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:

$$* : G \times G \to G.$$

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

- Abelian group: (1-5) or (6-10)
- Associative Ring: 1-6, with 11 and 12
- Semigroup: 1, 2 only
- Monoid: 1, 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 satisfies.

1. **(Closure)** $\forall a, b \in G, \quad a * b \in G.$
2. **(Associativity)** $\forall a, b, c \in G, \quad a * (b * c) = (a * b) * c \in G.$
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

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

is a non-abelian group under matrix multiplication.

Solution Check if $GL(2, \mathbb{R})$ is closure,asscoiative, 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 asscoiative.

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

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

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

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

   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 exists 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 viloates the asscoiative 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 $T_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2$ 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

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

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 $\gcd(xy, n) = \gcd(x, n)\ \gcd(y, n) = 1$.

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

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

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

◀

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

$$ea = a = ae \quad \forall a \in G. \tag{♡}$$

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

$$e'a = a = ae' \quad \forall a \in G. \tag{♣}$$

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

From (♣), 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. □

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

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

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 $be = ce \Rightarrow \boxed{b = c}$. The proof is now complete. □

Theorem 1.1 Socks-shoes property

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1} \tag{1.1}$$

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

$$\begin{aligned}
(ab)(b^{-1}\,a^{-1}) &= a(bb^{-1})a^{-1} && G \text{ is asscoiative} \\
&= aea^{-1} \\
&= aa^{-1} \\
&= \boxed{e} && \text{cancellation rule returns identity}
\end{aligned}$$

this equation states that

$$\boxed{(ab)(b^{-1}\,a^{-1}) = a(bb^{-1})a^{-1}} = e$$

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. □

Remark. *In abstract algebra, the position of inputs in binary operator is very important! The commutative property no necessary hold.* $a \circ b \neq b \circ a$. *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

$$\begin{aligned}
(a * b) * (a * b) = a * b &\Rightarrow a * (b * a) * b = (a * a) * (b * b) \\
&\Rightarrow a * (b * a) * b = a * a * b * b \\
&\Rightarrow a * (b * a) * b = a * (a * b) * b \\
&\Rightarrow \cancel{a} * (b * a) * \cancel{b} = \cancel{a} * (a * b) * \cancel{b} \\
&\Rightarrow \boxed{b * a = a * b}.
\end{aligned}$$

Thus $*$ commute and G is an abelian group. ◀

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 $\mathrm{ord}(g)$.

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. $H \neq \varnothing$,
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 $\varnothing \neq H \subseteq G$ such that for any a, b in subgroup H, we have

$$ab^{-1} \in H \tag{♡}$$

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 asscoiative 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 1.1.1. Let G be an abelian group with identity e. Then

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

is a subgroup of G.

Example 1.1.2. Let G be an abelian group under multiplication with identity e. Then

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

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

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)

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

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

If the group is abelian and is additive, then

$$\langle g \rangle = \{\underbrace{a + a + \cdots + a}_{n \text{ times}} \mid n \in \mathbb{Z}\} = \{ng \mid n \in \mathbb{Z}\} \tag{1.3}$$

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 $g \in \langle g \rangle \neq \varnothing$.
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 $n_+n_2 \in \mathbb{Z}$ 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. □

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

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

thus G is an abelian group. □

Definition 1.8 Center of group
The **center**, $Z(G)$, of a group G is a subset of elements in G that commute with every element of G, that is,

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

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 $a_1\, x = x a_1$ and $a_2\, x = x a_2$ for all $x \in G$. Proving $a_1\, a_2^{-1} \in Z(G)$ is equivalent to show

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

compute

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

which is what we desired.

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

Definition 1.9 Group centralizer
Let a be a **fixed** element of a group G. The centralizer of a in G is

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

Theorem 1.5
Let $\mathfrak{a}$ be a **fixed** element in group G. If $\mathfrak{a}$ has infinite order, then $\mathfrak{a}^i = \mathfrak{a}^j$ if and only if $i = j$. However, if $\mathfrak{a}$ has finite order, said, n, then

$$\langle \mathfrak{a} \rangle = \{e, \mathfrak{a}, \mathfrak{a}^2, \ldots, \mathfrak{a}^{n-1}\} \tag{1.6}$$

and $\mathfrak{a}^i = \mathfrak{a}^j$ if and only if $n | i - j$.

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

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

and we are done.

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

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

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

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

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

compute

$$\mathfrak{a}^k = \mathfrak{a}^{qn+r} = (\mathfrak{a}^n)^q\,\mathfrak{a}^r = e^q\mathfrak{a}^r = \mathfrak{a}^r$$

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

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

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

($\Rightarrow$) If $\mathfrak{a}^i = \mathfrak{a}^j$, 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

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

but n is the least integer such that $\mathfrak{a}^n = e$ 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

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

and we are done. □

Corollary 1.1
For any group element $\mathfrak{a}$, $\mathrm{ord}(a) = |\langle a \rangle|$.

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

Theorem 1.6
Let $\mathfrak{a}$ be an element of order n in a group and let k be a positive integer. Then

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

and

$$\operatorname{ord}(\mathfrak{a}) = \frac{n}{\gcd(n,k)}.$$

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

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

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

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

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

2. Certainly,

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

□

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

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

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

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

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 $\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$ 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	$\langle 1\rangle = \mathbb{Z}_{42}$

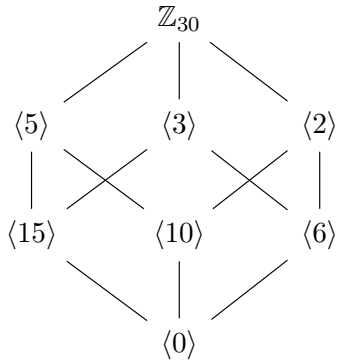
◀

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.

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

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

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

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

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

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

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. □

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.

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.

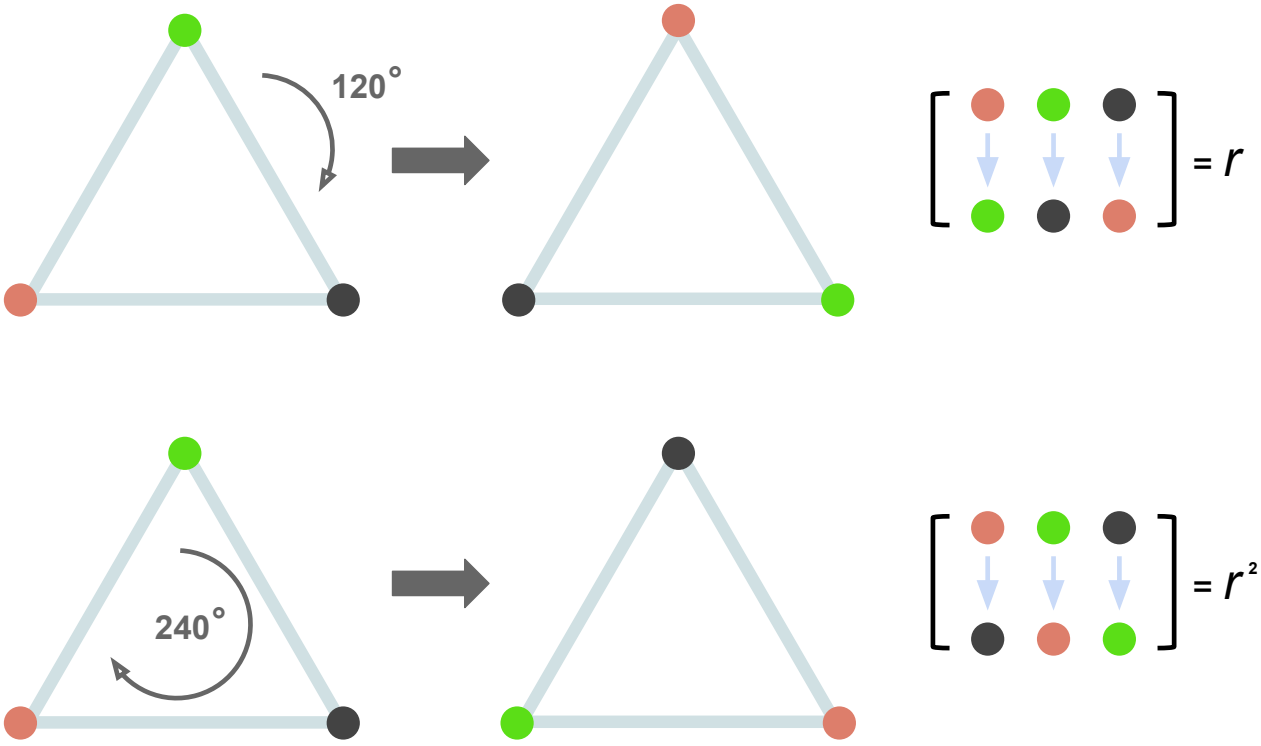
Theorem 1.9
For $n > 1$, A_n has order $n!/2$.

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_n 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.



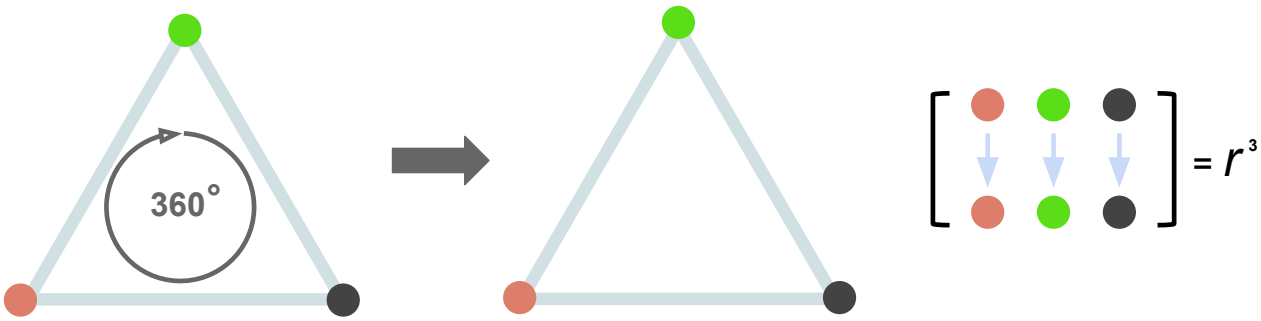


Figure 1.1: The rotation r on dihedral group D_3 with order 6. r in D_3 is described as rotating equilateral triangle 120 degree.

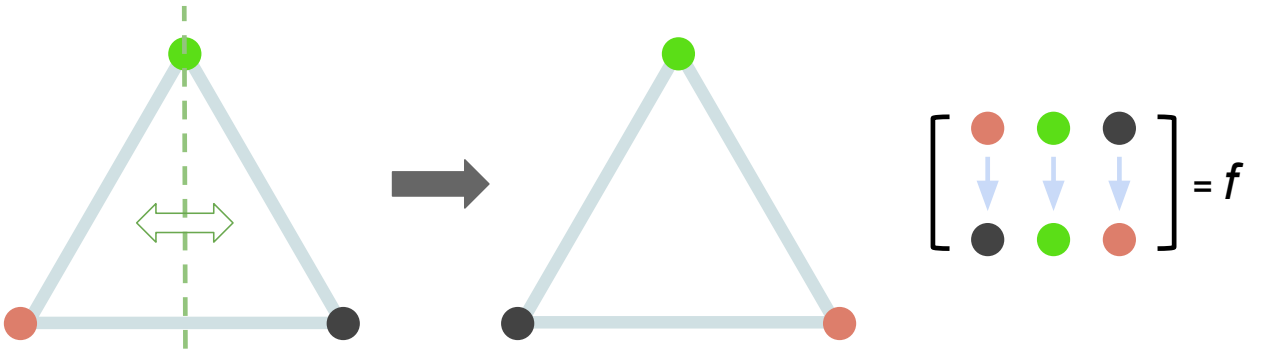


Figure 1.2: The group action f on dihedral group D_3 with order 6. f is a horizontal flip.

Theorem 1.10
Let the n-degree dihedral group

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

Then

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

Proof. 1. Compute

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

and we are done.

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

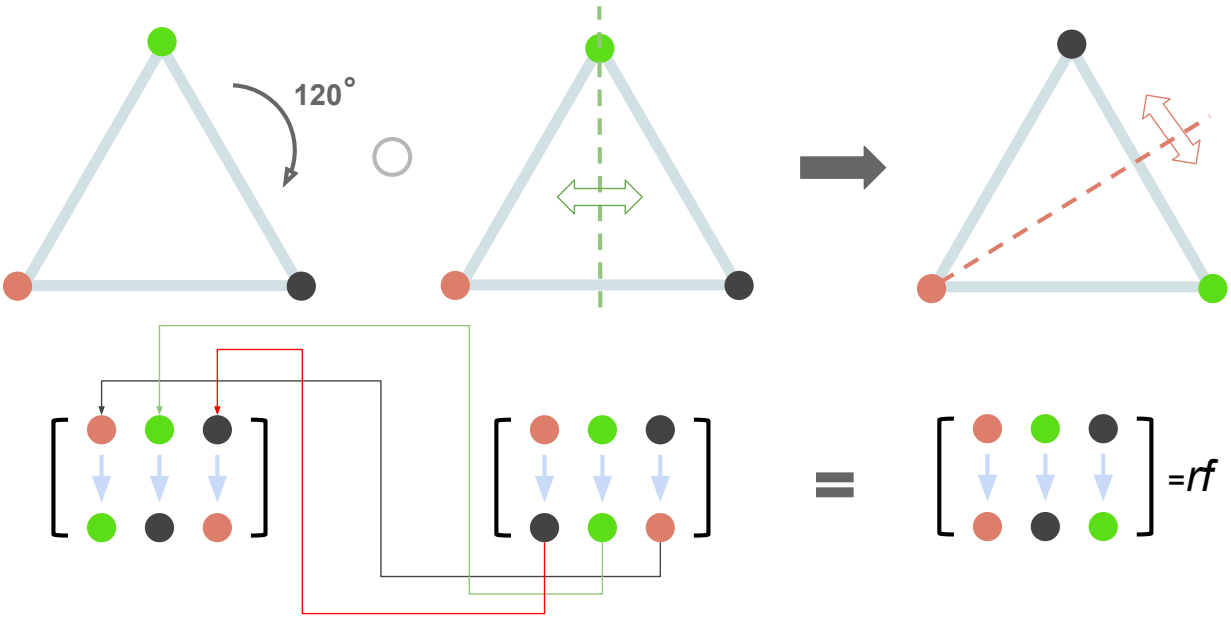


Figure 1.3: The composition of $120\,\mathrm{deg}$ rotation with horizontal reflection form another reflection line at vertice

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

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

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

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

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

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

□

Example 1.4.1. Let

$$G = SL_2(\mathbb{Z}_3) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, ad - bc \neq 0; a, b, c, d \in \mathbb{Z}_3 \right\}.$$

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 Automorphisms

Definition 1.13 Automorphisms
An isomorphism from a group G onto itself is called an automorphism.

Example 1.5.1. 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 1.5.2. 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

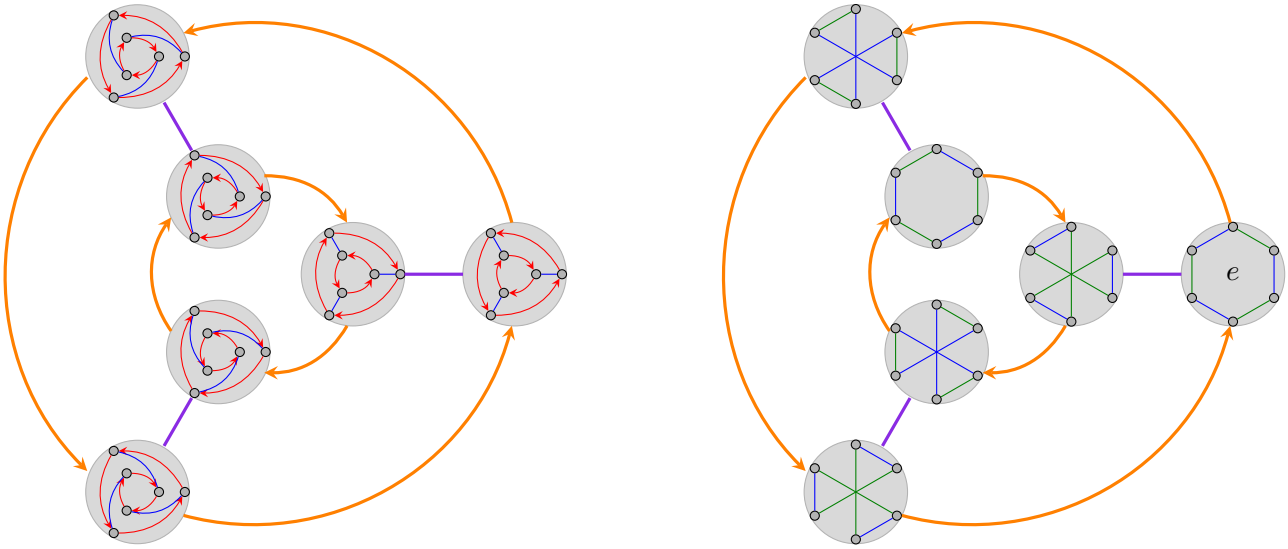
$$\begin{aligned} 1 \mapsto \alpha_1 : &\quad \mathbb{Z}_{10} \to \mathbb{Z}_{10}, \quad \alpha_1(x) = x \\ 3 \mapsto \alpha_3 : &\quad \mathbb{Z}_{10} \to \mathbb{Z}_{10}, \quad \alpha_3(x) = 3x \\ 7 \mapsto \alpha_7 : &\quad \mathbb{Z}_{10} \to \mathbb{Z}_{10}, \quad \alpha_7(x) = 7x \\ 9 \mapsto \alpha_9 : &\quad \mathbb{Z}_{10} \to \mathbb{Z}_{10}, \quad \alpha_9(x) = 9x \end{aligned}$$

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

Example 1.5.3. The automorphisms of D_3 is $\text{Aut}(D_3) = \langle \alpha, \beta \rangle \cong D_3$, where

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

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 1.14 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 1.11
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 $\phi_a \circ (\phi_b \circ \phi_c)$.

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

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

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

□

1.6 Normal subgroups, Quotient groups

1.6.1 Cosets

Definition 1.15 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 1.6.1. Consider $G = \mathbb{Z}_9 = \{0, 1, 2, \ldots, 8\} (\text{mod } 9)$. 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 $\{H, 1 +_9 H, 2 +_9 H\}$ where

$$\begin{aligned}
0 + H &= \{0 + 0, 0 + 3, 0 + 6\} \ (\text{mod } 9) = \{0, 3, 6\} = H \\
1H = 1 + H &= \{1 + 0, 1 + 3, 1 + 6\} \ (\text{mod } 9) = \{1, 4, 7\} \\
2H = 2 + H &= \{2 + 0, 2 + 3, 2 + 6\} \ (\text{mod } 9) = \{2, 5, 8\} \\
3H = 3 + H &= \{3 + 0, 3 + 3, 3 + 6\} \ (\text{mod } 9) = \{3, 6, 0\} = H
\end{aligned}$$

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.

$$\begin{aligned}
H + 0 &= \{0 + 0, 0 + 3, 0 + 6\} \ (\text{mod } 9) = \{0, 3, 6\} = H \\
H1 = H + 1 &= \{0 + 1, 3 + 1, 6 + 1\} \ (\text{mod } 9) = \{1, 4, 7\} \\
H2 = H + 2 &= \{0 + 2, 3 + 2, 6 + 2\} \ (\text{mod } 9) = \{2, 5, 8\} \\
H3 = H + 3 &= \{0 + 3, 3 + 3, 6 + 3\} \ (\text{mod } 9) = \{3, 6, 0\} = H
\end{aligned}$$

Also, we can draw Cayley 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	$1+H$

1.6.2 Normal subgroups

Definition 1.16 Normal subgroups
A subgroup H of $(G, \cdot)$ is called a normal subgroup if for all $g \in G$ we have

$$gH = Hg. \tag{1.7}$$

We shall denote that H is a subgroup of G by $H < G$, and that H is a normal subgroup of G by $H \lhd G$.
If H is a normal subgroup of G, and the order of H is equal to the order of G, we called 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 1.6.2. 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 $f \to f'$ 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 $H \lhd G$. The set G/H is defined by

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

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

Example 1.6.3. 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

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

◀

1.6.3 Quotient group

Definition 1.17 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 $gH = Hg \Longrightarrow gHg' = gg'H$ 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 asscoiative.
- The identity element is H since $H(gH) = gH$ for any g in G.

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

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

1.7 Group homomorphisms

Definition 1.18 Group homomorphisms
A group homomorphism is a map $f : (G, \diamond_G) \to (H, \bullet_H)$ 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 1.12 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 $\mathrm{ord}(g)$ is finite, then $\mathrm{ord}(\phi(g))$ divides $\mathrm{ord}(g)$.
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 1.7.1. Let G be any group and let a be any element of G. Let $\phi : \mathbb{Z} \to G$ 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,

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

◀

1.8 Isomorphism

Definition 1.19 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 $G \to G'$, 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 1.8.1. 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 $\phi : (G = \mathbb{R}, +) \to (G' = \mathbb{R}^+, \cdot)$. 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,

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

◀

Example 1.8.2. 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 $G \to G$ 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 $A_1 = A_2$.

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

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

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

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,

$$\begin{aligned}\phi_M(A_1\, A_2) &\Rightarrow MA_1\, A_2M^{-1}\\ &\Rightarrow MA_1\, I\, A_2M^{-1}\\ &\Rightarrow MA_1\, (M^{-1}M)\, A_2M^{-1}\\ &\Rightarrow (MA_1\, M^{-1})(MA_2\, M^{-1})\\ &\Rightarrow \phi_M(A_1)\phi_M(A_2).\end{aligned}$$

Therefore ϕ_M is an isomorphism. ◀

Example 1.8.3. The group $U(10)$ is not isomorphic to $U(12)$.

Theorem 1.13 Cayley's theorem
Every group is isomorphism to a group of permutation.

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

Step 1: construct permutation group $\overline{G}$

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

$$T_g(x) = gx.$$

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

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

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

2. (Associativity) For all $T_g, T_h, T_k \in \overline{G}$, 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 asscoiativity holds in $\overline{G}$.

3. (Existence of identity) For all $T_g \in \overline{G}$, there exists an $T_{g'} \in \overline{G}$ 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 $T_g \in \overline{G}$, the inverse of T_g is

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

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

Step 2: show that $\phi : G \to \overline{G}$ is isomorphism

We now define a mapping $\phi : G \to \overline{G}$, 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 $T_{g'} \in \overline{G}$, 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 1.20 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

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

Lemma 1.7
If G is a group of permutations of the set S and $s \in S$. Then $\mathrm{Stab}_G(s)$ is a subgroup of G.

Proof. Using two-step subgroup test to verify:

1. $\exists \phi : S \to S \in \mathrm{Stab}_G(s)\ s.t.\ \phi(x) = x$. Thus $\mathrm{Stab}_G(s) \neq \varnothing$.

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

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

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

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

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

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

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

Definition 1.21 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

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

Theorem 1.14 Orbit-Stabilizer theorem
For any group action $\phi : G \to \mathrm{Permutation}(S)$, and for any $s \in S$,

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

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

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

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

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

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

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

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

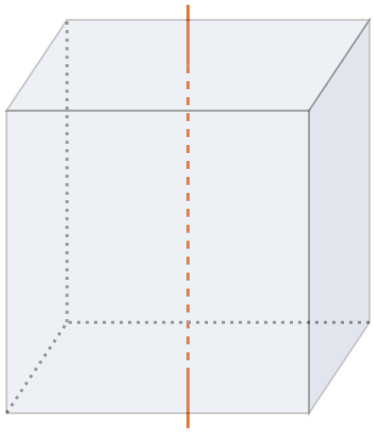
So f is both one-to-one and onto. Which means

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

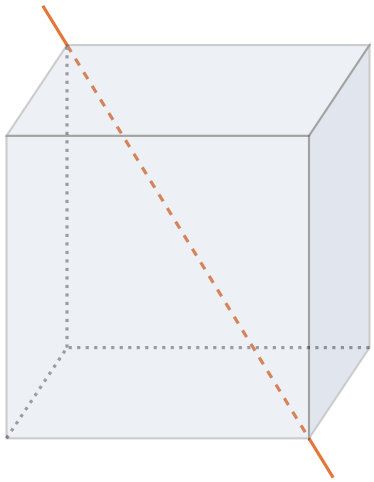
□

Theorem 1.15
The group of rotations of a cube is isomorphic to S_4.

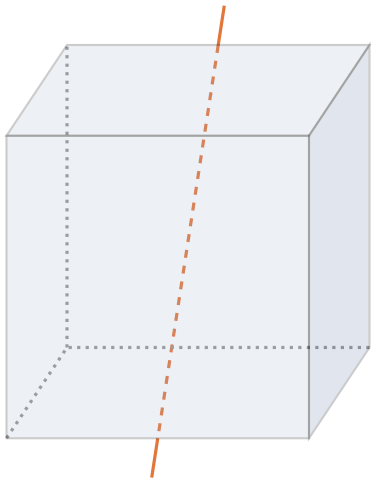
Proof. We can proof it by visualizing the rigid motions of a cube rotated along the possible axes.



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 1.16 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

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

2. Using the similar technique, we have

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

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 1.17 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 $\sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_{p^n}\} \in S$, then

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

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

$$f : \operatorname{Stab}(\sigma) \to \sigma$$

$$g \to g * \sigma_1$$

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

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

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

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

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

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

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

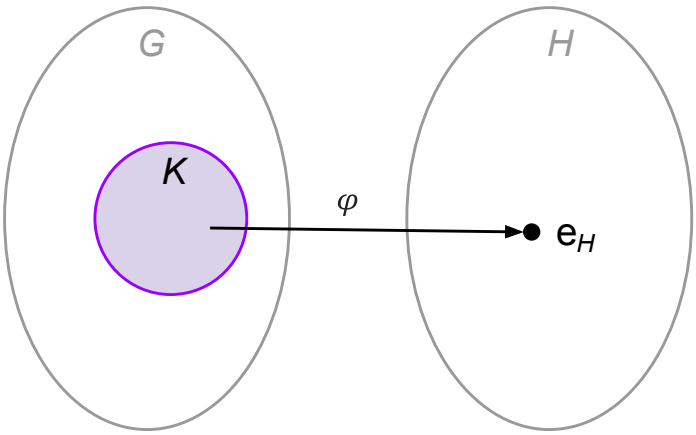
For this choice of $\sigma \in S$, $\operatorname{Stab}(\sigma)$ is thus a subgroup of size p^n. □

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.

1.8.1 Isomorphism theorems

Theorem 1.18 First Isomorphism theorem
Let $f : G \to H$ be a homomorphism of groups with kernel K. Then the quotient group G/K is isomorphic to $\operatorname{Im} f$.

Proof. Define $\varphi : G/N \to \operatorname{Im} f$ by $\varphi(K_a) = f(a)$.



1. Claim: φ is well-defined.

   Suppose that $K_a = K_b$. Then by lemma we have

   $$f(a) = f(b) \implies \varphi(K_a) = f(a) = f(b) = \varphi(K_b).$$

2. Claim: φ is surjective.

   Let $b \in Ima f$ then there exists an $a \in G$ such that $f(a) = b$. Then

   $$\varphi(K_a) = f(a) = b.$$

3. Claim: φ is injective.

   Since

   $$\varphi(K_a) = \varphi(K_b) \Leftrightarrow f(a) = f(b) \Leftrightarrow K_a = K_b.$$

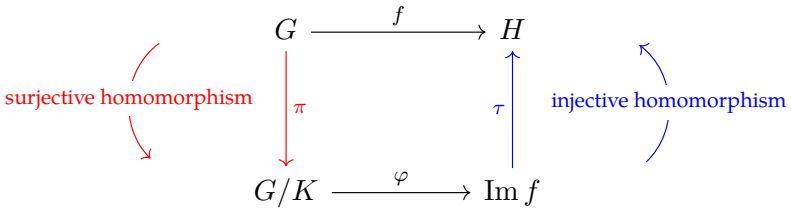
4. Claim: φ is homomorphism.

   Because

   $$\varphi(K_a K_b) = \varphi(K_{ab}) = f(ab) = f(a)f(b) = \varphi(K_a)\varphi(K_b).$$

   In all φ is an homomorphism.

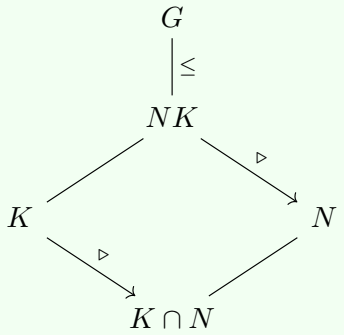
   Moreover, $\tau \circ \varphi \circ \pi(a) = \tau \circ \varphi(\pi(a)) = \tau \circ \varphi(N_a) = \tau\, f(a) = f(a)$.



□

Theorem 1.19 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

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

Thus $NK < G$.

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

   The kernel of f is

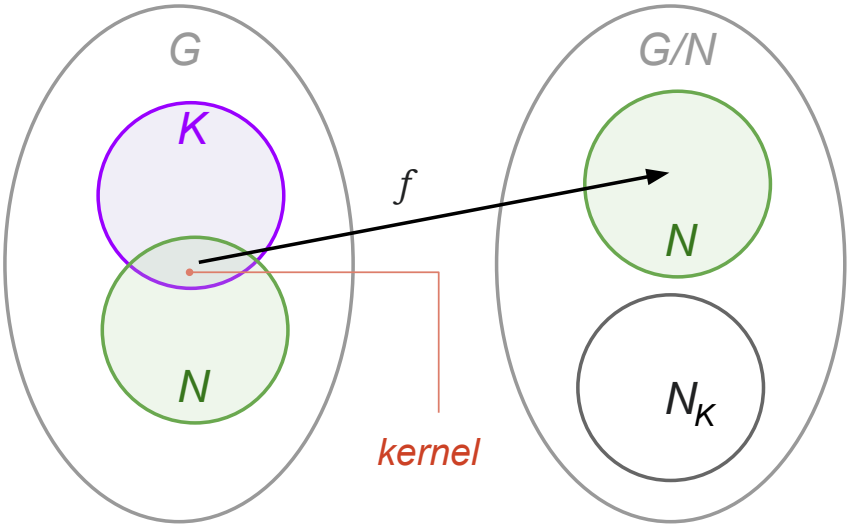
$$\begin{aligned} ker\, f &= \{k \in K \mid f(k) = Ne\} \\ &= \{k \in K \mid Nk = Ne\} \\ &= \{k \in K \mid k \in N\} \\ &= K \cap N. \end{aligned}$$

   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 1.20 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 1.21 Lagrange theorem
If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Proof. Let $a_1H, a_2H, \ldots, a_rH$ 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

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

Thus $|H|$ divides $|G|$ □

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

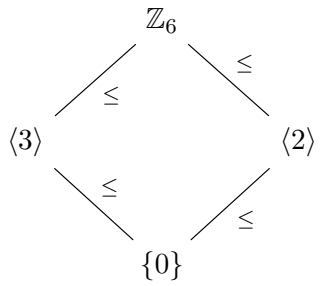
Solution Suppose H is a subgroup of G, $H \leq G$, and so by Lagrange's theorem we have

$$|H| \,\big|\, |G| = 6$$

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 1.22
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

$$|H| \,\big|\, |G| = p.$$

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 $\mathbb{Z}_{60}$.

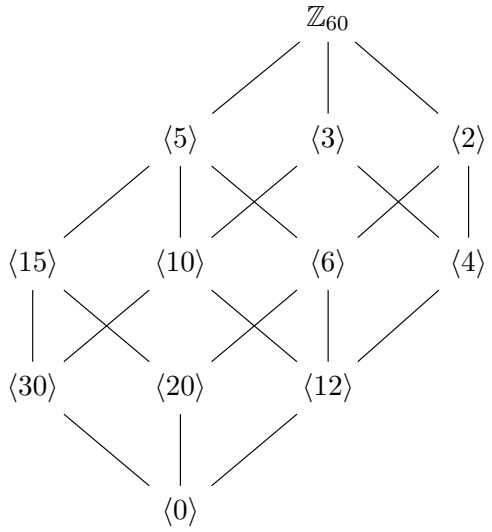
Solution Suppose H is a subgroup of $\mathbb{Z}_{60}$. By Lagrange theorem,

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

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 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 asscoiative.
- **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 | 1 3 7 9

◀

Theorem 1.23
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,

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

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

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

Thus $t \leq s$. But

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

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

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

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

For the general case, suppose the result holds for

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

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

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n$$

by induction. □

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

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 $\mathbb{Z}_3$.

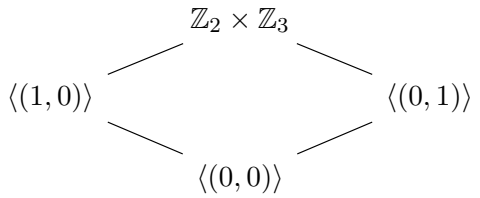
Solution The direct product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$ form a tuple,

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

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

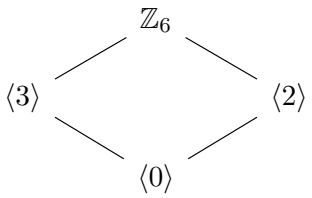
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 +_2 a_2, b_1 +_3 b_2).$$

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**)



$\cdot$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

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 1.24 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 $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ 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 $a_i, a_i^p, a_i^{p^2}, \ldots, a_i^{p^{k-1}}$ 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 $|G| = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, 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.
function Main_greedy_algorithm(G: FiniteGroup) → Product of CyclicGroups
    ā ← find_element_with_max_order(G)
    // Generated subgroup with first element ā_1 from ā.
    H ← ⟨ā_1⟩
    i ← 1
    while |H| ≠ |G| do                                  ▷ Greedy search for all cyclic groups
        max_cyclic_order = |G|/|H|
        ⟨a_i⟩ = [ ]
        while p^k ≤ max_cyclic_order do
            if ā_i^{p^{k-1}} ∉ H then                   ▷ Check if ā_i^{p^{k-1}} already in previous H
                ⟨a_i⟩.push(ā_i^{p^{k-1}})
            else
                continue
            k ← k + 1
        H ← H × ⟨a_i⟩
        i ← i + 1
    return H
// Compute the orders for all elements in group G.
function compute_orders(G: FiniteGroup) → orders
    orders = [ ]
    for a_i ∈ G do                                      ▷ elements in G
        if a_i == identity(G) then
            return 1                                    ▷ The order of identity element is one.
        else
            j ← 1
            while a_i^j ≠ e do
                j ← j + 1                               ▷ Find the order of each element.
            orders.push(j)
    return orders
// Filter out a_i with maximum order, return a list of tuple (a_i, |⟨a_i⟩|).
function find_element_with_max_order(G: FiniteGroup) → Array<tuple(element, order)>
    orders ← max_cyclic_order(G)
    return zip(G, orders).filter((_, o) → o == 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 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

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

is a group under matrix multiplication.

Exercise 1.12.4 Prove whether

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

is a non-abelian group under matrix multiplication.

Exercise 1.12.5 Prove whether

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

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 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 1.12.12 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 1.12.13 Show that a group with no proper nontrivial subgroup is cyclic.

Exercise 1.12.14 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 1.12.15 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 1.12.16

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 1.12.17

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 1.12.18 Find the conjugacy classes of dihedral group D_8.

Exercise 1.12.19 Show that a group that has only finite number of subgroups must be a finite group.

Exercise 1.12.20 Find all cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.

Exercise 1.12.21 Compute the quotient group $\mathbb{Z}_{12}/\langle 2\rangle$.

Exercise 1.12.22 Show that if H is a subgroup of index 2 in a finte group G, then every left coset of H is also a right coset of H.

Exercise 1.12.23 Let $\phi : G \to G$ 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 1.12.24 Let $\phi : G \to G$ 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 1.12.25 Let $\phi : G \to G$ 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 1.12.26 Let G be a group and g an element in G. Consider the mapping $\phi : G \to G$ defined as $\phi(x) = gxg^{-1}$. Show that ϕ is an isomorphism.

Exercise 1.12.27 Find $ker(\phi)$ for map $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ such that $\phi(1) = 8$.

Exercise 1.12.28 Find $ker(\phi)$ for map $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ such that $\phi(1, 0) = (2, -3)$ and $\phi(0, 1) = (-1, 5)$.

Exercise 1.12.29 Let $\phi : G \to H$ be a group homorphism. Show that $\phi(G)$ is abelian if and only if

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

Exercise 1.12.30 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 $N \lhd A$.
3. Show that the quotient group A/N is isomorphic to $\mathbb{R}^*$.

Exercise 1.12.31 Let $G = S_4$ and let

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

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

Exercise 1.12.32 Find (up to isomorphism) all abelian groups of order 45.

Exercise 1.12.33 Show that any group of order p^2 is abelian.

Exercise 1.12.34 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 1.12.35 If $H, K \leq G$, show that $H \cap K \leq G$.

Exercise 1.12.36 If $N \lhd G$ and $H \leq G$, show that $NH \leq G$.

Exercise 1.12.37 If $N_1, N_2 \lhd G$, show that $N_1 \cap N_2 \lhd G$.

Exercise 1.12.38 If $N \lhd G$ and $H \leq G$, show that $H \cap N \lhd G$.

2

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

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

2.1 subrings

Theorem 2.1 Subring test
A nonempty subset S of the ring R is a subring if S is closed under subtraction and multiplication, that is,

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

Definition 2.1 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 $\text{char}(R)$.

2.2 Quotient rings, Ideals

2.2.1 Ideals

Definition 2.2 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 2.1
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

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

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 $kb_2 \in I$, and so $a_2 j + kb_2 + jk \in I$.

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. □

Theorem 2.2 Ideal test
A nonempty subset A of a ring R is an ideal of R provided

1. $A \neq \varnothing$.
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

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

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 $n \cdot 0 = 0 \in n\mathbb{Z} \neq \varnothing$.
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
$$\langle \mathfrak{a} \rangle = \{r\mathfrak{a} \mid r \in R\}$$
is an ideal of R called the **principal ideal** generated by $\mathfrak{a}$.

Solution Using ideal test to check

1. Since R is a ring, then $0_R \in R$ and so $0_R = 0_R \cdot \mathfrak{a} \in \langle \mathfrak{a} \rangle \neq \varnothing$.
2. For all $b, c \in \langle \mathfrak{a} \rangle$, let $b = r_1\mathfrak{a}$, $c = r_2\mathfrak{a}$, where $r_1, r_2 \in R$. Then
$$b - c = r_1\mathfrak{a} - r_2\mathfrak{a} = (r_1 - r_2)\mathfrak{a} \in \langle \mathfrak{a} \rangle.$$
and $r_1 - r_2$ is in R.
3. For all $\bar{a} \in \langle \mathfrak{a} \rangle$, $r \in R$, we let $\bar{a} = r'\mathfrak{a}$ and
$$\bar{a}r = (r'\mathfrak{a})r = \mathfrak{a}(r'r) \in \langle \mathfrak{a} \rangle.$$
where $r'r \in R$.
On the other hand,
$$r\bar{a} = r(r'\mathfrak{a}) = \mathfrak{a}(rr') = \mathfrak{a}(r'r) = \bar{a}r \in \langle \mathfrak{a} \rangle.$$
Therefore $\langle \mathfrak{a} \rangle$ is a subring of R.

◀

2.2.2 Quotient Rings

Theorem 2.3
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.
$$\begin{aligned} s + A = s' + A &\Rightarrow s - s' \in A \\ &\Rightarrow s - s' = a_1 \in A \\ &\Rightarrow \boxed{s = a_1 + s'}, \quad a_1 \in A. \end{aligned} \tag{♡}$$
and
$$\begin{aligned} t + A = t' + A &\Rightarrow t - t' \in A \\ &\Rightarrow t - t' = a_2 \in A \\ &\Rightarrow \boxed{t = a_2 + t'}, \quad a_2 \in A. \end{aligned} \tag{♣}$$
Summing up (♡) together with (♣) 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
$$s + t - (s' + t') = a_1 + a_2, \Longrightarrow s + t - (s' + t') \in A.$$
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 (♡), (♣) we have
$$st - s't' = a_1a_2 + a_1t' + s'a_2$$
Is a_1t' in A? Of course, since $a_1 \in A, t' \in R \Longrightarrow a_1t' \in A \triangleleft R$. 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

$$4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\}.$$

The left ideals are

$$\begin{aligned}
1 +_4 4\mathbb{Z} &= \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\} \\
2 +_4 4\mathbb{Z} &= \{\ldots, -6, -2, 2, 6, 10, 14, \ldots\} \\
3 +_4 4\mathbb{Z} &= \{\ldots, -5, -1, 3, 7, 11, 15, \ldots\} \\
4 +_4 4\mathbb{Z} &= \{\ldots, -4, 0, 4, 8, 12, 16, \ldots\} = 4\mathbb{Z}
\end{aligned}$$

◀

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 2.2
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 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. □

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 2.3
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

$$(a + M)(b + M) = 1_R + M \Longrightarrow (1_R - ab) \in M \Longrightarrow ab + m = 1_R$$

for some $m \in M$. Since $ab \in I$ and $m \in M \subset I$. Also $1_R \in I \Longrightarrow I = R$. Thus M is a maximal ideal. □

Theorem 2.4
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 $N = R \Longrightarrow 1_R \in N$. $ra+m = 1_R$ 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. □

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. □

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 $\phi : \mathbb{Z} \to \mathbb{Z}_3$ defined by

$$\phi(x) = x \pmod 3 \quad \forall x \in \mathbb{Z}$$

is a ring homomorphism.

Solution Clearly, for all $x, y \in \mathbb{Z}$

$$\begin{aligned}\phi(x+y) = (x+y) \pmod 3 &= (x \bmod 3) + (y \pmod 3) \\ &= \phi(x) +_3 \phi(y)\end{aligned}$$

and

$$\begin{aligned}\phi(xy) = (xy) \pmod 3 &= (x \bmod 3) \cdot (y \pmod 3) \\ &= \phi(x) \cdot_3 \phi(y)\end{aligned}$$

This is an example of a map that respects both operations. ◀

Example 2.3.2. Consider the map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_6, \phi(x) = 3x$ for all x in $\mathbb{Z}_4$. ϕ is a ring homomorphism.

Solution For all $x, y \in \mathbb{Z}$, we check that

$$\begin{aligned}\phi(x+y) = 3(x+y) \pmod 6 &= (3x \bmod 6) + (3y \pmod 6) \\ &= \phi(x) +_6 \phi(y)\end{aligned}$$

and

$$\begin{aligned}\phi(xy) = 3(xy) \pmod 6 = 9(xy) \pmod 6 &= (3x \bmod 6) \cdot (3y \pmod 6) \\ &= \phi(x) \cdot_6 \phi(y)\end{aligned}$$

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

$$3 \pmod 6 = \phi(1) = \phi(1 \cdot 1) = \phi(1)\,\phi(1) = 3 \cdot 3 = 9 \pmod 6.$$

◀

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 $\phi : R \to \mathbb{C}$ 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

$$\begin{aligned}\phi(A(a,b)+A(c,d)) &= \phi\left(A(a+c,b+d)\right)\\ &= (a+c)+(b+d)i\\ &= (a+bi)+(c+di)\\ &= \phi\left(A(a,b)\right)+\phi\left(A(c,d)\right).\end{aligned}$$

For multiplication, we have

$$\begin{aligned}\phi(A(a,b)+A(c,d)) &= \phi\left(\begin{bmatrix}a & b\\ -b & a\end{bmatrix}\begin{bmatrix}c & d\\ -d & c\end{bmatrix}\right)\\ &= \phi\left(\begin{bmatrix}ac-bd & ad+bc\\ -(ad+bc) & ac-bd\end{bmatrix}\right)\\ &= \phi\left(A(ac-bd,ad+bc)\right)\\ &= (a+bi)(c+di)\\ &= \phi\left(A(a,b)\right)\,\phi\left(A(c,d)\right).\end{aligned}$$

Now, ϕ is one-to-one and onto since $\phi\left(A(a,b)\right) = a+bi = 0$ if and only if $a=b=0$, and $Ker\,\phi = \{A(0,0)\}$ is trivial. ◀

Example 2.3.4. Show that the equation $2x^3-5x^2+7x-8=0$ has no solutions in $\mathbb{Z}$.

Solution Let $\phi:\mathbb{Z}\to\mathbb{Z}_3$ 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. ◀

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 $\phi:2\mathbb{Z}\to 3\mathbb{Z}$ 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 $6k=9k^2 \Longrightarrow k=0$ or $k=\frac{2}{3}$.

For $k=0 \Longrightarrow \phi(x)=0$ is not one-to-one and not onto. Also, $k=\frac{2}{3}\notin\mathbb{Z}$, and thus ϕ cannot be an isomorphism. ◀

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 $f : \mathbb{Z} \to \mathbb{Z}_6$, 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 $0 = m - m^2 \ (\text{mod}6)$. Working modulo 6 one by one

$$0 - 0^2 = 0 - 0 = 0, 1 - 1^2 = 1 - 1 = 0, \qquad 2 - 2^2 = 2 - 4 = 4 \neq 0$$
$$3 - 3^2 = 3 - 9 = -6 = 0, 4 - 4^2 = 4 - 16 = 0, \qquad 5 - 5^2 = 5 - 25 = 2 \neq 0$$

The possible values of m are $0, 1, 3$ and 4. So the homomorphisms are as follow

- $f(a) = 0 \ (\text{mod}6), \quad \forall a \in \mathbb{Z}.$
- $f(a) = a \ (\text{mod}6), \quad \forall a \in \mathbb{Z}.$
- $f(a) = 3a \ (\text{mod}6), \quad \forall a \in \mathbb{Z}.$
- $f(a) = 4a \ (\text{mod}6), \quad \forall a \in \mathbb{Z}.$

◀

Theorem 2.5 The first isomorphism for rings
Let f be a ring homomorphism from ring R ro S. Then the mapping from $R/ker(f)$ to $f(R)$, given by

$$r + ker(f) \to f(r)$$

is an isomorphism. In symbols, $R/ker(f) \cong f(R)$.

Proof. Define a map $f : R/K \to \text{Im}\, \overline{f}$ by

$$f(a + K) = \overline{f}(a) \quad \forall a \in R, a + K \in R/K.$$

1. Since f is well defined, so

$$\begin{aligned} a + K = b + K &\Rightarrow a - b \in K \\ &\Rightarrow \overline{f}(a - b) = 0_S \\ &\Rightarrow \overline{f}(a) - \overline{f}(b) = 0_S \\ &\Rightarrow \overline{f}(a) = \overline{f}(b) \end{aligned}$$

2. f is injective since

$$\begin{aligned} f(a+K)=f(b+K) &\Rightarrow \overline{f}(a)=\overline{f}(b) \\ &\Rightarrow \overline{f}(a-b)=0_S \\ &\Rightarrow a-b\in K \\ &\Rightarrow a+K=b+K. \end{aligned}$$

3. f is surjective. For all $f(a)\in \operatorname{Im}\overline{f}, \exists a+K\in R/K$ such that $\overline{f}(a+K)=f(a)$.

4. f is homomorphism,

$$\begin{aligned} f(a+K+b+K) &\Rightarrow f((a+b)+K) \\ &\Rightarrow \overline{f}(a+b) \\ &\Rightarrow \overline{f}(a)+\overline{f}(b) \\ &\Rightarrow f(a+K)+f(b+K). \end{aligned}$$

$$\begin{aligned} f(a+K)\cdot f(b+K) &\Rightarrow f(ab+K) \\ &\Rightarrow \overline{f}(ab) \\ &\Rightarrow \overline{f}(a)\cdot\overline{f}(b) \\ &\Rightarrow f(a+K)\cdot f(b+K). \end{aligned}$$

Thus $f: R/K\cong \operatorname{Im} f$ as rings. □

Example 2.3.7. Let $\phi:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}_3$ 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 $\mathbb{Z}\times\mathbb{Z}$.

2.4 Polynomial rings

Definition 2.6
Let R be a commutative ring. We define

$$R[x]=\{r_nx^n+r_{n-1}x^{n-1}+\cdots+r_1x+r_0 \mid r_i\in R\}. \tag{2.1}$$

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 2.6 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

$$f(x) = q(x)g(x) + r(x) \tag{2.2}$$

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. □

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 2.7 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 $f(a) = 0$. So

$$f(x) = (x - a)q(x) + c \implies 0 = f(a) = (a - a)q(a) + c.$$

Thus $c = 0$, and $x - a$ is a factor of $f(x)$.

($\Leftarrow$) On the other way, we want to show □

Definition 2.7 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 $x = 0, 1, \ldots, 11$.

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 $Z_{11}[x]$.

Solution We can use synthetic division,

$$\begin{array}{cccc|c} 2 & 3=-8 & -7=4 & 6 & \\ & -2 & -10 & -6 & -1 \\ \hline 2 & -10=1 & -6 & & \\ & -4 & 6 & & -2 \\ \hline 2 & -3 & & & \end{array}$$

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 2.8 Rational root test
Let

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \qquad (\bigstar)$$

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 ($\bigstar$) and equating with zero. The equation is now

$$a_n\left(\frac{r}{s}\right)^n+a_{n-1}\left(\frac{r}{s}\right)^{n-1}+\cdots+a_1\left(\frac{r}{s}\right)+a_0=0.$$

Again multiplying s^n on both sides

$$a_nr^n+a_{n-1}r^{n-1}s+\cdots+a_1rs^{n-1}x+a_0s^n=0.$$

Factoring r out and moving a_0s^n to the right-hand side. We obtained

$$r(a_nr^{n-1}+a_{n-1}r^{n-2}s+\cdots+a_1s^{n-1}x)=-a_0s^n.$$

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

$$\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm6,\ \pm12,\ \pm\frac{1}{2},\ \pm\frac{3}{2}.$$

In fact, $f(x)=(x+3)\left(x-\frac{1}{2}\right)(2x^2-4x-8)\in\mathbb{Q}[x]$. ◀

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 2.9 Mod p Irreducibility test
Let p be a prime and let $f(x) \in \mathbb{Z}[x]$ with degree 1 or greater. Let $\overline{f} \in \mathbb{Z}_p[x]$ obtained by reducing all of $f(x)$'s coefficients mod p. Then if

$$\deg(\overline{f}) = \deg(f) \tag{2.3}$$

and $\overline{f}$ 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 $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ defined by $\phi f(x) = \overline{f}(x)$ is a ring homomorphism. So

$$\overline{f}(x) = \overline{p(x)q(x)} = \overline{p}(x)\overline{q}(x).$$

If $p \nmid a_k$, then p does not divide the leading coefficients of $p(x)$ and $q(x)$. Thus $\deg \overline{p}(x) = \deg p(x)$ and $\deg \overline{q}(x) = \deg q(x)$. □

Example 2.5.6. The polynomial $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ is irreducible in $\mathbb{Q}$.

Solution We define

$$\overline{f}(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x].$$

By rational root test, the only possible root is 0.1 from $\mathbb{R}$ but it is not an inetger. 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 $\overline{f}$. The only possible factor of $\overline{f}$ 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 $\mathbb{Q}[x]$. ◀

Theorem 2.10 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 $p|a_{n-1}, \ldots p|a_2$ 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

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$
$$g(x) = b_rx^r + b_{r-1}x^{r-1} + \cdots + b_1x + b_0,$$
$$h(x) = c_sx^s + c_{s-1}x^{s-1} + \cdots + c_1x + c_0.$$

Since $p|a_0 = b_0c_0 \Longrightarrow p|b_0$ 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 $p \nmid c_0 \Longrightarrow p|b_1$. Assume that $p|b_i \; \forall 0 \leq i < m$ for some $m \leq r$. Then

$$p|a_m = \sum_{\substack{i+j=m \\ j \leq s}} b_ic_j \Longrightarrow p|b_mc_0 \Longrightarrow p|b_m.$$

By mathematical induction, $p|b_r$. Thus $p|a_n = b_rc_s$. This contradicting the fact that $f(x)$ is reducible. □

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 $\zeta, \zeta^2, \ldots, \zeta^n$ 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 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:

$$\Phi_n(x) = \prod_{\substack{a=1 \\ \gcd(a,n)=1}}^{n} (x - \zeta^a). \tag{2.4}$$

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 $\overline{f}(x)$ be the polynomial whose coefficients are the residue classes (mod p) determined by the coefficients of $f(x)$. Thus the assertion $\overline{f} = \overline{g}$ means that there is a polynomial $h(x)$ with integral coefficients such that $f(x) = ph(x)$.

Lemma 2.4
(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 $\overline{C} = \overline{A}$.

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,

$$\frac{\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)^p - \sigma_k(\alpha_1^p, \alpha_2^p, \ldots, \alpha_n^p)}{p}$$

is a symmetric polynomial in the α, with integral coefficients, and hence by the symmetric function theorem the quantity must be a rational integer. □

Lemma 2.5
Put $f(x) = x^n - 1$. Then $\overline{f}$ is a squarefree if and only if $p \nmid n$.

Proof. By previous lemma we can see that if $p \nmid n$. Then $\gcd(\overline{f}, \overline{f}') = 1$, and hence that $\overline{f}$ is squarefree. On the other hand, if $p|n$, say $n = mp$ for some integer m, then

$$\overline{f} = \overline{(x^m - 1)^p}$$

and hence $\overline{f}$ 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 $\overline{\Phi_n}$ is also squarefree. □

Theorem 2.11
(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 $\overline{G}|B$ and $\overline{G}|C$. But $\overline{A} = \overline{C}$ by previous lemma, and hence $\overline{G}^2 | \overline{A}\overline{B}$. But Φ_n is squarefree, by previous lemma. Hence $G = \bar{1}$, 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. □

□

Theorem 2.12
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 □

Theorem 2.13 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 $\mathbb{R}$. □

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,

$$\begin{aligned} f(x) &= (r_1x+s_1)(r_2x+s_2)\dots(r_nx+s_n) \\ &= r_1\,r_2\dots r_n(x+s_1r_1^{-1})(x+s_2r_2^{-1})\dots(x+s_nr_n^{-1}). \end{aligned}$$

Since $f(x)$ has n unique roots, factorization is also unique. □

Lemma 2.6
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 $\varphi : \mathbb{C}[x] \to \mathbb{C}[x]$ 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 has 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 $\bar{z}$. □

Theorem 2.14
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 $1 \le j \le n$. 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

$$f(x) = ax^2 + bx + c \quad \forall a, b, c \in \mathbb{R} \tag{♣}$$

We now continue to work on the "formula" to solve x. Completing the square on (♣)

$$\begin{aligned} ax^2 + bx + c = 0 &\Rightarrow a\left[x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2\right] - \left(\frac{b}{2a}\right)^2 = 0 \\ &\Rightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \\ &\Rightarrow x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a} \\ &\Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \quad a \neq 0 \end{aligned}$$

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 $\mathbb{R}[x]$. □

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. □

2.6 Integral Domains

Let R be a commutative ring. A **zero divisor** is a nonzero element $a \in R$ such that

$$ab = 0 \tag{2.5}$$

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 $b = 0$.

Definition 2.8
A ring with unity 1 having no zero divisors is an integral domain.

Lemma 2.7
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 has an inverse a^{-1} such that $a^{-1}ab = a^{-1} \cdot 0 \Longrightarrow b = 0$. Therefore, F has no zero divisors, and so F is an integral domain. □

Definition 2.9
If F is a field, then the only ideals are $\{0\}$ and F itself.

Proof. 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 $I = F$. □

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 $2 \mid a^2 \implies 2 \mid a$. 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)**.** $M_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z} \right\}$ 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 2.15
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

$$D = \{a, a^2, a^3, \ldots, a^t\}$$

where $a \neq 0$ for some $t \in \mathbb{N}$. Consider two elements a^i, a^j from D, we have

$$\begin{aligned} a^i = a^j &\Rightarrow a^{i-j} = 1_D \\ &\Rightarrow a\, a^{i-j-1} = 1_D \\ &\Rightarrow a^{-1} = a^{i-j-1} \\ &\Rightarrow a \cdot a^{-1} = a^{i-j} = 1_D. \end{aligned}$$

and the multiplication is commutative, therefore D is a field. □

Remark.

$$\begin{aligned} \textit{if } \mathbb{Z}_p \textit{ is a field} &\Longrightarrow \mathbb{Z}_p \textit{ has no zero divisors.} \\ &\Longrightarrow \mathbb{Z}_p \textit{ is an integral domain.} \\ &\Longrightarrow |\mathbb{Z}_p| = p \textit{ is prime and is finite.} \end{aligned}$$

2.7 Principal Ideal Domain

Definition 2.10
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 2.16
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 alogrithm*, 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 $f(x) = q(x)\, g(x) \Longrightarrow f(x) \in \langle g(x) \rangle$. □

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.

Theorem 2.17
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

$$a = p_1 p_2 \cdots p_r \quad \text{and } a = q_1 q_2 \cdots q_s$$

where each p_i and q_j is irreducible in R, and $s \geq r$. Then p_1 divides the product $q_1, q_2, \cdots, q_s$ 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

$$1 = u_1 u_2 \ldots u_r\, q_{r+1} \ldots q_s.$$

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. □

Tutorials

Exercise 2.8.1 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 2.8.2 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 2.8.3 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 2.8.4 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 2.8.5 Show that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Exercise 2.8.6 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 2.8.7 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 2.8.8 If F is a field, show that $(F \setminus \{0\}, \cdot)$ is a group.

Exercise 2.8.9 Show that in a field F, the only ideals are F and $\{0\}$.

Exercise 2.8.10 Show that each homomorphism from a field to a ring is either one to one or maps everything onto 0.

Exercise 2.8.11 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 2.8.12 Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{Z})$.

Exercise 2.8.13 An element $\mathfrak{a}$ of a ring R is idempotent if $\mathfrak{a}^2 = \mathfrak{a}$. Show that a division ring contains exactly two idempotent elements.

Exercise 2.8.14 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 2.8.15 If A and B are ideals of a ring R, then the product AB of A and B is defined by

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}.$$

1. Show that AB is an ideal of R.
2. Show that $AB \subseteq (A \cap B)$.

Exercise 2.8.16 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 $\mathbb{Z}_{11}[x]$.

3

Fields

3.1 Extenstion Fields

3.1.1 Simple Extension

Definition 3.1
Let E be an extension field of a field F and let $\mathfrak{a} \in E$. We call an element $\mathfrak{a}$ **algebraic** over F if $\mathfrak{a}$ is the zero of some nonzero polynomial in $F[x]$. If $\mathfrak{a}$ 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 $p(x) = q(x)$. □

Remark. *The $p(x)$ is called the "minimal polynomial of u over F".*

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 $p(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$. ◀

Theorem 3.2
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. $\{1, u, u^2, \ldots, u^{n-1}\}$ 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

$$b_0 + b_1 u + b_2 u^2 + \cdots + b_t u^t \quad \forall b_i \in F.$$

We again define a function $\varphi : F[x] \to F(u)$ 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, $F[x]/p(x) \cong \operatorname{Im} \varphi$. Since $p(x)$ is irreducible, the quotient ring $F[x]/\langle p(x) \rangle$ is a field and $\operatorname{Im} \varphi$ is also a field.

Note that $\varphi(c) = c \; \forall c \in F$ and $\varphi(x) = u$. Thus $F \subset \operatorname{Im} \varphi$ and $u \in \operatorname{Im} \varphi$. By definition of simple extension, $F(u) = \operatorname{Im} \varphi$.

2. Since $F(u) = \operatorname{Im} \varphi$, $\forall w \in F(u), \exists f(x) \in F \; s.t. \; f(u) = w$. 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

$$r(x) = f(x) - p(x)q(x) \Longrightarrow r(u) = f(u) - p(u)q(u) = w$$

with $\deg r(x) < n$. Thus

$$F(u) = \text{Span}\{1, u, u^2, \ldots, u^{n-1}\}.$$

3. Let $c_0 + c_1u + c_2u^2 + \cdots + c_{n-1}u^{n-1} = 0$. 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 $\{1, u, u^2, \ldots, u^{n-1}\}$ is linearly independent and it is also a basis of $F(u)$ over $F \Longrightarrow |F(u) : F| = n$.

□

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 $\sigma : F \to E$ be an isomorphism then we again define $\bar{\sigma} : F[x] \to E[x]$ by for $a_0 + a_1x + \cdots + a_nx^n \in F[x]$. We can write

$$\sigma(a_0 + a_1x + \cdots + a_nx^n) = \sigma(a_0) + \sigma(a_1x) + \cdots + \sigma(a_nx^n) \tag{3.1}$$

and $\bar{\sigma}$ is also isomorphism.

Corollary 3.1
Let $\sigma : F \to E$ 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 $\bar{\sigma} : F(u) \to E(v)$ such that

$$\bar{\sigma}(u) = v \text{ and } \bar{\sigma}(c) = \sigma(c) \quad \forall c \in F.$$

Proof. By previous theorem, $\varphi : F[x]/(p(x)) \to F(u)$ and $\bar{\varphi} : E[x]/(\sigma p(x)) \to E(v)$ are isomorphism where $\varphi([f(x)]) = f(u)$ and $\bar{\varphi}([g(x)]) = g(v)$.

Furthermore, we let ξ be the surjective isomorphism

$$\bar{\xi} : E[x] \to E[x]/(\sigma p(x))$$

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 $\overline{xi}$ 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

$$F(u) \xleftarrow[\varphi]{} F[x]/\langle p(x) \rangle \xrightarrow{\theta} E(v)$$

$$f(u) \xleftarrow[\varphi]{} [f(x)] \xrightarrow{\theta} \sigma f(v)$$

$$c \xleftarrow[\varphi]{} [c] \xrightarrow{\theta} \sigma(c)$$

The composite function $\theta \circ \varphi^{-1} : F(u) \to E(v)$ is an isomorphism that extends σ and maps u to v.

$$\begin{array}{ccccc} F & & \xrightarrow{\sigma} & & E \\ \downarrow{\scriptstyle \subseteq} & & & & \downarrow{\scriptstyle \subseteq} \\ F[x] & & \xrightarrow{\sigma} & & E[x] \\ \downarrow{\scriptstyle \xi} & & & & \downarrow{\scriptstyle \bar{\xi}} \\ F(u) & \xrightarrow{\varphi} & F[x]/\langle p(x) \rangle & \xrightarrow{\sigma} & E[x]/\langle \sigma p(x) \rangle \xrightarrow{\bar{\varphi}} E(v) \end{array}$$

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 3.2 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 3.3
If K is a finite-dimensional extension field of F, then K is an algebraic extension of F.

Proof. Let $\{V_1, V_2, \ldots, V_n\}$ be the basis of K over F. For all $u \in K$, $\{1, u, u^2, \ldots, u^n\}$ is linearly dependent. That is,

$$\exists u^k \in K \; s.t. \; u^k = \text{Span}\{1, u, u^2, \ldots, u^n\} = c_0 + c_1 u + c_2 u^2 + \cdots + c_{k-1} u^{k-1} (k \geq 1).$$

Thus u is a root of $f(x) = x^k - c_{k-1}u^{k-1} - \cdots - c_0$, 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 transcental element u, then K must be infinite dimensional over F.

$$\text{Non algebraic} \Longrightarrow \text{Infinite dimension}$$

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 $u_1, u_2, \ldots, u_n$ are elements of an extension field K of F. Let $F(u_1, \ldots, u_n)$ denote the intersection of all the subfields of K that contain F and every u (known as generalized simple extension); $F(u, u_1, \ldots, u_n)$ is said to be a finitely generated extension of F.

Theorem 3.4
If $K = F(u_1, u_2, \ldots, u_n)$ 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

$$|F(u,v) : F(u)| \cdot |F(u) : F| < \infty \Longrightarrow |F(u,v) : F| = |F(u,v) : F(u)| \cdot |F(u) : F| < \infty.$$

By mathematical induction, we have

$$|F(u_1, u_2, \ldots, u_n) : F(u_1, u_2, \ldots, u_{n-1})| \ldots |F(u_1) : F| < \infty$$

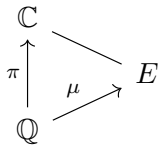
which is also finite. □

Corollary 3.2
If L is algebraic extension of K and K is an algebraic extension of L. Then L is an algebraic extension field of F.

Proof. $\forall \omega \in L,\ \exists f(x) \in K[x] \quad s.t.\ f(\omega) = a_0 + a_1\omega + \cdots + a_n\omega^n$.

Note that $F(a_0, a_1, \ldots, a_n)$ 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 $F(a_0, a_1, \ldots, a_n)$. So $F(a_0, a_1, \ldots, a_n)$ is finite dimensional extension of $F \implies \omega$ is algebraic over F. Thus L is an algebraic extension of F. □

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 K.*



- *μ denote algebraic extension over $\mathbb{Q}$, e.g.: $\sqrt{2}, \sqrt{3}, i, \ldots$.*
- *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. □

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 $\{u_1, u_2, \ldots, u_n\}$ is a basis of K over F. This implies $F(u_1, u_2, \ldots, u_n) \subseteq K$ and $K \subseteq F(u_1, u_2, \ldots, u_n)$. Thus,

$$K = F(u_1, u_2, \ldots, u_n) = \text{Span}\{u_1, u_2, \ldots, u_n\}.$$

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

$$\begin{aligned} (\sqrt{5} - a)^2 = (b\sqrt{3})^2 \quad &\Rightarrow 5 - 2\sqrt{5}a + a^2 = 3b^2 \\ &\Rightarrow \frac{5 + a^2 - 3b^2}{2a} = \sqrt{5} \quad (a \neq 0) \end{aligned}$$

However, when $a = 0$, we have $5 = 3b^2$. Which is a contradiction. ◀

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 3.3 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
$$f(x) = c(x - u_1) \ldots (x - u_n) \tag{3.2}$$
- and
$$K = \underbrace{F(u_1, u_2, \ldots, u_n)}_{\text{smallest field}}. \tag{3.3}$$

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 $\mathbb{Q}$.

3.3 Finite Fields

Theorem 3.5
Let R be a ring with identity. Then

1. The set
$$\mathfrak{P} = \{k \cdot 1_R \mid k \in \mathbb{Z}\}$$
is a subring of R.
2. If R has characteristic 0, then $\mathfrak{P}$ is isomorphic to $\mathbb{Z}$.
3. If R has characteristic $n > 0$, then $\mathfrak{P}$ is isomorphic to $\mathbb{Z}_n$.

Proof. We prove each of the statements listed above.

1. First of all, we use subring test to check if $\mathfrak{P}$ is a subring of R.
$$\begin{cases} a \cdot 1_R - b \cdot 1_R = (a-b) \cdot 1_R \in \mathfrak{P} \\ a \cdot 1_R \cdot b \cdot 1_R = ab\, 1_R \in \mathfrak{P} \end{cases}$$
so $\mathfrak{P}$ is a subring of R.

We now prove (2), (3) at once, We consider a map $f : \mathbb{Z} \to \mathbb{R}$ 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 $ker\, f = \langle 0 \rangle \Longrightarrow \mathbb{Z} \cong \mathbb{R}$.
- If R has a characteristic n, then $ker\, f = \langle n \rangle \Longrightarrow \mathbb{Z}/\langle n \rangle \cong \mathbb{R}$.

□

3.3.1 Order of finite field

Theorem 3.6
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 $\{u_1, u_2, \ldots, u_n\}$ is a basis of K.

$\forall k \in K$, k is represented uniquely be

$$k = c_1u_1 + c_2u_2 + \cdots + c_nu_n.$$

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

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}. \tag{3.4}$$

Proof. We will use the induction on n.

Assume $n = 1$, we expand $(a+b)^p$ with binomial theorem.

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{n-k}b^k = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p.$$

Note that

$$\binom{p}{k} = \frac{p!}{(p-k)!\,k!}, \quad k, p-k < p \text{ for } 1 \le k < p.$$

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. □

Theorem 3.7 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 $\mathbb{Z}_p$.

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 $n \ge 5$.

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.

Definition 3.4 Galois group
Let K be an extension field of F. An F-automorphism of K is an isomorphism $\sigma : K \to K$ that fixes F elementwise. That is, $\sigma(c) \to c, \forall c \in F$.
The set of all F-automorphisms of K is denoted $\mathrm{Gal}_F\, K$ and is called the Galois group of K over F.

Theorem 3.8
If K is an extension field of F, then $\mathrm{Gal}_F\, K$ is a group under the operation of composition of functions.

Proof. We need to show that the function composition from a group:

[Closedness]: $\forall \sigma, \tau \in \mathrm{Gal}_F\, K, \quad \sigma \circ \tau(c) = c\, \forall c \in F$.

[Associativity]: Associativity holds because of function composition's property.

[Existence of identity]: $\forall \sigma \in \mathrm{Gal}_F\, K, \sigma \circ \tau = \tau \circ \sigma = \sigma$.

[Existence of inverse]: $\forall \sigma \in \mathrm{Gal}_F\, K, \sigma^{-1}(c) = c\, \forall c \in F$. So σ^{-1} is the inverse in $\mathrm{Gal}_F\, K$. □

Theorem 3.9
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 $\sigma \in \mathrm{Gal}_F\, K$, then $\sigma(u)$ is also a root of $f(x)$.

Proof. Take a $u \in K$, $f(u) = 0 \Longrightarrow \sigma(f(u)) = \sigma(0) = 0$.

Since $\sigma \in \mathrm{Gal}_F\, K, \sigma\left(f(u)\right) = f\left(\sigma(u)\right) = 0$. □

Remark. *Every root of $p(x)$ in K is the image of u under some automorphism of* $\mathrm{Gal}_F\, K$.

Theorem 3.10
Let K be the splitting field of some polynomial over F and $u, v \in K$. Then there exists an $\sigma \in \mathrm{Gal}_F\, K$ 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

$$|K : F| \leq n! \Longrightarrow K \text{ is algebraic over } F.$$

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 $\sigma : F \to F$ to $\bar{\sigma} : \overline{F} \to \overline{F}$ 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 $\tilde{\sigma} : K \to K$. If $\sigma = 1$, then $\tilde{\sigma} \in \mathrm{Gal}_F\, K$. □

Example 3.4.1. Given that $\sigma \in \mathrm{Gal}_{\mathbb{R}}\, \mathbb{C}$, find $\sigma(i)$.

Solution By previous theorem,

$$\sigma(i) = \{i, -i\}.$$

Thus $\mathrm{Gal}_F\, K = \{1, \sigma\}$ is a group of order 2 and hence $\mathrm{Gal}_{\mathbb{R}}\, \mathbb{C}$ is isomorphic to $\mathbb{Z}_2$. ◀

Theorem 3.11 Galois group of finitely generated extension
Let $K = F(u_1, u_2, \ldots, u_n)$ be an algebraic extension field of F. If $\sigma \circ \tau \in \mathrm{Gal}_F\, K$ and $\sigma(u_i) = \tau(u_i)$ for each $i = 1, 2, \ldots, n$. Then $\sigma = \tau$.
In other words, an automorphism in $\mathrm{Gal}_F\, K$ is completely determined by its action on $u_1, u_2, \ldots u_n$.

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

$$c_0 + c_1 u_1 + \cdots + c_{n-1} u_1^{n-1} = w \Longrightarrow \beta(v) = v.$$

Again we let $w \in F(u_1, u_2)$, then there exists a constant $c_i \in F$ such that

$$c_0 + c_1 u_2 + \cdots + c_{n-1} u_2^{n-1} = w \Longrightarrow \beta(w) = w.$$

Repeating this process, we conclude that for all $v \in K$, $\beta(v) = v \Longrightarrow \beta = 1$. Thus $\tau = \sigma$. □

Example 3.4.2. Consider $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\, \mathbb{Q}[\sqrt{3}, \sqrt{5}]$. 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 $\mathrm{Gal}_{\mathbb{Q}}\, \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \tau, \alpha, \beta\}$ 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 $\mathrm{Gal}_{\mathbb{Q}}\, \mathbb{Q}[\sqrt{3}, \sqrt{5}] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Corollary 3.4
If K is splitting field of a separable polynomial $f(x)$ of degree n in $F[x]$, then $\mathrm{Gal}_F\, K$ is isomorphic to a subgroup of S_n.

Proof. Let $u_1, u_2, \ldots, u_n$ be distinct roots of $f(x)$. Then $K = F(u_1, u_2, \ldots, u_n)$ and let

$$\mathcal{U} = \{u_1, u_2, \ldots, u_n\}.$$

For all permutation $\sigma \in \mathrm{Gal}_F\, K$, $\forall 1 \leq i \leq n$, $\sigma(u_i) = u_j$ for some j.

Now define a function $\theta : \mathrm{Gal}_F K \to S_n$ defined by $\theta : \sigma \mapsto \sigma \circ 1_{\mathcal{U}}$. θ is well defined. Note that

$$\sigma \circ 1_{\mathcal{U}} = \tau \circ 1_{\mathcal{U}} \Longrightarrow \sigma = \tau$$

by previous theorem. Thus θ is injective, and θ is homomorphism.

By the first isomorphism theorem, we say that

$$\mathrm{Gal}_F K \cong \mathrm{Im}\,\theta = \text{a subgroup of } S_n.$$

□

Definition 3.5 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 $\mathrm{Gal}_E K \cong \mathrm{Gal}_F K$.

Theorem 3.12
Let K be an extension field of F. If H is a subgroup of $\mathrm{Gal}_F K$, 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 $a, b \in H$. For all $\sigma \in H$, we have

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$$

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

$$\sigma(0_K) = 0_K, \sigma(1_K) = 1_K$$

$$\sigma(-a) = -\sigma(a) = -a$$

$$\sigma(a^{-1}) = (\sigma(a))^{-1} = a^{-1}$$

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 $\mathrm{Gal}_{\mathbb{Q}[\sqrt{3}]} \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \alpha\}$, and $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \tau, \alpha, \beta\}$.

Example 3.4.4. $\mathrm{Gal}_{\mathbb{Q}[\sqrt{3}]} \mathbb{Q}[\sqrt{3}, \sqrt{5}] = \{1, \alpha\}$ 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 $a_2 a_3^{-1} \in \mathbb{Q} \implies -\sqrt{3} \in \mathbb{Q}$, which is a contradiction. ◀

Example 3.4.5. $\mathrm{Gal}_{\mathbb{R}}\,\mathbb{C} = \{1, \alpha\}$, and $\alpha(a + bi) \implies a - bi = a + bi \implies b = 0$. Thus fixed field of $\mathrm{Gal}_{\mathbb{R}}\,\mathbb{C}$ is the field $\mathbb{R}$.

Remark. *The ground field F need not always be the fixed field of the group $\mathrm{Gal}_F\,K$.*

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, $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \notin \mathbb{Q}[\sqrt[3]{2}]$. $\forall \sigma \in \mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}[\sqrt[3]{2}]$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Thus $\sigma = 1$. The fixed field of $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}[\sqrt[3]{2}]$ is $\mathbb{Q}[\sqrt[3]{2}]$.

3.4.1 Fundamental Theorem of Galois theory

Definition 3.6 Galois correspondence
Let K be a finite-dimensionalextension 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 $\mathrm{Gal}_F\,K$.
Define a map $\phi : T \to S$ by this rule. For each intermediate field E,

$$\phi(E) = \mathrm{Gal}_E\,K. \tag{3.5}$$

This function ϕ is called the Galois correspondence.

$$\begin{array}{ccc}
\mathrm{Gal}_K\,K & \longrightarrow & K \\
{\scriptstyle T}\uparrow & & \downarrow{\scriptstyle S} \\
\mathrm{Gal}_F\,K & \longrightarrow & F
\end{array}$$

Example 3.4.7.

$$\mathbb{Q} \to \mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{1, \tau, \alpha, \beta\}$$

Lemma 3.2
Let K be a finite-dimensional extension field of F. If H is a subgroup of the Galois group $\mathrm{Gal}_F\,K$ and E is the **fixed field** of H, then K is *simple, normal, separable extension* of E.

$$\begin{array}{ccc} \mathrm{Gal}_F K & & K \\ | & & | \\ H & \longrightarrow & E_H \end{array}$$

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

$$\mathfrak{U} = u_1, u_2, \ldots, u_t \in K, \quad \text{where } t \leq \deg\, p(x)$$

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

$$\mathfrak{U} \overset{H}{\hookrightarrow} \{u_1, u_2, \ldots, u_t\}$$

which $\{u_1, u_2, \ldots u_t\}$ is image of $\mathfrak{U}$. And $u_i = \tau(\mathfrak{U})$ for some $\tau \in H$. is injective

$$\{u_1, u_2, \ldots, u_t\} \xhookrightarrow[\text{permutation } \sigma]{} \{u_1, u_2, \ldots, u_t\}$$

Every automorphism in H permutes $u_1, u_2, \ldots, u_t$. Let

$$f(x) = (x - u_1)(x - u_2) \ldots (x - u_t)$$

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 $g(x) = (x - v)(x - v_2) \ldots (x - v_s)$ where $\{v_1 = v, v_2, \ldots, v_s\}$ 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. □

Definition 3.7 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 3.5
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. □

Theorem 3.13 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 $\mathrm{Gal}_F K$, given by assigning each intermediate field E to the subgroup $\mathrm{Gal}_E K$. Furthermore

$$|K : E| = |\mathrm{Gal}_E K|$$

and

$$|E : F| = |\mathrm{Gal}_F K : \mathrm{Gal}_E K|.$$

2. An intermediate field E is normal extension of F if and only if the corresponding group $\mathrm{Gal}_E K$ is a normal subgroup of $\mathrm{Gal}_F K$.

Proof. 1. By theorem, fixed field of $\mathrm{Gal}_E K$ is E. By theorem we have

$$|\mathrm{Gal}_E K| = |K : E|.$$

Similarly,

$$|\mathrm{Gal}_F K| = |K : F|.$$

In fact $|K : F| = |K : E|\,|E : F|$. Thus

$$|\mathrm{Gal}_F K| = |\mathrm{Gal}_E K| \cdot |E : F| \implies |E : F| = |\mathrm{Gal}_F K : \mathrm{Gal}_E K|.$$

2. ($\Leftarrow$) Assume first that $\mathrm{Gal}_E K$ is a normal subgroup of $\mathrm{Gal}_F K$. 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 $\sigma \in \mathrm{Gal}_F K$ such that $\sigma(u) = v$ by theorem. So $\mathrm{Gal}_F K = |K : F| = E$.

$$\begin{array}{ccc} K = F(u) & \xrightarrow{\sigma} & F(u) = K \\ \Big| & & \Big| \\ F & \xrightarrow{1} & F \end{array}$$

Now if τ is any element of $\mathrm{Gal}_E K$, then normality implies

$$\tau \circ \sigma = \sigma \circ \tau' \quad \text{for some } \tau' \in \mathrm{Gal}_E K.$$

Since $u \in E$, we have

$$\begin{aligned} \tau(v) &= \tau\left(\sigma(u)\right) \\ &= \sigma\left(\tau'(u)\right) \\ &= \sigma(u) \\ &= v. \end{aligned}$$

So $\mathrm{Gal}_E K$ 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 $\theta : \mathrm{Gal}_F K \to \mathrm{Gal}_F E$ whose kernel is $\mathrm{Gal}_E K$. Then $\mathrm{Gal}_E K$ is normal subgroup of $\mathrm{Gal}_F K$.

Therefore by First isomorphism theorem, $\mathrm{Gal}_F E \cong \mathrm{Gal}_F K / \mathrm{Gal}_E K$.

□

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

$$\theta : \mathrm{Gal}_F\, K \to \mathrm{Gal}_F\, E$$

where kernel of θ is $\mathrm{Gal}_E\, K$.

Proof. Let $\sigma \in \mathrm{Gal}_F\, K$ 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

$$\sigma(E) \subseteq E \quad \forall \sigma \in \mathrm{Gal}_F\, K.$$

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. $\forall \sigma \in \mathrm{Gal}_F\, E$. σ can be extended to an F-automorphism in $\mathrm{Gal}_F\, K$. Its kernel consists of the automorphisms of K whose restriction to E is the identity map as $\mathrm{Gal}_E\, K$. □

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

$$|\,\mathrm{Gal}_{\mathbb{Q}}\, K| = |K : \mathbb{Q}|$$

and $\mathrm{Gal}_{\mathbb{Q}}\, K$ 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 $\mathrm{Gal}_{\mathbb{Q}}\, K \cong S_3$.

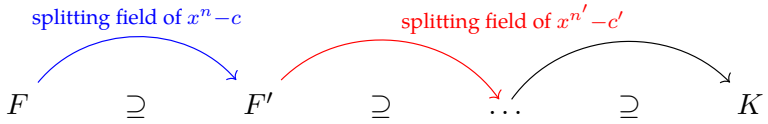
$\mathbb{Q}[\omega]$ is the splitting field of $x^2 + x + 1$ and hence $\mathbb{Q}[\omega]$ is normal and separable. Thus K is Galois over $\mathbb{Q}$.

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



Example 3.5.1. 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 3.8 Radical extensions
A field K is said to be a radical extension of a field F if there is a chain of fields

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_t = K$$

such that for each $i = 1, 2, \ldots, t$. $F_i = F_{i-1}(u_i)$ 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.

Definition 3.9 Solvable groups
A group G is said to be solvable if it has a "chain" of subgroups

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_{n-1} \triangleright G_n = \langle e \rangle$$

and G_{i-1}/G_i is abelian.

Example 3.5.2. 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 3.14
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

$$S_n = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = \langle 1 \rangle.$$

Let $(r\,s\,t)$ be any 3-cycle in S_n and let α, β be any element of $\{1, 2, \ldots, n\}$ 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, $\forall i \in \{1, 2, \ldots, n\}$, G_i contains all the 3-cycles. This contradicting the fact that S_n is solvable. □

Theorem 3.15
Every homomorphic image of a solvable group G is solvable.

Proof. Let G be a solvable group. Then there exists a chain of groups

$$G = G_0 \supseteq G_1 \ldots \supseteq G_n = \langle e\rangle$$

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

$$f(G) = f(G_0) \supseteq f(G_1) \ldots \supseteq f(G_n) = \langle e\rangle$$

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

$$\forall c, d \in f(G_{i-1}), \exists a, b \in G_{i-1} \quad s.t.\ f(a) = c \text{ and } f(b) = d.$$

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. □

Definition 3.10
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 $\zeta, \zeta^2, \ldots, \zeta^n$ are the n distinct n-th roots of unity.

Example 3.5.3. Consider $x^4 - 1 \in \mathbb{Q}[x]$. The 4-th roots of unity in $\mathbb{C} = \{1, -1, i, -1\} = \langle i\rangle$. i and $-i$ are primitive 4-th root of unity in $\mathbb{C}$.

Example 3.5.4. 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 3.16
Every homomorphic image of a solvable group G is solvable.

Proof. Let G be a solvable group. Then there exists a chain of groups

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \langle e \rangle$$

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

$$f(G) = f(G_0) \supseteq f(G_1) \supseteq \ldots \supseteq f(G_n) = \langle e \rangle$$

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. □

Lemma 3.4
Let F be a field and ζ a primitive n-th root of unity of F. Then F contains a primity 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 $\{\zeta^k, \zeta^{2k}, \ldots, \zeta^{nk}\}$ are all distinct and roots of $x^d - 1_F$. Thus ζ^k is a primitive d-th root of unity. □

Example 3.5.5. 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.

$$f'(x) = \frac{d}{dx}2x^5 - 10x + 5 = 10x^4 - 10 \Longrightarrow \text{roots are } \pm 1, \pm i$$

$$f''(x) = \frac{d}{dx}10x^4 - 10 = 40x^3 \Longrightarrow \text{the root is } 0.$$

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

$$|\operatorname{Gal}_{\mathbb{Q}} K| = [K : \mathbb{Q}]$$

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,

◀