Modern Algebra

September 11, 2023

Contents

0 Preliminary **1**
0.1 Notations of sets . . . 1
0.2 Relations between sets . . . 2

1 Groups **5**
1.1 Binary operations . . . 5
1.2 Isomorphic Binary Structures . . . 8
1.3 Groups . . . 11
1.4 Finite groups . . . 14
1.5 Subgroups . . . 15
1.6 Cyclic subgroups . . . 19
1.7 Properties of cyclic groups . . . 21
1.8 Cyclic subgroups of finite order . . . 25

2 Permutations, Cosets and Direct Product **29**
2.1 Permutations and Dihedral groups . . . 29
2.2 Cayley's Theorem . . . 34
2.3 Obits, Cycle and Alternating Groups . . . 35
2.4 Cosets and the theorem of lagrange . . . 39
2.5 Direct product and finitely generated abelian groups . . . 42

3 Homomorphisms and Quotient Groups **47**
3.1 Homomorphisms . . . 47
3.2 Factor groups . . . 50
3.3 Factor group computations and simple groups . . . 55
3.4 Group action on a set . . . 63
3.5 Application of G-sets to counting . . . 68

4 Rings and Fields **71**
4.1 Rings and fields . . . 71
4.2 Integral domains . . . 75
4.3 Fermat's and Euler's Theorems . . . 77
4.4 The field of quotients of an integral domain . . . 79

5 Ideals And Factor Rings **81**

Chapter 0

Preliminary

0.1 Notations of sets

Definition 0.1. Let S be a set. We use $s \in S$ to denote that s is an element of S. We use $\emptyset$ to denote the empty set.

Notation 0.2. The following are the most commonly used sets.

$$\begin{aligned}\mathbb{Z} &:= \text{the set of integers,}\\ \mathbb{Q} &:= \text{the set of rational numbers,}\\ \mathbb{R} &:= \text{the set of real numbers,}\\ \mathbb{C} &:= \text{the set of complex numbers,}\end{aligned}$$

where by convention, ":=" means "is defined by".

Notation 0.3 (Set-builder notation)**.** Let S be a set.

$$\begin{aligned}\{x \mid P(x)\} &:= \text{ the set of all elements } x \text{ such that the statement } P(x) \text{ about } x \text{ is true,}\\ \{x \in S \mid P(x)\} &:= \text{ the set of all elements } x \text{ in } S \text{ such that the statement } P(x) \text{ about } x \text{ is true.}\end{aligned}$$

Example 0.4.

$$\begin{aligned}S &:= \{2, 4, 6, \dots, 100\} = \{2x \mid x = 1, \dots, 50\},\\ 2\mathbb{Z} &:= \{\dots, -4, -2, 0, 2, 4, \dots\} = \{2x \mid x \in \mathbb{Z}\},\\ A &:= \{10, 11, 12, \dots\} = \{x \in \mathbb{Z} \mid x \geqslant 10\}.\end{aligned}$$

Example 0.5.

$$\begin{aligned}
\mathbb{N} &:= \{1, 2, 3, \dots\} = \{x \in \mathbb{Z} \mid x > 0\},\\
\mathbb{N}_0 &:= \{0, 1, 2, 3, \dots\} = \{x \in \mathbb{Z} \mid x \geqslant 0\},\\
\mathbb{Z}^{>0} &:= \{x \in \mathbb{Z} \mid x > 0\} = \mathbb{N},\\
\mathbb{Q}^{>0} &:= \{x \in \mathbb{Q} \mid x > 0\},\\
\mathbb{R}^{>0} &:= \{x \in \mathbb{R} \mid x > 0\},\\
\mathbb{Z}^{\geqslant 0} &:= \{x \in \mathbb{Z} \mid x \geqslant 0\} = \mathbb{N}_0,\\
\mathbb{Q}^{\geqslant 0} &:= \{x \in \mathbb{Q} \mid x \geqslant 0\},\\
\mathbb{R}^{\geqslant 0} &:= \{x \in \mathbb{R} \mid x \geqslant 0\}.
\end{aligned}$$

Definition 0.6. We say a set A is a subset of a set B, denoted by $A \subseteq B$ or $B \supseteq A$, if $a \in B$ for any $a \in A$. We use $A \subsetneq B$ or $B \supsetneq A$ to denote that A is a proper subset of B, that is, $A \subseteq B$ but $A \neq B$.

Definition 0.7. We define the Cartesian product of sets A and B by

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

Example 0.8. Let $A = \{1, 2\}$ and $B = \{5, 6, 9\}$. Then

$$A \times B = \{(1, 5), (1, 6), (1, 9), (2, 5), (2, 6), (2, 9)\}.$$

0.2 Relations between sets

Definition 0.9. A relation between sets A and B is a subset $\mathcal{R}$ of $A \times B$. For $(a, b) \in \mathcal{R}$, we write $a \mathcal{R} b$.

Example 0.10. Consider the sets A and B in Example 0.8. Since $\{(1, 5), (1, 9), (2, 6)\} \subseteq A \times B$, we have that it is a relation between A and B. The relation $\mathcal{R} = \{(a, b) \in A \times B \mid b - a = 4\} = \{(1, 5), (2, 6)\}$ makes more sense.

Example 0.11 (Equality Relation)**.** The equality relation $=$ on a set S is defined by

$$= := \{(x, x) \mid x \in S\}.$$

If $S = \{1, 2\}$, then $\underbrace{=}_{\text{a set}} = \{(1, 1), (2, 2)\}$. Since $(1, 1) \in =$, we write $1 = 1$.

Definition 0.12. A function or a map ϕ mapping a set X into a set Y, written as $\phi : X \longrightarrow Y$ or $X \xrightarrow{\phi} Y$, is a relation between X and Y such that each $x \in X$ appears as the first member of exactly one ordered pair (x, y) in ϕ, i.e., $\phi = \{(x, \phi(x)) \mid x \in X\}$. If $(x, y) \in \phi$, we write $\phi(x) = y$ or $x \longmapsto y$.

Example 0.13. Let $X = \{-1, 1, 2\}$, $Y = \mathbb{N}$ and the function ϕ be

$$\begin{aligned} \phi : X &\longrightarrow Y \\ -1 &\longmapsto 1 \\ 1 &\longmapsto 1 \\ 2 &\longmapsto 4 \end{aligned}$$

Note that ϕ can also be written as

$$\begin{aligned} \phi : \{-1, 1, 2\} &\longrightarrow \mathbb{N} \\ x &\longmapsto x^2 \end{aligned}$$

Definition 0.14. Let $\phi : X \to Y$, then X is called the domain of ϕ, and Y is called the codomain of ϕ. The image or range of ϕ is

$$\mathrm{Im}(\phi) := \phi(X) = \{\phi(x) \mid x \in X\}.$$

Example 0.15. In Example 0.13, we have that $\mathrm{Im}(\phi) = \{1, 4\}$.

Definition 0.16. The cardinality of a set X, denoted by $|X|$, is the number of elements in X. If $X = \emptyset$, then $|X| = 0$. If X is an infinite set, then let $|X| = \infty$.

Definition 0.17. Let $\phi : X \to Y$.

(a) ϕ is called one-to-one or an injection if $\phi(x_1) = \phi(x_2)$ with $x_1, x_2 \in X$ implies that $x_1 = x_2$.

(b) ϕ is called onto or a surjection if $\mathrm{Im}(\phi) = Y$.

(c) ϕ is called one-to-one correspondence or a bijection if ϕ is both one-to-one and onto. In this case, X and Y are said to have the same cardinality, i.e., $|X| = |Y|$.

Remark. If $|X| = \infty = |Y|$, then often one cannot say that $|X| = |Y|$ since we cannot compare two infinities, except for that there is a 1-1 correspondence between X and Y. For example, $|\mathbb{Z}| = |\mathbb{N}| = |\mathbb{Q}|$ (countable). Note that $\mathbb{R}$ is uncountable.

Definition 0.18. Let $\phi : X \to Y$ be 1-1. We defined the inverse function ϕ^{-1} by

$$\begin{aligned} \phi^{-1} : \mathrm{Im}(\phi) &\longrightarrow X \\ \phi(x) &\longmapsto x \end{aligned}$$

ϕ^{-1} is well-defined, because if there is $\phi(\tilde{x}) \in \mathrm{Im}(\phi)$ with $\tilde{x} \neq x$ such that $\phi(\tilde{x}) = \phi(x)$, then $\tilde{x} = x$ since ϕ is 1-1, a contradiction. Note that ϕ^{-1} is always a 1-1 correspondence.

Remark. If ϕ is a 1-1 correspondence, then $\mathrm{Im}(\phi) = Y$ and so

$$\begin{aligned} \phi^{-1} : Y &\longrightarrow X \\ \phi(x) &\longmapsto x \end{aligned}$$

Definition 0.19. A partition of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets. The subsets are called the *cells* of the partition.

Convention 0.20. When discussing a partition of a set S, we denote by $\bar{x}$ the cell containing the element x of S. Thus, $\bar{x} = \bar{y}$ if and only if x and y are in the same cell.

Example 0.21. The collection $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ forms a partition of $\mathbb{Z}$.

$$2\mathbb{Z} := \{2x \mid x \in \mathbb{Z}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} = \overline{-4} = \overline{-2} = \bar{0} = \bar{2} = \bar{4} = \cdots,$$

$$2\mathbb{Z}+1 := \{2x+1 \mid x \in \mathbb{Z}\} = \{\dots, -5, -3, -1, 1, 3, 5 \dots\} = \overline{-5} = \overline{-3} = \overline{-1} = \bar{1} = \bar{3} = \cdots.$$

When considering the partition $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ of $\mathbb{Z}$, we use $\bar{0}$ and $\bar{1}$ to represent the cells $2\mathbb{Z}$ and $2\mathbb{Z}+1$, respectively. When consider the partition $\{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$ of $\mathbb{Z}$, we use $\bar{0}$, $\bar{1}$ and $\bar{2}$ to represent the cells $3\mathbb{Z}$, $3\mathbb{Z}+1$, and $3\mathbb{Z}+2$, respectively.

In general, for an integer $n \geqslant 2$, we can partition $\mathbb{Z}$ into n cells $\bar{0}$, $\bar{1}$, $\bar{2}$, $\cdots$, $\overline{n-1}$ according to whether the remainder is $0, 1, 2, \dots, n-1$ when an integer is divided by n. They are called the residue classes module n in $\mathbb{Z}$.

Fact 0.22. Each partition of a set S yields a relation $\mathcal{R}$ on S naturally: let $x \mathcal{R} y$ ($(x, y) \in \mathcal{R}$) if and only if and only if $\bar{x} = \bar{y}$ (x and y are in the same cell).

Definition 0.23. An equivalence relation $\sim$ on a set S is one that satisfies these three properties for all $x, y, z \in S$.

- (Reflexive) $x \sim x$.
- (Symmetric) If $x \sim y$, then $y \sim x$.
- (Transitive) If $x \sim y$ and $y \sim z$, then $x \sim z$.

Theorem 0.24. *The relation $\mathcal{R}$ corresponding to a partition of a set S is an equivalence relation.*

Proof. It follows from Convention 0.20 and Fact 0.22: Let $x, y, z \in S$.

(Reflexive) Since $\bar{x} = \bar{x}$ (x and x are clearly in the same cell), we have that $x \mathcal{R} x$.

(Symmetric) If $x \mathcal{R} y$, then $\bar{x} = \bar{y}$, so $\bar{y} = \bar{x}$, and thus $y \mathcal{R} x$.

(Transitive) If $x \mathcal{R} y$ and $y \mathcal{R} z$, then $\bar{x} = \bar{y}$ and $\bar{y} = \bar{z}$, hence $\bar{x} = \bar{z}$ and so $x \mathcal{R} z$. □

Theorem 0.25. *An equivalence relation $\sim$ on a set S yield a natural partition of S, where the*

$$\bar{a} = \{x \in S \mid x \sim a\}.$$

Proof. Let $a \in S$. Since a must be in the "cell" $\bar{a}$ by the reflexive condition, the left is to show that if $a \in \bar{b}$, then $\bar{a} = \bar{b}$.

$\subseteq$ Let $x \in \bar{a}$. Then $x \sim a$. But $a \in \bar{b}$, so $a \sim b$. Thus, $x \sim b$ by the transitivity, and so $x \in \bar{b}$.

$\supseteq$ Let $y \in \bar{b}$. Then $y \sim b$. But $a \in \bar{b}$, so $a \sim b$, and then $b \sim a$ by symmetry. Hence $y \sim a$ by the transitivity, and so $y \in \bar{a}$. □

Definition 0.26. Each cell in the partition arising from an equivalence relation $\sim$ on a set S is an equivalence class. For $x \in S$, we have that the equivalence class containing x is $\bar{x} = \{y \in S \mid y \sim x\} = \{y \in S \mid x \sim y\}$ by Theorem 0.25 and symmetry.

Chapter 1

Groups

1.1 Binary operations

Definition 1.1. A binary operation $*$ on a set S is a function $* : S \times S \to S$. We write

$$\begin{aligned} * : S \times S &\longrightarrow S \\ (a, b) &\longmapsto a * b := *(a, b) \end{aligned}$$

Example 1.2. The usual addition on $\mathbb{R}$:

$$\begin{aligned} + : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (a, b) &\longmapsto a + b \end{aligned}$$

and the usual multiplication on $\mathbb{Z}$:

$$\begin{aligned} \cdot : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\longmapsto a \cdot b = ab \end{aligned}$$

are binary operations. The matrix addition on $m \times n$ matrices $\mathrm{Mat}_{m\times n}(\mathbb{R})$:

$$\begin{aligned} + : \mathrm{Mat}_{m\times n}(\mathbb{R}) \times \mathrm{Mat}_{m\times n}(\mathbb{R}) &\longrightarrow \mathrm{Mat}_{m\times n}(\mathbb{R}) \\ (M, N) &\longmapsto M + N \end{aligned}$$

and the matrix multiplication on $n \times n$ square matrices $\mathrm{Mat}_n(\mathbb{R})$:

$$\begin{aligned} \cdot : \mathrm{Mat}_n(\mathbb{R}) \times \mathrm{Mat}_n(\mathbb{R}) &\longrightarrow \mathrm{Mat}_n(\mathbb{R}) \\ (M, N) &\longmapsto M \cdot N \end{aligned}$$

are binary operations.

Fact 1.3. The usual $+$ and the usual $\cdot$ are binary operations on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, respectively.

Definition 1.4. Let $* : S \times S \to S$ and $H \subseteq S$. The subset H is closed under $*$ if $a * b \in H$ for all $a, b \in H$, that is to say, $\{a * b \mid a, b \in H\} \subseteq H$. In this case, the binary operation on H given by restricting $*$ to H is the induced operation of $*$ on H, that is to say, we have a binary operation $*$ on H:

$$* : H \times H \to H.$$

Example 1.5. Let $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be the usual multiplication. The subset $\mathbb{Z}$ of $\mathbb{R}$ is closed under $\cdot$ since $a \cdot b \in \mathbb{Z}$ for any $a, b \in \mathbb{Z}$. So we have an induced operation $\cdot$ on $\mathbb{Z}$:

$$\begin{aligned} \cdot : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

Example 1.6. Let $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$. We have that $\mathbb{R}^*$, as a subset of $\mathbb{R}$, is not closed under $+$ because $-2, 2 \in \mathbb{R}^*$ but $-2 + 2 = 0 \notin \mathbb{R}^*$. This also means that $+ : \mathbb{R}^* \times \mathbb{R}^* \to \mathbb{R}^*$ is not well-defined.

Example 1.7. Let $H := \{n^2 \mid n \in \mathbb{N}\} \subseteq \mathbb{Z}$. Then $H = \{1, 4, 9, 16, \dots\}$.

(a) H is not closed under $+$ since $1, 4 \in H$ but $1 + 4 = 5 \notin H$.

(b) H is closed under $\cdot$ because for any $n^2, m^2 \in H$ with $m, n \in \mathbb{N}$, we have that $nm \in \mathbb{N}$ and $n^2 \cdot m^2 = (nm)^2 \in H$ by the associativity and commutativity (defined later) of $\cdot$ on $\mathbb{Z}$

Definition 1.8. Let $F = \{f : \mathbb{R} \to \mathbb{R}\}$, i.e., F is the set of functions from $\mathbb{R}$ to $\mathbb{R}$. For any $f, g \in F$, define

$$\begin{aligned} f + g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) + g(x), \end{aligned}$$

$$\begin{aligned} f - g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) - g(x) \end{aligned}$$

$$\begin{aligned} f \cdot g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) \cdot g(x), \end{aligned}$$

$$\begin{aligned} f \circ g : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(g(x)). \end{aligned}$$

Then $f + g, f - g, f \cdot g, f \circ g \in F$ for any $f, g \in F$. So we have binary operations $+$, $-$, $\cdot$ and $\circ$ on F. For example,

$$\begin{aligned} + : F \times F &\longrightarrow F \\ (f, g) &\longmapsto f + g : \mathbb{R} \longrightarrow \mathbb{R} \\ &\qquad\qquad x \longmapsto f(x) + g(x) \end{aligned}$$

Remark. Let f, g be two functions. Then $f \circ g$ is well-defined if and only if $\mathrm{Im}(g) \subseteq \mathcal{D}(f)$, where $\mathcal{D}(f)$ is the domain of f. In particular, if $f : Y \to Z$ and $g : X \to Y$, then $\mathrm{Im}(g) \subseteq Y = \mathcal{D}(f)$ and so

$$X \xrightarrow{g} Y \xrightarrow{f} Z.$$

Definition 1.9. A binary operation $*$ on a set S is commutative if and only if $a * b = b * a$ for all $a, b \in S$.

Definition 1.10. A binary operation on a set S is associative if $(a * b) * c = a * (b * c)$.

Remark. If $*$ is associative, then the longer expression such as $a * b * c$ are not ambiguous.

Example 1.11. Define a relation $*$ on $\mathbb{Z}$ by

$$\begin{aligned} * : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\longmapsto ab + 2 \end{aligned}$$

Then $*$ is commutative since $a * b = ab + 2 = ba + 2 = b * a$ for any $a, b \in \mathbb{Z}$, but $*$ is not associative since for any $a, b, c \in \mathbb{Z}$ with $a \neq c$, we get $(a * b) * c \neq a * (b * c)$ by showing that

$$\begin{aligned} (a * b) * c &= (ab + 2) * c = (ab + 2)c + 2 = abc + 2c + 2, \\ a * (b * c) &= a * (bc + 2) = a(bc + 2) + 2 = abc + 2a + 2. \end{aligned}$$

Theorem 1.12. *Let S be a set and $H = \{f : S \to S\}$. Then $\circ$ is associative on H.*

Proof. Let $f, g, h \in H$. We want to prove $(f \circ g) \circ h = f \circ (g \circ h)$. Note that

$$\underbrace{S \xrightarrow{h} \underbrace{S \xrightarrow{g} S}_{f \circ g} \xrightarrow{f} S}_{(f \circ g) \circ h}, \qquad \underbrace{S \xrightarrow{h} \underbrace{S \xrightarrow{g} S}_{g \circ h} \xrightarrow{f} S}_{f \circ (g \circ h)}.$$

So $(f \circ g) \circ h : S \to S$ and $f \circ (g \circ h) : S \to S$. This shows that they have the same domain and codomain. Next, for $x \in S$, we have that

$$\begin{aligned} (f \circ g) \circ h(x) &= (f \circ g)(h(x)) = f(g(h(x))), \\ f \circ (g \circ h)(x) &= f((g \circ h)(x)) = f(g(h(x))). \end{aligned}$$

Since $x \in S$ is arbitrary, we have that $f \circ (g \circ h) = (f \circ g) \circ h$. □

Example 1.13. The following table defines a binary operation $*$ on $S = \{a, b, c\}$ by the following rule:

$$\begin{aligned} &(i^{\text{th}} \text{ entry on the left}) * (j^{\text{th}} \text{ entry on the top}) \\ &= (\text{entry in the } i^{th} \text{ row and } j^{\text{th}} \text{ column of the table body}). \end{aligned}$$

Table 1.1

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

Since $a * b = c$ and $b * a = a$, we have that $*$ is not commutative. Since $(a * b) * c = c * c = a$ and $a * (b * c) = a * b = c$, we have that $*$ is not associative.

A binary operation defined by a table is commutative if and only if the table is symmetric about the diagonal.

1.2 Isomorphic Binary Structures

Table 1.2

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

Table 1.3

$\star$	x	y	z
x	y	z	y
y	x	z	y
z	z	y	x

There are $3 \times 2 \times 1 = 6$ one-to-one correspondence functions from S to T. (First, the image of a has 3 choices, then the image b has 2 choices, and finally the image of c has 1 choice.)

$$\begin{array}{llllll} S \xrightarrow{f} T & S \xrightarrow{g} T & S \xrightarrow{h} T & S \xrightarrow{i} T & S \xrightarrow{j} T & S \xrightarrow{k} T \\ a \longmapsto x & a \longmapsto x & a \longmapsto y & a \longmapsto y & a \longmapsto z & a \longmapsto z \\ b \longmapsto y & b \longmapsto z & b \longmapsto x & a \longmapsto z & b \longmapsto x & b \longmapsto y \\ c \longmapsto z & c \longmapsto y & c \longmapsto z & c \longmapsto x & c \longmapsto y & c \longmapsto x \end{array}$$

The 1-1 correspondence f is what we are most interested in, because you can check that

$$f(\alpha * \beta) = f(\alpha) \star f(\beta), \forall \alpha, \beta \in S.$$

For example,

$$\begin{aligned} f(a * a) = f(b) = y = x \star x = f(a) \star f(a), \\ f(a * b) = f(c) = z = x \star y = f(a) \star f(b), \\ f(a * c) = f(b) = y = x \star z = f(a) \star f(c). \end{aligned}$$

Definition 1.14. Define a binary algebraic structure $\langle S, * \rangle$ to be a set S together with a binary operation $*$ on S.

Definition 1.15. Let $\langle S, * \rangle$ and $\langle T, \star \rangle$ be binary algebraic structures. A homomorphism of S with T is a function $\phi : S \to T$ such that

$$\phi(x * y) = \phi(x) \star \phi(y), \forall x, y \in S.$$

A homomorphism $\phi : S \to T$ is an isomorphism if ϕ is a 1-1 correspondence. S and T are isomorphic binary structures, denoted by $S \cong T$, if there is an isomorphism $\phi : S \to T$.

Example 1.16. Let $\mathbb{R}^+ := \{x \in \mathbb{R} \mid x > 0\}$. Let us show that

$$\langle \mathbb{R}, + \rangle \cong \langle \mathbb{R}^+, \cdot \rangle.$$

Define

$$\begin{aligned} \phi : \mathbb{R} &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto e^x. \end{aligned}$$

Since $e^x > 0$ for any $x \in \mathbb{R}$, we have that ϕ is well-defined. Since $\phi(x+y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$ for any $x, y \in \mathbb{R}$, we have that ϕ is a homomorphism. Let $x, y \in \mathbb{R}$ be such that $\phi(x) = \phi(y)$. Then $e^x = e^y$. Since $e^{(\cdot)} : \mathbb{R} \to \mathbb{R}^+$ is a strictly monotonic (increasing) function, we have that $x = y$. Hence ϕ is 1-1. Let $y \in \mathbb{R}^+$. Then $\phi(\ln y) = e^{\ln y} = y$, and so ϕ is onto.

Example 1.17. Let $n \in \mathbb{N}$. Let $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ be the residue classes module n in $\mathbb{Z}$, and

$$U_n := \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{i2\pi m/n} \mid m = 0, 1, \ldots, n-1\}$$

be the n^{th} roots of unity. Note that for $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$,

$$\begin{aligned}
\bar{x} &= \{y \mid x \sim y\} \\
&= \{y \mid x \text{ and } y \text{ are in the same cell}\} \\
&= \{y \mid n \text{ divides } (x-y)\} \\
&= \{y \mid x \equiv y \pmod{n}\}.
\end{aligned}$$

We define an operation $+$ on $\mathbb{Z}/n\mathbb{Z}$ by

$$\begin{aligned}
+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\
(\overline{m}, \bar{k}) &\longmapsto \overline{m+k}
\end{aligned}$$

We check that the operation $+$ is well-defined. Let $(\overline{m}_1, \bar{k}_1) = (\overline{m}, \bar{k})$, then $\overline{m}_1 = \overline{m}$ and $\bar{k}_1 = \bar{k}$. Then $n \mid (m_1 - m)$ and $n \mid (k_1 - k)$, and so $m_1 = na + m$ and $k_1 = nb + k$ for some $a, b \in \mathbb{Z}$. Hence $m_1 + k_1 = n(a+b) + (m+k)$, i.e., $n(a+b) = (m_1 + k_1) - (m+k)$, and so $n \mid ((m_1 + k_1) - (m+k))$. Thus, $\overline{m_1 + k_1} = \overline{m+k}$. This means that $+(\overline{m}, \bar{k}) = +(\overline{m}_1, \bar{k}_1)$ or $\overline{m} + \bar{k} = \overline{m}_1 + \bar{k}_1$.

Define

$$\begin{aligned}
\phi : \langle \mathbb{Z}/n\mathbb{Z}, + \rangle &\longrightarrow \langle U_n, \cdot \rangle \\
\overline{m} &\longmapsto e^{i2\pi m/n}.
\end{aligned}$$

First, we check that ϕ is well-defined. Let $\overline{m} = \bar{k}$ in $\mathbb{Z}/n\mathbb{Z}$. Then $n \mid (m-k)$ and so $m = na + k$ for some $a \in \mathbb{Z}$. Hence

$$\phi(\overline{m}) = e^{i2\pi m/n} = e^{i2\pi(na+k)/n} = e^{i2\pi a} \cdot e^{2\pi k/n} = e^{i2\pi k/n} = \phi(\bar{k}).$$

So ϕ is well-defined. Since

$$\phi(\overline{m} + \bar{k}) = \phi(\overline{m+k}) = e^{i2\pi(m+k)/n} = e^{i2\pi m/n} \cdot e^{i2\pi k/n} = \phi(\overline{m}) \cdot \phi(\bar{k}), \forall\, \overline{m}, \bar{k} \in \mathbb{Z}/n\mathbb{Z},$$

we have that ϕ is a homomorphism. ϕ is clearly onto. Next, we show that ϕ is 1-1. Suppose that $\overline{m}, \bar{k} \in \mathbb{Z}/n\mathbb{Z}$ be such that $\phi(\overline{m}) = \phi(\bar{k})$. Then $e^{i2\pi m/n} = e^{i2\pi k/n}$, so $e^{i2\pi(m-k)/n} = 1$, implying that $(m-k)/n$ is an integer, so $n \mid (m-k)$, and thus $\overline{m} = \bar{k}$.

Fact 1.18. Let $\langle S, * \rangle$ and $\langle T, \star \rangle$ be binary algebraic structures.

(a) If there is not 1-1 correspondence between S and T, then $S \ncong T$. For example, if $|S| < \infty$ but $|T| = \infty$, then $S \ncong T$. If $|S| = \infty = |T|$, and S is countable but T is uncountable, then $S \ncong T$.

(b) If $*$ is commutative on S, but $\star$ is not on T, then $S \ncong T$. (We cannot find any $\phi : S \to T$ such that ϕ is a homomorphism.)

(c) Let $\phi : S \to T$, if there are $x, y \in S$ such that $x * y = y * x$ but $\phi(x) \star \phi(y) \neq \phi(y) \star \phi(x)$, then ϕ is not a homomorphism.

(d) Let $\phi : S \to T$, if there are $x, y \in S$ such that $x * x = x$, but $\phi(x) \star \phi(x) \neq \phi(x)$, then ϕ is not a homomorphism.

Definition 1.19. Let $\langle S, * \rangle$ be a binary structure. An element e of S is an identity element for $*$ if $e * s = s = s * e$ for all $s \in S$.

Theorem 1.20. *If a binary structure $\langle S, * \rangle$ has an identity element, then it is unique.*

Proof. Suppose that we have two identity elements e and f. Then

$$e \overset{f \text{ is id.}}{=\!=\!=} e * f \overset{e \text{ is id.}}{=\!=\!=} f.$$ □

Theorem 1.21. *Suppose $\langle S, * \rangle$ has an identity element e. If $\phi : S \to T$ is a surjective homomorphism of $\langle S, * \rangle$ and $\langle T, \star \rangle$, then $\phi(e) \in T$ is an identity element for $\star$.*

Proof. Let $t \in T$. Since ϕ is surjective (onto), we have that there exists $s \in S$ such that $\phi(s) = t$. We have that

$$\phi(e) \star t = \underbrace{\phi(e) \star \phi(s) = \phi(e * s)}_{\phi \text{ is a homo.}} = \phi(s) = t,$$

$$t \star \phi(e) = \phi(s) \star \phi(e) = \underbrace{\phi(s * e) = \phi(s)}_{e \text{ is an id. elt.}} = t.$$

Thus, $\phi(e)$ is an identity element on T. □

Example 1.22. We have that $\langle \mathbb{Q}, + \rangle \ncong \langle \mathbb{Z}, + \rangle$.

Proof. Suppose that $\phi : \mathbb{Q} \to \mathbb{Z}$ is an isomorphism. Then ϕ is onto. So for $1 \in \mathbb{Z}$, there is an $x \in \mathbb{Q}$ such that $\phi(x) = 1$. Since $x/2 \in \mathbb{Q}$, we have that $2\phi(x/2) = \phi(x/2) + \phi(x/2) = \phi(x/2 + x/2) = \phi(x) = 1$, but $2y = 1$ has no solution in $\mathbb{Z}$, a contradiction. Thus, there is no isomorphic function from $\langle \mathbb{Q}, + \rangle$ to $\langle \mathbb{Z}, + \rangle$. □

Example 1.23. We have that $\langle \mathbb{C}, \cdot \rangle \ncong \langle \mathbb{R}, \cdot \rangle$.

Proof. Suppose that $\phi : \mathbb{C} \to \mathbb{R}$ is an isomorphism. Then ϕ is onto. So for $-1 \in \mathbb{R}$, there is an $x \in \mathbb{C}$ such that $\phi(x) = -1$. Since $\sqrt{x} \in \mathbb{C}$, we have that $(\phi(\sqrt{x}))^2 = \phi(\sqrt{x}) \cdot \phi(\sqrt{x}) = \phi(\sqrt{x} \cdot \sqrt{x}) = \phi(x) = -1$, but $y^2 = -1$ has no solution in $\mathbb{R}$, a contradiction. Thus, there is no isomorphic function from $\langle \mathbb{C}, \cdot \rangle$ to $\langle \mathbb{R}, \cdot \rangle$. □

1.3 Groups

Why define groups? $2x = 1$ has no solution in $\langle \mathbb{Z}, \cdot \rangle$, but $2 + x = 1$ has one in $\langle \mathbb{Z}, + \rangle$.

Definition 1.24. A group is a binary structure $\langle G, * \rangle$, such that the following axioms are satisfied:

$\mathscr{G}_1$: For all $a, b, c \in G$, we have that

$$(a * b) * c = a * (b * c). \qquad \textbf{associativity of } *$$

$\mathscr{G}_2$: There is $e \in G$ such that for all $a \in G$,

$$e * a = a = a * e. \qquad \textbf{identity element } e \textbf{ for } *$$

$\mathscr{G}_3$: Corresponding to each $a \in G$, there is an element $\tilde{a} \in G$ such that

$$\tilde{a} * a = e = a * \tilde{a}. \qquad \textbf{inverse } \tilde{a} \textbf{ of } a$$

Remark. If $\langle G, + \rangle$ is a group, then we write $-a$ for the inverse of $a \in G$.
If $\langle G, \cdot \rangle$ is a group, then we write a^{-1} for the inverse of $a \in G$.

Example 1.25. (a) $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{C}, + \rangle$ are groups with the (additive) identity 0.

(b) $\langle \mathbb{Q}^*, \cdot \rangle$, $\langle \mathbb{R}^*, \cdot \rangle$, $\langle \mathbb{C}^*, \cdot \rangle$ are groups with the (multiplicative) identity 1.

(c) $\langle \mathbb{Q}^{>0}, \cdot \rangle$, $\langle \mathbb{R}^{>0}, \cdot \rangle$ are group with the (multiplicative) identity 1.

Example 1.26. (a) $\langle \mathbb{Z}, \cdot \rangle$, $\langle \mathbb{Q}, \cdot \rangle$, $\langle \mathbb{R}, \cdot \rangle$, $\langle \mathbb{C}, \cdot \rangle$ are not groups.

(b) $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{N}, \cdot \rangle$ are not groups.

(c) $\langle \mathbb{Z}^*, + \rangle$, $\langle \mathbb{Z}^*, \cdot \rangle$ are not groups.

Example 1.27. $\langle n\mathbb{Z}, + \rangle$ is a group for each $n \in \mathbb{Z}$.

Example 1.28. (a) Let $n \geqslant 2$. Then $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ is a group with the (additive) identity $\bar{0}$, and for any $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, the (additive) inverse of $\bar{a}$ is $-\bar{a} := \overline{n - a}$, because

$$\bar{a} + (-\bar{a}) = \bar{a} + \overline{n - a} = \bar{n} = \bar{0}.$$

Note that you may say that $Z_n := \{0, \ldots, n-1\}$ under addition modulo n is a group with the (additive) identity 0 and the inverse $n - a$ for each $a \in \mathcal{Z}_n$.

(b) Let $p \in \mathbb{N}$ be a prime number. $\langle (\mathbb{Z}/p\mathbb{Z})^\times, \cdot \rangle$, is a group, where $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ and $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ (or $\bar{a}\bar{b} = \overline{ab}$) for any $\bar{a}, \bar{b} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Note that you may say that $Z_p^\times := \{1, 2, \ldots, p-1\}$ under multiplication modulo p is a group with the (multiplicative) identity 1.

In fact, for prime number p, we have that $\mathbb{F}_p := Z_p$ is a (finite) field, because $\langle \mathbb{F}_p, + \rangle$ is an (additive) group and $\langle \mathbb{F}_p^\times, \cdot \rangle$ is a (multiplicative) group.

Remark. Let $p \in \mathbb{N}$ be prime and $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. By Euclidean Algorithm, we can find $x, y \in \mathbb{Z}$ such that $ax + py = \gcd(a, p) = 1$. So $\bar{a}\bar{x} = \overline{ax} + \bar{0} = \bar{a}\bar{x} + \bar{0}\bar{y} = \bar{a}\bar{x} + \bar{p}\bar{y} = \bar{1}$, thus, $\bar{a}^{-1} = \bar{x}$.

Definition 1.29. A group $\langle G, * \rangle$ is abelian if its binary operation $*$ is commutative.

Example 1.30. (a) $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{C}, + \rangle$ are abelian groups.

(b) $\langle \mathbb{Q}^*, \cdot \rangle$, $\langle \mathbb{R}^*, \cdot \rangle$, $\langle \mathbb{C}^*, \cdot \rangle$ are abelian groups

(c) $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ is an abelian group.

(d) $\langle \mathrm{Mat}_{n \times m}(\mathbb{R}), + \rangle$ is an abelian group.

(e) The general linear group of degree n

$$\mathrm{GL}_n(\mathbb{R}) := \{M \in \mathrm{Mat}_n(\mathbb{R}) \mid M \text{ is invertible}\}$$

is a group under $\cdot$ for $n \in \mathbb{N}$, but not abelian under $\cdot$ when $n \in \mathbb{Z}^{\geqslant 2}$. Note that $\langle \mathrm{GL}_1(\mathbb{R}), \cdot \rangle = \langle \mathbb{R}^*, \cdot \rangle$.

(f) $\langle \{f : \mathbb{R} \to \mathbb{R}\}, + \rangle$ is an abelian group.

(g) For any $\mathbb{R}$-vector space $\langle V, +, \cdot \rangle$, $\langle V, + \rangle$ is an abelian group.

Theorem 1.31. *If $\langle G, * \rangle$ is a group, then for all $a, b, c \in G$,*

$$a * b = a * c \Longrightarrow b = c, \qquad \textbf{left cancellation law}$$
$$b * a = c * a \Longrightarrow b = c. \qquad \textbf{right cancellation law}$$

Proof. We have that

$$\begin{aligned} a * b = a * c &\overset{\mathscr{G}_3}{\Longrightarrow} \tilde{a} * (a * b) = \tilde{a} * (a * c) \\ &\overset{\mathscr{G}_1}{\Longrightarrow} (\tilde{a} * a) * b = (\tilde{a} * a) * c \\ &\overset{\mathscr{G}_2}{\Longrightarrow} e * b = e * c \\ &\overset{\mathscr{G}_2}{\Longrightarrow} b = c. \end{aligned}$$

□

Corollary 1.32. If $\langle G, * \rangle$ is a group, then for $a, b \in G$, the linear equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G.

Proof. Method 1. Existence. Since $a * (\tilde{a} * b) = (a * \tilde{a}) * b = e * b = b$, we have that $x = \tilde{a} * b$ is a solution of $a * x = b$. Uniqueness. Suppose that there exists $x_1, x_2 \in G$ such that $a * x_1 = b$ and $a * x_2 = b$. Then $a * x_1 = a * x_2$, and so $x_1 = x_2$ by the left cancellation law.

Method 2. If $a * x = b$, then $x = \tilde{a} * b$ by observing that

$$x = e * x = (\tilde{a} * a) * x = \tilde{a} * (a * x) = \tilde{a} * b.$$

□

Theorem 1.33. *If $\langle G, * \rangle$ is a group, then $e \in G$ is unique. For each $a \in G$, $\tilde{a} \in G$ is unique.*

Proof. Since $\langle G, * \rangle$ is a binary structure, we have that $e \in G$ is unique by Theorem 1.20. Suppose there exist $\tilde{a}, \hat{a} \in G$ such that $\tilde{a} * a = e = a * \tilde{a}$ and $\hat{a} * a = e = a * \hat{a}$. Then $\tilde{a} * a = \hat{a} * a$, and so $\tilde{a} = \hat{a}$ by the right cancellation law. □

Corollary 1.34. If $\langle G, * \rangle$ is a group, then $\tilde{\tilde{a}} = a$ for any $a \in G$.

Proof. Since $\tilde{a} * a = e = a * \tilde{a}$, we have that $a * \tilde{a} = e = \tilde{a} * a$, and so a is the inverse of $\tilde{a}$. Since $\tilde{\tilde{a}}$ is the inverse of $\tilde{a}$ by definition/notation, we have that $\tilde{\tilde{a}} = a$ by Theorem 1.33. □

Corollary 1.35. Let $\langle G, * \rangle$ be a group. For all $a, b \in G$, we have that the (unique) inverse of $a * b$ is $\tilde{b} * \tilde{a}$, i.e., $\widetilde{a * b} = \tilde{b} * \tilde{a}$.

Proof. Since

$$(\tilde{b} * \tilde{a}) * (a * b) = \tilde{b} * (\tilde{a} * a) * b = (\tilde{b} * e) * b = \tilde{b} * b = e,$$

and $(a * b) * (\tilde{b} * \tilde{a}) = e$, we have that $\widetilde{a * b} = \tilde{b} * \tilde{a}$. □

Remark. If $\langle G, + \rangle$ is a group, then we write that $-(a + b) = (-b) + (-a)$ for any $a, b \in G$.
If $\langle G, \cdot \rangle$ is a group, then we write that $(ab)^{-1} = b^{-1}a^{-1}$ for any $a, b \in G$.

Definition 1.36. A semigroup $\langle S, * \rangle$ is an binary structure such that $*$ is associative.
A monid is a semigroup $\langle S, * \rangle$ that has an identity element for the binary operation $*$.

We have an equivalent definition (via left axioms) for groups.

Definition 1.37. A group is a binary structure $\langle G, * \rangle$, such that the following axioms are satisfied:

$\mathscr{G}_{\mathrm{I}}$: For all $a, b, c \in G$, we have that

$$(a * b) * c = a * (b * c). \qquad \textbf{associativity of } *$$

$\mathscr{G}_{\mathrm{II}}$: There is $e \in G$ such that for all $a \in G$,

$$e * a = a. \qquad \textbf{(left) identity element } e \textbf{ for } *$$

$\mathscr{G}_{\mathrm{III}}$: Corresponding to each $a \in G$, there is an element $\tilde{a} \in G$ such that

$$\tilde{a} * a = e. \qquad \textbf{(left) inverse } \tilde{a} \textbf{ of } a$$

Remark. We proved the equivalence:

Proof. Condition $\mathscr{G}_{\mathrm{I}}$ is the same as $\mathscr{G}_1$. Clearly, we have that $\mathscr{G}_2 \implies \mathscr{G}_{\mathrm{II}}$ and $\mathscr{G}_3 \implies \mathscr{G}_{\mathrm{III}}$. The remaining is to show the following:
$\mathscr{G}_{\mathrm{II}} \implies \mathscr{G}_2$ For $a \in G$,

$$\begin{aligned} a * e = e * (a * e) = (\tilde{\tilde{a}} * \tilde{a}) * (a * e) = \tilde{\tilde{a}} * (\tilde{a} * a) * e = (\tilde{\tilde{a}} * e) * e \\ = \tilde{\tilde{a}} * (e * e) = \tilde{\tilde{a}} * e = \tilde{\tilde{a}} * (\tilde{a} * a) = (\tilde{\tilde{a}} * \tilde{a}) * a = e * a = a. \end{aligned}$$

$\mathscr{G}_{\mathrm{III}} \implies \mathscr{G}_3$ For $a \in G$,

$$\begin{aligned} a * \tilde{a} = e * (a * \tilde{a}) = (\widetilde{a * \tilde{a}} * (a * \tilde{a})) * (a * \tilde{a}) = \widetilde{a * \tilde{a}} * ((a * \tilde{a}) * (a * \tilde{a})) \\ = \widetilde{a * \tilde{a}} * (a * (\tilde{a} * a) * a) = \widetilde{a * \tilde{a}} * ((a * e) * \tilde{a}) = \widetilde{a * \tilde{a}} * (a * \tilde{a}) = e. \end{aligned}$$

□

By symmetry, we can define groups via right axioms.

1.4 Finite groups

Example 1.38. (a) If $G := \{e\}$ is a group, then e is the identity.

(b) Assume that $G := \{e, a\}$ is a group under $*$. Then

$*$	e	a
e	e	a
a	a	

$\Longrightarrow$

$*$	e	a
e	e	a
a	a	e

Suppose that $a*a = a$, then $a = e$ by multiplying by $\tilde{a}$ on both sides, contradicting $a \neq e$. Hence $a * a = e$. Hence the structure of groups of 2 elements are uniquely determined, up to isomorphism, and so $\langle G, * \rangle \cong \langle Z_2, +_2 \rangle$. Recall that if $\phi : \langle S, * \rangle \to \langle T, \star \rangle$ is a homomorphism, then $\phi(e)$ is the identity element of T by Theorem 1.21. Thus, we have a unique isomorphism given by

$$\begin{aligned} \langle G, * \rangle &\xrightarrow{\cong} \langle Z_2, +_2 \rangle \\ e &\longmapsto 0 \\ a &\longmapsto 1 \end{aligned}$$

Proposition 1.39. When giving a table for a finite group $\langle G, * \rangle$, each element $a \in G$ must appear once and only once in each row and each column of the table.

Proof. Let $x \in G$. Define a map by

$$\begin{aligned} \lambda_x : G &\longrightarrow G \\ a &\longmapsto x * a \end{aligned}$$

Let $a, b \in G$ such that $\varphi_x(a) = \varphi_x(b)$, i.e., $x * a = x * b$. Then $a = b$ by the left cancellation law. So φ_x is 1-1. By Pigeonhole Principle (PHP), φ_x is onto, which implies φ_x is a permutation map. Or we can check the onto-ness directly: for $b \in G$, letting $a := x^{-1}b \in G$, we have that

$$\varphi_x(a) = \varphi_x(x^{-1} * b) = x * (x^{-1} * b) = (x * x^{-1}) * b = e * b = b.$$

Hence for the row whose first element is x, elements in the table body of that row is a permutation. Since $x \in G$ is arbitrary, we have that each row in the table body is a permutation of G. Similarly, each column in the table body is a permutation of G. □

Fact 1.40. Let $\langle G, \cdot \rangle$ be an arbitrary group and $x \in G$. Then similar to the proof of Proposition 1.39, we have a 1-1 correspondence

$$\begin{aligned} \lambda_x : G &\longrightarrow G \\ a &\longmapsto xa \end{aligned}$$

So we get that

$$xG = \{xa \mid a \in G\} = \mathrm{Im}(\lambda_x) = G.$$

For $a, b \in G$, $\lambda(ab) = x(ab) = xab$ and $\lambda_x(a)\lambda_x(b) = (xa)(xb) = xaxb$, hence in general, λ_x is not an isomorphism. Check that the σ_x defined below is an isomorphism.

$$\begin{aligned} \sigma_x : G &\xrightarrow{\cong} G \\ a &\longmapsto xax^{-1}. \end{aligned}$$

Fact 1.41. When giving a table for a finite binary structure $\langle G, * \rangle$ such that each element $a \in G$ must appear once and only once in each row and each column of the table, then G is a group if and only if the associative law holds.

Example 1.42. Let $G := \{e, a, b\}$ be a group under $*$.

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

$\Longrightarrow$

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

where $a * a = b$ because b cannot occur in the 3rd row and in the 3rd column. So the table is uniquely determined for a group consisting of 3 elements. Thus, we say that there is only one group of 3 elements, up to isomorphism, and so $\langle G, * \rangle \cong \langle Z_3, +_3 \rangle$. Note that there are two isomorphisms between them:

$$\begin{aligned} G &\xrightarrow{\cong} Z_3 \\ e &\longmapsto 0 \\ a &\longmapsto 1 \\ b &\longmapsto 2 \end{aligned} \qquad\qquad \begin{aligned} G &\xrightarrow{\cong} Z_3 \\ e &\longmapsto 0 \\ a &\longmapsto 2 \\ b &\longmapsto 1 \end{aligned}$$

1.5 Subgroups

Convention 1.43. We use 0 to denote an additive identity for a group $\langle G, + \rangle$, and 1 to denote a multiplicative identity for a group $\langle G, \cdot \rangle$.

If we say that G is a group, we usually mean that the operation is $\cdot$, and then a^{-1} is used to denote the inverse of $a \in G$.

Definition 1.44. Let $\langle G, + \rangle$ be a group, $a \in G$, and $n \in \mathbb{N}$, define

$$\begin{aligned} 0a &= 0, \\ na &= \underbrace{a + \cdots + a}_{n \text{ times}}, \\ -na &= \underbrace{(-a) + \cdots + (-a)}_{n \text{ times}} = n(-a). \end{aligned}$$

Example 1.45. $\langle \mathbb{Z}, + \rangle$ is a group. Then for $m \in \mathbb{Z}$,

$$m(1) = (-m)(-1) = m = 1(m) = (-1)(-m).$$

For $m \in \mathbb{Z}$, since $m + (-m) = 0 = (-m) + m$, we have that $-(-m) = m$. Note that

$$(-0)(-1) = 0(-1) = 0.$$

For $m \in \mathbb{N}$,

$$\begin{aligned} m(1) &= \underbrace{1 + \cdots + 1}_{m \text{ times}} = m, \\ 1(m) &= \underbrace{m}_{1 \text{ time}} = m, \\ (-m)(-1) &= m(-(-1)) = m(1) = m, \\ (-1)(-m) &= 1(-(-m)) = 1(m) = m, \end{aligned}$$

and for $m \in \mathbb{Z}^{<0}$,

$$\begin{aligned} m(1) = -(-m)(1) &= \underbrace{(-1) + \cdots + (-1)}_{(-m) \text{ times}} = m, \\ 1(m) &= \underbrace{m}_{1 \text{ time}} = m, \\ (-m)(-1) &= \underbrace{(-1) + \cdots + (-1)}_{(-m) \text{ times}} = m, \\ (-1)(-m) &= 1(-(-m)) = 1(m) = m. \end{aligned}$$

More generally, we can prove that $(-m)(-k) = mk = (-k)(-m)$ for $m, k \in \mathbb{Z}$. From now on, you can directly use these results when working inside $\langle \mathbb{Z}, + \rangle$.

Definition 1.46. Let $\langle G, \cdot \rangle$ be a group, $a \in G$, and $n \in \mathbb{N}$, define

$$\begin{aligned} a^0 &= 1, \\ a^n &= \underbrace{a \cdots a}_{n \text{ times}}, \\ a^{-n} &= \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ times}} = (a^{-1})^n. \end{aligned}$$

Theorem 1.47. *Let $\langle G, \cdot \rangle$ be a group and $a \in G$. Then $a^m a^n = a^{m+n}$ for $m, n \in \mathbb{Z}$.*

Proof. If $mn = 0$, it is trivial. If $mn > 0$, it holds by definition. If $mn < 0$, then without loss of generality assume that $m > 0$ and $n < 0$, and so

$$\begin{aligned} a^m a^n = \underbrace{a \cdots a}_{m \text{ times}} \underbrace{a^{-1} \cdots a^{-1}}_{-n \text{ times}} &= \begin{cases} \underbrace{a \cdots a}_{m-(-n) \text{ times}} & \text{if } m \geqslant |n| \\ \underbrace{a^{-1} \cdots a^{-1}}_{-(m+n) \text{ times}} & \text{otherwise} \end{cases} \\ &= \begin{cases} a^{m+n} & \text{if } m \geqslant |n| \\ a^{-(-(m+n))} & \text{otherwise} \end{cases} = \begin{cases} a^{m+n} & \text{if } m \geqslant |n| \\ a^{m+n} & \text{otherwise} \end{cases} = a^{m+n}. \end{aligned}$$

□

Corollary 1.48. Let $\langle G, \cdot \rangle$ be a group, then

$$(a^n)^{-1} = a^{-n} = (a^{-1})^n, \forall n \in \mathbb{Z}$$

and so

$$(a^{-n})^{-1} = a^n = (a^{-1})^{-n}, \forall n \in \mathbb{Z}.$$

Proof. For each $n \in \mathbb{Z}$, since

$$a^n a^{-n} = a^{n+(-n)} = a^0 = 1 = a^0 = a^{(-n)+n} = a^{-n}a^n,$$

we have that $(a^n)^{-1} = a^{-n}$.

If $n = 0$, then $a^{-0} = a^0 = 1 = (a^{-1})^0$. If $n > 0$, then $a^{-n} = (a^{-1})^n$. If $n < 0$, then

$$a^{-n} = (a^n)^{-1} = (a^{-(-n)})^{-1} = ((a^{-1})^{-n})^{-1} = (a^{-1})^n.$$

Hence $a^{-n} = (a^{-1})^n$ for each $n \in \mathbb{Z}$. □

Definition 1.49. Let G be a group, then $|G|$ is called the order of G.

Definition 1.50. If $\langle G, * \rangle$ and $\langle H, * \rangle$ are groups and $H \subseteq G$, then H is a subgroup of G, denoted by $H \leqslant G$ or $G \geqslant H$. G itself is an improper subgroup of G. If $H \subsetneq G$, then H is a proper subgroup of G, denoted by $H \lneq G$ or $G \gneq H$. $\{e\} \leqslant G$ is the trivial subgroup of G.

Example 1.51. (a) $n\mathbb{Z} \leqslant \mathbb{Z} \lneq \mathbb{Q} \lneq \mathbb{R} \lneq \mathbb{C}$ under $+$, where $n \in \mathbb{Z}$. In particular, $n\mathbb{Z} = \mathbb{Z}$ if $n = \pm 1$, and $n\mathbb{Z} < \mathbb{Z}$ if $n \in \mathbb{Z} \setminus \{\pm 1\}$.

(b) $\mathbb{Q}^{>0} \lneq \mathbb{Q}^* \lneq \mathbb{R}^* \lneq \mathbb{C}^*$ and $U_n \lneq \mathbb{C}^*$ under $\cdot$.

(c) Let $n \in \mathbb{Z}^{\geqslant 2}$ and $H =: \{(0, a_2, \ldots, a_n) \mid a_2, \ldots, a_n \in \mathbb{R}\}$. Then $H \lneq \mathbb{R}^n$ under the coordinate-wise addition.

Remark. $\mathbb{R}^n$ is a group under component-wise addition with identity $(0, \ldots, 0)$. For the inverse of $(a_1, \ldots, a_n) \in \mathbb{R}^n$ is $(-a_1, \ldots, -a_n)$. Check that $\mathbb{R}^n$ is closed under component-wise addition and the operation is associative.

We have a natural isomorphism

$$\begin{aligned} H &\xrightarrow{\cong} \mathbb{R}^{n-1} \\ (0, a_2, \ldots, a_n) &\longmapsto (a_2, \ldots, a_n). \end{aligned}$$

Example 1.52. Let G be a group of $|G| = 4$. Then either $G \cong (Z_4, +_4)$, or $G \cong (Z_2^2, +_2)$. We call $\langle Z_2^2, +_2 \rangle$ the Klein 4-group with the operation given by $(a_1, b_1) +_2 (a_2, b_2) = (a_1 +_2 a_2, b_1 +_2 b_2)$.

Table 1.4

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	3	0	1	2
3	0	0	0	0

Table 1.5

$+_2$	$(0,0)$	$(0,1)$	$(1,0)$	(1,1)
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	(1,1)
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	(1,0)
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Since $1+1, 3+3 \neq 0$ modulo 4, but $(0,1)+(0,1), (1,0)+(1,0), (1,1)+(1,1) = (0,0)$ modulo 2, we have that $2x = 0$ has 2 solutions in $\mathbb{Z}_4$, but $2y = (0,0)$ has 4 solutions in Z_2^2. Thus, $Z_4 \ncong Z_2^2$.

Remark. The dihedral group of order 6 is the smallest finite non-abelian group.

It is often useful to draw a subgroup diagram of the subgroups of a group. In such a diagram, a line running downward from a group G to a group H means that H is a subgroup of G. Thus, the larger group is placed nearer the top of the diagram.

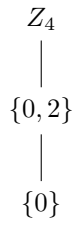


Figure 1.1

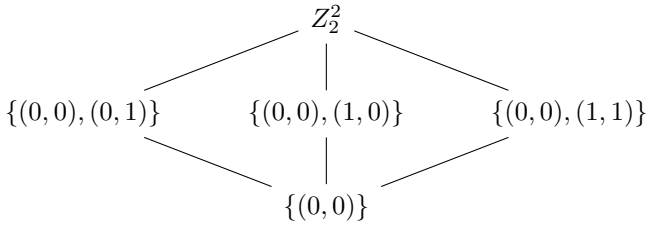


Figure 1.2

Example 1.53. Since Z_4 is 1 nontrivial subgroup and Z_2^2 has 3 nontrivial subgroups, we have that $Z_4 \ncong Z_2^2$.

Example 1.54. Under the function addition, we have the following subgroup diagram:

$$\{f : \mathbb{R} \to \mathbb{R}\}$$
$$|$$
$$\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous}\}$$
$$|$$
$$\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is differentiable}\}$$

Theorem 1.55 (Subgroup test 1)**.** *Let G be a group and $H \subseteq G$. Then $H \leqslant G$ if and only if*

(a) H is closed under the binary operation of G,

(b) the identity element $1_G \in H$, and

(c) $a^{-1} \in H$ for all $a \in H$.

Proof. $\implies$ Assume that $H \leqslant G$. Then clearly Condition (a) holds. Let 1_H be the identity element of H. Then $1_H = 1_H 1_H$. View the equation as one in G, we see that

$$1_H^{-1} 1_H = 1_H^{-1}(1_H 1_H) \implies 1_G = (1_H^{-1} 1_H) 1_H \implies 1_G = 1_G 1_H \implies 1_G = 1_H \in H.$$

Hence Condition (b) holds. Let a_H^{-1} be the inverse of a in H. Then $1_G = 1_H = a a_H^{-1}$. View the equation as on in G, we have that

$$a^{-1} 1_G = a^{-1}(a a_H^{-1}) \implies a^{-1} = (a^{-1} a) a_H^{-1} \implies a^{-1} = 1_G a_H^{-1} \implies a^{-1} = a_H^{-1} \in H.$$

$\Longleftarrow$ Condition (a) implies that H is a binary structure. By Condition (b) we have at once that $\mathscr{G}_2$ is satisfied. Also $\mathscr{G}_3$ is satisfied by Condition (c). For $a, b, c \in H$, we have that $(ab)c = a(bc)$ when viewed as an equation in G. So $(ab)c = a(bc)$ in H and thus $\mathscr{G}_1$ holds. Therefore, $H \leqslant G$. □

Theorem 1.56 (Subgroup test 2)**.** *Let G be a group and $\emptyset \neq H \subseteq G$. Then $H \leqslant G$ if and only if*

(a) H is closed under the binary operation of G, and

(b) $a^{-1} \in H$ for all $a \in H$.

Proof. By Theorem 1.57, it is enough to show that the identity element $1_G \in H$ from the forward direction. For $a \in H$, we have that $a^{-1} \in H$ by (b), and so $1_G = aa^{-1} \in H$ by (a). □

Combining Conditions (a) with (b) in Theorem 1.57, we have another elegant subgroup test criterion given below. The proof is left as an exercise.

Theorem 1.57 (Subgroup test 3)**.** *Let G be a group and $\emptyset \neq H \subseteq G$. Then $H \leqslant G$ if and only if $ab^{-1} \in H$ for $a, b \in H$.*

Fact 1.58. The proof of Theorem 1.55 provides us some byproducts about the relationship between elements of H and G when $H \leqslant G$:

(a) H and G share the same identity element.

(b) For $a \in H$, G and H share the same inverse a^{-1}.

Example 1.59. Let $n \in \mathbb{N}$. Define the special linear group of degree n by

$$\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid \det(M) = 1\}.$$

Note that $\mathrm{SL}_n(\mathbb{R}) \subseteq \mathrm{GL}_n(\mathbb{R})$, then $\mathrm{SL}_n(\mathbb{R}) \leqslant \mathrm{GL}_n(\mathbb{R})$ under $\cdot$ by subgroup test:

(a) For $M, N \in \mathrm{SL}_n(\mathbb{R})$, $MN \in \mathrm{SL}_n(\mathbb{R})$ because $\det(MN) = \det(M)\det(N) = 1 > 0$.

(b) For the identity matrix (element) $I_n \in \mathrm{GL}_n(\mathbb{R})$, $\det(I_n) = 1$, and so $I_n \in \mathrm{SL}_n(\mathbb{R})$.

(c) For $M \in \mathrm{SL}_n(\mathbb{R})$, $\det(M^{-1}) = 1/\det(M) = 1/1 = 1 > 0$, and so $M^{-1} \in \mathrm{SL}_n(\mathbb{R})$.

1.6 Cyclic subgroups

Theorem 1.60. *Let G be a group and $a \in G$. Then $H := \{a^n \mid n \in \mathbb{Z}\} \leqslant G$. If $a \in K \leqslant G$, then $H \leqslant K$.*

Proof. Subgroup test:

(a) Let $a^m, a^n \in H$. Then $a^m a^n = a^{m+n} \in H$.

(b) 1 is the identity element of G and $1 = a^0 \in H$.

(c) For $a^n \in H$, we have that in G the inverse of a^n is a^{-n}, but $a^{-n} \in H$.

Therefore, $H \leqslant G$.

Assume that $a \in K \leqslant G$. Then K is a group and, so $a^0 = 1 \in K$ and $a^{-1} \in K$ by Fact 1.58. Since K is closed under $\cdot$, we have that $a^m, a^{-k} \in K$ for all $m, k \in \mathbb{N}$. Hence $a^n \in K$ for any $n \in \mathbb{Z}$, implying that $H \subseteq G$. We just showed that $H \leqslant K$, so H is a group, and thus $H \leqslant K$. □

Definition 1.61. Let G be a group and $a \in G$. Then the subgroup $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$ of G is called the cyclic subgroup of G generated by a.

Remark. If $\langle G, + \rangle$ is a group, then $\langle a \rangle := \{na \mid n \in \mathbb{Z}\}$.

Definition 1.62. If G is a group and $G = \langle a \rangle$ for some $a \in G$, then G is cyclic, and we say that a generates G or a is a generator for G.

Example 1.63. $Z_4 = \langle 1 \rangle = \langle 3 \rangle$, but Z_2^2 is not cyclic, because $\langle (0,0) \rangle = \{(0,0)\}$, $\langle (0,1) \rangle = \{(0,0),(0,1)\}$, $\langle (1,0) \rangle = \{(0,0),(1,0)\}$, and $\langle (1,1) \rangle = \{(0,0),(1,1)\}$.

Example 1.64. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, and $\langle n \rangle = n\mathbb{Z} < \mathbb{Z}$ for $n \in \mathbb{Z} \setminus \{\pm 1\}$. Note that for $m \in \mathbb{Z}$, by Example 1.45, we have that $m = (-m)(-1) \in \langle -1 \rangle$, and so $\mathbb{Z} = \langle -1 \rangle$.

Example 1.65. For $n \in \mathbb{N}$, $Z_n = \langle 1 \rangle = \langle n-1 \rangle$, because for $m = 0, \ldots, n-1$,

$$\underbrace{(n-1) + \cdots + (n-1)}_{(n-m)\text{times}} = (n-m)(n-1) = n^2 - n - mn + m = n(n-1-m) + m \equiv m \pmod{n}.$$

Example 1.66. $U_n = \langle \zeta \rangle = \langle \zeta^{n-1} \rangle$, where $\zeta = e^{i2\pi/n}$, because for $m = 0, \ldots, n-1$,

$$(\zeta^{n-1})^{n-m} = (e^{2\pi i(n-1)/n})^{n-m} = e^{2\pi i(n-m)(n-1)/n} = e^{2\pi i(n(n-1-m)+m)/n} = e^{2\pi i m/n} = \zeta^m.$$

This actually follows from $Z \cong U_n$ through $m \leftrightarrow \zeta^m$ for all m.

For $a \in \{z \in \mathbb{C} \mid |z| = 1\} =: \mathbb{S}^1$, multiplying a by ζ^{n-1}, i.e., $\zeta^{n-1}a = e^{i(n-1)\frac{2\pi}{n}}a$ is equivalent to rotating the a along the unit circle $\mathbb{S}^1$ counterclockwise by $(n-1)\frac{2\pi}{n} = 2\pi - \frac{2\pi}{n}$, and this is equivalent to rotating that element along the circle clockwise by $\frac{2\pi}{n}$. For example, we get that $\zeta^{n-1}a = \zeta^{n-3}$ when $a = \zeta^{n-2}$. This can also be seen from that $\zeta^{n-1} = \zeta^{-1}$ and $\zeta^{n-2} = \zeta^{-2} = (\zeta^{-1})^2$, etc.

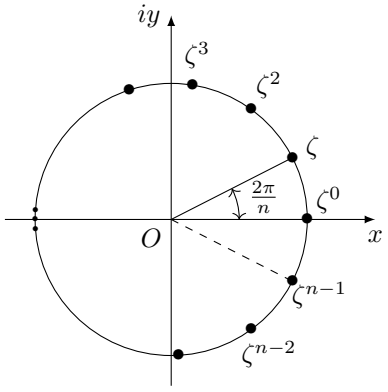


Figure 1.3

1.7 Properties of cyclic groups

Definition 1.67. Let G be a group and $a \in G$. The order of a is

$$|a| := |\langle a \rangle|.$$

Remark. We will see in this section that if $|\langle a \rangle| < \infty$, then

$$|a| = \min\{n \in \mathbb{N} \mid a^n = 1\}.$$

Cyclic groups are fundamental to the understanding of groups.

Theorem 1.68. *Every cyclic group is abelian.*

Proof. Let G be a group and $a \in G$ such that $G = \langle a \rangle$. Let $a^m, a^n \in G$ with $m, n \in \mathbb{Z}$. Then $a^m a^n = a^{m+n} = a^n a^m$. Thus, G is abelian. □

Proposition 1.69 (Division Algorithm)**.** If $m \in \mathbb{N}$ and $n \in \mathbb{Z}$, then there exists unique integers q and r such that

$$n = mq + r, \ 0 \leqslant r < m.$$

In particular, if $m \nmid n$, then $0 < r < m$.

Proof. Existence. Let $q_0 := \max\{q \in \mathbb{Z} \mid mq \leqslant n\}$. Then $m(q_0 + 1) > n$, i.e., $m > n - mq_0 =: r_0$. Then $n = mq_0 + r_0$ and $0 \leqslant r_0 < m$.

Uniqueness. Suppose that there exist another $r_1, q_1 \in \mathbb{Z}$ such that $n = mq_1 + r_1$ and $0 \leqslant r_1 < m$. Then $mq_0 + r_0 = mq_1 + r_1$, i.e., $m \mid (r_1 - r_0)$. Since $-m < r_1 - r_0 < m$, we have that $r_1 = r_0$. This implies that $mq_0 = mq_1$, i.e., $m(q_0 - q_1) = 0$. Since $\mathbb{Z}$ has no nonzero zero divisors and $m \in \mathbb{N}$, we have that $q_0 = q_1$. □

Definition 1.70. In the notation of the division algorithm, we regard q as the quotient and r as the nonnegative remainder when n is divided by m.

Example 1.71. (a) Find the quotient q and reminder r when $n = 38$ is divided by $m = 7$. By the division algorithm, $q = \max\{q \in \mathbb{Z} \mid 7q \leqslant 38\} = 5$, then $r = n - mq = 38 - 7(5) = 3$.

(b) Find the quotient q and reminder r when $n = -38$ is divided by $m = 7$. By the division algorithm, $q = \max\{q \in \mathbb{Z} \mid 7q \leqslant -38\} = -6$, then $r = n - mq = -38 - 7(-6) = 4$.

Theorem 1.72. *A subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle a \rangle$ be a cyclic group and $H \leqslant G$. If $H = \{1\}$, then $H = \langle 1 \rangle$ is cyclic. Assume now that $H \neq \{1\}$, then $a^k \in H$ for some $k \in \mathbb{Z} \setminus \{0\}$. Since $a^k a^{-k} = a^0 = 1$ and H is a group, we have that $a^{-k} = (a^k)^{-1} \in H$. This implies that $a^m \in H$ for some $m \in \mathbb{N}$. Let $m := \min\{m \in \mathbb{N} \mid a^m \in H\}$. We claim that $H = \langle a^m \rangle$. Let $b \in H \subseteq G$. Then $b = a^n$ for some $n \in \mathbb{Z}$. Find $q, r \in \mathbb{Z}$ such that

$$n = mq + r, \ 0 \leqslant r < m.$$

Then $b = a^n = a^{mq+r} = (a^m)^q a^r$, and so $a^r = (a^m)^{-q} a^n$. Since $a^m \in H$, similarly, we have that $(a^m)^{-q} \in H$. Also, since $a^n = b \in H$ and H is a group, we have that $a^r \in H$. By the definition of m and the fact that $r \in \{0, \ldots, m-1\}$, we have that $r = 0$. Hence $n = mq$, and thus $b = a^n = (a^m)^q$. Therefore, $H = \langle a^m \rangle$ since $b \in H$ is arbitrarily chosen. (Note that the definition of m also works for $H = \{1\}$.) □

Corollary 1.73. If $H \leqslant \mathbb{Z}$, then $H = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Proof. By Theorem 1.72,

$$H = \langle n \rangle = \{mn \mid m \in \mathbb{Z}\} = \{nm \mid m \in \mathbb{Z}\} = n\mathbb{Z},$$

where the third equality follows from that $\cdot$ in $\mathbb{Z}$ is commutative. □

Definition 1.74. Let $a \in \mathbb{Z} \setminus \{0\}$ and $b, c \in \mathbb{Z}$ such that $b \neq 0$ or $c \neq 0$.

(a) If $a \mid b$ and $a \mid c$, we say that a is a common divisor of b and c.

(b) The largest common positive divisor of b and c is called the greatest common divisor of b and c, denoted by $\gcd(b, c)$.

(c) Analogously define $\gcd(b_1, \ldots, b_n)$ for $n \in \mathbb{Z}^{\geqslant 3}$.

Convention 1.75. For $b, c \in \mathbb{Z}$, when we write $\gcd(b, c)$, we mean that $b \neq 0$ or $c \neq 0$.

Theorem 1.76. *Let $b, c \in \mathbb{Z}$. Then*

$$\gcd(b, c) = \min\{bx + cy > 0 \mid x, y \in \mathbb{Z}\}.$$

Proof. Let $D = \{bx + cy > 0 \mid x, y \in \mathbb{Z}\}$. Then $D \neq \emptyset$. Let $d := \min D$, then $d = bx + cy$ for some $x, y \in \mathbb{Z}$. Suppose that $d \nmid b$. Since $d > 0$, we can write $b = dq + r$ with $0 < r < d$. Then

$$r = b - dq = b - (bx + cy)q = b(1 - qx) + c(-yq) \in D,$$

contradicting $0 < r < d = \min D$. So $d \mid b$. Similarly, $d \mid c$. Hence $0 < d \leqslant \gcd(b, c) =: g$. Note that $b = gB$ and $c = gC$ for some $B, C \in \mathbb{Z}$. Then

$$d = bx + cy = (gB)x + (gC)y = g(Bx + Cy),$$

and so $g \mid d$. Thus, $g = d$. □

Corollary 1.77. If $b, c, m, n \in \mathbb{Z}$ is such that $bm + cn = 1$, then

$$\gcd(b, c) = \gcd(b, n) = \gcd(m, c) = \gcd(m, n) = 1.$$

Corollary 1.78. Let $b, c \in \mathbb{Z}$ and $n \in \mathbb{Z}$. Then

$$\gcd(b, c) = \gcd(c, b) = \gcd(-b, c) = \gcd(b, c + bn).$$

Proof. Note that

$$\gcd(b, c) = \min\{bx + cy > 0 \mid x, y \in \mathbb{Z}\} = \min\{cy + bx > 0 \mid y, x \in \mathbb{Z}\} = \gcd(c, b),$$
$$\gcd(b, c) = \min\{bx + cy > 0 \mid x, y \in \mathbb{Z}\} = \min\{-bx + cx > 0 \mid y, x \in \mathbb{Z}\} = \gcd(-b, c).$$

Next,

$$\gcd(b, c + bn) = \min\{bx + (c + bn)y > 0 \mid x, y \in \mathbb{Z}\} = \min\{b(x + ny) + cy > 0 \mid x, y \in \mathbb{Z}\}.$$

To show that $\gcd(b, c) = \gcd(b, c + bn)$, it suffices to show that $\{(x + ny, y) \mid x, y \in \mathbb{Z}\} = \mathbb{Z}^2$. This is true because for $(s, t) \in \mathbb{Z}^2$, letting $x := s - ny$ and $y := t$, we have that $(x + ny, y) = (s, t)$. □

Definition 1.79. If $b, c \in \mathbb{Z}$ such that $\gcd(b, c) = 1$, then a and b are relatively prime.

Theorem 1.80. *If $c \mid ab$ and $\gcd(b, c) = 1$, then $c \mid a$.*

Proof. Since $\gcd(b, c) = 1$, we have that there exist m, n such that $1 = bm+cn$. Then $a = abm+acn$. Since $c \mid ab$ and $c \mid ac$, we have that $c \mid abm$ and $c \mid acn$. Thus, $c \mid a$. □

Theorem 1.81 (Euclidean Algorithm)**.** *Let $b \in \mathbb{Z}$ and $c \in \mathbb{N}$. Repeat applying the division algorithm, write*

$$\begin{aligned} b &= cq_1 + r_1, 0 < r_1 < c, \\ c &= r_1q_2 + r_2, 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Then $r_n = \gcd(b, c)$. (As $r_1 > r_2 > \cdots > r_{n-1} > r_n > 0$, the algorithm terminates after finite steps.)

Proof. Note that

$$\begin{aligned} \gcd(b, c) &= \gcd(b - cq_1, c) = \gcd(r_1, c) = \gcd(r_1, c - r_1q_2) = \gcd(r_1, r_2) \\ &= \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1} - r_nq_{n+1}, r_n) = \gcd(0, r_n) = r_n. \end{aligned}$$

□

Remark. This allows us to solve the linear Diophantine equation $bx + cy = \gcd(b, c) = r_n$, i.e.,

$$r_n = r_{n-2} - r_{n-1}q_n = (r_{n-4} - r_{n-3}q_{n-2})q_{n-1} - (r_{n-3} - r_{n-2}q_{n-1})q_n = \cdots = bx + cy,$$

i.e., continue to let $r_j = r_{j-2} - q_jr_{j-1}$ for $j = n, \ldots, 3$, $r_2 = c - r_1q_2$, and $r_1 = b - cq_1$.

Example 1.82. Find integers x, y such that $95x + 432y = 1$. Note that

$$\begin{aligned} 432 &= 95(4) + 52, \\ 95 &= 52(1) + 43, \\ 52 &= 43(1) + 9, \\ 43 &= 9(4) + 7, \\ 9 &= 7(1) + 2, \\ 7 &= 2(3) + 1, \\ 2 &= 1(2). \end{aligned}$$

Hence $\gcd(95, 423) = 1$. Then

$$\begin{aligned} 1 &= 7 - 2(3) = 7 - (9 - 7)3 = -9(3) + 7(4) = -9(3) + (43 - 9(4))4 = 4(43) - 19(9) \\ &= 4(43) - 19(52 - 43(1)) = -19(52) + 23(43) = -19(52) + 23(95 - 52(1)) \\ &= 23(95) - 42(52) = 23(95) - 42(432 - 95(4)) = 95(191) - 432(42). \end{aligned}$$

Theorem 1.83. *Let G be a cyclic group.*

(a) If $|G| = \infty$, then $G \cong \mathbb{Z}$.

(b) If $|G| = n$, then $G \cong Z_n$.

Proof. Assume that $G = \langle a \rangle$ with $a \in G$.

(a) Define

$$\begin{aligned} \phi : G &\longrightarrow \mathbb{Z} \\ a^n &\longmapsto n \end{aligned}$$

Let $h, k \in \mathbb{Z}$ be such that $a^h = a^k$. Suppose without of loss of generality that $h < k$. Then $a^{k-h} = a^k a^{-h} = a^h a^{-h} = a^0 = 1$. Let $m := k - h \in \mathbb{N}$. We claim that

$$G = \{a^k \mid k = 0, \ldots, m-1\} =: H.$$

Let $a^n \in G$ with $n \in \mathbb{Z}$. Then by the division algorithm, $n = mq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leqslant r \leqslant m-1$, and so $a^n = a^{mq+r} = (a^m)^q a^r = 1^q a^r = a^r \in H$. Hence $G \subseteq H \subseteq G$, so $|G| = |H| \leqslant m$, contradicting $|G| = \infty$. Thus, $h = k$, and so ϕ is well-defined. Let $m = n$, then $a^m = a^n$, and so ϕ is 1-1. The onto-ness is clear. Also, $\phi(a^h a^k) = \phi(a^{h+k}) = h + k = \phi(a^h) + \phi(a^k)$ for $a^h, a^k \in G$, so ϕ is a binary structure (group) homomorphism. Therefore, ϕ is an isomorphism.

(b) Assume that $|G| = n$. Then there exists $h, k \in \mathbb{Z}$ with $h < k$ such that $a^h = a^k$. Then $a^{k-h} = 1$ with $k - h \in \mathbb{N}$. Let $m := \min\{i \in \mathbb{N} \mid a^i = 1\}$. Similar to the proof of the part (a), we have that $G = \{a^k \mid k = 0, \ldots, m-1\}$. Suppose without loss of generality that there exist $i, j \in \mathbb{Z}$ with $0 \leqslant i < j \leqslant m-1$ such that $a^i = a^j$. Then $a^{j-i} = 1$, contradicting the definition of m and the fact that $j - i \in \{1, \ldots, m-1\}$. Thus, the elements $a^0, a^1, \ldots, a^{m-1}$ are all distinct, and so

$$G = \{a^0, a^1, \ldots, a^{m-1}\}.$$

Since $|G| = n$, we have that $m = n$. Define

$$\begin{aligned} \psi : G &\longrightarrow Z_n \\ a^i &\longmapsto i. \end{aligned}$$

Then ψ is well-defined. The 1-1ness and onto-ness are clear. Let $a^i, a^j \in G$. Then $i + j = nq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leqslant r \leqslant m-1$. Hence $i +_n j = r$ and $a^{i+j} = a^{nq+r} = (a^n)^q a^r = 1^q a^r = a^r$, and so

$$\psi(a^i a^j) = \psi(a^{i+j}) = \psi(a^r) = r = i +_n j = \psi(a^i) +_n \psi(a^j).$$

Therefore, ψ is a binary structure (group) homomorphism, and thus ψ is an isomorphism. □

Corollary 1.84. Let G be a group. If $a \in G$ such that $|a| < \infty$, then

$$|a| = \min\{m \in \mathbb{N} \mid a^m = 1\}.$$

Proof. In the proof of Theorem 1.83(b), take G to be $H := \langle a \rangle$, to get that $H = \{a^0, \ldots, a^{m-1}\}$, where $m = \min\{i \in \mathbb{N} \mid a^i = 1\}$. Then

$$|a| = |\langle a \rangle| = |H| = \left|\{a^0, \ldots, a^{m-1}\}\right| = m = \min\{m \in \mathbb{N} \mid a^m = 1\}.$$ □

1.8 Cyclic subgroups of finite order

Proposition 1.85. Let G be a group, $a \in G$, and $n \in \mathbb{Z}$. Then $a^n = 1$ if and only if $|a| \mid n$.

Proof. $\Longrightarrow$ By the division algorithm, we have that $\langle a \rangle = \{a^k \mid k = 0, \ldots, |n| - 1\}$. Then $|a| = |\langle a \rangle| < \infty$. Let $m := |a| = \min\{m \in \mathbb{N} \mid a^m = 1\}$ by Corollary 1.84. Then $a^m = 1$. Write $n = mq + r$ with $q, r \in \mathbb{Z}$ such that $0 \leqslant r < m$. Then $1 = a^n = a^{mq+r} = a^r$. By the definition of m and the fact that $r \in \{0, \ldots, m-1\}$, we have that $r = 0$. Hence $n = mq = |a|q$, and so $|a| \mid n$.

$\Longleftarrow$ is straightforward. □

Theorem 1.86. *Let G be a group and $a \in G$. If $|a| = n$, then for $m \in \mathbb{Z}$, $|a^m| = \frac{n}{\gcd(m,n)}$.*

Proof. Since $(a^m)^{\frac{n}{\gcd(m,n)}} = a^{\frac{nm}{\gcd(m,n)}} = (a^n)^{\frac{m}{\gcd(m,n)}} = 1$, we have that $|a^m| \mid \frac{n}{\gcd(m,n)}$ by Proposition 1.85. On the other hand, Since $a^{m|a^m|} = (a^m)^{|a^m|} = 1$, we have that $n \mid (m|a^m|)$ by Proposition 1.85. Hence $\frac{n}{\gcd(m,n)} \mid \frac{m|a^m|}{\gcd(m,n)}$. Since $\gcd(\frac{n}{\gcd(m,n)}, \frac{m}{\gcd(m,n)}) = 1$, we have that $\frac{n}{\gcd(m,n)} \mid |a^m|$ by Theorem 1.80. Thus, $|a^m| = \frac{n}{\gcd(m,n)}$. □

Corollary 1.87. Let G be a group and $a \in G$. If $|a| = n$, then for $m \in \mathbb{Z}$, $\langle a \rangle = \langle a^m \rangle$ if and only if $\gcd(m, n) = 1$.

Proof. Since $\langle a^m \rangle \leqslant \langle a \rangle$, we have that

$$\begin{aligned} \langle a \rangle = \langle a^m \rangle &\Longleftrightarrow |\langle a \rangle| = |\langle a^m \rangle| \\ &\Longleftrightarrow |a| = |a^m| \\ &\Longleftrightarrow n = \frac{n}{\gcd(m,n)} \\ &\Longleftrightarrow \gcd(m,n) = 1, \end{aligned}$$

where the last to the third equivalence follows from Theorem 1.86. □

Example 1.88. Let $n \in \mathbb{N}$.

(a) $Z_n = \langle m \rangle$ if and only if $m \in \{0, \ldots, n-1\}$ is such that $\gcd(n, m) = 1$. (In particular, for $n \geqslant 2$, $Z_n = \langle 1 \rangle = \langle n - 1 \rangle$. This is consistent with Example 1.65.) For $n \geqslant 2$, by Corollary 1.87, there are $\varphi(n)$ such m's, where

$$\begin{aligned} \varphi(n) &= |\{0 \leqslant m \leqslant n-1 \mid \gcd(m,n) = 1\}| \\ &= |\{1 \leqslant m \leqslant n \mid \gcd(m,n) = 1\}| \end{aligned}$$

is called the *Euler's ϕ function*. When $n \in \mathbb{N}$,

$$\varphi(n) = |\{1 \leqslant m \leqslant n \mid \gcd(m,n) = 1\}|.$$

(b) $U_n = \langle \zeta^m \rangle$ if and only if $m \in \mathbb{Z}$ is such that $\gcd(m, n) = 1$.

Remark. Let $n \in \mathbb{N}$. Define

$$Z_n^\times = \{m \in Z_n \mid m \text{ has a } \cdot \text{ inverse modulo } n\}.$$

Then $\langle Z_n^\times, \cdot \rangle$ is a group for $n \in \mathbb{Z}_{\geqslant 2}$. Let $a \in \{1, \ldots, n-1\}$. Then

$$\begin{aligned} a \in Z_n^\times &\iff \exists b \in Z_n^\times \text{ s.t } ab \equiv 1 \pmod{n} \\ &\iff \exists b, k \in \mathbb{Z} \text{ s.t } ab + nk = 1 \\ &\iff \gcd(a, n) = 1. \end{aligned}$$

Note that if $ab + nk = 1$ with $b, k \in \mathbb{Z}$, then $ab \equiv 1 \pmod{n}$, write $b = nq + r$ such that $q, r \in \mathbb{Z}$ and $0 \leqslant r \leqslant n-1$, then $ar = a(b - nq) = ab - naq \equiv 1 \pmod{n}$, thus, there exists $r \in Z_n^\times$ such that $ar \equiv 1 \pmod{n}$.

Therefore, for $n \geqslant 2$,

$$\left|Z_n^\times\right| = \varphi(n).$$

Example 1.89. Note that $Z_{12} = \langle 1 \rangle$ with $|1| = 12$. Let $a := 1$.

$$\begin{aligned} &\text{For } ma \in Z_{12}, \langle ma \rangle = \langle a \rangle \text{ if and only if } \gcd(m, |a|) = 1 \\ \iff &\text{For } m \in Z_{12}, \langle m \rangle = \langle 1 \rangle \text{ if and only if } \gcd(m, 12) = 1. \end{aligned}$$

Such m's are $1, 5, 7, 11$, and so

$$\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = Z_{12}.$$

Starting with $b := 2$, where $|b| = |2| = |2a| = \frac{12}{\gcd(2,12)} = 6$,

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}.$$

We characterize all subgroups of $\langle 2 \rangle$.

$$\begin{aligned} &\text{For } mb \in \{0, 2, 4, 6, 8, 10\} = \langle b \rangle,\ \langle mb \rangle = \langle b \rangle \text{ if and only if } \gcd(m, |b|) = 1 \\ \iff &\text{For } 2m \in \{0, 2, 4, 6, 8, 10\} = \langle 2 \rangle,\ \langle 2m \rangle = \langle 2 \rangle \text{ if and only if } \gcd(m, 6) = 1 \\ \iff &\text{For } m \in \{0, 1, 2, 3, 4, 5\} = \langle 2 \rangle,\ \langle 2m \rangle = \langle 2 \rangle \text{ if and only if } \gcd(m, 6) = 1. \end{aligned}$$

Such m's are $1, 5$, and so

$$\langle 10 \rangle = \langle 5b \rangle = \langle b \rangle = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$$

Similarly, with $c := 4$, where $|c| = |4| = |4a| = \frac{12}{\gcd(4,12)} = 3$, we have that

$$\langle 8 \rangle = \langle 2c \rangle = \langle c \rangle = \langle 4 \rangle = \{0, 4, 8\},$$

for $d := 6$, where $|d| = |6| = |6a| = \frac{12}{\gcd(6,12)} = 2$, we have that

$$\langle 6 \rangle = \{0, 6\}.$$

Thus, we find all "descendants" of $\langle 2 \rangle$. For $e := 3$, where $|e| = |3| = |3a| = \frac{12}{\gcd(3,12)} = 4$, we have that

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

The subgroup diagram for these subgroups of Z_{12} is given in the following:

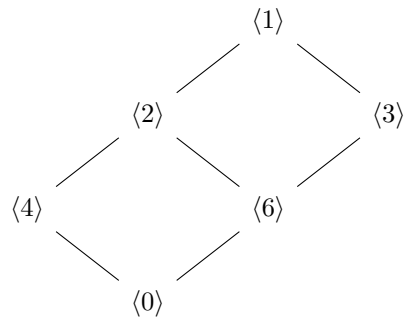


Figure 1.4

Proposition 1.90. Let $G = \langle a \rangle$ be a cyclic group with $|a| = n$. For $m \in \mathbb{N}$ such that $m \mid n$, there is a unique subgroup $H \leqslant G$ of order m. This subgroup is $H = \langle a^{n/m} \rangle$.

Proof. By Theorem 1.86, $\left|\langle a^{n/m} \rangle\right| = \left|a^{n/m}\right| = \frac{n}{\gcd(n/m,n)} = \frac{n}{n/m} = m$. Let $H \leqslant G$ such that $|H| = m$. Then $H = \langle a^i \rangle$ for some $i \in \mathbb{Z}$ (e.g, $i = \min\{j \in \mathbb{N} \mid a^j \in H\}$ by the proof of Theorem 1.72). Then $m = |H| = \left|a^i\right| = \frac{n}{\gcd(i,n)}$ by Theorem 1.86, so $\frac{n}{m} = \gcd(i,n)$, and thus $\frac{n}{m} \mid i$. Hence $a^i \in \langle a^{n/m} \rangle$, and so $H \leqslant \langle a^{n/m} \rangle$. Also, $|H| = m = \left|\langle a^{n/m} \rangle\right|$, so $H = \langle a^{n/m} \rangle$. □

Theorem 1.91. *Let $G = \langle a \rangle$ be a cyclic group with $|a| = n$. Then $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s,n) = \gcd(t,n)$.*

Proof. Note that

$$\begin{aligned} \langle a^s \rangle = \langle a^t \rangle &\iff |a^s| = \left|a^t\right| \\ &\iff \frac{n}{\gcd(s,n)} = \frac{n}{\gcd(t,n)} \\ &\iff \gcd(s,n) = \gcd(t,n), \end{aligned}$$

where the first equivalence follows from proposition 1.90 and the second equivalence follows from Theorem 1.86. □

Example 1.92. In Example 1.89, with $2 = 2a$ and $10 = 10a$, we have that $\gcd(2,12) = 2 = \gcd(10,12)$, and so $\langle 2 \rangle = \langle 2a \rangle = \langle 10a \rangle = \langle 10 \rangle$.

Chapter 2

Permutations, Cosets and Direct Product

2.1 Permutations and Dihedral groups

Let A be a nonempty set.

Definition 2.1. A permutation of A is a bijective function $\phi : A \to A$. Define the set S_A by

$$S_A := \{\text{permutations of } A\}.$$

Proposition 2.2. $(S_A, \circ)$ is a group.

Proof. Let $\sigma, \tau \in S_A$. Then $\sigma : A \to A$ and $\tau : A \to A$ are functions, and so we can write $\sigma\tau := \sigma \circ \tau$ as $A \xrightarrow{\tau} A \xrightarrow{\sigma} A$. Since compositions of bijective functions are bijective, we have that $\sigma \circ \tau \in S_A$. Hence $(S_A, \circ)$ is a binary structure. Note that the function composition is associative. Let $\mathrm{id}_A : A \to A$ be the identity map. Then id_A acts as the identity element of S_A. The function inverse σ^{-1} serves as inverse of σ under $\circ$ since $\sigma \circ \sigma^{-1} = \mathrm{id}_A = \sigma^{-1} \circ \sigma$. □

Definition 2.3. We call the permutation composition $\circ$ in S_A the permutation multiplication.

Definition 2.4. S_A is called the symmetric group on A. In particular, when $n \in \mathbb{N}$ and $A = \{1, \ldots, n\}$, the symmetric group on A is denoted by S_n, the symmetric group of degree n.

Proposition 2.5. $|S_n| = n! = n(n-1)\cdots(2)(1)$.

Proof. Let $\sigma \in S_n$. We can define $\sigma(1) = i$ for $i = 1, \ldots, n$ (n choices), then $\sigma(2) \in \{1, \ldots, n\} \setminus \{i\}$ ($n-1$ choices). In general, $\sigma(i)$ has $n - i + 1$ choices for $i = 1, \ldots, n$. Thus, there are $n(n-1)\cdots(n-(n-1)+1)(n-n+1) = n(n-1)\cdots(2)(1) = n!$ elements in S_n. □

Notation 2.6. Let $A = \{1, 2, 3, 4, 5\}$. For $\sigma \in S_A$ such that $\sigma(1) = 4$, $\sigma(2) = 2$, $\sigma(3) = 5$, $\sigma(4) = 3$, and $\sigma(5) = 1$, we use

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

to denote it. Let

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

Then

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

For example, multiplying in right-to-left order,

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 5.$$

Proposition 2.7. If $|A| = |B|$, then $S_A \cong S_B$.

Proof. Since $|A| = |B|$, there exists a bijection $f : A \to B$. Define a map ϕ by

$$\begin{aligned} \phi : S_A &\longrightarrow S_B \\ \sigma &\longmapsto f \circ \sigma \circ f^{-1}. \end{aligned}$$

For $\sigma \in S_A$, since $B \xrightarrow{f^{-1}} A \xrightarrow{\sigma} A \xrightarrow{f} B$ is a composition of bijective functions, we have that $f \circ \sigma \circ f^{-1} : B \to B$ is a bijection and then a permutation of B. So ϕ is well-defined. Define a map $\phi^{-1} : S_B \to S_A$ by

$$\begin{aligned} \phi^{-1} : S_B &\longrightarrow S_A \\ \tau &\longmapsto f^{-1} \circ \tau \circ f. \end{aligned}$$

Note that

$$\begin{aligned} \phi \circ \phi^{-1}(\tau) = \phi(\phi^{-1}(\tau)) = \phi(f^{-1} \circ \tau \circ f) = f \circ (f^{-1} \circ \tau \circ f) \circ f^{-1} = \tau, \forall \tau \in S_B, \\ \phi^{-1} \circ \phi(\sigma) = \phi^{-1}(\phi(\sigma)) = \phi^{-1}(f \circ \sigma \circ f^{-1}) = f^{-1} \circ (f \circ \sigma \circ f^{-1}) \circ f = \sigma, \forall \sigma \in S_A, \end{aligned}$$

so that $\phi \circ \phi^{-1} = \mathrm{id}_{S_B}$ and $\phi^{-1} \circ \phi = \mathrm{id}_{S_A}$. Hence ϕ is bijective. Also, ϕ is a binary structure (group) homomorphism since

$$\phi(\sigma\tau) = f \circ (\sigma\tau) \circ f^{-1} = (f \circ \sigma \circ f^{-1})(f \circ \tau \circ f^{-1}) = \phi(\sigma)\phi(\tau), \forall \sigma, \tau \in S_A.$$

Thus, ϕ is an isomorphism. □

Example 2.8. For $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$ and the function $f : A \to B$ defined as $f(1) = a$, $f(2) = b$, and $f(3) = c$, ϕ maps

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ into } \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = f \circ \sigma \circ f^{-1} =: \tilde{\sigma},$$

where, for example, $\tilde{\sigma}(a) = f \circ \sigma \circ f^{-1}(a) = f \circ \sigma(1) = f(3) = c$. Thus, any map in S_A becomes a map in B after renaming the elements of A by elements in B under f. Therefore, we can take S_n to be a prototype for the symmetric group of finite a set of n elements.

Theorem 2.9. *S_n is not abelian for $n \in \mathbb{Z}^{\geqslant 3}$.*

Proof. Since

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

but

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

we have that S_3 is not abelian. Define a map

$$\begin{gathered}\phi : S_3 \longrightarrow S_n\\ \begin{pmatrix}1&2&3\\m_1&m_2&m_3\end{pmatrix}\longmapsto\begin{pmatrix}1&2&3&4&\cdots&n\\m_1&m_2&m_3&4&\cdots&n\end{pmatrix}\end{gathered}$$

Let

$$\begin{pmatrix}1&2&3\\m_1&m_2&m_3\end{pmatrix},\ \begin{pmatrix}1&2&3\\k_1&k_2&k_3\end{pmatrix}\in S_3$$

be such that

$$\begin{pmatrix}1&2&3&4&\cdots&n\\m_1&m_2&m_3&4&\cdots&n\end{pmatrix}=\begin{pmatrix}1&2&3&4&\cdots&n\\k_1&k_2&k_3&4&\cdots&n\end{pmatrix}.$$

Then $m_1 = k_1$, $m_2 = k_2$ and $m_3 = k_3$, and so

$$\begin{pmatrix}1&2&3\\m_1&m_2&m_3\end{pmatrix}=\begin{pmatrix}1&2&3\\k_1&k_2&k_3\end{pmatrix}.$$

This proves that ϕ is 1-1. Let

$$\begin{pmatrix}1&2&3\\m_1&m_2&m_3\end{pmatrix},\ \begin{pmatrix}1&2&3\\k_1&k_2&k_3\end{pmatrix}\in S_3.$$

Assume that

$$\begin{pmatrix}1&2&3\\m_1&m_2&m_3\end{pmatrix}\begin{pmatrix}1&2&3\\k_1&k_2&k_3\end{pmatrix}=\begin{pmatrix}1&2&3\\x_1&x_2&x_2\end{pmatrix},$$

where x_1, x_2, x_3 are determined by m_1, m_2, m_3 and k_1, k_2, k_3. Then

$$\begin{aligned}\phi\left(\begin{pmatrix}1&2&3\\m_1&m_2&m_3\end{pmatrix}\begin{pmatrix}1&2&3\\k_1&k_2&k_3\end{pmatrix}\right)&=\phi\left(\begin{pmatrix}1&2&3\\x_1&x_2&x_3\end{pmatrix}\right)\\&=\begin{pmatrix}1&2&3&4&\cdots&n\\x_1&x_2&x_3&4&\cdots&n\end{pmatrix}\\&=\begin{pmatrix}1&2&3&4&\cdots&n\\k_1&k_2&k_3&4&\cdots&n\end{pmatrix}\begin{pmatrix}1&2&3&4&\cdots&n\\x_1&x_2&x_3&4&\cdots&n\end{pmatrix}\\&=\phi\begin{pmatrix}1&2&3\\m_1&m_2&m_3\end{pmatrix}\phi\begin{pmatrix}1&2&3\\k_1&k_2&k_3\end{pmatrix}.\end{aligned}$$

Thus, $\phi : S_3 \to S_n$ is an injective binary structure homomorphism. Also, restricting the codomain of ϕ we have that $S_3 \to \mathrm{Im}(\varphi)$ is onto, so $S_3 \cong \mathrm{Im}(\varphi)$. Since S_3 is not abelian and the binary structure isomorphism preserves the commutativity, we have that the permutation multiplication on $\phi(S_3)$ is not commutative. Therefore, S_n is not abelian as $\phi(S_3) \subseteq S_n$. □

Remark. We utilized the fact that if ϕ is a binary structure homomorphism, then $\mathrm{Im}(\phi)$ is a binary structure. In fact, we will prove soon that $\mathrm{Im}(\phi) \leqslant S_n$, so that $S_3 \to \mathrm{Im}(\varphi)$ is a group isomorphism. Thus, we regard S_3 a subset (subgroup) of S_n. For comparison, we regard $\mathbb{R}$ a subset (subfield) of $\mathbb{R}^2$ since $\mathbb{R}$ is isomorphic to any line in the plane $\mathbb{R}^2$: for $k, b \in \mathbb{R}$,

$$\begin{aligned} \varphi : \mathbb{R} &\longrightarrow \mathbb{R}^2, \\ r &\longmapsto (r, kr + b), \end{aligned}$$

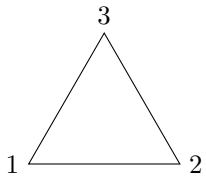
where $\mathrm{Im}(\varphi) \cong \mathbb{R}$ is the line $y = kx + b$ in $\mathbb{R}^2$, and for $c \in \mathbb{R}$,

$$\begin{aligned} \psi : \mathbb{R} &\longrightarrow \mathbb{R}^2, \\ r &\longmapsto (c, r), \end{aligned}$$

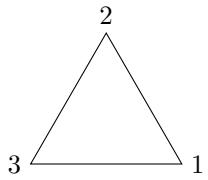
where $\mathrm{Im}(\psi) \cong \mathbb{R}$ is the line $x = c$ in $\mathbb{R}^2$.

Notation 2.10. We use the following to denote elements of S_3.

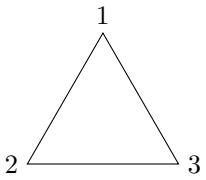
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



rotatation of 0 radians counterclockwise



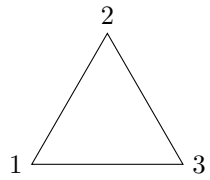
rotatation of $\pi/3$ radians counterclockwise



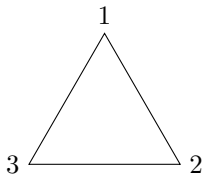
rotatation of $2\pi/3$ counterclockwise

and

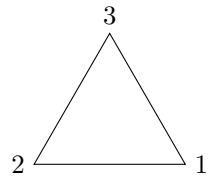
$$\mu_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



reflection on the line through 1 and the center of the 3-gon



reflection on the line through 2 and the center of the 3-gon



reflection on the line through 3 and the center of the 3-gon.

Definition 2.11. For $n \in \mathbb{Z}^{\geqslant 3}$, the n^{th} dihedral group D_n, is the set of symmetries of a regular n-gon, which includes rotations and reflections.

Example 2.12. Using ρ_i for rotations, μ_i for mirror images in perpendicular bisectors of sides, and δ_i for diagonal flips.

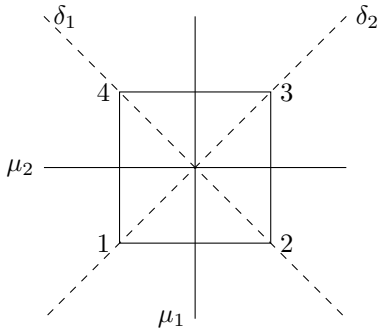


Figure 2.1

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

Fact 2.13. From for example the table for D_4, we get the subgroup diagram of D_4.

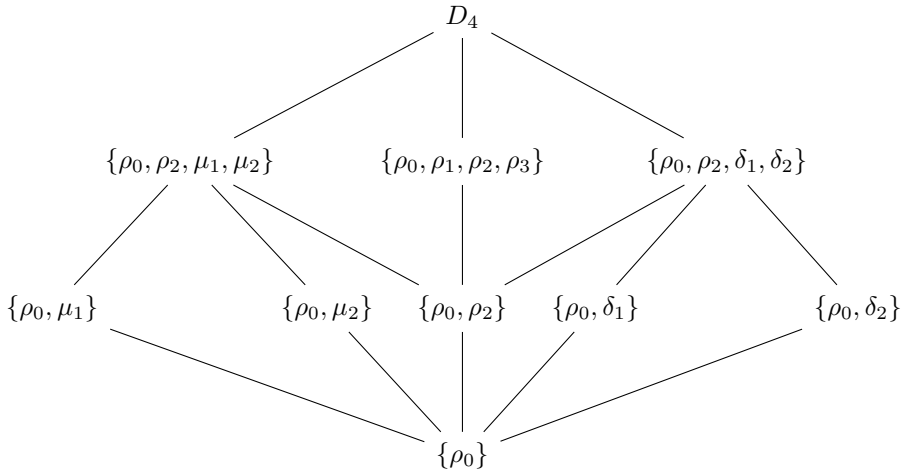


Figure 2.2

2.2 Cayley's Theorem

Lemma 2.14. Let G and G' be groups and $\phi : G \to G'$ 1-1 such that $\phi(xy) = \phi(x)\phi(y)$. Then $\mathrm{Im}(\phi) \leqslant G'$ and $G \cong \mathrm{Im}(\phi)$.

Proof. Let $x', y' \in \mathrm{Im}(\phi)$. Then there exist $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. Then $x'y' = \phi(x)\phi(y) = \phi(xy) \in \mathrm{Im}(\phi)$. So $\mathrm{Im}(\phi)$ is closed under the operation $\cdot$ of G'. Let e' be the identity element of G'. Then $e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e)$. Cancellation in G' shows that $e' = \phi(e) \in \mathrm{Im}(\phi)$. Since $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1})$, we have that $x'^{-1} = \phi(x^{-1}) \in \mathrm{Im}(\phi)$. Thus, $\mathrm{Im}(\phi) \leqslant G'$. Restricting the codomain of φ, we get a bijection $\varphi : G \to \mathrm{Im}(\phi)$ because ϕ is 1-1. Also, φ is a binary structure (group) homomorphism since $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. □

Theorem 2.15 (Cayley's Theorem)**.** *If G is a group, then G is isomorphic to a group of permutation.*

Proof. Let $x \in G$. Define $\lambda_x : G \to G$ by $g \mapsto xg$. Similar to the proof of Proposition 1.39, λ_x is bijective and so $\lambda_x \in S_G$. Define a map ϕ by

$$\begin{aligned} \phi : G &\longrightarrow S_G \\ x &\longmapsto \lambda_x. \end{aligned}$$

Let $x, y \in G$ be such that $\phi(x) = \phi(y)$. Then $\lambda_x = \lambda_y$, and so $x = xe = \lambda_x(e) = \lambda_y(e) = ye = y$. Hence ϕ is 1-1. Let $x, y \in G$. Then

$$\phi(xy)(g) = \lambda_{xy}(g) = (xy)g = x(yg) = \lambda_x(yg) = \lambda_x(\lambda_y g) = \lambda_x\lambda_y(g) = \phi(x)\phi(y)(g), \forall\, g \in G,$$

and so $\phi(xy) = \phi(x)(y)$. Thus, by Lemma 2.14,

$$G \cong \mathrm{Im}(\phi) = \{\lambda_x \mid x \in G\} \leqslant S_G.$$ □

Definition 2.16. The map $G \to S_G$ by $x \mapsto \lambda_x$ is the left regular representation of G. The map $G \to S_G$ by $x \mapsto \rho_x$ is the right regular representation of G, where $\rho_x : G \to G$ is given by $g \mapsto gx$.

Example 2.17. Given a group table

Table 2.1

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

we have that

$$\lambda_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}, \qquad \lambda_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}, \qquad \lambda_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}.$$

The group table of the group $\{\lambda_e, \lambda_a, \lambda_b\}$ is

Table 2.2

	λ_e	λ_a	λ_b
λ_e	λ_e	λ_a	λ_b
λ_a	λ_a	λ_b	λ_e
λ_b	λ_b	λ_e	λ_a

The table for this representation is just like the original table with x renamed λ_x.

2.3 Obits, Cycle and Alternating Groups

Definition 2.18 (equivalence relation **(1)**)**.** Let $\sigma \in S_A$. For $a, b \in A$, we write $a \sim_\sigma b$ if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$.

Remark. The equivalence relation **(1)** is an indeed an equivalence relation. Let $a, b, c \in A$.

(Reflexive) Clearly $a \sim_\sigma a$ since $a = \mathrm{id}_A(a) = \sigma^0(a)$ and $\mathrm{id}_A \in S_A$.

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

(Transitive) Assume that $a \sim_\sigma b$ and $b \sim_\sigma c$, then $b = \sigma^n(a)$ and $c = \sigma^m(b)$ for some $n, m \in \mathbb{Z}$. Note that $c = \sigma^m(b) = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a)$ with $m + n \in \mathbb{Z}$, so $a \sim_\sigma c$.

Definition 2.19. Let $\sigma \in S_A$. The equivalence classes in A determined by the equivalence relation **(1)** are the orbits of σ.

Example 2.20. The orbits of id_A are the one-element subsets of A, i.e., for any $a \in A$, the cell $\overline{a} = \{a\}$ is an orbit.

Example 2.21. Consider the permutation

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

Note that

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

To find the orbit $\overline{1}$, we apply σ repeatedly, obtaining symbolically

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma^{-1}} 6 \xrightarrow{\sigma^{-1}} 3 \xrightarrow{\sigma^{-1}} 1.$$

Hence $\overline{1} = \{1, 3, 6\} = \overline{3} = \overline{6}$. Similarly, $\overline{2} = \{2, 8\} = \overline{8}$ and $\overline{4} = \{4, 5, 7\} = \overline{5} = \overline{7}$.

$$2 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 2 \xrightarrow{\sigma^{-1}} 8 \xrightarrow{\sigma^{-1}} 2$$

$$4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 4 \xrightarrow{\sigma^{-1}} 5 \xrightarrow{\sigma^{-1}} 7 \xrightarrow{\sigma^{-1}} 4.$$

Thus, the complete list of orbits of σ is

$$\{1,3,6\},\ \{2,8\},\ \{4,5,7\}.$$

Definition 2.22. For an orbit $\bar{i}$ of $\sigma \in S_n$, defines

$$\mu_i^\sigma(x) = \begin{cases} \sigma(x) & \text{if } x \in \bar{i}, \\ x & \text{otherwise.} \end{cases}$$

Example 2.23. In Example 2.21, the orbit $\bar{1}$ corresponds to the permutation

$$\mu_1^\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix} \in S_8.$$

The complete list of orbits of μ_1^σ is

$$\{1,3,6\},\ \{2\},\ \{4\},\ \{5\},\ \{7\},\ \{8\}.$$

Similarly, the complete list of orbits of μ_2^σ and μ_4^σ are, respectively,

$$\{2,8\},\ \{1\},\ \{3\},\ \{4\},\ \{5\},\ \{6\},\ \{7\}.$$

and

$$\{4,5,7\},\ \{1\},\ \{2\},\ \{3\},\ \{6\},\ \{8\}.$$

Definition 2.24. $\sigma \in S_n$ is a cycle if it has at most one orbit containing more than one element. The length of a cycle is the number of elements in its largest orbit.

Example 2.25. In Example 2.23, μ_1^σ, μ_2^σ, and μ_4^σ are cycles.

Definition 2.26 (cyclic notation)**.** For a cycle $\sigma \in S_n$, we use $(a_1\ a_2\ \cdots\ a_{m-1}\ a_m)$ to denote the permutation which sends a_i to a_{i+1} for $i = 1, \ldots, m-1$ and sends a_m to a_1, while fixing any $b \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_m\}$. In particular, we use (1) to denote the $\mathrm{id}_{\{1,\ldots,n\}}$.

Example 2.27.

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

Observe that with different starting numbers,

$$(1\ 3\ 5\ 4) = (3\ 5\ 4\ 1) = (5\ 4\ 3\ 1) = (4\ 1\ 3\ 5).$$

Remark. Use the cyclic notation, it is easy to see that the map ϕ in the proof of Theorem 2.9 is an injective homomorphism:

$$\begin{aligned} \phi : S_3 &\hookrightarrow S_n \\ (1) &\longrightarrow (1) \\ (1,2) &\longrightarrow (1,2) \\ (1,3) &\longrightarrow (1,3) \\ (2,3) &\longrightarrow (2,3) \\ (1,2,3) &\longrightarrow (1,2,3) \\ (1,3,2) &\longrightarrow (1,3,2). \end{aligned}$$

Definition 2.28. Two cycles of S_n are called disjoint if they have no numbers in common.

Example 2.29. In Example 2.21,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\ 3\ 6)(2\ 8)(4\ 7\ 5) = \mu_1^\sigma \mu_2^\sigma \mu_4^\sigma.$$

Reading in right-to-left order, 4 is sent to 7 (7 is sent to 7, and 7 is sent to 7).

Theorem 2.30. *Each $\sigma \in S_n$ is a product of disjoint cycles. The representation is unique up to the order of the factors.*

Proof. Let $\bar{a}_1, \cdots, \bar{a}_r$ be the orbits of σ. Then $\sigma = \mu_{a_1}^\sigma \cdots \mu_{a_r}^\sigma$. Since the orbits (equivalence classes) $\bar{a}_1, \cdots, \bar{a}_r$ forms a partition of $\{1, \ldots, n\}$, we have that the cycles $\mu_{a_1}^\sigma, \ldots, \mu_{a_r}^\sigma$ are disjoint. The second statement is straightforward. □

Example 2.31.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 6)(2\ 5\ 3) \underbrace{= (2\ 5\ 3)(1\ 6)}_{\text{rarely used}}.$$

Example 2.32 (cycles are not disjoint)**.**

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

and

$$(2\ 1\ 5)(1\ 4\ 5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} \neq (1\ 4\ 5\ 6)(2\ 1\ 5).$$

Neither of these permutations is a cycle.

Definition 2.33. A cycle of length 2 in S_n is a transposition.

Proposition 2.34. Let $n \geqslant 2$. Then any $\sigma \in S_n$ is a product of transpositions.

Proof. For $(1) \in S_n$, $(1) = (1\ 2)(2\ 1)$. Let $(a_1\ a_2\ \cdots\ a_m) \in S_n$. Then

$$(a_1\ a_2\ \cdots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1\ a_3)\ (a_1\ a_2).$$

For a_1, it is sent to a_2 by the last transposition, and a_2 is fixed by the remaining $m-2$ transpositions, so a_1 is sent to a_2. For a_2, it is sent to a_1 by the last transposition, then a_1 is sent to a_3 by the second to last transposition, and a_3 is fixed by the remaining $m-3$ transpositions. Then the statement follows from induction. □

Remark. Naively, this corollary just states that any rearrangement of n objects can be achieved by successively interchanging pairs of them.

Example 2.35. We have that $\sigma := (1\ 6)(2\ 5\ 3) = (1\ 6)(2\ 3)(2\ 5)$ by the proof of Proposition 2.34.

Theorem 2.36. *Let $\sigma \in S_n$. If $\tau_1, \ldots, \tau_k, \gamma_1, \ldots, \gamma_\ell$ are transpositions in S_n such that $\tau_1 \ldots \tau_k = \sigma = \gamma_1 \cdots \gamma_\ell$, then $(-1)^k = (-1)^\ell$, i.e., the parity of the number of factors of any σ is well-defined.*

Proof. Refer to the proof 1 from textbook. □

Definition 2.37. A permutation of a finite set is even or odd according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions, respectively.

Example 2.38. Since

$$\sigma := (1\ 4\ 5\ 6)(2\ 1\ 5) = (1\ 6)(1\ 5)(1\ 4)(2\ 5)(2\ 1),$$

we have that σ is an odd permutation.

Definition 2.39. Let $n \in \mathbb{Z}_{\geqslant 2}$. Let A_n be the set of even permutations in S_n and B_n the set of odd permutations.

Proposition 2.40. Let $n \in \mathbb{Z}_{\geqslant 2}$. $|A_n| = |B_n| = n!/2$.

Proof. Let $\tau = (1\ 2) \in S_n$. Define a function $\lambda_\tau|_{A_n,B_n}$ from $\lambda_\tau : S_n \to S_n$ by

$$\begin{aligned} \lambda_\tau|_{A_n \to B_n} : A_n &\longrightarrow B_n \\ \sigma &\longmapsto \tau\sigma. \end{aligned}$$

For $\sigma \in A_n$, σ can be expressed as a product of a even number of transpositions, then $\tau\sigma = (1\ 2)\sigma$ is add, so $\tau\sigma \in B_n$, and hence λ_τ is well-defined. We have that λ_τ is 1-1, so $\lambda_\tau|_{A_n,B_n}$ is 1-1. Let $\rho \in B_n$. Then $\tau^{-1}\rho = (1\ 2)\rho \in A_n$ and $\lambda_\tau|_{A_n,B_n}(\tau^{-1}\rho) = \tau(\tau^{-1}\rho) = \rho$. So $\lambda_\tau|_{A_n,B_n}$ is onto. Thus, $\lambda_\tau|_{A_n,B_n}$ is a bijection, and so $|A_n| = |B_n|$. Also, $A_n \sqcup B_n = S_n$, hence $|A_n| = |B_n| = |S_n|/2 = n!/2$. □

Lemma 2.41. Let

$$\sigma = \tau_1 \cdots \tau_k = (a_{1,1}\ a_{1,2}\ \cdots\ a_{1,t_1-1}\ a_{1,t_1}) \cdots (a_{k,1}\ a_{k,2}\ \cdots\ a_{k,t_k-1}\ a_{k,t_k}).$$

Then

$$\sigma^{-1} = \tau_k^{-1} \cdots \tau_1^{-1} = (a_{k,1}\ a_{k,t_k}\ \cdots\ a_{k,2}) \cdots (a_{1,1}\ a_{1,t_1}\ \cdots\ a_{1,2}).$$

Hence σ and σ^{-1} have the same parity.

Example 2.42. If $\sigma = (1\ 2\ 4\ 3\ )(6\ 7) = (1\ 3)(1\ 4)(1\ 2)(6\ 7)$, then

$$\sigma^{-1} = (6\ 7)^{-1}(1\ 2\ 4\ 3\ )^{-1} = (6\ 7)(1\ 3\ 4\ 2) = (1\ 3\ 4\ 2)(6\ 7) = (1\ 2)(1\ 4)(1\ 3)(6\ 7).$$

Theorem 2.43. *Let $n \geqslant 2$. Then $A_n \leqslant S_n$.*

Proof. Let $\sigma_1, \sigma_2 \in A_n$. Then $\sigma_1\sigma_2$ is even, and so $\sigma_1\sigma_2 \in A_n$. Since $\mathrm{id}_{\{1,\ldots,n\}} = (1\ 2)(1\ 2)$, $\mathrm{id}_{\{1,\ldots,n\}}$ is even, and then $\mathrm{id}_{\{1,\ldots,n\}} \in A_n$. Let $\sigma \in A_n$. Then $\sigma^{-1} \in A_n$ by Lemma 2.41. Hence $A_n \leqslant S_n$ by subgroup test. □

Definition 2.44. Let $n \geqslant 2$. A_n is the alternating group on n letters.

2.4 Cosets and the theorem of lagrange

Definition 2.45. Let $H \leqslant G$. Define the relation $\sim_L$ on G by $a \sim_L b$ if $a^{-1}b \in H$. Define the relation $\sim_R$ on G by $a \sim_R b$ if $ab^{-1} \in H$.

Theorem 2.46. *$\sim_L$ and $\sim_R$ are both equivalence relations on G.*

Proof. We prove that $\sim_L$ is an equivalence relation on G. Let $a, b, c \in G$.

(Relexive) We have that $a^{-1}a = e \in H$ since $H \leqslant G$. Hence $a \sim_L a$.

(Symmetric) Let $a \sim_L b$. Then $a^{-1}b \in H$. Then $b^{-1}a = (a^{-1}b)^{-1} \in H$ since $H \leqslant G$. Hence $b \sim_L a$.

(Transitive) Let $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$. Hence $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$ since $H \leqslant G$, and so $a \sim_L c$. □

Remark. Let $H \leqslant G$. The equivalence relation $\sim_L$ defines a partition of G, as described in Theorem 0.25. For $a \in G$,

$$\begin{aligned}
\bar{a} &= \{x \in G \mid a \sim_L x\} \\
&= \{x \in G \mid a^{-1}x \in H\} \\
&= \{x \in G \mid a^{-1}x = h \text{ for some } h \in H\} \\
&= \{x \in G \mid x = ah \text{ for some } h \in H\} \\
&= \{ah \mid h \in H\} \\
&=: aH.
\end{aligned}$$

Similarly, the equivalence relation $\sim_R$ defines a partition of G: for $a \in G$,

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

Theorem 2.47. *Let $H \leqslant G$. Then for $a \in G$, $|aH| = H = |Ha|$.*

Proof. We have a well-defined injective map

$$\begin{aligned}
\lambda_a|_H : H &\longrightarrow G \\
h &\longmapsto ah.
\end{aligned}$$

Since $\mathrm{Im}(\lambda_a|_H) = \{ah \mid h \in H\} = aH$, we have that $|H| = |aH|$. □

Remark. $aH \leqslant G$ if and only if $a = 1$ since only the cell $\bar{1} = H$ contains 1.

Definition 2.48. Let $H \leqslant G$. Let the subset $aH = \{ah \mid h \in H\}$ of G be the <u>left coset</u> of H containing a, and

$$G//H := \{aH \mid a \in G\}.$$

Let the subset $Ha = \{ha \mid h \in H\}$ of G be the <u>right coset</u> of H containing a, and

$$G\backslash\backslash H := \{Ha \mid a \in G\}.$$

Remark. Let $H \leqslant G$. Since $1H = H = H1$, H is always a left and right coset (containing 1).

If G is abelian, then $aH = Ha$ for any $a \in G$. So the partition of G into left cosets $G//H$ of H and the partition into right cosets $G\backslash\backslash H$ are the same.

Example 2.49. Recall Example 0.20. For $3\mathbb{Z} \leqslant \mathbb{Z}$, we have that $\mathbb{Z}//3\mathbb{Z} = \{3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$, and they form a partition of $\mathbb{Z}$ into left cosets of $3\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, we have that $\mathbb{Z}\backslash\backslash 3\mathbb{Z} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\} = \mathbb{Z}//3\mathbb{Z}$.

Let $n \in \mathbb{Z}_{\geqslant 2}$. Then $n\mathbb{Z} \leqslant \mathbb{Z}$, and $\mathbb{Z}//n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\}$ with

$$\begin{aligned}
\bar{a} &= \{x \in \mathbb{Z} \mid a \sim_L x\} \\
&= \{x \in \mathbb{Z} \mid a \sim_R x\} \\
&= \{x \in \mathbb{Z} \mid a + (-x) \in n\mathbb{Z}\} \\
&= \{x \in \mathbb{Z} \mid a - x \in n\mathbb{Z}\} \\
&= \{x \in \mathbb{Z} \mid n \mid (a-x)\} \\
&= \{x \in \mathbb{Z} \mid a \equiv x \pmod{n}\}.
\end{aligned}$$

Thus, the partition of $\mathbb{Z}$ into cosets of $n\mathbb{Z}$ is the partition of $\mathbb{Z}$ into residue class modulo n. For that reason, we often refer to the cells of this partition $\mathbb{Z}//n\mathbb{Z}$ as cosets modulo $n\mathbb{Z}$. We have that

$$\mathbb{Z}//n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}.$$

Example 2.50. The group Z_6 is abelian and $H := \{0, 3\} \leqslant Z_6$. Find $Z_6//H$. One coset is H itself. The coset containing 1 is $1 + \{0, 3\} = \{1, 4\}$. The coset containing 2 is $2 + \{0, 3\} = \{2, 5\}$. Note that $\bar{0} = H$, $\bar{1} = 1 + H$, and $\bar{2} = 2 + H$ are all cosets of H.

Remark. We will see a corollary, says that if G is abelian and $H \leqslant G$, then the cosets of H forms a group G/H under the binary operation $(aH)(bH) = (ab)H$ or $\bar{a}\bar{b} = \overline{ab}$. For example, $n\mathbb{Z} \leqslant \mathbb{Z}$ with $n \geqslant 2$, then the cosets of $n\mathbb{Z}$ form the group $\mathbb{Z}/n\mathbb{Z}$ under the operation $\bar{a} + \bar{b} = \overline{a+b}$.

Example 2.51. S_3 is not abelian. Let $H := \langle \mu_1 \rangle = \{\rho_0, \mu_1\} = \{(1), (2\ 3)\} \leqslant S_3$. Then

$$\rho_1 H = \{\rho_1\rho_0, \rho_1\mu_1\} = \{\rho_1, (1\ 2\ 3)(2\ 3)\} = \{\rho_1, (1\ 2)\} = \{\rho_1, \mu_3\},$$

$$\rho_2 H = \{\rho_2\rho_0, \rho_2\mu_1\} = \{\rho_2, (1\ 3\ 2)(2\ 3)\} = \{\rho_2, (1\ 3)\} = \{\rho_2, \mu_2\}.$$

All right cosets of H are H,

$$H\rho_1 = \{\rho_0\rho_1, \mu_1\rho_1\} = \{\rho_1, (2\ 3)(1\ 2\ 3)\} = \{\rho_1, (1\ 3)\} = \{\rho_1, \mu_2\} \neq \rho_1 H,$$

$$H\rho_2 = \{\rho_0\rho_2, \mu_1\rho_2\} = \{\rho_2, (2\ 3)(1\ 3\ 2)\} = \{\rho_2, (1\ 2)\} = \{\rho_2, \mu_3\} \neq \rho_2 H.$$

Consider the set of left cosets $S_3//H := \{H, \rho_1 H, \rho_2 H\} = \{\bar{1}, \overline{\rho_1}, \overline{\rho_2}\}$. We try to define a map

$$\begin{aligned}
\phi : S_3//H \times S_3//H &\longrightarrow S_3//H \\
(\bar{a}, \bar{b}) &\longmapsto \overline{ab}.
\end{aligned}$$

Note that

$$\overline{\rho_1}\overline{\rho_2} = \overline{\rho_1\rho_2} = (\rho_1\rho_2)H = \{\rho_1\rho_2\rho_0, \rho_1\rho_2\mu_1\} = \{(1\ 2\ 3)(1\ 3\ 2), (1\ 2\ 3)(1\ 3\ 2)(2\ 3)\} = \{(1), (2\ 3)\},$$
$$\overline{\mu_3}\overline{\mu_2} = \overline{\mu_3\mu_2} = (\mu_3\mu_2)H = \{\mu_3\mu_2\rho_0, \mu_3\mu_2\mu_1\} = \{(1\ 2)(1\ 3), (1\ 2)(1\ 3)(2\ 3)\} = \{(1\ 3\ 2), (1\ 3)\}.$$

Since $(\overline{\rho_1}, \overline{\rho_2}) = (\overline{\mu_3}, \overline{\mu_2})$ but $\overline{\rho_1\rho_2} \neq \overline{\mu_3\mu_2}$, we have that ϕ is not well-defined. Thus, $S_3//H$ is not a group under $\bar{a}\bar{b} = \overline{ab}$. An alternative proof for this result is from $S_3//H \neq S_3\backslash\backslash H$.

Theorem 2.52 (Lagrange's Theorem)**.** *Let $|G| < \infty$ and $H \leqslant G$. Then $|H| \,\big|\, |G|$.*

Proof. Since $|G| < \infty$, we have that $|G//H| < \infty$. Without loss of generality, assume that $G//H = \{a_1H, \ldots, a_rH\}$. Then $a_1H, \cdots, a_rH$ are mutually disjoint and their union is G. By Theorem 2.47, we have that

$$|G| = \sum_{i=1}^{r} |a_iH| = \sum_{i=1}^{r} |H| = r|H|.$$

Thus, $|H| \,\big|\, |G|$. □

Corollary 2.53. If G is a group of $|G| = p$ with p prime, then G is cyclic.

Proof. Let $a \in G \setminus \{1\}$. Then $\{1, a\} \subseteq \langle a \rangle$, and so $|\langle a \rangle| \geqslant 2$. Since $|a| \leqslant G$, we have that $|\langle a \rangle| \,\big|\, p$ by Theorem 2.52. Hence $|\langle a \rangle| = p = |G|$, and so $G = \langle a \rangle$. □

Corollary 2.54. If G is a group of $|G| = p$ with p prime, then $G \cong Z_p$.

Proof. It follows from Theorem 1.83(b) and Corollary 2.53. □

Remark. This says that there is only one group structure, up to isomorphism, of a given prime order p.

Corollary 2.55. Let $|G| < \infty$ and $a \in G$. Then $|a| \,\big|\, |G|$.

Proof. It follows from $|a| = |\langle a \rangle|$ and Theorem 2.52. □

Corollary 2.56. Let $|G| < \infty$ and $H \leqslant G$. Then

$$|G//H| = \frac{|G|}{|H|}.$$

Definition 2.57. Let $H \leqslant G$. Define the <u>index</u> $[G : H]$ of H in G by

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

Remark. $[G : H] = |G \backslash\backslash H|$.

Theorem 2.58. *Let $|G| < \infty$ and $H \leqslant G$. Then*

$$[G : H] = \frac{|G|}{|H|}.$$

Theorem 2.59. *Let $K \leqslant H \leqslant G$. Then*

$$[G : K] = [G : H][H : K].$$

Proof. The proof that $[G : H]$ and $[H : K]$ are finite is left as an exercise. □

2.5 Direct product and finitely generated abelian groups

Notation 2.60. The Cartesian product is denoted by either $S_1 \times \cdots \times S_n$ or by $\prod_{i=1}^n S_i$.

Theorem 2.61. *Let $G_1, \ldots, G_n$ be groups. Then $\prod_{i=1}^n G_i$ is a group under componentwise multiplication.*

Proof. Let $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \prod_{i=1}^n G_i$. Then for $i = 1, \ldots, n$, $a_i, b_i \in G_i$, and so $a_i b_i \in G_i$ since G_i is a group. Hence $(a_1, \ldots, a_n), (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) \in \prod_{i=1}^n G_i$.

The associative law in $\prod_{i=1}^n G_i$ follows from the associative law of $G_1, \ldots, G_n$. Check that $(e_1, \ldots, e_n)$ is the identity of $\prod_{i=1}^n G_i$ if e_i is the identity of G_i for $i = 1, \ldots, n$. Finally, the inverse of $(a_1, \ldots, a_n) \in \prod_{i=1}^n G_i$ is $(a_1^{-1}, \ldots, a_n^{-1})$. □

Remark. If each G_i is additive, then we often use $\bigoplus_{i=1}^n G_i$ or $G_1 \oplus \cdots \oplus G_n$ in place of $\prod_{i=1}^n G_i$.

Fact 2.62. Let $G_1, \ldots, G_n$ be groups. Then

$$\left| \prod_{i=1}^n G_i \right| = \prod_{i=1}^n |G_i|.$$

Theorem 2.63. *Let G, G' be groups. Then we have a group isomorphism*

$$\begin{aligned} G \times G' &\xrightarrow{\cong} G' \times G \\ (a, a') &\longmapsto (a', a). \end{aligned}$$

Theorem 2.64. *Let $G_1, \ldots, G_n$ be groups and $H_i \leqslant G_i$ for $i = 1, \ldots, n$. Then*

$$H_1 \times \cdots \times H_n \leqslant G_1 \times \cdots \times G_n.$$

Proof. By Theorem 2.61, $H_1 \times \cdots \times H_n$ is a group under $\cdot$. It is straightforward to see that $H_1 \times \cdots \times H_n \subseteq G_1 \times \cdots G_n$. By definition of the subgroups, $H_1 \times \cdots \times H_n \leqslant G_1 \times \cdots \times G_n$. □

Definition 2.65. Let $n \in \mathbb{Z}_{\geqslant 2}$, and $r_1, \ldots, r_n \in \mathbb{Z} \setminus \{0\}$.

(a) We say $b \in \mathbb{Z}$ is a common multiple of $r_1, \ldots, r_n$ if $r_i \mid b$ for $i = 1, \ldots, n$.

(b) The least common multiple of $r_1, \ldots, r_n$ is the smallest positive common multiples, denoted by $\operatorname{lcm}(r_1, \ldots, r_n)$.

Theorem 2.66. *Let $G_1, \ldots, G_n$ be groups. Let $(a_1, \ldots, a_n) \in \prod_{i=1}^n G_i$ be such that $|a_i| < \infty$ in G_i for $i = 1, \ldots, n$. Then*

$$|(a_1, \ldots, a_n)| = \operatorname{lcm}(|a_1|, \ldots, |a_n|).$$

Proof. For $i = 1, \ldots, n$, since $|a_i| \mid \operatorname{lcm}(|a_1|, \ldots, |a_n|)$, we have that $a_i^{\operatorname{lcm}(|a_1|, \ldots, |a_n|)} = 1$ by Proposition 1.85. Then

$$(a_1, \ldots, a_n)^{\operatorname{lcm}(|a_1|, \ldots, |a_n|)} = (a_1^{\operatorname{lcm}(|a_1|, \ldots, |a_n|)}, \ldots, a_n^{\operatorname{lcm}(|a_1|, \ldots, |a_n|)}) = (e_1, \ldots, e_n).$$

Hence $|(a_1, \ldots, a_n)| \leqslant \operatorname{lcm}(|a_1|, \ldots, |a_n|)$ by the minimality of $|(a_1, \ldots, a_n)|$.

Suppose that there is an $s \in \mathbb{N}$ with $s < \operatorname{lcm}(|a_1|, \ldots, |a_n|)$ such that $(a_1, \ldots, a_n)^s = (e_1, \ldots, e_n)$. Then $(a_1^s, \ldots, a_n^s) = (e_1, \ldots, e_n)$. Then for $i = 1, \ldots, n$, $|a_i| \mid s$ by Proposition 1.85. Hence $s \geqslant \operatorname{lcm}(|a_1|, \ldots, |a_n|)$, contradicting $s < \operatorname{lcm}(|a_1|, \ldots, |a_n|)$. Thus, $|(a_1, \ldots, a_n)| \geqslant \operatorname{lcm}(|a_1|, \ldots, |a_n|)$. □

Example 2.67. (a) The order of $(1,1)$ in the group $Z_2 \times Z_3$ is $\text{lcm}(2,3) = 2(3) = 6$ since the order of 1 in Z_2 is 2 and the order of 1 in Z_3 is 3, because $Z_2 = \langle 1 \rangle$ and $Z_3 = \langle 1 \rangle$.

(b) The order of $(1,1,1)$ in the group $Z_3 \times Z_4 \times Z_{35}$ is

$$\text{lcm}(|1|,|1|,|1|) = \text{lcm}(3,4,35) = 3(4)(35) = 420.$$

(c) The order of $(8,4,10)$ in the group $Z_{12} \times Z_{60} \times Z_{24}$ is

$$\text{lcm}(|8|,|4|,|10|) = \text{lcm}\left(\frac{12}{\gcd(8,12)}, \frac{60}{\gcd(4,60)}, \frac{24}{\gcd(10,24)}\right) = \text{lcm}(3,15,12) = 60.$$

by Theorem 1.86.

Theorem 2.68. *The group $Z_m \times Z_n \cong Z_{mn}$ if and only if $\gcd(m,n) = 1$.*

Proof. $\Longrightarrow$ Suppose that $\gcd(m,n) \neq 1$. Let $(a,b) \in Z_m \times Z_n$ with $a \in Z_m$ and $b \in Z_n$. Then $|a| \mid m$ and $|b| \mid n$ by Corollary 2.55. Then $\text{lcm}(m,n)(a,b) = (\text{lcm}(m,n)a, \text{lcm}(m,n)b) = (0,0)$ by Proposition 1.85. Sice $(0,0)$ is the identity of $Z_m \times Z_n$, we have that every element of $Z_m \times Z_n$ has order at most $\text{lcm}(m,n)$, but $\text{lcm}(m,n) < mn$. Thus, $Z_m \times Z_n$ is not cyclic, contradicting $Z_m \times Z_n \cong Z_{mn}$.

$\Longleftarrow$ Let $\gcd(m,n) = 1$. Then by Theorem 2.66, $|(1,1)| = \text{lcm}(|1|,|1|) = \text{lcm}(m,n) = mn$. So $Z_m \times Z_n = \langle (1,1) \rangle$ is cyclic. Thus, $Z_m \times Z_n \cong Z_{mn}$ by Theorem 1.83(b). □

Example 2.69. (a) $Z_2 \times Z_3 \cong Z_6$.

(b) $|Z_3 \times Z_3| = |Z_3| \times |Z_3| = 3(3) = 9$, and $Z_3 \times Z_3 \ncong Z_9$.

Corollary 2.70. The group $\prod_{i=1}^{n} Z_{m_i} \cong Z_{m_1 \cdots m_n}$ if and only if $\gcd(m_i, m_j) = 1$ for all i, j with $i \neq j$.

Example 2.71. (a) $Z_2 \times Z_3 \times Z_5 \cong Z_{30}$.

(b) $Z_2 \times Z_{3^2} \cong Z_{18}$.

(c) $Z_2 \times Z_3 \times Z_3 \ncong Z_{18}$ since $\gcd(3,3) \neq 1$.

Corollary 2.72. Assume that $n \in \mathbb{Z}_{\geqslant 2}$ and $n = (p_1)^{n_1} \cdots (p_r)^{n_r}$ such that $p_1, \ldots, p_r$ are different primes and $n_1, \ldots, n_r \in \mathbb{N}$, then

$$Z_n \cong Z_{(p_1)^{n_1}} \times \cdots \times Z_{(p_r)^{n_r}}.$$

Example 2.73. $Z_{72} \cong Z_8 \times Z_9$.

Example 2.74. The group $\mathbb{Z} \times Z_2$ is generated by $(1,0)$ and $(0,1)$ because $(n,0) = n(1,0)$ for any $n \in \mathbb{Z}$ and $(m,1) = m(1,0) + (0,1)$ for any $m \in \mathbb{Z}$. We write that $\mathbb{Z} \times Z_2 = \langle (1,0), (0,1) \rangle$.

Definition 2.75. Let $G_1, \ldots, G_n$ be groups. For $i = 1, \ldots, n$, define a subgroup $\overline{G}_i$ of $\prod_{i=1}^{n} G_i$ by

$$\overline{G}_i = \{(e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \mid a_i \in G_i\}.$$

We consider $\prod_{i=1}^{n} G_i$ to be the internal direct product of these subgroups $\overline{G}_i$, and $\prod_{i=1}^{n} G_i$ is called the external direct product of the groups G_i.

Remark. We shall usually omit the words external and internal and just say direct product.

Proposition 2.76. We have a natural (group) isomorphism

$$\begin{aligned} \overline{G}_i &\xrightarrow{\cong} G_i \\ (e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) &\longmapsto a_i. \end{aligned}$$

Definition 2.77. Let G be a group and $A \subseteq G$. Define the subgroup of G generated by A by

$$\langle A \rangle = \{a_1^{r_1} \cdots a_n^{r_n} \mid n \in \mathbb{N}, a_i \in A, r_i \in \mathbb{Z}\}.$$

If $G = \langle a_1, \ldots, a_k \rangle$ for some $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in G$, then G is finitely generated (by $a_1, \ldots, a_k$).

Remark. If G is finite, then G is finitely generated as $G = \langle G \rangle$.

Definition 2.78. Let $m \in \mathbb{Z}_{\geqslant 0}$. Then $\mathbb{Z}^m$ is the free abelian group of rank m.

Remark. (a) By convention, $\mathbb{Z}^0 = \{0\}$.

(b) If $m \in \mathbb{N}$, then $\mathbb{Z}^m = \langle \boldsymbol{e}_1, \ldots, \boldsymbol{e}_r \rangle$, where $\boldsymbol{e}_i \in \mathbb{Z}^m$ with $\boldsymbol{e}_{i,j} = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$. For example, $\mathbb{Z}^2 = \langle (1,0), (0,1) \rangle$ with $\boldsymbol{e}_1 = (1,0)$ and $\boldsymbol{e}_2 = (0,1)$, where $\boldsymbol{e}_{1,1} = \delta_{11} = 1$, $\boldsymbol{e}_{12} = \delta_{12} = 0$ and $\boldsymbol{e}_{2,1} = \delta_{11} = 1$, $\boldsymbol{e}_{22} = \delta_{22} = 0$.

Theorem 2.79 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let G be a finitely generated abelian group, then*

$$G \cong \mathbb{Z}^m \times Z_{p_1^{r_1}} \times \cdots \times Z_{p_n^{r_n}}$$

for some $m \in \mathbb{Z}_{\geqslant 0}$ and $n \in \mathbb{N}$, $p_1, \ldots, p_n$ primes and $r_1, \ldots, r_n \in \mathbb{Z}_{\geqslant 0}$. The direct product is unique except for possible rearrangement of the factors. The number m is the Betti number of G.

Proof. We omit the proof of existence. The uniqueness follows from Theorem 2.63. □

Remark. If $G = \{1\}$, then since $Z_1 = \{0\}$,

$$G = \{1\} \cong \{0\} \cong \{0\} \times \{0\} = \mathbb{Z}^0 \times Z_1 = \mathbb{Z}^0 \times Z_{p_1^0}.$$

Example 2.80. Find all abelian groups, up to isomorphism, of order 360.

Since $|G| = 360 < \infty$, we have that the Betti number m of G is 0. Then $G \cong Z_{p_1^{r_1}} \times \cdots \times Z_{p_n^{r_n}}$ for some $n \in \mathbb{N}$, $p_1, \ldots, p_n$ primes and $r_1, \ldots, r_n \in \mathbb{Z}_{\geqslant 0}$ such that $p_1^{r_1} \cdots p_n^{r_n} = 360$. Note that $360 = 2^3 3^2 5$. Hence we get as possibilities

$$\begin{gathered} Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5, \\ Z_2 \times Z_4 \times Z_3 \times Z_3 \times Z_5, \\ Z_8 \times Z_3 \times Z_3 \times Z_5, \\ Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_5, \\ Z_2 \times Z_4 \times Z_9 \times Z_5, \\ Z_8 \times Z_9 \times Z_5. \end{gathered}$$

Thus, there are 6 different abelian groups (up to isomorphism) of order 360.

Definition 2.81. A group G is decomposable if $G = H \times K$ with $\{1\} \lneq H, K \lneq G$. Otherwise G is indecomposable.

Theorem 2.82. *Let G be a finite abelian group. Then G is indecomposable if and only if $G \cong Z_{p^r}$ for some p prime and $r \in \mathbb{Z}_{\geqslant 0}$.*

Proof. $\Longrightarrow$ Since G is finite and abelian, we have that $G \cong Z_{p_1^{r_1}} \times \cdots \times Z_{p_n^{r_n}}$ for some $n \in \mathbb{N}$, $p_1, \ldots, p_n$ primes and $r_1, \ldots, r_n \in \mathbb{Z}_{\geqslant 0}$. Since G is indecomposable, $n = 1$.

$\Longleftarrow$ Let $\{1\} \lneq H \lneq G$. Since G is cyclic, we have that H is cyclic by Theorem 1.72. Since $|H| \mid |G|$ by Theorem 2.52 and $|G| = p^r$, we have that $|H| = p^i$ for some $i \in \mathbb{N}$ with $i < r$. Hence $H \cong Z_{p^i}$ by Theorem 1.83(b). Suppose that $Z_{p^r} \cong Z_{p^i} \times Z_{p^j}$ with $i, j \in \mathbb{N}$ and $i + j = r$. Without loss of generality, assume $i \leqslant j$. Let $(a, b) \in Z_{p^i} \times Z_{p^j}$. Then $p^j(a, b) = (p^j a, p^j b) = (p^{j-i}(p^i a), p^j b) = (0, 0)$ by Corollary 2.55. So every element in $Z_{p^i} \times Z_{p^j}$ would have an order at most $p^j < p^{i+j} = p^r$, contradicting $Z_{p^i} \times Z_{p^j} \cong Z_{p^r}$. □

Theorem 2.83. *Let G be a finite abelian group. If $m \mid |G|$, then there exists an $H \leqslant G$ of $|H| = m$.*

Proof. By Theorem 2.79, $G \cong Z_{p_1^{r_1}} \times \cdots \times Z_{p_n^{r_n}}$ for some $n \in \mathbb{N}$, $p_1, \ldots, p_n$ primes and $r_1, \ldots, r_n \in \mathbb{Z}_{\geqslant 0}$. Since $|G| = p_1^{r_1} \cdots p_n^{r_n}$ and $m \mid |G|$, we have that $m = p_1^{s_1} \cdots p_n^{s_n}$ with $0 \leqslant s_i \leqslant r_i$. For $i = 1, \ldots, n$, in the cyclic group $Z_{p_i^{r_i}}$, $|1| = p_i^{r_i}$, so $\left|\langle p_i^{r_i - s_i}\rangle\right| = \left|p_i^{r_i - s_i}\right| = \frac{p_i^{r_i}}{\gcd(p_i^{r_i - s_i}, p_i^{r_i})} = p_i^{s_i}$ by Theorem 1.86. Let

$$H := \langle p_1^{r_1 - s_1}\rangle \times \cdots \times \langle p_n^{r_n - s_n}\rangle.$$

Then $|H| = \left|\langle p_1^{r_1 - s_1}\rangle\right| \cdots \left|\langle p_1^{r_n - s_n}\rangle\right| = p_1^{s_1} \cdots p_n^{s_n} = m$. For $i = 1, \ldots, n$, $\langle p_i^{r_i - s_i}\rangle \leqslant Z_{p_i^{r_i}}$ since $p_i^{r_i - s_i} \in Z_{p_i^{r_i}}$. Thus, $H \leqslant G$ by Theorem 2.64. □

Theorem 2.84. *Let G be an abelian group of $|G| = m$ such that $m \in \mathbb{N}$ is square free, then G is cyclic.*

Proof. By Theorem 2.79, $G \cong Z_{p_1^{r_1}} \times \cdots \times Z_{p_n^{r_n}}$ for some $n \in \mathbb{Z}$, $p_1, \ldots, p_n$ primes and $r_1, \ldots, r_n \in \mathbb{Z}_{\geqslant 0}$. Then $m = p_1^{r_1} \cdots p_n^{r_n}$. Since m is square free, $r_i = 1$ for all i, and $p_1, \ldots, p_n$ are distinct. Thus, $G \cong Z_{p_1} \times \cdots \times Z_{p_n} \cong Z_{p_1 \cdots p_n}$ by Corollary 2.70. □

Chapter 3

Homomorphisms and Quotient Groups

3.1 Homomorphisms

Definition 3.1. Let $\phi : G \to G'$ be a map of groups. ϕ is a group homomorphism if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Remark. If $\phi(a) = 1_{G'}$ for all $a \in G$, then ϕ is the trivial group homomorphism.

Example 3.2. Let $\phi : G \to G'$ be a surjective group homomorphism. If G is abelian, then G' is also abelian since one can show that if $\phi : \langle S, * \rangle \to \langle T, \star \rangle$ be a surjective binary structure homomorphism and $*$ is commutative, then $\star$ is also commutative.

Example 3.3. Let $\phi : S_n \to Z_2$ be defined by $\phi(\sigma) = 0$ if $\sigma \in A_n$ and $\phi(\sigma) = 1$ if $\sigma \in B_n$. Let $\sigma, \mu \in S_n$.

(a) If $\sigma, \mu \in A_n$, then $\sigma\mu \in A_n$, so $\phi(\sigma\mu) = 0 = 0 +_2 0 = \phi(\sigma) + \phi(\mu)$.

(b) If $\sigma, \mu \in B_n$, then $\sigma\mu \in A_n$, so $\phi(\sigma\mu) = 0 = 1 +_2 1 = \phi(\sigma) + \phi(\mu)$.

(c) If $\sigma \in A_n$ and $\mu \in B_n$, then $\sigma\mu \in B_n$, so $\phi(\sigma\mu) = 1 = 0 +_2 1 = \phi(\sigma) + \phi(\mu)$.

(d) If $\sigma \in B_n$ and $\mu \in A_n$, then $\sigma\mu \in B_n$, so $\phi(\sigma\mu) = 1 = 1 +_2 0 = \phi(\sigma) + \phi(\mu)$.

Thus, ϕ is a group homomorphism.

Example 3.4. Let $F := \langle \{f : \mathbb{R} \to \mathbb{R}\}, + \rangle$. Then F is a group. Let $c \in \mathbb{R}$ and $\phi_c : F \to \mathbb{R}$ be the valuation map defined by $\phi_c(f) = f(c)$. Then ϕ_c is a group homomorphism since $\phi_c(f + g) = (f + g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)$ for all $f, g \in F$.

Example 3.5. Let $A \in \mathrm{Mat}_{m \times n}(\mathbb{R})$. Let $\phi : \mathbb{R}^n \to \mathbb{R}^m$ be defined by $\phi(\boldsymbol{v}) = A\boldsymbol{v}$. Then ϕ is a group homomorphism since $\phi(\boldsymbol{v} + \boldsymbol{w}) = A(\boldsymbol{v} + \boldsymbol{w}) = A\boldsymbol{v} + A\boldsymbol{w} = \phi(\boldsymbol{v}) + \phi(\boldsymbol{w})$ for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^n$.

Example 3.6. Let $\det : \langle \mathrm{GL}_n(\mathbb{R}), \cdot \rangle \to \langle \mathbb{R}^*, \cdot \rangle$. Then det is a group homomorphism since $\det(AB) = \det(A)\det(B)$ for all $A, B \in \mathrm{GL}_n(\mathbb{R})$.

Homomorphisms of a group G into itself are often useful for studying the structure of G.

Example 3.7. Let $r \in \mathbb{Z}$ and $\phi_r : \mathbb{Z} \to \mathbb{Z}$ be define by $\phi_r(n) = rn$. Then ϕ_r is a group homomorphism since $\phi_r(m+n) = r(m+n) = rm + rn = \phi_r(m) + \phi_r(n)$ for all $m, n \in \mathbb{Z}$. Note that ϕ_0 is the trivial group homomorphism, $\phi_1 = \mathrm{id}_{\mathbb{Z}}$, and ϕ_r is onto if and only if $r = \pm 1$.

Example 3.8. Let $G_1, \ldots, G_n$ be groups. For $i = 1, \ldots, n$, the projection map $\pi_i : G_1 \times \cdots \times G_n \to G_i$ defined by $\pi_i(a_1, \ldots, a_n) = a_i$ is a group homomorphism since

$$\pi_i((a_1, \ldots, a_n)(b_1, \ldots, b_n)) = \pi_i(a_1b_1, \ldots, a_nb_n) = a_ib_i = \pi_i(a_1, \ldots, a_n)\pi_i(b_1, \ldots, b_n)$$

for all $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \cdots \times G_n$.

Example 3.9. Let $F = \langle \mathcal{C}[0,1], + \rangle$, where $\mathcal{C}[0,1] = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$. Then F is a group. Let $\phi : F \to \mathbb{R}$ be defined by $\phi(f) = \int_0^1 f(x)dx$. Then ϕ is a group homomorphism, for

$$\phi(f+g) = \int_0^1 (f+g)(x)dx = \int_0^1 (f(x) + g(x))dx = \int_0^1 f(x)dx + \int_0^1 g(x)dx = \phi(f) + \phi(g),$$

for all $f, g \in F$.

Example 3.10. Let $n \in \mathbb{N}$ and $\phi : \mathbb{Z} \to Z_n$ be given by $\phi(m) = r$, where $m = nq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leqslant r \leqslant n-1$ by division algorithm. Let $s, t \in \mathbb{Z}$. Then $s = q_1n + r_1$ and $t = q_2n + r_2$, where $q_i, r_i \in \mathbb{Z}$ such that $0 \leqslant r_i \leqslant n-1$ for $i = 1, 2$. Write $r_1 + r_2 = q_3n + r_3$ for some $q_3, r_3 \in \mathbb{Z}$ such that $0 \leqslant r_3 \leqslant n-1$ by division algorithm. Then $s + t = (q_1 + q_2 + q_3)n + r_3$, so that $\phi(s+t) = r_3 = r_1 +_n r_2 = \phi(r_1) +_n \phi(r_2)$. Thus, ϕ is a group homomorphism.

Proposition 3.11. If $\phi : G \to G'$ and $\varphi : G' \to G''$ are group homomorphisms, then $\varphi \circ \phi$ is a group homomorphism.

Definition 3.12. Let $\phi : X \to Y$ and $B \subseteq Y$. The inverse image of B in X is

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

Fact 3.13. Let $\phi : X \to Y$ and $B \subseteq Y$. Then $x \in \phi^{-1}(B)$ if and only if $\phi(x) \in B$. In particular, for $b \in Y$, $x \in \phi^{-1}(\{b\})$ if and only if $\phi(x) = b$.

Theorem 3.14. *Let $\phi : G \to G'$ be a group homomorphism.*

(a) $\phi(1) = 1_{G'}$.

(b) $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$.

(c) If $H \leqslant G$, then $\phi(H) \leqslant G'$.

(d) If $K' \leqslant G'$, then $\phi^{-1}(K') \leqslant G$.

Proof. (a) It follows from Theorem 1.21.

(b) For $a \in G$, $1_{G'} = \phi(1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ since ϕ is a group homomorphism. Hence $\phi(a^{-1}) = \phi(a)^{-1}$.

(c) Let $\phi(a), \phi(b) \in \phi(H)$ with $a, b \in H$. Since $H \leqslant G$, we have that $ab \in H$. Also, since ϕ is a group homomorphism, we have that $\phi(a)\phi(b) = \phi(ab) \in \phi(H)$. Since $H \leqslant H$, $1 \in H$. Then by (a), $1_{G'} = \phi(1) \in \phi(H)$. Since $H \leqslant G$, $a^{-1} \in H$. Then by (b), $\phi(a)^{-1} = \phi(a^{-1}) \in \phi(H)$.

(d) Let $a, b \in \phi^{-1}(K')$. Then $\phi(a), \phi(b) \in K'$. Since ϕ is a group homomorphism, we have that $\phi(ab) = \phi(a)\phi(b) \in K'$ as $K' \leqslant G$. Hence $ab \in \phi^{-1}(K')$ by Fact 3.13. By (a), $\phi(1) = 1_{G'} \in K'$ since $K' \leqslant G'$. Hence $1 \in \phi^{-1}(K')$ by Fact 3.13. By (b), $\phi(a^{-1}) = \phi(a)^{-1} \in K'$ since $\phi(a) \in K' \leqslant G$. Hence $a^{-1} \in \phi(K^{-1})$ by Fact 3.13. □

Definition 3.15. Let $\phi : G \to G'$ be a group homomorphism. The kernel of ϕ is

$$\mathrm{Ker}(\phi) = \phi^{-1}(\{1_{G'}\}) = \{a \in G \mid \phi(a) = 1_{G'}\}.$$

Remark. By Theorem 3.14(d), $\mathrm{Ker}(\phi) \leqslant G$.

Example 3.16. In Example 3.5, $\mathrm{Ker}(\phi)$ is the null space of A.

Theorem 3.17. *Let $\phi : G \to G'$ be a group homomorphism and $H = \mathrm{Ker}(\phi)$. Then for $a \in G$,*

$$\phi^{-1}(\{\phi(a)\}) = \{x \in G \mid \phi(x) = \phi(a)\} = aH = Ha.$$

Consequently, $G//H = G\backslash\backslash H$.

Proof. The first equality follows from Fact 3.13. Note that for $a \in G$,

$$\begin{aligned}
\{x \in G \mid \phi(x) = \phi(a)\} &= \{x \in G \mid \phi(a)^{-1}\phi(x) = 1_{G'}\} \\
&= \{x \in G \mid \phi(a^{-1})\phi(x) = 1_{G'}\} \\
&= \{x \in G \mid \phi(a^{-1}x) = 1_{G'}\} \\
&= \{x \in G \mid a^{-1}x \in \phi^{-1}(\{1_{G'}\})\} \\
&= \{x \in G \mid a^{-1}x \in \mathrm{Ker}(\phi)\} \\
&= \{x \in G \mid a^{-1}x \in H\} \\
&= aH.
\end{aligned}$$

where the second equality follows from Theorem 3.14(b), the third equality follows from that ϕ is a group homomorphism, the fourth equality follows from Fact 3.13, and the last equality follows from the remark after Theorem 2.46. □

Example 3.18. Let $|\cdot| : \mathbb{C}^* \to \mathbb{R}^{>0}$ be given by $|z| = \sqrt{z\bar{z}}$. Then $|\cdot|$ is a group homomorphism, and $\mathrm{Ker}(|\cdot|) = \{z \in \mathbb{C} \mid |z| = 1\} = \mathbb{S}_1$, which is the unit circle in the complex plane. The cosets of $\mathbb{S}_1$ are of the form

$$z'\mathbb{S}_1 = z'\{z \in \mathbb{C} \mid |z| = 1\} = \{z'z \mid z \in \mathbb{C} \text{ and } |z| = 1\} = \{z \in \mathbb{C} \mid |z| = |z'|\},$$

i.e., the cosets of $\mathbb{S}_1$ are circles with center at the origin.

Example 3.19. Let $D := \langle \mathcal{D}(\mathbb{R}), + \rangle$, where $\mathcal{D}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is differentiable}\}$. Let $F = \langle \{f : \mathbb{R} \to \mathbb{R}\}, + \rangle$. Then D, F are groups. Let $\phi : D \to F$ be defined by $\phi(f) = f'$. Then ϕ is a group homomorphism since $\phi(f + g) = (f + g)' = f' + g' = \phi(f) + \phi(g)$ for all $f, g \in F$.

Note that $\mathrm{Ker}(\phi) = \{f \in D \mid f' = 0\} = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is constant}\} := C$. Then the set of functions in D mapped to x^2 is

$$\phi^{-1}(\{x^2\}) = \phi^{-1}(\{\phi(x^3/3)\}) = x^3/3 + C.$$

Corollary 3.20. Let $\phi : G \to G'$ be a group homomorphism. Then ϕ is 1-1 if and only if $\mathrm{Ker}(\phi) = \{1\}$.

Proof.
$$\phi \text{ is 1-1} \iff \text{for } a \in G,\ \phi(a) = 1_{G'} \text{ if and only if } a = 1 \iff \mathrm{Ker}(\phi) = \{1\}. \qquad \square$$

Remark. Let $H \leqslant G$. We will see that if $gH = Hg$ for all $g \in G$, then $G//H$ forms a group under $(aH)(bH) = (ab)H$, and then we write $(G//H, \cdot)$ as G/H. Let $\phi : G \to G'$ be a group homomorphism and $H := \mathrm{Ker}(\phi)$. Then G/H is a group, and there is a natural group homomorphism

$$\begin{aligned} \phi : G &\longrightarrow G/H \\ a &\longmapsto aH. \end{aligned}$$

Definition 3.21. H is a normal subgroup of G, written as $H \trianglelefteq G$, if $H \leqslant G$, and $gH = Hg$ for all $g \in G$.

Corollary 3.22. If $\phi : G \to G'$ is a group homomorphism, then $\mathrm{Ker}(\phi) \trianglelefteq G$.

Proof. It follows from Theorem 3.17. $\square$

Remark. For a group homomorphism $\phi : G \to G'$, $\mathrm{Ker}(\phi)$ and $\mathrm{Im}(\phi)$ are two primary important things. We will show in the next setion that there is a well-defined isomorphism

$$\begin{aligned} G/\mathrm{Ker}(\phi) &\xrightarrow{\cong} \mathrm{Im}(\phi) \\ \bar{a} &\longmapsto \phi(a). \end{aligned}$$

3.2 Factor groups

Definition 3.23. Let $\phi : G \to G'$ be a group homomorphism with $H = \mathrm{Ker}(\phi)$. Then the cosets of H form a factor group, $G/H := \{aH \mid a \in G\}$, where $(aH)(bH) = (ab)H$ or $\bar{a}\bar{b} = \overline{ab}$.

Remark. We will prove the binary operation is well-defined in Theorem 3.26, i.e., the coset multiplication is independent of the choices a and b from the cosets.

Example 3.24. Let $n \in \mathbb{N}$. Define a map

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow Z_n \\ m &\longmapsto r, \end{aligned}$$

where $m = nq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leqslant r \leqslant n - 1$ by division algorithm. Then ϕ is a homomorphism by Example 3.10, with

$$\mathrm{Ker}(\phi) = \{m \in G \mid \phi(m) = 0\} = \{nm \mid m \in \mathbb{Z}\} = n\mathbb{Z}.$$

Hence $\mathbb{Z}/n\mathbb{Z}$ is a factor group.

Example 3.25. In $\mathbb{Z}/5\mathbb{Z}$, $(2+5\mathbb{Z})+(4+5\mathbb{Z}) = (2+4)+5\mathbb{Z} = 6+5\mathbb{Z} = 1+5\mathbb{Z}$. Note that $27 \in \bar{2} = 2+5\mathbb{Z}$ and $-16 \in \bar{4} = 4+5\mathbb{Z}$ (or because $2 \equiv 27 \pmod 5$ and $4 \equiv -16 \pmod 5$ by Example 2.49), but $(27+5\mathbb{Z})+(-16+5\mathbb{Z}) = (27-16)+5\mathbb{Z} = 11+5\mathbb{Z} = 1+5\mathbb{Z}$, or $\overline{27} + \overline{-16} = \overline{27-16} = \overline{11} = \bar{1}$.

Remark. In the factor group $\mathbb{Z}/n\mathbb{Z}$,

$$\begin{aligned} a + n\mathbb{Z} = b + n\mathbb{Z} &\iff a \equiv b \pmod{n} \\ &\iff a - b \in n\mathbb{Z} \\ &\iff n \mid (a-b) \\ &\iff n \mid (b-a). \end{aligned}$$

We prove that the coset multiplication is independent of the choices a and b from the cosets of H when $H \trianglelefteq G$.

Theorem 3.26. *Let $H \leqslant G$. Then left coset multiplication is well-defined by the equation $(aH)(bH) = (ab)H$ if and only if $H \trianglelefteq G$.*

Proof. $\Longrightarrow$ Let $a \in G$. We claim that $aH = Ha$. "$\subseteq$". Let $x \in aH$. Choose representatives $x \in aH$ and $a^{-1} = a^{-1}1 = a^{-1}H$, we have that $(xH)(a^{-1}H) = (xa^{-1})H$. On the other hand, choosing representatives $a \in aH$ and $a^{-1} \in a^{-1}H$, we see that $(aH)(a^{-1}H) = 1H = H$. Using our assumption that left coset multiplication by representatives is well-defined, we must have $xa^{-1} = H$ and so $xa^{-1} = h$ for some $h \in H$. Then $x = ha \in Ha$. Hence $aH \subseteq Ha$. "$\supseteq$" is left as an exercise. Thus, $H \trianglelefteq G$.

$\Longleftarrow$ Assume that $H \trianglelefteq G$. Suppose we wish to compute $(aH)(bH)$. Due to our hypothesis, we can simply say cosets, omitting left and right. Choosing $a \in aH$ and $b \in bH$, we obtain the coset $(ab)H$. Choosing different representatives $ah_1 \in aH$ and $bh_2 \in bH$ with $h_1, h_2 \in H$, we obtain the coset $(ah_1bh_2)H$. We need to show that $(ab)H = (ah_1bh_2)H$. Now $h_1b \in Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Thus,

$$ah_1bh_2 = a(h_1b)h_2 = a(bh_3)h_2 = (ab)(h_3h_2) \in (ab)H. \qquad \square$$

Corollary 3.27. Let $H \trianglelefteq G$. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$.

Proof. By definition, the operation is closed. The associativity in G/H follows from associativity in G. Because $(aH)(1H) = (a1)H = aH = (1a)H = (1H)(aH)$, we see that $1H = H$ is the identity element in G/H. Finally, $(a^{-1}H)(aH) = (a^{-1}a)H = 1H = (aa^{-1})H = (aH)(a^{-1}H)$ shows that $a^{-1}H = (aH)^{-1}$. $\square$

Remark. Let $H \trianglelefteq G$. Then $(aH)^{-1} = a^{-1}H$ for $aH \in G/H$.

Definition 3.28. Let $H \trianglelefteq G$. Then G/H is the factor group (or quotient group) of G by H.

Example 3.29. Since $\mathbb{Z}$ is an abelian group, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z}$ is a factor group, and we will see $\mathbb{Z}/n\mathbb{Z} \cong Z_n$ from Example 3.33.

Theorem 3.30. *Let $H \trianglelefteq G$. Then we have a surjective homomorphism*

$$\begin{aligned} \gamma : G &\longrightarrow G/H \\ a &\longmapsto aH \end{aligned}$$

with $\mathrm{Ker}(\gamma) = H$.

Proof. Let $a, b \in G$. Then

$$\gamma(ab) = (ab)H = (aH)(bH) = \gamma(a)\phi(b).$$

Note that

$$\mathrm{Ker}(\gamma) = \{a \in G \mid \gamma(a) = H\} = \{a \in G \mid aH = H\} = H. \qquad \square$$

Proposition 3.31. We have the following.

(a) Let $H \leqslant G$. Then $aH = bH$ if and only if $a^{-1}b \in H$ if and only if $b^{-1}a \in H$.

(b) Let $H \trianglelefteq G$. Then $aH = bH$ if and only if $ab^{-1} \in H$ if and only if $ba^{-1} \in H$.

Proof. (a) $\Longrightarrow$ If $aH = bH$, then $ah_1 = bh_2$ for some $h_1, h_2 \in H$, so $a^{-1}b = h_1h_2^{-1} \in H$ because $H \leqslant G$.

$\Longleftarrow$ If $a^{-1}b \in H$, then $a^{-1}b = h$ for some $h \in H$, so $b = ah \in aH$, and hence $aH = bH$.

(b) The proof is similar to the proof of (a) with the condition that $Ha = aH$ for each $a \in G$ when $H \trianglelefteq G$. $\square$

Remark. Let $H \leqslant G$ and $a \in G$. Then $aH = H$ if and only if $a^{-1} \in H$ if and only if $a \in H$.

Theorem 3.32 (The Fundamental Homomorphism Theorem)**.** *Let $\phi : G \to G'$ be a group homomorphism with $H = \mathrm{Ker}(\phi)$. Then we have a <u>natural</u> group isomorphism*

$$\begin{aligned} \mu : G/H &\xrightarrow{\cong} \mathrm{Im}(\phi) \\ aH &\longmapsto \phi(a). \end{aligned}$$

Let $\gamma : G \to G/H$ be the <u>natural</u> group homomorphism given by $\gamma(a) = aH$, then the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\ \phi\ } & \mathrm{Im}(\phi) \\ & \searrow^{\gamma} & \uparrow{\scriptstyle \mu} \\ & & G/H \end{array}$$

i.e., $\phi = \mu\gamma$, i.e., $\phi(a) = \mu\gamma(a)$ for each $a \in G$.

Proof. Let $aH = bH \in G/H$. Then $a^{-1}b \in H = \mathrm{Ker}(\phi)$ by proposition 3.31(a). Since ϕ is a group homomorphism, we that $1_{G'} = \phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a)^{-1}\phi(b)$. Then $\phi(a) = \phi(b)$. Hence μ is well-defined. Let $aH, bH \in G/H$. Then

$$\mu((aH)(bH)) = \mu((ab)H) = \phi(ab) = \phi(a)\phi(b) = \mu(aH)\mu(bH),$$

and so μ is a group homomorphism. Note that

$$\begin{aligned} \mathrm{Ker}(\mu) &= \{aH \in G/H \mid \mu(aH) = 1_{G'}\} \\ &= \{aH \in G/H \mid \phi(a) = 1_{G'}\} \\ &= \{aH \in G/H \mid a \in \mathrm{Ker}(\phi)\} \\ &= \{aH \in G/H \mid a \in H\} \\ &= \{H\} \\ &= \{1_{G/H}\}. \end{aligned}$$

The ontoness of μ is straightforward. At last, for $a \in G$, $\mu\gamma(a) = \mu(aH) = \phi(a)$. $\square$

Example 3.33. In Example 3.24, since ϕ is surjective, we have an isomorphism

$$\begin{aligned}\mu : \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\cong} Z_n \\ m + n\mathbb{Z} &\longmapsto \phi(m) = m \pmod{n}.\end{aligned}$$

$m \pmod{n}$ is the remainder of m divided by n, For example, when $n = 5$, $\mu(\overline{19}) = \mu(19 + 5\mathbb{Z}) = \phi(19) = 19 \pmod{5} = 4$, since $19 = 3(5) + 4$.

Example 3.34. Classify the group $(Z_4 \times Z_2)/(\{0\} \times Z_2)$. We have a projection map

$$\begin{aligned}\phi : Z_4 \times Z_2 &\longrightarrow Z_4 \\ (x, y) &\longmapsto x.\end{aligned}$$

Then ϕ is a surjective group homomorphism with

$$\mathrm{Ker}(\phi) = \{(x, y) \in Z_4 \times Z_2 \mid \phi(x, y) = 0\} = \{(x, y) \in Z_4 \times Z_2 \mid x = 0\} = \{0\} \times Z_2.$$

Hence $(Z_4 \times Z_2)/(\{0\} \times Z_2) \cong Z_4$.

Theorem 3.35. *Let G, G' be groups. We have a group isomorphism*

$$\begin{aligned}\mu : (G \times G')/\overline{G}' &\xrightarrow{\cong} G \\ (a, a')\overline{G}' &\longmapsto a,\end{aligned}$$

where $\overline{G}' = \{1\} \times G' = \{(1, a') \mid a' \in G'\}$. Similarly, $(G \times G')/\overline{G} \xrightarrow{\cong} G'$ in a natural way.

Proof. We have a surjective group homomorphism (projection map)

$$\begin{aligned}\phi : G \times G' &\longrightarrow G \\ (a, a') &\longmapsto a\end{aligned}$$

with

$$\mathrm{Ker}(\phi) = \{(a, a') \in G \times G' \mid \phi(a, a') = 1\} = \{(a, a') \in G \times G' \mid a = 1\} = \{1\} \times G'.$$

Hence $(G \times G')/(\{1\} \times G') \cong G$ by Theorem 3.32. □

Lemma 3.36. Let $H \leqslant G$. Then for $g \in G$,

$$gH = Hg \iff gHg^{-1} = H.$$

Also,

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

Proof. Note that for $g \in G$,

$$\begin{aligned}gH = Hg &\iff \{gh \mid h \in H\} = \{hg \mid h \in H\} \\ &\iff \{gh \mid h \in H\}g^{-1} = \{hg \mid h \in H\}g^{-1} \\ &\iff \{ghg^{-1} \mid h \in H\} = \{hgg^{-1} \mid h \in H\} \\ &\iff \{ghg^{-1} \mid h \in H\} = \{h \mid h \in H\} \\ &\iff gHg^{-1} = H.\end{aligned}$$

Also,

$$\begin{aligned} gHg^{-1} \subseteq H, \forall g \in G &\iff \{ghg^{-1} \mid h \in H\} \subseteq \{h \mid h \in H\}, \forall g \in G \\ &\iff g^{-1}\{ghg^{-1} \mid h \in H\}g \subseteq g^{-1}\{h \mid h \in H\}g, \forall g \in G \\ &\iff \{g^{-1}ghg^{-1}g \mid h \in H\} \subseteq \{g^{-1}hg \mid h \in H\}, \forall g \in G \\ &\iff H \subseteq \{g^{-1}hg \mid h \in H\}, \forall g \in G \\ &\iff H \subseteq \{ghg^{-1} \mid h \in H\}, \forall g \in G \\ &\iff H \subseteq gHg^{-1}, \forall g \in G, \end{aligned}$$

where all the equivalences holds for a fixed $g \in G$ except for the fifth one. □

Remark. The following are direct results of Lemma 3.36.

$$\begin{aligned} gH = Hg, \forall g \in G &\iff gHg^{-1} = H, \forall g \in G \\ &\iff gHg^{-1} \subseteq H, \forall g \in G \\ &\iff H \subseteq gHg^{-1}, \forall g \in G. \end{aligned}$$

Theorem 3.37. *Let $H \leqslant G$. The following conditions are equivalent.*

(a) $H \trianglelefteq G$.

(b) $gH = Hg$ for all $g \in G$.

(c) $gHg^{-1} = H$ for all $g \in G$.

(d) $gHg^{-1} \subseteq H$ for all $g \in G$.

(e) $gHg^{-1} \supseteq H$ for all $g \in G$.

The condition (c) is often taken as the definition of a normal subgroup H of a group G.

Proof. (a)$\iff$(b) follows from the original definition of the normal subgroup, i.e., Definition 3.21. The remaining equivalence follows from Lemma 3.36. □

Corollary 3.38. If G is abelian and $H \leqslant G$, then $H \trianglelefteq G$.

Proof. It follows from that

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} = \{gg^{-1}h \mid h \in H\} = \{h \mid h \in H\} = H.$$ □

Definition 3.39. An isomorphism $\phi : G \to G$ of a group G with itself is an automorphism of G. The automorphism $i_g : G \to G$, where $i_g(x) = gxg^{-1}$, is the inner automorphism of G by g. Performing i_g on a is called conjugation of x by g.

Remark. Let $H \leqslant G$. The equivalence of conditions (b) and (c) in Theorem 3.37 shows that $gH = Hg$ for all $g \in G$ if and only if $\mathrm{Im}(i_g) = H$ for all $g \in G$, that is, if and only if H is invariant under all inner automorphisms of G. Thus,

$$\{H \mid H \trianglelefteq G\} = \{H \leqslant G \mid i_g(H) = H, \forall g \in G\}.$$

Definition 3.40. Let $H, K \leqslant G$. Then K is a conjugate subgroup of H if $K = i_g(H) = gHg^{-1}$ for some $g \in G$.

Remark. If $H \trianglelefteq G$, then H is the only conjugate subgroup of H by Theorem 3.37.

3.3 Factor group computations and simple groups

Example 3.41. $N = \{0\} \trianglelefteq \mathbb{Z}$ since $\{0\}$ is the trivial subgroup of $\mathbb{Z}$ and $\mathbb{Z}$ is abelian. Compute $\mathbb{Z}/\{0\}$.

Method 1. Since $N = \{0\}$ has only one element, every coset of N has only one element. That is, the cosets are of the form $\{m\}$ for $m \in \mathbb{Z}$. Thus, there is a natural (well-defined) bijection

$$\begin{aligned} \mathrm{id} : \mathbb{Z}/\{0\} &\longrightarrow \mathbb{Z} \\ \{m\} &\longmapsto m. \end{aligned}$$

Each $m \in \mathbb{Z}$ is simply renamed $\{m\}$ in $\mathbb{Z}/\{0\}$.

Method 2. W have a surjective (and injective) group homomorphism

$$\begin{aligned} \mathrm{id} : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ m &\longmapsto m, \end{aligned}$$

with $\mathrm{Ker}(\mathrm{id}) = \{0\}$. Then by Theorem 3.32,

$$\begin{aligned} \mu : \mathbb{Z}/\{0\} &\xrightarrow{\cong} \mathbb{Z} \\ m + \{0\} &\longmapsto m \\ \text{or } \{m\} &\longmapsto m. \end{aligned}$$

Remark. In general, we have a surjective (and injective) group homomorphism

$$\begin{aligned} \mathrm{id} : G &\longrightarrow G \\ g &\longmapsto g, \end{aligned}$$

with $\mathrm{Ker}(\mathrm{id}) = \{1\}$. Then by Theorem 3.32,

$$\begin{aligned} \mu : G/\{1\} &\xrightarrow{\cong} G \\ g\{1\} &\longmapsto g \\ \text{or } \{g\} &\longmapsto g. \end{aligned}$$

Moreover,

$$\begin{aligned} \phi : G &\longrightarrow G \\ g &\longmapsto 1, \end{aligned}$$

is a group homomorphism with $\mathrm{Ker}(\phi) = G$ and $\mathrm{Im}(\phi) = \{1\}$. Then by Theorem 3.32,

$$\begin{aligned} \mu : G/G &\xrightarrow{\cong} \{1\} \\ gG &\longmapsto 1 \\ \text{or } G &\longmapsto 1. \end{aligned}$$

This implies that $G/G = \{G\}$.

Theorem 3.42. *Let $|G| < \infty$ and $N \leqslant G$. Then $N \trianglelefteq G$ is of $|G/N| = 2$ if and only if $|G| = 2|N|$.*

Proof. $\Longrightarrow$ Since $G/N = \{aN \mid a \in G\}$ and $|G/N| = 2$, we have that $G/N = \{N, aN\}$ for some $a \in G \setminus N$. Since $|N| = |aN|$ and $aN \sqcup N = G$, we have that $|G| = 2|N|$ (and $aN = G \setminus N$).

$\Longleftarrow$ Note that for all $a \in G \setminus N$, $aN \cap N = \emptyset$, and so $aN = G \setminus N$ since G is finite and $|aN| = |N| = \frac{1}{2}|G|$. Hence by definition of G/N, $|G/N| = 2$. Similarly, for all $a \in G \setminus N$, $Na = G \setminus N = aN$. Also, for all $a \in N$, $aN = N = Na$. Thus, $aN = Na$ for all $a \in G$, and so $N \trianglelefteq G$. □

Example 3.43. Let $n \in \mathbb{Z}_{\geqslant 2}$. Because $A_n \leqslant S_n$, $|S_n| = n! < \infty$, and $|S_n| = 2|A_n|$ by Proposition 2.40, we see that $A_n \trianglelefteq S_n$. Let $\sigma \in B_n = S_n \setminus A_n$ so that $S_n/A_n = \{A_n, \sigma A_n\}$. Using the definition of the operation $(aA_n)(bA_n) = (ab)A_n$ in S_n/A_n, we get the following table:

Table 3.1

	A_n	σA_n
A_n	A_n	σA_n
σA_n	σA_n	A_n

Note that $(\sigma A_n)(\sigma A_n) = \sigma^2 A_n = A_n$ since $\sigma^2 \in A_n$. Renaming the element A_n "even" and the elements σA_n "odd", the multiplication shown in above table becomes

Table 3.2

	even	odd
even	even	odd
even	odd	even

This example illustrates that while knowing the product of two cosets in G/N does not tell us what the product of two elements of G is, it may tell us that the product in G of two types of elements is itself of a certain type.

Example 3.44 (Falsity of the converse of the theorem of Lagrange)**.** $|A_4| = \frac{1}{2}(4!) = 12$, and $6 \mid 12$, but A_4 contains no subgroup of 6. Suppose that $H \leqslant A_4$ is of $|H| = 6 = \frac{1}{2}|A_4|$. Then $H \trianglelefteq A_4$, $|A_4/H| = 2$, and $A_4/H = \{H, \sigma H\}$ with $\sigma \in A_4 \setminus H$ by Theorem 3.42. Since A_4/H is a group of $|A_4/H| = 2$, we have that $A_4/H \cong Z_2$ by Example 1.38(b). Hence $A_4/H = \langle \sigma H \rangle$, and so for each $\alpha \in \sigma H$, we have that

$$\alpha^2 H = (\alpha H)(\alpha H) = (\sigma H)(\sigma H) = 1_{A_4/H} = H,$$

and so $\alpha^2 \in H$. For each $\alpha \in H$, we must have $(\alpha^2 H) = (\alpha H)(\alpha H) = HH = H$, and so $\alpha^2 \in H$. Thus, for each $\alpha \in A_4$, we have that $\alpha^2 \in H$. But in A_4, we have that $(1\ 2\ 3) = (1\ 3\ 2)^2 \in H$, $(1\ 3\ 2) = (1\ 2\ 3)^2 \in H$. A similar computation shows that

$$(1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3) \in H.$$

This shows that $|H| \geqslant 8$, contradicting $|H| = 6$.

Lemma 3.45. Let $N \trianglelefteq G$ and $g \in G$. Then $(gN)^n = g^n N$ for all $n \in \mathbb{Z}$.

Proof. Note that G/N is a group since $N \trianglelefteq G$, with $gN \in G/N$. If $n = 0$, then $(gN)^0 = N = 1N = g^0 N$. If $n > 0$, then $(gN)^n = \underbrace{gN \cdots gN}_{n \text{ times}} = g^n N$. If $n < 0$, then

$$(gN)^n = \underbrace{(gN)^{-1} \cdots (gN)^{-1}}_{-n \text{ times}} = \underbrace{(g^{-1}N) \cdots (g^{-1}N)}_{-n \text{ times}} = (g^{-1}N)^{-n} = (g^{-1})^{-n}N = g^n N,$$

where the fourth equality follows from the discussion of the case $n > 0$ and the last equality follows from Corollary 1.48. □

Theorem 3.46. *Let $N \trianglelefteq G$.*

(a) If G is abelian, then so is G/N.

(b) If $G = \langle g_1, \ldots, g_k \rangle$, then $G/N = \langle g_1 N, \cdots, g_k N \rangle$. In particular, if G is cyclic, then so is G/N.

Proof. (a) For $gN, hN \in G/N$, $(gN)(hN) = (gh)N = (hg)N = (hN)(gN)$, where the second equality follows from that G is abelian.

(b) Let $g \in G = \langle g_1, \ldots, g_k \rangle$, then $g = g_1^{n_1} \cdots g_k^{n_k}$ for some $n_1, \ldots, n_k \in \mathbb{Z}$ by Defintion 2.77. Hence

$$gN = (g_1^{n_1} \cdots g_k^{n_k})N = (g_1^{n_1}N) \cdots (g_k^{n_k}N) = (g_1N)^{n_1} \cdots (g_kN)^{n_k} \in \langle g_1N, \cdots, g_kN \rangle,$$

where the third identity follows from Lemma 3.45. □

Example 3.47. Let us compute the factor group $(Z_4 \times Z_6)/\langle (0,1) \rangle$, where

$$H := \langle (0,1) \rangle = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5)\} = \{0\} \times Z_6 = \overline{Z_6}.$$

Since $|H| = 6$, we have that all cosets of H must have 6 elements. Also,

$$|(Z_4 \times Z_6)/H| = \frac{|Z_4 \times Z_6|}{|H|} = \frac{|Z_4||Z_6|}{6} = \frac{4(6)}{6} = 4.$$

Method 1. From Proposition 3.31, for $(a_1, a_2) + H, (a_1', a_2') + H \in Z_4 \times Z_6/H$, we know that $(a_1, a_2) + H \neq (a_1', a_2') + H$ if and only if $-(a_1, a_2) + (a_1', a_2') \notin H$ if and only if $(a_1' - a_1, a_2' - a_2) \notin H$ if and only if $a_1' - a_1 \neq 0$ if and only if $a_1' \neq a_1$. Thus, the cosets of H are

$$(0,0) + H,\ (1,0) + H,\ (2,0) + H,\ (3,0) + H.$$

Method 2. Similar to the proof of Theorem 3.35, we have a surjective group homomorphism,

$$\begin{aligned} \phi : Z_4 \times Z_6 &\longrightarrow Z_4 \\ (a_1, a_2) &\longmapsto a_1, \end{aligned}$$

with

$$\mathrm{Ker}(\phi) = \{(a_1, a_2) \in Z_4 \times Z_6 \mid \phi(a_1, a_2) = 0\} = \{(a_1, a_2) \in Z_4 \times Z_6 \mid a_1 = 0\} = \{0\} \times Z_6 = H.$$

Then by Theorem 3.32, we have a group isomorphism

$$\begin{aligned} \mu : (Z_4 \times Z_6)/H &\xrightarrow{\cong} Z_4 \\ (a_1, a_2) + H &\longmapsto a_1, \end{aligned}$$

Since $|Z_4| = 4$, we have that $|Z_4 \times Z_6/H| = 4$. For each $a_1 \in Z_4$, we have a corresponding coset $(a_1, a_2) + H$, where $a_2 \in Z_6$ can be arbitrarily chosen.

Example 3.48. Let us compute the factor group $(Z_4 \times Z_6)/\langle(0,2)\rangle$, where

$$H := \langle(0,2)\rangle = \{(0,0),(0,2),(0,4)\} = \{0\} \times \{0,2,4\} = \{0\} \times K,$$

where $K := \{0,2,4\} \trianglelefteq Z_6$ since Z_6 is abelian and $K \leqslant Z_6$.

Method 1. Similar to Example 3.10, there is a surjective group homomorphism,

$$\begin{aligned} \phi : Z_4 \times Z_6 &\longrightarrow Z_4 \times Z_2 \\ (a_1, a_2) &\longmapsto (a_1, a_2 \pmod 2) \end{aligned}$$

with

$$\mathrm{Ker}(\phi) = \{(a_1, a_2) \in Z_4 \times Z_6 \mid (a_1, a_2 \pmod 2) = 0\} = \{(0,0),(0,2),(0,4)\}.$$

Then by Theorem 3.32, we have a group isomorphism

$$\begin{aligned} \mu : (Z_4 \times Z_6)/H &\xrightarrow{\cong} Z_4 \times Z_2 \\ (a_1, a_2) + H &\longmapsto (a_1, a_2 \pmod 2). \end{aligned}$$

Method 2. Since the surjective group homomorphism

$$\begin{aligned} \varphi : Z_6 &\longrightarrow Z_2 \\ a &\longmapsto a \pmod 2 \end{aligned}$$

has $\mathrm{Ker}(\varphi) = \{0,2,4\} = K$, we have that $Z_6/K \cong Z_2$ by Theorem 3.32. By the following remark, we have that

$$(Z_4 \times Z_6)/(\{0\} \times K) \cong Z_4/\{0\} \times Z_6/K \cong Z_4 \times Z_2,$$

where the fact that if $G \cong G_1$ and $G' \cong G'_1$, then $G \times G' \cong G_1 \times G'_1$, is used in the last isomorphism.

Remark. In fact, if $N \trianglelefteq G$ and $N' \trianglelefteq G'$, then we have a surjective group homomorphism

$$\begin{aligned} \phi : G \times G' &\xrightarrow{\cong} G/N \times G'/N' \\ (g, g') &\longmapsto (gN, g'N'), \end{aligned}$$

with

$$\begin{aligned} \mathrm{Ker}(\phi) &= \{(g, g') \in G \times G' \mid (gN, g'N') = (N, N')\} \\ &= \{(g, g') \in G \times G' \mid gN = N \text{ and } g'N' = N'\} \\ &= \{(g, g') \in G \times G' \mid g \in N \text{ and } g' \in N\} \\ &= \{(g, g') \in N \times N'\} \\ &= N \times N'. \end{aligned}$$

Thus, by Theorem 3.32, we have a group isomorphism

$$\begin{aligned}\mu : (G \times G')/(N \times N') &\xrightarrow{\cong} G/N \times G'/N' \\ (g, g')(N \times N') &\longmapsto (gN, g'N').\end{aligned}$$

Summary 3.49. Let $m, n \in \mathbb{N}$. Let us compute the factor group $Z_m \times Z_n/\langle 0, k\rangle$, where $k \in Z_n$. Note that we have a surjective group homomorphism

$$\begin{aligned}\varphi : Z_n &\longrightarrow Z_{\gcd(k,n)} \\ a &\longmapsto a \pmod{\gcd(k, n)}.\end{aligned}$$

We claim that $\mathrm{Ker}(\varphi) = kZ_n = \langle k\rangle = \{(ik) \pmod n \mid i \in \mathbb{Z}\} =: K$. The second and third equalities follows from definitions.

$\subseteq$ Let $a \in \mathrm{Ker}(\varphi)$. Then $a \pmod{\gcd}(k, n) = 0$, so $a = j \gcd(k, n)$ for some $j \in \mathbb{N}$, and hence $a = j(kx + ny)$ for some $x, y \in \mathbb{Z}$ by Theorem 1.76. Thus, $a = jxk + njy \equiv jxk \pmod n$. Take $i := jx \in \mathbb{Z}$, since $0 \leqslant a \leqslant n - 1$, we have that $a = (jxk) \pmod n = (ik) \pmod n \in K$.

$\supseteq$ Let $r := (ik) \pmod n \in K$ for some $i \in \mathbb{Z}$. Then $r \in \mathbb{Z}$ with $0 \leqslant r \leqslant n - 1$ and there exists $q \in \mathbb{Z}$ such that $ik = nq + r$. Then $r = ik - nq$. Since $\gcd(k, n) \mid k$ and $\gcd(k, n) \mid n$, we have that $\gcd(k, n) \mid r$. Hence $r \pmod{\gcd}(k, n) = 0$, and so $r \in \mathrm{Ker}(\varphi)$.

Therefore, $Z_n/K \cong Z_{\gcd(k,n)}$ by Theorem 3.32. By the above remark, we have that

$$Z_m \times Z_n/\langle 0, k\rangle = (Z_m \times Z_n)/(\{0\} \times K) \cong Z_m/\{0\} \times Z_n/K \cong Z_m \times Z_{\gcd(k,n)}.$$

In particular, if $\gcd(k, n) = 1$, then

$$Z_m \times Z_n/\langle 0, k\rangle \cong Z_m \times Z_{\gcd(k,n)} = Z_m \times Z_1 = Z_m \times \{0\} \cong Z_m.$$

Example 3.50. Let us compute the factor group $(Z_4 \times Z_6)/\langle(2, 3)\rangle$. Since $H := \langle(2, 3)\rangle = \{(0, 0), (2, 3)\}$, we have that $|((Z_4 \times Z_6)/\langle(2, 3)\rangle)| = \frac{24}{2} = 12$.

Method 1. The possible abelian groups of order 12 are $Z_4 \times Z_3$ and $Z_2 \times Z_2 \times Z_3$. Note that the element $(1, 0) \in Z_4 \times Z_3$ is of $|(1, 0)| = \mathrm{lcm}(|1|, |0|) = \mathrm{lcm}(4, 1) = 4$. We claim that no element in $Z_2 \times Z_2 \times Z_3$ has order 4. Suppose that $(a, b, c) \in Z_2 \times Z_2 \times Z_3$ is of $|(a, b, c)| = 4$, then $\mathrm{lcm}(|a|, |b|, |c|) = 4$, so $|a| = 4$ or $|b| = 4$ or $|c| = 4$, contradicting $|a| \leqslant 2$, $|b| \leqslant 2$, and $|c| \leqslant 3$. Thus, the claim holds. Note that in $(Z_4 \times Z_6)/H$, by Lemma 3.45, $4((1, 0) + H) = 4(1, 0) + H = (0, 0) + H$, and $n((1, 0) + H) = n(1, 0) + H = (n, 0) + H \neq (0, 0) + H$ when $1 \leqslant n \leqslant 3$. Hence $|(1, 0) + H| = 4$.

Method 2. Similar to Example 3.10, there is a surjective group homomorphism

$$\begin{aligned}\phi : Z_4 \times Z_6 &\longrightarrow Z_4 \times Z_3 \\ (a_1, a_2) &\longmapsto ((3a_1 + 2a_2) \pmod 4, a_2 \pmod 3)\end{aligned}$$

with

$$\mathrm{Ker}(\phi) = \{(a_1, a_2) \in Z_4 \times Z_6 \mid (3a_1 + 2a_2) \pmod 4, a_2 \pmod 3) = (0, 0)\} = \{(0, 0), (2, 3)\} = H.$$

Then by Theorem 3.32, we have a group isomorphism

$$\begin{aligned}\mu : (Z_4 \times Z_6)/H &\xrightarrow{\cong} Z_4 \times Z_3 \\ (a_1, a_2) + H &\longmapsto ((3a_1 + 2a_2) \pmod 4, a_2 \pmod 3).\end{aligned}$$

Method 3. It follows from that $Z_4 \times Z_3 \cong Z_{12}$ and that we have a surjective group homomorphism

$$\begin{aligned} \phi : Z_4 \times Z_6 &\longrightarrow Z_{12} \\ (a_1, a_2) &\longmapsto (3a_1 + 2a_2) \pmod 1 2 \end{aligned}$$

with

$$\mathrm{Ker}(\phi) = \{(a_1, a_2) \in Z_4 \times Z_6 \mid (3a_1 + 2a_2) \pmod 1 2 = (0, 0)\} = \{(0, 0), (2, 3)\} = H.$$

Remark. Sine $\mathbb{Z}/n\mathbb{Z} \cong Z_n$ for all $n \in \mathbb{N}$, to check ϕ is a group homomorphism, an easy way is to check the following map is a group homomorphism:

$$\begin{aligned} \phi : Z_4 \times Z_6 &\longrightarrow \mathbb{Z}/\mathbb{Z}_4 \times \mathbb{Z}/\mathbb{Z}_3 \\ (a_1, a_2) &\longmapsto (\overline{3a_1 + 2a_2}, \overline{a_2}). \end{aligned}$$

It is straightforward since for $(a_1, a_2), (b_1, b_2) \in Z_4 \times Z_6$,

$$\begin{aligned} \phi((a_1, a_2) + (b_1, b_2)) &= \phi(a_1 + b_1, a_2 + b_2) \\ &= (\overline{3(a_1 + b_1) + 2(a_2 + b_2)}, \overline{a_2 + b_2}) \\ &= (\overline{(3a_1 + 2a_2) + (3b_1 + 2b_2)}, \overline{a_2} + \overline{b_2}) \\ &= (\overline{3a_1 + 2a_2} + \overline{3b_1 + 2b_2}, \overline{a_2} + \overline{b_2}) \\ &= (\overline{3a_1 + 2a_2}, \overline{a_2}) + (\overline{3b_1 + 2b_2}, \overline{b_2}) \\ &= \phi(a_1, a_2) + \phi(b_1, b_2). \end{aligned}$$

Definition 3.51. A group G is <u>simple</u> if $|G| \geqslant 2$ and the only normal subgroups of G are $\{1\}$ and G.

Theorem 3.52. *The alternating group A_n is simple for $n \geqslant 5$.*

Theorem 3.53. *Let $\phi : G \to G'$ be a group homomorphism. If $N \trianglelefteq G$, then $\phi(N) = \mathrm{Im}(\phi|_N) \trianglelefteq \mathrm{Im}(\phi) = \phi(G)$. Also, if $N' \trianglelefteq G'$, then $\phi^{-1}(N') \trianglelefteq G$.*

Remark. $\phi(N)$ may not be a normal subgroup of G' even though ϕ is a group homomorphism and $N \trianglelefteq G$. In Example 2.51, we showed that for $H = \{\rho_0, \mu_1\} \leqslant S_3$, $\rho_1 H \neq H\rho_1$. Hence $H \not\trianglelefteq S_3$. Consider the map A

$$\begin{aligned} \phi : Z_2 &\longrightarrow S_3 \\ 0 &\longmapsto \rho_0 \\ 1 &\longmapsto \mu_1. \end{aligned}$$

Then ϕ is a group homomorphism. We have $Z_2 \trianglelefteq Z_2$, but $\phi(Z_2) = H \not\trianglelefteq S_3$.

Definition 3.54. $M \trianglelefteq G$ is <u>maximal</u> if $M \subsetneq G$ and there is no $N \trianglelefteq G$ such that $M \subsetneq N \subsetneq G$.

Fact 3.55. Let G be a group. Then G is simple if and only if $\{1\} \trianglelefteq G$ is maximal.

Lemma 3.56. Let $N \trianglelefteq G$ and consider the natural group homomorphism

$$\begin{aligned} \gamma : G &\longrightarrow G/N \\ g &\longmapsto gN. \end{aligned}$$

(a) If $N \subseteq M$ and $M \trianglelefteq G$ is maximal, then $\gamma(M) \trianglelefteq G/N$ is maximal.

(b) If $X \trianglelefteq G/N$ is maximal, then $N \subseteq \gamma^{-1}(X)$, and $\gamma^{-1}(X) \trianglelefteq G$ is maximal.

Proof. By Theorem 3.53, we just need to prove the maximalities. □

Theorem 3.57. *$M \trianglelefteq G$ is maximal if and only if G/M is simple.*

Proof. $\Longrightarrow$ Consider the natural group homomorphism

$$\begin{aligned} \gamma : G &\longrightarrow G/M \\ g &\longmapsto gM. \end{aligned}$$

Since $M \subseteq M$ and $M \trianglelefteq G$ is maximal, we have that $\{M\} = \gamma(M) \trianglelefteq G/M$ is maximal by Lemma 3.56(a). So G/M is simple by fact 3.55.

$\Longleftarrow$ By Fact 3.55, $\{M\} \trianglelefteq G/M$ is maximal. Then $M = \gamma^{-1}(\{M\}) \trianglelefteq G$ is maximal by Lemma 3.56(b). □

Example 3.58. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is maximal if and only if $\mathbb{Z}/n\mathbb{Z} \cong Z_n$ is simple if and only if n is prime.

Definition 3.59. Let G be a group. Then the <u>center</u> $Z(G)$ is defined by

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Remark. We have that $1 \in Z(G)$. If $Z(G) = \{1\}$, we say that the center of G is <u>trivial</u>.

Fact 3.60. Let G be a group. Then G is abelian if and only if $Z(G) = G$.

Theorem 3.61. *Let $G_1, \cdots, G_n$ be groups. Then*

$$Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n).$$

Proof.

$$\begin{aligned} (g_1, \ldots, g_n) \in Z(G_1 \times \cdots \times G_n) &\iff (g_1, \ldots, g_n)(h_1, \ldots, h_n) = (h_1, \ldots, h_n)(g_1, \ldots, g_n), \\ &\qquad \forall (h_1, \ldots, h_n) \in G_1 \times \cdots \times G_n \\ &\iff (g_1h_1, \ldots, g_nh_n) = (h_1g_1, \ldots, h_ng_n), \\ &\qquad \forall (h_1, \ldots, h_n) \in G_1 \times \cdots \times G_n \\ &\iff g_1h_1 = h_1g_1, \cdots, g_nh_n = h_ng_n, \\ &\qquad \forall h_1 \in G_1, \cdots, h_n \in G_n \\ &\iff g_1 \in Z(G_1), \cdots, g_n \in Z(G_n) \\ &\iff (g_1, \ldots, g_n) \in Z(G_1) \times \cdots \times Z(G_n). \end{aligned}$$

Hence $Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n)$. □

Corollary 3.62. Let $G_1, \cdots, G_n$ be groups. Then $G_1 \times \cdots \times G_n$ is abelian if and only if $G_1, \ldots, G_n$ are abelian.

Theorem 3.63. *If G is a nonabelian group of order pq with p, q primes, then $Z(G) = \{1\}$.*

Example 3.64. Since S_3 is nonabelian of $|S_3| = 6 = 2(3)$, we have that $Z(S_3) = \{\rho_0\}$. Consequently,

$$Z(S_3 \times Z_5) = Z(S_3) \times Z(Z_5) = \{\rho_0\} \times Z_5 \cong Z_5.$$

Theorem 3.65. *Let G be a group. Then $Z(G) \trianglelefteq G$ and $Z(G)$ is abelian.*

Definition 3.66. Let G be a group. An element $[a, b] = aba^{-1}b^{-1}$ is called a commutator of $a, b \in G$. Define $[G, G] = \langle [a, b] \mid a \in G, b \in G \rangle$, the commutator subgroup of G.

Proposition 3.67. Let $a, b \in G$. Then $[a, b]ba = ab = ba[a^{-1}, b^{-1}]$.

Theorem 3.68. *Let G be a group. Then $[G, G] \trianglelefteq G$.*

Proof. By definition, $[G, G]$ is a group. Also, since $[G, G] \subseteq G$, we have that $[G, G] \leqslant G$. Let $[a, b] \in [G, G]$. Then for $g \in G$,

$$\begin{aligned} g[a, b]g^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= gaba^{-1}(g^{-1}b^{-1}bg)b^{-1}g^{-1} \\ &= (gaba^{-1}g^{-1}b^{-1})(bgb^{-1}g^{-1}) \\ &= ((ga)b(ga)^{-1}b^{-1})(bgb^{-1}g^{-1}) \\ &= [ga, b][b, g] \\ &\in [G, G], \end{aligned}$$

since $[G, G]$ is a group and $[ga, b], [b, g] \in [G, G]$. Let $x \in [G, G] = \langle [a, b] \mid a \in G \text{ and } b \in G \rangle$. Then by Definition 2.77, $x = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n]$ for some $n \in \mathbb{N}$ and $[a_i, b_i] \in [G, G]$. Note that

$$\begin{aligned} gxg^{-1} &= g[a_1, b_1][a_2, b_2] \cdots [a_n, b_n]g^{-1} \\ &= g[a_1, b_1](g^{-1}g)[a_2, b_2](g^{-1}g) \cdots (g^{-1}g)[a_n, b_n]g^{-1} \\ &= (g[a_1, b_1]g^{-1})(g[a_2, b_2]g^{-1}) \cdots (g[a_n, b_n]g^{-1}) \\ &\in [G, G], \end{aligned}$$

since $g[a_i, b_i]g^{-1} \in [G, G]$ for all i and $[G, G]$ is a group. Hence $g[G, G]g^{-1} \subseteq [G, G]$, and so $[G, G] \trianglelefteq G$ by Theorem 3.37. □

Theorem 3.69. *If $N \trianglelefteq G$, then G/N is abelian if and only if $[G, G] \leqslant N$.*

Proof. $\Longrightarrow$ Let $[a, b] \in [G, G]$. Then $a, b, a^{-1}, b^{-1} \in G$. Since G/N is abelian, $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$, i.e., $(a^{-1}b^{-1})N = (b^{-1}a^{-1})N$. Hence $[a, b] = aba^{-1}b^{-1} = (b^{-1}a^{-1})^{-1}(a^{-1}b^{-1}) \in N$ by Proposition 3.31(a).

$\Longleftarrow$ Let $aN, bN \in G/N$. Then

$$(aN)(bN) = (ab)N = (ba[a^{-1}, b^{-1}])N = (ba)([a^{-1}, b^{-1}]N) = (ba)N = (bN)(aN),$$

where the the third equality follows from Proposition 3.67 and the fourth equality follows from that $[a^{-1}, b^{-1}] \in [G, G] \subseteq N$. □

Example 3.70. Since $\rho_1 = [\rho_2, \mu_1] \in [S_3, S_3]$ and $\rho_2 = [\rho_1, \mu_1] \in [S_3, S_3]$, we have that $A_3 = \{\rho_0, \rho_1, \rho_2\} \subseteq [S_3, S_3]$. By Example 3.43, $A_3 \trianglelefteq S_3$. But $|S_3/A_3| = \frac{|S_3|}{|A_3|} = 2$, so $S_3/A_3 \cong Z_2$, and hence S_3/A_3 is abelian. Thus, $[S_3, S_3] \subseteq A_3$ by Theorem 3.69. Therefore, $[S_3, S_3] = A_3$.

3.4 Group action on a set

Definition 3.71. Let X be a set and G a group. An action of G on X is a map

$$\begin{aligned} * : G \times X &\longrightarrow X \\ (g, x) &\longmapsto *(g, x) = g * x \end{aligned}$$

such that

(a) $1 * x = x$ for all $x \in X$,

(b) $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a G-set.

Example 3.72. Let X be a set and $H \leqslant S_X$. Consider the map

$$\begin{aligned} * : H \times X &\longrightarrow X \\ (\sigma, x) &\longmapsto \sigma(x). \end{aligned}$$

Note that

(a) $\mathrm{id}_X * x = \mathrm{id}_X(x) = x$ for all $x \in X$,

(b) $(\sigma_1 \sigma_2) * x = (\sigma_1 \sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_1 * (\sigma_2 * x)$ for all $x \in X$ and all $g_1, g_2 \in G$, where the second equality follows from that permutation multiplications are function compositions.

Thus, X is a H-set.

Theorem 3.73. *Let X be a G-set. For each $g \in G$, define*

$$\begin{aligned} \sigma_g : X &\longrightarrow X \\ x &\longmapsto g * x. \end{aligned}$$

(a) $\sigma_g \in S_X$ for $g \in G$.

(b) The function

$$\begin{aligned} \phi : G &\longrightarrow S_X \\ g &\longmapsto \sigma_g \end{aligned}$$

is a group homomorphism with

$$\mathrm{Ker}(\phi) = \{g \in G \mid g * x = x, \forall x \in X\}.$$

Proof. (a) For $x \in X$,

$$(\sigma_{g^{-1}} \sigma_g)(x) = \sigma_{g^{-1}}(\sigma_g(x)) = g^{-1} * (g * x) = (g^{-1} g) * x = 1 * x = x = \mathrm{id}_X(x),$$

where the third equality follows from that X is a G-set. Hence $\sigma_{g^{-1}} \circ \sigma_g = \mathrm{id}_X$. Interchange the role of g and g^{-1} to obtain $\sigma_g \circ \sigma_{g^{-1}} = \mathrm{id}_X$. Thus, $\sigma_g : X \to X$ is a bijection and hence $\sigma_g \in S_X$.

(b) By (a), $\sigma_g \in S_X$, so ϕ is well-defined. Let $g_1, g_2 \in G$. Then for $x \in X$,

$$\phi(g_1g_2)(x) = \sigma_{g_1g_2}(x) = (g_1g_2) * x = g_1 * (g_2 * x) = \sigma_{g_1}(\sigma_{g_2}(x)) = (\sigma_{g_1}\sigma_{g_2})(x) = (\phi(g_1)\phi(g_2))(x),$$

where the third equality follows from that X is a G-set and the fifth equality folows from that permutation multiplications are function compositions. Hence $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$, and so ϕ is a group homomorphism.

$$\mathrm{Ker}(\phi) = \{g \in G \mid \sigma_g = \mathrm{id}\} = \{g \in G \mid \sigma_g(x) = \mathrm{id}_X(x), \forall x \in X\} = \{g \in G \mid g * x = x, \forall x \in X\}.$$

□

Remark. From Theorem 3.73, we have that

$$\begin{aligned} * : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g * x = \sigma_g(x). \end{aligned}$$

So actions of G on X is essentially the action of $\phi(G)$ on X, where $\phi(G) = \{\sigma_g \mid g \in G\} \leqslant S_X$.

$$\begin{aligned} * : \phi(G) \times X &\longrightarrow X \\ (\sigma_g, x) &\longmapsto \sigma_g(x). \end{aligned}$$

By Example 3.72, X is also a $\phi(G)$-set. When studying the set X, actions using subgroups of S_X suffice. However, sometimes a set X is used to study G via a group action of G on X.

Remark. By Theorem 3.32, with $N = \mathrm{Ker}(\phi)$ we have a group isomorphism

$$\begin{aligned} \mu : G/N &\xrightarrow{\cong} \phi(G) \\ gN &\longmapsto \sigma_g. \end{aligned}$$

Hence we can regard X as a G/N-set, where

$$\begin{aligned} * : G/N \times X &\longrightarrow X \\ (gN, x) &\longmapsto \sigma_g(x) = g * x. \end{aligned}$$

Definition 3.74. Let X be a G-set. We say that G <u>acts faithful</u> on X if

$$\{g \in G \mid g * x = x, \forall x \in X\} = \{1\}.$$

We say a group G is <u>transitive</u> on X if for each $x_1, x_2 \in X$, there exists $g \in G$ such that $g * x_1 = x_2$.

Remark. G acts faithful on X if and only if $\mathrm{Ker}(\phi) = \{1\}$ in Theorem 3.73.

Proposition 3.75. Let X be a G-set. G is transitive on X if and only if $\phi(G)$ is transitive on X in Theorem 3.73.

Example 3.76. G is itself a G-set, where

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (g_1, g_2) &\longmapsto g_1 * g_2 = \lambda_{g_1}(g_2) = g_1g_2. \end{aligned}$$

If $H \leqslant G$, then G is also an H-set, where

$$\begin{aligned} * : H \times G &\longrightarrow G \\ (h, g) &\longmapsto hg \end{aligned}$$

Example 3.77. Let $H \leqslant G$. Then G is an H-set under conjugation, where

$$\begin{aligned} * : H \times G &\longrightarrow G \\ (h, g) &\longmapsto hgh^{-1}. \end{aligned}$$

(a) $1 * g = 1g1^{-1} = g$ for all $g \in G$,

(b) For all $g \in G$ and all $h_1, h_2 \in H$,

$$(h_1h_2) * g = (h_1h_2)g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1} = h_1(h_2 * g)h_1^{-1} = h_1 * (h_2 * g).$$

Example 3.78. Let V be an F-vector space, where F is $\mathbb{R}$ or $\mathbb{C}$. Then V is an F^*-set, where

$$\begin{aligned} * : F \times V &\longrightarrow V \\ (r, \boldsymbol{v}) &\longmapsto r\boldsymbol{v}. \end{aligned}$$

It follows from the two axioms

$$(rs)\boldsymbol{v} = r(s\boldsymbol{v}), \forall r, s \in F \text{ and } \forall \boldsymbol{v} \in V$$

and

$$1\boldsymbol{v} = \boldsymbol{v}, \forall \boldsymbol{v} \in V.$$

Example 3.79. Let $H \leqslant G$. Then $G//H$ is a G-set, where

$$\begin{aligned} * : G \times G//H &\longrightarrow G//H \\ (g, xH) &\longmapsto (gx)H. \end{aligned}$$

Let $(g, xH), (g, yH)$ be such that $(g, xH) = (g, yH)$. Then $xH = yH$, so $y = xh$ for some $h \in H$, and hence

$$*(g, yH) = g * (yH) = (gy)H = (gxh)H = (gx)(hH) = (gx)H = g * (xH) = *(g, xH).$$

Thus, the action $*$ is well-defined.

(a) $1 * (xH) = (1x)H = xH$ for all $xH \in G//H$,

(b) For all $xH \in G//H$ and all $g_1, g_2 \in G$,

$$(g_1g_2) * (xH) = (g_1g_2x)H = (g_1(g_2x))H = g_1 * ((g_2x)H) = g_1 * (g_2 * (xH)).$$

Example 3.80. Let G be the group $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$ of symmetries of the square. In Figure 3.1, we show the square with vertices 1,2,3,4 as in Figure 2.1. We also label the sides s_1, s_2, s_3, s_4, the diagonals d_1 and d_2, vertical and horizontal axes m_1 and m_2, the center point C, and midpoints P_i of the sides s_i. Recall that ρ_i corresponds to rotating the square counterclockwise through $\pi i/2$ radians, μ_i corresponds to flipping on the axis m_i, and δ_i to flipping on the diagonal d_i. We let

$$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}.$$

Then X can be regarded as a D_4-set in a natural way. Table 3.3 describes completely the action of D_4 on X and is given to provide geometric illustrations of ideas to be introduced. We should be sure that we understand how this table is formed before continuing.

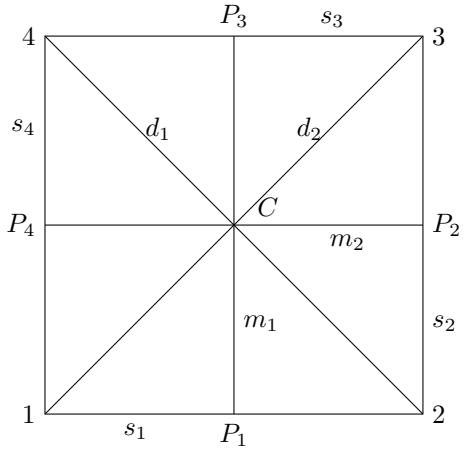


Figure 3.1

Table 3.3

	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_0	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_1	2	3	4	1	s_2	s_3	s_4	s_1	m_2	m_1	d_2	d_1	C	P_2	P_3	P_4	P_1
ρ_2	3	4	1	2	s_3	s_4	s_1	s_2	m_1	m_2	d_1	d_2	C	P_3	P_4	P_1	P_2
ρ_3	4	1	2	3	s_4	s_1	s_2	s_3	m_2	m_1	d_2	d_1	C	P_4	P_1	P_2	P_3
μ_1	2	1	4	3	s_1	s_4	s_3	s_2	m_1	m_2	d_2	d_1	C	P_1	P_4	P_3	P_2
μ_2	4	3	2	1	s_3	s_2	s_1	s_4	m_1	m_2	d_2	d_1	C	P_3	P_2	P_1	P_4
δ_1	3	2	1	4	s_2	s_1	s_4	s_3	m_2	m_1	d_1	d_2	C	P_2	P_1	P_4	P_3
δ_2	1	4	3	2	s_4	s_3	s_2	s_1	m_2	m_1	d_1	d_2	C	P_4	P_3	P_2	P_1

Definition 3.81. Let X be a G-set. Let $x \in X$ and $g \in G$. Let

$$X_g = \{x \in X \mid g * x = x\} \text{ and } G_x = \{g \in G \mid g * x = x\}.$$

Example 3.82. For the D_4-set X in Example 3.1, we have

$$X_{\rho_0} = X, \quad X_{\rho_1} = \{C\}, \quad X_{\mu_1} = \{s_1, s_3, m_1, m_2, C, P_1, P_3\}.$$

Also, with $G = D_4$,

$$G_1 = \{\rho_0.\delta_2\}, \quad G_{s_3} = \{\rho_0, \mu_1\}, \quad G_{d_1} = \{\rho_0, \rho_2, \delta_1, \delta_2\}.$$

Theorem 3.83. *Let X be a G-set. Then $G_x \leqslant G$ for each $x \in X$.*

Proof. Let $x \in X$ and $g_1, g_2 \in G_x$. Then $g_1 * x = x = g_2 * x$, and $(g_1 g_2) * x = g_1 * (g_2 * x) = g_1 * x = x$, and hence $g_1 g_2 \in G_x$. Thus, G_x is a binary structure. Since $1 * x = x$, we have that $1 \in G_x$. If $g \in G_x$, then $g * x =$, so $g^{-1} * x = g^{-1} * (g * x) = (g^{-1} g) * x = 1 * x = x$, and consequently $g^{-1} \in G_x$. Thus, $G_x \leqslant G$. □

Definition 3.84. Let X be a G-set and $x \in X$. The subgroup G_x is the isotropy subgroup of x.

Theorem 3.85. *Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $g * x_1 = x_2$. Then $\sim$ is an equivalence relation on X.*

Proof. (Reflexive) For $x \in X$, we have that $1 * x = x$.

(Symmetric) Assume that $x_1 \sim x_2$. Then $g * x_1 = x_2$ for some $g \in G$, and so $g^{-1} * x_2 = g^{-1} * (g * x_1) = (g^{-1} g) * x_1 = 1 * x_1 = x_1$, and hence $x_2 \sim x_1$.

(Transitive) If $x_1 \sim x_2$ and $x_2 \sim x_3$, then $g_1 * x_1 = x_2$ and $g_2 * x_2 = x_3$ for some $g_1, g_2 \in G$. Then $(g_2 g_1) * x_1 = g_2 (g_1 * x_1) = g_2 * x_2 = x_3$, and so $x_1 \sim x_3$. □

Definition 3.86. Let X be a G-set. Each cell in the partition of the equivalence relation described in Theorem 3.85 is an orbit in X under G. If $x \in X$, the cell $\bar{x}$ containing x is the orbit of x. We let this cell be $G * x$ i.e.,

$$G * x = \bar{x} = \{g * x \mid g \in G\}.$$

The relationship between the orbits in X and the group structure of G lies at the heart of the applications that appear in next section.

Theorem 3.87. *Let X be a G-set and $x \in X$. Then $|G * x| = [G : G_x]$. If $|G| < \infty$, then $|G_x| \mid |G|$.*

Proof. Define

$$\begin{aligned} \phi : G * x &\longrightarrow G//G_x \\ g * x &\longmapsto g G_x. \end{aligned}$$

Let $g * x, h * x \in G * x$. Then

$$\begin{aligned} g * x = h * x &\iff h^{-1} * (g * x) = h^{-1} * (h * x) \\ &\impliedby h^{-1} g * x = x \\ &\iff h^{-1} g \in G_x \\ &\iff g G_x = h G_x. \end{aligned}$$

So ϕ is well-defined and is 1-1. The ontoness is straightforward. Thus, φ is bijective. □

Corollary 3.88. Let X be a G-set and $x \in X$. For $h \in G$,

$$\{g \in G \mid g * x = h * x\} = h G_x.$$

Proof. By the proof of Theorem 3.87,

$$g * x = h * x \iff g G_x = h G_x \iff g \in h G_x.$$ □

Remark. When $h = 1$, it is the form of the definition of G_x.

Corollary 3.89. Let X be a G-set and $x \in X$. For $y \in G * x$,

$$G * y = G * x.$$

Proof. Note that $y = g_1 * x$ for some $g_1 \in G$. Then

$$\begin{aligned} G * y &= \{g * y \mid g \in G\} \\ &= \{g * (g_1 * x) \mid g \in G\} \\ &= \{(gg_1) * x \mid g \in G\} \\ &= \{g * x \mid g \in G\} \\ &= G * x, \end{aligned}$$

where the fourth equality follows from that $\rho_{g_1} : G \to G$ given by $g \to gg_1$ is a bijection. □

Example 3.90. Let X be the D_4-set in Example 3.80. With $G = D_4$, we have $G * 1 = \{1, 2, 3, 4\}$ and $G_1 = \{\rho_0, \delta_2\}$. Since $|G| = 8$, we have that $|G * 1| = [G : G_1] = \frac{|G|}{|G_1|} = \frac{8}{2} = 4$.

3.5 Application of G-sets to counting

Theorem 3.91 (Burnside's Formula)**.** *Let G be a finite group and X a finite G-set. If $r := |\{G * x \mid x \in X\}|$, i.e., r is the number of orbits in X under G, then*

$$r \cdot |G| = \sum_{g \in G} |X_g|.$$

Proof. Let

$$N = |\{(g, x) \in G \times X \mid g * x = x\}|.$$

Then

$$\sum_{g \in G} |X_g| = N = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|G * x|} = |G| \sum_{x \in X} \frac{1}{|G * x|},$$

where the third equality follows from Theorem 3.87. Now $\frac{1}{|G*x|}$ has the same value for all y in the same orbit $G * x$, then

$$\sum_{y \in G*x} \frac{1}{|G * x|} = 1.$$

Let $x_1, \ldots, x_r$ be the representatives of the r orbits, then by Corollary 3.89, $X = \bigsqcup_{i=1}^{r} G * x_i$, i.e., X is the disjoint union of the $G * x_i$'s. Thus, by splitting the summation over x into r parts, we get

$$\sum_{g \in G} |X_g| = |G| \sum_{x \in X} \frac{1}{|G * x|} = |G| \sum_{i=1}^{r} \sum_{y \in G*x_i} \frac{1}{|G * x_i|} = |G| \sum_{i=1}^{r} 1 = r \cdot |G|.$$ □

Corollary 3.92. If G is a finite group and X a finite G-set, then

$$|\{G * x \mid x \in X\}| = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Example 3.93. Suppose that we wish to count how many distinguishable ways the six faces of a cube can be marked with from one to six dots to form a die. Let us distinguish between the faces of the cube for the moment and call them the bottom(bm), top(tp), left(lt), right(rt), front(ft), and back(bk). Then the bottom can have any one of six marks from one dot to six dots, the top any one of the five remaining marks, and so on. There are $6! = 720$ ways the cube faces can be marked in all. We consider X to be the set of these 720 possible ways. Some markings yield the same die as others, in the sense that one marking can be carried into another by a rotation of the marked cube.

There are 24 possible positions of a cube on a table, for any one of six faces can be placed down, and the any one of four to the front, giving $6(4) = 24$ possible positions. Let

$$G = \left\{ \begin{array}{cccc} \{bm, ft\}, & \{bm, lt\}, & \{bm, rt\}, & \{bm, bk\}, \\ \{tp, ft\}, & \{tp, lt\}, & \{tp, rt\}, & \{tp, bk\}, \\ \{lt, ft\}, & \{lt, bm\}, & \{lt, tp\}, & \{lt, bk\}, \\ \{rt, ft\}, & \{rt, bm\}, & \{rt, tp\}, & \{rt, bk\}, \\ \{ft, lt\}, & \{ft, rt\}, & \{ft, bm\}, & \{ft, tp\}, \\ \{bk, lt\}, & \{bk, rt\}, & \{bk, bm\}, & \{bk, tp\} \end{array} \right\}.$$

For an element (a, b) in G, the first spot denotes that we put the face a to the bottom and put the face b to the front. We consider two markings to give the same die if one can be carried into the other under action by an element of G. For example, we have a marking x that 6 is on the bottom, 2 is toward the font, 3 is on the left, 4 is on the right, 5 is on the back, and 1 is on the top, then it can be carried into the marking that 1 is on the bottom, 2 is toward the font, 3 is on the left, 4 is on the right, 5 is on the back, and 6 is on the top under $\{tp, ft\}$. In other words, we consider each orbit in X under G to correspond to a single die, and differentiable orbits to give differentiable dice. We have that $|X_g| = 0$ for $g \in G \setminus \{1\}$, and $|X_1| = 720$. Thus,

$$\sharp \text{orbits} = \frac{1}{24}720 = 30.$$

Example 3.94. How many distinguishable ways can seven people be seated at a round table, where there is no distinguishable "head" to the table? There are 7! ways ti assign to the different chairs. A rotation of people achieved by asking each person to move one place to the right results in the same arrangement. Such a rotation generates a cyclic group G of order 7, which we consider to act on X in the obvious way. We have that $|X_g| = 0$ for $g \in G \setminus \{1\}$, and $|X_1| = 7!$. Thus,

$$\sharp \text{orbits} = \frac{1}{7}7! = 6! = 120.$$

Example 3.95. Let us find the number of distinguishable ways the edges of an equilateral triangle can be painted if four different colors of paint are available, assuming only one color is used on each edge, and the same color may be used on different edges.

There are $4^3 = 64$ ways of painting the edges in all. We consider X to be the set of these 64 possible painted triangles. The group G acting on X is the group symmetries of the triangle, which is isomorphic to S_3, and which we consider to be S_3. Note that $|X_{\rho_0}| = 64$, $|X_{\rho_1}| = 4 = |X_{\rho_2}|$, because to be invariant under ρ_i for $i = 1, 2$, all edges must be the same color, and there are 4 possible colors. $|X_{\mu_1}| = 16 = X_{\mu_2} = X_{\mu_2}$, since the edges that are interchanged must be the same color (4 possibilities) and the other edge may also be any of the colors (times 4 possibilities). Then

$$\sum_{g \in S_3} |X_g| = 64 + 4 + 4 + 16 + 16 + 16 = 120.$$

Thus,

$$\sharp \text{orbits} = \frac{1}{6}120 = 20,$$

so there are 20 distinguishable triangles.

Example 3.96. We repeat Example 3.95, with the assumption that a different color is used on each edge. The number of possible ways of painting the edges is then $4(3)(2) = 24$, and we let X be the set of 24 possible painted triangles. Again, the group acting on X can be considered to be S_3. Since all edges are a different color, we see that $|X_{\rho_0}| = 24$ while $|X_g| = 0$ for $g \in S_3 \setminus \{\rho_0\}$. Thus,

$$\sharp \text{orbits} = \frac{1}{6}24 = 4,$$

so there are four distinguishable triangles.

Chapter 4

Rings and Fields

4.1 Rings and fields

Definition 4.1. A ring $\langle R, +, \cdot \rangle$ is a set R together with two binary structures $\langle R, + \rangle$ and $\langle R, \cdot \rangle$ such that the following axioms are satisfied:

(a) $\mathscr{R}_1$: $\langle R, + \rangle$ is an abelian group.

(b) $\mathscr{R}_2$: $\cdot$ is associative.

(c) $\mathscr{R}_3$: For all $a, b, c \in R$, the left distributive law $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the right distributive law $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Example 4.2. $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$ are rings.

Remark. It is customary to denote multiplication in a ring by juxtaposition, using ab in place of $a \cdot b$. We shall also observe that the usual convention that multiplication is performed before addition in the absence of parentheses, so the left distributive law, for example, becomes

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

without the parentheses on the right side of the equation. Also, as a convenience analogous to our notation in group theory, we shall somewhat incorrectly refer to a ring R in place of a ring $\langle R, +, \cdot \rangle$, provided that no confusion will result. In particular, from now on $\mathbb{Z}$ will always be $\langle \mathbb{Z}, +, \cdot \rangle$, and $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ will also be the rings in Example 4.2.

Example 4.3. Let R be a ring and $\mathrm{Mat}_n(R)$ the collection of all $n \times n$ matrices having elements of R as entries. Since $\langle R, + \rangle$ is abelian, we have that $\mathrm{Mat}_n(R)$ is abelian. The associativity of matrix multiplication and the two distributive laws in $\mathrm{Mat}_n(R)$ follow from the same properties in R. In particular, we have the rings $\mathrm{Mat}_n(\mathbb{Z})$, $\mathrm{Mat}_n(\mathbb{Q})$, $\mathrm{Mat}_n(\mathbb{R})$, and $\mathrm{Mat}_n(\mathbb{C})$. Note that multiplication is not a commutative operation in any of these rings for $n \geqslant 2$.

Example 4.4. (a) Let $F = \{f : \mathbb{R} \to \mathbb{R}\}$. Then $\langle F, +, \circ \rangle$ is a ring, where $\circ$ on F is the function composition.

(b) Let $F = \{f : \mathbb{R} \to \mathbb{R}\}$. Then $\langle F, +, \cdot \rangle$ is a ring, where for $f, g \in F$,

$$\begin{aligned} fg : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x)g(x). \end{aligned}$$

Example 4.5. $\langle n\mathbb{Z}, +, \cdot \rangle$ is a ring, because $\langle n\mathbb{Z}, + \rangle$ is an abelian group, $\langle n\mathbb{Z}, \cdot \rangle$ is a binary structure, and the associative and distributive laws inherit from the ones in $\mathbb{Z}$ since $n\mathbb{Z} \subseteq \mathbb{Z}$ and $\mathbb{Z}$ is a ring.

Example 4.6. Let $n \in \mathbb{N}$. The cyclic group $\langle Z_n, +, \cdot \rangle$ is a ring, where

$$a \cdot b = (ab) \pmod{n}.$$

From now on, Z_n will always be the ring $\langle Z_n, +, \cdot \rangle$.

Definition 4.7. Let $R_1, \ldots, R_n$ be rings. The direct product $R_1 \times \cdots \times R_n$ of rings R_i is a ring under addition and multiplication by components.

Remark. Continuing matters of notation, we shall always let 0 be the additive identity of a ring R. The additive inverse of an element of a of a ring is $-a$.

Convention 4.8. For $a \in R$, and $n \in \mathbb{N}$, define

$$\begin{aligned} 0_{\mathbb{Z}} \cdot a &= 0_R, \\ n \cdot a &= \underbrace{a + \cdots + a}_{n \text{ times}}, \\ -n \cdot a &= \underbrace{(-a) + \cdots + (-a)}_{n \text{ times}} = n(-a). \end{aligned}$$

Here $m \cdot a$ with $m \in \mathbb{Z}$ is not to be constructed as a multiplication of m and a in the ring R, for the m may not be in the ring at all.

Theorem 4.9. *If R is a ring, then for any $a, b \in R$, we have that*

(a) $0a = a0 = 0$,

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

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

Proof. (a) Note that $a0 + a0 = a(0 + 0) = a0 = 0 + a0$, then by cancellation law for the additive group $(R, +)$, we have that $a0 = 0$. Likewise, $0a = 0$.

(b) To prove $a(-b)$ is the additive inverse of ab, it is enough to show that

$$a(-b) + ab = 0 = ab + a(-b),$$

which is true since by the left distributive law and by (a),

$$a(-b) + ab = a(-b + b) = a0 = 0 = a0 = a(b + (-b)) = ab + a(-b).$$

(c) By (b),

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

where the last equality follows from Corollary 1.34. □

Definition 4.10. For rings R and R', a map $\phi : R \to R'$ is a ring homomorphism if the following two conditions are satisfied for all $a, b \in R$:

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

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

Remark. ϕ is 1-1 if and only if $\text{Ker}(\phi) = \{0\}$. $\langle R/\text{Ker}(\phi), +\rangle$ is a factor group. We will see that $\langle R/\text{Ker}(\phi), +, \cdot\rangle$ is a factor ring.

Example 4.11. Let $\langle F, +, \cdot\rangle$ be the ring in Example 4.4(b) and $a \in \mathbb{R}$. Then the evaluation homomorphism

$$\begin{aligned} \phi_a : F &\longrightarrow \mathbb{R} \\ f &\longmapsto f(a) \end{aligned}$$

is a ring homomorphism.

Example 4.12. The map

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow Z_n \\ a &\longmapsto a \pmod n \end{aligned}$$

is a ring homomorphism. By Example 3.10, it is enough to show that $\phi(ab) = \phi(ab)$ for $a, b \in \mathbb{Z}$. Write $a = q_1 n + r_1$ and $b = q_2 n + r_2$ by the division algorithm. Then

$$ab = n(q_1 q_2 n + r_1 q_2 + q_1 r_2) + r_1 r_2 = n(q_1 q_2 n + r_1 q_2 + q_1 r_2) + q_3 n + r_3,$$

where by division algorithm $r_1 r_2 = q_3 n + r_3$. Hence

$$\phi(ab) \equiv ab \equiv r_3 \equiv r_1 r_2 \equiv \phi(a)\phi(b) \pmod n.$$

Example 4.13 (Projection Homomorphisms)**.** Let $R_1, \cdots, R_n$ be rings. For each i, the map

$$\begin{aligned} \pi_i : R_1 \times \cdots R_n &\longrightarrow R_i \\ (r_1, \ldots, r_n) &\longmapsto r_i \end{aligned}$$

is a ring homomorphism, projection onto the i^{th} component.

Definition 4.14. A ring isomorphism $\phi : R \to R'$ is a ring homomorphism that is bijective, written as $\phi : R \xrightarrow{\cong} R'$. The rings R and R' are then isomorphic, written as $R \cong R'$.

Remark. We will see that there are ring isomorphisms

$$\begin{aligned} Z_n &\xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z} \\ a &\longmapsto a + n\mathbb{Z} \end{aligned} \qquad \begin{aligned} \mathbb{Z}/\mathbb{Z}_n &\xrightarrow{\cong} Z_n \\ a + n\mathbb{Z} &\longmapsto a \pmod n. \end{aligned}$$

Theorem 4.15. *Let $\mathcal{S}$ be a collection of rings such that for any $S, T \in \mathcal{S}$, we have that $S \cong T$, then $\cong$ is an equivalence relation on $\mathcal{S}$.*

Example 4.16. The map

$$\begin{aligned} \mathbb{Z} &\longrightarrow 2\mathbb{Z} \\ x &\longmapsto 2x \end{aligned}$$

is a additive group isomorphism, but not a ring isomorphism because $\phi(xy) = 2xy \neq (2x)(2y) = \phi(x)\phi(y)$ for $x, y \in \mathbb{Z}^*$.

Definition 4.17. $\{0\}$ is the zero ring. Here 0 acts as multiplicative as well as additive identity.

Remark. Theorem 1.20 shows that if a ring has a multiplicative identity element 1, then it is unique.

Remark. Let R be a ring and $1 \in R$. Then $1 = 0$ if and only if R is a zero ring.

Definition 4.18. A ring in which the multiplication is commutative is a commutative ring. A ring with a multiplicative identity is a ring with unity; the multiplicative identity element 1 is called "unity".

Remark.

$$(\underbrace{1 + \cdots + 1}_{n \text{ times}})(\underbrace{1 + \cdots + 1}_{m \text{ times}}) = \underbrace{1 + \cdots + 1}_{nm \text{ times}},$$

i.e.,

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

Example 4.19. Let $r, s \in \mathbb{Z}$ be such that $\gcd(r, s) = 1$. Then

$$\begin{aligned} \phi : Z_{rs} &\longrightarrow Z_r \times Z_s \\ n &\longmapsto (n \pmod r, n \pmod s) \\ \text{or } n &\longmapsto n \cdot (1, 1) \end{aligned}$$

is a ring homomorphism. Let $m, n \in Z_{rs}$. Then

$$\begin{aligned} \phi(m + n) &= (m + n) \cdot (1, 1) \\ &= ((m + n) \cdot 1 \pmod r, (m + n) \cdot 1 \pmod s) \\ &= (m \cdot 1 \pmod r, m \cdot 1 \pmod s) + (n \cdot 1 \pmod r, n \cdot 1 \pmod s) \\ &= m \cdot (1, 1) + n \cdot (1, 1) \\ &= \phi(m) + \phi(n). \end{aligned}$$

and

$$\begin{aligned} \phi(mn) &= mn \cdot (1, 1) \\ &= (mn \cdot 1 \pmod r, mn \cdot 1 \pmod s) \\ &= ((m \cdot 1)(n \cdot 1) \pmod r, (m \cdot 1)(n \cdot 1) \pmod s) \\ &= (m \cdot 1 \pmod r, m \cdot 1 \pmod r)(n \cdot 1 \pmod r, n \cdot 1 \pmod s) \\ &= (m \cdot (1, 1))(n \cdot (1, 1)) \\ &= \phi(m)\phi(n) \end{aligned}$$

Fact 4.20. A direct product $R_1 \cdots \times \cdots \times R_n$ of rings is commutative or has unity if and only if each R_i is commutative or has unity, respectively.

Definition 4.21. Let R be a ring with unity $1 \neq 0$. An element u in R is a unit of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a division ring (or skew field). A field is a commutative division ring. A noncommutative division ring is called a "strictly skew field".

Example 4.22. (a) $\mathbb{Z}$ is not a field because 2, for example, has no multiplicative inverse, so 2 is not a unit in $\mathbb{Z}$.

(b) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

Example 4.23. Let $n \in \mathbb{N}$. The units in Z_n are precisely those $m \in Z_n \setminus \{0\}$ such that $\gcd(m, n) = 1$ by the remark after Example 1.88. Thus, Z_n is a field if and only if n is a prime.

Definition 4.24. A subring of a ring is a subset of the ring that is a ring under induced operations from the whole ring; a subfield is defined similarly for a subset of a field.

4.2 Integral domains

Definition 4.25. If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are 0 divisors.

Remark. $a \in R$ is a not a 0 divisor if and only if whenever $ab = 0$ for some $b \in R$, we have that $b = 0$.

Remark. If $a \in R$ is a unit, then a is not a 0 divisor because if $ab = 0$ for some $b \in R$, then

$$0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b.$$

Thus, a field has no 0 divisors.

Theorem 4.26. *The 0 divisors of Z_n are precisely those $m \in Z_n \setminus \{0\}$ such that $\gcd(m, n) \neq 1$. Thus, Z_n is a disjoint union of 0, units, and 0 divisors.*

Proof. Let $m \in Z_n \setminus \{0\}$ be such that $\gcd(m, n) \neq 1$. Then $\frac{n}{\gcd(m,n)} \in Z_n \setminus \{0\}$ and

$$m\frac{n}{\gcd(m, n)} = \frac{m}{\gcd(m, n)}n = 0,$$

and so m is a 0 divisor. For $m \in Z_n \setminus \{0\}$ such that $\gcd(m, n) = 1$, we know that m is a unit by Example 4.23. □

Corollary 4.27. If p is a prime, then Z_p has no 0 divisors.

Definition 4.28. The cancellation laws hold in R if $ab = ac$ with $a \neq 0$ implies that $b = c$, and $ba = ca$ with $a \neq 0$ implies that $b = c$.

Theorem 4.29. *The cancellation laws hold in a ring R if and only if R has no 0 divisors.*

Proof. It is straightforward. □

Definition 4.30. An integral domain D is a commutative ring with unity $1 \neq 0$ and containing no 0 divisors.

Remark. If the coefficients of a polynomial are from an integral domain, one can solve a polynomial equation in which the polynomial can be factored into linear factors in the usual fashion by setting each factor equal to 0.

Remark. Theorem 4.29 shows that the cancellation laws hold in integral domains.

Example 4.31. $\mathbb{Z}$ and Z_p with p a prime, are integral domains. The direct product $R \times S$ of two integral domains R and S is not an integral domain because $(1_R, 0)(0, 1_S) = (0, 0)$, and $1_R \neq 0_R$ and $1_S \neq 0_S$.

Example 4.32. $\mathrm{Mat}_2(Z_2)$ is not an integral domain because

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Theorem 4.33. *Every field is an integral domain.*

Proof. It follows from the second remark after Definition 4.25. □

Theorem 4.34. *Every finite integral domain is a field.*

Proof. Let R be a finite integral domain. Then $0 \neq 1 \in R$ and so we can find $a \in R \setminus 0$. Define a map

$$\begin{aligned} \varphi_a : R &\longrightarrow R \\ r &\longmapsto ar \end{aligned}$$

Since R is an integral domain, cancellation laws implies that φ_a is 1-1. Since R is finite, φ is onto by Pigeonhole principle. Since $1 \in R$, there exists $b \in R$ such that $ab = 1$. □

Corollary 4.35. If p is a prime, Z_p is a field.

Definition 4.36. Let R be a ring, if there exists $n \in \mathbb{N}$ such that $n \cdot a = 0$ for all $a \in R$, then the characteristic

$$\mathrm{char}(R) = \min\{n \in \mathbb{N} \mid n \cdot a = 0, \forall a \in R\},$$

otherwise, $\mathrm{char}(R) = 0$.

Example 4.37. For $n \in \mathbb{N}$, $\mathrm{char}(Z_n) = n$, while $\mathrm{char}(\mathbb{Z}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$.

Theorem 4.38. *Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then* $\mathrm{char}(R) = 0$. *If $n \cdot 1 = 0$ for some $n \in \mathbb{N}$, then*

$$\mathrm{char}(R) = \min\{n \in \mathbb{N} \mid n \cdot 1 = 0\}.$$

Proof. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then we cannot have $n \cdot a = 0$ for all $a \in R$ for some $n \in \mathbb{N}$, and so $\mathrm{char}(R) = 0$.

Suppose that there exists $n \in \mathbb{N}$ such that $n \cdot 1 = 0$. Then for any $a \in R$, we have that

$$n \cdot a = \underbrace{a + \cdots + a}_{n \text{ times}} = a(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = a(n \cdot 1) = a0 = 0.$$ □

4.3 Fermat's and Euler's Theorems

Theorem 4.39 (Little Theorem of Fermat)**.** *If $a \in \mathbb{Z}$ and p is a prime, then for $a \not\equiv 0 \pmod{p}$, $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. It is a special case of Euler's Theorem. □

Example 4.40. Let us compute the remainder of 8^{103} when divided by 13.

$$8^{103} \equiv (8^{12})^8(8^7) \equiv (1^8)(8^7) \equiv 8^7 \equiv (-5)^7 \equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv 5 \pmod{13}.$$

Example 4.41. Show that $2^{11213} - 1$ is not divisible by 11.

Proof. Since $2^{10} \equiv 1 \pmod{11}$, we have that

$$2^{11213} - 1 \equiv (2^{10})^{1121}(2^3) - 1 \equiv 1^{1121}(2^3) - 1 \equiv 2^3 - 1 \equiv 8 - 1 \equiv 7 \pmod{11}.$$ □

Definition 4.42. Primes of the form $2^p - 1$ where p is prime are known as Mersenne primes.

Example 4.43. Show that for every $n \in \mathbb{Z}$, the number $n^{33} - n$ is divisible by 15.

Proof. It is enough to show that $3 \mid n^{33} - n$ and $5 \mid n^{33} - n$. Note that $n^{33} - n = n(n^{32} - 1)$. If $3 \mid n$, then $3 \mid n(n^{32} - 1)$.

If $3 \nmid n$, i.e., $n \not\equiv 0 \pmod{3}$, then $n^2 \equiv 1 \pmod{3}$, so

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

and hence $3 \mid n^{32} - 1$.

If $5 \mid n$, then $5 \mid n(n^{32} - 1)$. If $5 \nmid n$, i.e., $n \not\equiv 0 \pmod{5}$, then $n^4 \equiv 1 \pmod{5}$, so

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

and hence $5 \mid n^{32} - 1$. □

Theorem 4.44. *Let R be a ring and $R^\times$ the set of units in R. Then $\langle R^\times, \cdot \rangle$ is a group.*

Proof. Let $a, b \in R^\times$. Then there exists $a^{-1}, b^{-1} \in R$ such that $aa^{-1} = 1 = a^{-1}a$ and $bb^{-1} = 1 = b^{-1}b$. Then

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1,$$
$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1.$$

Hence $ab \in R^\times$, and so $R^\times$ is closed under $\cdot$.

$\mathscr{G}_1$: The associativity of $\cdot$ on elements in $\langle R^\times, \cdot \rangle$ is inherited from the associativity of $\cdot$ on elements in $\langle R, +, \cdot \rangle$.

$\mathscr{G}_2$: Since $1 * 1 = 1$, $1 \in R^\times$.

$\mathscr{G}_3$: Let $a \in R^\times$. Then a has the multiplicative inverse a^{-1}.

□

Definition 4.45. Let $n \in \mathbb{N}$, and define

$$\begin{aligned} G_n &:= Z_n^\times \\ &= \{a \in Z_n \setminus \{0\} \mid a \text{ is a unit}\} \\ &= \{a \in Z_n \setminus \{0\} \mid a \text{ is not a 0 divisor}\} \\ &= \{a \in Z_n \setminus \{0\} \mid \gcd(a,n) = 1\}. \end{aligned}$$

Corollary 4.46. For $n \in \mathbb{Z}_{\geqslant 2}$, G_n is a group under multiplication modulo n.

Definition 4.47. Define the Euler phi-function $\varphi : \mathbb{N} \to \mathbb{N}$ by

$$\varphi(n) = |\{1 \leqslant m \leqslant n \mid \gcd(m,n) = 1\}|.$$

In particular, $\varphi(1) = 1$, and when $n \in \mathbb{Z}_{\geqslant 2}$,

$$\varphi(n) = |G_n|.$$

Theorem 4.48 (Euler's Theorem)**.** *Let $n \in \mathbb{N}$. If $a \in \mathbb{Z}$ and $\gcd(a,n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. If $n = 1$, then it is trivial. Assume now that $n \in \mathbb{Z}_{\geqslant 2}$. By the division algorithm, $a = nq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leqslant r < n$. Since $\gcd(a,n) = 1$, we have that $r \neq 0$. Note that $\gcd(r,n) = \gcd(a - nq, n) = \gcd(a,n) = 1$, where the second equality follows from Corollary 1.78. Hence $r \in G_n$, so $|r| \mid |G_n|$ by Corollary 2.55, and thus $r^{\varphi(n)} = r^{|G_n|} \equiv 1 \pmod{n}$. Therefore,

$$a^{\varphi(n)} = (nq+r)^{\varphi(n)} = \sum_{i=0}^{\varphi(n)} \binom{\varphi(n)}{i} (nq)^i r^{\varphi(n)-i} \equiv \binom{\varphi(n)}{0} (nq)^0 r^{\varphi(n)-0} = r^{\varphi(n)} \equiv 1 \pmod{n}. \quad \square$$

Example 4.49. Let $n = 12$. Then $\varphi(12) = 4$. Since $\gcd(7,12) = 1$, we have that $7^4 \equiv 1 \pmod{12}$.

Theorem 4.50. *Let $m \in \mathbb{N}$ and $a \in Z_m$ be such that $\gcd(a,m) = 1$. For each $b \in Z_m$, the equation $ax = b$ has a unique solution in Z_m.*

Proof. Since $\gcd(a,m) = 1$, $a \in G_m$, and then a is a unit in Z_m. The unique solution is $a^{-1}b \pmod{m}$. $\square$

Corollary 4.51. Let $a, m, b \in \mathbb{Z}$ be such that $\gcd(a,m) = 1$, then $ax \equiv b \pmod{m}$ has as solutions all integers in precisely d reside class modulo m.

Theorem 4.52. *Let $m \in \mathbb{N}$ and $a, b \in Z_m$. Let $d = \gcd(a,m)$. The equation $ax = b$ has a solution in Z_m if and only if $d \mid b$. When $d \mid b$, the equation has exactly d solutions in Z_m.*

Corollary 4.53. Let $a, m, b \in \mathbb{Z}$ be such that $\gcd(a,m) = d$, then $ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$. When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m.

Example 4.54. Find all solutions of the congruence $15x \equiv 27 \pmod{18}$.

Note that $\gcd(15,18) = 3$ and $3 \mid 27$. We divide everything by 3 and consider $5x \equiv 9 \pmod{6}$, which amounts to solving the equation $5x \equiv 3 \pmod{6}$. It has a unique solution $5^{-1}(3) \equiv 5(3) \equiv 3 \pmod{6}$. Consequently, the solution of $15x \equiv 27 \pmod{18}$ are the integers in the three residue classes: $3 + 18\mathbb{Z}$, $3 + 6 + 18\mathbb{Z}$ and $3 + 2(6) + 18\mathbb{Z}$, i.e., $3 + 18\mathbb{Z}$, $9 + 18\mathbb{Z}$ and $15 + 18\mathbb{Z}$.

4.4 The field of quotients of an integral domain

Let D be an integral domain in this section.

Definition 4.55. Let S be the subset of $D \times D$ given by

$$S = \{(a, b) \mid a, b \in D \text{ and } b \neq 0\} = D \times D^*.$$

Definition 4.56. Two elements (a, b) and (c, d) in S are equivalent, denoted by $(a, b) \sim (c, d)$ if and only if $ad = bc$.

Lemma 4.57. The relation $\sim$ in Definition 4.56 is an equivalence relation.

Definition 4.58. Define

$$F = \{\overline{(a, b)} \mid (a, b) \in S\}.$$

Lemma 4.59. For $\overline{(a, b)}$ and $\overline{(c, d)}$ in F, the equations

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$$

and

$$\overline{(a, b)}\,\overline{(c, d)} = \overline{(ac, bd)}$$

give well-defined operations of addition and multiplication on F.

Theorem 4.60. *F is a field under the operations addition and multiplication, with unity $\overline{(1, 1)}$.*

Remark. For $\overline{(a, b)} \in F$,

$$\overline{(a, b)}\,\overline{(b, a)} = \overline{(ab, ab)} = \overline{(1, 1)} = \overline{(ba, ba)} = \overline{(b, a)}\,\overline{(b, a)},$$

we have that $\overline{(a, b)}^{-1} = \overline{(b, a)}$, it can also be written as $1/\overline{(a, b)} = \overline{(b, a)}$.

Lemma 4.61. We have a ring isomorphism

$$\begin{aligned} i : D &\longrightarrow F \\ a &\longmapsto \overline{(a, 1)} \end{aligned}$$

Thus, D can be regarded as a subring of F.

Example 4.62. We have a ring isomorphism

$$\begin{aligned} i : \mathbb{Z} &\longrightarrow \mathbb{Q} \\ a &\longmapsto \overline{(a, 1)} = \overline{a/1}. \end{aligned}$$

Since $\overline{(a, b)} = \overline{(a, 1)}\,\overline{(1, b)} = \overline{(a, 1)}/\overline{(b, 1)} = i(a)/i(b)$ clearly holds in F, we have now proved the following theorem.

Theorem 4.63. *Any integral domain D can be enlarged to (or embedded in) a field F such that every element of F can be expressed as a quotient of two elements of D. (Such a field F is a field of quotients of D.)*

Theorem 4.64. *Let F be a field of quotients of D and L be any field containing D. Then there exists 1-1 ring homomorphism*

$$\begin{aligned} \psi : F &\longrightarrow L \\ a &\longmapsto a. \end{aligned}$$

Corollary 4.65. Every field L containing an integral domain D contains a field of quotients of D.

Corollary 4.66. Any two fields of quotients of an integral domain D are isomorphic.

Chapter 5

Ideals And Factor Rings

Theorem 5.1. *Let $\phi : R \to R'$ be a ring homomorphism. Then*

(a) $\phi(0) = 0_{R'}$.

(b) $\phi(a) = -\phi(a)$ for $a \in R$.

(c) If S is a subring of R, then $\phi(S) = \mathrm{Im}(\phi|_S)$ is a subring of R'.

(d) If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.

(e) If $1 \in R$, then $\phi(1)$ is the unity for $\phi(R) = \mathrm{Im}(\phi)$.

Definition 5.2. Let $\phi : R \to R'$ be a ring homomorphism. The subring

$$\mathrm{Ker}(\phi) := \phi^{-1}(0_{R'}) = \{r \in R \mid \phi(r) = 0_{R'}\}$$

is the kernel of ϕ.

Theorem 5.3. *Let $\phi : R \to R'$ be a ring homomorphism, and $H = \mathrm{Ker}(\phi)$. Let $a \in R$. Then*

$$\phi^{-1}(\{\phi(a)\}) = a + H = H + a.$$

Corollary 5.4. A ring homomorphism $\phi : R \to R'$ is 1-1 if and only if $\mathrm{Ker}(\phi) = \{0\}$.

Theorem 5.5. *Let $\phi : R \to R'$ be a ring homomorphism with $\mathrm{Ker}(\phi) = H$. Then $R/H = \{a + H \mid a \in R\}$ forms a ring, where for $a + H, b + H \in R/H$,*

$$(a + H) + (b + H) = (a + b) + H,$$

and

$$(a + H)(b + H) = (ab) + H.$$

Also, we have a ring isomorphism

$$\begin{aligned} \mu : R/H &\longrightarrow \mathrm{Im}(\phi) \\ a + H &\longmapsto \phi(a). \end{aligned}$$

Example 5.6. Example 4.12 shows that

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow Z_n \\ a &\longmapsto a \pmod{n} \end{aligned}$$

is a ring homomorphism. Since $\mathrm{Ker}(\phi) = n\mathbb{Z}$, we have that $\mathbb{Z}/n\mathbb{Z}$ is a ring.

Theorem 5.7. *Let H be a subring of the ring R. Multiplication of additive cosets of H is well-defined by the equation*

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

if and only if $ah \in H$ and $hb \in H$ for all $a, b \in R$ and $h \in H$.

Definition 5.8. An additive subgroup N of a ring R satisfying the properties $aN \subseteq N$ and $Nb \subseteq N$ for all $a, b \in R$ is an ideal.

Example 5.9. We see that $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$ since we know it is a subring, because $s(nm) = n(sm) \in n\mathbb{Z}$ and $(nm)t = n(mt) \in n\mathbb{Z}$ for all $s, t \in \mathbb{Z}$ and $nm \in n\mathbb{Z}$.

Corollary 5.10. Let N be an ideal of a ring R. Then $R/N = \{a + N \mid a \in R\}$ forms a ring, where for $a + N, b + N \in R/N$,

$$(a + N) + (b + N) = (a + b) + N,$$

and

$$(a + N)(b + N) = (ab) + N.$$

Definition 5.11. The ring R/N in the preceding corollary is the factor ring (or quotient ring) of R by N.

Theorem 5.12. *Let N be an ideal of R. Then*

$$\begin{aligned} \gamma : R &\longrightarrow R/N \\ x &\longmapsto x + N \end{aligned}$$

is a ring homomorphism with kernel N.

Theorem 5.13. *Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then $\mathrm{Im}(\phi)$ is a ring, and we have a ring isomorphism*

$$\begin{aligned} \mu : R/N &\xrightarrow{\cong} \mathrm{Im}(\phi) \\ x + N &\longmapsto \phi(x) \end{aligned}$$

Let $\gamma : R \to R/N$ be the natural ring homomorphism given by $\gamma(x) = x + N$, then the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & \mathrm{Im}(\phi) \\ & \searrow^{\gamma} & \uparrow{\scriptstyle \mu} \\ & & R/N \end{array}$$

i.e., $\phi = \mu\gamma$, i.e., $\phi(x) = \mu\gamma(x)$ for each $x \in R$.