1

Groups

Definition 1.1
A group $(G, *)$ is a set G, together with a binary operator $*$ such that

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

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 1.0.1. Consider (a, b) to be a fixed point on the 2-dimensional cartesian plane $\mathbb{R}^2$, we define a translation map $T_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2$ such that

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

we again define $G = \{T_{a,b} \mid a, b \in \mathbb{R}\}$. Show that $(G, \circ)$ is a group under function composition.

Solution 1. (Closure) 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

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

which closed under G.

2. ()

◀

Theorem 1.2
The following statements are equivalent.

1. Every subgroup of a cyclic group (multiplicative group) is cyclic.
2. If $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n.
3. For each positive divisor $k|n$, $\langle a\rangle$ has exactly one subgroup of order k. $\langle a^{n/k}\rangle$ if multiplicative group, $\langle \frac{n}{k}a\rangle$ if additive group.

Proof. Let G be a cyclic group and H be a subgroup of G. We need to show that H is also cyclic. Example: $H = \langle a^m\rangle$ s.t. m is the least positive integer.

By randomly pick integer $b \in H$, $b = a^k, k \in \mathbb{Z}^+$. By division algorithm, $k = qm + r$, where $0 \leq r < m$.

$$\begin{aligned} b = a^k = a^{qm+r} = (a^m)^q a^r &\Rightarrow a^r = (a^m)^{-q} b \in H \\ &\Rightarrow a^r \in H, \quad 0 \leq r < m \\ &\Rightarrow r = 0 \end{aligned}$$

□

1.1 Finite groups and Subgroups

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 1.3 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.

Theorem 1.4 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 1.5 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 1.2 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 1.3 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 1.4 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 1.5 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 1.6
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

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

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

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

and we are done. □

1.3 Permutation

Definition 1.6
A permutation of a set A is a function from A to A that is both one-to one and onto. A permutation group of a set A is the set of permutations of A that forms a group under function composition

1.3.1 Dihedral Group

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

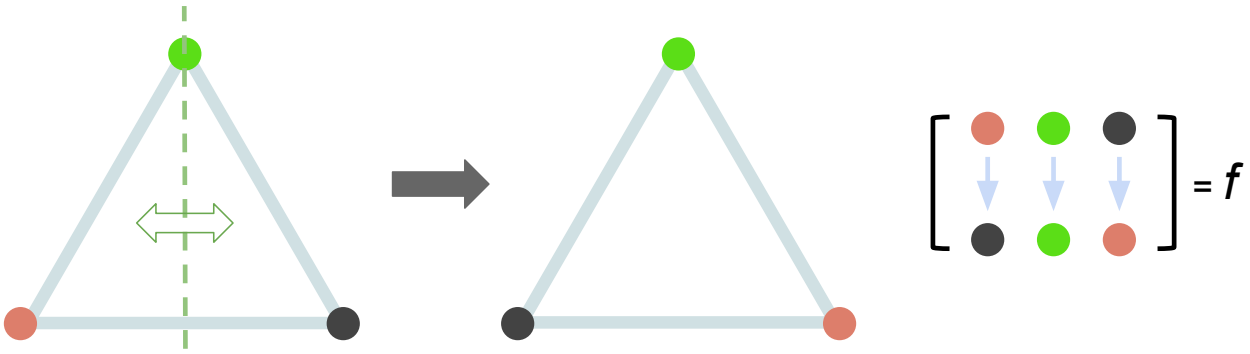


Figure 1.1: The group action f on dihedral group D_3 with order 6. f is a horizontal flip.

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.

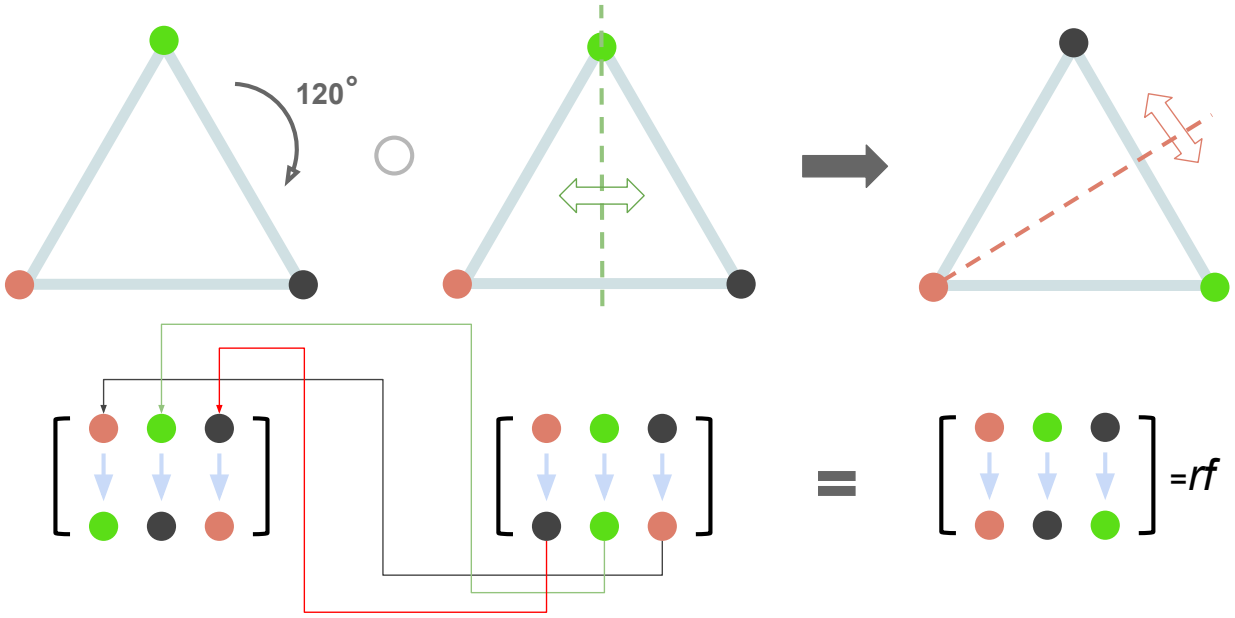


Figure 1.2: The composition of $120\,\mathrm{deg}$ rotation with horizontal reflection form another reflection line at vertice

Lemma 1.6
Dihedral group D_3 is isomorphic to S_3.

1.4 Sylow's theorem

Theorem 1.7
$C_5 \times C_2$ and C_{10} are two isomorphism classes.

Proof. From the *Third Sylow's theorem*, the number of Sylow 5-groups divides 2 and is $1(mod5)$, so there is only one Sylow 5-group. And there is a normal subgroup $K \trianglelefteq G$ such that $|K| = 5$. □

1.5 Isomorphism

Example 1.5.1. The group $U(10)$ is not isomorphic to $U(12)$.

Theorem 1.8 Cayley's theorem
Every group is isomorphism to a group of permutation.

1.6 Automorphisms

Definition 1.7
An isomorphism from a group G onto itself is called an automorphism.

Example 1.6.1. 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 1.6.2. Compute Aut$(\mathbb{Z}_{10})$.

Solution For any $\alpha \in$ 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, Aut$(\mathbb{Z}_{10})$ is isomorphic to $U(10) = \{1, 3, 7, 9\}$. ◀

Definition 1.8 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 1.9
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

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

□

1.7 Cosets

Example 1.7.1. 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 $(G, \oplus)$. All **left cosets** of G with respect to H are $\{H, 1 \oplus H, 2 \oplus H\}$ where

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

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

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

1.8 Normal subgroups, Quotient groups

1.8.1 Normal subgroups

Definition 1.9 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 1.8.1. 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

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

Theorem 1.10 Orbit-Stabilizer theorem
For any group action $\phi : G \to \text{Permutation}(S)$, and for any $s \in S$,

$$|\text{Orb}(s)| \cdot |\text{Stab}(s)| = |G|. \tag{1.8}$$

Theorem 1.11
The group of rotations of a cube is isomorphic to S_4.

1.9 Group homomorphisms

Definition 1.10
A group homomorphism is a map $f : (G, \diamond_G) \to (H, \bullet_H)$ that respects binary operations:

$$f(a) \bullet_H f(b) = f(a \diamond_G b) \quad \forall a, b \in G \tag{1.9}$$

1.10 Tutorials

Exercise 1.10.1 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 $G = \mathbb{R}^\times$ by letting $a * b = \sqrt{ab} \quad \forall a, b \in \mathbb{R}^\times$.
4. Let $*$ defined on $G = \mathbb{Z}$ by letting $a * b = \max\{a, b\} \quad \forall a, b \in \mathbb{Z}$.

Exercise 1.10.2 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 1.10.3 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 1.10.4 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 1.10.5 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 1.10.6 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 1.10.7 Show that if every element of the group G is its own inverse, then G is abelian.

Exercise 1.10.8 Show that every group with identity e and $x \cdot x = x$ for all $x \in G$ is abelian.

Exercise 1.10.9 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 1.10.10 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 1.10.11 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 1.10.12 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 1.10.13 Show that a group with no proper nontrivial subgroup is cyclic.

Exercise 1.10.14 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 1.10.15 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. $\mathbf{Z}_{36}$
2. $\mathbf{Z}_{60}$

Exercise 1.10.16

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 1.10.17

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 1.10.18 Find the conjugacy classes of dihedral group D_8.

Exercise 1.10.19 Show that a group that has only finite number of subgroups must be a finite group.

Exercise 1.10.20 Find all cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.

Exercise 1.10.21 Compute the quotient group $\mathbb{Z}_{12}/\langle 2 \rangle$.

Exercise 1.10.22 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 1.10.23 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 1.10.24 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 1.10.25 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 1.10.26 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 1.10.27 Find $ker(\phi)$ for map $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ such that $\phi(1) = 8$.

Exercise 1.10.28 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 1.10.29 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 1.10.30 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 1.10.31 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 1.10.32 Find (up to isomorphism) all abelian groups of order 45.

Exercise 1.10.33 Show that any group of order p^2 is abelian.

Exercise 1.10.34 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 1.10.35 If $H, K \leq G$, show that $H \cap K \leq G$.

Exercise 1.10.36 If $N \lhd G$ and $H \leq G$, show that $NH \leq G$.

Exercise 1.10.37 If $N_1, N_2 \lhd G$, show that $N_1 \cap N_2 \lhd G$.

Exercise 1.10.38 If $N \lhd G$ and $H \leq G$, show that $H \cap N \lhd G$.

2

Rings

2.1 Polynomial rings

Definition 2.1
Let R be a commutative ring. We define

$$R[x] = \{r_n x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \mid r_i \in R\}. \tag{2.1}$$

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.

2.2 Factorization of polynomials

Theorem 2.1 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 2.2.1. 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 2.2 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 2.2 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 2.2.2. 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 2.2.3. 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,

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

Thus, $2x^3 + 3x^2 - 7x - 5 = (x+1)(x+2)(2x-3)$ in $\mathbb{Z}_{11}[x]$. ◀

2.2.1 Irreducibility tests

Theorem 2.3 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 $\mathbb{Q}$.

Theorem 2.4 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 $\mathbb{Q}$.

Theorem 2.5
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 □

2.3 Integral Domains

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

$$ab = 0 \tag{2.4}$$

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 2.3
A ring with unity 1 having no zero divisors is an integral domain.

Lemma 2.1
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 $a^{-1}\,ab = a^{-1} \cdot 0 \implies b = 0$. Therefore, F has no zero divisors, and so F is an integral domain. □

Definition 2.4
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 2.3.1. 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. ◀

Theorem 2.6
A finite integral domain is a field

Proof. Let R be a finite domain. For instance,

$$R = \{r_1, r_2, \ldots, r_n\}.$$

We want to show that every nonzero element is invertible. Let $r \in R, r \neq 0$.

Consider the products $rr_1, rr_2, \ldots, rr_n$. If $rr_i = rr_j$, then $r_i = r_j$ by left cancellation rule. Therefore, the rr_i are distinct. Since there are n of them, they must be exactly all the elements of R:

$$R = \{rr_1, rr_2, \ldots, rr_n\}.$$

Then $1 \in R$ equals rr_i for some integer i, so r is invertible. □

2.4 Principal Ideal Domain

Definition 2.5
An integral domain R is called a **principal ideal domain** (or **PID**) if every ideal in R is principal.

Example 2.4.1. The integers $\mathbb{Z}$ and polynomial rings over fields are principal ideal domains.

Theorem 2.7
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 $f(x) = q(x)\, g(x) \Longrightarrow f(x) \in \langle g(x) \rangle$. □

2.5 Unique Factorization Domain

Definition 2.6
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 2.8
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. □

3

Fields

3.1 Extenstion Fields

3.1.1 Simple Extension

Example 3.1.1. $\mathbb{Q}[\sqrt{3}]$ is isomorphic to $\mathbb{Q}[\sqrt{3}]/\langle x^2-3\rangle$

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,

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

□

3.1.2 Algebraic Extension

Definition 3.1 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 3.1.2. $\mathbb{C}$ 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 3.1
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 3.2
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

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

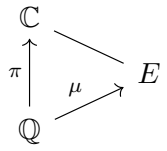
which is also finite. □

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 $F \Longrightarrow \omega$ 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 3.1.3.

$$\mathbb{Q}(i, -i) = \mathbb{Q}(i)$$

Example 3.1.4.

$$\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3})(i)$$

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 3.1.5. 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 3.1.6 (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 3.2 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 3.3
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.
$$\begin{cases} a \cdot 1_R - b \cdot 1_R = (a - b) \cdot 1_R \in \mathfrak{P} \\ a \cdot 1_R b \cdot 1_R = ab\, 1_R \in \mathfrak{P} \end{cases}$$
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 3.4
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 3.5 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 Fundamental Theorem of Galois theory

Definition 3.3 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 3.4.1.

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

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.

We state that $K = E(V)$ for some $V \in K$. □