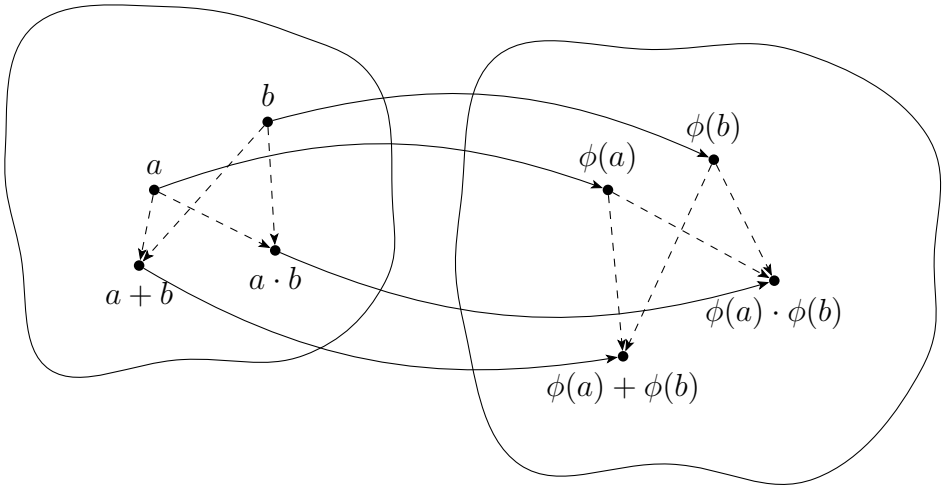
MODERN ALGEBRA



Daoud Siniora

September 8, 2025

Contents

Introduction

Modern Algebra or Abstract Algebra is a branch of mathematics concerned with the study of algebraic structures such as groups, rings, fields, vector spaces, and modules. An algebraic structure consists of a set together with a collection of operations on the set, such as addition and multiplication, where the set and the operations satisfy certain axioms.

Elementary algebra deals with manipulations of variables or symbols in an equation towards finding all solutions of the equation. The roots of Algebra dates back to the ancient Babylonians (1700 BC - 500 BC) in Mesopotamia who developed formulas to solve linear and quadratic equations. Babylonian mathematical works were written on clay tablets. Their work covered the Pythagorean theorem. The Babylonian numeral system of mathematics was a sexagesimal (base 60) system. Diophantus (3rd century AD) was an Greek mathematician living in Alexandria and the author of a series of books called Arithmetica studying methods for solving equations.

In Baghdad, Iraq, Muhammad ibn Mūsā al-Khwārizmī (830) who was working at the House of Wisdom wrote "The Compendious Book on Calculation by Completion and Balancing" which established algebra as a mathematical discipline that is independent of geometry and arithmetic: the two main subfields of mathematics before the 16th century. The word "algebra" is derived from the Arabic word "aljabr" that appears in the title of al-Khawarizmi's book and it means completion or restoring and it refers to the method of passing one term of the equation from one side to the other, after changing its sign. In surgery, aljabr refers to setting broken or dislocated bones.

Before the 19th century, algebra meant the study of the solution of polynomial equations. During the 19th century complex problems arose in various fields of mathematics and as a result solution methods were developed to tackle such problems which in their turn have led to the birth of group theory. Group theory has three main historical sources: number theory, the theory of algebraic equations, and geometry. In number theory, Euler and Gauss worked on modular arithmetic and additive and multiplicative groups. In the quest for general solutions of polynomial equations of high degree, results about permutation groups were obtained by Lagrange, Ruffini, and Abel. In 1832 the French mathematician Évariste Galois (1811 – 1832) coined the term"group" and established a connection, now known as Galois theory, between group theory and field theory. Galois was working on the problem of deciding whether a given equation could be solved using radicals (meaning square roots, cube roots, and so on, together with the usual operations of arithmetic). By using the group of all permutations of the solutions, now known as the Galois group of the equation, Galois showed whether or not the solutions could be expressed in terms of radicals. Arthur Cayley and Augustin Louis Cauchy pushed these investigations further

by creating the theory of permutation groups. In geometry, groups first became important in projective geometry and, later, non-Euclidean geometry. Group theory has been ever growing, giving rise to the birth of abstract algebra in the early 20th century.

Other pioneers in the field include Emmy Noether (1882 – 1935), David Hilbert (1862 – 1943), Emil Artin (1898 – 1962), and Alexander Grothendieck (1928 - 2014).

Group theory has applications in other fields of mathematics such as Galois theory, algebraic geometry, algebraic topology, algebraic number theory, harmonic analysis, and combinatorics. In physics, group theory is used in quantum mechanics, particle physics, and gauge theory. Other applications of group theory are in the fields of chemistry and cryptography.

A mathematician specialized in algebra is called an *algebraist*.

This set of notes is based on the book "*Contemporary Abstract Algebra*" by Joseph Gallian.

Chapter 1

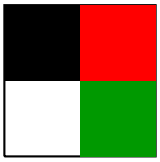
Dihedral Groups

Groups are algebraic structures composed of a set of elements equipped with a binary operation satisfying certain properties. To motivate the idea, let us examine some examples. Consider the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition modulo 4 and construct its *Cayley table*.

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

1.1 Symmetries of a Square

Another example of an algebraic structure is the set of symmetries of a square. Suppose we remove a square region from the plane, and then we return it back in such a way that it occupies the original space it was occupying.



We can do this motion in exactly 8 different ways listed in the set below.

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, L\}.$$

- The motion R_θ is rotating the square by θ degrees counter clockwise.
- The motion H is a reflection of the square about the horizontal axis.
- The motion V is a reflection of the square about the vertical axis.
- The motion D is a reflection of the square about the main diagonal.
- The motion L is a reflection of the square about the non-main diagonal.

We can compose two motions by applying one after the other to obtain a single motion in the same fashion we compose functions. Starting with the square above, then applying a

motion X and after that applying on the outcome a motion Y is represented by writing $Y \circ X$. Check the following computations.

- $H \circ R_{90} = D$
- $R_{90} \circ R_{180} = R_{270}$
- $R_{180} \circ H = V$
- $R_{90} \circ H = L$
- $R_{180} \circ R_{90} = R_{270}$
- $D \circ V = R_{90}$
- $V \circ V = R_0$
- $D \circ R_{90} = V$
- $V \circ D = R_{270}$

Cayley table of D_4

$\circ$	R_0	R_{90}	R_{180}	R_{270}	H	V	D	L
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	L
R_{90}	R_{90}	R_{180}	R_{270}	R_0	L	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	L	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	L	V	H
H	H	D	V	L	R_0	R_{180}	R_{90}	R_{270}
V	V	L	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	L	H	R_{270}	R_{90}	R_0	R_{180}
L	L	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Definition 1.1.1. (Dihedral Group)

The *dihedral group* D_n of order $2n$ is the group of all symmetries of a regular polygon with n sides. (The group D_n contains n rotations and n reflections.)

We may think of rotations and reflections of a regular polygon as functions from the shape to itself preserving distances. More generally, we define a symmetry of any area A of the plane as follows.

Definition 1.1.2. (Plane Symmetry)

Let $A \subseteq \mathbb{R}^2$. A *plane symmetry* of A is a bijection $f : A \to A$ which preserves distances; that is, for any points $a, b \in A$ we have that

$$d(a, b) = d(f(a), f(b)).$$

Chapter 2

Groups

The British mathematician *Arthur Cayley* introduced around the year 1850 the notion of an abstract group, and it took another quarter century before the idea firmly took hold.

Definition 2.0.1. (Binary Operation)

A *binary operation* on a set G is a function $f : G \times G \to G$. That is, for every pair $(g, h) \in G \times G$, we assign exactly one element gh in G (closed operation).

Remark. For an element $(g, h) \in G \times G$, we denote its image under a given binary operation f in several ways: $f(g, h) = gh$ or $g \cdot h$ or $g \circ h$ or $g * h$ or $g + h$.

Observe that if G is a finite, say $|G| = n$, then there are $n^{(n^2)}$ different binary operations on G. For example, there are 16 binary operations on the set $\{a, b\}$, and there are 19 683 binary operations on the set $\{a, b, c\}$. Some of the binary operations on a set are very special and we give them the name "groups" as described by the definition below.

2.1 Definition of a Group

Definition 2.1.1. (Group)

A *group* is a set G together with a (closed) binary operation such that the following axioms are satisfied, called the *group axioms*.

(i) For any $g, h, k \in G$, we have that $(gh)k = g(hk)$. (Associativity)

(ii) There exists an element $e \in G$ such that $eg = g = ge$ for all $g \in G$. (Identity)

(iii) For any $g \in G$, there exists $h \in G$ such that $gh = e = hg$. (Inverses)

Remark. A set equipped with a binary operation is called a *magma*. A set with an associative binary operation is called a *semigroup*. A set with an associative binary operation and an identity element is called a *monoid*.

Definition 2.1.2. (Abelian Group)

A group G is *abelian* iff for every $g, h \in G$ we have that $gh = hg$.

Definition 2.1.3. (Order of a Group)

The *order* of a group G is the number of elements in G. We denote the order of G by $|G|$.

Example 2.1 (Examples of groups)**.**

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
- $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^+, \cdot)$.
- $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$.
- The set $\{1, -1, i, -i\}$ with complex multiplication.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

- The complex unit circle $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ with complex multiplication.
- The set of all 2×2 matrices under matrix addition.
- The *general linear group* $\mathrm{GL}_n(\mathbb{R})$ of invertible $n \times n$ real matrices with matrix multiplication.
- The *special linear group* $\mathrm{SL}_n(\mathbb{R})$ of $n \times n$ real matrices with determinant 1 with matrix multiplication.
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition modulo n. Below is 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

- The group of units $U(n) = U_n = \{k \in \mathbb{Z} \mid 1 \leq k < n \text{ and } \gcd(k, n) = 1\}$ under multiplication modulo n. Below the Cayley table of $U_8 = \{1, 3, 5, 7\}$.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

- The dihedral group D_n of order $2n$.
- The n-dimensional space $\mathbb{R}^n$ with componentwise addition.

- The underlying set of a vector space together with vector addition is an abelian group.
- The set of all complex nth roots of unity under complex multiplication.

$$\{z \in \mathbb{C} \mid z^n = 1\} = \left\{ \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \mid k = 0, 1, \ldots, n-1 \right\}.$$

Example 2.2 (Non-examples of groups)**.** The following are not groups.

- $(\mathbb{Z}, \cdot)$.
- $(\mathbb{Z}, -)$.
- $\{1\} \cup \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$ under multiplication.
- $\mathbb{Z}_6$ under multiplication modulo 6.
- The integers $\mathbb{Z}$ under multiplication modulo 5.
- The set of all 2×2 matrices under matrix multiplication.

Theorem 2.1.4.

In a group, the identity element is unique. Moreover, every element has a unique inverse.

Proof. Let G be a group and suppose that e_1 and e_2 are both identity elements of G. Since e_1 is an identity element, it follows that $e_1 e_2 = e_2$, and since e_2 is an identity element, we get that $e_1 e_2 = e_1$. Thus,

$$e_1 = e_1 e_2 = e_2.$$

Next, suppose that $g \in G$ has h and k as additive inverses. Then,

$$h = he = h(gk) = (hg)k = ek = k.$$

Therefore, g has a unique additive inverse. ■

Notation. In a group, we denote the unique inverse of an element g by g^{-1}.

Exercise 2.3. Find all groups with underlying set $\{e, a, b\}$ where e is the identity element.

Lemma 2.1.5. (Cancellation)

Let G be a group and let $a, b, c \in G$.
If $ab = ac$, then $b = c$. And if $ba = ca$, then $b = c$

2.2 The Order of a Group Element

Let G be a group and $g \in G$. Let n be a *positive* integer.

- We define $g^0 = e$.

- We define g^n to be the element in G obtained by multiplying g with itself n times.
- We define $g^{-n} = (g^{-1})^n$. That is, g^{-n} is the element obtained by multiplying g^{-1} with itself n times.

Lemma 2.2.1.

Let G be a group and $g \in G$. For any $m, n \in \mathbb{Z}$ we have that

- $g^m g^n = g^{m+n}$,
- $(g^m)^n = g^{mn}$, *and*
- $(g^m)^{-1} = (g^{-1})^m$.

Lemma 2.2.2. (Socks-Shoes Property)

For any elements g and h in a group G we have that

$$(gh)^{-1} = h^{-1}g^{-1}.$$

Proof. Let g and h be elements of a group G. We check, using associativity, that the inverse of the element gh is indeed the element $h^{-1}g^{-1}$ by showing that their product is the identity element.

$$(gh)(h^{-1}g^{-1}) = ((gh)h^{-1})g^{-1} = (g(hh^{-1}))g^{-1} = (ge)g^{-1} = gg^{-1} = e.$$

■

Notation for a multiplicative group and an additive group.

Multiplication	gh or $g \cdot h$	Addition	$g + h$
Identity or one	e or 1	Zero	0
Multiplicative inverse	g^{-1}	Additive inverse	$-g$
Power	g^n	Multiple	ng
Quotient	gh^{-1}	Difference	$g - h$

Definition 2.2.3. (Order of a Group Element)

The *order* of an element g in a group is the least positive integer n such that $g^n = e$. We denote the order of g by $|g|$. If no such integer exists, we say that g has *infinite order*.

Remark. To find the order of an element g of a group, you need only compute the *sequence of products*

$$g, g^2, g^3, g^4, \ldots$$

until you hit the identity element for the first time. Thus, if k is a positive integer such that $g^k = e$, then $|g| \leq k$.

Example 2.4.

- In U_{15} we have that
  $|7| = 4$, $|11| = 2$, $|1| = 1$, $|2| = 4$, $|4| = 2$, $|8| = 4$, $|13| = 4$, $|14| = 2$.

- In $\mathbb{Z}_{10}$ we have that
  $|2| = 5, |0| = 1, |7| = 10, |5| = 2, |6| = 5$.
- In $(\mathbb{Z}, +)$ we have that
  $|0| = 1$ and every nonzero integer has infinite order.

Lemma 2.2.4.

Let g be a group element and $k \in \mathbb{Z}^+$. If $g^k = e$, then $|g|$ divides k.

Proof. Suppose that $g^k = e$ and put $|g| = n$. By the division algorithm, there are unique integers q and r such that $k = qn + r$ and $0 \leq r < n$. Now,

$$e = g^k = g^{qn+r} = g^{qn}g^r = (g^n)^q g^r = e^q g^r = eg^r = g^r.$$

Thus, $g^r = e$. Since $0 \leq r < n$ and n is the order of g, we get that $r = 0$, otherwise, if $0 < r < n$, we contradict that n is the least positive integer such that $g^n = 0$. As r must be 0, it follows that $k = qn$, and so n divides k as desired. ■

Definition 2.2.5. (Involution)

An element of a group which has order 2 is called an *involution.*

So an involution is a nonidentity group element g that is its own inverse, that is, $g^{-1} = g$.

Lemma 2.2.6.

A group whose all nonidentity elements are involutions is abelian.

Lemma 2.2.7.

Let G be a finite group and $g \in G$.
(i) If $|g| = km$ for some positive integers k and m, then $|g^k| = m$.
(ii) If G is a nontrivial group, then it contains elements of prime order.

Chapter 3

Subgroups

Some subsets of a given group are themselves groups, we give them a special name.

3.1 Definition of Subgroups

Definition 3.1.1. (Subgroup)

A subset H of a group G is a *subgroup* of G if H itself is a group under the operation of G. We write $H \leq G$ to say that H is a subgroup of G.

Clearly, G is a subgroup of itself. When $H \leq G$ and $H \neq G$, we say that H is a *proper subgroup* of G and we write $H < G$. The singleton $\{e\}$ is a subgroup of G and it is called the *trivial subgroup* of G. If $H \leq G$ and $H \neq \{e\}$, we say H is a *nontrivial subgroup* of G.

Example 3.1. Here are examples of subgroups.

- $\mathbb{Q}^* \leq (\mathbb{R}^*, \cdot)$.
- $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ is a subgroup of $(\mathbb{R}^*, \cdot)$.
- The subset $\{1, -1, i, -i\}$ is a subgroup of $(\mathbb{C}^*, \cdot)$.
- $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.
- Let n be a positive integer. Define the set $n\mathbb{Z} = \{k \cdot n \mid k \in \mathbb{Z}\}$, that is, $n\mathbb{Z}$ is the set of all multiples of n. For example, $2\mathbb{Z}$ is the set of all even integers. Then $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.
- The subset $\{R_0, R_{90}, R_{180}, R_{270}\}$ is a subgroup of the dihedral group D_4.
- Also $\{R_0, H\}$ is a subgroup of D_4.

Lemma 3.1.2.

Suppose that H is a subgroup of G. Then the identity element of H is the same element as the identity element of G.

Proof. Let e_H be the identity element of the subgroup H and e_G be the identity element of the group G. Since both e_G and e_H are elements of G and e_G is the identity element of G we know that $e_H e_G = e_H$. Since e_H is the identity element of H, we know that $e_H e_H = e_H$. Therefore, $e_H e_G = e_H e_H$. By cancellation, we obtain that $e_G = e_H$. ■

3.2 Subgroup Tests

Suppose that G is a group and $H \subseteq G$. We say that H is closed under the operation if whenever a and b are in H, then $ab \in H$ (in additive notation, whenever a and b are in H, then $a+b \in H$). Similarly, H is closed under taking inverses if whenever $a \in H$, then $a^{-1} \in H$ (in additive notation, whenever $a \in H$, then $-a \in H$).

Theorem 3.2.1. (Two-Step Subgroup Test)

Let H be a nonempty subset of a group G. If H is closed under the operation and under taking inverses, then H is a subgroup of G.

Proof. Let G be a group and let $H \subseteq G$ be a nonempty subset. By assumption, the operation on H is closed and every element in H has an inverse. Moreover, the operation is associative on H as it is already associative on G. It remains to check that $e \in H$. Since $H \neq \emptyset$, there is an element $h \in H$. Since H is closed under inverses, the element $h^{-1} \in H$. Finally, as H is closed under multiplication, we get that $e = hh^{-1} \in H$. Thus, H is a subgroup of G. ■

Theorem 3.2.2. (One-Step Subgroup Test)

Let H be a nonempty subset of a group G. Suppose that whenever $a, b \in H$, then $ab^{-1} \in H$. Then H is a subgroup of G.
(In additive notation, suppose that whenever $a, b \in H$, then $a - b \in H$. Then $H \leq G$.)

Proof. Since the operation is associative on G, it is also associative on H since $H \subseteq G$. Since $H \neq \emptyset$, there is an element $a \in H$. By the hypothesis of the theorem we get that $aa^{-1} \in H$, and so $e \in H$. Next, we show that H is closed under taking inverses. So let $h \in H$. Since $e, h \in H$, by the hypothesis, we get that $eh^{-1} = h^{-1} \in H$. Finally we need to show that H is closed under the operation. So choose any two elements $b, h \in H$. Then we have already shown that $h^{-1} \in H$. Now by the hypothesis applied to b and h^{-1} we get that $b(h^{-1})^{-1} \in H$. As $bh = b(h^{-1})^{-1}$, we have that $bh \in H$ as desired. Thus, H is a subgroup of G. ■

Theorem 3.2.3.

Let G be an abelian group. Then $H = \{g \in G \mid g^2 = e\}$ is a subgroup of G.

Proof. Observe that H is the subset of all elements of G of order at most 2. We will use that two-step subgroup test. Clearly, $e \in H$ and so H is a nonempty subset of G. Choose

any elements $a, b \in H$. We will show that $ab \in H$ and $a^{-1} \in H$. Be definition of H, we have that $a^2 = e$ and $b^2 = e$. Now, by associativity and commutativity we get that

$$(ab)^2 = (ab)(ab) = a(b(ab)) = a((ba)b) = a((ab)b) = a(a(bb)) = (aa)(bb) = a^2b^2 = ee = e.$$

Therefore, $(ab)^2 = e$, and so $ab \in H$. Finally, it remains to show that a^{-1} is also in H. We proceed as follows, $(a^{-1})^2 = (a^2)^{-1} = e^{-1} = e$. Thus, $a^{-1} \in H$. Therefore, H is a subgroup of G. ■

Theorem 3.2.4.

Suppose that G is an abelian group. Then $H = \{g^2 \mid g \in G\}$ is a subgroup of G.

Proof. The subset H is the set of all squares of elements of G. Clearly, $e^2 \in H$ and so $H \neq \emptyset$. Now pick two elements $a, b \in H$. We will show that $ab \in H$ and $a^{-1} \in H$. By definition of H, there are $x, y \in G$ such that $a = x^2$ and $b = y^2$. Now, $ab = x^2y^2 = xxyy = xyxy = (xy)^2$. Thus the element ab is a square and so $ab \in H$. Next, we have that $a^{-1} = (x^2)^{-1} = (x^{-1})^2$, and so a^{-1} is also a square, and so $a^{-1} \in H$ as wanted. Thus, H is a subgroup of G. ■

Theorem 3.2.5.

Suppose that G is an abelian group. The torsions $Tor(G) = \{g \in G : |g| \text{ is finite}\}$ is a subgroup of G.

Definition 3.2.6.

Suppose that H and K are subsets of a group. We define the set of products of elements in H with elements in K to be the set

$$HK = \{hk \mid h \in H, k \in K\}.$$

Theorem 3.2.7.

Let H and K be subgroups of an abelian group G. Then HK is a subgroup of G.

Proof. Since $e \in H$ and $e \in K$, we have that $e = ee \in H$. So $H \neq \emptyset$. Let $a, b \in HK$. Thus, $a = hk$ and $b = h'k'$ for some $h, h' \in H$ and $k, k' \in K$. We will show that $ab \in HK$ and $a^{-1} \in HK$. First, and as G is abelian, we get that $ab = hkh'k' = (hh')(kk') = h''k''$ where $h'' = hh' \in H$ since $H \leq G$ and similarly $k'' = kk' \in K$. Thus, $ab \in HK$. Secondly, $a^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$ since both H and K are closed under taking inverses as they are subgroups. So $a^{-1} \in HK$. Therefore, by the two-step subgroup test, HK is a subgroup of G. ■

Theorem 3.2.8. (Finite Subgroup Test)

Let H be a nonempty subset of a group G. If H is finite and closed under the operation of G, then $H \leq G$.

Proof. By the two-step subgroup test it remains to check that H is closed under taking inverses. So pick an element $h \in H$. We need to show that $h^{-1} \in H$. If $h = e$, then $e^{-1} = e \in H$. Otherwise assume that $h \neq e$ and consider the sequence of powers of h:

$$h, h^2, h^3, h^4, \ldots.$$

As H is closed under multiplication, all these powers of h belong to H. Since H is finite, the above sequence has repetitions. So there are positive integers m and n with $m < n$ such that $h^m = h^n$. Multiply both sides of the equation by the element h^{-m} to get $h^m h^{-m} = h^n h^{-m}$ and so $h^0 = h^{n-m}$. Thus $h^{n-m} = e$. Since $h \neq e$ and $n - m \geq 1$, it must be that $n - m \geq 2$. Thus, $e = h^{n-m} = hh^{n-m-1}$. This shows that $h^{-1} = h^{n-m-1}$ and since $n - m - 1 \geq 1$ and H is closed under multiplication we get that $h^{-1} = h^{n-m-1} \in H$ as desired. ■

3.3 The Center and the Centralizer

Definition 3.3.1. (Center of a Group)

The *center* of a group G is the set

$$Z(G) = \{h \in G \mid \forall g \in G(gh = hg)\}.$$

Said differently, the center of a group contains precisely those elements which commute with every element of the group. In German, center is "Zentrum". The elements of the center of a group are called *central* elements.

Theorem 3.3.2.

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

Proof. We will use the two-step subgroup test. Clearly the center is nonempty as $e \in Z(G)$ since the identity element commutes with all group elements. Now suppose that a and b belong to $Z(G)$, and so they commute with all elements of G. To show that their product ab is also in the center we need to show that the element ab commute with any member of G. Pick an arbitrary element $g \in G$. Then

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab).$$

Thus, $ab \in Z(G)$. Next, we need to show that the center is closed under taking inverses, that is, we need to show that a^{-1} commute with any element of the group. Since $a \in Z(G)$ and $g \in G$ we have that $ag = ga$. We then multiply both sides of this equation by a^{-1} from left and right to get the following.

$$\begin{aligned} ag &= ga \\ a^{-1}(ag)a^{-1} &= a^{-1}(ga)a^{-1} \\ (a^{-1}a)ga^{-1} &= a^{-1}g(aa^{-1}) \\ ega^{-1} &= a^{-1}ge \\ ga^{-1} &= a^{-1}g \end{aligned}$$

So $ga^{-1} = a^{-1}g$. Therefore, a^{-1} commute with all members of G and so $a^{-1} \in Z(G)$. Thus, $Z(G)$ is a subgroup of G. ■

Example 3.2.

- If G is an abelian group, then $Z(G) = G$.
- The center of D_4 is $Z(D_4) = \{R_0, R_{180}\}$.
- If n is even, then $Z(D_n) = \{R_0, R_{180}\}$.
- If n is odd, then $Z(D_n) = \{R_0\}$.

Definition 3.3.3. (Centralizer of an element)

The *centralizer* of an element g of a group G is the set

$$C(g) = \{h \in G \mid gh = hg\}.$$

In words, the centralizer of an element in a group is the set of all elements which commute with it. Clearly, the identity and the element itself belong to its centralizer. The centralizer of an element is always a subgroup. It should be clear that $Z(G) \subseteq C(g)$ for any element g in a group G.

Theorem 3.3.4.

Let g be in a group G. Then the centralizer $C(g)$ is a subgroup of G.

Proof. Clearly, the identity $e \in C(g)$ and so $C(g)$ is nonempty. Now, suppose that $a, b \in C(g)$. This means that both a and b commute with g. It follows that

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab).$$

Thus, ab commutes with g. Therefore, the centralizer $C(g)$ is closed under products. Next, we have that

$$a^{-1}g = a^{-1}gaa^{-1} = a^{-1}aga^{-1} = ga^{-1}.$$

Thus, $a^{-1} \in C(g)$ and so $C(g)$ is closed under taking inverses. Therefore, $C(g)$ is a subgroup of G. ■

Example 3.3. Compute all centralizers in the group D_4.

- $C(R_0) = C(R_{180}) = D_4$.
- $C(R_{90}) = C(R_{270}) = \{R_0, R_{90}, R_{180}, R_{270}\}$.
- $C(H) = C(V) = \{R_0, R_{180}, H, V\}$.
- $C(D) = C(L) = \{R_0, R_{180}, D, L\}$.

Observe that D_4 has three different subgroups of order 4.

Lemma 3.3.5.

Let G be a group. Then

$$Z(G) = \bigcap_{g \in G} C(g).$$

Proof. We know that $Z(G) \subseteq C(g)$ for every $g \in G$. Thus, $Z(G) \subseteq \bigcap_{g \in G} C(g)$. For the other containment, let $x \in \bigcap_{g \in G} C(g)$. Therefore, $x \in C(g)$ for every $g \in G$, and so x commutes with every $g \in G$ and so $x \in Z(G)$. Thus, $\bigcap_{g \in G} C(g) \subseteq Z(G)$. ■

Chapter 4

Cyclic Groups

We aim to study in this chapter a special kind of abelian groups called cyclic groups.

4.1 Definition of Cyclic Groups

The definition below gives a nice way to find subgroups in a given group.

Definition 4.1.1. (Subgroup Generated by an Element)

Let G be a group and $g \in G$. The *subgroup generated by* g in G is

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \} = \{e, g, g^{-1}, g^2, g^{-2}, g^3, g^{-3}, \ldots\}.$$

The reader needs to check that $\langle g \rangle$ is indeed a subgroup of G. Moreover, $\langle g \rangle$ is an abelian group. In additive notation, the subgroup generated by $g \in G$ is

$$\langle g \rangle = \{kg \mid k \in \mathbb{Z} \} = \{0, g, -g, 2g, -2g, 3g, -3g, \ldots\}.$$

Remark. The subgroup $\langle g \rangle$ is the smallest subgroup of G containing the element g, that is, if $g \in H \leq G$, then $\langle g \rangle \subseteq H$.

Example 4.1.

- In D_4, we have $\langle R_{90} \rangle = \{R_0, R_{90}, R_{180}, R_{270}\}$, and $\langle H \rangle = \{R_0, H\}$.
- In $(\mathbb{Z}, +)$, we have $\langle 1 \rangle = \mathbb{Z}$, $\langle -1 \rangle = \mathbb{Z}$, and $\langle 2 \rangle = \{0, 2, -2, 4, -4, \ldots\}$.
- In U_{10}, we have $\langle 3 \rangle = \{1, 3, 9, 7\} = U_{10}$, $\langle 1 \rangle = \{1\}$, and $\langle 9 \rangle = \{1, 9\}$.
- In $(\mathbb{Z}_{10}, +)$, we have $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$, and $\langle 3 \rangle = \{0, 3, 6, 9, 2, 5, 8, 1, 4, 7\} = \mathbb{Z}_{10}$.
- In $(\mathbb{C}^*, \cdot)$, we have $\langle i \rangle = \{1, i, -1, -i\}$.

When it happens that the subgroup generated by an element is the entire group we call the group cyclic.

Definition 4.1.2. (Cyclic Group)

A group G is *cyclic* if there exists an element $g \in G$ such that $G = \langle g \rangle$. We call such an element a *generator* of G.

So a group G is cyclic if there exists an element $g \in G$ such that for any element $h \in G$, there exists an integer k such that $h = g^k$.

Clearly, the subgroup $\langle g \rangle$ generated by an element $g \in G$ is cyclic. Thus, to find a cyclic group, simply pick an element in a group of your choice and consider the subgroup generated by the chosen element.

Remark. Every cyclic group is abelian and, moreover, cyclic groups play the role of building blocks for all finite abelian groups (see Chapter 11).

Example 4.2 (Non-example)**.** The group U_8 is not cyclic. To show this one needs to check that every element of $U_8 = \{1, 3, 5, 7\}$ does not generate U_8.

- $\langle 1 \rangle = \{1\} \neq U_8$.
- $\langle 3 \rangle = \{1, 3\} \neq U_8$.
- $\langle 5 \rangle = \{1, 5\} \neq U_8$.
- $\langle 7 \rangle = \{1, 7\} \neq U_8$.

Definition 4.1.3.

Let G be a group and $S \subseteq G$. The subgroup generated by S in G is the smallest subgroup of G containing S, and it is denoted by $\langle S \rangle$. Observe that $\langle S \rangle$ contains all members of S and their inverses together with all the products of these.

Example 4.3. In the dihedral group D_4 we have that

- $\langle H, V \rangle = \{R_0, R_{180}, H, V\}$.
- $\langle R_{90}, V \rangle = D_4$.

In $(\mathbb{C}, +)$ we have that $\langle 1, i \rangle = \{a + ib \mid a, b \in \mathbb{Z}\}$. This group is called the *Gaussian integers*.

4.2 Properties of Cyclic Groups

Theorem 4.2.1.

Let G be a group and let $g \in G$ be an element of infinite order. Then for any integers k, m, if $k \neq m$, then $g^k \neq g^m$.

Proof. Suppose that $g \in G$ is of infinite order. We will show the contrapositive of the statement. Assume that $g^k = g^m$. For the contrary, assume that $k \neq m$ and without loss of generality assume further that $k < m$. It follows that $g^k g^{-k} = g^m g^{-k}$, and this implies that $g^0 = g^{m-k}$. Thus, $g^{m-k} = e$ where $m - k$ is a positive integer. This contradicts that g is of infinite order. Therefore, $k = m$. ∎

Remark. For $g \in G$ of infinite order, the theorem above says that all terms in the sequence below are distinct.

$$\ldots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots$$

Thus, $\langle g \rangle$ looks like the group of integers $(\mathbb{Z}, +)$ in the sense that one may think of the element g^i in $\langle g \rangle$ as the integer i and to multiply elements g^i and g^j in $\langle g \rangle$ we get the

element $g^i g^j = g^{i+j}$ similar to when we add integers i and j in the group $(\mathbb{Z}, +)$ we get the integer $i + j$. The group of integers $(\mathbb{Z}, +)$ serves as a prototype for an infinite cyclic group.

Next, we aim to study the subgroup $\langle g \rangle$ generated by an element g in a group G where g has finite order.

Theorem 4.2.2.

Let G be a group and let $g \in G$ be an element of order n. Let k, m be any integers, then the following hold.

(i) $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.

(ii) $g^k = g^m$ *if and only if* $k \equiv m \pmod{n}$.

Proof.

(i) We will show that the two sets are subsets of each other. Clearly, we have that $\{e, g, g^2, \ldots, g^{n-1}\} \subseteq \langle g \rangle$. For the other containment let $h \in \langle g \rangle$. So $h = g^k$ for some $k \in \mathbb{Z}$. By the division algorithm, $k = qn + r$ for some $0 \leq r < n$. Then $h = g^k = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = e^q g^r = g^r$. Since $r \in \{0, 1, 2, \ldots, n-1\}$, it follows that $h = g^r \in \{e, g, g^2, \ldots, g^{n-1}\}$. Thus, $\langle g \rangle \subseteq \{e, g, g^2, \ldots, g^{n-1}\}$.

(ii) Suppose $g^k = g^m$. This implies that $g^{k-m} = e$. By Lemma 2.2.4, we obtain that n divides $k - m$, and therefore $k \equiv m \pmod{n}$.
Conversely, assume that $k \equiv m \pmod{n}$. Thus, $k - m = nl$ for some integer l. So $k = m + nl$. Now $g^k = g^{m+nl} = g^m g^{nl} = g^m (g^n)^l = g^m e^l = g^m e = g^m$, as desired.

■

Corollary 4.2.3.

Suppose that g is a group element of finite order. Then the order of the subgroup $\langle g \rangle$ is equal to the order of g. In symbols,

$$|\langle g \rangle| = |g|.$$

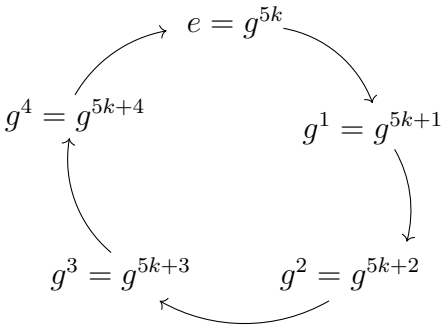
Proof. When $|g| = n$ we know from Theorem 4.2.2 that $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$. So it remains to show that all the elements $e, g, g^2, \ldots, g^{n-1}$ are distinct. Suppose for the contrary that $g^i = g^j$ where $0 \leq i < j < n$. By multiplying both sides of this equation by $(g^i)^{-1}$ it follows that $e = g^{(j-i)}$ where $0 < j - i < n$, but this contradicts that n is the order of g. ■

Remark. Suppose that $g \in G$ where $|g| = n$. Then $\langle g \rangle$ looks like $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition modulo n. To see this, first notice that both $\langle g \rangle$ and $\mathbb{Z}_n$ have n elements where $n = |g|$. Moreover, the group operation in $\langle g \rangle$ is essentially done by addition modulo n since to multiply elements g^i and g^j in $\langle g \rangle$ we obtain that

$$g^i g^j = g^{i+j} = g^{(i+j) \bmod n}.$$

This follows from Theorem 4.2.2(ii) and the fact that $(k \bmod n) \equiv k \pmod{n}$ for any $k \in \mathbb{Z}$.

Here is a diagram illustrating the subgroup $\langle g \rangle$ where $|g| = 5$. We have $\langle g \rangle = \{e, g, g^2, g^3, g^4\}$.



Corollary 4.2.4.

Let G be a group and let $g \in G$ be an element of order n. If $h \in \langle g \rangle$ has order n as well, then $\langle h \rangle = \langle g \rangle$.

Notation. A cyclic group of order n is usually denoted by C_n where

$$C_n = \{e, g, g^2, \ldots, g^{n-1}\},$$

or by $(\mathbb{Z}_n, +)$ in the additive notation.

Theorem 4.2.5.

Let G be a finite cyclic group generated by an element $g \in G$. Let k, m be any positive integers, then the following hold.

(i) $\langle g^k \rangle = \langle g^{\gcd(k,n)} \rangle$.
(ii) $|g^k| = \frac{n}{\gcd(k,n)}$.
(iii) $\langle g^k \rangle = \langle g^m \rangle$ *if and only if* $\gcd(k, n) = \gcd(m, n)$.
(iv) $|g^k| = |g^m|$ *if and only if* $\gcd(k, n) = \gcd(m, n)$.
(v) $|g^k| = |g^m|$ *if and only if* $\langle g^k \rangle = \langle g^m \rangle$.

Proof.

(i) Let $d = \gcd(k, n)$. We will show that $\langle g^k \rangle = \langle g^d \rangle$ by showing that they are subsets of each other. First, as d divides k we get that $k = di$ for some integer i. Thus, $g^k = g^{di} = (g^d)^i$. This means that $g^k \in \langle g^d \rangle = \{(g^d)^i \mid i \in \mathbb{Z}\}$, and by closure of the group operation we have that $\langle g^k \rangle \subseteq \langle g^d \rangle$. Next, by Bezout's Theorem, we know that $\gcd(k, n) = d = sk + tn$ for some integers s and t. Thus,

$$g^d = g^{sk+tn} = g^{sk} g^{tn} = g^{sk} (g^n)^t = g^{sk} e^t = g^{sk} e = g^{sk} = (g^k)^s \in \langle g^k \rangle.$$

So $g^d \in \langle g^k \rangle$, and by closure, we have that $\langle g^d \rangle \subseteq \langle g^k \rangle$. Therefore, we have verified that $\langle g^k \rangle = \langle g^d \rangle$.

(ii) Let $d = \gcd(k, n)$ and let $n = d\alpha$ for some integer α. We need to show that $|g^k| = \alpha$. First, we will show that $|g^d| = \alpha$. To see this, we first check that $(g^d)^\alpha = g^{d\alpha} = g^n = e$. Thus, $|g^d| \leq \alpha$. Now assume for the contrary that $|g^d| < \alpha$ and so there is an integer r with $1 \leq r < \alpha$ and $(g^d)^r = e$. This means that $g^{dr} = e$

where $dr < d\alpha = n$ contradicting that n is the order of g. To finalise, we use Part (i) and Corollary 4.2.3 as follows.

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

(iii) For the forward direction, suppose that $\langle g^k\rangle = \langle g^m\rangle$. Using Part (ii) we proceed as follows:

$$\begin{aligned}\langle g^k\rangle = \langle g^m\rangle &\implies |\langle g^k\rangle| = |\langle g^m\rangle| \\ &\implies |g^k| = |g^m| \\ &\implies n/\gcd(k,n) = n/\gcd(m,n) \\ &\implies \gcd(k,n) = \gcd(m,n).\end{aligned}$$

For the converse, assume that $\gcd(k,n) = \gcd(m,n)$. So certainly $\langle g^{\gcd(k,n)}\rangle = \langle g^{\gcd(m,n)}\rangle$. Using Part (i) we obtain that

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

(iv) For the forward direction, suppose that $|g^k| = |g^m|$. Using Part (ii) this implies that $n/\gcd(k,n) = n/\gcd(m,n)$ and so $\gcd(k,n) = \gcd(m,n)$. For the converse, assume that $\gcd(k,n) = \gcd(m,n)$. By Part (iii) we get that $\langle g^k\rangle = \langle g^m\rangle$ and so $|\langle g^k\rangle| = |\langle g^m\rangle|$. Finally, by Corollary 4.2.3, we deduce that $|g^k| = |g^m|$.

■

We next present important consequences of Theorem 4.2.5.

Corollary 4.2.6.

The order of any element in a finite cyclic group H divides the order of the group H.

Proof. Suppose that H is a finite cyclic group of order n. So $H = \langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ for some element $g \in H$ of order n. Choose an element $h \in \langle g\rangle$, we need to show that $|h|$ divides n. Since $h \in \langle g\rangle$ it follows that $h = g^k$ for some integer $0 \leq k < n$. If $k = 0$, then $h = e$ and so $|e| = 1$ and 1 divides n. Otherwise, $1 \leq k \leq n-1$. By Theorem 4.2.5(ii) we get that $|h| = |g^k| = \frac{n}{\gcd(k,n)}$, which implies that $n = |g^k| \cdot \gcd(n,k) = |h| \cdot \gcd(n,k)$ which shows that $|h|$ divides n. ■

Corollary 4.2.7.

Let G be a finite cyclic group of order n and let $g \in G$ be a generator. For $k \in \mathbb{Z}$, we have that $\langle g^k\rangle = \langle g\rangle$ if and only if $\gcd(k,n) = 1$. That is, the generators of the cyclic group G are precisely the elements g^k where k is coprime with n.

Corollary 4.2.8.

The set of all generators of the group $(\mathbb{Z}_n, +)$ is exactly U_n.

Example 4.4. The elements $1, 5, 7, 11$ are the generators of $\mathbb{Z}_{12}$ under addition modulo 12.

Example 4.5. Let G be a group and $g \in G$ with $|g| = 30$.

- $\langle g^{26} \rangle = \langle g^{\gcd(26,30)} \rangle = \langle g^2 \rangle = \{e, g^2, g^4, g^6, \ldots, g^{28}\}$.
- $|g^{26}| = \frac{30}{\gcd(26,30)} = \frac{30}{2} = 15$.
- $\langle g^{17} \rangle = \langle g^{\gcd(17,30)} \rangle = \langle g \rangle = \{e, g, g^2, g^3, \ldots, g^{29}\}$.
- $|g^{17}| = \frac{30}{\gcd(17,30)} = \frac{30}{1} = 30$.
- $\langle g^{18} \rangle = \langle g^{\gcd(18,30)} \rangle = \langle g^6 \rangle = \{e, g^6, g^{12}, g^{18}, g^{24}\}$.
- $|g^{18}| = |g^6| = \frac{30}{\gcd(6,30)} = \frac{30}{6} = 5$.

4.3 Fundamental Theorem of Cyclic Groups

Our next goal is to investigate the structure of subgroups of a given cyclic group. How many subgroups of a cyclic group are there? How do they look like? We will see that in a cyclic group all of its subgroups are also cyclic. Furthermore, in the case of finite cyclic groups there is a unique subgroup for every divisor of the group order.

Theorem 4.3.1. (Fundamental Theorem of Cyclic Groups)

(i) Any subgroup of a cyclic group is cyclic.
(ii) Suppose that $G = \langle g \rangle$ is a finite cyclic group of order n. Then,
  (a) If $H \leq G$, then $|H|$ divides $|G|$.
  (b) If k divides n, then there is exactly one subgroup of G of order k, namely, the subgroup $\langle g^{\frac{n}{k}} \rangle$.

Proof.

(i) Let G be a (finite or infinite) cyclic group and let H be a subgroup of G. As G is cyclic we have that $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ for some element $g \in G$. If H is the trivial subgroup, i.e. $H = \{e\}$, then it is clear that H is cyclic as $H = \langle e \rangle$. Otherwise, H is nontrivial. Let m be the least positive integer such that $g^m \in H$. We claim that

$$H = \langle g^m \rangle = \{(g^m)^k \mid k \in \mathbb{Z}\} = \{e, g^m, g^{-m}, g^{2m}, g^{-2m}, g^{3m}, g^{-3m}, \ldots\}.$$

As $g^m \in H$, we get by closure that $\langle g^m \rangle \subseteq H$. To show the other inclusion, pick an arbitrary element $h \in H$. Since $H \subseteq G$ we have that $h = g^k$ for some $k \in \mathbb{Z}$. Next apply the division algorithm to k and m to obtain $q, r \in \mathbb{Z}$ such that $k = qm + r$ and $0 \leq r < m$. It follows that $h = g^k = g^{qm+r} = g^{qm} g^r$ and so $g^r = g^{-qm} h$. As both h and g^{-qm} are both in H and H is a group it follows by closure of the operation that their product g^r is also in H. If $r > 0$, then this contradicts our choice of m since $r < m$. Thus, r must be 0, and so $k = qm$. Thus, $h = g^k = g^{qm} = (g^m)^q$ and so $h \in \langle g^m \rangle$. We have established that $H \subseteq \langle g^m \rangle$ and therefore $H = \langle g^m \rangle$ showing that H is cyclic generated by the element g^m.

(ii) Let $G = \langle g \rangle$ be a finite cyclic group of order n. By Corollary 4.2.3 we get that $|g| = n$.

(a) Suppose that H is a subgroup of G. If H is the trivial subgroup, then the result follows trivially. Otherwise, by Part (i) we know that H is cyclic and $H = \langle g^m \rangle$ for some positive integer m. Using Corollary 4.2.3 and Theorem 4.2.5(ii) we obtain that

$$|H| = |\langle g^m \rangle| = |g^m| = n/\gcd(m, n).$$

Thus, $|G| = n = |H| \cdot \gcd(m, n)$. That is, $|H|$ divides $|G|$.

(b) Suppose that k is a divisor of n and let $n = k\alpha$ for some integer α. We need to show that the subgroup $\langle g^\alpha \rangle$ is the only subgroup of G of order k. First,

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

Next, suppose that K is a subgroup of G of order k as well. We know that K is cyclic and $K = \langle g^m \rangle$ for some positive integer m. So $|\langle g^\alpha \rangle| = k = |\langle g^m \rangle|$ and so $|g^\alpha| = |g^m|$. By Theorem 4.2.5(v) we deduce that $\langle g^\alpha \rangle = \langle g^m \rangle = K$. Therefore, $\langle g^\alpha \rangle$ is the only subgroup of G of order k.

■

Since $\mathbb{Z}_n = \langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\}$, under addition modulo n, we get the following.

Corollary 4.3.2.

The subgroups of $(\mathbb{Z}_n, +)$ are precisely the sets $\langle k \cdot 1 \rangle$ where k is a divisor of n. The subgroup $\langle k \cdot 1 \rangle$ has n/k many elements.

Exercise 4.6. Find all subgroups of $\mathbb{Z}_{30}$ and draw the lattice of subgroups of $\mathbb{Z}_{30}$.

The divisors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$. Consequently the subgroups are:

- $\langle 1 \rangle = \mathbb{Z}_{30}$,
- $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, \ldots, 24, 26, 28\}$,
- $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\}$,
- $\langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}$,
- $\langle 6 \rangle = \{0, 6, 12, 18, 24\}$,
- $\langle 10 \rangle = \{0, 10, 20\}$,
- $\langle 15 \rangle = \{0, 15\}$,
- $\langle 0 \rangle = \{0\}$.

Example 4.7 (Non-example)**.** The dihedral group D_4 has five subgroups of order 2 and three subgroups of order 4. The following are subgroups of D_4:

- $\{R_0, R_{180}\}$,
- $\{R_0, H\}$,
- $\{R_0, V\}$,
- $\{R_0, D\}$,
- $\{R_0, L\}$,
- $\{R_0, R_{90}, R_{180}, R_{270}\}$,
- $\{R_0, R_{180}, H, V, \}$,
- $\{R_0, R_{180}, D, L, \}$.

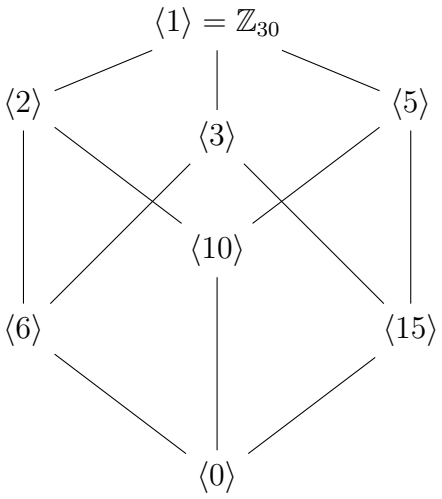


Figure 4.1: Subgroup lattice of $\mathbb{Z}_{30}$.

4.4 Number of elements of a certain order

Example 4.8. We know that $\mathbb{Z}_{36}$ has exactly one subgroup of order 9, call it H. Find all generators of the subgroup of H.
The subgroup H is cyclic and 4 is one of its generators. So

$$H = \langle 4 \rangle = \{k \cdot 4 \mid k \in \mathbb{Z}\} = \{0, 4, 8, 12, 16, 20, 24, 28, 32\}.$$

Observe that $|4| = 9$. By Corollary 4.2.7, an element $k \cdot 4$ is a generator of $\langle 4 \rangle$ iff $\gcd(k, 9) = 1$. Thus, $k \in \{1, 2, 4, 5, 7, 8\}$, and so the generators of the subgroup $\langle 4 \rangle$ are $4, 8, 16, 20, 28, 32$. Moreover, these elements are the only elements in $\mathbb{Z}_{36}$ of order 9. Why?

Definition 4.4.1. (Euler's Totient Function)

The *Euler phi function* (or *Euler's totient function*) is the function ϕ given by $\phi(1) = 1$ and for $n \geq 2$, we set $\phi(n)$ to be the number of positive integers less than n which are coprime with n.

Remark. The order of the group of units U_n is $\phi(n)$, that is, $|U_n| = \phi(n)$.

Exercise 4.9. Find $\phi(n)$ for $n = 2, 3, 4, 5, 8, 9, 10, 22, 30, 40$.

Lemma 4.4.2.

Let ϕ be the Euler phi function. Then
(i) For prime p, we have $\phi(p^n) = p^n - p^{(n-1)}$.
(ii) For relatively prime m and n, we have $\phi(mn) = \phi(m)\phi(n)$.

Theorem 4.4.3.

Let G be a finite cyclic group of order n, and let d be a divisor of n. Then the number of elements of order d is $\phi(d)$.

Proof. Suppose that $G = \langle g \rangle$ is a cyclic group of order n. Let d be a divisor of n and so $n = d\alpha$ for some $\alpha \in \mathbb{Z}$. By the fundamental theorem of cyclic groups, G has exactly

one subgroup of order d, namely, $H = \langle g^\alpha \rangle$. Consequently, all the elements of order d in G must belong to the subgroup H. For notational simplicity, we shall put $h = g^\alpha$ and so $H = \langle h \rangle = \{e, h, h^2, \ldots, h^{d-1}\}$. Moreover, $h^k \in H$ has order d if and only if h^k is a generator of H if and only if $\gcd(k, d) = 1$ (see Corollary 4.2.7). The number of such generators is thus the number of integers $1 \leq k < d$ which are coprime with d, and so there are $\phi(d)$ many elements of order d in G. ■

Corollary 4.4.4.

A finite cyclic group of order n has exactly $\phi(n)$ many generators.

Corollary 4.4.5.

Let G be a finite group (not necessarily cyclic). Then the number of elements of order d in G is a multiple of $\phi(d)$.

Proof. Let G be any finite group. If there are no elements of order d, then the statement holds trivially since $\phi(d)$ divides 0. Otherwise, let $a \in G$ be an element of order d. By Theorem 4.4.3 there are $\phi(d)$ many elements of order d in the subgroup $\langle a \rangle$. If there are no other elements of order d, we are done. Otherwise, let $b \notin \langle a \rangle$ be an element of G of order d. We claim that $\langle a \rangle \cap \langle b \rangle$ has no elements of order d. Suppose there is one, call it c. Then, as $c \in \langle a \rangle$ and $|c| = d$ it must be that $\langle a \rangle = \langle c \rangle$, and similarly, $\langle b \rangle = \langle c \rangle$. Thus, $\langle a \rangle = \langle b \rangle$ contradicting the choice of b. So $\langle b \rangle$ has another $\phi(d)$ elements of order d different than those in $\langle a \rangle$. We continue in this fashion collecting in every step $\phi(d)$ many new elements of order d. Since G is finite, this process must terminate, say after k many step where there will be $k \cdot \phi(d)$ many elements of order d in G. ■

We conclude this chapter by stating the following result which answers the question: When the group of units U_n is cyclic?

Theorem 4.4.6.

The group of units U_n is cyclic if and only if $n = 2$, $n = 4$, $n = p^k$, or $n = 2p^k$ for any odd prime p.

Chapter 5

Permutation Groups

Permutation groups were the only groups investigated by mathematicians during the first half of the 19th century. Recall that the notion of an abstract group was introduced by Cayley around 1850.

5.1 Symmetric Groups and Permutation Groups

Let $f : X \to Y$ be a function. Recall that we say that f is *injective* if for any $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$. Moreover, we say that f is *surjective* if for any $y \in Y$, there exists $x \in X$ such that $f(x) = y$. A function which is both injective and surjective is called a *bijection*. When $f : A \to B$ is a bijection, we define its inverse function to be $f^{-1} : B \to A$ where for any $b \in B$ we define $f^{-1}(b) = a$ where a is the unique preimage of b under the function f. Moreover, we have that $f \circ f^{-1}$ is the identity function on B, and $f^{-1} \circ f$ is the identity function on A.

The central theme of interest in this chapter is explore groups whose members are bijections from a set to itself.

Definition 5.1.1. (Permutation)

A *permutation* of a set A is a bijection from A to itself.

When f is a permutation of a finite set A, one way to express f is in a 2-row array where in the first row we list the elements of the domain, and then below each entry of the first row we write down its corresponding image under f. Usually we consider the set $A = \{1, 2, 3, \ldots, n\}$ and so in this case a permutation f of A has the form

$$\begin{bmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & f(3) & \ldots & f(n) \end{bmatrix}.$$

Note that when $|A| = n$, there are exactly $n!$ many permutations of A.

Consider the set $A = \{a, b, c, d\}$ together with a permutation $f : A \to A$ given by the assignment: $f(a) = c$, $f(b) = a$, $f(c) = d$ and $f(d) = b$. Thus, in array notation,

$$f = \begin{bmatrix} a & b & c & d \\ c & a & d & b \end{bmatrix}.$$

Given another permutation g of A, where

$$g = \begin{bmatrix} a & b & c & d \\ b & d & c & a \end{bmatrix},$$

we may form their composition $f \circ g$ by appying g first to elements of A and then apply f to obtain a new permutation of A.

$$f \circ g = fg = \begin{bmatrix} a & b & c & d \\ c & a & d & b \end{bmatrix} \begin{bmatrix} a & b & c & d \\ b & d & c & a \end{bmatrix} = \begin{bmatrix} a & b & c & d \\ a & b & d & c \end{bmatrix}.$$

For instance, we have that $(f \circ g)(d) = f(g(d)) = f(a) = c$, thus $(f \circ g)(d) = c$ as expressed by the last column of the array representing $f \circ g$.

Example 5.1. List all of the 6 permutations of the set $A = \{1, 2, 3\}$, and check whether they form a group under function composition.

- $\epsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$
- $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$
- $\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$
- $\gamma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$
- $\eta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$
- $\theta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$

Clearly the identity map ϵ is the identity element of the group. Observe that the inverse of η is γ (i.e. $\eta^{-1} = \gamma$) since $\eta\gamma = \epsilon$. This group is called the *symmetric group of degree* 3 and is denoted by S_3. The orders of elements of S_3 are: $|\epsilon| = 1$, $|\alpha| = 2$, $|\beta| = 2$, $|\gamma| = 3$, $|\eta| = 3$, and $|\theta| = 2$.

Cayley table of S_3

$\circ$	ϵ	α	β	γ	η	θ
ϵ	ϵ	α	β	γ	η	θ
α	α	ϵ		θ		
β	β		ϵ			
γ	γ	β		η	ϵ	
η	η			ϵ	γ	
θ	θ	η	γ	β	α	ϵ

Clearly, S_3 is non-abelian since $\gamma\alpha = \beta$, however, $\alpha\gamma = \theta$.

Lemma 5.1.2.

The set of all permutations of a (finite or infinite) set A is a group under function composition.

Clearly, the identity element of this group is the identity function which we will denote by ϵ, more precisely, it is the function $\epsilon : A \to A$ where $\epsilon(x) = x$ for every $x \in A$.

Definition 5.1.3. (Symmetric Group)

The group of all permutations of a set A is called the *symmetric group* of A and is denoted by $\mathrm{Sym}(A)$. If $|A| = n$, the group $\mathrm{Sym}(A)$ is called the *symmetric group of degree* n and is also denoted by S_n.

Lemma 5.1.4.

The groups S_1 and S_2 are abelian. The group S_n is nonabelian for $n \geq 3$.

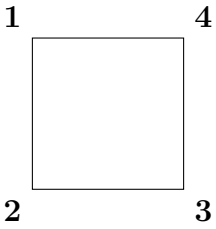
Symmetric groups are rich in subgroups, for example, S_4 has 30 subgroups and S_5 has more than 100 subgroups. Subgroups of symmetric groups are called permutation groups.

Definition 5.1.5. (Permutation Group)

A *permutation group* is a subgroup of some symmetric group.

So a permutation group is a collection of permutations of some given set which satisfies the group axioms under the operation of function composition. For example, the group $\{\epsilon, \gamma, \eta\}$ from Example 5.1 is a permutation group since it is a subgroup of the symmetric group S_3. Of course, every symmetric group is a permutation group.

Example 5.2. Think of D_4 as a permutation group by labelling the 4 corners of the square by the integers $1, 2, 3, 4$.



Consequently, each motion in D_4 can be thought of as a permutation of the 4 corners of the square. In this way we can see that D_4 as a subgroup of S_4. For example, the motions R_{90} and H are represented as permutations of the set $\{1, 2, 3, 4\}$ according to their actions on the square corners as follows.

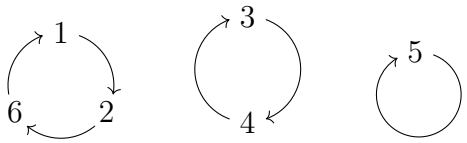
$$R_{90} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}, \qquad H = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

5.2 Cycle Decomposition of Permutations

Cycle notation was introduced by the French mathematician Augustin-Louis Cauchy in 1815 to represent permutations. Consider the permutation below.

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 3 & 5 & 1 \end{bmatrix}.$$

Observe that the action of the permutation α consists of 3 cycles: the first cycle is $1 \mapsto 2 \mapsto 6 \mapsto 1$, the second cycle is $3 \mapsto 4 \mapsto 3$, and the third cycle is $5 \mapsto 5$.



In this case we write: $\alpha = (1\,2\,6)(3\,4)(5)$, $\alpha = (6\,1\,2)(3\,4)(5)$, or $\alpha = (4\,3)(1\,2\,6)(5)$.

Definition 5.2.1. (Cycle)

Let A be a set of symbols. A *cycle* of length m or an m-cycle is a sequence of distinct elements from A of the form

$$(a_1, a_2, a_3, \ldots, a_{m-1}, a_m).$$

Such an m-cycle can be thought of as a permutation of A where the image of a symbol appearing in the cycle is its successor and the image of a symbol not in the cycle is itself, more precisely, the cycle $(a_1, a_2, \ldots, a_{m-1}, a_m)$ is the permutation α of A given by:

$$\begin{cases} \alpha(a_i) = a_{i+1} & \text{if } 1 \leq i < m, \\ \alpha(a_m) = a_1, & \\ \alpha(x) = x & \text{if } x \text{ is a symbol not appearing in the cycle.} \end{cases}$$

For example, the cycle $(1, 3, 4)$ represents the following permutation in S_5.

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

When no confusion arises, it is a common practice to omit the commas in the cycle notation. So we write $(1\,3\,4)$ for the cycle $(1, 3, 4)$. Clearly, any 1-cycle such as (3) represents the identity function. Since we think of a cycle as a permutation we may multiply cycles by composing them as permutations. Remember that composing functions is done from right to left. For instance, consider the cycles $\alpha = (1\,3\,4)$ and $\beta = (2\,4\,6)$. The image of 2 under the composition $\alpha \circ \beta$ is computed by applying β first and then α. So $(\alpha \circ \beta)(2) = \alpha(\beta(2)) = \alpha(4) = 1$.

$$2 \xrightarrow{\beta} 4 \xrightarrow{\alpha} 1$$

So the composition $\alpha \circ \beta$ maps 2 to 1. By computing the images of all elements of the domain $\{1, 2, 3, 4, 5, 6\}$, their composition is

$$\alpha \circ \beta = \alpha\beta = (1\,3\,4)(2\,4\,6) = (1\,3\,4\,6\,2) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 5 & 2 \end{bmatrix}.$$

In general when we compose cycles we think of each input entering the very right cycle, and then moving from one cycle to the one on its left side until exiting the very left cycle keeping in mind that a symbol is fixed by a cycle not containing it.

Example 5.3. Find $\alpha\beta$ where $\alpha = (1\,3)(2\,7)(4\,5\,6)(8)$ and $\beta = (1\,2\,3\,7)(6\,4\,8)(5)$. Remember we move through cycles from right to left.

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

By definition of the inverse of a bijective function, we get that the inverse of the cycle $\alpha = (a_1\ a_2\ \ldots\ a_{n-1}\ a_n)$ is the cycle

$$\alpha^{-1} = (a_n\ a_{n-1}\ \ldots\ a_2\ a_1).$$

Example 5.4. Find the inverse of the cycle $\alpha = (3\,1\,5\,2)$ in S_5 and its order.

The inverse of α is $\alpha^{-1} = (2\,5\,1\,3)$, one can check that $(3\,1\,5\,2)(2\,5\,1\,3) = (1)$. Now to find the order of α we start computing its positive powers until we hit the identity map.

- $\alpha^2 = (3\,1\,5\,2)(3\,1\,5\,2) = (1\,2)(3\,5)$.
- $\alpha^3 = \alpha^2\alpha = (1\,2)(3\,5)(3\,1\,5\,2) = (1\,3\,2\,5)$.
- $\alpha^4 = \alpha^3\alpha = (1\,3\,2\,5)(3\,1\,5\,2) = (1)$.

Therefore, the order of α is 4, in symbols, $|\alpha| = 4$.

Lemma 5.2.2.

In the group S_n, the order of an m-cycle is m.

Example 5.5. Use cycle notation to compute $\eta\,\theta$ where

$$\eta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{bmatrix} \text{ and } \theta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}.$$

First we convert the array notation of η and θ to cycle notation. So $\eta = (1\,2)(4\,5)$ and $\theta = (1\,5\,3)(2\,4)$. Now,

$$\eta\,\theta = (1\,2)(4\,5)(1\,5\,3)(2\,4) = (1\,4)(2\,5\,3).$$

Theorem 5.2.3. (Disjoint Cycles Commute)

Suppose that cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no symbols in common. Then $\alpha\beta = \beta\alpha$.

Proof. Let $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$. Suppose that α and β are permutations of the set

$$X = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_k\}$$

where the c_i's are the symbols not appearing in the cycle α nor β. To show that $\alpha\beta = \beta\alpha$ we need to show that $\alpha\beta$ agree with $\beta\alpha$ on every symbol in X. First, as β fixes all symbols in α we have $(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$ and $(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$. So $(\alpha\beta)(a_i) = (\beta\alpha)(a_i)$. Second, as α fixes all symbols in β we have $(\alpha\beta)(b_i) = \alpha(\beta(b_i)) = \alpha(b_{i+1}) = b_{i+1}$ and $(\beta\alpha)(b_i) = \beta(\alpha(b_i)) = \beta(b_i) = b_{i+1}$. So $(\alpha\beta)(b_i) = (\beta\alpha)(b_i)$. Third, as both α and β fix the symbol c_i we have $(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i$ and $(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i$. So $(\alpha\beta)(c_i) = (\beta\alpha)(c_i)$. Therefore, $\alpha\beta$ and $\beta\alpha$ agree on all symbols of the set S. ■

We have seen that a cycle gives rise to a permutation. On the other hand, not every permutation can be represented by a single cycle, however, it can be broken down into a composition of cycles.

Theorem 5.2.4. (Disjoint Cycle Decomposition)

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

Proof. Suppose that α is a permutation of a finite nonempty set A. We start by choosing some element $a_1 \in A$. Then we construct a sequence (a_i) by setting $a_{i+1} = \alpha(a_i)$. So $a_2 = \alpha(a_1)$, $a_3 = \alpha(a_2) = \alpha(\alpha(a_1)) = \alpha^2(a_1)$, and so on. In general, $a_{i+1} = \alpha^i(a_1)$. This sequence

$$a_1,\ \alpha(a_1),\ \alpha^2(a_1),\ \alpha^3(a_1),\ \ldots$$

lies in A and as A is finite there must be repetitions. So there are integers i and j such that $\alpha^i(a_1) = \alpha^j(a_1)$ where $i < j$. Composing both sides with $(\alpha^i)^{-1}$ gives $a_1 = \alpha^{j-i}(a_1)$. Therefore, for some positive integer k we have $a_{k+1} = \alpha^k(a_1) = a_1$, let k be the least such integer. At this point we have obtained our first cycle of α, it is the cycle $(a_1\, a_2\, a_3\, \cdots\, a_k)$. Observe that $\alpha^i(a_1)$ lies in this cycle for every $i \in \mathbb{Z}$. If the symbols in this cycles are all the elements of A we are done and $\alpha = (a_1\, a_2\, a_3\, \cdots\, a_k)$. Otherwise, let b_1 be a symbol in A not appearing in the first cycle. Similarly, we proceed to create a new cycle by defining $b_{i+1} = \alpha^i(b_1)$ until we reach the first positive integer l where $b_{l+1} = \alpha^l(b_1) = b_1$. This new cycle $(b_1\, b_2\, b_3\, \cdots\, b_l)$ has no symbols in common with the first cycle. To see this, suppose for the contrary that there are integers i and j with $a_{i+1} = b_{j+1}$. It follows that $\alpha^i(a_1) = \alpha^j(b_1)$ and so $\alpha^{i-j}(a_1) = b_1$. This means that b_1 lies in the first cycle, contradicting the choice of b_1. We continue in this fashion until all the symbols of A appear in the cycles we are creating. As A is finite, this process terminates and the permutation α is written as a product of disjoint cycles:

$$\alpha = (a_1\, a_2\, a_3\, \cdots\, a_k)\,(b_1\, b_2\, b_3\, \cdots\, b_l)\, \cdots\, \cdots\, (x_1\, x_2\, x_3\, \cdots\, x_m).$$

As any element of A exists in exactly one of the cycles we created above, it is clear that the composition of all these cycles indeed gives our permutation α. ■

Expressing permutations as products of disjoint cycles has a great advantage as shown in the next theorem.

Theorem 5.2.5. (Ruffini; 1799)

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles. In other words, suppose that a permutation $f = \alpha_1\alpha_2\cdots\alpha_n$ where the α_i's are disjoint cycles. Then

$$|f| = \operatorname{lcm}(|\alpha_1|, |\alpha_2|, \ldots, |\alpha_n|).$$

Proof. For simplicity, we will prove the theorem for a permutation written as the product of two disjoint cycles. We already know that the order of an m-cycle is m. Now suppose that that α and β are disjoint cycles of length m and n, respectively, where $\alpha, \beta \in \operatorname{Sym}(A)$ for some finite set A. Thus, $|\alpha| = m$ and $|\beta| = n$. Let l be the least common multiple of m and n, and let t be the order of $\alpha\beta$. We will show that $t = l$. Both m and n divide l and so $l = rm$ and $l = sn$ for some integers r and s. Since disjoint cycles commute it follows that $(\alpha\beta)^k = \alpha^k\beta^k$ for any integer k. Thus,

$$(\alpha\beta)^l = \alpha^l\beta^l = \alpha^{rm}\beta^{sn} = (\alpha^m)^r(\beta^n)^s = \epsilon^r\epsilon^s = \epsilon.$$

Thus, we obtain that t divides l by Lemma 2.2.4. So $t \leq l$. Next, as $|\alpha\beta| = t$ we get that:

$$\epsilon = (\alpha\beta)^t = \alpha^t\beta^t.$$

We now prove that $\beta^t = \epsilon$, the identity map. Towards this, let $x \in A$. If x does not appear in the cycle β, then $\beta^t(x) = x$ since $\beta(x) = x$. Otherwise, let x be one of the symbols in β and let $\beta^t(x) = y$ for some $y \in A$. Notice that y also lies in the cycle β. Thus, the symbol y does not appear in α as the cycles α and β are disjoint and so y is fixed by α, and thus $\alpha^t(y) = y$. It follows that

$$x = \epsilon(x) = (\alpha^t\beta^t)(x) = \alpha^t(\beta^t(x)) = \alpha^t(y) = y.$$

Therefore, $x = y$ and so $\beta^t(x) = x$ in this case as well. Therefore, $\beta^t = \epsilon$. Similarly, we show that $\alpha^t = \epsilon$ as well. By Lemma 2.2.4, the orders of α and β divide t, and so $m \mid t$ and $n \mid t$. This means that t is a common multiple of m and n and so $l = \text{lcm}(m, n) \leq t$. Finally, as $t \leq l$ and $l \leq t$, we get that $t = l$, in other words,

$$|\alpha\beta| = \text{lcm}(|\alpha|, |\beta|).$$

The general case where the permutation is a composition of three or more disjoint cycles can be treated in a similar fashion. ■

Example 5.6. Compute the orders of the following permutations in the symmetric group S_8.

- $|(1\,3\,2)(4\,5)| = \text{lcm}(3, 2) = 6$.
- $|(1\,4\,3\,2)(5\,6)| = \text{lcm}(4, 2) = 4$.
- $|(1\,2\,3)(4\,5\,6)(7\,8)| = \text{lcm}(3, 3, 2) = 6$.
- $|(1\,2\,3)(1\,4\,5)| = |(1\,4\,5\,2\,3)| = 5$.

We already know that any permutation of a finite set can be written as a product of disjoint cycles. The information about the number of cycles of each length that are present in the cycle decomposition is called the *cycle type* of the permutation. Denote an m-cycle by $[m]$ and in each cycle type arrange the cycles from longest to shortest. For example, if the cycle type of a permutation α is $[3]\,[3]\,[2]\,[1]$, it means that the cycle decomposition of α has two 3-cycles, one 2-cycle, and one 1-cycle. For instance, $\alpha = (3\,7\,4)(1\,5\,8)(2\,9)(6)$ in S_9 has such cycle type.

Example 5.7 (Cycle types)**.** Consider the symmetric group S_7.

1. List all cycle types of permutations in S_7.
   - $[7]$
   - $[6]\,[1]$
   - $[5]\,[2]$
   - $[5]\,[1]\,[1]$
   - $[4]\,[3]$
   - $[4]\,[2]\,[1]$
   - $[4]\,[1]\,[1]\,[1]$
   - $[3]\,[3]\,[1]$
   - $[3]\,[2]\,[2]$
   - $[3]\,[2]\,[1]\,[1]$
   - $[3]\,[1]\,[1]\,[1]\,[1]$
   - $[2]\,[2]\,[2]\,[1]$
   - $[2]\,[2]\,[1]\,[1]\,[1]$
   - $[2]\,[1]\,[1]\,[1]\,[1]\,[1]$
   - $[1]\,[1]\,[1]\,[1]\,[1]\,[1]\,[1]$
2. Consequently, find all orders of permutations in S_7. Using Theorem 5.2.5, we can compute the orders of all permutations in the symmetric group S_7 by finding the least common multiple of lengths of cycles in each cycle type. The orders of elements in S_7 are: $7, 6, 10, 5, 12, 4, 3, 2, 1$.

3. How many permutations in S_7 have order 12 are there? Well, a permutation in S_7 has order 12 if and only if its cycle type $[4]\,[3]$. That is, we need to count the number of permutations whose disjoint cycle decomposition is of the form $(a_1\,a_2\,a_3\,a_4)\,(b_1\,b_2\,b_3)$. Thus, there are

$$\frac{7\cdot 6\cdot 5\cdot 4}{4}\times\frac{3\cdot 2\cdot 1}{3}=420$$

permutations in S_7 of order 12. (Notice that an m-cycle can be written in m different ways, for instance, $(1\,3\,6\,4)=(4\,1\,3\,6)=(6\,4\,1\,3)=(3\,6\,4\,1)$.)

4. How many permutations in S_7 have order 3 are there? Permutations of order 3 have cycle type $[3]\,[3]\,[1]$ or $[3]\,[1]\,[1]\,[1]\,[1]$. We need to find permutations of the form $(a_1\,a_2\,a_3)(b_1\,b_2\,b_3)$ and of the form $(a_1\,a_2\,a_3)$. Since each 3-cycle can be written in 3 ways and $(a_1\,a_2\,a_3)(b_1\,b_2\,b_3)=(b_1\,b_2\,b_3)(a_1\,a_2\,a_3)$ as permutations there are

$$\frac{7\cdot 6\ \cdot 5}{3}\times\frac{4\cdot 3\cdot 2}{3}\times\frac{1}{2}+\frac{7\cdot 6\cdot 5}{3}=280+70=350$$

permutations in S_7 of order 3.

5. How many permutations in S_7 have cycle type $[2]\,[2]\,[2]\,[1]$? We need to find permutations whose disjoint cycle decomposition is of the form $(a_1\,a_2)(b_1\,b_2)(c_1\,c_2)$. Since any reordering of these three 2-cycles will give the same permutations, the number is

$$\frac{7\cdot 6}{2}\times\frac{5\cdot 4}{2}\times\frac{3\cdot 2}{2}\times\frac{1}{3!}=105$$

permutations in S_7 of cycle type $[2]\,[2]\,[2]\,[1]$.

5.3 Alternating Groups

Our aim is to study an important subgroup of the symmetric group called the alternating group.

Definition 5.3.1. (Transposition)

A cycle of length 2 is called a *transposition*.

So a transposition $(a\,b)$ maps a to b and maps b to a, and fixes every other symbol. Observe that the inverse of a transposition is itself.

Example 5.8. Write the following cycles as a product of transpositions.

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

Lemma 5.3.2.

A permutation is an involution if and only if it can be written as a product of disjoint transpositions.

Lemma 5.3.3.

Every permutation in S_n is a product of transpositions.

Proof. The identity map can be expressed as $\epsilon = (1\,2)(1\,2)$. A cycle of length at least 2, say $(a_1\,a_2\,a_3\,\ldots\,a_{n-1}\,a_n)$, can be expressed as

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

Any other permutation can be written as a product of disjoint cycles by Theorem 5.2.4, and then by writing each of these cycles as a product of transpositions as described above we obtain the desired product of transpositions. ■

Example 5.9. Express the permutation below as a product of transpositions.

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 2 & 1 & 3 & 4 & 7 & 5 \end{bmatrix}.$$

We proceed by writing α as a product of cycles and then writing every cycle as a product of transpositions as follows $\alpha = (1\,6\,4)\,(2\,8\,5\,3) = (1\,4)\,(1\,6)\,(2\,3)\,(2\,5)\,(2\,8)$.

As seen above, the same permutation can be written as a product of transpositions in more than way. We will show next that the number of transpositions used to express the same permutation is always odd or always even.

Lemma 5.3.4.

Any product of transpositions giving the identity permutation ϵ has even many transpositions.

Proof. We will prove by strong induction that for every $n \geq 1$ we have that:

$$\text{if } \epsilon = \tau_1\tau_2\cdots\tau_n \text{ where each } \tau_i \text{ is a transposition, then } n \text{ is even.}$$

When $n = 1$, then $\epsilon = \tau_1$ is false as a single transposition is not the identity map. If $n = 2$, then there is nothing to show as 2 is even. Now suppose that $n > 2$ and the statement holds for all integers less than n. We need to show that the statement holds for n. So suppose that

$$\epsilon = \tau_1\tau_2\cdots\tau_{n-1}\tau_n.$$

We now need to show that n is even. Consider the last two transpositions $\tau_{n-1}\tau_n$ in this product. There are four cases to consider listed below.

1. If $\tau_{n-1}\tau_n = (a\,b)(a\,b)$, then delete $\tau_{n-1}\tau_n$ from the product as $(a\,b)(a\,b) = \epsilon$.
2. If $\tau_{n-1}\tau_n = (a\,c)(a\,b)$, then replace $(a\,c)(a\,b)$ with $(a\,b)(b\,c)$ as they are equal.
3. If $\tau_{n-1}\tau_n = (b\,c)(a\,b)$, then replace $(b\,c)(a\,b)$ with $(a\,c)(b\,c)$ as they are equal.
4. If $\tau_{n-1}\tau_n = (c\,d)(a\,b)$, then replace $(c\,d)(a\,b)$ with $(a\,b)(c\,d)$ as they are equal.

In the first case, we get that $\epsilon = \tau_1\tau_2\cdots\tau_{n-2}$, and so by induction hypothesis it must be that $n-2$ is even, and so n is even as desired. In the other three cases, what we did is that we expressed the identity map as a product of n transpositions where the rightmost occurrence of the symbol a is in the second-from-the-last transposition of the product.

Next, we reapply the procedure just described to the pair of transpositions located at the third-from-the-last and second-from-the-last positions of the product. Consequently, as before, we either get a product of $n-2$ transpositions equal to the identity map or a new product of n transpositions where the rightmost occurrence of the symbol a occurs in the third-from-the-last transposition. Continuing in this fashion we must arrive to a product of $n-2$ transpositions equal to the identity map as otherwise we will keep moving the symbol a to the left until we can express the identity map as a product of n transpositions where the symbol a only appears in the leftmost transposition. However, such a product of transpositions is not the identity map since it does not fix the symbol a, whereas the identity map does. So eventually we will express the identity map as a product of $n-2$ transpositions, an so by the induction hypothesis $n-2$ must be even, and so is n. ■

Theorem 5.3.5. (Cauchy)

If a permutation α can be expressed as the product of an even number of transpositions, then every decomposition of α into a product of transpositions must have an even number of transpositions. Similarly, for an odd number of transpositions.

Proof. Suppose that α is a permutation such that $\alpha = \tau_1\tau_2\cdots\tau_n$ and $\alpha = \chi_1\chi_2\cdots\chi_k$ where all τ_i's and χ_i's are transpositions. Then $\tau_1\tau_2\cdots\tau_n = \chi_1\chi_2\cdots\chi_k$ and so as a transposition is its own inverse (i.e. $\tau_i^{-1} = \tau_i$) we get that

$$\epsilon = \tau_n\cdots\tau_2\tau_1\,\chi_1\chi_2\cdots\chi_k.$$

It follows that the identity map is a product of $n+k$ many transpositions. Therefore, by Lemma 5.3.4, we get that $n+k$ must be an even integer. It follows that n and k are both even or both odd. ■

Definition 5.3.6. (Even and Odd Permutations)

An *even* permutation is a permutation that can be expressed as a product of an even number of transpositions. An *odd* permutation is a permutation that can be expressed as a product of an odd number of transpositions.

Lemma 5.3.7.

The set of all even permutations forms a subgroup of S_n.

Definition 5.3.8. (Alternating Group)

The subgroup of S_n consisting of all even permutations is called the *alternating group* of degree n, denoted by A_n.

Example 5.10. Find the alternating group A_4 of degree 4. (Elements of A_4 can be thought of as the 12 rotations of the regular tetrahedron.)

$A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$.

Lemma 5.3.9.

The order of A_n is $n!/2$.

Proof. Let B_n be the set of all odd permutations in S_n. Then $S_n = A_n \cup B_n$ and $A_n \cap B_n = \emptyset$. We will show that $|A_n| = |B_n|$. Towards, consider the function $f : A_n \to B_n$ where $f(\alpha) = (1\,2) \circ \alpha = (1\,2)\alpha$ for each even permutation α. Clearly, the permutation $(1\,2)\alpha$ is odd whenever α is an even permutation. Next, we show that f is injective. Let $\alpha, \beta \in A_n$ and assume that $f(\alpha) = f(\beta)$. Then $(1\,2)\alpha = (1\,2)\beta$, and by the cancellation property in groups, we get that $\alpha = \beta$. Second, let γ be in B_n. So γ is an odd permutation, and thus $(1\,2)\gamma$ is even, that is, $(1\,2)\gamma \in A_n$. We now have that $f((1\,2)\gamma) = (1\,2)(1\,2)\gamma = \gamma$ showing that f is surjective. Therefore, f is bijective and so $|A_n| = |B_n|$. Finally, $n! = |S_n| = |A_n| + |B_n| = |A_n| + |A_n| = 2|A_n|$. Therefore, $|A_n| = n!/2$. ■

To conclude this chapter we present an application of permutation groups in cryptography.

Example 5.11 (Cryptography)**.** Use the permutation below to encrypt the message "ATTACK AT DAWN".

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

First we write the sentence in blocks of 4 letters to obtain

"ATTA CKAT DAWN".

Permute the letters in each block according to α. For example, $\alpha(1) = 3$ means move the first letter of the block to the third position, and so on. In the end, the encrypted message will be

"ATAT TACK NWDA".

To decrypt the message use α^{-1} where

$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix}.$$

Chapter 6

Group Isomorphisms

Counting in English: "one, two, three, four, five" is similar to counting in German: "eins, zwei, drei, vier, fünf". Similarly, adding in English: "two plus three is five" is similar to doing the same operation in German: "zwei und drei ist fünf". The same happens for groups when the same group structure is described in two different ways, for example we have the seen before that the elements of the dihedral group D_4 can be seen as geometric symmetries of the square or as permutations of the set of 4 corners of the square. Another example is that any cyclic group of order n is the same as the cyclic group $(\mathbb{Z}_n, +)$. The term *isomorphism* is derived from the Greek words: *isos* meaning "same", and *morphe* meaning "form".

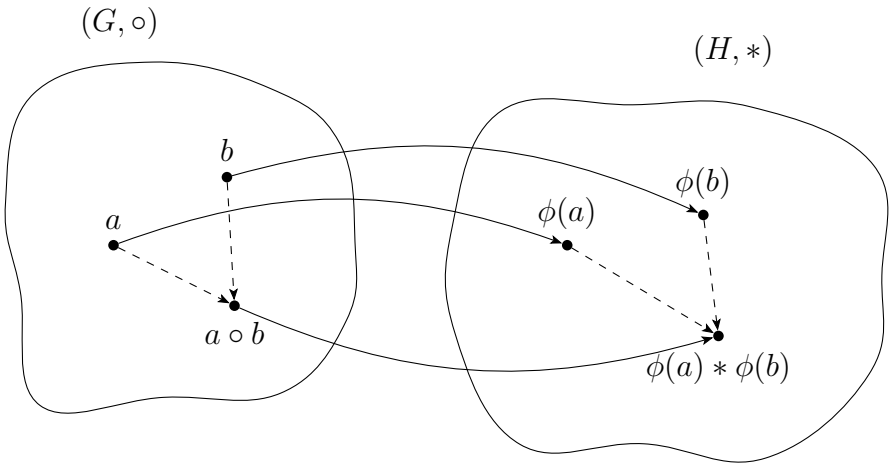
6.1 Isomorphisms

Definition 6.1.1. (Group Homomorphism and Isomorphism)

Let $(G, \circ)$ and $(H, *)$ be groups. A *homomorphism* from G to H is a function $\phi : G \to H$ that preserves the group operation, that is, for any $a, b \in G$ we have that

$$\phi(a \circ b) = \phi(a) * \phi(b).$$

An *isomorphism* from G to H is a bijective homomorphism from G to H. We say that G and H are *isomorphic*, and write $G \cong H$, if there exists an isomorphism from G to H.



When two groups are isomorphic, they have the same cardinality and, moreover, their binary operations essentially behave in the same way. When G and H are finite isomorphic groups and you replace every symbol in the Cayley table of G by its image under the isomorphism you will get the Cayley table of H. To an algebraist two isomorphic groups are the same group.

Example 6.1. Examples of isomorphic groups.

1. $U_{10} \cong \mathbb{Z}_4 \cong U_5$.
2. An infinite cyclic group $G = \langle g \rangle$ is isomorphic to $(\mathbb{Z}, +)$. See below.
3. A finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$.
4. $U_{43} \cong U_{49} \cong \mathbb{Z}_{42}$.
5. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. See below.
6. D_4 is isomorphic to a subgroup of S_4.
7. $(\mathbb{R}, +) \cong (\mathbb{C}, +)$.
8. $(\mathbb{C}^*, \cdot)$ is isomorphic to the complex unit circle.

Lemma 6.1.2.

Group isomorphism is an equivalence relation on groups. More precisely, let A, B, C be groups. Then

- *$A \cong A$.* *(Reflexive)*
- *If $A \cong B$, then $B \cong A$.* *(Symmetric)*
- *If $A \cong B$ and $B \cong C$, then $A \cong C$.* *(Transitive)*

Remark. In order to show that a group G is isomorphic to a group H one needs to do the following:

1. Find a suitable map $\phi : G \to H$.
2. Show that ϕ is injective.
3. Show that ϕ is surjective.
4. Show that ϕ preserves the group operation.

Example 6.2. The additive group of real numbers is isomorphic the group of positive real numbers under multiplication, that is, $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. To see this, consider the map $\phi : \mathbb{R} \to \mathbb{R}^+$ given by $\phi(x) = 2^x$ for every $x \in \mathbb{R}$. To show that ϕ is injective, let $x, y \in \mathbb{R}$ and suppose that $\phi(x) = \phi(y)$. So $2^x = 2^y$. Then $\log_2(2^x) = \log_2(2^y)$, and thus $x = y$. For surjectivity, let $y \in \mathbb{R}^+$, and take $x = \log_2(y)$. Then $\phi(x) = 2^x = 2^{\log_2(y)} = y$, as desired. Finally, we need to show that ϕ is operation-preserving. So let $x, y \in R$, then

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

Lemma 6.1.3.

Any infinite cyclic group is isomorphic to the additive group of integers.

Proof. Let $G = \langle g \rangle = \{g^k \mid k \in Z\}$ be an infinite cyclic group. We need to show that $(\mathbb{Z}, +) \cong G$. Consider the mapping $\phi : \mathbb{Z} \to G$ given by

$$\phi(k) = g^k$$

for every integer k. Since G is cyclic, any element of G is a power of the generator g and so this map is clearly surjective. Moreover, we know that all distinct powers of g are distinct elements in G, that is, if $k \neq m$, then $g^k \neq g^m$ (see Theorem 4.2.1), and so ϕ is injective. It remains to show that ϕ preserves the group operation. Towards this end, let $k, m \in \mathbb{Z}$, then

$$\phi(k + m) = g^{k+m} = g^k g^m = \phi(k)\phi(m).$$

■

Example 6.3. The map $\phi : \mathbb{R} \to \mathbb{R}$ given by $\phi(x) = x^3$ is not an isomorphism from $(\mathbb{R}, +)$ to itself. Although $(\mathbb{R}, +)$ is isomorphic to itself, of course. Although ϕ is a bijective map, it does not preserve addition. To see this, notice that $\phi(1+1) = \phi(2) = 2^3 = 8$, however, $\phi(1) + \phi(1) = 1^3 + 1^3 = 2$.

Example 6.4 (Non-example)**.** The groups $(\mathbb{R}, +)$ and $(\mathbb{R}^*, \cdot)$ are not isomorphic, that is, there exists no isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^*, \cdot)$.
Suppose for the sake of contradiction that $\phi : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ is an isomorphism. Let $b \in \mathbb{R}$ be the unique real number such that $\phi(b) = -1$. Moreover, let $c \in \mathbb{R}$ be such that $\phi(\frac{b}{2}) = c$. Then, as ϕ is an isomorphism, we get

$$-1 = \phi(b) = \phi\left(\frac{b}{2} + \frac{b}{2}\right) = \phi\left(\frac{b}{2}\right) \cdot \phi\left(\frac{b}{2}\right) = c^2.$$

It follows that -1 has a square root in $\mathbb{R}$ which is a contradiction. Similarly, we get that $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$.

6.2 Properties of Isomorphisms

Recall that an isomorphism of groups is a bijective homomorphism between groups.

Theorem 6.2.1.

Let G and H be groups and suppose that $\phi : G \to H$ is an homomorphism. Then the following hold.

(i) $\phi(e_G) = e_H$ *where* e_G, e_H *are the identity elements of* G *and* H*, respectively.*

(ii) For any $g \in G$ *we have that* $\phi(g^{-1}) = (\phi(g))^{-1}$.

(iii) For any $g \in G$ *and* $n \in \mathbb{Z}$ *we have* $\phi(g^n) = (\phi(g))^n$*. In additive notation, we write* $\phi(n\, g) = n\, \phi(g)$.

Proof. Suppose that $\phi : G \to H$ is a group homomorphism.

(i) We know that $e_G = e_G\, e_G$ and so $\phi(e_G) = \phi(e_G\, e_G)$. Since ϕ preserves the group operation we get that $\phi(e_G) = \phi(e_G)\phi(e_G)$. By multiplying both sides with the inverse of the element $\phi(e_G) \in H$ we get that $e_H = \phi(e_G)$ as desired.

(ii) Let $g \in G$ and observe that

$$\phi(g)\phi(g^{-1}) = \phi(g\, g^{-1}) = \phi(e_G) = e_H.$$

Therefore, in the group H, we have that $(\phi(g))^{-1} = \phi(g^{-1})$.

(iii) First, we show that $\phi(g^n) = (\phi(g))^n$ for every $n \geq 0$ by induction. For the base case, by Part (i) we get that $\phi(g^0) = \phi(e_G) = e_H = (\phi(g))^0$. Next, for the induction step, suppose that $\phi(g^n) = (\phi(g))^n$ for some integer $n \geq 0$. Then, as ϕ preserves the operation, we get

$$\phi(g^{n+1}) = \phi(g^n g) = \phi(g^n)\phi(g) = (\phi(g))^n \phi(g) = (\phi(g))^{n+1}.$$

To show the result for negative integers, let n be a negative integer and so $n = -k$ where k is a positive integer. By what we have just shown and Part (ii) we get that

$$\phi(g^n) = \phi(g^{-k}) = \phi((g^{-1})^k) = (\phi(g^{-1}))^k = ([\phi(g)]^{-1})^k = (\phi(g))^{-k} = (\phi(g))^n.$$

■

Theorem 6.2.2.

Let G and H be groups and suppose that $\phi : G \to H$ is an isomorphism. Then the following hold.

(i) For any $g_1, g_2 \in G$*, we have that* g_1 *and* g_2 *commute iff* $\phi(g_1)$ *and* $\phi(g_2)$ *commute.*

(ii) $G = \langle g \rangle$ *if and only if* $H = \langle \phi(g) \rangle$*. In words, if* g *is a generator of* G*, then* $\phi(g)$ *is a generator of* H*, and conversely.*

(iii) For any $g \in G$ *we have that* $|g| = |\phi(g)|$.

(iv) G *and* H *have the same number of elements of every order.*

(v) Let $b \in G$ *and* $k \in \mathbb{Z}$*. The equation* $x^k = b$ *has the same number of solutions in* G *as does* $x^k = \phi(b)$ *in* H.

Proof. Suppose that $\phi : G \to H$ is a group isomorphism.

(ii) Suppose that $G = \langle g \rangle$ for some element $g \in G$. Since $\phi(g) \in H$, it is clear by closure of the operation that $\langle \phi(g) \rangle \subseteq H$. Next, let $h \in H$. Because ϕ is surjective, there exists $a \in G$ such that $\phi(a) = h$, and as G is generated by g, there is an integer k such that

$a = g^k$. So $h = \phi(g^k) = \phi(g)^k$, and thus $h \in \langle \phi(g) \rangle$. Therefore, $H \subseteq \langle \phi(g) \rangle$. This proves that $H = \langle \phi(g) \rangle$.
Now to prove the converse, suppose that $H = \langle \phi(g) \rangle$. We need to show that g generates G. Clearly, $\langle g \rangle \subseteq G$. Now let $a \in G$ and so $\phi(a) \in H$. Since H is generated by $\phi(g)$, there is an integer k such that $\phi(a) = (\phi(g))^k = \phi(g^k)$. As ϕ is injective, it follows that $a = g^k$ and so $a \in \langle g \rangle$ showing that $G \subseteq \langle g \rangle$. This shows that $G = \langle g \rangle$. ■

Corollary 6.2.3.

Two groups G and H are not isomorphic when the number of elements having a specific order in G is different than that in H. In other words, if there is a positive integer d such that

$$|\{g \in G : |g| = d\}| \neq |\{h \in H : |h| = d\}|,$$

then $G \ncong H$.

Example 6.5. Which of the groups $\mathbb{Z}_{12}$, D_6, A_4 are isomorphic? No two are isomorphic. To see this, observe that the largest order of an element these groups are 12, 6, 3, respectively. Alternatively, count the number of elements of order 2, it is 1, 7, 3 respectively.

Example 6.6. $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$.
No non-identity element in $(\mathbb{Q}, +)$ has finite order, however, -1 has order 2 in $(\mathbb{Q}^*, \cdot)$.

Definition 6.2.4.

Let $\phi : X \to Y$ be a function. Consider subsets $A \subseteq X$ and $B \subseteq Y$. We define the subsets $\phi(A) \subseteq Y$ and $\phi^{-1}(B) \subseteq X$ as follows.

- $\phi(A) = \{\phi(a) \mid a \in A\}$.
- $\phi^{-1}(B) = \{x \in X \mid \phi(x) \in B\}$.

Theorem 6.2.5.

Let G and H be groups and suppose that $\phi : G \to H$ is an isomorphism. Then the following hold.

(i) $\phi^{-1} : H \to G$ is an isomorphism.
(ii) G is abelian if and only if H is abelian.
(iii) G is cyclic if and only if H is cyclic.
(iv) If $K \leq G$, then $\phi(K)$ is a subgroup of H.
(v) If $L \leq H$, then $\phi^{-1}(L)$ is a subgroup of G.
(vi) $\phi(Z(G)) = Z(H)$.

Proof. Suppose that $\phi : G \to H$ is a group isomorphism.

(iv) Let K be a subgroup of G. We need to show that

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

is a subgroup of H. As $e_G \in K$, we get that $\phi(e_G) = e_H \in \phi(K)$, so $\phi(K)$ is nonempty. Next we need to show that $\phi(K)$ is closed under multiplication and taking inverses. So let $x, y \in \phi(K)$. Thus, there are $a \in K$ and $b \in K$ such that $x = \phi(a)$ and $y = \phi(b)$. As K is

a subgroup, we know that $ab \in K$ and so $\phi(ab) \in \phi(K)$. But $xy = \phi(a)\phi(b) = \phi(ab) \in K$ as needed. Next, as $a \in K$ and $K \leq G$, we get $a^{-1} \in K$ and so $\phi(a^{-1}) \in \phi(K)$, but by isomorphism properties, we know that $x^{-1} = (\phi(a))^{-1} = \phi(a^{-1}) \in \phi(K)$. So $\phi(K)$ is closed under taking inverses. This shows that $\phi(K) \leq H$.

(v) Let L be a subgroup of H. We need to show that

$$\phi^{-1}(L) = \{g \in G \mid \phi(g) \in L\}$$

is a subgroup of G. Since $\phi(e_G) = e_H \in L$, we get that $e_G \in \phi^{-1}(L)$. So $\phi^{-1}(L)$ is nonempty. We need to show that $\phi^{-1}(L)$ is closed under multiplication and taking inverses. Now take any elements $a, b \in \phi^{-1}(L)$. Thus, we know that $\phi(a)$ and $\phi(b)$ are in L. Observes that, as ϕ preserves the operation, $\phi(ab) = \phi(a)\phi(b)$, moreover, $\phi(a)\phi(b) \in L$ since L is a subgroup of H. So $\phi(ab) \in L$ meaning that $ab \in \phi^{-1}(L)$. Next, observe that, by the properties of isomorphisms, $\phi(a^{-1}) = (\phi(a))^{-1}$, and as $\phi(a) \in L$ and $L \leq H$, we have $(\phi(a))^{-1} \in L$. So $\phi(a^{-1}) \in L$ meaning that $a^{-1} \in \phi^{-1}(L)$. This shows that $\phi^{-1}(L) \leq G$. ■

6.3 Automorphisms

Definition 6.3.1. (Automorphism)

An isomorphism from G to itself is called an *automorphism* of G.

Example 6.7.

(i) The map $0 \mapsto 0$, $1 \mapsto 3$, $2 \mapsto 2$, $3 \mapsto 1$ is an automorphism of $(\mathbb{Z}_4, +)$.

(ii) The map $\phi : \mathbb{Q} \to \mathbb{Q}$ where $\phi(x) = 3x$ is an automorphism of the group $(\mathbb{Q}, +)$.

(iii) The map $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ where $\phi(a, b) = (b, a)$ is an automorphism of $(\mathbb{R}^2, +)$.

(iv) The map $\phi : \mathbb{C} \to \mathbb{C}$ where $\phi(a + bi) = a - bi$ is an automorphism of $(\mathbb{C}, +)$.

(v) The map $\phi : \mathbb{C}^* \to \mathbb{C}^*$ where $\phi(a + bi) = a - bi$ is an automorphism of $(\mathbb{C}^*, \cdot)$.

Theorem 6.3.2.

The set of all automorphisms of a group G is a group under function composition, denoted as $\mathrm{Aut}(G)$.

Corollary 6.3.3.

Let G be a group. Then $\mathrm{Aut}(G)$ *is a subgroup of* $\mathrm{Sym}(G)$.

Lemma 6.3.4.

Let G be a cyclic group of order n, and let g and h be generators of G. Then the map $\alpha : G \to G$ given by $\phi(g^k) = h^k$ for $k \in \mathbb{Z}_n$ is an automorphism of G.

Example 6.8. Find $\mathrm{Aut}(\mathbb{Z}_{10})$.
We need to find all automorphisms $\alpha : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$. Recall that $(\mathbb{Z}_{10}, +)$ is cyclic and

$\mathbb{Z}_{10} = \langle 1 \rangle$. Since 1 is a generator and α is an automorphism, its image $\alpha(1)$ must be a generator of $\mathbb{Z}_{10}$ as well. We know that the generators of $\mathbb{Z}_{10}$ are precisely the integers coprime with 10, and so the only candidates for $\alpha(1)$ are 1, 3, 7, 9. Furthermore, the value $\alpha(1)$ determines the whole automorphism α. To see this, suppose that $\alpha(1) = a$ where a is one of the generators, and let k be any element in $\mathbb{Z}_{10}$. Then, by Theorem 6.2.1(iii), we get

$$\alpha(k) = \alpha(\underbrace{1 + 1 + \ldots + 1}_{k \text{ times}}) = \alpha(k \cdot 1) = k \cdot \alpha(1) = k \cdot a = \underbrace{a + a + \ldots + a}_{k \text{ times}}.$$

So $\alpha(k) = k \cdot a$, this is an automorphism of $\mathbb{Z}_{10}$ by Lemma 6.3.4. Thus, we have four automorphisms, one for each choice of the generator $a \in \{1, 3, 7, 9\}$. Let us call them $\alpha_1, \alpha_3, \alpha_7, \alpha_9$, respectively.

- $\alpha_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}$
- $\alpha_3 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 3 & 6 & 9 & 2 & 5 & 8 & 1 & 4 & 7 \end{bmatrix}$
- $\alpha_7 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{bmatrix}$
- $\alpha_9 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$

So $\mathrm{Aut}(\mathbb{Z}_{10}) = \{\alpha_1, \alpha_3, \alpha_7, \alpha_9\}$. But what is the group structure of $\mathrm{Aut}(\mathbb{Z}_{10})$? For example, to know the composition $\alpha_7\alpha_9$ we need to find the value $(\alpha_7\alpha_9)(1) = \alpha_7(\alpha_9(1)) = \alpha_7(9) = 3$. Therefore, $\alpha_7\alpha_9 = \alpha_3$. Here is the Cayley table of $\mathrm{Aut}(\mathbb{Z}_{10})$.

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

It is clear that this Cayley table is identical to that of the group of units $U_{10} = \{1, 3, 7, 9\}$. Therefore, $\mathrm{Aut}(\mathbb{Z}_{10}) \cong U_{10}$.

Motivated by the analysis done in the example above we can work out the automorphism group of $\mathbb{Z}_n$ and prove the following theorem.

Theorem 6.3.5.

Let $n \geq 1$. Then $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to U_n.

Proof. Let $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ be an automorphism of the group $\mathbb{Z}_n$. As 1 is a generator of $\mathbb{Z}_n$ and α is an automorphism, it must be that $\alpha(1)$ is also a generator of $\mathbb{Z}_n$. Since the generators of $\mathbb{Z}_n$ are elements which are coprime with n, we get that $\alpha(1) \in U_n$. We define a map $F : \mathrm{Aut}(\mathbb{Z}_n) \to U_n$ by setting $F(\alpha) = \alpha(1)$ for every $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$. We first show that F is injective. Let $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}_n)$ and assume that $F(\alpha) = F(\beta)$. Then $\alpha(1) = \beta(1)$. Now, take any $k \in \mathbb{Z}_n$ and, using Theorem 6.2.1(iii), observe that $\alpha(k) = \alpha(k \cdot 1) = k \cdot \alpha(1) = k \cdot \beta(1) = \beta(k \cdot 1) = \beta(k)$. Therefore, α and β agree on every $k \in \mathbb{Z}_n$ and so $\alpha = \beta$. Thus, F is injective. For surjectivity, choose any $a \in U_n$. A preimage of a under F is the automorphism $\gamma(k) = k \cdot a$ for $k \in \mathbb{Z}_n$ (see Lemma 6.3.4).

We check that $F(\gamma) = \gamma(1) = 1 \cdot a = a$ as wanted. Finally, we need to check that F is operation preserving. So let $\alpha, \beta \in \text{Aut}(\mathbb{Z}_n)$. Then,

$$F(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(\beta(1) \cdot 1) = \beta(1) \cdot \alpha(1) = \alpha(1) \cdot \beta(1) = F(\alpha) \cdot F(\beta).$$

Therefore, we have shown that $\text{Aut}(\mathbb{Z}_n) \cong U_n$. ■

Lemma 6.3.6.

Let G and H be groups. If $G \cong H$, then $\text{Aut}(G) \cong \text{Aut}(H)$.

Question. Is the converse of the previous lemma true?

Corollary 6.3.7.

Let C_n be a cyclic group of order n. Then $\text{Aut}(C_n) \cong U_n$.

Example 6.9. Find the automorphism group of the group of integers $(\mathbb{Z}, +)$.
The group of integers is cyclic and its only generators are 1 and -1. This gives two automorphisms of $\mathbb{Z}$, the first sends 1 to itself and the other sends 1 to -1. Thus, the only automorphisms of $\mathbb{Z}$ are the identity function and the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = -n$ for every $n \in Z$. It follows that $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

We next study a special type of group automorphisms.

Definition 6.3.8. (Conjugation)

Let G be a group and fix some element $g \in G$. The map of *conjugation by g* is the map $\phi_g : G \to G$ where for any $x \in G$ we define

$$\phi_g(x) = gxg^{-1}.$$

Notation. We often write x^g for the element gxg^{-1}.

Lemma 6.3.9.

Let G be a group and $g \in G$. Then the conjugation-by-g map ϕ_g is an automorphism of G.

Proof. We first show that ϕ_g is injective. So suppose that $\phi_g(x) = \phi_g(y)$ for some elements $x, y \in G$. It follows that $gxg^{-1} = gyg^{-1}$. By multiplying the equation by g^{-1} from the left and by g from the right we get that $x = y$ as desired. Next, we show that ϕ_g is surjective. So let $h \in G$. Then a preimage of h is the element $g^{-1}hg \in G$ since $\phi_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h$. It remains to show that the bijection $\phi_g : G \to G$ preserves the operation of G. So let $x, y \in G$. Then

$$\phi_g(xy) = g(xy)g^{-1} = gxeyg^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y).$$

Thus, ϕ_g is an automorphism of the group G for any $g \in G$. ■

Definition 6.3.10. (Inner Automorphism)

The conjugation-by-g map ϕ_g is called the *inner automorphism* of G induced by g.

Example 6.10.

(1) Fix a matrix A in the group $GL(n,\mathbb{R})$. Then the inner automorphism of $GL(n,\mathbb{R})$ induced by A is the map $\phi_A(X) = AXA^{-1}$ for any $X \in GL(n,\mathbb{R})$.
For example, let $A = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix}$ and $X = \begin{bmatrix} 4 & 5 \\ 2 & 3 \end{bmatrix}$ be matrices in $GL(2,\mathbb{R})$. Then,

$$\phi_A(X) = AXA^{-1} = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 10 & -8 \\ 4 & -3 \end{bmatrix}.$$

(2) Find the inner automorphism $\phi_{R_{90}}$ of D_4 induced by the rotation R_{90}. Let $X \in D_4$. Then $\phi_{R_{90}}(X) = R_{90}\, X\, (R_{90})^{-1} = R_{90}\, X\, R_{270}$. This gives the following map.

X	R_0	R_{90}	R_{180}	R_{270}	H	V	D	L
$\phi_{R_{90}}(X)$	R_0	R_{90}	R_{180}	R_{270}	V	H	L	D

Recall that rotations commute with each other.

Theorem 6.3.11.

The set of all inner automorphisms of a group G, denoted by $\mathrm{Inn}(G)$*, is a group under function decomposition.*

Corollary 6.3.12.

For any group G, we have that

$$\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq \mathrm{Sym}(G).$$

Example 6.11. If G is abelian, then $\mathrm{Inn}(G)$ is the trivial group, that is, $\mathrm{Inn}(G) = \{\phi_e\}$ where e is the identity of G. To see this, let g be any element in G. As G is abelian, we get that $\phi_g(x) = gxg^{-1} = xgg^{-1} = xe = x$ for every $x \in G$. Therefore, ϕ_g is the identity map for all $g \in G$ and so the only inner automorphism is the identity automorphism.

Example 6.12. Show that $\mathrm{Inn}(D_4) = \{\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D\}$.
The inner automorphisms of D_4 are ϕ_{R_0}, $\phi_{R_{90}}$, $\phi_{R_{180}}$, $\phi_{R_{270}}$, ϕ_H, ϕ_V, ϕ_D, ϕ_L. However, this list may have repetitions, that is, two or more different elements of D_4 induce the same inner automorphism.

- Since R_{180} belongs to the center of D_4 we obtain that

  $$\phi_{R_{180}}(X) = R_{180}\, X\, (R_{180})^{-1} = X\, R_{180}\, (R_{180})^{-1} = X$$

  for any $X \in D_4$. So $\phi_{R_{180}} = \phi_{R_0}$.

- Since $R_{270} = R_{90}R_{180}$, we have

  $$\phi_{R_{270}}(X) = R_{270}X(R_{270})^{-1} = R_{90}R_{180}X(R_{180})^{-1}(R_{90})^{-1} = R_{90}X(R_{90})^{-1} = \phi_{R_{90}}(X)$$

for any $X \in D_4$. So $\phi_{R_{270}} = \phi_{R_{90}}$.

- Since $H = VR_{180}$, we have

$$\phi_H(X) = HXH^{-1} = VR_{180}X(R_{180})^{-1}V^{-1} = VXV^{-1} = \phi_V(X)$$

for any $X \in D_4$. So $\phi_H = \phi_V$.

- Since $D = LR_{180}$, we have

$$\phi_D(X) = DXD^{-1} = LR_{180}X(R_{180})^{-1}(L)^{-1} = LX(L)^{-1} = \phi_L(X)$$

for any $X \in D_4$. So $\phi_D = \phi_L$.

Thus, the previous list of inner automorphisms of D_4 reduces to ϕ_{R_0}, $\phi_{R_{90}}$, ϕ_H, ϕ_D. It remains to check that these four automorphisms are distinct.

6.4 Cayley's Theorem

Cayley's Theorem says that any group lives inside some symmetric group as a subgroup.

Theorem 6.4.1. (Cayley's Theorem; 1854)

Any group is isomorphic to a permutation group.

Proof. Let $(G, \cdot)$ be a group. We will show that G is isomorphic to a subgroup of the symmetric group $\mathrm{Sym}(G)$. Fix an element $g \in G$. We define a permutation α_g of the set G as follows: for any $x \in G$, define $\alpha_g(x) = g \cdot x$. By closure of the group operation, the function α_g is a function from G to G. We now show that α_g is a bijection and so it is a permutation of the set G. Suppose that $\alpha_g(x) = \alpha_g(y)$. Then $g \cdot x = g \cdot y$. By the cancellation property in groups, we obtain that $x = y$ showing that α_g is injective. For surjectivity, choose any element $y \in G$, then the group element $x = g^{-1} \cdot y$ is its preimage. To see this, observe that $\alpha_g(x) = g \cdot x = g \cdot (g^{-1} \cdot y) = (g \cdot g^{-1}) \cdot y = e \cdot y = y$. Therefore, the map $\alpha_g : G \to G$ is a bijection and so α_g belongs to $\mathrm{Sym}(G)$.

Claim. For any $g, h \in G$, we have that $\alpha_g \circ \alpha_h = \alpha_{(g \cdot h)}$.
To see this, choose an element $x \in G$ and observe that

$$(\alpha_g \circ \alpha_h)(x) = \alpha_g(\alpha_h(x)) = \alpha_g(h \cdot x) = g \cdot (h \cdot x) = (g \cdot h) \cdot x = \alpha_{g \cdot h}(x).$$

Thus, the permutations $\alpha_g \circ \alpha_h$ and $\alpha_{g \cdot h}$ agree on every point in their domain. This proves the claim.

Next, let $H = \{\alpha_g \mid g \in G\}$. Clearly, $H \subseteq \mathrm{Sym}(G)$. We claim that H is a subgroup of $\mathrm{Sym}(G)$. Clearly, H is not empty since it contains the identity map $\alpha_e : G \to G$ where e is the identity of G. Now, let α_g and α_h be in H. We need to show that their composition $\alpha_g \circ \alpha_h$ is in H as well, but it follows from the claim that $\alpha_g \circ \alpha_h = \alpha_{(g \cdot h)}$ and as $g \cdot h \in G$ by closure of the group operation, we get $\alpha_{g \cdot h} \in H$. Next, we need to show that H is closed under taking inverses. From what we have just established it follows that $\alpha_g \circ \alpha_{g^{-1}} = \alpha_{g \cdot g^{-1}} = \alpha_e$ and as α_e is the identity element of $\mathrm{Sym}(G)$ it follows that $(\alpha_g)^{-1} = \alpha_{g^{-1}}$. As $\alpha_{g^{-1}} \in H$ we have that $(\alpha_g)^{-1} \in H$ as wanted. Therefore, H is a subgroup of $\mathrm{Sym}(G)$.

It remains to show that the group $(G, \cdot)$ is isomorphic to $(H, \circ)$. The isomorphism is obvious, consider the function $\phi : G \to H$ where $\phi(g) = \alpha_g$ for every $g \in G$. (The map ϕ is called the *left regular representation of* G.) First, we need to show that ϕ is injective. So suppose that $g, h \in G$ and that $\phi(g) = \phi(h)$. Then $\alpha_g = \alpha_h$, and so $\alpha_g(e) = \alpha_h(e)$ which implies that $g \cdot e = h \cdot e$, and thus $g = h$ showing that ϕ is injective. By construction of the group H we see that ϕ is surjective. It remains to show that ϕ is operation-preserving, choose any elements $g, h \in G$ and by the claim we get that

$$\phi(g \cdot h) = \alpha_{g \cdot h} = \alpha_g \circ \alpha_h = \phi(g) \circ \phi(h).$$

Therefore, ϕ is an isomorphism from G to H and also $H \leq \mathrm{Sym}(G)$, that is, G is isomorphic to a subgroup of a symmetric group. ■

Example 6.13. Compute the left regular representation for $U_{12} = \{1, 5, 7, 11\}$. We need to compute the function ϕ which sends every element $g \in U_{12}$ to the permutation $\alpha_g : U_{12} \to U_{12}$ given by $\alpha_g(x) = gx$ for every $x \in U_{12}$.

- $\alpha_1 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}$.
- $\alpha_7 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}$.
- $\alpha_5 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix}$.
- $\alpha_{11} = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}$.

Observe that $H = \{\alpha_1, \alpha_5, \alpha_7, \alpha_{11}\}$ is a subgroup of $\mathrm{Sym}(U_{12})$ and it is isomorphic to U_{12}.

Chapter 7

Cosets

7.1 Properties of Cosets

Let G be a group and $H \subseteq G$. For a fixed $g \in G$ we define the following subsets of G:

- $gH = \{gh \mid h \in H\}$
- $Hg = \{hg \mid h \in H\}$
- $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$

Definition 7.1.1. (Coset)

Suppose that H is a subgroup of G and $g \in H$. We call the set gH the *left coset* of H containing g. And we call the set Hg the *right coset* of H containing g. We also say that g is a *coset representative* of the cosets gH and Hg.

Observe that an element $a \in G$ belongs to the coset gH if and only if there exists $h \in H$ such that $a = gh$.

Example 7.1.

- In S_3, find all left cosets of the subgroup $H = \{(1), (13)\}$.
  1. $(1)H = H = (13)H$.
  2. $(12)H = \{(12), (132)\} = (132)H$.
  3. $(23)H = \{(23), (123)\} = (123)H$.
- In D_4, find all left cosets of the subgroup $\mathcal{K} = \{R_0, R_{180}\}$.
  1. $R_0\,\mathcal{K} = \{R_0, R_{180}\} = \mathcal{K} = R_{180}\,\mathcal{K}$.
  2. $R_{90}\,\mathcal{K} = \{R_{90}, R_{270}\} = R_{270}\,\mathcal{K}$.
  3. $H\,\mathcal{K} = \{H, V\} = V\,\mathcal{K}$.
  4. $D\,\mathcal{K} = \{D, L\} = L\,\mathcal{K}$.
- In $\mathbb{Z}_9 = \{0, 1, 2, \ldots, 8\}$, find all left cosets of the subgroup $H = \{0, 3, 6\}$.
  1. $0 + H = \{0, 3, 6\} = 3 + H = 6 + H$.

2. $1 + H = \{1, 4, 7\} = 4 + H = 7 + H$.

3. $2 + H = \{2, 5, 8\} = 5 + H = 8 + H$.

- In $(\mathbb{R}^3, +)$, consider the subgroup $H = \{(x, y, 0) \mid x, y \in \mathbb{R}\}$. The coset of H represented by an element $(a, b, c) \in \mathbb{R}^3$ is the set

$$(a, b, c) + H = \{(a + x, b + y, c) \mid x, y \in \mathbb{R}\} = \{(u, v, c) \mid u, v \in \mathbb{R}\}$$

which is the plane parallel to H containing the point (a, b, c).

Theorem 7.1.2.

Let H be a subgroup of G, and let $a, b \in G$. Then the following hold.

(i) $a \in aH$. *In words, The coset aH contains its representative a.*

(ii) $a \in H$ *if and only if* $aH = H$. *In words, H absorbs its elements.*

(iii) $(ab)H = a(bH)$ *and* $H(ab) = (Ha)b$.

(iv) $a \in bH$ *if and only if* $aH = bH$. *In words, any element in a coset represents the coset.*

(v) $aH = bH$ *if and only if* $a^{-1}b \in H$.

(vi) $aH = bH$ *or* $aH \cap bH = \emptyset$. *In words, Two cosets are either equal or disjoint.*

(vii) $|aH| = |bH|$. *In words, all cosets have the same cardinality.*

(viii) $|aH| = |H|$. *In words, the number of elements in any coset is equal to the number of elements in the subgroup H.*

(ix) $aH = Ha$ *if and only if* $H = aHa^{-1}$.

(x) aH *is a subgroup of G if and only if $a \in H$. In words, the only coset of H that is a subgroup of G is H itself.*

Proof. Let H be a subgroup of G, and let $a, b \in G$.

(i) As H is a subgroup of G we know that the identity $e \in H$. So $ae \in aH$ and also $a = ae$, thus $a \in aH$.

(ii) Suppose $a \in H$. We will show that aH and H are subsets of each other. To show that $aH \subseteq H$, let $x \in aH$. So there is $h \in H$ such that $x = ah$. Since both $a, h \in H$ and H is a subgroup, their product $ah \in H$, so $x \in H$ showing that $aH \subseteq H$. Next, choose an element $h \in H$. As $a \in H$ and H is a subgroup we know that $a^{-1} \in H$ and consequently $a^{-1}h \in H$. It follows that $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$.So $H \subseteq aH$, and therefore $aH = H$. We have show that if $a \in H$, then $aH = H$.
For the converse, suppose that $aH = H$. Since $a \in aH$ by Part (i), we get that $a \in H$.

(iii) Since the group operation is associative, it follows that $(ab)H = \{(ab)h \mid h \in H\} = \{a(bh) \mid h \in H\} = a\{bh \mid h \in H\} = a(bH)$.

(iv) Suppose that $a \in bH$. Then there exists $h \in H$ such that $a = bh$. We then have that $aH = (bh)H = b(hH) = bH$ since $hH = H$ by Part (ii). For the converse, assume that $aH = bH$. Then, by Part (i), we know that $a \in aH$, so $a \in bH$.

(v) By Part (ii) and Part (iii) we have that $aH = bH$ if and only if $a^{-1}(aH) = a^{-1}(bH)$ if and only if $(aa^{-1})H = (a^{-1}b)H$ if and only if $eH = (a^{-1}b)H$ if and only if $H = (a^{-1}b)H$ if only if $a^{-1}b \in H$.

(vi) If $aH \cap bH = \emptyset$, we are done. Otherwise, there exists $c \in aH \cap bH$. Since $c \in aH$, we get that $cH = aH$. Also, since $c \in bH$, we get that $cH = bH$. Therefore, $aH = cH = bH$.

(vii) To show that $|aH| = |bH|$ we show that the map $f : aH \to bH$ which maps $ah \mapsto bH$ for each $h \in H$ is a bijection. Clearly, f is surjective. For injectivity, assume that $f(ah_1) = f(ah_2)$. Then $bh_1 = bh_2$, and by left cancellation, we get that $h_1 = h_2$, and so $ah_1 = ah_2$.

(viii) By Part (vii), we have that $|aH| = |eH| = |H|$.

(ix) $aH = Ha$ if and only if $a^{-1}(aH) = a^{-1}(Ha)$ if and only if $(a^{-1}a)H = a^{-1}Ha$ if and only if $eH = a^{-1}Ha$ if and only if $H = a^{-1}Ha$.

(x) Suppose that the coset aH is a subgroup of G. Then $e \in aH$ and so $eH = aH$. But $eH = H$, so $H = aH$, and thus $a \in H$. Conversely, if $a \in H$, then $aH = H$, and H is a subgroup of G.

■

Recall that a partition of a set S is a collection of a pairwise disjoint nonempty subsets whose union is the whole set S. These subsets are called the parts of the partition.

Corollary 7.1.3.

The distinct left cosets of a subgroup H of a group G partition G.

Proof. For simplicity suppose G is a finite group. Let $a_1H, a_2H, a_3H, \ldots, a_nH$ be a list of all distinct cosets of H in G. Since these cosets are distinct, they must be disjoint. Since $a_i \in a_iH$ we know that a_iH is a nonempty set. Finally, it remains to show that $G = a_1H \cup a_2H \cup \cdots \cup a_nH$. Clearly, $a_1H \cup a_2H \cup \cdots \cup a_nH \subseteq G$. For the other inclusion, let $g \in G$, and consider the coset gH. There must be some $1 \leq i \leq n$ such that $gH = a_iH$. Thus, $g \in a_iH$ and so $G \subseteq a_1H \cup a_2H \cup \cdots \cup a_nH$. ■

Given a partition of a set S, we know that the relation on S defined by declaring two elements in S to be related if they belong to the same part is an equivalence relation.

Corollary 7.1.4.

Let H be a subgroup of G. The relation $\sim$ defined by $a \sim b$ if and only if $aH = bH$ for any $a, b \in G$ is an equivalence relation on G. Moreover, the equivalence classes of $\sim$ are the cosets of H.

7.2 Lagrange's Theorem

Theorem 7.2.1. (Lagrange's Theorem)

The order of a subgroup of a finite group divides the order of the group.

Proof. Let H be a subgroup of a finite group G. Let n be the number of distinct cosets of H in G. And let $a_1H, a_2H, a_3H, \ldots, a_nH$ be a list of all distinct (not equal as sets) cosets of H in G. We know that $G = a_1H \cup a_2H \cup \cdots \cup a_nH$. As distinct cosets are disjoint and all cosets have the same cardinality we get the following

$$\begin{aligned} |G| &= |a_1H \cup a_2H \cup \cdots \cup a_nH| \\ &= |a_1H| + |a_2H| + \cdots + |a_nH| \\ &= |H| + |H| + \cdots + |H| \\ &= n|H|. \end{aligned}$$

Therefore, $|G| = n|H|$, meaning that $|H|$ divides $|G|$. ■

Definition 7.2.2. (Index of a Subgroup)

The *index* of a subgroup H in G is the number of distinct left cosets of H in G. This number is denoted by $[G : H]$ or $|G : H|$.

The proof of Lagrange's Theorem tells us how to compute the index of H in G.

Corollary 7.2.3.

Let G be a finite group and let H be a subgroup of G. Then

$$[G : H] = |G| \Big/ |H|.$$

Corollary 7.2.4.

Suppose that G is a finite group. If m does not divide $|G|$, then G has no subgroups of order m.

Corollary 7.2.5.

Let G be a finite group. Then for any $g \in G$, we have that
(i) $|g|$ divides $|G|$.
(ii) $g^{|G|} = e$.

Proof. (i) Let $g \in G$. By Lagrange's Theorem, we know that the order of the subgroup $\langle g \rangle$ generated by g divides $|G|$. But $|\langle g \rangle| = |g|$. So $|g|$ divides $|G|$.

(ii) Let $|g| = m$. We know that m divides $|G|$, and so $|G| = km$ for some integer k. Thus, $g^{|G|} = g^{km} = (g^m)^k = e^k = e$. ■

Corollary 7.2.6.

If G is a finite group of prime order, then G is cyclic. Moreover, all non-identity elements of G are generators.

Proof. Suppose that G is a group where $|G| = p$ for some prime p. Let $g \in G$ be an element different from the identity element which exists since $p \geq 2$. By Lagrange's

Theorem we know that $|g|$ divides $|G|$, and so $|g|$ divides the prime p meaning that $|g| = 1$ or $|g| = p$. As $g \neq e$, it must be $|g| = p$. Therefore, $\langle g \rangle$ contains p elements. Since G has exactly p elements and $\langle g \rangle \subseteq G$, it must be that $G = \langle g \rangle$. ■

Corollary 7.2.7.

If G is a group of prime order p, then $G \cong \mathbb{Z}_p$.

The converse of Lagrange's Theorem is false. That is, if d divides the order of a finite group G, then we cannot guarantee the existence of a subgroup of G of order d.

Example 7.2. We will show that the converse of Lagrange's Theorem is false by showing that the alternating group A_4 of order 12 has no subgroups of order 6.

$$A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$$

Towards a contradiction, assume A_4 has a subgroup H of order 6. Let $\alpha \in A_4$ be an arbitrary permutation of order 3. We will show that $\alpha \in H$. Towards a contradiction, suppose that $\alpha \notin H$. It follows that the coset $\alpha H \neq H$ and so $A_4 = H \cup \alpha H$. Now, either $\alpha^2 \in H$ or $\alpha^2 \in \alpha H$. If $\alpha^2 \in H$, then $\alpha^4 \in H$ but $\alpha^4 = \alpha^3\alpha = \alpha$, a contradiction as $\alpha \notin H$. So it must be that $\alpha^2 \in \alpha H$. This means that $\alpha^2 = \alpha h$ for some $h \in H$. By left cancellation, we get $\alpha = h$ and so $\alpha \in H$, a contradiction as well. Therefore, α must be in H, and since α was arbitrary we conclude that H contains all permutations of order 3. Observe that A_4 has eight permutations of order 3 (those of cycle type [3]). It follows that all of the eight permutations of order 3 are in H, but H has six elements!

Corollary 7.2.8. (Fermat's Little Theorem)

For every prime p and every integer a, we have that

$$a^p \equiv a \pmod{p}.$$

Proof. Let p be a prime and let a be an integer. By the division algorithm, there are integers k and r such that $a = kp + r$ and $0 \leq r < p$. First, we will show the theorem for the remainder r. If $r = 0$, then $0^p \equiv 0 \pmod{p}$. Otherwise, $1 \leq r \leq p - 1$, and thus, $r \in U_p$. The order of the group $U_p = \{1, 2, \ldots, p - 1\}$ is $p - 1$. By a corollary of Lagrange's Theorem, we know that $r^{|U_p|} = 1$, and so $r^{p-1} = 1$. It follows that $r^p = r$ in U_p, which means $r^p \bmod p = r \bmod p$. Recall that two integers have the same remainder modulo p if and only if they are congruent modulo p. Therefore, $r^p \equiv r \pmod{p}$.
Next, as $a \equiv r \pmod{p}$, we get $a^p \equiv r^p \pmod{p}$. Since $a^p \equiv r^p \pmod{p}$ and $r^p \equiv r \pmod{p}$, we get $a^p \equiv r \pmod{p}$. Finally, since $a^p \equiv r \pmod{p}$ and $r \equiv a \pmod{p}$, we get $a^p \equiv a \pmod{p}$ as desired. ■

Theorem 7.2.9.

Suppose that H and K are finite subgroups of a group. Then,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Remark. The dihedral group D_n is completely determined by the following properties.

(i) D_n has an element r of order n.

(ii) D_n has an element f of order 2.

(iii) These two elements satisfy $rf = fr^{-1}$.

(iv) $D_n = \langle r, f \rangle$. (We say that r and f are the generators of D_n.)

We express this by writing the "*presentation*" of D_n as

$$D_n = \langle r, f \mid r^n = e,\ f^2 = e,\ rfrf = 1 \rangle.$$

Theorem 7.2.10.

Let G be a group of order $2p$ for some prime $p > 2$. Then $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.

Corollary 7.2.11.

$S_3 \cong D_3$.

Chapter 8

Quotient Groups

8.1 Normal Subgroups

Are left cosets equal to right cosets in general? Consider the subgroup $H = \{(1), (12)\}$ of the symmetric group S_3. The left coset of H represented by (123) is not equal to the corresponding right coset, that is, $(123)H \neq H(123)$. To see this observe that the left coset is $(123)H = \{(123), (13)\}$, however, the right coset is $H(123) = \{(123), (23)\}$. Some subgroups are special in the sense that each left coset of such a subgroup is equal to its corresponding right coset. We will see that this is also equivalent to having that these subgroups are invariant under conjugation by members of the group which they live in. Such subgroups are essential in constructing quotient groups.

Definition 8.1.1. (Normal Subgroup)

A subgroup N of a group G is called *normal* if for any $g \in G$ and for any $n \in N$ we have that $gng^{-1} \in N$. We denote this by $N \trianglelefteq G$ or $N \triangleleft G$.

The following remark is an immediate consequence of the definition of a normal subgroup. It says that we can flip the order of multiplying a group member with a member of the normal subgroup with possibly changing the latter with another member from the normal subgroup.

Lemma 8.1.2.

Suppose $N \trianglelefteq G$. Then for any $g \in G$ and any $n \in N$, there exist $n', n'' \in N$ such that $gn = n'g$ and $ng = gn''$.

Proof. Let $N \trianglelefteq G$. Choose $g \in G$ and $n \in N$. Since N is normal we know that $gng^{-1} \in N$ and $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Thus, there are $n', n'' \in N$ such that $gng^{-1} = n'$ and $g^{-1}ng = n''$. Therefore, $gn = n'g$ and $ng = gn''$. ■

Example 8.1.

- $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$ for any group G.
- Any subgroup of an abelian group is normal.
  Suppose that G is an abelian group and $N \leq G$. For any $g \in G$ and $n \in N$, we have that $gng^{-1} = ngg^{-1} = ne = n \in N$.

- The center of any group is a normal subgroup.
  Let G be a group. Choose $g \in G$ and $z \in Z(G)$. Then $gzg^{-1} = zgg^{-1} = ze = z \in Z(G)$. Therefore, $Z(G) \trianglelefteq G$.
- The alternating subgroup A_n is a normal subgroup of the symmetric group S_n for every $n \geq 1$. To show this one needs to check that the conjugation of an even permutation with any permutation is also even. For example, for $(12) \in S_3$ and $(123) \in A_3$, we have $(12)(123)((12))^{-1} = (12)(123)(12) = (132) \in A_3$.
- Any subgroup of rotations is normal in D_n. To see this observe that for any rotation R and and any reflection F, we have that $FR = R^{-1}F$.
- If H is the only subgroup of G of order $|H|$, then $H \trianglelefteq G$.
- $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

Example 8.2 (Non-example)**.** The subgroup $K = \{(1), (123), (132)\}$ is *not* normal in A_4. To see this choose the permutation $\alpha = (12)(34) \in A_4$ and the permutation $\beta = (123) \in K$, and then consider the conjugation of β by α.

$$\alpha\beta\alpha^{-1} = (12)(34)\,(123)\,((12)(34))^{-1} = (12)(34)\,(123)\,(34)(12) = (142) \notin K.$$

The following notions are all equivalent to the notion of a normal subgroup.

Theorem 8.1.3.

Let G be a group and N be a subgroup of G. Then the following are equivalent.

(i) For any $g \in G$ and for any $n \in N$ we have that $gng^{-1} \in N$.

(ii) For any $g \in G$ we have that $gNg^{-1} \subseteq N$.

(iii) For any $g \in G$ we have that $gNg^{-1} = N$. In words, the subgroup N is invariant under conjugation (inner automorphisms).

(iv) For any $g \in G$ we have that $gN = Ng$. In words, each left coset of N is equal to the corresponding right coset.

Proof. $(i) \Rightarrow (ii)$ Suppose (i). Let $g \in G$, and choose an element $x \in gNg^{-1}$. Thus, there exists $n \in N$ such that $x = gng^{-1}$. By (i), the element $gng^{-1} \in N$ and so $x \in N$. Thus, $gNg^{-1} \subseteq N$.

$(ii) \Rightarrow (iii)$ Assume (ii). Let $g \in G$. By (ii) we get that $gNg^{-1} \subseteq N$. It remains to show that $N \subseteq gNg^{-1}$. Pick an element $n \in N$. By (ii) we know that $g^{-1}ng \in N$. And so $n = (gg^{-1})n(gg^{-1}) = g(g^{-1}ng)g^{-1} \in gNg^{-1}$. This shows that $N \subseteq gNg^{-1}$. Thus, $gNg^{-1} = N$.

$(iii) \Rightarrow (iv)$ Assume (iii). Let $g \in G$. By (iii) we know that $gNg^{-1} = N$, it follows that $(gNg^{-1})g = Ng$, and thus $gN(g^{-1}g) = Ng$, and so $gNe = Ng$, and therefore $gN = Ng$.

$(iv) \Rightarrow (i)$ Assume (iv) and let $g \in G$ and $n \in N$. By (iv), we get that $gN = Ng$, and so $gNg^{-1} = N$. Since $gng^{-1} \in gNg^{-1}$, it follows that $gng^{-1} \in N$. ∎

In general the set of products HK of subgroups H and K need not to be a subgroup. However, if one of the subgroups is normal, then this is sufficient for their product to be a subgroup as well.

Lemma 8.1.4.

Let G be a group, $N \trianglelefteq G$, and $K \leq G$. Then

$$NK = \{nk \mid n \in N, k \in K\}$$

is a subgroup of G.

Proof. The set NK is nonempty as it contains the identity element since $e = ee \in NK$. Let x and y be any members of NK. In order to show that NK is a subgroup we will show that $xy^{-1} \in NK$. We know that there are $n_1, n_2 \in N$ and $k_1, k_2 \in K$ such that $x = n_1k_1$ and $y = n_2k_2$. Since N is a normal subgroup and $n_2^{-1} \in N$, there exists an element $n' \in N$ such that $(k_1k_2^{-1})n_2^{-1} = n'(k_1k_2^{-1})$. We now proceed as follows,

$$xy^{-1} = n_1k_1(n_2k_2)^{-1} = n_1k_1k_2^{-1}n_2^{-1} = n_1(k_1k_2^{-1})n_2^{-1} = n_1n'(k_1k_2^{-1}) = (n_1n')(k_1k_2^{-1}) \in NK.$$

This shows that NK is a subgroup. ■

Example 8.3. In D_4, let $N = \{R_0, R_{180}\}$, and $K = \{R_0, H\}$. Observe that $N \trianglelefteq D_4$. Thus, we get that $NK = \{RF \mid R \in N, F \in K\} = \{R_0, R_{180}, H, V\}$ is a subgroup of D_4.

8.2 Quotient Groups

Theorem 8.2.1. (Otto Hölder; 1889)

Let N be a normal subgroup of a group G. The set

$$G/N = \{gN \mid g \in G\}$$

of all left cosets of N in G is a group under the binary operation

$$(aN) * (bN) = (ab)N$$

for any $a, b \in G$.

Proof. First, we need to show that the operation of coset multiplication defined above from $G/N \times G/N \to G/N$ is well-defined, that is, this operation does not depend on the coset representatives but only on the cosets themselves. We will show that for any $a, b, x, y \in G$, if $aN = xN$ and $bN = yN$, then $(aN) * (bN) = (xN) * (yN)$, that is, $(ab)N = (xy)N$. Suppose $aN = xN$ and $bN = yN$. Then $a \in xN$ and $b \in yN$ and thus there exist $n, m \in N$ such that $a = xn$ and $b = ym$. Recall that a subgroup absorbs its elements and each left coset of the normal subgroup N is equal to its corresponding right coset. This being said, we proceed as follows.

$$(ab)N = abN = xnymN = xnyN = xnNy = xNy = xyN = (xy)N.$$

The identity element of G/N is $N = eN$. To see this, let $gN \in G/N$. Observe that $(eN) * (gN) = (eg)N = gN$. The inverse of the coset gN is the coset $g^{-1}N$ because

$(gN) * (g^{-1}N) = (gg^{-1})N = eN = N$. It remains that coset multiplication is associative. Let $a, b, c \in G$ and observe that

$$(aN * bN) * cN = (ab)N * cN = ((ab)c)N = (a(bc))N = aN * (bc)N = aN * (bN * cN).$$

This proves that the set G/N with coset multiplication is a group. ■

Definition 8.2.2. (Quotient Group)

Let N be a normal subgroup of a group G. The *quotient group* (or *factor group*) of G by N is the group whose underlying set is the set of all left cosets of N in G, that is, $G/N = \{gN \mid g \in G\}$, and whose binary operation is coset multiplication where $(aN) * (bN) = (ab)N$ for any $a, b \in G$.

Remark. For a finite group G, the order of a quotient group G/N is the index of N in G. That is,

$$|G/N| = [G : N] = |G|/|N|.$$

Lemma 8.2.3.

Let H be a subgroup of a group G. If the set of all left cosets of H in G forms a group under coset multiplication, then H is normal in G.

Proof. Let $H \leq G$ and assume that the set G/H of left cosets is a group under coset multiplication. We need to show that H is a normal subgroup. So let $g \in G$ and $h \in H$. On one hand, $(gH) * (hH) * (g^{-1}H) = (ghg^{-1})H$. On the other hand, as the H is the identity element of the group G/H we get that $(gH)*(hH)*(g^{-1}H) = (gH)*H*(g^{-1}) = (gH) * (g^{-1}H) = (gg^{-1})H = eH = H$. Thus, $(ghg^{-1})H = H$ and so $ghg^{-1} \in H$. This proves that $H \trianglelefteq G$. ■

Example 8.4 (Non-example)**.** We have seen previously that the subgroup K given below is not normal in A_4. The left cosets of K are:

- $K = \{(1), (123), (132)\}$
- $(124)K = \{(124), (14)(23), (134)\}$
- $(142)K = \{(142), (234), (13)(24)\}$
- $(143)K = \{(143), (12)(34), (243)\}$

So the set of left cosets is $G/K = \{K, (124)K, (142)K, (143)K\}$. The product of cosets is not a well-defined binary operation on G/K. To see this, observe that:

$$(124)K * (142)K = (124)(142)K = (1)K = K;$$
$$(124)K * (142)K = (134)K * (234)K = (134)(234)K = (13)(24)K = (142)K.$$

However, $K \neq (142)K$. Thus, the product $(124)K * (142)K$ is not defined. The moral of the story is that when a subgroup H is not normal in G the coset operation given by $(aH) * (bH) = (ab)H$ is not a function from $G \times G \to G$.

Remark. When we quotient G by a normal subgroup N, we are declaring every element in N to represent the identity element of G/N. Algebraists refer to this process as "killing" the subgroup N.

Example 8.5. Compute the following quotient groups. Remember that any subgroup of an abelian group is normal.

- Find the quotient group G/N of the group $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ by the subgroup $N = \{1, 4\}$. The left cosets of N in U_{15} are N, $2N = \{2, 8\}$, $7N = \{7, 13\}$, and $11N = \{11, 14\}$.

$$U_{15}/N = \{N,\ 2N,\ 7N,\ 11N\}$$

Here is the Cayley table of the group U_{15}/N.

$*$	N	$2N$	$7N$	$11N$
N	N	$2N$	$7N$	$11N$
$2N$	$2N$	N	$11N$	$7N$
$7N$	$7N$	$11N$	N	$2N$
$11N$	$11N$	$7N$	$2N$	N

Observe that this group is not cyclic and so it is not isomorphic to $\mathbb{Z}_4$.

- Recall that $Z = Z(D_4) = \{R_0, R_{180}\}$. We know that $Z \trianglelefteq D_4$. Then the quotient group of D_4 by its center is $D_4/Z = \{Z, R_{90}Z, HZ, DZ\}$.

$*$	Z	$R_{90}Z$	HZ	DZ
Z	Z	$R_{90}Z$	HZ	Dz
$R_{90}Z$	$R_{90}Z$	Z	DZ	HZ
HZ	HZ	DZ	Z	$R_{90}Z$
DZ	DZ	HZ	$R_{90}Z$	Z

- Recall that $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ is a subgroup of the group of integers $(\mathbb{Z}, +)$. The quotient group of $\mathbb{Z}$ by $4\mathbb{Z}$ is $\mathbb{Z}/4\mathbb{Z} = \Big\{4\mathbb{Z},\ 1 + 4\mathbb{Z},\ 2 + 4\mathbb{Z},\ 3 + 4\mathbb{Z}\Big\}$.

$+$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$0 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$1 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$
$2 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$
$3 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$

Observe that $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$.

- In the group $\mathbb{Z}_{18}$ we have that $\langle 6\rangle = \{0, 6, 12\}$. The left cosets of $\langle 6\rangle$ in $\mathbb{Z}_{18}$ are $\mathbb{Z}_{18}/\langle 6\rangle = \Big\{\langle 6\rangle,\ 1 + \langle 6\rangle,\ 2 + \langle 6\rangle,\ 3 + \langle 6\rangle,\ 4 + \langle 6\rangle,\ 5 + \langle 6\rangle\Big\}$. For instance, observe that

$$(4 + \langle 6\rangle) + (5 + \langle 6\rangle) = (4 + 5) + \langle 6\rangle = 9 + \langle 6\rangle = \{9, 15, 3\} = 3 + \langle 6\rangle.$$

Lemma 8.2.4.

For any positive integer n, we have that $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Moreover,

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z},\ 1 + n\mathbb{Z},\ 2 + n\mathbb{Z},\ \ldots,\ (n-1) + n\mathbb{Z}\} \quad \textit{and} \quad \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

Remark. The importance of quotient groups is that the structure of G/N is usually less complicated than that of G, but still we can deduce information about G from G/N.

Theorem 8.2.5.

Let $Z(G)$ be the center of a group G. If $G/Z(G)$ is cyclic, then G is abelian.

Proof. Let G be a group and let Z be the center of G. Suppose that the quotient group G/Z is cyclic and that gZ is a generator of G/Z. Pick an arbitrary element $a \in G$. Then there is an integer k such that the coset $aZ = (gZ)^k = g^kZ$. It follows that there is a central element $z \in Z$ such that $a = g^kz$. Since both g^k and z are in the centralizer $C(g)$ of the element g it follows that their product a is also in the centralizer of g. Because the element a is an arbitrary element of G it means that $G = C(g)$, in other words, g commutes with all elements of the group. Therefore, $g \in Z$, and thus, the generator $gZ = Z$. But then $G/Z = \langle gZ \rangle = \langle Z \rangle = \{(eZ)^k \mid k \in \mathbb{Z}\} = \{Z\}$. This means that G/Z is the trivial group, remember that Z is the identity element of the quotient group G/Z. Since $G/Z = \{hZ \mid h \in G\} = \{Z\}$, it means that for any $h \in G$ we get that the coset $hZ = Z$, and so $h \in Z$. Thus, $G = Z = Z(G)$, and so the center is the whole group, this is equivalent to G is abelian. ■

Lemma 8.2.6.

Suppose that N is a normal subgroup of G, and that K is a subgroup of the quotient group G/N. Then the union of all cosets of N in K forms a subgroup of G.

Theorem 8.2.7.

For any group G, we have that $G/Z(G) \cong \text{Inn}(G)$.

Proof. Let $Z = Z(G)$. Consider the map $\Phi : G/Z \to \text{Inn}(G)$ where for any coset $gZ \in G/Z$ we have $gZ \mapsto \phi_g$. Recall that ϕ_g is the inner automorphism of G induced by g, that is, $\phi_g(x) = gxg^{-1}$ for each $x \in G$. We need to show that the map Φ depends only on the coset itself and not on the element representing the coset, that is, we need to show that Φ is well-defined. So suppose that $gZ = hZ$. It follows that there is a central element $z \in Z$ such that $g = hz$. Then for any $x \in G$ we have $\phi_g(x) = gxg^{-1} = (hz)x(hz)^{-1} = hzxz^{-1}h^{-1} = hxzz^{-1}h^{-1} = hxh^{-1} = \phi_h(x)$. Thus, $\phi_g = \phi_h$ and so $\Phi(gZ) = \Phi(hZ)$. We now show that Φ preserves the group operation. Let gZ and hZ be in G/Z, then

$$\Phi(gZ * hZ) = \Phi((gh)Z) = \phi_{gh} = \phi_g \circ \phi_h = \Phi(gZ) \circ \Phi(hZ).$$

It remains to check that Φ is injective and surjective. This is left to the reader. ■

Corollary 8.2.8.

$\text{Inn}(D_6) \cong D_3$.

The next theorem is in the direction of the converse of Lagrange's theorem.

Theorem 8.2.9. (Cauchy)

Let G be a finite abelian group, and suppose that p is a prime that divides $|G|$. Then G has an element of order p.

Proof. We will prove the theorem by strong induction on the order of the group. For the base case, assume that we have an abelian group of order 2, then the only prime which divides 2 is 2 and moreover such a group is cyclic and so its generator has order 2 as desired.

Next, fix some integer $n > 2$ and assume that theorem holds for all abelian groups of order less than n. Let G be any abelian group of order n and assume that $p \mid n$. We need to find some element in G of order p. By Lemma 2.2.7, we know that there exist some $b \in G$ and a prime q such that $|b| = q$. If $p = q$, then we are done, as b is the desired element.

Otherwise, assume that $p \neq q$. Let $H = \langle b \rangle = \{e, b, b^2, \ldots, b^{q-1}\}$. Clearly $|H| = q$, and since q is prime, all nonidentity elements of H have order q. And as G is abelian, we get that H is a normal subgroup of G. Consequently, we can form the quotient group $G/H = \{aH \mid a \in G\}$ which has order n/q. One can check that G/H is an abelian group of order less than n and p divides $|G/H|$. By induction hypothesis, there is an element of G/H which has order p. So for some $g \in G$, the coset gH has order p in G/H. As a result $g \notin H$, as otherwise, we get $gH = H$ and the order of H is 1 in G/H since H is the identity element of the quotient group G/H. Also, it follows that $H = (gH)^p = g^pH$. Thus, $g^p \in H$. Now, if $g^p = e$, then $|g| = p$ and so g is an element of order p in G as desired.

Otherwise, the element g^p is a nonidentity element of the subgroup H. Thus, we get that $|g^p| = q$. From this we obtain that $(g^q)^p = e$. From which we deduce that $|g^q|$ divides p implying that $|g^q| = 1$ or $|g^q| = p$. For the sake of contradiction, assume that $|g^q| = 1$. Then it must be that $g^q = e$ and so $|g|$ divides q which implies either $|g| = 1$ or $|g| = q$. Obviously, $|g| \neq 1$ since $g \neq e$ because $g \notin H$. Also, $|g| \neq q$, to see this, assume for the contrary that $|g| = q$. So $g^q = e$, and thus $(gH)^q = g^qH = eH = H$ implying that the order of gH divides q, and so $p \mid q$, which is a contradiction since p and q are distinct primes. Therefore, it must be that $|g^q| = p$. Thus, the element g^q is an element of order p in the group G and this finishes the proof. ■

8.3 Simple Groups

Suppose the G has a nontrivial proper normal subgroup N. Then we can "break" the group G into two smaller subgroups, namely, the normal subgroup N and the quotient group G/N.

Definition 8.3.1. (Simple Group)

A nontrivial group is *simple* if its only normal subgroups are the trivial subgroup and the group itself. That is, if $N \trianglelefteq G$, then $N = \{e\}$ or $N = G$.

Lemma 8.3.2.

If N is a maximal proper normal subgroup of G, then G/N is simple.

Lemma 8.3.3.

If G is a nontrivial finite abelian simple group, then G is cyclic of prime order.

Proof. Suppose G is a nontrivial finite abelian simple group. Let g be a nonidentity element of G. So $|g| \geq 2$. For the sake of contradiction, suppose that $|g| \neq |G|$. Then as $|g| = |\langle g \rangle|$, the subgroup $\langle g \rangle$ is a nontrivial proper subgroup of G, moreover, as G is abelian, $\langle g \rangle$ is normal in G. This contradicts that G is simple. Thus, it must be that $|g| = |G|$. Therefore, $G = \langle g \rangle$, and so G is cyclic.
Now suppose $|G|$ is not prime, and let d be a divisor of $|G|$ such that $1 < d < |G|$. As G is cyclic, we know that G has exactly one subgroup of order d, but again this is a nontrivial proper normal subgroup of G, contradicting that G is simple. So $|G|$ must be prime. Thus, G is cyclic of prime order. ■

Finite simple groups serve as the basic building blocks for finite groups; similar to the way prime numbers build the integers. The process of breaking a finite group into simple subgroups is described by the Jordan–Hölder theorem. The classification of finite simple groups, completed in 2004, is one of the major milestones in the history of mathematics.

Theorem 8.3.4.

[Classification of Finite Simple Groups.] Any finite simple group belongs to one of the following classes:

- *Cyclic groups $\mathbb{Z}_p$ of prime order. (If n is not prime, then $\mathbb{Z}_n$ is not simple.)*
- *The alternating group A_n for every $n \geq 5$.*
- *Groups of Lie type.*
- *26 sporadic simple groups.*
  The largest sporadic group is called the Monster group; proved to exist by Robert Griess. Twenty of these 26 sporadic groups are subgroups or subquotients of the Monster group called the "Happy Family" and the remaining six groups are referred to as the "pariahs".

The proof of the classification of finite simple groups is spread throughout mathematics literature in hundreds of journal articles written by about 100 authors published mostly between 1955 and 2004. The collective work consists of approximately 10,000 pages in length.

Theorem 8.3.5. (Feit-Thompson Theorem; 1963)

Any finite nonabelian simple group must have even order.

Chapter 9

Direct Products

9.1 External Direct Product

Definition 9.1.1. (External Direct Product)

Let $(G, \cdot)$ and $(H, *)$ be groups. The (external) *direct product* of G and H is the group $G \oplus H$ whose underlying set is the set $\{(g, h) \mid g \in G, h \in H\}$ and its binary operation is done componentwise, that is, for any pairs (g_1, h_1) and (g_2, h_2) in $G \oplus H$ we have

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

Remark. For finite groups, the order of their direct product $G \oplus H$ is $|G|\,|H|$.

We generalize the definition above as follows. Given groups $G_1, G_2, \ldots, G_n$, their direct product is the group $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ whose underlying set is the set $\{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$ and the multiplication is performed componentwise: for any two n-tuples $(g_1, g_2, \ldots, g_n)$ and $(g_1', g_2', \ldots, g_n')$ we have

$$(g_1, g_2, \ldots, g_n)\,(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n').$$

Exercise 9.1. The reader needs to check that the direct product of groups is a group. The identity of the group $G \oplus H$ is the pair (e_G, e_H). Also for any element $(g, h) \in G \oplus H$, we have $(g, h)^{-1} = (g^{-1}, h^{-1})$ and $(g, h)^n = (g^n, h^n)$ for any integer n.

Example 9.2. Examples of direct products of groups.

- $U_8 \oplus U_{10} = \{(1,1),\ (1,3),\ (1,7),\ (1,9),\ (3,1),\ (3,3),\ (3,7),\ (3,9),$
  $(5,1),\ (5,3),\ (5,7),\ (5,9),\ (7,1),\ (7,3),\ (7,7),\ (7,9)\}$.

  For instance, in the group $U_8 \oplus U_{10}$ we have these computations: $(3,7)\,(7,3) = (5,1)$ and $(5,9)\,(3,3) = (7,7)$.

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2)\}$.

  Observe that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic and the element $(1,1)$ is a generator, so $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$.

- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0),\ (0,1),\ (1,0),\ (1,1)\}$.

  Observe that $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic.

Question. The examples above trigger the question: When the direct product of cyclic groups is cyclic?

Lemma 9.1.2.

Suppose that G is a group of order 4. Then $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Proof. Suppose that G is a group of order 4. If G is cyclic, then $G \cong \mathbb{Z}_4$. Otherwise, assume G is not cyclic. So no element of G is of order 4. By Lagrange's theorem it follows that every no-identity element is of order 2. Suppose that $G = \{e, a, b, c\}$ where the e is the identity element and a, b, c are distinct non-identity elements each is of order 2, meaning that each of these is its own inverse. We aim to find the product ab. First, $ab \neq e$, because if so, then $a^{-1} = b$ but we know that $a^{-1} = a$. Second, $ab \neq a$, because if so, then $b = e$ by cancellation. Similarly, $ab \neq b$. Thus, it must be that $ab = c$. Also, $ba = b^{-1}a^{-1} = (ab)^{-1} = c^{-1} = c$. Similar computations show that $ac = ca = b$ and $bc = cb = a$. This determines the Cayley table of G as follows.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Compare this table with the Cayley table of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Clearly, $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ via the isomorphism $e \mapsto (0,0)$, $a \mapsto (1,0)$, $b \mapsto (0,1)$, $c \mapsto (1,1)$. ■

Theorem 9.1.3.

Let G and H be finite groups and let $(g,h) \in G \oplus H$. Then

$$|(g,h)| = lcm(|g|, |h|).$$

Proof. Let G and H be finite groups and let $g \in G$ and $h \in H$. Put $|g| = m$, $|h| = n$, $|(g,h)| = t$, and $l = \text{lcm}(m,n)$. We need to show that $t = l$. Because l is divisible by m and n, there are integers α and β such that $l = \alpha m$ and $l = \beta n$. First, we find that

$$(g,h)^l = (g^l, h^l) = (g^{\alpha m}, h^{\beta n}) = ((g^m)^\alpha, (h^n)^\beta) = (e_G, e_h).$$

This gives t divides l, and so $t \leq l$. On the other hand,

$$(e_G, e_H) = (g,h)^t = (g^t, h^t).$$

This implies that $e_G = g^t$ and $e_H = h^t$ and thus $m \mid t$ and $n \mid t$ showing that t is a common multiple of m and n. Thus, $l \leq t$. Therefore, $t = l$ as desired. ■

The same proof above gives the more general theorem below.

Theorem 9.1.4.

The order of an element in a direct product of a finite number of finite groups, $G_1, G_2, \ldots, G_n$, is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$$

for any element $(g_1, g_2, \ldots, g_n) \in G_1 \oplus G_2 \oplus \cdots \oplus G_n$.

Exercise 9.3. Use the theorem above to show that following groups are nonisomorphic groups of order 100.

- $\mathbb{Z}_{100}$
- $\mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4$.
- $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- D_{50}.
- $D_{10} \oplus \mathbb{Z}_5$.
- $D_5 \oplus \mathbb{Z}_{10}$.
- $D_5 \oplus D_5$

Example 9.4. In the group $\mathbb{Z}_5 \oplus \mathbb{Z}_{25}$, how many elements of order 5 are there?

Consider an element $(g, h) \in \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$. Then $|(g, h)| = 5$ if and only if $\text{lcm}(|g|, |h|) = 5$. We know that the possible order of elements in $\mathbb{Z}_5$ are 1 or 5, and in $\mathbb{Z}_{25}$ are $1, 5, 25$. To obtain $\text{lcm}(|g|, |h|) = 5$ we have three cases. Recall that the number of elements of order d in a finite cyclic group is $\phi(d)$ if d is a divisor of the group order.
Case 1: $|g| = 5$ and $|h| = 1$. Here there are 4 choices for g, namely, $1, 2, 3, 4$ and one choice for h, namely, the identity 0. So there are 4 elements in this case, namely, $(1, 0)$, $(2, 0)$, $(3, 0)$, $(4, 0)$.
Case 2: $|g| = 1$ and $|h| = 5$. Here there is one choice for g, namely, 0 and $\phi(5) = 4$ choices for h, namely, the identity $5, 10, 15, 20$. So there are 4 elements in this case, namely, $(0, 5)$, $(0, 10)$, $(0, 15)$, $(0, 20)$.
Case 3: $|g| = 5$ and $|h| = 5$. Here there are 4 choices for g, namely, $1, 2, 3, 4$. And there are 4 choices for h, namely, $5, 10, 15, 20$. So there are 16 elements in this case.

Therefore, in total, we have 24 elements in $\mathbb{Z}_5 \oplus \mathbb{Z}_{25}$ of order 5.

Example 9.5. In the group $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$, how many elements of order 10 are there? How many cyclic subgroups of order 10 are there?

Consider an element $(g, h) \in \mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$. Then $|(g, h)| = 10$ if and only if $\text{lcm}(|g|, |h|) = 10$. We know that the possible order of elements in $\mathbb{Z}_{100}$ are $1, 2, 4, 5, 10, 20, 25, 50, 100$, and in $\mathbb{Z}_{25}$ are $1, 5, 25$. To obtain $\text{lcm}(|g|, |h|) = 10$ we have three cases.
Case 1: $|g| = 10$ and $|h| = 1$. Here there are $\phi(10) = 4$ choices for g, namely, $10, 30, 70, 90$ and one choice for h, namely, the identity 0. So there are 4 elements in this case, namely, $(10, 0)$, $(30, 0)$, $(70, 0)$, $(90, 0)$.
Case 2: $|g| = 10$ and $|h| = 5$. Here there are $\phi(10) = 4$ choices for g, and $\phi(5) = 4$ choices for h, namely, $5, 10, 15, 20$. So there are 16 elements in this case.
Case 3: $|g| = 2$ and $|h| = 5$. Here there is one choice for g, namely, 50 and $\phi(5) = 4$ choices for h. So there are 4 elements in this case.

Thus, in total, we have 24 elements in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ of order 10. Moreover, we know that any cyclic subgroup of order 10 has exactly 4 elements of order 10 and two distinct cyclic subgroups of order 10 have no elements of order 10 in common (see the proof of Corollary 4.4.5). It follows that there are $24/4 = 6$ cyclic subgroups of $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ of order 10.

Lemma 9.1.5.

Let G and H be groups.
(i) $G \oplus H \cong H \oplus G$.
(ii) $G \oplus H$ contains subgroups isomorphic to G and H, respectively.
(iii) If $A \leq G$ and $B \leq H$, then $A \oplus B \leq G \oplus H$.
(iv) If $K \cong G$ and $L \cong H$, then $K \oplus L \cong G \oplus H$.

Example 9.6. Find a subgroup of $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$ that is isomorphic to $\mathbb{Z}_6 \oplus \mathbb{Z}_4$.
Observe that $H = \langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}$ is a cyclic subgroup of $\mathbb{Z}_{30}$ of order 6, and $K = \langle 3 \rangle = \{0, 3, 6, 9\}$ is a cyclic subgroup of $\mathbb{Z}_{12}$ of order 4. Therefore, by the above lemma, we obtain that $H \oplus K$ is a subgroup of $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$ isomorphic to $\mathbb{Z}_6 \oplus \mathbb{Z}_4$.

Theorem 9.1.6.

Let G and H be finite groups. Then $G \oplus H$ is cyclic if and only if G and H are cyclic and $|G|$ and $|H|$ are coprime.

Proof. Let $|G| = m$ and $|H| = n$, it follows that $|G \oplus H| = mn$.

($\Rightarrow$) Suppose that $G \oplus H$ is cyclic. Let (g, h) be a generator of $G \oplus H$ and so $|(g, h)| = mn$. Choose any $x \in G$ and $y \in H$. Then $(x, y) \in G \oplus H$, and so there is $k \in \mathbb{Z}$ such that $(x, y) = (g, h)^k = (g^k, h^k)$. Thus, $x = g^k$ and $y = h^k$. This shows that $G = \langle g \rangle$ and $H = \langle h \rangle$, and so both G and H are cyclic with generators g and h, respectively. It follows that $|g| = m$ and $|h| = n$. Now let d be a positive common divisor of m and n. So $m = d\alpha$ and $n = d\beta$ for some positive integers α and β. Observe that

$$(g, h)^{d\alpha\beta} = (g^{d\alpha\beta}, h^{d\alpha\beta}) = ((g^{d\alpha})^\beta, (h^{d\beta})^\alpha) = ((g^m)^\beta, (h^n)^\alpha) = (e_G, e_H).$$

It follows that $|(g, h)|$ divides $d\alpha\beta$. So there is a positive integer k such that $k|(g, h)| = d\alpha\beta$, and so $kmn = d\alpha\beta$, and so $kd^2\alpha\beta = d\alpha\beta$, and so $kd = 1$. This implies that $d = 1$, and thus, $\gcd(m, n) = 1$.

($\Leftarrow$) Conversely, suppose that $G = \langle a \rangle$ and $H = \langle b \rangle$, and assume that $\gcd(m, n) = 1$. Clearly, $(a, b) \in G \oplus H$. We now compute the order of the element (a, b).

$$|(a, b)| = \operatorname{lcm}(|a|, |b|) = \operatorname{lcm}(m, n) = \operatorname{lcm}(m, n) \cdot 1 = \operatorname{lcm}(m, n) \gcd(m, n) = mn = |G \oplus H|.$$

Therefore, the element (a, b) generates $G \oplus H$, and so $G \oplus H$ is cyclic. ■

Corollary 9.1.7.

Suppose that $k = mn$ for integers k, m, n. Then $\mathbb{Z}_k \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ if and only if m and n are coprime.

Example 9.7. Using the corollary above we get the following facts.

- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$.
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$.
- $\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10} \ncong \mathbb{Z}_{60}$.

The next theorem describes when we can express the group of units modulo n as a direct product of groups of units.

Theorem 9.1.8.

Suppose that $n = st$ and that s and t are coprime. Then

$$U(n) \cong U(s) \oplus U(t).$$

Proof. Suppose that $n = st$ and that s and t are coprime. The reader needs to show that the map $\phi : U_n \to U_s \oplus U_t$ given by $\phi(k) = (k \bmod s,\ k \bmod t)$ for any $k \in U_n$ is a group isomorphism. ■

9.2 Internal Direct Product

We will discuss here when we can express a group as a direct product of its own subgroups.

Definition 9.2.1. (Internal Direct Product)

We say that a group G is the *internal direct product* of its subgroups H and K, and write $G = H \times K$, if the following conditions are satisfied:

(i) H and K are both normal subgroups of G;
(ii) $G = HK = \{hk \mid h \in H,\ k \in K\}$;
(iii) $H \cap K = \{e\}$.

Definition 9.2.2.

Suppose that s is a divisor of n. We define the subgroup $U_s(n)$ of $U(n)$ as follows:

$$U_s(n) = \{k \in U(n) \mid k \bmod s = 1\}.$$

Example 9.8. Consider the group $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$, and its normal subgroups $H = U_3(15) = \{1, 4, 7, 13\}$ and $K = U_5(15) = \{1, 11\}$. Clearly, $H \cap K = \{1\}$. Moreover,

$$HK = \{1,\ 11,\ 4,\ (4 \cdot 11),\ 7,\ (7 \cdot 11),\ 13,\ (13 \cdot 11)\} = \{1, 11, 4, 14, 7, 2, 13, 8\} = U(15).$$

Therefore, $U(15) = H \times K$. Observe that $U(15) \cong H \oplus K$ via the map $1 \mapsto (1, 1)$, $2 \mapsto (7, 11)$, $4 \mapsto (4, 1)$, $7 \mapsto (7, 1)$, $8 \mapsto (13, 11)$, $11 \mapsto (1, 11)$, $13 \mapsto (13, 1)$, $14 \mapsto (4, 11)$.

Lemma 9.2.3.

Let $n = st$ where s and t are coprime positive integers. Then,

$$U(n) = U_s(n) \times U_t(n).$$

Example 9.9. In D_6, the dihedral group of order 12, let F denote some reflection. Then,

$$D_6 = \{R_0, R_{180}\} \times \{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\}.$$

Example 9.10. In S_3, let $H = \langle(123)\rangle = \{(1), (123), (132)\}$ and $K = \{(1), (12)\}$. Then $S_3 = HK$ and $H \cap K = \{(1)\}$, however, $S_3 \neq H \times K$ because K is not a normal subgroup. Observe that $S_3 \ncong H \oplus K$ because $H \oplus K$ is cyclic because both H and K are cyclic with coprime orders, however, S_3 is not cyclic.

Theorem 9.2.4.

Let H and K be subgroups of G. If G is the internal direct product of H and K, then G is isomorphic to the external direct product of H and K. In symbols, if $G = H \times K$, then $G \cong H \oplus K$.

Proof. Suppose that $G = H \times K$. This means that $H \trianglelefteq G$, $K \trianglelefteq G$, $G = HK$, and $H \cap K = \{e\}$. We will show two claims.

Claim 1. Any element $g \in G$ can be written uniquely as the product of an element from H and an element from K.
Towards this end, choose any $g \in G$. Since $G = HK$, there are $h \in H$ and $k \in K$ such that $g = hk$. For uniqueness, assume also that $g = h'k'$ for some elements $h' \in H$ and $k' \in K$. Then $hk = h'k'$, and so $(h')^{-1}h = k'k^{-1}$. Since $(h')^{-1}h \in H$ and $k'k^{-1} \in K$, it follows that $(h')^{-1}h \in H \cap K$. Therefore, it must be that $(h')^{-1}h = e$ and so $h = h'$, and also, $k'k^{-1} = (h')^{-1}h = e$ and so $k = k'$.

Claim 2. Elements of H commute with elements of K.
Let $h \in H$ and $k \in K$, and consider the element $hkh^{-1}k^{-1}$. Since $H \trianglelefteq G$ and $K \trianglelefteq G$ we know that H and K are closed under conjugation and consequently we see that $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$, and similarly, $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$. Thus, $hkh^{-1}k^{-1} \in H \cap K$, and so $hkh^{-1}k^{-1} = e$, and therefore, $hk = kh$ as desired.

We are ready to define an isomorphism ϕ from G to $H \oplus K$. Let $g \in G$. By above we know that $g = hk$ for some unique elements $h \in H$ and $k \in K$. Declare the image of g under ϕ as follows:

$$\phi(g) = \phi(hk) = (h, k) \in H \oplus K.$$

Surjectivity of ϕ is straightforward, as for any $(h, k) \in H \oplus K$, we take $g = hk \in G$. Then $\phi(g) = (h, k)$ by definition of ϕ. We next show that ϕ is injective and preserves the operation. Choose any elements $g, b \in G$. Then there are unique $h, h' \in G$ and $k, k' \in H$ such that $g = hk$ and $b = h'k'$. By definition of the map, we get that $\phi(g) = (h, k)$ and $\phi(b) = (h', k')$. Now assume that $\phi(g) = \phi(b)$. It follows that $(h, k) = (h', k')$, and so $h = h'$ and $k = k'$. Thus, $g = hk = h'k' = b$ as wanted. It remains to show that ϕ is operation-preserving. As elements of H commute with elements from K we get that $hkh'k' = h(kh')k' = h(h'k)k' = (hh')(kk')$, and therefore,

$$\phi(gb) = \phi(hkh'k') = \phi\left((hh')(kk')\right) = (hh',\, kk') = (h, k)\,(h', k') = \phi(g)\phi(b).$$

This proves that G is isomorphic to the external direct product $H \oplus K$. ∎

What we have established above can be generalised to any finite number of subgroups of a group as described below.

Definition 9.2.5. (Internal Direct Product)

We say that a group G is the *internal direct product* of subgroups $H_1, H_2, \ldots, H_n$, and write $G = H_1 \times H_2 \times \cdots \times H_n$, if the following conditions are satisfied:

(i) Every $H_i \trianglelefteq G$;
(ii) $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n \mid h_i \in H_i\}$;
(iii) $(H_1H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for each $i = 1, 2, \ldots, n-1$.

Theorem 9.2.6.

Suppose that $H_1, H_2, \ldots, H_n$ are subgroups of a group G. Then, if $G = H_1 \times H_2 \times \cdots \times H_n$, then $G \cong H_1 \oplus H_2 \oplus \cdots \oplus H_n$.

Theorem 9.2.7.

Let G be a group of order p^2 for some prime p. Then either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Corollary 9.2.8.

Every group of order p^2, where p is a prime, is abelian.

Chapter 10

Group Homomorphisms

Camille Jordan introduced the concept of group homomorphisms in 1870 in his book "*Traité des substitutions et des équations algébriques*".

10.1 Homomorphisms

Definition 10.1.1. (Group Homomorphism)

Let $(G, \cdot)$ and $(H, *)$ be groups. A *homomorphism* $\varphi : G \to H$ is a function that preserves the group operation; that is, for any $a, b \in G$ we have that

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b).$$

Remark. Every group isomorphism is a group homomorphism.

For every homomorphism $\varphi : G \to H$ we associate a special subset of G called the kernel of φ.

Definition 10.1.2. (Kernel of Homomorphism)

Let $\varphi : G \to H$ be a group homomorphism. The *kernel* of φ is the set

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}.$$

Example 10.1. The following are group homomorphisms.

- Let $\varphi : G \to H$ be a group isomorphism, then $\ker \varphi = \{e_G\}$.
- The determinant map, $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$. Here, $\ker(\det) = SL_n(\mathbb{R})$.
- The map $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ defined by $\varphi(x) = |x|$. Here, $\ker \varphi = \{1, -1\}$.
- The map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ where $\varphi(k) = k \bmod n$ is a homomorphism. Here, $\ker \varphi = n\mathbb{Z}$.
- The map $\varphi : (\mathbb{R}, +) \to \{z \in \mathbb{C} : |z| = 1\}$ defined by $\varphi(x) = e^{ix} = \cos x + i \sin x$. Here, $\ker \varphi = \{2\pi k \mid k \in \mathbb{Z}\}$.
- The map $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ defined by $\varphi(x) = x^2$. Here, $\ker \varphi = \{1, -1\}$.

- The map $\varphi : S_n \to \mathbb{Z}_2$ given by $\varphi(\alpha) = 0$ if α is even, and $\varphi(\alpha) = 1$ if α is odd. Here, $\ker \varphi = A_n$.
- Let $\mathbb{R}[x]$ be the group of all polynomials with real coefficients under the addition operation. The derivative map $D : \mathbb{R}[x] \to \mathbb{R}[x]$ where $D(f) = f'$ for any $f \in \mathbb{R}[x]$ is a homomorphism. Moreover, its kernel is the set of all constant polynomials.
- Let V and W be vector spaces. Any linear transformation $T : V \to W$ is a group homomorphism from $(V, +)$ to $(W, +)$.

10.2 Properties of Homomorphisms

Theorem 10.2.1.

Suppose that $\varphi : G \to H$ is a group homomorphism. Then:
(i) $\varphi(e_G) = e_H$.
(ii) For any $g \in G$ and any $n \in \mathbb{Z}$ we have that $\varphi(g^n) = (\varphi(g))^n$.
(iii) If $g \in G$ is of finite order, then $|\varphi(g)|$ divides $|g|$.

Proof. Statements (i) and (ii) were proved in Theorem 6.2.1. For (iii) Suppose that $g \in G$ with $|g| = n$. It follows that $\varphi(g) \in H$ and, moreover, we have $(\varphi(g))^n = \varphi(g^n) = \varphi(e_G) = e_H$. Thus, $|\varphi(g)|$ divides n. ■

Theorem 10.2.2.

Let $\varphi : G \to H$ be a group homomorphism. Then $\ker \varphi$ is a normal subgroup of G. In symbols, $\ker \varphi \trianglelefteq G$.

Proof. We will first show that $\ker \varphi$ is a subgroup by the one-step subgroup test. Because $\varphi(e_G) = e_H$ we get that $e_G \in \ker \varphi$ and so $\ker \varphi \neq \emptyset$. Next, let $a, b \in \ker \varphi$, this means that $\varphi(a) = e_H$ and $\varphi(b) = e_H$. Observe that $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H e_H = e_H$. Thus, $ab^{-1} \in \ker \varphi$. This shows that $\ker \varphi$ is a subgroup of G.

Next we show that the kernel of φ is normal. So choose any $g \in G$ and $k \in \ker \varphi$. We have to show that $gkg^{-1} \in \ker \varphi$. Towards, we proceed as follows:

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)e_H\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H.$$

Therefore, $gkg^{-1} \in \ker \varphi$ as desired. ■

Theorem 10.2.3.

Suppose that $\varphi : G \to H$ is a group homomorphism. Then:
(i) $\varphi(a) = \varphi(b)$ if and only if $a \ker \varphi = b \ker \varphi$, for any $a, b \in G$.
(ii) Let $g \in G$. If $\varphi(g) = h$, then $\varphi^{-1}(h) = \{x \in G \mid \varphi(x) = h\} = g \ker \varphi$.
(iii) φ is injective if and only if $\ker \varphi = \{e_G\}$.

Proof. (i) For the forward direction assume that $\varphi(a) = \varphi(b)$. This implies $(\varphi(b))^{-1}\varphi(a) = e_H$, and so $\varphi(b^{-1})\varphi(a) = e_H$, and thus, $\varphi(b^{-1}a) = e_H$. This shows that $b^{-1}a \in \ker \varphi$.

Therefore, $(b^{-1}a)\ker\varphi = \ker\varphi$, and so $a\ker\varphi = b\ker\varphi$.
For the converse assume that $a\ker\varphi = b\ker\varphi$. Then $(b^{-1}a)\ker\varphi = \ker\varphi$, and so we get $b^{-1}a \in \ker\varphi$. This implies that $\varphi(b^{-1}a) = e_H$, and so we get $\varphi(b^{-1})\varphi(a) = e_H$, and then $(\varphi(b))^{-1}\varphi(a) = e_H$, thus, $\varphi(a) = \varphi(b)$.

(ii) Suppose that $g \in G$ and $\varphi(g) = h$. Now using (i) observe that for any $x \in G$ we have that $x \in \varphi^{-1}(h)$ if and only if $\varphi(x) = h$ if and only if $\varphi(x) = \varphi(g)$ if and only if $x\ker\varphi = g\ker\varphi$ if and only if $x \in g\ker\varphi$. This shows that $\varphi^{-1}(h) = g\ker\varphi$.

(iii) Suppose that φ is injective. Let $x \in \ker\varphi$. Then $\varphi(x) = e_H$ and so $\varphi(x) = \varphi(e_G)$, and so by injectivity, we get $x = e_G$. Thus, $\ker\varphi = \{e_G\}$.
Conversely, suppose that $\ker\varphi = \{e_G\}$ and that $\varphi(a) = \varphi(b)$ for some elements $a, b \in G$. Then, $\varphi(ab^{-1}) = e_H$, and so $ab^{-1} \in \ker\varphi$. As e_G is the only element in the kernel, it must be that $ab^{-1} = e_G$. Therefore, $a = b$ showing that φ is injective. ■

Theorem 10.2.4.

Suppose that $\varphi : G \to H$ is a group homomorphism, and let S be a subgroup of G. Then the following hold.

(i) $\varphi(S) = \{\varphi(x) \mid x \in S\}$ is a subgroup of H. In particular, $\varphi(G) \leq H$.

(ii) If S is abelian, then $\varphi(S)$ is abelian.

(iii) If S is cyclic, then $\varphi(S)$ is cyclic.

(iv) If $S \trianglelefteq G$, then $\varphi(S) \trianglelefteq \varphi(G)$.

(v) If $|\ker\varphi| = n$, then φ is an n-to-1 map (i.e. $|\varphi^{-1}(h)| = n$ for any $h \in \varphi(G)$).

(vi) If G is finite, then $|\varphi(G)|$ divides $|G|$.

Theorem 10.2.5.

Suppose that $\varphi : G \to H$ is a group homomorphism, and let L be a subgroup of H. Then the following hold.

(i) The subset $\varphi^{-1}(L) = \{g \in G \mid \varphi(g) \in L\}$ is a subgroup of G.

(ii) If $L \trianglelefteq H$, then $\varphi^{-1}(L) \trianglelefteq G$.

Example 10.2. Define $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ by $\varphi(k) = 3k$. Then φ is a homomorphism.

- $\ker\varphi = \{0, 4, 8\}$.
- Thus, φ is a 3-to-1 mapping.
- Since $\varphi(2) = 6$, we have that $\varphi^{-1}(6) = 2 + \ker\varphi = 2 + \{0, 4, 8\} = \{2, 6, 10\}$.
- $\langle 2\rangle = \{0, 2, 4, 6, 8, 10\}$ is cyclic. So $\varphi(\langle 2\rangle) = \{0, 6\} = \langle 6\rangle$ is cyclic as well.
- $|2| = 6$ and $|\varphi(2)| = |6| = 2$. So $|\varphi(2)|$ divides $|2|$.

Example 10.3. Define $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ by $\varphi(z) = z^4$. Then φ is a homomorphism.

- Let $w, z \in \mathbb{C}^*$. Then $\varphi(wz) = (wz)^4 = w^4z^4 = \varphi(w)\varphi(z)$.
- $\ker\varphi = \{z \in \mathbb{C}^* \mid z^4 = 1\} = \{1, -1, i, -i\}$.
- Thus, φ is a 4-to-1 mapping.
- Since $\varphi(\sqrt[4]{2}) = 2$, we have that $\varphi^{-1}(2) = \sqrt[4]{2}\ker\varphi = \{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}\,i, -\sqrt[4]{2}\,i\}$.

Example 10.4. Find all homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$.
A homomorphism $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$ is determined by knowing $\varphi(1)$. Say, $\varphi(1) = m$ for some $m \in \mathbb{Z}_{30}$. Then $|m|$ must divide $|1| = 12$ and must divide $|\mathbb{Z}_{30}| = 30$. Therefore, $|m| \in \{1, 2, 3, 6\}$. Therefore, $m \in \{0, 15, 10, 20, 5, 25\}$. Check that each of these choices for m gives rise to a homomorphism from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$.

10.3 Isomorphism Theorems for Groups

Theorem 10.3.1.

Suppose that N is a normal subgroup of G. The map $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a homomorphism, called the natural projection. Moreover, $\ker \pi = N$.

Proof. Consider the map $\pi : G \to G/N$ defined by $\pi(g) = gN$. We will show that π is a group homomorphism. So Let $g, h \in G$. Then,

$$\pi(gh) = (gh)N = (gN)(hN) = \pi(g)\pi(h).$$

Also, $\ker \pi = \{g \in G \mid \pi(g) = N\} = \{g \in G \mid gN = N\} = \{g \in G \mid g \in N\} = N$. ■

Corollary 10.3.2.

Normal subgroups are kernels and kernels are normal subgroups.

Theorem 10.3.3. (First Isomorphism Theorem)

Let $\varphi : G \to H$ be a group homomorphism. Then,

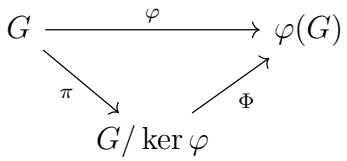
$$G/\ker \varphi \cong \varphi(G).$$

Proof. Let $\varphi : G \to H$ be a group homomorphism. Then we will show that the map $\Phi : G/\ker \varphi \to \varphi(G)$ given by $\Phi(g \ker \varphi) = \varphi(g)$ is an isomorphism. We already know that $a \ker \varphi = b \ker \varphi$ if and only if $\varphi(a) = \varphi(b)$, for any $a, b \in G$. The forward direction of this equivalence shows that the map Φ is well-defined (that is, the map is independent of the coset representative chosen), and its converse shows that Φ is injective. Next, we show that Φ is surjective. Let $y \in \varphi(G)$. Then, there exists $x \in G$ such that $\varphi(x) = y$. Observe that $\Phi(x \ker \varphi) = \varphi(x) = y$ showing that the coset $x \ker \varphi$ is a preimage of y as needed. It remains to show that Φ preserves the group operation. Let $a \ker \varphi$ and $b \ker \varphi$ be cosets in $G/\ker \varphi$. Then,

$$\Phi((a \ker \varphi)(b \ker \varphi)) = \Phi(ab \ker \varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(a \ker \varphi)\Phi(b \ker \varphi).$$

This proves that the quotient group $G/\ker \varphi$ is isomorphic to the subgroup $\varphi(G)$ of the group H. ■

Below is a diagram representing the First Isomorphism Theorem. The diagram commutes, that is, $\Phi \circ \pi = \varphi$.



Corollary 10.3.4.

If $\varphi : G \to H$ is a surjective group homomorphism, then

$$G/\ker\varphi \cong H.$$

Corollary 10.3.5.

Suppose that $\varphi : G \to H$ is a group homomorphism and that G has finite order. Then, $|\varphi(G)|$ divides $|G|$.

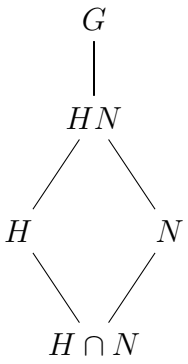
Example 10.5. As the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism we obtain

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*.$$

Theorem 10.3.6. (Second Isomorphism Theorem)

Let G be a group. If $H \leq G$ and $N \trianglelefteq G$, then

$$HN/N \cong H/(H \cap N).$$



Theorem 10.3.7. (Third Isomorphism Theorem)

Suppose that N and K are normal subgroups of group G with $N \subseteq K \subseteq G$. Then $K/N \trianglelefteq G/N$ and

$$(G/N)/(K/N) \cong G/K.$$

Chapter 11

Fundamental Theorem of Finite Abelian Groups

The fundamental theorem of finite abelian groups (FTFAG) was first proved by Leopold Kronecker in 1858. Recall that a cyclic group of order n is isomorphic to the group $(\mathbb{Z}_n, +)$. Also, $G = H \times K$ says that group G is the internal direct product of subgroups H and K.

11.1 Statement of the Fundamental Theorem

Theorem 11.1.1. (Fundamental Theorem of Finite Abelian Groups)

Every finite abelian group is isomorphic to a direct product of cyclic groups of prime-power order.

In other words, if G is a finite abelian nontrivial group, then there exist primes $p_1, p_2, \ldots, p_k$ (not necessarily distinct) and positive integers $n_1, n_2, \ldots, n_k$ such that

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

Corollary 11.1.2.

The only finite abelian groups which are simple are the cyclic groups of prime order.

A *partition* of a positive integer n is a sequence of positive integers $n_1 \geq n_2 \geq \cdots \geq n_k$ such that

$$n = n_1 + n_2 + \cdots + n_k.$$

We start our discussion with abelian groups of prime-power order. Let p be a prime number and n be a positive integer. The fundamental theorem of finite abelian groups states that for each partition $(n_1, n_2, \ldots, n_k)$ of n we have, up to isomorphism, one abelian group of order p^n, namely the group

$$\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}.$$

Notice that $p^n = p^{n_1}p^{n_2}\cdots p^{n_k}$ since $n = n_1 + n_2 + \cdots + n_k$.

Furthermore, FTFAG states that distinct partitions of the exponent n yield nonisomorphic abelian groups of order p^n.

For a prime p we find all *isomorphism classes* of abelian groups of order p, p^2, p^3, and p^4.

- Abelian groups of order p.

Partitions of 1	Isomorphism Class
1	$\mathbb{Z}_p$

- Abelian groups of order p^2.

Partitions of 2	Isomorphism Class
2	$\mathbb{Z}_{p^2}$
1+1	$\mathbb{Z}_p \oplus \mathbb{Z}_p$

- Abelian groups of order p^3.

Partitions of 3	Isomorphism Class
3	$\mathbb{Z}_{p^3}$
2+1	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$
1+1+1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

- Abelian groups of order p^4.

Partitions of 4	Isomorphism Class
4	$\mathbb{Z}_{p^4}$
3+1	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$
2+2	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
2+1+1	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
1+1+1+1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

Lemma 11.1.3.

Suppose that G, H, K are groups where G is finite. Then,

$$\text{if } G \oplus H \cong G \oplus K, \text{ then } H \cong K.$$

In general, for an abelian group whose order m has two or more distinct prime divisors, we start by finding the prime-power decomposition of n. Say $m = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ for distinct primes p_i. Next, we find all abelian groups of order $p_i^{n_i}$ for each $i = 1, 2, \ldots, k$ as we did earlier. Finally, we put all these groups together in direct products.

Example 11.1. Find all isomorphism classes of abelian groups of order 1176. We start by finding the prime factorization: $1176 = 2^3 \cdot 3 \cdot 7^2$. Then any abelian group of order 1176 is isomorphic to one of the following groups:

- $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \cong \mathbb{Z}_{1176}$
- $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{168} \oplus \mathbb{Z}_7$

- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \cong \mathbb{Z}_{588} \oplus \mathbb{Z}_2$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{84} \oplus \mathbb{Z}_{14}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \cong \mathbb{Z}_{294} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{42} \oplus \mathbb{Z}_{14} \oplus \mathbb{Z}_2$

Example 11.2. Consider the group

$$G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$$

under multiplication modulo 65. Since G is abelian and $|G| = 16 = 2^4$ we know that G is isomorphic to one of the following groups:

$$\mathbb{Z}_{16} \qquad \mathbb{Z}_8 \oplus \mathbb{Z}_2 \qquad \mathbb{Z}_4 \oplus \mathbb{Z}_4$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Next, we calculate the orders of the elements of G to know which one is isomorphic to G.

Element	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
Order	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

Clearly, $G \ncong \mathbb{Z}_{16}$ because G has no element of order 16. Similarly, $G \ncong \mathbb{Z}_8 \oplus \mathbb{Z}_2$ because G has no element of order 8. Since $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has no element of order 4, it cannot be isomorphic to G. Finally, as $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has more than three elements of order 2 it cannot be isomorphic to G. Therefore, it must be that $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

11.2 Greedy Algorithm

Since a finite abelian group G is isomorphic to an external direct product of cyclic groups of prime-power order, it follows that we can express the group G as an internal direct product of some of its cyclic subgroups of prime-power order. How can we find these subgroups?

Greedy Algorithm for an Abelian Group G of Order p^n

1. Compute the orders of all elements of the group G.
2. Select an element $g_1 \in G$ of maximum order.
3. Define $G_1 = \langle g_1 \rangle$ and set $i = 1$.
4. If $|G| = |G_i|$, then stop. Otherwise, replace i by $i + 1$.
5. Select an element $g_i \in G$ of maximum order p^k such that $p^k \leq |G|/|G_i|$ and $G_{i-1} \cap \{g_i, g_i^p, g_i^{p^2}, g_i^{p^3}, \ldots, g_i^{p^{k-1}}\} = \emptyset$.
6. Define $G_i = G_{i-1} \times \langle g_i \rangle$ and jump to step 4.

In general, for an abelian group G of order $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, we first apply the algorithm to build an internal direct product of order $p_1^{n_1}$, and then another of order $p_2^{n_2}$, and so on. The internal direct product of all these subgroups is the desired decomposition of G.

Example 11.3. Let's express the group G in the previous example as an internal direct product of some of its cyclic subgroups. We apply the algorithm above. Choose an element g of maximum order, say $g = 8$. Define $G_1 = \langle g \rangle = \langle 8 \rangle = \{1, 8, 64, 57\}$. The subgroup $\langle 8 \rangle$ is our first direct factor. Next, choose an element h such that $|h| \leq |G|/|G_1| = 16/4 = 4$ and where h and h^2 do not belong to G_1. Select $h = 12$ and compute $\langle h \rangle = \langle 12 \rangle = \{1, 12, 14, 38\}$. The subgroup $\langle 12 \rangle$ will be the second direct factor. Now, define $G_2 = G_1 \times \langle h \rangle$. We stop here as $|G| = |G_2|$. Therefore, $G = \langle 8 \rangle \times \langle 12 \rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Example 11.4. Suppose that G is an abelian group of order 24. Moreover, we know that G has distinct elements $a, b, c \in G$ such that $|a| = 12$, $|b| = 2$, and $|c| = 2$. Find the isomorphism class of G.
As $24 = 2^3 \cdot 3$, the group G is isomorphic to one of the following three groups:

- $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{24}$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

We can rule out the third group in the list as it does not have an element of order 12. The first group $\mathbb{Z}_{24}$ has exactly one element of order 2 since $\phi(2) = 1$, thus we can rule it out as well. It follows that $G \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2$.

11.3 The Proof of the Fundamental Theorem

The proof of the fundamental theorem of finite abelian groups (FTFAG) can be broken down into the following series of theorems.

Theorem 11.3.1.

Let G be a finite abelian group of order $p^n m$ where p is a prime that does not divide m. Then $G = H \times K$ where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.

Lemma 11.3.2.

Let G be an abelian group of order $p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ for distinct primes p_i. Define $G_{p_i} = \{x \in G \mid x^{p_i^{n_i}} = e\}$. Then $|G_{p_i}| = p_i^{n_i}$ and

$$G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k}.$$

Theorem 11.3.3.

Suppose that G is an abelian group of prime-power order and let $g \in G$ be an element of maximum order. Then $G = \langle g \rangle \times K$ for some subgroup K.

Theorem 11.3.4.

An abelian group of prime-power order is an internal direct product of cyclic groups.

So now we know that a finite abelian group is an internal direct product of subgroups of prime-power order (as in above: $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k}$), and each G_{p_i} which

is an abelian group of prime-power order can be written as an internal direct product of cyclic groups. Thus, every finite abelian group is an internal direct product of cyclic subgroups of prime-power order. All that remains to prove the fundamental theorem of finite abelian groups is to show that there is only one way (up to isomorphism) to write each factor G_{p_i} as an internal direct product of cyclic groups.

Theorem 11.3.5.

Suppose that G is a finite abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_k$ and $G = K_1 \times K_2 \times \cdots \times K_m$ where each H_i and K_i is a nontrivial cyclic subgroup with $|H_i| \geq |H_{i+1}|$ and $|K_i| \geq |K_{i+1}|$, then $k = m$ and $|H_i| = |K_i|$ for all i.

The following is a consequence of the fundamental theorem of finite abelian groups.

Corollary 11.3.6.

Suppose that G is a finite abelian group. If m divides $|G|$, then G has a subgroup of order m.

Lemma 11.3.7.

Two finite abelian groups are isomorphic if and only if they have the same number of elements of each order.

Chapter 12

Rings and Fields

A ring is an algebraic structure composed of a set equipped with two binary operations, usually called addition and multiplication. The notion of a ring originates from the work of Richard Dedekind in the 19th century. The term "ring" was first used by the German mathematician David Hilbert in 1897.

12.1 Definition of Rings and Fields

Definition 12.1.1. (Ring)

A *ring* is a set R equipped with two binary operations, called addition $(+)$ and multiplication $(\cdot)$, satisfying the following axioms, called the *ring axioms*.

(i) For any $a, b, c \in R$ we have that $(a + b) + c = a + (b + c)$. (Addition associativity)

(ii) There exists an element $0 \in R$ such that $a + 0 = a$ for any $a \in R$. (Additive identity)

(iii) For any $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$. (Additive inverses)

(iv) For any $a, b \in R$ we have that $a + b = b + a$. (Addition commutativity)

(v) For any $a, b, c \in R$ we have that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (Multiplication associativity)

(vi) For any $a, b, c \in R$ we have that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$. (Left distributivity)

(vii) For any $a, b, c \in R$ we have that $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$. (Right distributivity)

In short, a ring is a triple $(R, +, \cdot)$ such that R is an abelian group under addition, and where multiplication is an associative operation that is left and right distributive over addition. We call the additive identity the *zero* of the ring R and denote it by 0_R or 0.

Definition 12.1.2. (Commutative Rings; Unity; and Units)

- A ring whose multiplication is commutative is called a *commutative ring*.
- A ring R with a multiplicative identity element (denoted by 1_R or 1) is called a *ring with unity*. In other words, there is an element $1_R \in R$ such that for all $r \in R$ we have $r \cdot 1_R = r$ and $1_R \cdot r = r$.
- An element in a ring R with unity which has a multiplicative inverse is called a *unit* of the ring. That is, a unit of R is an element $u \in R$ such that there exists $v \in R$ such that $u \cdot v = 1$ and $v \cdot u = 1$.
- The set of all units of R forms a group, denoted by R^* or $R^\times$ or $U(R)$, under the ring multiplication called the *group of units* of R.

Definition 12.1.3. (Field)

A *field* is a commutative ring with unity in which every nonzero element is a unit.

In other words, a field is a set F equipped with two binary operations satisfying the following axioms, called the *field axioms*.

(i) For any $a, b, c \in F$ we have that $(a + b) + c = a + (b + c)$. (Addition associativity)

(ii) There exists an element $0 \in F$ such that $a + 0 = a$ for any $a \in F$. (Additive identity)

(iii) For any $a \in F$, there exists $-a \in F$ such that $a + (-a) = 0$. (Additive inverses)

(iv) For any $a, b \in F$ we have that $a + b = b + a$. (Addition commutativity)

(v) For any $a, b, c \in F$ we have that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (Multiplication associativity)

(vi) There exists an element $1 \in F$ such that $1 \cdot a = a$ for any $a \in F$. (Multiplication identity)

(vii) For any nonzero $a \in F$, there is $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$. (Multiplicative inverses)

(viii) For any $a, b \in F$ we have that $a \cdot b = b \cdot a$. (Multiplication commutativity)

(ix) For any $a, b, c \in F$ we have that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$. (Distributivity)

Remark. A field is a ring $(R, +, \cdot)$ where both $(R, +, 0_R)$ and $(R^*, \cdot, 1_R)$ are abelian groups and also multiplication is distributive over addition.

Lemma 12.1.4.

If a ring has a unity, it is unique. If an element r in a ring has a multiplicative inverse, then it is unique and is denoted be r^{-1}.

Example 12.1 (Examples of Rings)**.**

- The integers $(\mathbb{Z}, +, \cdot)$ with ordinary addition and multiplication is a commutative ring with unity. The units of $\mathbb{Z}$ are 1 and -1.
- The set $\mathbb{Z}_n$ of integers modulo n with addition and multiplication modulo n is a commutative ring with unity. The set of units of $\mathbb{Z}_n$ is U_n.

- The even integers $(2\mathbb{Z}, +, \cdot)$ with ordinary addition and multiplication is a commutative ring without unity.
- The rationals $\mathbb{Q}$, the reals $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields under ordinary addition and multiplication.
- The set $M_n(\mathbb{Z})$ of all $n \times n$ matrices with integer entries is a noncommutative ring with unity (the identity matrix I_n).
- The set $\mathbb{Z}[x]$ of all polynomials in the variable x with integer coefficients under polynomial addition and multiplication is a
- Similarly, the set $\mathbb{R}[x]$ of all polynomials in the variable x with real number coefficients under polynomial addition and multiplication is a commutative ring with unity.
- The set of all continuous real-valued functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(1) = 0$ is a commutative ring without unity under pointwise addition and multiplication. That is, for any such functions f and g we define $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$.

Definition 12.1.5. (Direct Sum of Rings)

Let R and S be rings. The *direct sum* of R and S is the ring

$$R \oplus S = \{(a, b) \mid a \in R, b \in S\}$$

under componentwise addition and multiplication, that is,

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2,\ b_1 + b_2)$$

and

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

12.2 Properties of Rings

Let $(R, +, \cdot)$ be a ring and let $a, b \in R$. Recall that $-a$ is the additive inverse of a in R. For the integer 0 we set $0a = 0_R$, and for any positive integer n we define

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}}.$$

Moreover, we define

$$(-n)a = n(-a) = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ times}}.$$

Finally, we write $a - b$ to denote $a + (-b)$.

Lemma 12.2.1.

Suppose that $(R, +, \cdot)$ is a ring. Let $a, b, c \in R$. Then
(i) $a \cdot 0_R = 0_R$ *and* $0_R \cdot a = 0_R$.
(ii) $a \cdot (-b) = -(a \cdot b)$ *and* $(-a) \cdot b = -(a \cdot b)$.
(iii) $(-a) \cdot (-b) = a \cdot b$.
(iv) $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$ *and* $(b - c) \cdot a = (b \cdot a) - (c \cdot a)$.

Proof. Suppose that $(R, +, \cdot)$ is a ring. Let $a, b, c \in R$.

(i) Since $0_R = 0_R + 0_R$ we have that

$$\begin{aligned} a \cdot 0_R &= a \cdot 0_R \\ a \cdot 0_R &= a \cdot (0_R + 0_R) \\ a \cdot 0_R &= (a \cdot 0_R) + (a \cdot 0_R) \end{aligned}$$

Next, we add the additive inverse of the element $a \cdot 0_R$ to both sides of the equation:

$$\begin{aligned} (a \cdot 0_R) + -(a \cdot 0_R) &= \big((a \cdot 0_R) + (a \cdot 0_R)\big) + -(a \cdot 0_R) \\ 0_R &= (a \cdot 0_R) + \big((a \cdot 0_R) + -(a \cdot 0_R)\big) \\ 0_R &= (a \cdot 0_R) + 0_R \\ 0_R &= a \cdot 0_R. \end{aligned}$$

(ii) Observe that $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0_R = 0_R$. Therefore, $a \cdot (-b)$ is the additive inverse of $a \cdot b$, in symbols, $a \cdot (-b) = -(a \cdot b)$.

(iii) Using (ii) we get $(-a) \cdot (-b) = -((-a) \cdot b) = -(-(a \cdot b)) = a \cdot b$.

(iv) $a \cdot (b - c) = a \cdot (b + -c) = (a \cdot b) + (a \cdot (-c)) = (a \cdot b) + -(a \cdot c) = (a \cdot b) - (a \cdot c)$. ■

Lemma 12.2.2.

Suppose that $(R, +, \cdot)$ is a ring with unity element 1_R. Let $a \in R$. Then
(i) $(-1_R) \cdot a = -a$.
(ii) $(-1_R) \cdot (-1_R) = 1_R$.

Proof. (i) Since $a + (-1_R) \cdot a = 1_R \cdot a + (-1_R) \cdot a = (1_R - 1_R) \cdot a = 0_R \cdot a = 0_R$, we know that $(-1_R) \cdot a$ is the additive inverse of a.

(ii) Using (i) we get $(-1_R) \cdot (-1_R) = -(-1_R) = 1_R$. ■

Lemma 12.2.3.

Let $(R, +, \cdot)$ be a ring and let $a, b \in R$. For any $m, n \in \mathbb{Z}$ we have that

$$(ma) \cdot (nb) = (mn)(a \cdot b).$$

12.3 Subrings

Definition 12.3.1. (Subring)

A subset S of a ring R is a *subring* of R if and only if S itself is a ring under the addition and multiplication of R.

Remember that the one-step subgroup test says that a nonempty subset of an additive group is a subgroup if this subset is closed under subtraction. Consequently, we obtain the following test for subrings.

Lemma 12.3.2. (Subring Test)

Let $(R, +, \cdot)$ be a ring. Suppose that S is a nonempty subset of R. If S is closed under subtraction and multiplication (that is, whenever $a, b \in S$, then both $a - b$ and $a \cdot b$ are in S), then S is a subring of R.

Proof. Since S is closed under subtraction, we get by the one-step subgroup test that S is a subgroup of $(R, +)$. Since S is closed under multiplication, then the multiplication of R is a closed binary operation on S. Since multiplication of R is associative and distributive over addition for elements of R, it is certainly the same for all elements of S. Therefore, the subset S is a ring under the addition and multiplication inherited from R. So S is a subring of R. ■

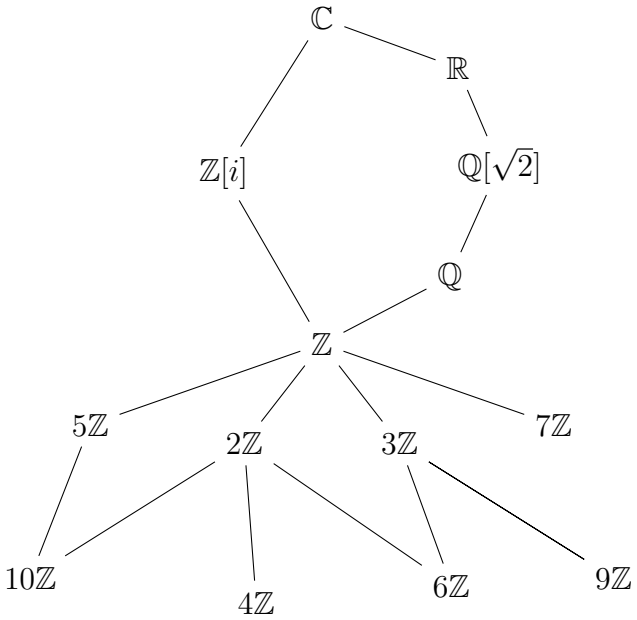
Example 12.2. Here are examples of subrings.

- The trivial subring $\{0_R\}$ and R are subrings of any ring R.
- For each positive integer n, the set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subring of the ring of integers $(\mathbb{Z}, +, \cdot)$.
- The *Gaussian integers* $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ is a subring of the ring of complex numbers $(\mathbb{C}, +, \cdot)$.
- Let R be the ring of all real-valued functions $f : \mathbb{R} \to \mathbb{R}$ under pointwise addition and multiplication. Then the set $S = \{f \in R \mid f(0) = 0\}$ is a subring of R.
- The set of all diagonal matrices,

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z} \right\},$$

  is a subring of the ring of all 2×2 matrices with integer entries.

Example 12.3. Subring lattice of some subrings of the complex numbers.


$\mathbb{C}$
$\mathbb{R}$
$\mathbb{Z}[i]$
$\mathbb{Q}[\sqrt{2}]$
$\mathbb{Q}$
$\mathbb{Z}$
$5\mathbb{Z}$
$2\mathbb{Z}$
$3\mathbb{Z}$
$7\mathbb{Z}$
$10\mathbb{Z}$
$4\mathbb{Z}$
$6\mathbb{Z}$
$9\mathbb{Z}$

Chapter 13

Integral Domains

Commutative rings with unity are not the desirable abstraction of the integers as, in general, they still miss an essential feature of the integers. Towards this end, we introduce integral domains which would capture the algebraic properties of the integers in an abstract setting.

13.1 Definition of Integral Domains

Definition 13.1.1. (Integral Domain)

An *integral domain* is a commutative ring with unity such that the product of any two nonzero elements is nonzero.

In other words, an integral domain D is a commutative ring with unity where for any elements a and b in D, if $a \neq 0_D$ and $b \neq 0_D$, then $a \cdot b \neq 0_D$, equivalently, if $a \cdot b = 0_D$, then $a = 0_D$ or $b = 0_D$. So in an integral domain, whenever the product of two elements in zero, then at least one of them must be zero.

Definition 13.1.2. (Zero Divisor)

Let R be a commutative ring. An element $a \in R$ is called a *zero-divisor* if $a \neq 0_R$ and there exists a nonzero element $b \in R$ such that $a \cdot b = 0_R$.

Remark. An integral domain is a commutative ring with unity which has no zero-divisors.

Example 13.1 (Examples of integral domains)**.**

- The ring of integers $(\mathbb{Z}, +, \cdot)$.
- The ring of Gaussian integers $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.
- The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients.
- The ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.
- The ring $(\mathbb{Z}_p, +, \cdot)$ of integers modulo a prime p.
  Suppose that $a, b \in \mathbb{Z}_p$ and $ab = 0$. By definition of multiplication modulo p we get

$ab \bmod p = 0$, and so $p \mid ab$. Since p is prime, by Euclid's Lemma, it follows that $p \mid a$ or $p \mid b$. Since $0 \leq a, b \leq p-1$, it must be that $a = 0$ or $b = 0$ since 0 is the only integer in $\mathbb{Z}_p$ which is divisible by p. Thus, $\mathbb{Z}_p$ is an integral domain.

Lemma 13.1.3.

Any field is an integral domain.

Proof. Let $(F, +, \cdot)$ be a field and suppose that $a \cdot b = 0$ for any arbitrary $a, b \in F$. If $a = 0$, we are done. Otherwise, assume that $a \neq 0$. Since F is a field, the element a must be a unit, and so its multiplicative inverse a^{-1} exists. It follows that $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$, and so $1 \cdot b = 0$, and thus $b = 0$ as desired. ■

Example 13.2 (Nonexamples of integral domains)**.**

- The ring $\mathbb{Z} \oplus \mathbb{Z}$.
- If n is not prime, then $(\mathbb{Z}_n, +, \cdot)$ is not an integral domain.
- The ring $M_n(\mathbb{Z})$ of $n \times n$ matrices with integer entries.

Lemma 13.1.4. (Cancellation in Integral Domains)

Let a, b, c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Proof. Suppose $a \neq 0$ and $ab = ac$. Then $ab - ac = 0$, and so $a(b - c) = 0$. Since we are in an integral domain we know that $a = 0$ or $b - c = 0$. But we assumed $a \neq 0$, so it must be $b - c = 0$, and so $b = c$ as desired. ■

Theorem 13.1.5.

Any finite integral domain is a field.

Proof. Let D be a finite integral domain. So D is a commutative ring with unity 1. It remains to show that nonzero elements are units. Choose some nonzero element $a \in D$. If $a = 1$, then a is its own multiplicative inverse and we are done. So we may assume that $a \neq 1$. Consider the sequence of powers of a:

$$a, a^2, a^3, a^4, \ldots$$

All terms of this sequence belong to D since D is closed under multiplication. Since D is finite, there must be some integers $i < j$ such that $a^i = a^j$. It follows that $a^j - a^i = 0$ and so $a^i(a^{j-i} - 1) = 0$. Since D is an integral domain we know that $a^i = 0$ or $a^{j-i} - 1 = 0$. Since $a \neq 0$ and D is an integral domain we get $a^i \neq 0$ as well. Thus, it must be $a^{j-i} - 1 = 0$ and so $a^{j-i} = 1$. Since $a \neq 1$ we get $j - i > 1$ and so $j - i - 1 \geq 1$ meaning that $a^{j-i-1} \in D$. But $1 = a^{j-i} = a\, a^{j-i-1}$, so $a^{j-i-1} \in D$ is the multiplicative inverse of a. So a is a unit. ■

Corollary 13.1.6.

The ring $(\mathbb{Z}_p, +, \cdot)$ of integers modulo p is a field, for any prime p.

Example 13.3. Here is another example of a finite field of 9 elements, it is the field of Gaussian integers modulo 3.

$$\mathbb{Z}_3[i] = \{a + ib \mid a, b \in \mathbb{Z}_3\} = \{0,\ 1,\ 2,\ i,\ 1+i,\ 2+i,\ 2i,\ 1+2i,\ 2+2i\}.$$

Elements of $\mathbb{Z}_3[i]$ are added and multiplied as in the complex numbers, and then the coefficients are reduced modulo 3. In particular, $i^2 = -1 \equiv 2 \pmod 3$. So $i \cdot i = 2$ in the field $\mathbb{Z}_3[i]$. Here are the Cayley tables of addition and multiplication in this field.

$+$	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
0	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
1	1	2	0	$1+i$	$2+i$	i	$1+2i$	$2+2i$	$2i$
2	2	0	1	$2+i$	$0+i$	$1+i$	$2+2i$	$0+2i$	$1+2i$
i	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$	0	1	2
$1+i$	$1+i$	$2+i$	i	$1+2i$	$2+2i$	$2i$	1	2	0
$2+i$	$2+i$	$3+i$	$1+i$	$2+2i$	$2i$	$1+2i$	2	0	1
$2i$	$2i$	$1+2i$	$2+2i$	0	1	2	i	$1+i$	$2+i$
$1+2i$	$1+2i$	$2+2i$	$2i$	1	2	0	$1+i$	$2+i$	i
$2+2i$	$2+2i$	$2i$	$1+2i$	2	0	1	$2+i$	i	$1+i$

$\cdot$	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
2	0	2	1	$2i$	$2+2i$	$1+2i$	i	$2+i$	$1+i$
i	0	i	$2i$	2	$2+i$	$2+2i$	1	$1+i$	$1+2i$
$1+i$	0	$1+i$	$2+2i$	$2+i$	$2i$	1	$1+2i$	2	i
$2+i$	0	$2+i$	$1+2i$	$2+2i$	1	i	$1+i$	$2i$	2
$2i$	0	$2i$	i	1	$1+2i$	$1+i$	2	$2+2i$	$2+i$
$1+2i$	0	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	i	1
$2+2i$	0	$2+2i$	$1+i$	$1+2i$	i	2	$2+i$	1	$2i$

In the table of multiplication, the row of any nonzero element has 1 showing that every nonzero element has a multiplicative inverse.

13.2 Characteristic of a Ring

Consider the subring $S = \{0, 3, 6, 9\}$ of the ring $(\mathbb{Z}_{12}, +, \cdot)$. Observe that for any $x \in S$ we have that $x+x+x+x = 0$. Similarly, for any $z \in \mathbb{Z}_3[i]$, we have that $z+z+z = 0$. Recall that for a positive integer n and a ring element x, we write nx to denote the element obtained by adding x with itself n times.

Definition 13.2.1. (Characteristic of a Ring)

The *characteristic* of a ring R is the least positive integer n such that for all $x \in R$ we have that $\underbrace{x + x + \cdots + x}_{n \text{ times}} = 0_R$.
If no such integer exists, we say R has characteristic 0. The characteristic of R is denoted by $\text{char}(R)$.

Example 13.4.

$$\text{char}(\mathbb{Z}) = 0, \quad \text{char}(\mathbb{Z}_n) = n, \quad \text{char}(\mathbb{Z}_2[x]) = 2, \quad \text{char}(\mathbb{Z}_3[i]) = 3,$$
$$\text{char}(\mathbb{Z}_2 \oplus \mathbb{Z}_3) = 6, \quad \text{char}(\mathbb{Q}) = 0, \quad \text{char}(\mathbb{R}) = 0, \quad \text{char}(\mathbb{C}) = 0.$$

Remark. Let R be a ring. If $\text{char}(R) = 0$, then R has infinitely many elements. However, the converse is not true, that is, there are infinite rings with positive characteristic.

Example 13.5. Let S be a set. We will make the powerset $\mathcal{P}(S)$ a ring by defining addition and multiplication as follows. Let $A, B \in \mathcal{P}(S)$, define

$$A + B = (A \cup B) \setminus (A \cap B) \qquad \text{and} \qquad A \cdot B = A \cap B.$$

This makes $(\mathcal{P}(S), +, \cdot)$ a commutative ring with unity. The zero element is the empty set $\emptyset$ and the unity is the whole set S. Moreover, $\text{char}(\mathcal{P}(S)) = 2$.

Lemma 13.2.2.

Let R be a ring with unity 1_R. If 1_R has infinite order under addition, then $\text{char}(R) = 0$. Otherwise, the characteristic of R is the order of 1_R under addition, that is, $\text{char}(R) = n$ where n is the least positive integer such that

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} = 0_R.$$

Proof. If the additive order of 1 is infinite, then there exists no positive integer n such that adding 1 with itself n times gives 0. Thus, $\text{char}(R) = 0$. On the other hand, assume that $|1_R| = n$. Now choosr an arbitrary $x \in R$ and observe that

$$\begin{aligned} n\,x = \underbrace{x + x + \cdots + x}_{n \text{ times}} &= x \cdot 1_R + x \cdot 1_R + \cdots + x \cdot 1_R \\ &= x \cdot (1_R + 1_R + \cdots + 1_R) = x \cdot (n\,1_R) = x \cdot 0_R = 0_R. \end{aligned}$$

Thus for every $x \in R$ we have $n\,x = 0_R$. Moreover, we know that n is the least positive integer such that $n\,1_R = 0_R$ since n is the additive order of 1_R. Therefore, $\text{char}(R) = n$ as desired. ∎

Theorem 13.2.3.

The characteristic of an integral domain is either 0 or prime.

Proof. Let D be an integral domain of positive characteristic. By the previous result we get $\text{char}(D) = |1_D|$. Let $|1_D| = n$. We need to show that n must be prime. Assume that $m \in \mathbb{Z}^+$ and $m \mid n$. Then there is an integer $k \in \mathbb{Z}$ such that $n = mk$. We now get the following using Lemma 12.2.3.

$$0_D = n\,1_D = (mk)\,(1_D \cdot 1_D) = (m\,1_D) \cdot (k\,1_D).$$

Since D is an integral domain we get $m\,1_D = 0_D$ or $k\,1_D = 0_D$. If $m\,1_D = 0_D$, then since m is positive and $m \leq n$, we must have that $m = n$ as n is the least positive integer such that $n\,1_D = 0_D$. On the other hand, if $k\,1_D = 0_D$, then similarly we get that $k = n$ and so $m = 1$. Therefore, m is either 1 or n. This shows that the only positive divisors of n are 1 and itself, that is, n is prime as we wanted to show. ■

Corollary 13.2.4.

The characteristic of a field is either 0 *or prime.*

Lemma 13.2.5.

Suppose that R is a finite ring. Then

$$1 \leq \text{char}(R) \leq |R|.$$

Moreover, $\text{char}(R)$ *divides* $|R|$.

Chapter 14

Quotient Rings

14.1 Ideals

Ideals in rings are the analogue of normal subgroups in groups.

Definition 14.1.1. (Ideal)

A subring I of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in I$ we have that $ra \in I$ and $ar \in I$.

Thus, an ideal is a subring that absorbs all elements of the ring. In other words, $rI = \{ra \mid a \in I\} \subseteq I$ and $Ir = \{ar \mid a \in I\} \subseteq I$ for any r in the ring R. An ideal I of a ring R is called *proper* if I is a proper subset of R.

Lemma 14.1.2. (Ideal Test)

Let I be a nonempty subset of a ring R. Suppose that
(i) for any $a, b \in I$, we have that $a - b \in I$, and
(ii) for any $r \in R$ and $a \in I$, we have that $ra \in I$ and $ar \in I$.
Then I is an ideal of R.

Example 14.1.

- For any ring R, we have that $\{0_R\}$ and R are ideals of R.
- For any positive integer n, the set $n\mathbb{Z}$ is an ideal of the ring of integers $(\mathbb{Z}, +, \cdot)$.
- Let R be the ring of all real-valued functions $f : \mathbb{R} \to \mathbb{R}$ under pointwise addition and multiplication. The subset $S \subseteq R$ of all differentiable functions is a subring of R but not an ideal of R.

Definition 14.1.3. (Principal Ideal)

Let R be a commutative ring with unity.

- The *principal ideal* generated by an element $a \in R$ is the set

$$\langle a \rangle = \{ra \mid r \in R\}.$$

- The *principal ideal* generated by elements $a_1, a_2, \ldots, a_n \in R$ is the set

$$\langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

Example 14.2.

- Let $\mathbb{R}[x]$ be the ring of all polynomials in one variable with real coefficients. Then

$$\langle x \rangle = \{f \cdot x \mid f \in \mathbb{R}[x]\} = \{0, x, x^2 + x, 5x, x^3 - 7x, x^4 + x^2 + 6x, \ldots\}.$$

  So the ideal $\langle x \rangle$ generated by the polynomial $f(x) = x$ is the set of all polynomials with constant term 0.

- Let $\mathbb{Z}[x]$ be the ring of all polynomials in one variable with integer coefficients. Then

$$\langle x, 2 \rangle = \{f \cdot x + g \cdot 2 \mid f, g \in \mathbb{Z}[x]\} = \{0, x, x^2 + x, 5x + 4, x^3 - 7x + 6, x^4 + x^3 + 6x - 8, \ldots\}.$$

  So the ideal $\langle x, 2 \rangle$ generated by the polynomials x and 2 is the set of all polynomials with even constant terms.

14.2 Quotient Rings

Let $(R, +, \cdot)$ be a ring, and let A be a subring of R. Observe that A is a subgroup of the abelian group $(R, +)$, and the set of all cosets of A in $(R, +)$ is

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

Moreover, since A is a normal subgroup of $(R, +)$ we get that R/A with coset addition forms an abelian group whose additive identity is $0_R + A$ and where coset addition is defined as follows:

$$(r + A) + (s + A) = (r + s) + A.$$

We have shown previously that coset addition in this case is a well-defined operation since A is a normal subgroup of $(R, +)$. We aim to enrich R/A with coset multiplication towards making it a ring. Let r and s be any elements in the ring R. Similarly, we use the multiplication in R to define coset multiplication in the set R/A:

$$(r + A) \cdot (s + A) = (r \cdot s) + A.$$

The questions now are: is this definition of coset multiplication well-defined? If yes, is the set of cosets R/A with coset addition and coset multiplication a ring?

Theorem 14.2.1.

If I is an ideal of a ring R, then the set R/I of cosets is a ring under coset addition and coset multiplication called the quotient ring (or factor ring) of R by the ideal I.

Proof. We know that R/I is an abelian group under coset addition. We need now to show that coset multiplication is well-defined. Towards this end, suppose that $r + I = r' + I$ and $s + I = s' + I$. We need to show that $(r + I) \cdot (s + I) = (r' + I) \cdot (s' + I)$, that is, coset multiplication does not depend on the coset representatives. From our assumption, it follows that there are $a, b \in I$ such that $r = r' + a$ and $s = s' + b$. Since I is an ideal and $a, b \in I$, we obtain that the elements $r'b, as', ab \in I$ and so their sum $r'b + as' + ab$ is also in I, meaning that $(r'b + as' + ab) + I = I$. We now proceed as follows:

$$\begin{aligned}(r + I) \cdot (s + I) &= rs + I = (r' + a)(s' + b) + I \\ &= (r's' + r'b + as' + ab) + I = r's' + ((r'b + as' + ab) + I) \\ &= r's' + I = (r' + I) \cdot (s' + I).\end{aligned}$$

This shows that multiplication of cosets in R/I is a well-defined operation. It is easy to check that coset multiplication is associative and distributes over coset addition. Thus, the set R/I of cosets of I forms a ring under coset addition and coset multiplication. ■

The converse of the previous result also holds.

Theorem 14.2.2.

Suppose that A is a subring of a ring R. If the set R/A of cosets of I is a ring under coset addition and multiplication, then A is an ideal of R.

Proof. We will show the contrapositive. Suppose that $A \subseteq$ R is a subring which is not an ideal of R. Thus, there are elements $a \in A$ and $r \in R$ such that $ar \notin A$ or $ra \notin A$. Without loss of generality, say $ar \notin A$. It follows that $ra + A \neq A$ and $a + A = 0 + A$. Now $(a + A) \cdot (r + A) = ar + A \neq A$, however, $(0 + A) \cdot (r + A) = (0 \cdot r) + A = 0 + A = A$, showing that coset multiplication is not well-defined. ■

Example 14.3.

- $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z},\ 1 + 4\mathbb{Z},\ 2 + 4\mathbb{Z},\ 3 + 4\mathbb{Z}\}$.
- $2\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z},\ 2 + 6\mathbb{Z},\ 4 + 6\mathbb{Z}\}$.
- Let $R = M_2(\mathbb{Z})$, the ring of 2×2 matrices with integers entries. And let $I \subseteq R$ consisting of matrices of even integers. Show that I is an ideal of R. Moreover, show that $|R/I| = 16$, in fact, the quotient ring is

$$R/I = \left\{ \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} + I \mid b_i \in \{0, 1\} \right\}$$

- Let $\langle 2-i\rangle$ be the ideal generated by the complex number $2-i$ in the ring of Gaussian integers $\mathbb{Z}[i]$. Observe that $(2-i) \in \langle 2-i\rangle$ and so

$$\begin{aligned}(2-i)+\langle 2-i\rangle &= 0+\langle 2-i\rangle \\ 2+\langle 2-i\rangle &= i+\langle 2-i\rangle \qquad (*)\\ (2+\langle 2-i\rangle)^2 &= (i+\langle 2-i\rangle)^2 \\ 4+\langle 2-i\rangle &= -1+\langle 2-i\rangle \\ 5+\langle 2-i\rangle &= 0+\langle 2-i\rangle \qquad (**)\end{aligned}$$

  For instance, let us show that $(3+4i)+\langle 2-i\rangle = 1+\langle 2-i\rangle$.

$$\begin{aligned}(3+4i)+\langle 2-i\rangle &= 3+(4i+\langle 2-i\rangle) = 3+(4+\langle 2-i\rangle)\cdot(i+\langle 2-i\rangle)\\ &\overset{(*)}{=} 3+(4+\langle 2-i\rangle)(2+\langle 2-i\rangle) = 3+(8+\langle 2-i\rangle)\\ &= 11+\langle 2-i\rangle = 1+5+5+\langle 2-i\rangle\\ &\overset{(**)}{=} 1+5+\langle 2-i\rangle \overset{(**)}{=} 1+\langle 2-i\rangle.\end{aligned}$$

  In a similar fashion, using $(*)$ and $(**)$ one can show that

$$\mathbb{Z}[i]/\langle 2-i\rangle = \{0+\langle 2-i\rangle,\ 1+\langle 2-i\rangle,\ 2+\langle 2-i\rangle,\ 3+\langle 2-i\rangle,\ 4+\langle 2-i\rangle\}.$$

- Let $\langle x^2+1\rangle$ be the principal ideal generated by the polynomial x^2+1 in the ring $\mathbb{R}[x]$. In other words,

$$\langle x^2+1\rangle = \{f(x)(x^2+1) \mid f(x) \in \mathbb{R}[x]\rangle\}.$$

  By definition of the quotient ring, a member of $\mathbb{R}[x]/\langle x^2+1\rangle$ is a coset

$$g(x)+\langle x^2+1\rangle$$

  for some polynomial $g(x) \in \mathbb{R}[x]$. We now use the Division Algorithm of polynomials over $\mathbb{R}$ to divide $g(x)$ by x^2+1 we obtain polynomials q and r in $\mathbb{R}[x]$ such that

$$g(x) = q(x)(x^2+1)+r(x)$$

  where $r(x)$ is either the zero polynomial or $\deg(r) < 2$. Therefore, $r(x) = ax+b$ where $a, b \in \mathbb{R}$. It follows

$$\begin{aligned}g(x)+\langle x^2+1\rangle &= q(x)(x^2+1)+r(x)+\langle x^2+1\rangle\\ &= r(x)+q(x)(x^2+1)+\langle x^2+1\rangle\\ &= r(x)+\langle x^2+1\rangle.\end{aligned}$$

  The last equality holds because the ideal $\langle x^2+1\rangle$ absorbs its elements. Therefore,

$$\begin{aligned}\mathbb{R}[x]/\langle x^2+1\rangle &= \{g(x)+\langle x^2+1\rangle \mid g(x) \in \mathbb{R}[x]\}\\ &= \{(ax+b)+\langle x^2+1\rangle \mid a, b \in \mathbb{R}\}.\end{aligned}$$

Now let us see how multiplication works in this ring $\mathbb{R}[x]/\langle x^2+1\rangle$. Observe that

$$\begin{aligned}(x^2+1)+\langle x^2+1\rangle &= 0+\langle x^2+1\rangle\\ x^2+\langle x^2+1\rangle &= -1+\langle x^2+1\rangle\end{aligned}$$

Therefore x^2 and -1 represent the same of coset of the ideal $\langle x^2+1\rangle$. Let us use this fact to compute the following product.

$$\begin{aligned}(x+3+\langle x^2+1\rangle)\cdot(2x+5+\langle x^2+1\rangle) &= (x+3)(2x+5)+\langle x^2+1\rangle\\ &= 11x+15+2x^2+\langle x^2+1\rangle\\ &= 11x+15+2(-1)+\langle x^2+1\rangle\\ &= (11x+13)+\langle x^2+1\rangle.\end{aligned}$$

One may have the feeling that $\mathbb{R}[x]/\langle x^2+1\rangle$ is isomorphic to the field of complex numbers $\mathbb{C}$.

14.3 Prime Ideals and Maximal Ideals

Definition 14.3.1. (Prime and Maximal Ideals)

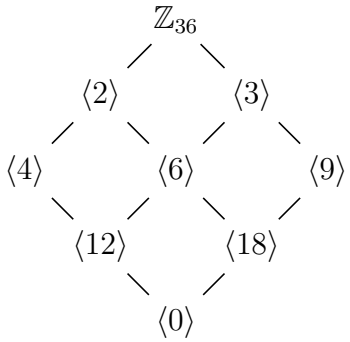
Let I be a proper ideal of a commutative ring R.

- The ideal I is *prime* if for any elements $a, b \in R$, if $a \cdot b \in I$, then $a \in I$ or $b \in I$.
- The ideal I is *maximal* if for any ideal J, if $I \subseteq J \subseteq R$, then $J = I$ or $J = R$.

Example 14.4. Examples of prime and maximal ideals.

- Let $n > 1$. Then $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ if and only if n is prime.
  ($\Rightarrow$) Assume $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Pick any positive divisor m of n. So there is a positive integer k such that $n = km$. It follows that $1 \leq m \leq n$ and $1 \leq k \leq n$. Since $n \in n\mathbb{Z}$ we get that $km \in n\mathbb{Z}$, and as $n\mathbb{Z}$ is a prime ideal we must have $k \in n\mathbb{Z}$ or $m \in n\mathbb{Z}$. Therefore $n \mid k$ or $n \mid m$, and as $k, m \leq n$, we must have $k = n$ or $m = n$, which leads to $m = 1$ or $m = n$. Thus any positive divisor of n is either 1 or n, so n is prime.
  ($\Leftarrow$) Assume p is a prime integer. Choose any $a, b \in \mathbb{Z}$ and assume that $ab \in p\mathbb{Z}$. Therefore $p \mid ab$. As p is prime, by Euclid's lemma we have $p \mid a$ or $p \mid b$, which leads to $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$, showing that $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

- The principal ideals $\langle 2 \rangle$ and $\langle 3 \rangle$ are the only maximal ideals of the ring $\mathbb{Z}_{36}$.



- The principal ideal $\langle x^2 + 1 \rangle$ is not prime in the ring $\mathbb{Z}_2[x]$, because it contains the product $(x+1)(x+1)$ but it does not contain $x+1$. Observe that $(x+1)(x+1) = x^2 + x + x + 1 = x^2 + 0x + 1 = x^2 + 1$.

- The principal ideal $\langle x \rangle$ is a prime ideal of the ring $\mathbb{Z}[x]$ which is not maximal. To see $\langle x \rangle$ is not maximal, observe that $\langle x \rangle \subsetneq \langle x, 2 \rangle \subsetneq \mathbb{Z}[x]$. To see it is prime, first observe that

$$\langle x \rangle = \{f \in \mathbb{Z}[x] \mid f(0) = 0\}.$$

  Let $g, h \in \mathbb{Z}[x]$ and assume that $gh \in \langle x \rangle$. Then $(gh)(0) = 0$, but $(gh)(0) = g(0)h(0)$, and so $g(0)h(0) = 0$. Since $g(0)$ and $h(0)$ are integers and $\mathbb{Z}$ is an integral domain, we get that $g(0) = 0$ or $h(0) = 0$, and so $g \in \langle x \rangle$ or $h \in \langle x \rangle$.

Lemma 14.3.2.

The principal ideal $\langle x^2 + 1 \rangle$ is maximal in the ring $\mathbb{R}[x]$.

Proof. Suppose that A is an ideal of $\mathbb{R}[x]$ that properly contains $\langle x^2+1\rangle$. That is $\langle x^2+1\rangle \subsetneq A \subseteq \mathbb{R}[x]$. We will show that $A = \mathbb{R}[x]$. Choose some polynomial $f \in A \setminus \langle x^2+1\rangle$. Use the Division Algorithm of polynomials over $\mathbb{R}$ to divide $f(x)$ by x^2+1. As a result, there are polynomials q and r in $\mathbb{R}[x]$ such that

$$f(x) = q(x)(x^2+1) + r(x)$$

where $r(x)$ is either the zero polynomial or $\deg(r) < 2$. However, $r(x) \neq 0$ because $f(x) \notin \langle x^2+1\rangle$. Therefore, $r(x) = ax + b$ where $a \neq 0$ or $b \neq 0$. Moreover, since $\langle x^2+1\rangle \subseteq A$, it follows that $(x^2+1) \in A$, and as A is ideal we get $q(a)(x^2+1) \in A$. Therefore, the polynomial $r(x) = f(x) - q(x)(x^2+1)$ must be in A since A is closed under subtraction. So $ax + b$ is in A. Also any multiple of $ax + b$ is in A since A is an ideal, namely, the polynomial $(ax+b)(ax-b)$ belongs to A. Again, as A is an ideal we get $a^2(x^2+1) \in A$. Finally, as A is closed under subtraction, we conclude that

$$a^2(x^2+1) - (ax+b)(ax-b) = a^2x^2 + a^2 - a^2x^2 + b^2 = a^2 + b^2$$

belongs to A. Let $c = a^2+b^2$, and as $a \neq 0$ or $b \neq 0$, we know that $c \neq 0$. So the constant nonzero polynomial $h(x) = c$ belongs to A. Now let $g(x) = 1/c$ and as A is an ideal we get $h(x)g(x) = c(1/c) = 1$ belongs to A, but this implies that $A = \mathbb{R}[x]$ as desired. Therefore, the ideal $\langle x^2+1\rangle$ is maximal in $\mathbb{R}[x]$. ■

Theorem 14.3.3.

Let I be an ideal of a commutative ring R with unity. Then R/I is an integral domain if and only if I is prime.

Proof. Let I be an ideal of a commutative ring R with unity.

($\Rightarrow$) Suppose that the quotient ring R/I is an integral domain. To show that I is a prime ideal suppose that $ab \in I$ for any arbitrary $a, b \in I$. It follows that $ab + I = I = 0 + I$ (recall that $0 + I$ is the zero of R/I). By definition of coset multiplication, we get that $(a+I)\cdot(b+I) = ab + I = 0 + I$. Since R/I is an integral domain, either $a + I = I$ or $b + I = I$, and therefore, $a \in I$ or $b \in I$ establishing that I is a prime ideal.

($\Leftarrow$) Suppose that I is a prime ideal. Clearly, R/I is a commutative ring with unity since R is. It remains to show that R/I has no zero divisors. So we now assume that $(a+I)\cdot(b+I) = 0+I$ for any arbitrary cosets $a+I$ and $b+I$ in the quotient ring R/I. It follows that $ab+I = (a+I)\cdot(b+I) = 0+I$, and so $ab+I = I$, and thus, $ab \in I$. Since I is a prime ideal, we get that $a \in I$ or $b \in I$, which implies that $a+I = I$ or $b+I = I$ as desired. This shows that R/I is an integral domain. ■

Theorem 14.3.4.

Let I be an ideal of a commutative ring R with unity. Then R/I is a field if and only if I is maximal.

Proof. Let I be an ideal of a commutative ring R with unity.

($\Rightarrow$) Suppose that R/I is a field. Towards showing that I is a maximal ideal, let J be an ideal such that $I \subseteq J \subseteq R$ and $I \neq J$. We will show that $J = R$. Towards this, let

pick an element $b \in J \setminus I$. Since $b \notin I$, we know that $b + I \neq I$, and so $b + I$ is a nonzero element of the field R/I. Therefore, $b + I$ has a multiplicative inverse, say $c + I$ for some $c \in R$. This means that $bc + I = (b + I) \cdot (c + I) = 1 + I$. Since the unity 1 belongs to the coset $1 + I$, there exists $a \in I$ such that $1 = bc + a$. Since $b \in J$ and J is an ideal, we know that $bc \in J$. Since $a \in I$ and $I \subseteq J$, we know that $a \in J$. Since a and bc are in J and J is closed under addition, we get that $bc + a$ is in J, implying that $1 \in J$. But any ideal which contains the unity must be the whole ring. So $J = R$.

($\Leftarrow$) Assume that I is a maximal ideal. Clearly, R/I is a commutative ring with unity since R is. It remains to show that every nonzero element of R/I is a unit. So suppose that $b + I \neq 0 + I$ for some element $b \in R$. It follows that $b \notin I$. Now consider the subset

$$J = I + \langle b \rangle = \{a + rb \mid a \in I \text{ and } r \in R\}.$$

Clearly, the set J properly contains the ideal I, that is, $I \subseteq J$, and $I \neq J$ because $b \in J \setminus I$ as $b = 0 + 1b$. Moreover, one can show by the Ideal Test that J is an ideal of R. It follows that $J = R$ because I is a maximal ideal. So the unity 1 belongs to J, and therefore, there exist some elements $a \in I$ and $r \in R$ such that $1 = a + rb$. We now observe that

$$1 + I = (a + rb) + I = (rb + a) + I = rb + (a + I) = rb + I = (r + I) \cdot (b + I).$$

Therefore, $(r + I) \cdot (b + I) = 1 + I$ which means that $r + I$ is the multiplicative inverse of $b + I$, showing that $b + I$ is a unit. As $b + I$ was an arbitrary nonzero coset, this shows that R/I is a field. ■

We have seen previously that prime ideals need not be maximal. What about the converse?

Corollary 14.3.5.

Let R be a commutative ring with unity. If I is a maximal ideal of R, then I is prime.

Proof. An ideal I being maximal implies that R/I is a field, which implies that R/I is an integral domain, which implies that I is a prime ideal. ■

Chapter 15

Ring Homomorphisms

15.1 Ring Homomorphisms

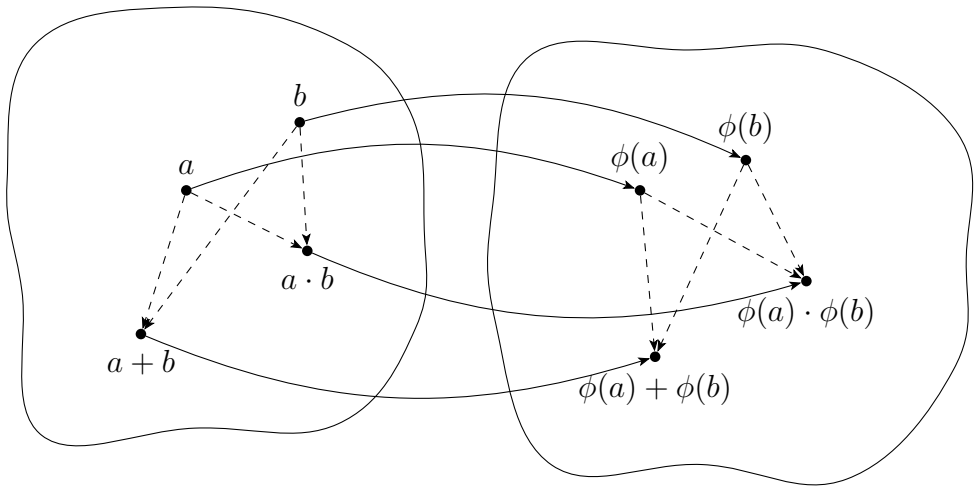
A ring homomorphism is a map between rings which preserves both of the ring operations.

Definition 15.1.1. (Ring Homomorphism and Isomorphism)

A *ring homomorphism* from a ring R to a ring S is a function $\varphi : R \to S$ such that for all elements $a, b \in R$ we have that

$$\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \text{and} \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

A *ring isomorphism* is a bijective ring homomorphism. We write $R \cong S$ when there exists at least one isomorphism from ring R to ring S, and say R is *isomorphic* to S.



Definition 15.1.2. (Kernel)

Let $\varphi : R \to S$ be a ring homomorphism. The *kernel* of φ is the following subset of R:

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0_S\}.$$

We now give some examples of homomorphisms between rings.

Example 15.1.

- The map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(k) = k \bmod n$ is a ring homomorphism, called the *natural homomorphism* from $\mathbb{Z}$ to $\mathbb{Z}_n$.
- The map $\varphi : \mathbb{C} \to \mathbb{C}$ given by $\varphi(a + bi) = a - bi$ is a ring isomorphism.
- The map $\varphi : \mathbb{R}[x] \to \mathbb{R}$ given by $\varphi(f) = f(1)$ is a ring homomorphism.
- Let R be a commutative ring of characteristic 2. The map $\varphi : R \to R$ given by $\varphi(a) = a^2$ is a ring homomorphism.
  To see this, choose arbitrary $a, b \in R$. Then:

  (1) $\varphi(a + b) = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2 = a^2 + 0 + b^2 = a^2 + b^2 = \varphi(a) + \varphi(b)$.

  (2) $\varphi(ab) = (ab)^2 = abab = aabb = a^2b^2 = \varphi(a)\varphi(b)$.
- The ring of even integers $(2\mathbb{Z}, +, \cdot)$ is not isomorphic to the ring of integers $(\mathbb{Z}, +, \cdot)$, although they are isomorphic as groups. To see that they are not isomorphic as rings, one needs to notice that $\mathbb{Z}$ has a multiplicative identity by $2\mathbb{Z}$ does not.

Example 15.2. We aim to determine all ring homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$. From group theory, the only group homomorphisms from $(\mathbb{Z}_{12}, +)$ to $(\mathbb{Z}_{30}, +)$ are of the form $\varphi(x) = xk$ where $k \in \{0, 15, 10, 20, 5, 25\}$. Here xk means adding k to itself x times modulo 30. To see this, a group homomorphism is determined by knowing the image of $1 \in \mathbb{Z}_{12}$, say $\varphi(1) = k$ where $k \in \mathbb{Z}_{30}$. So $|k|$ divides 30 by Lagrange's Theorem and $|k|$ must divide $|1| = 12$ as φ is a homomorphism. Thus, $|k|$ is a common divisor of 12 and 30, and so $|k|$ is either 1, 2, 3, or 6.
For a ring homomorphism, we also have to preserve multiplication. For instance,

$$k = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = k \cdot k.$$

So $k = k^2$ in $\mathbb{Z}_{30}$. This condition rules out 20 and 5 as possible values for k. The remaining choices do yield a ring homomorphism (check it). So there are four ring homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$, namely, $\varphi(x) = 0$, $\alpha(x) = 15x$, $\beta(x) = 10x$, and $\gamma(x) = 25x$.

Lemma 15.1.3.

An integer n with decimal representation $a_k a_{k-1} \cdots a_1 a_0$ is divisible by 9 if and only if $a_k + a_{k-1} + \cdots + a_1 + a_0$ is divisible by 9.

Proof. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_9$ be the natural homomorphism where $\varphi(n) = n \bmod 9$. Let n be an integer whose decimal representation is $a_k a_{k-1} \cdots a_1 a_0$. Thus $n = a_0 + a_1 \cdot 10 + a_2 \cdot$

$10^2 + \cdots + a_k \cdot 10^k$. Then as $\varphi(10) = 1$ we get the following:

$$\begin{aligned}
n \text{ is divisible by } 9 &\iff n \bmod 9 = 0 \iff \varphi(n) = 0 \\
&\iff \varphi(a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k) = 0 \\
&\iff \varphi(a_0) + \varphi(a_1 \cdot 10) + \varphi(a_2 \cdot 10^2) + \cdots + \varphi(a_k \cdot 10^k) = 0 \\
&\iff \varphi(a_0) + \varphi(a_1) \cdot \varphi(10) + \varphi(a_2) \cdot \varphi(10^2) + \cdots + \varphi(a_k) \cdot \varphi(10^k) = 0 \\
&\iff \varphi(a_0) + \varphi(a_1) + \varphi(a_2) + \cdots + \varphi(a_k) = 0 \\
&\iff \varphi(a_0 + a_1 + a_2 + \cdots + a_k) = 0 \\
&\iff a_k + a_{k-1} + \cdots + a_1 + a_0 \text{ is divisible by } 9.
\end{aligned}$$

This completes the proof. ■

15.2 Properties of Ring Homomorphisms

Theorem 15.2.1.

Let $\varphi : R \to S$ be a ring homomorphism. Let A be a subring of R and let I be an ideal of S. The following hold.

(i) For any $r \in R$ and any integer n, we have $\varphi(nr) = n\varphi(r)$.

(ii) For any $r \in R$ and any positive integer n, we have $\varphi(r^n) = [\varphi(r)]^n$.

(iii) $\varphi(A) = \{\varphi(a) \mid a \in A\}$ is a subring of S.

(iv) If A is an ideal and φ is surjective, then $\varphi(A)$ is an ideal of S.

(v) $\varphi^{-1}(I) = \{r \in R \mid \varphi(r) \in I\}$ is an ideal of R.

(vi) If R is commutative, then $\varphi(R)$ is a commutative ring.

(vii) If R has a unity, S is nontrivial, and φ is surjective, then $\varphi(1_R)$ is the unity of S.

(viii) φ is injective if and only if $\ker \varphi = \{0_R\}$.

(ix) If $\varphi : R \to S$ is a ring isomorphism, then $\varphi^{-1} : S \to R$ is also a ring isomorphism.

As one may expect, kernels are ideals and ideals are kernels. On one hand, we can use the Ideal Test to show that the kernel of a ring homomorphism is an ideal.

Lemma 15.2.2.

Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker \varphi$ is an ideal of R.

On the other hand, every ideal is the kernel of the natural homomorphism.

Theorem 15.2.3.

Let I be an ideal of a ring R. The map $\pi : R \to R/I$ given by $\pi(r) = r + I$ is a ring homomorphism. Moreover, $\ker \pi = I$. The map π is called the natural projection.

As in groups, the quotient by the kernel of a homomorphism is isomorphic to the homomorphic image.

Theorem 15.2.4. (First Isomorphism Theorem for Rings)

Let $\varphi : R \to S$ be a ring homomorphism. Then the map $\psi : R/\ker\varphi \to \varphi(R)$ given by $\psi(r + \ker\varphi) = \varphi(r)$ is an isomorphism. Thus,

$$R/\ker\varphi \cong \varphi(R).$$

Example 15.3. The map $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ given by $\varphi(f(x)) = f(0)$ is a ring homomorphism. Observe that $\ker\varphi = \langle x\rangle$. By the First Isomorphism Theorem we get that

$$\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}.$$

Moreover, since $\mathbb{Z}$ is an integral domain but not a field, we get that the ideal $\langle x\rangle$ is prime but not maximal in $\mathbb{Z}[x]$.

Theorem 15.2.5.

Suppose that R is a ring with unity 1_R. The map $\varphi : \mathbb{Z} \to R$ given by $\varphi(n) = n1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}}$ is a ring homomorphism.

Proof. We need to show that φ preserves addition and multiplication. Let $m, n \in \mathbb{Z}$.

$$\begin{aligned}\varphi(m+n) = (m+n)1_R &= \underbrace{1_R + 1_R + \cdots\cdots + 1_R}_{m+n \text{ times}} \\ &= \underbrace{(1_R + \cdots + 1_R)}_{m \text{ times}} + \underbrace{(1_R + \cdots + 1_R)}_{n \text{ times}} = \varphi(m) + \varphi(n).\end{aligned}$$

For the preservation of multiplication we use Lemma 12.2.3.

$$\varphi(m \cdot n) = (m \cdot n)\,1_R = (m \cdot n)(1_R \cdot 1_R) = (m\,1_R) \cdot (n\,1_R) = \varphi(m) \cdot \varphi(n).$$

Thus $\varphi : \mathbb{Z} \to R$ is a ring homomorphism. ■

Corollary 15.2.6.

Let R be a ring with unity.
(i) If $\operatorname{char}(R) = n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$.
(ii) If $\operatorname{char}(R) = 0$, then R contains a subring isomorphic to $\mathbb{Z}$.

Proof. Let $(R, +, \cdot)$ be a ring with unity 1_R. Consider from the previous theorem the ring homomorphism $\varphi : \mathbb{Z} \to R$ given by $\varphi(n) = n1_R$. We know that the image $\varphi(\mathbb{Z}) = S = \{n\,1_R \mid n \in Z\}$ is a subring of R. Notice that S is the additive subgroup generated by 1_R in $(R, +)$. By the First Isomorphism Theorem for rings we know that $S \cong \mathbb{Z}/\ker\varphi$.

For the first case, assume that $\operatorname{char}(R) = n > 0$. Therefore, by Lemma 13.2.2, the additive order of 1_R in R is n. Now for any integer k we have that $k \in \ker\varphi$ if and only if $\varphi(k) = 0_R$ if and only if $k\,1_R = 0_R$ if and only if n divides k. Therefore, the members of $\ker\varphi$ are precisely the integer multiples of n, in other words, $\ker\varphi = n\mathbb{Z}$. Therefore, it follows that $S \cong \mathbb{Z}/\ker\varphi = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ as desired.

For the second case, assume that $\text{char}(R) = 0$. Therefore, by Lemma 13.2.2, the additive order of 1_R in R is infinite. This means that there is no positive integer k such that $k\,1_R = 0_R$. Consequently, if $\varphi(k) = k\,1_R = 0_R$, it must be that $k = 0$. Therefore, $\ker\varphi = \{0\}$. Thus, $S \cong \mathbb{Z}/\ker\varphi = \mathbb{Z}/\{0\} \cong \mathbb{Z}$ as desired. ■

15.3 Field of Quotients

We will show that every integral domain lives inside a field as a subring. This is similar to the construction of the field of rationals $\mathbb{Q}$ from the integral domain of the integers $\mathbb{Z}$.

Theorem 15.3.1. (Field of Quotients)

Let D be an integral domain. Then there exists a field F that contains a subring isomorphic to D.

Proof. Let $(D, +, \cdot)$ be an integral domain. So D is a commutative ring with unity with no zero divisors. Let $S = \{(a, b) \in D \times D \mid b \neq 0_D\}$. We define an equivalence relation on S as follows:

$$(a, b) \sim (m, n) \text{ if and only if } a \cdot n = b \cdot m.$$

Let $\frac{a}{b}$ denotes the equivalence class of $(a, b) \in S$, that is,

$$\frac{a}{b} = [\,(a, b)\,] = \{(x, y) \in S \mid (x, y) \sim (a, b)\}.$$

Let $F = \{\frac{a}{b} \mid (a, b) \in S\}$. Next, we intend to define addition and multiplication on the set F using the addition and multiplication from the integral domain F. Let $\frac{a}{b}$ and $\frac{m}{n}$ be elements in F, we define addition and multiplication on F as follows:

$$\frac{a}{b} + \frac{m}{n} = \frac{a \cdot n + b \cdot m}{b \cdot n} \quad \text{and} \quad \frac{a}{b} \cdot \frac{m}{n} = \frac{a \cdot m}{b \cdot n}\,.$$

We will show that $(F, +, \cdot)$ is a field. First we need to show that the addition and multiplication just defined on F are well-defined. That is, these definitions do not depend on the representatives of the equivalence classes. Towards this end, assume that $\frac{a}{b} = \frac{c}{d}$ and $\frac{m}{n} = \frac{r}{s}$. And so $(a, b) \sim (c, d)$ and $(m, n) \sim (r, s)$, which implies that $a \cdot d = b \cdot c$ and $m \cdot s = n \cdot r$. First, we need to show that $\frac{a}{b} + \frac{m}{n} = \frac{c}{d} + \frac{r}{s}$. Using the commutativity, associativity, and distributivity of multiplication in D we obtain the following:

$$\begin{aligned}(an + bm)\,ds &= ands + bmds = (ad)ns + (ms)bd \\ &= (bc)ns + (nr)bd = bncs + bnrd = bn\,(cs + rd).\end{aligned}$$

This shows that $(an + bm, bn) \sim (cs + rd, ds)$, and so these pairs represent the same equivalence class. It follows,

$$\frac{a}{b} + \frac{m}{n} = \frac{an + bm}{bn} = [\,(an + bm, bn)\,] = [\,(cs + rd, ds)\,] = \frac{cs + rd}{ds} = \frac{c}{d} + \frac{r}{s}.$$

Next, to show that multiplication in F is well-defined, observe that

$$(am)(ds) = (ad)(ms) = (bc)(nr) = (bn)(cr).$$

This shows that $(am, bn) \sim (cr, ds)$ which yields to

$$\frac{a}{b} \cdot \frac{m}{n} = \frac{am}{bn} = [\,(am, bn)\,] = [\,(cr, ds)\,] = \frac{cr}{ds} = \frac{c}{d} \cdot \frac{r}{s}\ .$$

Next, we need to show that the operations are closed on F. For this, choose elements $\frac{a}{b}$ and $\frac{m}{n}$ in F. Then the pairs (a, b) and (m, n) are in S and so $b \neq 0$ and $n \neq 0$. Since D is an integral domain $bn \neq 0$ and so both pairs $(an + bm, bn)$ and (am, bn) belong to S yielding that their equivalence classes $\frac{an+bm}{bn}$ and $\frac{am}{bn}$ are in F which shows that the sum and the product of $\frac{a}{b}$ and $\frac{m}{n}$ are also in F.

We leave it to the reader to check that addition and multiplication are associative and commutative in F and that multiplication distributes over addition. Moreover, the additive identity in F is $[\,(0_D, 1_D)\,]$ that is $\frac{0_D}{1_D}$. To see this, let $\frac{a}{b}$ be any element in F. Then

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a + 0}{b} = \frac{a}{b}\ .$$

Moreover, the additive inverse of $\frac{a}{b}$ is $\frac{-a}{b}$ since

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{b^2} = \frac{ab - ab}{b^2} = \frac{0_D}{b^2} = [\,(0_D, b^2)\,] = [\,(0_D, 1_D)\,] = \frac{0_D}{1_D} = 0_F.$$

The multiplicative identity in F is $\frac{1_D}{1_D}$. To see this, let $\frac{a}{b}$ be any element in F and check that

$$\frac{a}{b} \cdot \frac{1_D}{1_D} = \frac{a \cdot 1_D}{b \cdot 1_D} = \frac{a}{b}\ .$$

To show that F is a field, it remains to show that every nonzero element in F has a multiplicative inverse. Let $\frac{a}{b} \neq 0_F$. So $\frac{a}{b} \neq \frac{0_D}{1_D}$ implying that $(a, b) \not\sim (0_D, 1_D)$ and so $a \cdot 1_D \neq b \cdot 0_D$, that is, $a \neq 0_D$. Thus, the pair $(b, a) \in S$ and so $\frac{b}{a}$ is a member of F. We claim that the multiplicative inverse of $\frac{a}{b}$ is $\frac{b}{a}$. To see this, observe that

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = [\,(ab, ab)\,] = [\,(1_D, 1_D)\,] = \frac{1_D}{1_D} = 1_F.$$

Therefore, we have shown that F is a field. By the subring test one can show that $\bar{D} = \{\frac{a}{1_D} \mid a \in D\}$ is a subring of F. Moreover, consider the function $\phi : D \to \bar{D}$ given by $\phi(a) = \frac{a}{1_D}$ for every $a \in D$. Clearly ϕ is bijective. We now show that ϕ preserves the ring operations. Choose any elements $a, b \in D$. Then

- $\phi(a + b) = \frac{a+b}{1} = \frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1} = \frac{a}{1} + \frac{b}{1} = \phi(a) + \phi(b)$.
- $\phi(ab) = \frac{ab}{1} = \frac{ab}{1 \cdot 1} = \frac{a}{1} \cdot \frac{b}{1} = \phi(a) \cdot \phi(b)$.

Thus, the map ϕ is an isomorphism of rings from D to $\bar{D}$. Therefore, the integral domain D is isomorphic to a subring of the field F as desired. ■

In the proof above, we call F the field of quotients (or the field of fractions) of the integral domain D.

Chapter 16

Polynomial Rings

16.1 Polynomials over Rings

Definition 16.1.1. (Polynomial)

Let $(R, +, \cdot)$ be a commutative ring. A *polynomial* $f(x)$ over R in the variable x is a string of symbols of the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \qquad \text{where } a_i \in R \quad \text{and} \quad n \geq 0.$$

Given two polynomials $f(x) = a_0+a_1x+\cdots+a_nx^n$ and $g(x) = b_0+b_1x+\cdots+b_mx^m$, we define $f(x) = g(x)$ if and only if $a_i = b_i$ for every i, where we set $a_i = 0_R$ when $i > n$, and similarly $b_i = 0_R$ when $i > m$. We usually write x^k for the term $(1_R)x^k$, and write $-a_kx^k$ for $+(-a_k)x^k$.

Remark. We think of the symbols $x, x^2, x^3, \ldots$ as placeholders that separate the ring elements a_i. Consequently, another way to think of a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is as an infinite sequence of the ring elements:

$$f(x) = (a_0, a_1, a_2, \ldots, a_n, 0_R, 0_R, 0_R, \ldots\ldots).$$

Definition 16.1.2. (Sum and Product of Polynomials)

Given two polynomials over a commutative ring R, say

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \quad \text{and} \quad g(x) = b_0 + b_1x + \cdots + b_mx^m,$$

we define their addition as follows.

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_s + b_s)x^s,$$

where $s = \max(m, n)$, and $a_i = 0_R$ for $i > n$, and $b_i = 0_R$ for $i > m$. Moreover, we define their multiplication as,

$$f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n},$$

where for each $k = 0, 1, \ldots, m + n$ we have that

$$c_k = \sum_{i=0}^{k} a_ib_{k-i} = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0.$$

For example,

$$\begin{aligned} c_0 &= a_0 \cdot b_0. \\ c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0. \\ c_2 &= a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0. \\ c_3 &= a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0. \end{aligned}$$

One can check that these definitions of polynomial addition and multiplication are associative and commutative, and that multiplication is distributive over addition.

Definition 16.1.3. (Polynomial Ring)

Let $(R, +, \cdot)$ be a commutative ring. The *ring of polynomials over R in the variable x* is the set $R[x]$ of all polynomials over R in the variable x with polynomial addition and multiplication.

$$R[x] = \left\{ a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \geq 0 \text{ and } a_i \in R \right\}.$$

Example 16.1. Find the sum and product of the following two polynomials in $\mathbb{Z}_3[x]$.

$$f(x) = 2 + 2x + x^2 + 2x^3 \quad \text{and} \quad g(x) = 1 + 2x + 2x^2.$$

$$\begin{aligned} f(x) + g(x) &= (2 + 1) + (2 + 2)x + (1 + 2)x^2 + (2 + 0)x^3 \\ &= 0 + 1x + 0x^2 + 2x^3 \\ &= x + 2x^3. \end{aligned}$$

$$\begin{aligned} f(x)\cdot g(x) &= (2\cdot 1)+(2\cdot 1+2\cdot 2)x+(1\cdot 1+2\cdot 2+2\cdot 2)x^2 \\ &\quad +(2\cdot 1+1\cdot 2+2\cdot 2+2\cdot 0)x^3 \\ &\quad +(0\cdot 1+2\cdot 2+1\cdot 2+2\cdot 0+2\cdot 0)x^4 \\ &\quad +(2\cdot 0+2\cdot 0+1\cdot 0+2\cdot 2+0\cdot 2+0\cdot 1)x^5 \\ &= 2+0x+0x^2+2x^3+0x^4+1x^5 \\ &= 2+2x^3+x^5. \end{aligned}$$

Lemma 16.1.4.

Suppose that D is an integral domain. Then the units of $D[x]$ are precisely the units of D.

Definition 16.1.5. (Degree of a Polynomial)

Suppose that $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ with $a_n\neq 0_R$ is a polynomial over a commutative ring R.

- We say $f(x)$ has *degree* n, and we write $\deg(f)=n$.
- The term a_n is called the *leading coefficient* of $f(x)$.
- If $a_n=1_R$, then we say that $f(x)$ is a *monic* polynomial.
- Polynomials of the form $f(x)=a_0$ are called *constant polynomials*.
- The zero polynomial $f(x)=0_R$ has no degree. However, nonzero constant polynomials have degree 0.

Lemma 16.1.6. (Degree Rule)

Suppose that f,g,h are nonzero polynomials over an integral domain. If $f(x)=g(x)h(x)$, then

$$\deg(f)=\deg(g)+\deg(h).$$

Theorem 16.1.7.

If D is an integral domain, then the ring $D[x]$ of polynomials over D is an integral domain.

16.2 The Division Algorithm for $F[x]$

Example 16.2. Find the quotient and remainder upon dividing $f(x)=3x^4+x+1$ by $g(x)=2x^2+2$ in the ring $\mathbb{R}[x]$.

Theorem 16.2.1. (Division Algorithm)

Let F be a field. Then for any polynomials $f(x)$ and $g(x)$ in $F[x]$ with $g(x)\neq 0$, there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x)=q(x)\cdot g(x)+r(x) \text{ and either } r(x)=0 \text{ or } \deg r(x)<\deg g(x).$$

Example 16.3. Find the quotient and remainder upon dividing $f(x) = 3x^4+x^3+2x^2+1$ by $g(x) = x^2+4x+2$ in the ring $\mathbb{Z}_5[x]$. The quotient is $q(x) = 3x^2+4x$ and the remainder is $r(x) = 2x + 1$.

$$3x^4 + x^3 + 2x^2 + 1 = (3x^2 + 4x) \cdot (x^2 + 4x + 2) + (2x + 1).$$

Definition 16.2.2. (Roots; Divisibility; and Multiplicity)

- Let R be a commutative ring and let $f(x)$ be a polynomial over R. For an element $a \in R$, we mean by $f(a)$ the element in R obtained by substituting a for x in the expression for $f(x)$.
- An element $a \in R$ is a *zero* (or a *root*) of a polynomial $f(x)$ if $f(a) = 0_R$.
- Let D be an integral domain and let $g(x)$ and $f(x)$ be in $D[x]$. We say that $g(x)$ *divides* $f(x)$ in $D[x]$ if there exists a polynomial $h(x) \in D[x]$ such that $f(x) = g(x)h(x)$. In this case, we write $g(x) \mid f(x)$.
- If $g(x)$ divides $f(x)$, then we say that $g(x)$ is a *factor* of $f(x)$.
- Let F be a field, $f(x) \in F[x]$, and $a \in F$. We say a is a zero of $f(x)$ of *multiplicity* k if $(x - a)^k$ is a factor of $f(x)$ but $(x - a)^{k+1}$ is not a factor of $f(x)$.

Corollary 16.2.3.

Let F be a field, $f(x) \in F[x]$, and $a \in F$. Then $f(a)$ is the remainder upon dividing $f(x)$ by $x - a$.

Corollary 16.2.4.

Let F be a field, $f(x) \in F[x]$, and $a \in F$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Theorem 16.2.5.

A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Example 16.4 (Nonexample)**.** In $\mathbb{Z}_8[x]$, the polynomial $x^2 + 7$ has $1, 3, 5, 7$ as zeros.

16.3 Principal Ideal Domains

Definition 16.3.1. (Principal Ideal Domain)

A *principal ideal domain* (PID) is an integral domain D in which every ideal is principal, that is, every ideal is of the form $\langle a \rangle = \{ra \mid r \in D\}$ for some element $a \in D$.

Theorem 16.3.2.

Let F be a field. Then $F[x]$ is a principal ideal domain.

Chapter 17

Irreducible Polynomials

Irreducible polynomials are the counterpart of prime integers.

Definition 17.0.1. (Irreducible Polynomial)

Let D be an integral domain. A nonzero, nonunit polynomial $f(x)$ over D is said to be *irreducible* over D if whenever $f(x)$ can be expressed as a product $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

A nonzero, nonunit polynomial that is not irreducible is called *reducible*. (So a reducible polynomial can be expressed as a product of two polynomials which are both nonunits.)

17.1 Polynomials over a Field

Lemma 17.1.1.

Let $f(x)$ be a polynomial over a field F with $\deg(f) \geq 1$. The following are equivalent.

(i) $f(x)$ is irreducible over F.

(ii) $f(x)$ cannot be expressed as a product of two polynomials of lower degree.

(iii) If $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, then $g(x)$ or $h(x)$ is a constant polynomial.

Theorem 17.1.2.

Let F be a field and let $f(x) \in F[x]$ with $\deg(f)$ is 2 or 3. Then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Theorem 17.1.3.

Let F be a field and let $f(x) \in F[x]$. Then the ideal $\langle f(x) \rangle$ is maximal in $F[x]$ if and only if $f(x)$ is irreducible over F.

Corollary 17.1.4.

Suppose that $f(x)$ is an irreducible polynomial over a field F. Then the quotient $F[x]/\langle f(x)\rangle$ is a field.

Corollary 17.1.5. (Euclid's Lemma for Polynomials)

Suppose that $p(x), f(x), g(x)$ are polynomials over a field F. If $p(x)$ is irreducible over F and $p(x) \mid f(x)g(x)$, then $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

17.2 Polynomials with Integer Coefficients

Recall that $\mathbb{Z}[x]$ is the ring of all polynomials with integer coefficients.

Definition 17.2.1. (Content of a Polynomial)

The *content* of a nonzero polynomial $f(x) \in \mathbb{Z}[x]$ is the greatest common divisor of the nonzero coefficients of $f(x)$. We say that $f(x) \in \mathbb{Z}[x]$ is *primitive* if its content is 1.

Lemma 17.2.2. (Gauss's Lemma)

The product of primitive polynomials is primitive.

Lemma 17.2.3.

If a polynomial $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$, then $f(x)$ is reducible over $\mathbb{Z}$.

Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime. We denote by $\bar{f}(x)$ the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p.

Theorem 17.2.4.

Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial (so $\deg(f) \geq 1$). If $\deg(\bar{f}) = \deg(f)$ and $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 17.2.5. (Eisenstein's Criterion; 1850)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial from $\mathbb{Z}[x]$. If there exists a prime p such that $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_0$, and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.