 - 9x + 12$ is irreducible in $\mathbb{Q}[x]$ with $p = 3$.

Example 2.5.9. $x^n + 5$ is irreducible in $\mathbb{Q}[x]$ for all $n \geq 1$. There are irreducible polynomials of every degree in $\mathbb{Q}[x]$.

Corollary 2.2

For any prime p , the p -th cyclotomic polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over \mathbb{Q} .

Proof. Let $\zeta = e^{2\pi i/n}$. Then $\zeta, \zeta^2, \dots, \zeta^n$ are the n -th roots of unity. They form the vertices of a regular n -gon in the complex plane. If $\gcd(a, n) > 1$ then ζ^a is a root of unity of order $n/\gcd(a, n) < n$, but if $\gcd(a, n) = 1$ then ζ^a is not a root of lower order, and in this case we call ζ^a a primitive n -th root of unity. We define the n -th cyclotomic polynomial $\Phi_n(x)$ to be the monic polynomial of degree $\phi(n)$ whose roots are the primitive n -th root of unity:

$$\Phi_n(x) = \prod_{\substack{a=1 \\ \gcd(a,n)=1}}^n (x - \zeta^a). \quad (2.7)$$

The first few cyclotomic polynomials are as follows:

$n =$	
1	$\Phi_1(x) = x - 1$
2	$\Phi_2(x) = x + 1$
3	$\Phi_3(x) = x^2 + x + 1$
4	$\Phi_4(x) = x^2 + 1$
5	$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
6	$\Phi_6(x) = x^2 - x + 1$
7	$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$\Phi_8(x) = x^4 + 1$
9	$\Phi_9(x) = x^6 + x^3 + 1$
10	$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$
11	$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
12	$\Phi_{12}(x) = x^4 - x^2 + 1$
13	$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
14	$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
15	$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
16	$\Phi_{16}(x) = x^8 + 1$

Let p denote a given prime number. For any polynomial $f(x)$ with integral coefficients let $\bar{f}(x)$ be the polynomial whose coefficients are the residue classes $(\bmod p)$ determined by the coefficients of $f(x)$. Thus the assertion $\bar{f} = \bar{g}$ means that there is a polynomial $h(x)$ with integral coefficients such that $f(x) = ph(x)$.

Lemma 2.5

(Schönemann, 1846) Let $A(x)$ be a monic polynomial with integral coefficients, for instance

$$A(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \prod_{i=1}^n (x - \alpha_i).$$

Let p be a prime, and put

$$C(x) = \prod_{i=1}^n (x - \alpha_i^p).$$

Then $\bar{C} = \bar{A}$.

Proof. Let $\sigma_k(\alpha)$ denote the k -th symmetric function of α_i . When $\sigma_k(\alpha)^p$ is expanded by the multinomial theorem, all coefficients except the extreme ones are divisible by p . That is,

$$\frac{\sigma_k(\alpha_1, \alpha_2, \dots, \alpha_n)^p - \sigma_k(\alpha_1^p, \alpha_2^p, \dots, \alpha_n^p)}{p}$$

is a symmetric polynomial in the α , with integral coefficients, and hence by the symmetric function theorem the quantity must be a rational integer. \square

Lemma 2.6

Put $f(x) = x^n - 1$. Then \bar{f} is a squarefree if and only if $p \nmid n$.

Proof. By previous lemma we can see that if $p \nmid n$. Then $\gcd(\bar{f}, \bar{f}') = 1$, and hence that \bar{f} is squarefree. On the other hand, if $p|n$, say $n = mp$ for some integer m , then

$$\bar{f} = \overline{(x^m - 1)^p}$$

and hence \bar{f} is not squarefree.

Let $\Phi_n(x)$ denote the n -th cyclotomic polynomial. Since $\Phi_n|f$, it follows from the above that if $p \nmid n$, then $\bar{\Phi}_n$ is also squarefree. \square

Theorem 2.12

(Kronecker, 1854) The polynomial $\Phi_n(x)$ is irreducible over \mathbb{Q} .

Proof. Suppose that A and B are monic polynomials with rational coefficients such that $\Phi_n = AB$, and suppose also that $\deg A > 0$. We know that A and B have integral coefficients. Let Z denote the roots of A . Let C be the monic polynomial whose roots are the numbers ζ^p for $\zeta \in Z$. Here p is an arbitrary prime not dividing n . Our first step is to show that $A = C$.

Since the map $\zeta \mapsto \zeta^p$ merely permutes the roots of Φ_n , we know that $C|\Phi_n$. Let $G = \gcd(B, C)$. Then $\bar{G}|B$ and $\bar{G}|C$. But $\bar{A} = \bar{C}$ by previous lemma, and hence $\bar{G}^2|\bar{A}\bar{B}$. But Φ_n is squarefree, by previous lemma. Hence $G = 1$, so $G = 1$, and consequently $C|A$. But C and A have the same degree, so in fact $A = C$.

Now let ζ be a root of A , and ζ' a root of Φ_n . Then there exists a positive integer a , $\gcd(a, n) = 1$, such that $\zeta' = \zeta^a$. We factor a , $a = p_1 p_2 \dots p_k$. Since ζ is a root of A , it follows from the argument above that ζ^{p_1} is also a root of A . Then by a second application of the above argument, we see that

$\zeta^{p_1 p_2}$ is also a root of A . Continuing in this manner, we deduce that ζ' is a root of A . Since this is valid for every root ζ' of Φ_n , we conclude that $A = \Phi_n$. Hence Φ_n is irreducible. \square

\square

Theorem 2.13

Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F .

Proof. Suppose $\langle p(x) \rangle$ is a maximal ideal in $F[x]$. We know that $p(x) \neq 0$ and $p(x)$ is not a unit since neither $\{0\}$ nor $\langle 1_F \rangle = F[x]$ is a maximal ideal in $F[x]$. Let

$$p(x) = g(x)h(x)$$

be a factorization. Then $\langle p(x) \rangle \subseteq \langle g(x) \rangle \subseteq \langle F[x] \rangle$ and since $\langle p(x) \rangle$ is maximal we either have $\langle g(x) \rangle = \langle p(x) \rangle$ or $\langle g(x) \rangle = F[x]$. In the first case we get \square

Theorem 2.14 Fundamental Theorem of Algebra

Every nonconstant polynomial in $\mathbb{C}[x]$ has a root in \mathbb{C} .

Remark. *The field \mathbb{C} is algebraically closed.*

Corollary 2.3

A polynomial is irreducible in $\mathbb{C}[x]$ if and only if it has a degree 1.

Proof. All linear equation with degree 1 only have one root in \mathbb{R} . \square

Corollary 2.4

Every nonconstant polynomial $f(x)$ of degree n can be written in the form

$$c(x - a_1)(x - a_2) \dots (x - a_n)$$

for some $c, a_1, a_2, \dots, a_n \in \mathbb{C}$. This factorization is unique except for the order of the factors.

Proof. By the fundamental theorem of algebra,

$$\begin{aligned} f(x) &= (r_1 x + s_1)(r_2 x + s_2) \dots (r_n x + s_n) \\ &= r_1 r_2 \dots r_n (x + s_1 r_1^{-1})(x + s_2 r_2^{-1}) \dots (x + s_n r_n^{-1}). \end{aligned}$$

Since $f(x)$ has n unique roots, factorization is also unique. \square

Lemma 2.7

If $f(x)$ is a polynomial in $\mathbb{R}[x]$ and $a + bi$ is a root of $f(x)$ in \mathbb{C} , then $a - bi$ is also a root of $f(x)$.

Proof. Let $z = a + bi$ and the conjugate $\bar{z} = a - bi$. Define a map $\varphi : \mathbb{C}[x] \rightarrow \mathbb{C}[x]$ by $\varphi f(x) = \bar{f}$. Bijective is trivial in φ , e.g. $\varphi(f + g) = \bar{f} + \bar{g}$ and $\varphi(fg) = \bar{f}\bar{g}$ since

$$\overline{(a+bi)(c+di)} = \overline{(a+bi)} \overline{(c+di)}.$$

If $f(x)$ has a root z then $\bar{f}(x)$ will have a root \bar{z} . If coefficients of $f(x)$ are all real numbers, then $f(x) = \bar{f}(x)$. Thus $f(x)$ has a root \bar{z} . \square

Theorem 2.15

A polynomial $f(x)$ is irreducible in $\mathbb{R}[x]$ if and only if $f(x)$ is a first-degree polynomial or $f(x) = ax^2 + bx + c$ with $b^2 - 4ac < 0$.

Proof. In $\mathbb{C}[x]$,

$$f(x) = c(x - a_1)(x - a_2) \dots (x - a_n).$$

If $a_i = c + di$, $a_j = c - di$ for some $1 \leq j \leq n$. The product of the conjugates are

$$(x - a_i)(x - a_j) = (x - c - di)(x - c + di) = x^2 - 2cx + c^2 + d^2 \in \mathbb{R}[x].$$

Thus we can pair them and so $f(x)$ can be split by irreducible polynomials whose degree is either 1 or 2.

Now we knew every irreducible polynomial has a degree 1 or 2. When its degree is 2, then

$$f(x) = ax^2 + bx + c \quad \forall a, b, c \in \mathbb{R} \quad (\clubsuit)$$

We now continue to work on the "formula" to solve x . Completing the square on (\clubsuit)

$$\begin{aligned} ax^2 + bx + c = 0 &\Rightarrow a \left[x^2 + \frac{b}{a}x + \left(\frac{b}{2a} \right)^2 \right] - \left(\frac{b}{2a} \right)^2 = 0 \\ &\Rightarrow \left(x + \frac{b}{2a} \right)^2 = \frac{b^2 - 4ac}{4a^2} \\ &\Rightarrow x + \frac{b}{2a} = \pm \frac{\sqrt{b^2 - 4ac}}{2a} \\ &\Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \quad a \neq 0 \end{aligned}$$

Now we can take a look on determinant $\Delta = b^2 - 4ac$. If $\Delta < 0$, the two roots will be in $\mathbb{C} \setminus \mathbb{R}$, else the two roots are in \mathbb{R} . (Either $\Delta > 0$ or $\Delta = 0$). Hence the first-degree polynomial or quadratic polynomial is irreducible in $\mathbb{R}[x]$. \square

Corollary 2.5

Every polynomial $f(x)$ of odd degree in $\mathbb{R}[x]$ has a root in \mathbb{C} .

Proof. Consequently, we can tell if a polynomial in $\mathbb{R}[x]$ or $\mathbb{C}[x]$ is irreducible without any elaborate tests. \square

2.6 Integral Domains

Let R be a commutative ring. A **zero divisor** is a nonzero element $a \in R$ such that

$$ab = 0 \quad (2.8)$$

for some nonzero $b \in R$. The most familiar integral domain is \mathbb{Z} . It is a commutative ring with unity one. If $a, b \in \mathbb{Z}$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Theorem 2.16

If $x \neq 0$ is not a zero divisor in a ring R and $xy = xz$, then $y = z$.

Proof. Since $xy = xz$, we have $x(y - z) = 0$. Since $x \neq 0$ and is not a zero divisor, it follows that $y - z = 0 \implies y = z$. \square

Definition 2.9 Integral Domains

A ring with unity 1 having no zero divisors is an **integral domain**.

Lemma 2.8

Fields are integral domain

Proof. Let F be a field. We want to show that F has no zero divisors. Suppose $ab = 0$ and $a \neq 0$. Then a must have an inverse a^{-1} such that $a^{-1}ab = a^{-1} \cdot 0 \implies b = 0$. Therefore, F has no zero divisors, and so F is an integral domain. \square

Corollary 2.6

\mathbb{Z}_p is a field.

Proof. According to previous theorem, we need only prove that \mathbb{Z}_p has no zero divisors.

Suppose that $a, b \in \mathbb{Z}_p$ and $ab = 0$. Then $ab = pk$ for some integer k . But then we have either $p \mid a$ or $p \mid b$ and in \mathbb{Z}_p is equivalent to either $a = 0$ or $b = 0$. \square

Lemma 2.9

If R is an integral domain, then the characteristic of R is either 0 or a positive prime.

Proof. Suppose not, suppose R has characteristic $n = ab$ with $1 < a < b < n$. Then

$$\underbrace{(1_R + \cdots + 1_R)}_{a \text{ times}} \underbrace{(1_R + \cdots + 1_R)}_{b \text{ times}} = ab1_R = n1_R = 0.$$

Since R is an integral domain, it is either $a \cdot 1_R = 0$ or $b \cdot 1_R = 0$. This is contradicts with our assumption that n is not prime. \square

Example 2.6.1. The extended ring

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

is a field and that every nonzero element has a multiplicative inverse.

☞ Solution This is clearly a ring. To show that every nonzero element has a multiplicative inverse. Consider $a + b\sqrt{2} \neq 0 \in \mathbb{Q}[\sqrt{2}]$. The multiplicative inverse is

$$\frac{1}{a + b\sqrt{2}}$$

Then multiplying top and bottom by conjugate, we have

$$\frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

Now we want to show $a^2 - 2b^2 \neq 0$.

If $a = 0$ and $b \neq 0$ or if $a \neq 0$ and $b = 0$, then $a^2 - 2b^2 \neq 0$. Since $a^2 - 2b^2 \neq 0$, the only other possibility is $a, b \neq 0$.

Thus, $a^2 = 2b^2$ with $a, b \neq 0$. We may assume that a and b are integers – in fact, now we can see 2 divides $2b^2$, so $2 | a^2 \implies 2 | a$. So $a = 2c$ for some integer c . Plugging in gives $4c^2 = 2b^2 \implies 2c^2 = b^2$.

It follows that every nonzero element of $\mathbb{Q}[\sqrt{2}]$ is invertible, so $\mathbb{Q}[\sqrt{2}]$ is a field. ◀

☞ Example 2.6.2 (Non-example). $M_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ is not an integral domain.

☞ Solution Choose

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

from $M_2(\mathbb{Z})$, and compute the matrix product

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathbf{0}.$$

A, B are zero divisors but none of them are zero. Thus $M_2(\mathbb{Z})$ is not an integral domain. ◀

Theorem 2.17

A finite integral domain is a field

Proof. Let D be a finite integral domain. Since D is an integral domain, then D is a commutative ring with unity, and hence we need to show that D is a field. In order to do this, we want to show $\forall a \neq 0 \in D, \exists a^{-1} \in D$ such that

$$a \cdot a^{-1} = 1_D = a^{-1} \cdot a.$$

Without loss of generality, we let

$$D = \{a, a^2, a^3, \dots, a^t\}$$

where $a \neq 0$ for some $t \in \mathbb{N}$. Consider two elements a^i, a^j from D , we have

$$\begin{aligned} a^i = a^j &\Rightarrow a^{i-j} = 1_D \\ &\Rightarrow a \cdot a^{i-j-1} = 1_D \\ &\Rightarrow a^{-1} = a^{i-j-1} \\ &\Rightarrow a \cdot a^{-1} = a^{i-j} = 1_D. \end{aligned}$$

and the multiplication is commutative, therefore D is a field. \square

Remark.

*if \mathbb{Z}_p is a field $\implies \mathbb{Z}_p$ has no zero divisors.
 $\implies \mathbb{Z}_p$ is an integral domain.
 $\implies |\mathbb{Z}_p| = p$ is prime and is finite.*

Theorem 2.18

Let R be a commutative ring with unity and let A be an ideal of R . Then R/A is an integral domain if and only if A is prime.

Proof. We are going to prove in two directions:

(\Rightarrow) Suppose R/A is an integral domain and $ab \in A$. Then

$$(a + A)(b + A) = ab + A = A$$

is the zero element of the ring R/A . So it is either $a + A = A$ or $b + A = A$; that is, either $a \in A$ or $b \in A$. Thus A is prime.

(\Leftarrow) On the other hand, observe that R/A is a commutative ring with unity for any proper ideal A . Thus, we only need to show that when A is prime, R/A has no zero divisors.

Now suppose that A is prime and

$$(a + A)(b + A) = 0 + A = A.$$

Then $ab \in A$, and therefore, it is either $a \in A$ or $b \in A$. Thus, one of $a + A$ or $b + A$ is the zero coset in R/A . Now we are done. \square

2.7 Principal Ideal Domain

Definition 2.10 Principal Ideal Domain

An integral domain R is called a **principal ideal domain** (or **PID**) if every ideal in R is principal.

☞ **Example 2.7.1.** The integers \mathbb{Z} and polynomial rings over fields are principal ideal domains.

Theorem 2.19

If F is a field then $F[x]$ is a PID.

Proof. We know $F[x]$ is integral domain since F is an integral domain. Let I be an ideal of $F[x]$.

Case 1: If $I = \{0\}$ then $I = \langle 0 \rangle$ and we are done.

Case 2: If $I \neq \{0\}$ let $g(x)$ be a nonzero polynomial of minimal degree in I (which exists by well-ordering). If $g(x)$ is constant then $g(x) = \alpha \in F$ and then $I = F = \langle \alpha \rangle$ because for any $r \in F$ we have

$$r = r\alpha^{-1}\alpha \in \langle \alpha \rangle.$$

Suppose then that $g(x)$ is not constant, we claim $I = \langle g(x) \rangle$. Since $g(x) \in I$ we have $\langle g(x) \rangle \subseteq I$. We claim $I \subseteq \langle g(x) \rangle$. Let $f(x) \in I$. By the *division algorithm*, we can write

$$f(x) = q(x)g(x) + r(x)$$

with $0 \leq \deg(r(x)) < \deg(g(x))$. Since

$$r(x) = f(x) - q(x)g(x)$$

we have $r(x) \in I$ and the fact that $g(x)$ is a nonzero polynomial of minimal degree implies that $r(x) = 0$ and so $f(x) = q(x)g(x) \implies f(x) \in \langle g(x) \rangle$. \square

2.8 Unique Factorization Domain

Definition 2.11

An integral domain D is a **unique factorization domain** (**UFD** in short) if

1. Every nonzero element of D that is not a unit can be written as a product of irreducibles of D , and
2. The factorization into irreducibles is unique up to associates and the order in which the factors appear.

Example 2.8.1. 3 is prime in \mathbb{Z} but not prime in $\mathbb{Z}[\sqrt{-2}]$. Since

$$3 = (1 + \sqrt{-2})(1 - \sqrt{-2}),$$

which $(1 + \sqrt{-2})$ and $(1 - \sqrt{-2})$ are two essentially different factors in $\mathbb{Z}[\sqrt{-2}]$.

Theorem 2.20

Every PID is a UFD.

Proof. Let R be a PID and suppose that a nonzero element a of R can be express in two different ways as a product of irreducibles. Suppose

$$a = p_1 p_2 \cdots p_r \quad \text{and} \quad a = q_1 q_2 \cdots q_s$$

where each p_i and q_j is irreducible in R , and $s \geq r$. Then p_1 divides the product q_1, q_2, \dots, q_s and so $p_1 | q_j$ for some j , as p_1 is prime. After reordering the q_j we can consider $p_1 | q_1$. Then $q_1 = u_1 p_1$ for some unit u_1 of R , since q_1 and p_1 are both irreducible. Thus

$$p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s$$

and cancelling p_1 on both side

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

Continuing this process we reach

$$1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s.$$

Since none of the q_j is a unit, this means that $r = s$ and $p_1 p_2 \cdots p_r$ are associates of $q_1 q_2 \cdots q_r$ in some order. Thus R is a unique factorization domain. \square

Theorem 2.21

Every field is a UFD.

Proof. Every field F is a UFD because it is PID \Rightarrow it is an integral domain and every nonzero is a unit, and it contains no prime. \square

Lemma 2.10 Bézout's lemma

Let R be a PID. If $a, b \in R$, then there exists integers $s, t \in R$ such that

$$\gcd(a, b) = sa + tb. \quad (2.9)$$

In other words, the greatest common divisor of a and b can be expressed as a linear combination of a and b .

Proof. Let $I = \langle a, b \rangle = \{xa + yb \mid x, y \in R\}$. Then I is an ideal of R and so $I = \{c\}$ for some $c \in R$. Since $a, b \in I$, we have

$$c = xa + yb \quad \text{for some } x, y \in R; a, b \in I.$$

Since $c|a$ and $c|b$. Moreover, if $d|a$ and $d|b$, then $d|(xa + yb)$ for any $x, y \in R$; in particular, $a = \alpha d$ and $b = \beta d$ for some $\alpha, \beta \in R$. Thus

$$c = x(\alpha d) + y(\beta d) = (x\alpha + y\beta)d$$

and so $d|c$. Therefore, $c = \gcd(a, b)$.

If q is another greatest common divisor of a and b , then $q = uc$ for some unit $u \in R$;

$$q = (ux)a + (uy)b = xa + yb.$$

Hence greatest common divisor is unique up to multiplication by a unit. \square

2.9 Euclidean Domains

Definition 2.12

An integral domain D is called a **Euclidean Domain** if there is a function d (called the measure) from the nonzero elements of D to the positive integers such that

1. $d(a) \leq d(ab)$ for all nonzero $a, b \in D$; and
2. If $a, b \in D$, $b \neq 0$, then there exists elements $q, r \in D$ such that

$$a = bq + r$$

where $r = 0$ or $d(r) < d(b)$.

☞ **Example 2.9.1.** The ring \mathbb{Z} is a Euclidean domain with $d(a) = |a|$.

☞ **Example 2.9.2.** Let F be a field. Then $F[x]$ is a Euclidean domain with $d(f(x)) = \deg f(x)$.

☞ **Example 2.9.3.** Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain with

$$d(a + bi) = \|a + bi\| = a^2 + b^2. \quad (2.10)$$

Theorem 2.22

Every Euclidean domain is a PID.

Proof. Let E be a Euclidean domain. Consider an ideal I of E . If $I = \{0\}$, then $I = \langle 0 \rangle$.

Let $I \neq \{0\}$. Then $N = \{d(x) \mid x \in I, x \neq 0\}$ is a nonempty set of nonnegative integers; and so, by the well-ordering principle it has the least element.

Let $a \in I, a \neq 0$ such that $d(a)$ is the least element of N . i.e. $d(a) \leq d(x)$ for all nonzero x in I . We want to show $I = Ea$. Since $a \in I$, it follows that

$$Ea \subseteq I.$$

Let $b \in I$. Since E is a Euclidean domain, there exist $q, r \in E$ such that

$$b = aq + r, \quad \text{where } r = 0 \text{ or } d(r) < d(a).$$

If $r \neq 0$, then $r = b - aq \in I$ shows that $d(r) \in N$; and since $d(r) < d(a)$, this contradicts the minimality of $d(a)$ in N . Therefore, $r = 0$ and so $b = aq \in Ea$. Thus $I \subseteq Ea$ and hence $I = Ea$. \square

Remark. If D is Euclidean domain, then it is both PID and UFD.

Theorem 2.23

If D is UFD, then $D[x]$ is UFD.

Proof. Let D be an Euclidean domain and $\emptyset \neq I \triangleleft D$.

Among all the nonzero elements of I , let $a \in I$ be such that $d(a)$ is a minimum. Then

$$I = \langle a \rangle.$$

For if $b \in I$, there exist some q, r such that

$$b = aq + r,$$

where $r = 0$ or $d(r) < d(a)$. But $r = b - aq \in I$, so $d(r)$ cannot be less than $d(a)$. Thus, $r = 0$ and $b = aq \in \langle a \rangle$. \square

Theorem 2.24

Let R be an Euclidean Domain and $I \triangleleft R$. Then I is PID.

Proof. If $I = 0_R$ then $I = \langle 0_R \rangle$ and we are done.

If not, said $\exists x \in R$ with $x \neq 0_R$ and $d(x)$ is minimal. Certainly, $\langle x \rangle \subseteq I$. Conversely if $y \in I$ then there must be some $q, r \in R$ such that

$$y = qx + r$$

where $d(r) < d(x)$ or $r = 0$. As $r = y - qx \in I$ then $r = 0$ by the minimality of $d(x)$. So $y = qx$ and hence $I \subseteq \langle x \rangle$. Thus I is principal. \square

2.9.1 Gaussian Integers

Theorem 2.25

The Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain with

$$d(a + bi) = N(a + bi) = a^2 + b^2.$$

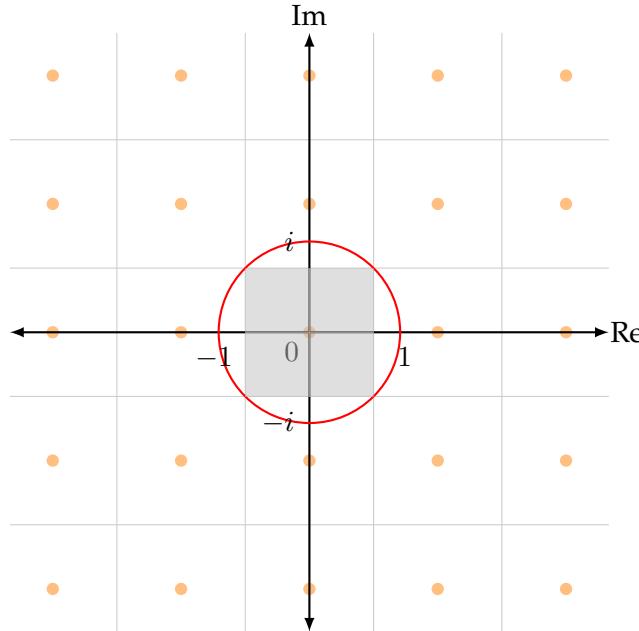
Proof. We construct a map

$$N : \mathbb{Z}[i] \rightarrow \mathbb{Z}^{\geq 0}, \quad N(z) := |z|^2$$

where $|z|$ is the complex norm. Notice that for every integers a and b , we have $N(a + bi) = a^2 + b^2 \in \mathbb{Z}^{\geq 0}$ using Pythagorean theorem. Notice also that for every complex number z , $N(z) = 0$ iff $|z| = 0 \iff z = 0$. Now it is remained to show a type of division algorithm holds in $\mathbb{Z}[i]$ with respect to the function N .

We start with the division in \mathbb{C} : Given any $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, and $\alpha \in \mathbb{Z}[i] \setminus \{0\}$, we have

$$\frac{z}{\alpha} \in \mathbb{C}$$



Notice that the square tiling in the given figure implies that there is a $q \in \mathbb{Z}[i]$ such that $\frac{z}{\alpha} - q$ lies in the centered square. Therefore

$$\left| \frac{z}{\alpha} - q \right| \leq \frac{\sqrt{2}}{2} < 1. \quad (2.11)$$

and so the complex norm of $r := z - q\alpha$ is at most $\frac{\sqrt{2}}{2}|q| < |q|$.

Since z, α, q are in $\mathbb{Z}[i]$, so is $r \in \mathbb{Z}[i]$. All together we obtained the existence of q, r and the division algorithm in $\mathbb{Z}[i]$ as such

$$z = q\alpha + r, \quad \text{where } r = 0 \text{ or } N(r) < N(q).$$

This shows that $\mathbb{Z}[i]$ is a Euclidean domain. An Euclidean domain is a PID, which completes the proof. \square

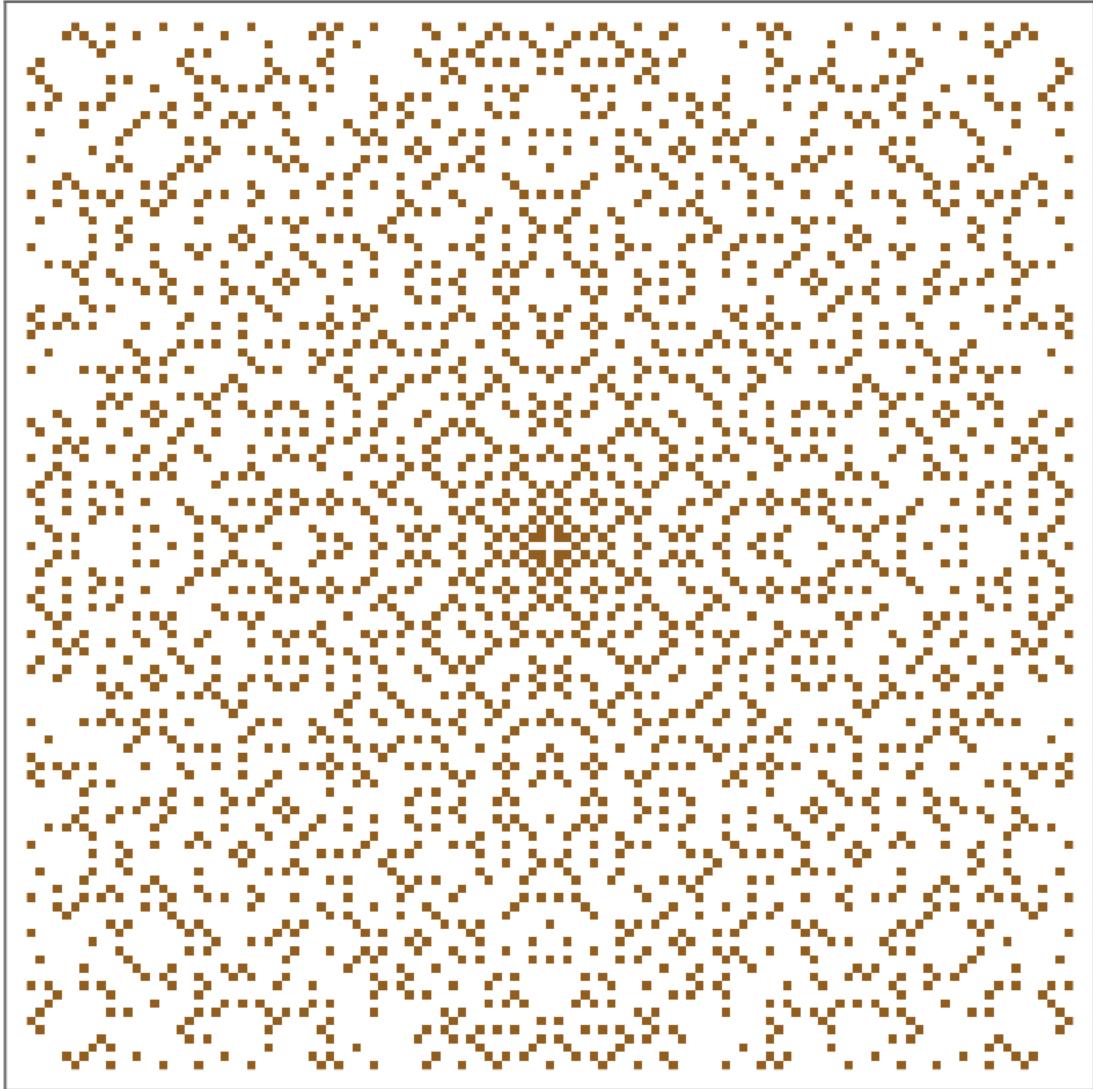


Figure 2.1: The distribution of Gaussian integers in the complex plane.

Example 2.9.4. Factorize $17 - i$ into the product of irreducibles in $\mathbb{Z}[i]$.

Solution Since $d(17 - i) = 17^2 + 1^2 = 290$. The prime factors of 290 are 2, 5, and 29. This indicates that $17 - i$ contains at most three irreducibles. Up to multiplication by units, the only element in $\mathbb{Z}[i]$ with norm of 2 are $1 \pm i$. Now notice that

$$\frac{17 - i}{1 + i} = \frac{(17 - i)(1 - i)}{(1 + i)(1 - i)} = \frac{16 - 18i}{2} = 8 - 9i.$$

Likewise, the only Gaussian integers with a norm of 5 is $1 \pm 2i$ up to units. Now compute

$$\frac{8 - 9i}{1 + 2i} = \frac{(8 - 9i)(1 - 2i)}{(1 + 2i)(1 - 2i)} = \frac{-10 - 25i}{5} = -2 - 5i.$$

Thus

$$17 - i = (1 + i)(8 - 9i)(-2 - 5i)$$

and is the product of three irreducibles. ◀

Tutorials

Exercise 2.9.1 For each of the following, decide whether the indicated operations on the set will form a ring. If a ring is not formed, state the reason why this is the case. If a ring is formed state whether the ring is commutative, whether it has unity, and whether it is a field.

1. $n\mathbb{Z}$, under the usual addition and multiplication.
2. $n\mathbb{R}^+$, under the usual addition and multiplication.
3. $n\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components.
4. $n\mathbb{Z} \times 2\mathbb{Z}$ with addition and multiplication by components.
5. $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication.
6. $\{ri \mid r \in \mathbb{R}\}$ with the usual addition and multiplication where $i^2 = -1$.

Exercise 2.9.2 Let $\alpha = \sqrt[3]{5}$ and $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$. Prove whether $\mathbb{Z}[\alpha]$ is a subring of \mathbb{R} .

Exercise 2.9.3 Let X be some arbitrary set, and $P(X)$ be the set of all subsets of X . Define operators on $P(X)$ as follows, where a, b in $P(X)$:

$$a + b = (a \cup b) \setminus (a \cap b)$$

and

$$ab = a \cap b.$$

Show that $P(X)$ is a commutative ring.

Exercise 2.9.4 Let \mathbb{A} be the set $\mathbb{A} = \{a + bi \mid a, b \in \mathbb{Q}\}$ where $i^2 = -1$. Here,

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

and

$$(a + bi)(c + di) = (ac - bd) + (ad - bc)i.$$

Show that \mathbb{A} is a field.

Exercise 2.9.5 Show that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Exercise 2.9.6 Show that

$$a^2 - b^2 = (a + b)(a - b)$$

for all elements a, b in a ring R if and only if R is commutative.

Exercise 2.9.7 Suppose $x \cdot x = x$ for every element x in a ring R .

1. Show that $x = -x$.
2. Show that R is commutative.

Exercise 2.9.8 Show that a ring R has no nonzero nilpotent element if and only if 0 is the only solution of $x^2 = 0$ in R .

Exercise 2.9.9 Show that a factor ring of a field is either the trivial ring of one element or is isomorphic to a field.

Exercise 2.9.10 Show that if R is a ring with unity and N is an ideal of R such that $N \neq R$, then R/N is a ring with unity.

Exercise 2.9.11 If F is a field, show that $(F \setminus \{0\}, \cdot)$ is a group.

Exercise 2.9.12 Show that in a field F , the only ideals are F and $\{0\}$.

Exercise 2.9.13 Show that each homomorphism from a field to a ring is either one to one or maps everything onto 0.

Exercise 2.9.14 Find the characteristic of the following rings:

1. $2\mathbb{Z}$.
2. $\mathbb{Z}_3 \times 3\mathbb{Z}$.

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

Exercise 2.9.15 Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{Z})$.

Exercise 2.9.16 An element a of a ring R is idempotent if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

Exercise 2.9.17 Let $A = \{a_1, a_2, \dots, a_n\}$ be a finite subset of a commutative ring R with unity. Then show that the set

$$S = Ra_1 + Ra_2 + \cdots + Ra_n = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_i \in R\}$$

is the smallest ideal of R containing A .

Exercise 2.9.18 If A and B are ideals of a ring R , then the sum $A + B$ of A and B is defined by

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

1. Show that $A + B$ is an ideal of R .
2. Show that $A \subseteq A + B$.

Exercise 2.9.19 If A and B are ideals of a ring R , then the product AB of A and B is defined by

$$AB = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}.$$

1. Show that AB is an ideal of R .
2. Show that $AB \subseteq (A \cap B)$.

Exercise 2.9.20 Show that if A and B are coprime ideals of a ring R , then $AB = A \cap B$.

Exercise 2.9.21 If A and B are ideals of a commutative ring R , then the quotient $A \div B$ of A by B is defined by

$$A \div B = \{r \in R \mid rb \in A \quad \forall b \in B\}.$$

Show that $A \div B$ is an ideal of R .

Exercise 2.9.22 Find $q(x)$ and remainder $r(x)$ as described by the division algorithm so that

$$f(x) = g(x)q(x) + r(x)$$

with $r(x) = 0$ or of degree less than the degree of $g(x)$.

1. $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = x^2 + 2x - 3$ in $\mathbb{Z}_7[x]$.
2. $f(x) = x^5 - 2x^4 + 3x - 5$ and $g(x) = 2x + 1$ in $\mathbb{Z}_{11}[x]$.

Exercise 2.9.23 The polynomial $x^4 + 4$ can be factored into linear factors over $\mathbb{Z}_5[x]$. Find this factorization.

Exercise 2.9.24 The polynomial $x^3 + 2x^2 + 2x + 1$ can be factored into linear factors over $\mathbb{Z}_7[x]$. Find this factorization.

Exercise 2.9.25 Let R be a ring that contains at least two elements. Consider for each nonzero $a \in R$, there exists a unique b such that $aba = a$.

1. Show that R has no zero divisors.
2. Show that $bab = b$ is an idempotent.
3. Show that R has unity
4. Show that R is a division ring.

Exercise 2.9.26 Let R be a commutative ring and N be an ideal of R . Show that the set \sqrt{N} of all elements a in R such that $a^n \in N$ for some positive integer n is an ideal of R .

Exercise 2.9.27 Show that the ring $\mathbb{Z}[\sqrt{3}]$ is an Euclidean domain.

Exercise 2.9.28 Suppose D is an integral domain, and let $a, b \in D \setminus \{0\}$. Show that $\langle a \rangle \subseteq \langle b \rangle$ if and only if b divides a .

Exercise 2.9.29 Show that N is a maximal ideal of a ring R if and only if R/N is nontrivial and has no proper nontrivial ideals.

Exercise 2.9.30 Prove that if F is a field, then every proper nontrivial prime ideal of $F[x]$ is maximal.

3

Fields

3.1 Extension Fields

3.1.1 Simple Extension

Definition 3.1 Field Extension

Let F be a field. A **field extension** K of F is a field that contains F as subfield. We denote this by K/F or $K : F$. The degree of the extension K over F is denoted $[K : F]$ or $\dim_F K$, and is defined as the dimension of K as a vector space over F .

Definition 3.2

Let E be an extension field of a field F and let $a \in E$. We call an element a **algebraic** over F if a is the zero of some nonzero polynomial in $F[x]$. If a is not algebraic over F , it is called **transcendental** over F .

Example 3.1.1. \mathbb{C} is an extension field of \mathbb{R} .

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$$

The imaginary number $i = \sqrt{-1}$ is said to be algebraic since $x^2 + 1 = 0 \in \mathbb{R}[x]$. While π is transcendental since it is not a zero in $\mathbb{R}[x]$.

Theorem 3.1

Let K be an extension field of F , and $u \in K$ is an algebraic element over F . Then there exists a unique monic irreducible polynomial $p(x)$ in $F[x]$ that has u as a root. Furthermore if u is a root of $g(x) \in F[x]$, then $p(x)$ divide $g(x)$.

Proof. Notice that $u \in K$ is algebraic over F if and only if there is a nonzero polynomial $f(x) \in F[x]$ such that $f(u) = 0_K$.

Let S be the set of all nonzero polynomials in $F[x]$ that have u as a root, then S is nonempty set. By well-ordering principle, $\exists p(x) \in S$ such that $p(x)$ has the smallest degree in S .

Suppose that $f(x) \in F[x]$ with $f(u) = 0_K$. By division algorithm,

$$f(x) = p(x)q(x) + r(x)$$

with $\deg p(x) > \deg r(x)$ or $r(x) = 0$.

If $r(x) \neq 0$,

$$f(x) - p(x)q(x) = r(x) \implies f(u) - p(u)q(u) = r(u) = 0.$$

This contradicting the fact that $p(x)$ is the smallest polynomial. Thus $r(x) = 0$ and $p(x)$ divide $f(x)$. And now if we let $p(x)$ and $q(x)$ be the smallest polynomial. Then, $p(x)|q(x)$ and $q(x)|p(x)$ implies that $p(x) = q(x)$. \square

Remark. The $p(x)$ is called the "minimal polynomial of u over F ".

Theorem 3.2 Minimal polynomial

Suppose E is a field extension of F , and $\alpha \in E$ is algebraic over F . Suppose the degree of the minimal polynomial $m_\alpha(x)$ of α over F is n . Then every element of $F(\alpha)$ can be written uniquely in the form

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} \quad (3.1)$$

for some c_i 's in F

Proof. By the first isomorphism theorem of rings, we said that

$$\bar{\phi}_\alpha : F[x]/\langle m_\alpha(x) \rangle \rightarrow F[\alpha], \quad \bar{\phi}_\alpha(f(x) + \langle m_\alpha(x) \rangle) := f(\alpha)$$

is an isomorphism. Every element of $F[x]/\langle m_\alpha(x) \rangle$ can be uniquely written as $(\sum_{i=0}^{n-1} c_i x^i) + \langle m_\alpha(x) \rangle$ for some c_i 's in F . Hence, we obtain the conclusion that every element of $F[\alpha]$ can be uniquely written as

$$\bar{\phi}_\alpha \left(\sum_{i=0}^{n-1} c_i x^i + \langle m_\alpha(x) \rangle \right) = \sum_{i=0}^{n-1} c_i \alpha^i.$$

This completes the proof. \square

☞ **Example 3.1.2.** \mathbb{R} is an extension field of \mathbb{Q} and $\sqrt{3} \in \mathbb{R}$ is algebraic, then

$$p(x) = x^2 - 3 \in \mathbb{Q}[x]$$

☞ **Example 3.1.3.** \mathbb{R} is an extension field of \mathbb{Q} and $\sqrt{3} + \sqrt{5} \in \mathbb{R}$ is algebraic, Then

$$p(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x].$$

☞ **Solution** Let $x = \sqrt{3} + \sqrt{5} \in \mathbb{R}$, then

$$\begin{aligned} x^2 &= 3 + 2\sqrt{15} + 5 \Rightarrow x^2 - 8 = 2\sqrt{15} \\ &\Rightarrow (x^2 - 8)^2 = 4 \cdot 15 \\ &\Rightarrow x^4 - 16x^2 + 4 = 0 \end{aligned}$$

Thus $p(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$. \blacktriangleleft

Theorem 3.3

Let K be an extension field of F and $u \in K$ is an algebraic element over F with minimal polynomial $p(x)$ of degree n , then

1. $F[u]$ is a field isomorphism of $F[x]/p(x)$.

2. $\{1, u, u^2, \dots, u^{n-1}\}$ is a basis of the vector space $F(u)$ over F .
3. $[F(u) : F] = n$.

Proof. 1. Since $F(u)$ contains F and u , so $F(u)$ contains every element of the form

$$b_0 + b_1 u + b_2 u^2 + \dots + b_t u^t \quad \forall b_i \in F.$$

We again define a function $\varphi : F[x] \rightarrow F(u)$ by

$$\varphi(f(x)) = f(u).$$

Then φ is ring homomorphism.

Note that $\ker \varphi = \langle p(x) \rangle$ where $p(x)$ is the minimal polynomial of u over F . By the first isomorphism theorem, $F[x]/\langle p(x) \rangle \cong \text{Im } \varphi$. Since $p(x)$ is irreducible, the quotient ring $F[x]/\langle p(x) \rangle$ is a field and $\text{Im } \varphi$ is also a field.

Note that $\varphi(c) = c \ \forall c \in F$ and $\varphi(x) = u$. Thus $F \subset \text{Im } \varphi$ and $u \in \text{Im } \varphi$. By definition of simple extension, $F(u) = \text{Im } \varphi$.

2. Since $F(u) = \text{Im } \varphi$, $\forall w \in F(u), \exists f(x) \in F$ s.t. $f(u) = w$. If $\deg f(x) > n$. By division algorithm, we have

$$f(x) = p(x)q(x) + r(x)$$

If $r(x) = 0$, $f(u) = p(u)q(u) = 0 = w$.

Otherwise, if $r(x) \neq 0$, then

$$r(x) = f(x) - p(x)q(x) \implies r(u) = f(u) - p(u)q(u) = w$$

with $\deg r(x) < n$. Thus

$$F(u) = \text{Span}\{1, u, u^2, \dots, u^{n-1}\}.$$

3. Let $c_0 + c_1 u + c_2 u^2 + \dots + c_{n-1} u^{n-1} = 0$. If $\exists c_k \in F$ s.t. $c_k \neq 0$. Then $p(x)$ is not the minimal polynomial of u over F . Thus $c_i = 0 \forall c_i \in F$. Hence, we can say that $\{1, u, u^2, \dots, u^{n-1}\}$ is linearly independent and it is also a basis of $F(u)$ over $F \implies [F(u) : F] = n$.

□

Example 3.1.4. $\mathbb{Q}[\sqrt{3}]$ is isomorphic to $\mathbb{Q}[\sqrt{3}]/\langle x^2 - 3 \rangle$

Example 3.1.5. If u and v have the same minimal polynomial $p(x)$ in $F[x]$, then $F(u)$ is isomorphic to $F(v)$. For instance,

$$\mathbb{Q}[\sqrt{3}] \cong \mathbb{Q}[-\sqrt{3}].$$

Let $\sigma : F \rightarrow E$ be an isomorphism then we again define $\bar{\sigma} : F[x] \rightarrow E[x]$ by for $a_0 + a_1 x + \dots + a_n x^n \in F[x]$. We can write

$$\sigma(a_0 + a_1 x + \dots + a_n x^n) = \sigma(a_0) + \sigma(a_1 x) + \dots + \sigma(a_n x^n) \quad (3.2)$$

and $\bar{\sigma}$ is also isomorphism.

Corollary 3.1

Let $\sigma : F \rightarrow E$ be an isomorphism of fields. Let u be an algebraic element in "some" extension field of F with minimal polynomial $p(x) \in F[x]$. Again we let v be an algebraic element in some extension field of E with minimal polynomial $\sigma p(x) \in E[x]$. Then σ extends to an isomorphism of fields $\bar{\sigma} : F(u) \rightarrow E(v)$ such that

$$\bar{\sigma}(u) = v \text{ and } \bar{\sigma}(c) = \sigma(c) \quad \forall c \in F.$$

Proof. By previous theorem, $\varphi : F[x]/(p(x)) \rightarrow F(u)$ and $\bar{\varphi} : E[x]/(\sigma p(x)) \rightarrow E(v)$ are isomorphism where $\varphi([f(x)]) = f(u)$ and $\bar{\varphi}([g(x)]) = g(v)$.

Furthermore, we let ξ be the surjective isomorphism

$$\bar{\xi} : E[x] \rightarrow E[x]/(\sigma p(x))$$

defined by $\bar{\xi}(g(x)) = |g(x)|$.

Note that

$$\begin{array}{ccccccc} F[x] & \xrightarrow{\sigma} & E[x] & \xrightarrow{\bar{\xi}} & E[x]/(\sigma p(x)) & \xrightarrow{\bar{\varphi}} & E[v] \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ f(x) & \longrightarrow & \sigma f(x) & \longrightarrow & [\sigma f(x)] & \longrightarrow & \sigma f(v) \end{array}$$

Since $\sigma, \bar{\varphi}$ and $\bar{\xi}$ are surjective, so is the composite function.

$$\begin{aligned} \ker \bar{\phi}(\bar{\xi}(\sigma)) &= \{f(x) \in F[x] \mid \sigma f(v) = 0\} \\ &= \{f(x) \in F[x] \mid \sigma f(x) \in \langle \sigma f(x) \rangle\} \\ &= \langle p(x) \rangle \end{aligned}$$

By First isomorphism theorem,

$$F(u) \cong F[x]/\langle p(x) \rangle \cong^{\theta} E(v)$$

Since $\theta([f(x)]) = \sigma f(v)$. Note that

$$\theta([x]) = \sigma \cdot 1_F \cdot v = 1_V \cdot v = v$$

so we have the following situation

$$\begin{array}{ccccc} F(u) & \xleftarrow{\varphi} & F[x]/\langle p(x) \rangle & \xrightarrow{\theta} & E(v) \\ f(u) & \xleftarrow{\varphi} & [f(x)] & \xrightarrow{\theta} & \sigma f(v) \\ c & \xleftarrow{\varphi} & [c] & \xrightarrow{\theta} & \sigma(c) \end{array}$$

The composite function $\theta \circ \varphi^{-1} : F(u) \rightarrow E(v)$ is an isomorphism that extends σ and maps u

to v .

$$\begin{array}{ccc}
 F & \xrightarrow{\sigma} & E \\
 \downarrow \subseteq & & \downarrow \subseteq \\
 F[x] & \xrightarrow{\sigma} & E[x] \\
 \downarrow \xi & & \downarrow \bar{\xi} \\
 F(u) & \xrightarrow{\varphi} & F[x]/\langle p(x) \rangle \xrightarrow{\sigma} E[x]/\langle \sigma p(x) \rangle \xrightarrow{\bar{\varphi}} E(v)
 \end{array}$$

By First isomorphism thm.

□

Example 3.1.6. $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion. $\sqrt[3]{2} \in \mathbb{R}$ is a root of it. Verify that $\sqrt[3]{2}\omega$ is also a root of $x^3 - 2$ in \mathbb{C} where

$$\omega = \frac{-1 + \sqrt{3}i}{2}$$

is a complex cube root of 1.

Solution Let σ be the identity function from \mathbb{Q} to \mathbb{Q} . By applying the previous corollary, we have

$$\mathbb{Q}(\sqrt[3]{2}) \cong^\theta \mathbb{Q}(\sqrt[3]{2}\omega)$$

such that $\bar{\sigma}(\sqrt[3]{2}) = \sqrt[3]{2}\omega$. And now $(\sqrt[3]{2}\omega)^3 = 2\omega^3 = 2$.

3.1.2 Algebraic Extension

Definition 3.3 Algebraic extension

An extension field K of a field F is said to be an algebraic extension of F if every element of K is algebraic over F .

Example 3.1.7. \mathbb{C} is an algebraic extension of \mathbb{R} . $\forall a + bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$. We have

$$(x + a + bi)(x + a - bi) = x^2 + 2ax + a^2 + b^2.$$

Thus $a + bi$ is a root of $x^2 + 2ax + a^2 + b^2 = 0$.

Theorem 3.4

If K is a finite-dimensional extension field of F , then K is an algebraic extension of F .

Proof. Let $\{V_1, V_2, \dots, V_n\}$ be the basis of K over F . For all $u \in K$, $\{1, u, u^2, \dots, u^n\}$ is linearly dependent. That is,

$$\exists u^k \in K \text{ s.t. } u^k = \text{Span}\{1, u, u^2, \dots, u^n\} = c_0 + c_1u + c_2u^2 + \dots + c_{k-1}u^{k-1} (k \geq 1).$$

Thus u is a root of $f(x) = x^k - c_{k-1}u^{k-1} - \dots - c_0$, this implies K is an algebraic extension.

In fact, a simple extension is an algebraic extension if u is algebraic. If extension field K contains a transcendental element u , then K must be infinite dimensional over F .

Non algebraic \implies Infinite dimension

Note that $F(u)$ denote the intersection of all subfields of K that contains both F and u . It said to be a simple extension of F . If u_1, u_2, \dots, u_n are elements of an extension field K of F . Let $F(u_1, \dots, u_n)$ denote the intersection of all the subfields of K that contain F and every u_i (known as generalized simple extension); $F(u, u_1, \dots, u_n)$ is said to be a finitely generated extension of F .

Theorem 3.5

If $K = F(u_1, u_2, \dots, u_n)$ is a finitely generated extension field of F and each u_i is algebraic over F , then K is a finite-dimensional algebraic extension of F .

Proof. Note that if u, v is algebraic over F , then v is algebraic over $F(u)$. Thus

$$|F(u, v) : F(u)| \cdot |F(u) : F| < \infty \implies |F(u, v) : F| = |F(u, v) : F(u)| \cdot |F(u) : F| < \infty.$$

By mathematical induction, we have

$$|F(u_1, u_2, \dots, u_n) : F(u_1, u_2, \dots, u_{n-1})| \dots |F(u_1) : F| < \infty$$

which is also finite. \square

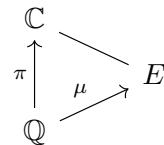
Corollary 3.2

If L is algebraic extension of K and K is an algebraic extension of F . Then L is an algebraic extension field of F .

Proof. $\forall \omega \in L, \exists f(x) \in K[x] \text{ s.t. } f(\omega) = a_0 + a_1\omega + \dots + a_n\omega^n$.

Note that $F(a_0, a_1, \dots, a_n)$ is finitely generated extension of F and all a_i 's are algebraic. Thus it is finite dimensional algebraic extension of F . Since ω is algebraic over $F(a_0, a_1, \dots, a_n)$. So $F(a_0, a_1, \dots, a_n)$ is finite dimensional extension of $F \implies \omega$ is algebraic over F . Thus L is an algebraic extension of F . \square

Remark. Algebraic subfield E of \mathbb{C} over \mathbb{Q} is called the **field of algebraic numbers**. Where E is an finite-dimensional algebraic extension over \mathbb{Q} .



- μ denote algebraic extension over \mathbb{Q} , e.g.: $\sqrt{2}, \sqrt{3}, i, \dots$
- π denote non-algebraic extension.

Corollary 3.3

Let K be an extension field of F and let E be the set of all elements of K that are algebraic over F . Then E is a subfield of K and an algebraic extension field of F .

Proof. We only need to show that E is a field. Let $u, v \in F$, note that $F(u, v)$ is finitely generated extension of F , so E is algebraic extension. E is closed under subtraction and multiplication. Moreover u^{-1} is algebraic over F . Thus E is a subfield of K . \square

Example 3.1.8.

$$\mathbb{Q}(i, -i) = \mathbb{Q}(i)$$

Example 3.1.9.

$$\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3})(i)$$

Solution

$$\begin{aligned} |\mathbb{Q}(\sqrt{3}, i)| &= |\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}| \\ &= |\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})| \cdot |\mathbb{Q}(\sqrt{3}) : \mathbb{Q}| \\ &= 2 \cdot 2 \\ &= 4 \end{aligned}$$



Example 3.1.10. Every finite-dimensional extension is also finitely generated. If $\{u_1, u_2, \dots, u_n\}$ is a basis of K over F . This implies $F(u_1, u_2, \dots, u_n) \subseteq K$ and $K \subseteq F(u_1, u_2, \dots, u_n)$. Thus,

$$K = F(u_1, u_2, \dots, u_n) = \text{Span}\{u_1, u_2, \dots, u_n\}.$$

Example 3.1.11 (Non-example).

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) \neq \mathbb{Q}(\sqrt{3})$$

Solution For the sake of contradiction, consider $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3})$, then

$$\sqrt{5} = a + b\sqrt{3}, \quad \forall a, b \in \mathbb{Q}$$

Altering this equation by moving a to left-hand side, then squaring both sides. We obtain

$$\begin{aligned} (\sqrt{5} - a)^2 &= (b\sqrt{3})^2 \Rightarrow 5 - 2\sqrt{5}a + a^2 = 3b^2 \\ &\Rightarrow \frac{5 + a^2 - 3b^2}{2a} = \sqrt{5} \quad (a \neq 0) \end{aligned}$$

However, when $a = 0$, we have $5 = 3b^2$. Which is a contradiction. \blacktriangleleft

3.2 Splitting Field

In last chapter we had discussed about the integral domain. Suppose polynomial $f(x)$ has degree n . Then $f(x)$ has at most n roots in *any* field. Suppose that K contains fewer than n roots of $f(x)$. It might be possible to find an extension field of K that contains additional roots of $f(x)$.

Definition 3.4 Splitting field

If F is a field and $f(x) \in F[x]$, then an extension field K of F is said to be a **splitting field** (or **root field**) of $f(x)$ over F provided that

- $f(x)$ splits over K , say

$$f(x) = c(x - u_1) \dots (x - u_n) \quad (3.3)$$

- and

$$K = \underbrace{F(u_1, u_2, \dots, u_n)}_{\text{smallest field}}. \quad (3.4)$$

Example 3.2.1. If $f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$ in $\mathbb{Q}[x]$. Then

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = \mathbb{Q}(\sqrt{2}, i)$$

is a splitting field of $f(x)$ over \mathbb{Q} .

3.2.1 Separability

Definition 3.5 Separable polynomial

Let K to be a field. A nonzero polynomial $f(x) \in K[x]$ is *separable* when it has distinct roots in a splitting field over K . That is, each root of $f(x)$ can only appear one at the time. If $f(x)$ has multiple root then $f(x)$ is called *inseparable*.

Example 3.2.2. In $\mathbb{R}[x]$, the polynomial $f(x) = x^2 - x$ is separable since it has two distinct roots: 0 and 1. And $x^3 - 2$ is separable since there are three distinct roots: $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ in the complex plane.

Example 3.2.3. In $\mathbb{F}_3[x]$ the polynomial $f(x) = x^3 - 1 = (x - 1)^3 = (x + 1)^3$ is inseparable since it has a multiple root 1.

Theorem 3.6

A nonzero polynomial $f(x) \in K[x]$ is separable if and only if it is relatively prime to its derivative $f'(x)$ in $K[x]$.

Proof. Let $f(x)$ be a nonzero polynomial in $K[x]$.

(\Rightarrow) Suppose that $f(x)$ is separable and let α be a root of $f(x)$ in some extension field of K . Then

$$f(x) = (x - \alpha)g(x), \quad \text{with } g(\alpha) \neq 0.$$

Since $f'(\alpha) = g(\alpha) \neq 0$, so α is not a root of $f'(x)$. Thus $f(x)$ and $f'(x)$ have no common roots, and hence they have no common factor in $K[x]$ — they are relatively prime.

(\Leftarrow) If $f(x)$ is not separable, so by definition it has a repeated root α in some extension field of K . This root is also a root $f'(x)$. Thus $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in K[x]$. By product rule, we have

$$f'(x) = (x - \alpha)^2 g'(x) + 2(x - \alpha)g(x)$$

So $f'(\alpha) = 0$ implies that $f(x)$ and $f'(x)$ have a common factor $(x - \alpha)$ in $K[x]$. In particular, $f(x)$ and $f'(x)$ are not relatively prime (in $K[x]$). Taking the contrapositive, if $f(x)$ and $f'(x)$ are relatively prime, then $f(x)$ is separable. \square

Example 3.2.4. In $\mathbb{F}_3[x]$, let $f(x) = x^6 + x^5 + x^4 + 2x^3 + 2x^2 + x + 2$. Using Euclid's algorithm to verify that $f(x)$ is inseparable.

Solution We first compute the derivative

$$f'(x) = 6x^5 + 5x^4 + 4x^3 + 6x^2 + 4x = 2x^4 + x^3 + x.$$

Then we apply Euclid's algorithm:

$$f(x) = f'(x) \cdot (2x^2 + 2) + (2x^2 + 2)$$

$$f'(x) = (2x^2 + 2) \cdot (x^2 + 2x + 2) + 0.$$

The greatest common divisor is $2x^2 + 2 \neq 1$. Thus $f(x)$ is not separable in $\mathbb{F}_3[x]$. \blacktriangleleft

Example 3.2.5. Let $f(x) = x^4 - 3x - 2$ in $\mathbb{Q}[x]$. Using Euclid's algorithm to verify that $f(x)$ is separable.

Solution We first compute $f'(x) = 4x^3 - 3$. Then we apply Euclid's algorithm to find

$$\begin{aligned} f(x) &= f'(x) \cdot \left(\frac{1}{4}x \right) - \frac{9}{4}x - 2 \\ f'(x) &= \left(-\frac{9}{4}x - 2 \right) \left(-\frac{16}{9}x^2 + \frac{128}{81}x - \frac{1024}{729} \right) \underbrace{-\frac{4235}{729}}_{\text{remainder}}. \end{aligned}$$

By inspection, we have reached a remainder that is a nonzero constant. Thus $f(x)$ and $f'(x)$ are relatively prime in $\mathbb{Q}[x]$. Hence, $f(x)$ is separable. \blacktriangleleft

3.3 Finite Fields

Theorem 3.7

Let R be a ring with identity. Then

1. The set

$$\mathfrak{G} = \{k \cdot 1_R \mid k \in \mathbb{Z}\}$$

is a subring of R .

2. If R has characteristic 0, then \mathfrak{G} is isomorphic to \mathbb{Z} .

3. If R has characteristic $n > 0$, then \mathfrak{G} is isomorphic to \mathbb{Z}_n .

Proof. We prove each of the statements listed above.

- First of all, we use subring test to check if \mathfrak{G} is a subring of R .

$$\begin{cases} a \cdot 1_R - b \cdot 1_R = (a - b) \cdot 1_R \in \mathfrak{G} \\ a \cdot 1_R \cdot b \cdot 1_R = ab \cdot 1_R \in \mathfrak{G} \end{cases}$$

so \mathfrak{G} is a subring of R .

We now prove (2), (3) at once, We consider a map $f : \mathbb{Z} \rightarrow \mathbb{R}$ defined by

$$f(n) = n \cdot 1_R \quad \forall n \in \mathbb{Z}.$$

Then f is homomorphism because

$$f(n+m) = (n+m) \cdot 1_R = f(n) + f(m)$$

and the kernel is

$$\ker f = \{n \in \mathbb{Z} \mid n \cdot 1_R = 0_R\}.$$

By the first isomorphism theorem, $\mathbb{Z}/\ker f$ is isomorphic to \mathbb{R} .

- If R has a characteristic 0, then $\ker f = \langle 0 \rangle \implies \mathbb{Z} \cong \mathbb{R}$.
- If R has a characteristic n , then $\ker f = \langle n \rangle \implies \mathbb{Z}/\langle n \rangle \cong \mathbb{R}$.

□

Corollary 3.4

Every finite field has characteristic p for some prime p .

Proof. Since finite field is integral domain, it must has characteristic prime p . □

Remark. 1. The converse of it is false. There are infinite fields of characteristic p (i.e. $\mathbb{Z}_p[x]$).

$$\mathfrak{G} = \{k \cdot 1_R \mid k \in \mathbb{Z}\}$$

is called the prime subfield of K and is contained in every subfield of K . Which means every field of characteristic p must contains \mathbb{Z}_p .

2. The number of elements in a finite field K is called the order of K .

3.3.1 Order of finite field

Theorem 3.8

A finite field K has order p^n , where p is the characteristic of K and $n = |K : \mathbb{Z}_p|$.

Proof. Let K be a finite dimensional extension of \mathbb{Z}_p . Let $n = |K : \mathbb{Z}_p|$, then $\{u_1, u_2, \dots, u_n\}$ is a basis of K .

$\forall k \in K$, k is represented uniquely be

$$k = c_1 u_1 + c_2 u_2 + \cdots + c_n u_n.$$

There are precisely p^n distinct linear combinations of the form. Thus $|K| = p^n$. □

Lemma 3.1 The Freshman's dream

Let R be a commutative ring with identity of characteristic p , where p is a prime. Then for every $a, b \in R$ and for all positive integer n we have

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}. \quad (3.5)$$

Proof. We will use the induction on n .

Assume $n = 1$, we expand $(a + b)^p$ with binomial theorem.

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^{n-k} b^k = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Note that

$$\binom{p}{k} = \frac{p!}{(p-k)! k!}, \quad k, p-k < p \text{ for } 1 \leq k < p.$$

This implies that p divide $\binom{p}{k} \implies \binom{p}{k} a^{p-k} b^k = 0 \pmod{p}$. Thus $(a + b)^p = a^p + b^p$. We are done for base case.

Assume that it holds for all less than n .

$$\begin{aligned} (a + b)^{p^n} &= ((a + b)^p)^{p^{n-1}} \\ &= (a^p + b^p)^{p^{n-1}} \\ &= (a^p)^{p^{n-1}} + (b^p)^{p^{n-1}} \\ &= a^{p^n} + b^{p^n}. \end{aligned}$$

Therefore the theorem is true for every positive integer n . Now we are done. \square

Theorem 3.9 Existence of finite field

Let K be an extension field \mathbb{Z}_p . For all positive integer n , K has order p^n if and only if K is a splitting field of $x^{p^n} - x$ over \mathbb{Z}_p .

Proof. (\Rightarrow) Let $f(x) = x^{p^n} - x$ over \mathbb{Z}_p . Then

$$f(x) = p^n x^{p^n-1} - 1 = -1$$

and so $f(x)$ and $f'(x)$ are relatively prime $\implies f(x)$ is separable. Then $f(x)$ has p^n distinct roots in splitting field. Let c be any nonzero element of K . Let $\{c_1, c_2, \dots, c_{p^n-1}\}$ be all the nonzero elements of K and let

$$u = c_1 c_2 \cdots c_k.$$

Note that $\{cc_1, cc_2, \dots, cc_k\}$ are all distinct and nonzero elements of K . Thus

$$\{cc_1, cc_2, \dots, cc_k\} = \{c_1, c_2, \dots, c_{p^n-1}\}$$

and

$$cc_1 \cdot cc_2 \cdots cc_{p^n-1} = c_1 \cdot c_2 \cdots c_{p^n-1} \Rightarrow c^{p^n-1} = 1_K \Rightarrow c^{p^n} - c = 0.$$

So all nonzero elements of K consisting of the p^n distinct roots of $x^{p^n} - x$ over \mathbb{Z}_p .

(\Leftarrow) On the other hand, let E be the subset of K consisting of the p^n distinct roots of $x^{p^n} - x$. We want to show E is a subfield of K .

For all a, b in E , $a^{p^n} = a$ and $b^{p^n} = b$. So

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} = a + b \Rightarrow a + b \in E$$

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab \Rightarrow ab \in E$$

$$(-a)^{p^n} = (-1)^{p^n} a^{p^n} = -a \Rightarrow -a \in E$$

and

$$(a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1}.$$

Clearly $0, 1 \in E$. Since K is a field, the rest of axioms are true. Since K is splitting field of $x^{p^n} - x$, $K \subseteq E$. Hence $K = E$ and $|K| = |E| = p^n$. \square

3.4 Galois Theory

The classical question of algebra : Whether or not there were formulas for the solution of higher degree polynomial equations. There are no formula for the solution of all polynomial equations of degree n when $n \geq 5$.

Galois theory had a profound influence on the development of later mathematics for beyond the scope of the original solvability problem. Why? Because his theory connecting the field extensions with groups.

The *Galois group* of an extension E/F , denoted $\text{Gal}_F E$, is the group of automorphisms of E which are the identity on field F .

Definition 3.6 Galois group

Let K be an extension field of F . An F -automorphism of K is an isomorphism $\sigma : K \rightarrow K$ that fixes F elementwise. That is, $\sigma(c) \rightarrow c, \forall c \in F$.

The set of all F -automorphisms of K is denoted $\text{Gal}_F K$ and is called the Galois group of K over F .

Remark. Some books use the notation $\text{Gal}(E/F)$ to denote the galois group of extension E/F . In this notes we write $\text{Gal}_F E$, the subscript represents the field

Theorem 3.10

If K is an extension field of F , then $\text{Gal}_F K$ is a group under the operation of composition of functions.

Proof. We need to show that the function composition from a group:

[Closedness]: $\forall \sigma, \tau \in \text{Gal}_F K, \quad \sigma \circ \tau(c) = c \quad \forall c \in F$.

[Associativity]: Associativity holds because of function composition's property.

[Existence of identity]: $\forall \sigma \in \text{Gal}_F K, \sigma \circ \tau = \tau \circ \sigma = \sigma$.

[Existence of inverse]: $\forall \sigma \in \text{Gal}_F K, \sigma^{-1}(c) = c \quad \forall c \in F$. So σ^{-1} is the inverse in $\text{Gal}_F K$. \square

Theorem 3.11

Let K be an extension field of F and $f(x) \in F[x]$. If $u \in K$ is a root of $f(x)$ and $\sigma \in \text{Gal}_F K$, then $\sigma(u)$ is also a root of $f(x)$.

Proof. Take a $u \in K$, $f(u) = 0 \implies \sigma(f(u)) = \sigma(0) = 0$.

Since $\sigma \in \text{Gal}_F K$, $\sigma(f(u)) = f(\sigma(u)) = 0$. \square

Remark. Every root of $p(x)$ in K is the image of u under some automorphism of $\text{Gal}_F K$.

Theorem 3.12

Let K be the splitting field of some polynomial over F and $u, v \in K$. Then there exists an $\sigma \in \text{Gal}_F K$ such that $\sigma(u) = v$ if and only if u and v have the same minimal polynomial.

Proof. (\Rightarrow) Note that if K is splitting field of $f(x)$ with $\deg f = n$. Then

$$|K : F| \leq n! \implies K \text{ is algebraic over } F.$$

So u has a minimal polynomial $q(x)$ over F .

By previous theorem, $p(v) = 0$ and $q(u) = 0$. These imply $p(x)|q(x)$ and $q(x)|p(x)$ and hence $p(x) = q(x)$. We are done for this direction.

(\Leftarrow) On the other hand, in simple extension, we can extend an isomorphism $\sigma : F \rightarrow F$ to $\bar{\sigma} : \bar{F} \rightarrow \bar{F}$ such that $\bar{\sigma}(u) = v$ and $\bar{\sigma}(c) = c$ for all constant $c \in F$.

Since K is splitting field of some polynomial over F , which is also a splitting field of $F(u)$ and $F(v)$. We can extend an isomorphism $\bar{\sigma}$ to an isomorphism $\tilde{\sigma} : K \rightarrow K$. If $\sigma = 1$, then $\tilde{\sigma} \in \text{Gal}_F K$. \square

Example 3.4.1. Given that $\sigma \in \text{Gal}_{\mathbb{R}} \mathbb{C}$, find $\sigma(i)$.

Solution By previous theorem,

$$\sigma(i) = \{i, -i\}.$$

Thus $\text{Gal}_F K = \{1, \sigma\}$ is a group of order 2 and hence $\text{Gal}_{\mathbb{R}} \mathbb{C}$ is isomorphic to \mathbb{Z}_2 . \blacktriangleleft

Theorem 3.13 Galois group of finitely generated extension

Let $K = F(u_1, u_2, \dots, u_n)$ be an algebraic extension field of F . If $\sigma \circ \tau \in \text{Gal}_F K$ and $\sigma(u_i) = \tau(u_i)$ for each $i = 1, 2, \dots, n$. Then $\sigma = \tau$.

In other words, an automorphism in $\text{Gal}_F K$ is completely determined by its action on u_1, u_2, \dots, u_n .

Proof. Let $\beta = \sigma^{-1} \circ \tau$, then

$$\sigma^{-1} \circ \tau(u_i) = \sigma^{-1} \circ \sigma(u_i) = u_i.$$

Let $v \in F(u_i)$, then there exists a constant $c_i \in F$ such that

$$c_0 + c_1 u_1 + \dots + c_{n-1} u_1^{n-1} = w \implies \beta(v) = v.$$

Again we let $w \in F(u_1, u_2)$, then there exists a constant $c_i \in F$ such that

$$c_0 + c_1 u_2 + \cdots + c_{n-1} u_2^{n-1} = w \implies \beta(w) = w.$$

Repeating this process, we conclude that for all $v \in K$, $\beta(v) = v \implies \beta = 1$. Thus $\tau = \sigma$. \square

 **Example 3.4.2.** Consider $\sigma \in \text{Gal}_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}, \sqrt{5}]$. We let two actions

$$\tau(\sqrt{3}) = -\sqrt{3}, \quad \tau(\sqrt{5}) = \sqrt{5}$$

and

$$\alpha(\sqrt{3}) = \sqrt{3}, \quad \alpha(\sqrt{5}) = -\sqrt{5}$$

and defined $\beta = \alpha \circ \tau$.

Then $\text{Gal}_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \tau, \alpha, \beta\}$ such that

	1	τ	α	β
$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
$\sqrt{5}$	$\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$

Note that τ, α, β both have an order 2. Thus $\text{Gal}_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}, \sqrt{5}] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Corollary 3.5

If K is splitting field of a separable polynomial $f(x)$ of degree n in $F[x]$, then $\text{Gal}_F K$ is isomorphic to a subgroup of S_n .

Proof. Let u_1, u_2, \dots, u_n be distinct roots of $f(x)$. Then $K = F(u_1, u_2, \dots, u_n)$ and let

$$\mathcal{U} = \{u_1, u_2, \dots, u_n\}.$$

For all permutation $\sigma \in \text{Gal}_F K$, $\forall 1 \leq i \leq n$, $\sigma(u_i) = u_j$ for some j .

Now define a function $\theta : \text{Gal}_F K \rightarrow S_n$ defined by $\theta : \sigma \mapsto \sigma \circ 1_{\mathcal{U}}$. θ is well defined. Note that

$$\sigma \circ 1_{\mathcal{U}} = \tau \circ 1_{\mathcal{U}} \implies \sigma = \tau$$

by previous theorem. Thus θ is injective, and θ is homomorphism.

By the first isomorphism theorem, we say that

$$\text{Gal}_F K \cong \text{Im } \theta = \text{a subgroup of } S_n.$$

\square

Definition 3.7 Intermediate field

Let K be an extension field of F . A field E such that

$$F \subseteq E \subseteq K$$

is called an **intermediate field** of the extension. Clearly that $\text{Gal}_E K \cong \text{Gal}_F K$.

Theorem 3.14

Let K be an extension field of F . If H is a subgroup of $\text{Gal}_F K$, let

$$E_H = \{k \in K \mid \sigma(k) = k \text{ for every } \sigma \in H\}.$$

Then E_H is an intermediate field of the extension K . The field E_H is called the "fixed field" of subgroup H .

Proof. It is clear that $F \subseteq E_H \subseteq K$. So we only want to show that E_H is a subfield.

Let $a, b \in E_H$. For all $\sigma \in H$, we have

$$\begin{aligned}\sigma(a + b) &= \sigma(a) + \sigma(b) = a + b \\ \sigma(ab) &= \sigma(a)\sigma(b) = ab \\ \sigma(0_K) &= 0_K, \sigma(1_K) = 1_K \\ \sigma(-a) &= -\sigma(a) = -a \\ \sigma(a^{-1}) &= (\sigma(a))^{-1} = a^{-1}\end{aligned}$$

Thus E_H is a subfield of K . □

Example 3.4.3. From previous example,

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{3}, \sqrt{5}].$$

And $\text{Gal}_{\mathbb{Q}[\sqrt{3}]} \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \alpha\}$, and $\text{Gal}_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \tau, \alpha, \beta\}$.

Example 3.4.4. $\text{Gal}_{\mathbb{Q}[\sqrt{3}]} \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \alpha\}$ is the fixed field of $\mathbb{Q}[\sqrt{3}] = \{1, \alpha\}$, where

$$\alpha(\sqrt{3}) = \sqrt{3}, \alpha(\sqrt{5}) = -\sqrt{5}.$$

Solution For all $a_i \in \mathbb{Q}$. Compute

$$\begin{aligned}\alpha(a_0 + a_1\sqrt{3} + a_2\sqrt{5} + a_3\sqrt{15}) &= a_0 + a_1\sqrt{3} + a_2\sqrt{5} + a_3\sqrt{15} \\ \iff a_0 + a_1\sqrt{3} - a_2\sqrt{5} - a_3\sqrt{15} &= a_0 + a_1\sqrt{3} + a_2\sqrt{5} + a_3\sqrt{15} \\ \iff a_2\sqrt{5} + a_3\sqrt{15} &= 0 \\ \iff a_2 + a_3\sqrt{3} &= 0\end{aligned}$$

Since $a_2a_3^{-1} \in \mathbb{Q} \implies -\sqrt{3} \in \mathbb{Q}$, which is a contradiction. ◀

Example 3.4.5. $\text{Gal}_{\mathbb{R}} \mathbb{C} = \{1, \alpha\}$, and $\alpha(a + bi) \implies a - bi = a + bi \implies b = 0$. Thus fixed field of $\text{Gal}_{\mathbb{R}} \mathbb{C}$ is the field \mathbb{R} .

Remark. The ground field F need not always be the fixed field of the group $\text{Gal}_F K$.

Example 3.4.6. $\sqrt[3]{2}$ is the root of $x^3 - 2 = 0$. So $\sqrt[3]{2} \mapsto \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$, where ω is the cube root of unity.

However, $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \notin \mathbb{Q}[\sqrt[3]{2}]$. $\forall \sigma \in \text{Gal}_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}], \sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Thus $\sigma = 1$. The fixed field of $\text{Gal}_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}]$ is $\mathbb{Q}[\sqrt[3]{2}]$.

Theorem 3.15

Suppose the extension E/F is a splitting field of some polynomial. Then $\forall \alpha \in E$, the minimal polynomial of α must split completely (into the linear factors) in E .

Proof. Suppose E is the splitting field of some polynomial Q , and we fix $\alpha \in E$ with polynomial $p(x)$; then we want to show that $p(x)$ splits completely in E .

Let K be a subfield of E where $p(x)$ splits completely. Then in K , we have

$$p(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

where $\alpha_i \in K$ for all i and $\alpha_1 = \alpha$. We need to check that $\alpha_i \in E$ for all i , and we already know $\alpha \in E$.

Again, we have that $F(\alpha_i) \cong F(\alpha)$, since α_i and α have the same minimal polynomial. Now consider E from the perspective of these intermediate fields. We know that E is the splitting field from Q over $F(\alpha)$. But we do not yet know whether α_i is in E or not, but at least we know that if we adjoin it, then $E(\alpha_i)$ is the splitting field for Q over $F(\alpha_i)$.

By the uniqueness of the splitting field, there exists an isomorphism $E \cong E(\alpha_i)$ extending the isomorphism $F(\alpha) \cong F(\alpha_i)$. We had identified both $F(\alpha)$ and $F(\alpha_i)$, and since Q has coefficients in F (which preserved by the isomorphism). It is the same polynomial in both fields — the isomorphism takes one copy of Q to the other.

Since our isomorphism is the identity of F , this means

$$[E : F] = [E(\alpha_i) : F],$$

and since $E(\alpha_i) \supset E$, this means we must have $E(\alpha_i) = E$, and therefore $\alpha_i \in E$. \square

3.4.1 Fundamental Theorem of Galois theory

Definition 3.8 Galois correspondence

Let K be a finite-dimensional extension field of F , and let S be the set of all intermediate fields. Again we let T be the set of all subgroups of the Galois group $\text{Gal}_F K$.

Define a map $\phi : T \rightarrow S$ by this rule. For each intermediate field E ,

$$\phi(T) = \text{Gal}_E K. \quad (3.6)$$

This function ϕ is called the Galois correspondence.

$$\begin{array}{ccc} \text{Gal}_K K & \longrightarrow & K \\ T \uparrow & & \downarrow S \\ \text{Gal}_F K & \longrightarrow & F \end{array}$$

Example 3.4.7.

$$\mathbb{Q} \rightarrow \text{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{1, \tau, \alpha, \beta\}$$

Lemma 3.2

Let K be a finite-dimensional extension field of F . If H is a subgroup of the Galois group $\text{Gal}_F K$ and E is the **fixed field** of H , then K is *simple, normal, separable extension* of E .

$$\begin{array}{ccc} \text{Gal}_F K & & K \\ | & & | \\ H & \longrightarrow & E_H \end{array}$$

Proof. Since K is finite-dimensional extension field, so K is algebraic over F . Let $\mathfrak{U} \in K$ and $p(x) \in E[x]$ be minimal polynomial of \mathfrak{U} , and $\forall \sigma \in H, \sigma(\mathfrak{U})$ is some root of $p(x)$.

Therefore, \mathfrak{U} has a finite number of distinct images under automorphisms in H , said

$$\mathfrak{U} = u_1, u_2, \dots, u_t \in K, \quad \text{where } t \leq \deg p(x)$$

If $\sigma \in H$ and $u_i = \tau(\mathfrak{U})$ with $\tau \in H$, then $\sigma(u_i) = \sigma \circ \tau(\mathfrak{U})$.

Since σ is injective, so

$$\mathfrak{U} \xrightarrow{H} \{u_1, u_2, \dots, u_t\}$$

which $\{u_1, u_2, \dots, u_t\}$ is image of \mathfrak{U} . And $u_i = \tau(\mathfrak{U})$ for some $\tau \in H$. is injective

$$\{u_1, u_2, \dots, u_t\} \xrightarrow[\text{permutation } \sigma]{} \{u_1, u_2, \dots, u_t\}$$

Every automorphism in H permutes u_1, u_2, \dots, u_t . Let

$$f(x) = (x - u_1)(x - u_2) \dots (x - u_t)$$

Since all u_i 's are distinct, $f(x)$ is separable.

Now we claim that $f(x) \in E[x]$. Note that $\sigma f(x) = f(x)$ for all $\sigma \in H$. All coefficients of $f(x)$ is fixed by $\sigma \in H$. Thus $f(x) \in E[x]$. Since $u = u_1$ is a root of $f(x) \in E[x]$, u is separable over $E \implies K$ is separable extension of E .

From the previous theorem, $K = E(V)$ for some $V \in K$. Let $g(x) = (x - v)(x - v_2) \dots (x - v_s)$ where $\{v_1 = v, v_2, \dots, v_s\}$ are images of $\sigma \in H$. Similarly, $g(x) \in E[x]$ and $K = E(v)$ is splitting field of $g(x)$. Therefore K is normal extension of E . \square

Definition 3.9 Galois extension

If K is a finite dimensional, normal, separable extension field of the field F , we say that K is a Galois extension of F or that K is Galois over F .

Corollary 3.6

Let K be a finite dimensional extension field of F . Then K is Galois over F if and only if F is fixed field of the Galois group over F .

Proof. (\Rightarrow) By previous theorem, $E = F$. Thus F is fixed field of the Galois group over F .

(\Leftarrow) By lemma, K is simple, normal, separable extension of F . \square

Theorem 3.16 Fundamental theorem of Galois Theory

If K is a Galois extension field of F ,

1. There is a bijection between the set S of all the intermediate fields of the extension and the set T of all subgroups of the Galois group $\text{Gal}_F K$, given by assigning each intermediate field E to the subgroup $\text{Gal}_E K$. Furthermore

$$|K : E| = |\text{Gal}_E K|$$

and

$$|E : F| = |\text{Gal}_F K : \text{Gal}_E K|.$$

2. An intermediate field E is normal extension of F if and only if the corresponding group $\text{Gal}_E K$ is a normal subgroup of $\text{Gal}_F K$.

Proof. 1. By theorem, fixed field of $\text{Gal}_E K$ is E . By theorem we have

$$|\text{Gal}_E K| = |K : E|.$$

Similarly,

$$|\text{Gal}_F K| = |K : F|.$$

In fact $|K : F| = |K : E| |E : F|$. Thus

$$|\text{Gal}_F K| = |\text{Gal}_E K| \cdot |E : F| \implies |E : F| = |\text{Gal}_F K : \text{Gal}_E K|.$$

2. (\Leftarrow) Assume first that $\text{Gal}_E K$ is a normal subgroup of $\text{Gal}_F K$. If $p(x)$ is an irreducible polynomial in $F[x]$ with a root $u \in E$, we must show that $p(x)$ splits in $E[x]$.

Since K is normal over F . We know that $p(x)$ splits in $K[x]$. So we know that $p(x)$ also splits in $K[x]$. So we need to show that each root v of $p(x)$ in K is actually in E . There is an automorphism $\sigma \in \text{Gal}_F K$ such that $\sigma(u) = v$ by theorem. So $\text{Gal}_F K = |K : F| = E$.

$$\begin{array}{ccc} K = F(u) & \xrightarrow{\sigma} & F(u) = K \\ \downarrow & & \downarrow \\ F & \xrightarrow{1} & F \end{array}$$

Now if τ is any element of $\text{Gal}_E K$, then normality implies

$$\tau \circ \sigma = \sigma \circ \tau' \quad \text{for some } \tau' \in \text{Gal}_E K.$$

Since $u \in E$, we have

$$\begin{aligned} \tau(v) &= \tau(\sigma(u)) \\ &= \sigma(\tau'(u)) \\ &= \sigma(u) \\ &= v. \end{aligned}$$

So $\text{Gal}_E K$ fixes other roots for all $v \in E$. Thus E is normal extension of F .

(\Rightarrow) Assume that E is normal subgroup of F . Then there exists a surjective homomorphism of groups $\theta : \text{Gal}_F K \rightarrow \text{Gal}_F E$ whose kernel is $\text{Gal}_E K$. Then $\text{Gal}_E K$ is normal subgroup

of $\text{Gal}_F K$.

Therefore by First isomorphism theorem, $\text{Gal}_F E \cong \text{Gal}_F K / \text{Gal}_E K$. □

Lemma 3.3

Let K be a finite-dimensional normal extension field of F and E an intermediate field which is normal over F . Then there is a surjective homomorphism of groups

$$\theta : \text{Gal}_F K \rightarrow \text{Gal}_F E$$

where kernel of θ is $\text{Gal}_E K$.

Proof. Let $\sigma \in \text{Gal}_F K$ and an $u \in E$. Then u is algebraic over F with minimal polynomial $p(x)$.

Since E is normal, all roots of $p(x)$ are in E . Since $\sigma(u)$ is also root of $p(x)$, $\sigma(u) \in E$. Therefore

$$\sigma(E) \subseteq E \quad \forall \sigma \in \text{Gal}_F K.$$

Thus we can restrict σ to E and $\sigma \circ 1_E$ is an F -isomorphism that is $E \cong \sigma(E)$. Hence,

$$|E : F| = |\sigma(E) : F|.$$

Since K is splitting field over F , K is also splitting field over E . $\forall \sigma \in \text{Gal}_F E$. σ can be extended to an F -automorphism in $\text{Gal}_F K$. Its kernel consists of the automorphisms of K whose restriction to E is the identity map as $\text{Gal}_E K$. □

Example 3.4.8. Let K be the splitting field of $x^3 - 2$. Note that

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}] \subseteq K$$

and $|\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| = 3$. K is Galois extension of \mathbb{Q} such that

$$|\text{Gal}_{\mathbb{Q}} K| = |K : \mathbb{Q}|$$

and $\text{Gal}_{\mathbb{Q}} K$ is isomorphic to a subgroup of S_3 .

$$\begin{aligned} 3 < |K : \mathbb{Q}| \leq 6 &\implies 3 < |K : \mathbb{Q}[\sqrt[3]{2}]| \cdot |\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| \leq 6 \\ &\implies 3 < 3 |K : \mathbb{Q}[\sqrt[3]{2}]| \leq 6 \\ &\implies 1 < |K : \mathbb{Q}[\sqrt[3]{2}]| \leq 2. \end{aligned}$$

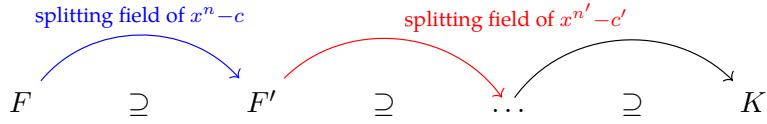
We must have $|K : \mathbb{Q}| = 6$ and $\text{Gal}_{\mathbb{Q}} K \cong S_3$.

$\mathbb{Q}[\omega]$ is the splitting field of $x^2 + x + 1$ and hence $\mathbb{Q}[\omega]$ is normal and separable. Thus K is Galois over \mathbb{Q} .

3.5 Solvability by Radicals

We shall assume that all fields have characteristic 0. A "formula" is a specific procedure that starts with coefficients of the polynomial $f(x) \in F[x]$ and arrives at the solutions of equation $f(x) = 0_F$ by using only the field operations $(+_F, -_F, \times_F, \div_F)$ and the extraction of roots (such as $\sqrt[n]{\cdot}$).

In this context, an n -th root of an element c in field F is any root of the polynomial $x^n - c$ in some extension field of F . If that "formula" really exists, then there exists an extension field K of F such that



Definition 3.10 Radical extensions

A field K is said to be a radical extension of a field F if there is a chain of fields

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_t = K$$

such that for each $i = 1, 2, \dots, t$, $F_i = F_{i-1}(u_i)$ and some power of u_i is in F_{i-1} ($u_i^{k_i} \in F_{i-1}$). The equation $f(x) = 0_F$ is said to be solvable by radicals if there is a radical extension of F that contains a splitting field of $f(x)$. If not, then $f(x)$ is not solvable by radical.

Think of this, said K is a radical extension of a field F if there exist nonzero elements $u_1, u_2, \dots, u_m \in K$ and positive integers n_1, n_2, \dots, n_m such that $K = F(u_1, u_2, \dots, u_m)$, and

$$\begin{aligned} u_1^{n_1} &\in F, \\ u_2^{n_2} &\in F(u_1), \\ u_3^{n_3} &\in F(u_1, u_2), \\ &\vdots \\ u_k^{n_k} &\in F(u_1, u_2, \dots, u_{k-1}). \end{aligned}$$

The definition expresses that u_i is an n_i -th root of some element in $F(u_1, u_2, \dots, u_{i-1})$, so K may be thought of as being built by iteratively adding in n -th roots of elements. The picture depicted as following:

$$\begin{array}{c} K = F(u_1, u_2, \dots, u_m) \\ | \\ u_m^{n_m} \in F(u_1, u_2, \dots, u_{m-1}) \\ | \\ \vdots \\ | \\ u_2^{n_2} \in F(u_1) \\ | \\ u_1^{n_1} \in F \end{array}$$

Example 3.5.1. Show that the field $\mathbb{Q}(\sqrt{3 + \sqrt{21}})$ has degree 4 over \mathbb{Q} and hence find a basis.

☞ **Solution** We let $\alpha = \sqrt{3 + \sqrt{21}}$, and

$$\alpha^2 = 3 + \sqrt{21} \implies \alpha^2 - 3 = \sqrt{21}.$$

Squaring both sides gives

$$(\alpha^2 - 3)^2 = 21 \implies x^4 - 6x^2 - 12 = 0$$

However, the polynomial $q(x) = x^4 - 6x^2 - 12$ is irreducible over \mathbb{Q} by Eisenstein's criterion with $p = 3$. Thus, $q(x)$ must be the minimal polynomial of α .

Therefore, by results, we see that $[\mathbb{Q} : \mathbb{Q}(\alpha)]$ and that the basis is $\{1, \alpha, \alpha^2, \alpha^3\}$. ◀

☞ **Example 3.5.2.** The solutions of $x^3 + 3x + 2 = 0 \in \mathbb{Q}[x]$ are

$$\boxed{\sqrt[3]{-1 + \sqrt{2}} + \sqrt[3]{-1 - \sqrt{2}}} \quad \boxed{\omega \sqrt[3]{-1 + \sqrt{2}} + (\omega^2) \sqrt[3]{-1 - \sqrt{2}}} \quad \boxed{(\omega^2) \sqrt[3]{-1 + \sqrt{2}} + \omega \sqrt[3]{-1 - \sqrt{2}}}$$

Definition 3.11 Solvable groups

A group G is said to be solvable if it has a "chain" of subgroups

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{n-1} \triangleright G_n = \langle e \rangle$$

and G_{i-1}/G_i is abelian.

☞ **Example 3.5.3.** Every abelian group G is solvable. $G \supseteq \langle e \rangle$ and $G/\langle e \rangle \cong G$ is abelian.

☞ **Solution** Since $S_3 \triangleright \langle (1 2 3) \rangle$, and

$$(1 2) \langle (1 2 3) \rangle = \{(1 2), (1 3), (2 3)\}$$

$$\langle (1 2 3) \rangle (1 2) = \{(1 2), (2 3), (1 3)\}$$

Theorem 3.17

Let K be a field extension of F . If $\text{char } K \nmid n$ and K contains a primitive n -th root of unity, then

1. For $a \in K$, let $F = K(\sqrt[n]{a})$. The extension F/K is cyclic of degree d , a divisor of n .
2. Conversely, if F/K is a cyclic extension of degree n , then $F = K(\sqrt[n]{a})$ for some $a \in K$.

Proof. 1. The statement hold trivially when $a = 0$. So we further assume that $a \neq 0$. Because $K \subset F$ contains a primitive n -th root of unity, F is the splitting field of $x^n - a$ over K . Since $\text{char } K \nmid n$, there are n distinct n -th roots of unity, so the polynomial $x^n - a$ must have n number of roots $\sqrt[n]{a}\xi^i$ for all $i = 0, 1, \dots, n-1$, where ξ is a primitive n -th root of unity in K . Therefore $x^n - a$ is separable and F/K is Galois extension.

Consider each σ in $\text{Gal}_F K$ is completely determined by $\sigma(\sqrt[n]{a})$, which must equal to $\sqrt[n]{a}\xi^{i_\sigma}$. Consider the map

$$\text{Gal}_F K \rightarrow \mathbb{Z}_n$$

$$\sigma \mapsto i_\sigma$$

Clearly, this map is injective homomorphism, and it is easy to check

$$\tau\sigma(\sqrt[n]{a}) = \tau(\sqrt[n]{a}\xi^{i_\sigma}) = \sqrt[n]{a}\xi^{i_\sigma}\xi^{i_\tau} = \sqrt[n]{a}\xi^{i_\sigma+i_\tau}.$$

2. Let $\text{Gal}_F K = \langle \sigma \rangle$ be cyclic group of order n . For $\alpha \in F$ and ξ a primitive n -th root of unity, define the *Lagrange resolvent* by

$$P(\alpha, \xi) := \alpha + \xi\sigma(\alpha) + \xi^2\sigma^2(\alpha) + \dots + \xi^{n-1}\sigma^{n-1}(\alpha).$$

By corollary, $\{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ are linearly independent over F . So we have

$$1 + \xi\sigma + \xi^2\sigma^2 + \dots + \xi^{n-1}\sigma^{n-1} \neq 0 \quad (3.7)$$

so there is $\alpha \in F$ such that $P(\alpha, \xi) \neq 0$. Now let $\rho := P(\alpha, \xi)$. Since $\xi \in K$, we have $\sigma(\rho) = \xi^{-1}\rho$, and that

$$\sigma(\rho^n) = \xi^{-n}\rho^N = \rho^n.$$

So $\rho^n \in F_{\langle \sigma \rangle} = K$. Moreover,

$$\sigma^i(\rho) = \xi^{-i}\rho \neq \rho \quad \forall i = 0, 1, \dots, n-1.$$

Thus $\sigma^i \notin \text{Aut}_{K(\rho)} F$. i.e. $|\text{Aut}_{K(\rho)} F| = 1$. Therefore it deduce to

$$F = K(\rho) = K(\sqrt[n]{a}),$$

where $a = \rho^n \in K$.

$$\begin{array}{c} F \\ | \\ K(\rho) \\ | \\ K \end{array}$$

□

Theorem 3.18

For $n \geq 5$ the group S_n is not solvable.

Proof. For the sake of contradiction, suppose that S_n is solvable and that

$$S_n = G_0 \supseteq G_1 \supseteq \dots \supseteq G_t = \langle 1 \rangle.$$

Let $(r s t)$ be any 3-cycle in S_n and let α, β be any element of $\{1, 2, \dots, n\}$ other than r, s, t (they always exist since $n \geq 5$). Since S_n/G_1 is abelian, by theorem of dihedral group,

$$\begin{aligned} (t \alpha s)(s r \beta)(t \alpha s)^{-1}(s r \beta)^{-1} &= (t \alpha s)(s r \beta)(t s \alpha)(s \beta r) \\ &= (r s t) \in G_1 \end{aligned}$$

Note that the cycle $\langle(r s t)\rangle \subseteq G_1$, and G_1 definitely contains all the 3-cycles since G_1/G_2 is abelian, repeating upper process, G_2 also contains $\langle(r s t)\rangle$.

In conclusion, $\forall i \in \{1, 2, \dots, n\}$, G_i contains all the 3-cycles. This contradicting the fact that S_n is solvable. \square

Theorem 3.19

Every homomorphic image of a solvable group G is solvable.

Proof. Let G be a solvable group. Then there exists a chain of groups

$$G = G_0 \supseteq G_1 \dots \supseteq G_n = \langle e \rangle$$

such that for all i , $G_{i-1} \triangleright G_i$ and G_{i-1}/G_i is abelian.

Consider f is the homomorphism of G . Then $f(G_i)$ is also a group, and the chain of group is now

$$f(G) = f(G_0) \supseteq f(G_1) \dots \supseteq f(G_n) = \langle e \rangle$$

and $aba^{-1}b^{-1} \in G_i$ whenever a, b in G_{i-1} . This implies

$$f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} \in f(G_i) \quad \forall a, b \in G_{i-1}$$

and

$$\forall c, d \in f(G_{i-1}), \exists a, b \in G_{i-1} \quad \text{s.t. } f(a) = c \text{ and } f(b) = d.$$

So we have

$$f(a)f(b)f(a)^{-1}f(b)^{-1} = cdc^{-1}d^{-1} \in f(G_i).$$

Therefore $f(G_{i-1})/f(G_i)$ is abelian. Hence $f(G)$ is solvable group. \square

Definition 3.12

A generator of this cyclic group of n -th roots of unity in K is called a primitive n -th root of unity.

This definition states that ζ is a primitive n -th roots of unity iff $\zeta, \zeta^2, \dots, \zeta^n$ are the n distinct n -th roots of unity.

Example 3.5.4. Consider $x^4 - 1 \in \mathbb{Q}[x]$. The 4-th roots of unity in $\mathbb{C} = \{1, -1, i, -i\} = \langle i \rangle$. i and $-i$ are primitive 4-th root of unity in \mathbb{C} .

Example 3.5.5. According to De Moivre's theorem,

$$\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

is a primitive n -th root of unity in \mathbb{C} .

Theorem 3.20

Every homomorphic image of a solvable group G is solvable.

Proof. Let G be a solvable group. Then there exists a chain of groups

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \langle e \rangle$$

such that $G_{i-1} \triangleright G_i$ and G_{i-1}/G_i is abelian $\forall i$.

Let f be the homomorphism of G , then $f(G_i)$ is also a group. The chain of group is now

$$f(G) = f(G_0) \supseteq f(G_1) \supseteq \dots \supseteq f(G_n) = \langle e \rangle$$

and $\forall a, b \in G_{i-1}$, we have $aba^{-1}b^{-1} \in G_i$. And

$$f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} \in f(G_i).$$

And for all c, d in $f(G_i)$, there exists some $a, b \in G_i$ such that $f(a) = c$ and $f(b) = d$. So

$$f(a)f(b)f(a)^{-1}f(b)^{-1} = cdc^{-1}d^{-1} \in f(G_i).$$

Thus $f(G_{i-1})/f(G_i)$ is abelian. Thus $f(G)$ is solvable group. \square

Lemma 3.4

Let F be a field and ζ a primitive n -th root of unity of F . Then F contains a primitive d -th root of unity for every positive divisor d of n .

Proof. Because ζ is a primitive n -th root of unity of F , that is, $\zeta^n = 1_F$. If ζ has order n and $n = dk$, ζ^k has order d .

Note that $\{\zeta^k, \zeta^{2k}, \dots, \zeta^{nk}\}$ are all distinct and roots of $x^d - 1_F$. Thus ζ^k is a primitive d -th root of unity. \square

☞ **Example 3.5.6.** There is no formula (involving only field operations and extraction of roots) for the solution of all 5th-degree polynomial equations.

☞ **Solution** Consider $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$. We check the zeros of the derivatives.

$$f'(x) = \frac{d}{dx}(2x^5 - 10x + 5) = 10x^4 - 10 \implies \text{roots are } \pm 1, \pm i$$

$$f''(x) = \frac{d^2}{dx^2}(2x^5 - 10x + 5) = 40x^3 \implies \text{the only root is } 0.$$

Note that by Eisenstein's criterion, $5|10$, $5|4$, but $5 \nmid 2$ and $5^2 \nmid 5$. So $f(x)$ is irreducible in $\mathbb{Q}[x]$.

If K is splitting field of $f(x)$ in \mathbb{C} . Then

$$|\text{Gal}_{\mathbb{Q}} K| = [K : \mathbb{Q}]$$

Since K is Galois field of \mathbb{Q} .

If r is any root of $f(x)$, then

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(r)] \cdot [\mathbb{Q}(r) : \mathbb{Q}] = 5 [K : \mathbb{Q}(r)].$$

Thus $|K : \mathbb{Q}|$ is divisible by 5. By Cauchy's theorem, there exists $\sigma \in \text{Gal}_{\mathbb{Q}} K$ with $\text{ord}(\sigma) = 5$. Note that $\text{Gal}_{\mathbb{Q}} K \subseteq S_5$ and the only elements of order 5 are (5-cycles), the 5-cycle is in $\text{Gal}_{\mathbb{Q}} K$.

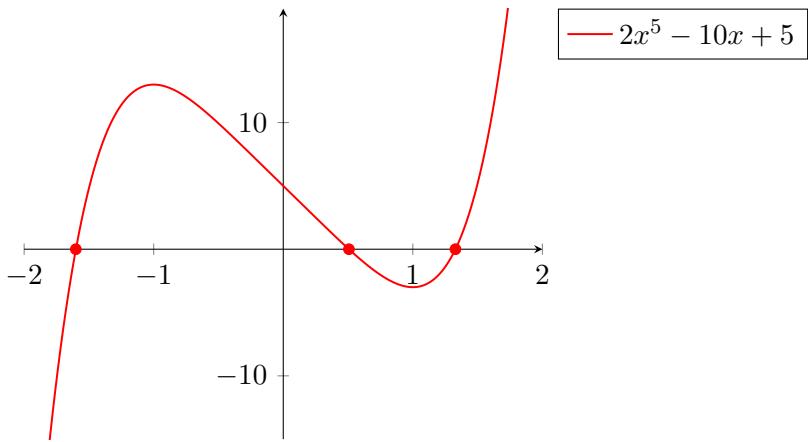


Figure 3.1: By graph, $f(x) = 2x^5 - 10x + 5$ has 3 real roots.

The complex conjugation $a + bi \mapsto a - bi$ induces an automorphism on K since $\sigma \in \text{Gal}_{\mathbb{Q}} \mathbb{C}, \sigma|_K \in \text{Gal}_{\mathbb{Q}} K$.

Since $\sigma|_K$ interchanges the two nonreal roots of $f(x)$, implies that $\text{Gal}_{\mathbb{Q}} K$ contains a transposition (2-cycle). Note that the only subgroup of S_5 that contains both a 5-cycle and a transposition is S_5 itself. So $\text{Gal}_{\mathbb{Q}} K = S_5 \implies f(x)$ is not solvable by radicals. ◀

Tutorials

Exercise 3.5.1 Let F be a field and F^* be its multiplication group. Show that the abelian groups $(F, +)$ and (F^*, \cdot) are not isomorphic.

Exercise 3.5.2 Let F be a finite field. Show that the product of all the nonzero elements of F is -1 .

Exercise 3.5.3 Show that any two finite fields of the same order are isomorphic.

Exercise 3.5.4

1. Prove that a finite integral domain is a field.
2. Prove that if R is an integral domain that is finite dimensional over a subfield $F \subseteq R$, then R is a field.

Exercise 3.5.5 Let F be a field extension of the rational numbers.

1. Show that $\{a + b\sqrt{2} \mid a, b \in F\}$ is a field.
2. Give necessary and sufficient conditions for $\{a + b\sqrt[3]{2} \mid a, b \in F\}$ to be a field.

Exercise 3.5.6 Let

$$f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Q}[x]$$

be an irreducible polynomial of degree greater than 1, in which all roots lie on the unit circle of \mathbb{C} . Show that $a_i = a_{n-i}$ for all i .

Exercise 3.5.7 Find the minimal polynomial of $\alpha = \sqrt{3 + 2\sqrt{2}}$ over the field \mathbb{Q} of rational numbers.

Exercise 3.5.8 Find the minimal polynomial of $\alpha = \sqrt[3]{2 + \sqrt{2}}$ over the field \mathbb{Q} of rational numbers.

Exercise 3.5.9 Let p be a prime, and $f(x) \in \mathbb{Z}_p[x]$ be irreducible polynomial of degree m . Show that $f(x)|(x^{p^m} - x)$ if and only if $m|n$.

Exercise 3.5.10 Let p and q be distinct primes. Show that \sqrt{q} is not an element of $\mathbb{Q}(\sqrt{p})$.

Exercise 3.5.11 Determine the Galois group of $x^4 - 3$ over the field \mathbb{Q} .

Exercise 3.5.12 Determine the Galois group of $x^3 + 3x^2 - 1$ over the field \mathbb{Q} .

[Hint]: The discriminant for general cubic equation $ax^3 + bx^2 + cx + d = 0$ is

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Exercise 3.5.13 Let $f(x) = x^4 + x^3 + 4x - 1 \in \mathbb{Z}_5[x]$. Find the Galois group of the splitting field of f over \mathbb{Z}_5 .

Exercise 3.5.14 Let K be a Galois extension of the field F with Galois group G . Let $g(x)$ be a monic polynomial over F that splits over K (that is, K contains a splitting field for $g(x)$ over F) and let $\Gamma \subseteq K$ be the set of roots of $g(x)$. Show that $g(x)$ is a power of a polynomial that is irreducible over F if and only if G is transitive on Γ .

Exercise 3.5.15 Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 with exactly two real roots. Show that the Galois group of f over \mathbb{Q} is either S_4 or the dihedral group of order 8.

Exercise 3.5.16 Show that the multiplicative group of a finite field must be cyclic.

Exercise 3.5.17 Show that every finite extension of a finite field is a Galois extension.

Exercise 3.5.18 Let E be an extension field of a field F and let $\alpha \in E$ be transcendental over F . Show that every element of $F(\alpha)$ is not in F is also transcendental over F .

Exercise 3.5.19 Let F be a finite field of characteristic p . Show that every element of F is algebraic over the prime field $\mathbb{Z}_p \leq F$.

This page intentionally left blank.

Modules and Vector Spaces

Modules are essentially the equivalent of vector spaces when the scalars come from a ring rather than a field. Throughout this notes we will consider only modules over Euclidean domains.

Axiom 4.1 Modules

Let R be a ring. A left R -module M consists of an abelian group $(M, +)$, together with scalar multiplication $\cdot : R \times M \mapsto M$ such that

- $r(m_1 + m_2) = rm_1 + rm_2, \quad \forall r \in R \text{ and } m_1, m_2 \in M.$
- $(r_1 + r_2)m = r_1m + r_2m, \quad \forall r_1, r_2 \in R \text{ and } m \in M.$
- $(r_1r_2)m = r_1(r_2m), \quad \forall r_1, r_2 \in R \text{ and } m \in M.$
- $1_R \cdot m = m, \quad \forall m \in M.$

If R is a field, then the R -module is called a **vector space** over R .

Definition 4.1 Vector Space (defn. from linear algebra)

A **vector space** is a nonempty set V of objects, known as *vectors*, on which are defined by two operations: *addition* and *scalar multiplication* in \mathbb{R}^n . The properties of modules must hold for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$; and for all $c, d \in \mathbb{R}^n$.

- $\mathbf{u}, \mathbf{v} \in V.$
- $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w}).$
- $c\mathbf{u} \in V.$
- $(cd)\mathbf{u} = c(d\mathbf{u}).$
- $1\mathbf{u} = \mathbf{u}.$

Definition 4.2

Let R be a ring, and let M be an R -module.

1. We say that elements $x_1, \dots, x_n \in M$ are **linearly independent** if the only way to express the zero element as a linear combination of these elements is with all coefficients equal to zero.
2. We say that elements $x_1, \dots, x_n \in M$ are a **basis** for R -module M if they are linearly independent and generate M .
3. We say that element x_1, \dots, x_n of an R -module M **generate** or **span** M if every element

of M can be expressed as a linear combination of x_1, \dots, x_n . That is,

$$\bar{x} = \text{Span}\{x_1, \dots, x_n\} = r_1x_1 + r_2x_2 + \dots + r_nx_n \quad (4.1)$$

for some $r_1, r_2, \dots, r_n \in R$.

Theorem 4.1

A submodule of a free module is free.

Proof. Let R be a PID. Suppose $P = \bigoplus_{j \in J} R_j$ be a free R -module with basis J , and suppose $M \subset P$ is a submodule.

Construct a well-ordering of the set J . $\forall j \in J$, we set $P_j := \bigoplus_{i \leq j} R_i$ and \bar{R}_i , so that $P_j = \bar{P}_j \oplus R$.

Let ϕ_i be the composite

$$P_i \cap M \hookrightarrow P_j = \bar{P}_j \oplus R \rightsquigarrow R. \quad (4.2)$$

The $\text{Ker } \phi_i = \bar{P}_j \cap M$, and $\text{Im } \phi_i \subset R$ is an ideal. Hence let

$$\text{Im } \phi_i = (\lambda_j) \quad \text{for some } \lambda_j \in R.$$

Pick some $c_j \in P_i \cap M$ such that $\phi(c_j) = \lambda_j$. Let

$$J' = \{j \in J \mid \lambda_j \neq 0\}. \quad (4.3)$$

To complete the proof.

[Claim]: $\{c_j\}_{j \in J'}$ is a basis.

Suppose that $\{c_j\}_{j \in J'}$ is linearly independent.

$$\sum_{k=1}^n a_k c_{j_k} = 0 \quad (4.4)$$

□

Bibliography

- [1] Fraleigh.J.B (2003) *A First Course in Abstract Algebra*, Addison-Wesley Professional, USA, 7th ed.
- [2] Rotman, J.J (2005) *A First Course in Abstract Algebra*, Prentice-Hall, New Jersey, 3rd ed.
- [3] James S. Milne (2020) *Algebraic Number Theory*, www.jmilne.org/math/, v3.08 ed.

Answers for selected questions

Answer of exercise 1.12.1

1. Yes
2. Yes
3. No, because $-1, 2 \in \mathbb{R}^*$ but $\sqrt{-1 \times 2} \notin \mathbb{R}^*$.
4. No, because there is no inverse.

Answer of exercise 1.12.6

$$\begin{aligned} a * b * c &= e \\ \Rightarrow a^{-1} * a * b * c &= a^{-1} * e \\ \Rightarrow e * b * c &= a^{-1} \\ \Rightarrow b * c * a &= a^{-1} * a \\ \Rightarrow b * c * a &= e \end{aligned}$$

Answer of exercise 1.12.7

For all a, b in G , since every element is its own inverse in G . Hence

$$\begin{aligned} ab = (ab)^{-1} &\implies ab = b^{-1}a^{-1} && \text{socks-shoes theorem} \\ &\implies ab = ba && \text{since } a = a^{-1} \text{ and } b = b^{-1} \end{aligned}$$

Answer of exercise 1.12.27

Check that $\phi(x + y) = \phi(x)\phi(y)$.

$$\phi(x + y) = 5^{x+y} = 5^x \cdot 5^y = \phi(x)\phi(y)$$

which preserves the group operation.

1. (One-to-one) Suppose $\phi(x) = \phi(y)$,

$$\begin{aligned} \phi(x) = \phi(y) &\Rightarrow 5^x = 5^y \\ &\Rightarrow \log_5 5^x = \log_5 5^y \\ &\Rightarrow x = y. \end{aligned}$$

2. (Onto) For all $x, y \in G$, we have

$$\phi(x) = y \Rightarrow 5^x = y \Rightarrow x = \log_5 y. \forall y > 0$$

Thus, ϕ is a homomorphism. The kernel of ϕ is

$$\begin{aligned} \ker(\phi) &= \{x \in G \mid \phi(x) = 1\} \\ &= \{x \in G \mid 5^x = 1\} \\ &= \{x \in G \mid x = \log_5 1 = 0\} \\ &= \{0\} \end{aligned}$$

Answer of exercise 1.12.32

Since ϕ is a homomorphism, then for all $n \in \mathbb{Z}_{10}$, we have

$$\phi(n) = \phi(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}) = n \cdot \phi(1) = 8n \mod 20.$$

Thus,

$$\begin{aligned} \ker(\phi) &= \{n \in \mathbb{Z}_{10} \mid \phi(n) = 0\} \\ &= \{n \in \mathbb{Z}_{10} \mid 8n \equiv 0 \mod 20\} \\ &= \{n \in \mathbb{Z}_{10} \mid n = 0, 5\} \\ &= \{0, 5\} \end{aligned}$$

Answer of exercise 1.12.36

The dihedral group of order 8 is

$$D_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

The members of a conjugacy class of D_8 are different but have the same type of effect on a 2D square: r and r^3 are a 90 degree rotation in clockwise and counter-clockwise respectively; s and sr^2 are reflections across a diagonal; and sr and sr^3 are reflections across an edge bisector.

$$\{e\}\{r, r^3\}, \{r^2\}, \{s, sr^2\}, \{sr, sr^3\}.$$

Answer of exercise 1.12.37

Suppose N is a normal subgroup of S_4 . Since $|S_4| = 24$, then by Lagrange's theorem, the possible orders of N are 1, 2, 3, 4, 6, 8, 12, 24. If $|N| = 1$, then $N = \{e\}$. And If $|N| = 24$, then $N = S_4$.

Now suppose $1 < |N| < 24$. We know that N is a union of conjugacy classes including $Cl(e)$. The conjugacy classes, as described as above, have size 1, 6, 8, 6 and 3 respectively. It is possible to have $|N| = 2, 3$. Thus $|N|$ is even.

Since $Cl(e) \subseteq N$, we must also have $Cl((12)(34)) \subseteq N$ in order to have $|N|$ be even. Notice that

$$H = Cl(e) \cup Cl((1\ 2)(3\ 4)) \leq S_4.$$

Therefore, H is a normal subgroup of S_4 .

If N includes one of the conjugacy classes of size 6, then $|N|$ cannot be a proper divisor of 24, as it would have to be

$$1 + 3 + 6 = 10, \quad 1 + 3 + 6 + 8 = 18, \quad 1 + 3 + 6 + 6 = 16.$$

It is possible for N to contain the conjugacy class of size 8 because $1 + 3 + 8 = 12$. In fact,

$$A_4 = Cl(e) \cup Cl((1\ 2\ 3)) \cup Cl((1\ 2)(3\ 4))$$

is a normal subgroup of S_4 with order 12.

Answer of exercise 1.12.39

For the sake of contradiction, suppose G is non-abelian group of order p^2 , then $Z(G) < G$; Since $Z(G)$ is nontrivial ($Z(G) \neq \{e\}$), then $|Z(G)| = p$. By Lagrange's theorem, $|G/Z(G)| = p^2/p = p$. Since $G/Z(G)$ is of prime order, then $G/Z(G)$ is cyclic. By theorem, if $G/Z(G)$ is cyclic, then G is abelian. This contradicts our assumption that G is non-abelian. Therefore, G is abelian.

Answer of exercise 1.12.43

Let $H \cap K = M$. We want to show M is a subgroup of G . Applying one-step subgroup test:

1. Since H and K are subgroups of G , then $e \in H$ and $e \in K$. Thus, $e \in M$. M is nonempty set.
2. Let $a, b \in M$. Then $a, b \in H$ and $a, b \in K$. Since H and K are subgroups of G , then $ab^{-1} \in H$ and $ab^{-1} \in K$. Therefore, $ab^{-1} \in M$.

Therefore, by one-step subgroup test, $M \leq G$.

Answer of exercise 2.9.6

(\Rightarrow) Assume that $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$. Then

$$\begin{aligned} a^2 - b^2 &= (a + b)(a - b) \\ \Rightarrow a^2 - b^2 &= a^2 - ab + ba - b^2 \\ \Rightarrow 0_R &= -ab + ba \\ \Rightarrow ab &= ba. \end{aligned}$$

then R is commutative.

(\Leftarrow) On the other hand, assume that R is commutative. We start from simplifying the right hand side:

$$\begin{aligned} (a + b)(a - b) &= aa - ab + ba - bb \\ &= a^2 - ab + ab - b^2 && \text{Since } ba = ab \\ &= a^2 + (-ab + ab) - b^2 \\ &= a^2 + 0_R - b^2 \\ &= a^2 - b^2. \end{aligned}$$

which is what we desired.

Answer of exercise 2.9.7

1. Since $x \cdot x = x$, this implies that $(x + 1_R) \cdot (x + 1_R) = x + 1_R$. Continue expand the

left-hand side:

$$\begin{aligned}
 (x + 1_R) \cdot (x + 1_R) &= x + 1_R \\
 \Rightarrow x^2 + 2x + 1_R &= x + 1_R \\
 \Rightarrow x^2 &= x + 1_R - 2x - 1_R \\
 \Rightarrow x^2 &= -x + 0_R \\
 \Rightarrow \boxed{x^2 = -x}.
 \end{aligned}$$

Since $x^2 = x$, then from the result above we have $x = -x$.

2. For all $a, b \in R$,

$$\begin{aligned}
 (ab)(ab) &= ab \\
 \Rightarrow abab &= (aa)(bb) \\
 \Rightarrow \cancel{abab} &= \cancel{aabb} \\
 \Rightarrow ba &= ab.
 \end{aligned}$$

Thus R is commutative.

Answer of exercise 2.9.12

Let F be a field, and let $I \subset F$ be an ideal. Assume $I \neq \{0\}$, and find $x \neq 0 \in I$. Since F is a field, x is invertible; Since I is an ideal, $1 = x^{-1} \cdot x \in I$. Therefore $I = F$.

Answer of exercise 2.9.15

To show that $A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{Z})$, we need to find a nonzero matrix B such that $AB = 0$. Notice that $\det A = 0$ and is not invertible. We can try to find B (one of the possible matrices) using eigenvalues and eigenvectors.

Solve the equation $\det(A - \lambda I) = 0$:

$$\begin{aligned}
 \det \begin{bmatrix} 1 - \lambda & 2 \\ 2 & 4 - \lambda \end{bmatrix} = 0 &\implies (1 - \lambda)(4 - \lambda) - 4 = 0 \\
 &\implies \lambda^2 - 5\lambda = 0
 \end{aligned}$$

On solving, we get $\lambda_1 = 0$ and $\lambda_2 = 5$. Note that we only need to find the eigenvector corresponding to $\lambda_1 = 0$ for this case, and solve

$$\begin{bmatrix} 1 - 0 & 2 \\ 2 & 4 - 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Setting x_2 as a free variable, we get $x_1 = -2x_2$. Thus one of the eigenvectors is

$$\vec{v}_1 = \begin{bmatrix} -2 \\ 1 \end{bmatrix}.$$

Now, let \vec{v}_1 to be the first and second columns of matrix B , said $B = \begin{bmatrix} -2 & -2 \\ 1 & 1 \end{bmatrix}$. Then $AB = 0$. Therefore, A is a zero divisor in $M_2(\mathbb{Z})$.

Answer of exercise 2.9.20

If A and B are coprime, this implies that we can find $a \in A$ and $b \in B$ such that $a + b = 1$. Now if $x \in A \cap B$ we can also have

$$x = 1x = (a + b)x = ax + bx.$$

Since $x \in B$, we have $ax \in AB$; and since $x \in A$, we have $bx \in AB$. It follows that $x \in AB$.

Answer of exercise 2.9.23

Compute $x^4 + 4$ for $x = 0, 1, 2, 3, 4$ in \mathbb{Z}_5 :

x	0	1	2	3	4
$x^4 + 4 \pmod{5}$	4	0	0	0	0

The zeros are 1, 2, 3, 4. Thus the factorization is

$$x^4 + 4 = (x - 1)(x - 2)(x - 3)(x - 4).$$

Answer of exercise 2.9.24

Compute $x^3 + 2x^2 + 2x + 1$ for $x = 0, \dots, 6$ in \mathbb{Z}_7 :

x	0	1	2	3	4	5	6
$x^3 + 2x^2 + 2x + 1 \pmod{7}$	1	6	0	3	0	4	0

The zeros are 2, 4, 6. Thus the factorization is

$$x^3 + 2x^2 + 2x + 1 = (x - 2)(x - 4)(x - 6).$$

Answer of exercise 2.9.27

Consider ring $R = \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ with norm

$$N(a + b\sqrt{3}) = |a^2 - 3b^2|.$$

To show $\mathbb{Z}[\sqrt{3}]$ is Euclidean domain. We need to find a division algorithm in $\mathbb{Z}[\sqrt{3}]$. For all $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ with $\beta \neq 0$, $\exists q, r \in \mathbb{Z}[\sqrt{3}]$ such that

$$\alpha = q\beta + r, \quad N(r) < N(\beta).$$

Intuition: Construct the quotient and remainder in $\mathbb{Z}[\sqrt{3}]$.

Consider the division $\frac{\alpha}{\beta}$ in the field $\mathbb{Q}[\sqrt{3}]$. Let

$$\frac{\alpha}{\beta} = x + y\sqrt{3}, \quad \text{where } x, y \in \mathbb{Q}.$$

Our goal is to find integers p, q that are closest to x, y respectively, such that $|x - p| \leq \frac{1}{2}$ and $|y - q| \leq \frac{1}{2}$.

Let $\mathfrak{Q} = p + q\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ to be our proposed quotient. Define the remainder

$$\gamma = \alpha - \mathfrak{Q}\beta \in \mathbb{Z}[\sqrt{3}].$$

We want to show $N(\gamma) < N(\beta)$ or $N(\gamma) = 0$. Compute

$$\begin{aligned}\gamma &= \alpha - \mathfrak{Q}\beta \\ &= \alpha - (p + q\sqrt{3})\beta \\ &= \beta \left(\frac{\alpha}{\beta} - (p + q\sqrt{3}) \right) \\ &= \beta[(x - p) + (y - q)\sqrt{3}]\end{aligned}$$

Using the norm property $N(uv) = N(u)N(v)$, we have

$$N(\gamma) = N(\beta)N\left((x - p) + (y - q)\sqrt{3}\right)$$

and

$$N\left((x - p) + (y - q)\sqrt{3}\right) = |(x - p)^2 - 3(y - q)^2|.$$

Since $|x - p| \leq \frac{1}{2}$ and $|y - q| \leq \frac{1}{2}$, we have

$$\begin{aligned}|(x - p)^2 - 3(y - q)^2| &\leq \max\{(x - p)^2, 3(y - q)^2\} \\ &\leq \max\left\{\frac{1}{4}, \frac{3}{4}\right\} = \frac{3}{4}.\end{aligned}$$

Thus, $N(\gamma) \leq \frac{3}{4}N(\beta) < \beta$.

Answer of exercise 3.5.3

[Claim]: Any finite field F with p^n elements is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p[x]$.

Let F be a finite field with p^n elements. Consider $F \setminus \{0\}$, the set of all nonzero elements of F . Since F is a finite field, $F \setminus \{0\}$ form a multiplicative group of order $p^n - 1$. It follows that F coincides with the set of roots of the polynomial $x^{p^n} - x$. Hence, F is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$. This completes the proof of our claim.

Consequently, any two finite fields with p^n number of elements are isomorphic. This is exactly what we wanted to show.

Let E and F be two finite fields with p^n number of elements. By theorem E and F must contain subfields E_p and F_p , each also have p elements. Hence E and F are splitting fields of $x^{p^n} - x$ over E_p and F_p , respectively. Again, we have

$$E_p \cong \mathbb{Z}/\langle p \rangle, \text{ and } F_p \cong \mathbb{Z}/\langle p \rangle \implies E_p \cong F_p.$$

Hence, by uniqueness of splitting fields (up to isomorphism), it follows that E isomorphic to F . This completes the proof.

Answer of exercise 3.5.8

Let $\alpha = \sqrt[3]{2 + \sqrt{2}}$. Then

$$\alpha^3 = 2 + \sqrt{2} \implies (\alpha^3 - 2)^2 = 2 \implies \alpha^6 - 4\alpha^3 + 2 = 0.$$

So the minimal polynomial is $f(x) = x^6 - 4x^3 + 2$ over \mathbb{Q} that has α as a root.

Answer of exercise 3.5.10

We proof by contradiction. Suppose not, suppose that \sqrt{q} is an element of $\mathbb{Q}(\sqrt{p})$. Then $\mathbb{Q}(\sqrt{p})$

is the smallest subfield containing \mathbb{Q} and \sqrt{q} . Notice that every element can be expressed as $a + b\sqrt{p}$ where $a, b \in \mathbb{Q}$. So now we let

$$\sqrt{q} = a + b\sqrt{p}. \quad (\heartsuit)$$

Now squaring both sides:

$$\begin{aligned} q = (a + b\sqrt{p})^2 &\implies q = a^2 + 2ab\sqrt{p} + b^2p \\ &\implies 2ab\sqrt{p} = q - a^2 - b^2p. \end{aligned} \quad (\clubsuit)$$

Now consider three possible cases:

Case 1: If $2ab \neq 0$, then from (\clubsuit) we express \sqrt{p} in term of p, q, a, b :

$$\sqrt{p} = \frac{q - a^2 - b^2p}{2ab}$$

and \sqrt{p} is rational and this contradicts the fact that p is prime.

Case 2: If $a = 0$, then (\heartsuit) becomes $\sqrt{q} = b\sqrt{p}$. Squaring both sides gives $q = b^2p$, so

$$\frac{q}{p} = b^2, \text{ where } b \in \mathbb{Q}.$$

Because b is rational, so is b^2 . However, $\frac{q}{p}$ should be the ratio of distinct primes, which is not a perfect square of a rational. Again, this is a contradiction.

Case 3: If $b = 0$, then (\heartsuit) becomes $\sqrt{q} = a \implies q = a^2$. Since q is prime, it cannot be the square of rational numbers (Unless $a = 0$, but q is prime. So q always greater than zero). And if a is rational, $a^2 = q$ and $a = \pm\sqrt{q}$, which is absurd.

In conclusion, with all these cases, we said that $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ if p and q are coprime. This completes the proof.

Answer of exercise 3.5.11

The roots of polynomial $p(x) = x^4 - 3$ are

$$\alpha_1 = \sqrt[4]{3}, \quad \alpha_2 = -\sqrt[4]{3}, \quad \alpha_3 = i\sqrt[4]{3}, \quad \alpha_4 = -i\sqrt[4]{3}.$$

The splitting field K that generated by all the roots over \mathbb{Q} is $K = \mathbb{Q}(\sqrt[4]{3}, i)$. Now we need to determine the degree of field extension $[K : \mathbb{Q}]$.

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{3}, i) \\ \downarrow \\ \mathbb{Q}(\sqrt[4]{3}) \\ \downarrow \\ \mathbb{Q} \end{array}$$

The polynomial $x^4 - 3$ is irreducible over \mathbb{Q} by Eisenstein's criterion with $p = 3$, and $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$. and the imaginary unit i is not in the subfield $\mathbb{Q}(\sqrt[4]{3})$, so

$$[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 2.$$

The total degree of the field extension is

$$\begin{aligned}[K : \mathbb{Q}] &= [\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}(\sqrt[4]{3})] \times [\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] \\ &= 2 \times 4 \\ &= 8\end{aligned}$$

The degree of field extension is equal to the order of galois group $\text{Gal}_{\mathbb{Q}} K$. So the order of $\text{Gal}_{\mathbb{Q}} K$ is also 8.

The automorphisms of the galois group $\text{Gal}_{\mathbb{Q}} K$ is generated by $\sqrt[4]{3}$ and i . We can define two automorphisms:

$$\begin{aligned}\sigma : \sigma(\sqrt[4]{3}) &= i\sqrt[4]{3}, \quad \sigma(i) = i; \\ \rho : \rho(\sqrt[4]{3}) &= \sqrt[4]{3}, \quad \rho(i) = -i;\end{aligned}$$

Now, notice that these automorphisms satisfies $\sigma^4 = 1$, $\rho^2 = 1$, and $\rho\sigma\rho^{-1} = \sigma^3$. This is isomorphic to dihedral group of order 8, D_8 . Thus $\text{Gal}_{\mathbb{Q}} K \cong D_8$.

Answer of exercise 3.5.12

First off, we perform a basic calculus — find the derivative of polynomial $f(x) = x^3 + 3x^2 - 1$. The derivative of f is

$$f'(x) = 3x^2 + 6x, \quad \Rightarrow \text{ roots are } -2, 0.$$

Check that $f(-3) = -1 < 0$; $f(-1) = 1 > 0$; $f(1) = 3 > 0$. There is one root in \mathbb{R} , two roots in \mathbb{C} . Since there are no rational roots, f is irreducible over \mathbb{Q} .

The galois group of irreducible cubic polynomial is either A_3 or S_3 — we want determine which is it. If the discriminant of an irreducible cubic is a perfect square in \mathbb{Q} , then the galois group is cyclic with order 3 and hence isomorphic to A_3 . Otherwise the galois group is S_3 .

Check the discriminant for $f(x) = x^3 + 3x^2 - 1$:

$$\Delta = (3^2 * 0^2) - 4(1)(0)^3 - 4(3^3)(-1) - 27(-1)^2 + 18(1 * 3 * 0 * -1) = 81.$$

Since $\Delta = \sqrt{81} = 9 \in \mathbb{Q}$, so the galois group of $x^3 + 3x^2 - 1$ over \mathbb{Q} is A_3 .

Answer of exercise 3.5.16

Let F be a finite field with $|F| = q$. Consider the multiplicative group $F^* = F \setminus \{0_F\}$. So $|F^*| = q - 1$. We want to show that there exists an element $a \in F^*$ such that $\text{ord}(a) = q - 1$. We will appeal to a property of finite abelian groups: the order of every element in a finite abelian group divides the maximum order of all the elements.

Let m be the maximum order of all the elements in F^* . Since the order of every element in F^* divides m , each $a \in F^*$ satisfies $a^m = 1_F$. Thus, every element of F^* is a root of the polynomial $x^m - 1_F$. Since $x^m - 1_F$ has at most m roots in F , we have $q - 1 \leq m$. At the same time, by Lagrange's theorem, m divides $q - 1$. Thus $m = q - 1$. Hence, this implies that there exists an element $a \in F^*$ such that $\text{ord}(a) = q - 1 = |F^*|$. Therefore, F^* is cyclic.