Chapter 1

Group Theory

Definition: Group

A ***group*** is an algebraic structure $\langle G; 1, {}^{-1}, \cdot \rangle$ consisting of:

- a set G, called the ***underlying set***;
- a distinguished element $1 \in G$, called the ***identity element***;
- a unary operation ${}^{-1} : G \to G$, written as $x \mapsto x^{-1}$, called ***inversion***;
- a binary operation $\cdot : G \times G \to G$, written as $(x, y) \mapsto x \cdot y$, called the ***group operation*** or ***group product***;

satisfying the following requirements:

- ***Associative property***: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in G$.
- ***Identity property***: $1 \cdot x = x \cdot 1 = x$ for all $x \in G$.
- ***Inverse property***: $x \cdot x^{-1} = x^{-1} \cdot x = 1$ for all $x \in G$.

Cancellation Laws

Theorem: Let $\langle G; 1, {}^{-1}, \cdot \rangle$ be a group, and let $x, y, z \in G$.

- ***Left cancellation law***: If $x \cdot y = x \cdot z$, then $y = z$.
- ***Right cancellation law***: If $x \cdot z = y \cdot z$, then $x = y$.

Proof: If $x \cdot y = x \cdot z$, then:

$$
\begin{aligned}
y &= 1 \cdot y && \text{(identity property)} \\
&= (x^{-1} \cdot x) \cdot y && \text{(inverse property)} \\
&= x^{-1} \cdot (x \cdot y) && \text{(associative property)} \\
&= x^{-1} \cdot (x \cdot z) && \text{(by hypothesis)} \\
&= (x^{-1} \cdot x) \cdot z && \text{(associative property)} \\
&= 1 \cdot z && \text{(inverse property)}
\end{aligned}
$$

$= z$ (identity property)

Similarly, if $x \cdot z = y \cdot z$, then

$$x = x \cdot 1 = x \cdot (z \cdot z^{-1}) = (x \cdot z) \cdot z^{-1} = (y \cdot z) \cdot z^{-1} = y \cdot (z \cdot z^{-1}) = y \cdot 1 = y.$$

Uniqueness of Inverses

Theorem: Let $\langle G; 1, {}^{-1}, \cdot \rangle$ be a group, and let $x, y \in G$. If $x \cdot y = 1$ or $y \cdot x = 1$, then $y = x^{-1}$.

Proof: If $x \cdot y = 1$, then

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 1 = x^{-1}.$$

Similarly, if $y \cdot x = 1$, then

$$y = y \cdot 1 = y \cdot (x \cdot x^{-1}) = (y \cdot x) \cdot x^{-1} = 1 \cdot x^{-1} = x^{-1}.$$

Inversion is an Involution

Theorem: Let $\langle G; 1, {}^{-1}, \cdot \rangle$ be a group. For all $x \in G$, we have $(x^{-1})^{-1} = x$.

Proof: By the uniqueness of inverses, in order to show that x is the inverse of x^{-1}, it suffices to show that $x \cdot x^{-1} = 1$. This is guaranteed by the inverse property.

Identity Element is its own Inverse

Theorem: If $\langle G; 1, {}^{-1}, \cdot \rangle$ is a group, then $1^{-1} = 1$.

Proof: By the uniqueness of inverses, in order to show that 1 is its own inverse, it suffices to show that $1 \cdot 1 = 1$. This is guaranteed by the identity property.

When dealing with more than one group in the same context, it is often helpful to label the identity elements, inversion operations, and product operations by the name of the group they belong to. For example, instead of naming the elements of a group $\langle G; 1, {}^{-1}, \cdot \rangle$, we might choose to name them $\langle G; 1_G, {}^{-1_G}, \cdot_G \rangle$.

Definition: Group Homomorphism

Let $\langle G; 1_G, {}^{-1_G}, \cdot_G \rangle$ and $\langle H; 1_H, {}^{-1_H}, \cdot_H \rangle$ be groups. A ***group homomorphism*** is a function $f : G \to H$ that satisfies the following requirements:

- ***Preserves the identity***: $f(1_G) = 1_H$.
- ***Preserves inverses***: $f(x^{-1_G}) = f(x)^{-1_H}$ for all $x \in G$.
- ***Preserves products***: $f(x \cdot_G y) = f(x) \cdot_H f(y)$ for all $x, y \in G$.

Preserving Products is Sufficient

Theorem: Let $\langle G; 1_G, \overline{}^{1}_{G}, \cdot_G \rangle$ and $\langle H; 1_H, \overline{}^{1}_{H}, \cdot_H \rangle$ be groups. If a function $f : G \to H$ satisfies $f(x \cdot_G y) = f(x) \cdot_H f(y)$ for all $x, y \in G$, then f is a group homomorphism.

Proof: We must show that f preserves the identity and inverses. For preservation of the identity, we apply preservation of products to the equation $1_G = 1_G \cdot_G 1_G$ to conclude that

$$f(1_G) = f(1_G \cdot_G 1_G) = f(1_G) \cdot_H f(1_G).$$

By cancellation, it follows that $f(1_G) = 1_H$. For preservation of inverses, let $x \in G$ be given. Since $1_G = x \cdot_G x_G^{-1}$, we can apply preservation of products and the identity to write

$$1_H = f(1_G) = f(x \cdot_G x_G^{-1}) = f(x) \cdot_H f(x_G^{-1}).$$

By uniqueness of inverses, it follows that $f(x_G^{-1}) = f(x)_H^{-1}$.

Definition: Kernel, $\ker f$

Let $\langle G; 1_G, \overline{}^{1}_{G}, \cdot_G \rangle$ and $\langle H; 1_H, \overline{}^{1}_{H}, \cdot_H \rangle$ be groups, and let $f : G \to H$ be a group homomorphism. The ***kernel*** of f is the subset $\ker f \subseteq G$ defined by

$$\ker f \coloneqq \{x \in G : f(x) = 1_H\}.$$

Definition: Subgroup, $H \leq G$

Let $\langle G; 1, {}^{-1}, \cdot \rangle$ be a group. A ***subgroup*** of $\langle G; 1, {}^{-1}, \cdot \rangle$ is a subset $H \subseteq G$ such that $\langle H; 1, {}^{-1}|_H, \cdot|_H \rangle$ is a group, where ${}^{-1}|_H$ denotes the restriction of ${}^{-1}$ to $H \subseteq G$, and $\cdot|_H$ denotes the restriction of $\cdot$ to $H \times H \subseteq G \times G$. Explicitly, this means that:

- ***Contains the identity***: $1 \in H$.
- ***Closed under inverses***: If $x \in H$, then $x^{-1} \in H$.
- ***Closed under products***: If $x, y \in H$, then $x \cdot y \in H$.

We write $H \leq \langle G; 1, {}^{-1}, \cdot \rangle$ to denote that H is a subgroup of $\langle G; 1, {}^{-1}, \cdot \rangle$.

Kernels are Subgroups

Theorem: Let $\langle G; 1_G, \overline{}^{1}_{G}, \cdot_G \rangle$ and $\langle H; 1_H, \overline{}^{1}_{H}, \cdot_H \rangle$ be groups. If $f : G \to H$ is a group homomorphism, then $\ker f \leq \langle G; 1_G, \overline{}^{1}_{G}, \cdot_G \rangle$.

Proof: We need to verify that $\ker f$ contains the identity, is closed under inverses, and is closed under products.

- A homomorphism must preserve the identity, i.e., $f(1_G) = 1_H$, so $1_G \in \ker f$.
- Let $x \in \ker f$ be given. By applying f to both sides of the equation $1_G = x \cdot_G x_G^{-1}$, we obtain

  $$1_H = f(1_G) = f(x \cdot_G x_G^{-1}) = f(x) \cdot_H f(x_G^{-1}) = 1_H \cdot_H f(x_G^{-1}) = f(x_G^{-1})$$

  which proves that $x_G^{-1} \in \ker f$.

- If $x, y \in \ker f$, then
$$f(x \cdot_G y) = f(x) \cdot_H f(y) = 1_H \cdot_H 1_H = 1_H$$
which proves that $x \cdot_G y \in \ker f$.

- We will henceforth refer to a group $\langle G; 1, {}^{-1}, \cdot \rangle$ simply by the name of its underlying set G, omitting explicit mention of its identity element, inversion operation, and product operation. Thus, instead of saying "let $\langle G; 1, {}^{-1}, \cdot \rangle$ be a group," we will simply say "let G be a group."
- When discussing a particular group G, the symbols 1, ${}^{-1}$, and $\cdot$ will be implicitly understood to refer to identity element, inversion operation, and product operation of the group G under discussion. When multiple groups are being discussed simultaneously, we will disambiguate these symbols using the name of the underlying set of the group they belong to (for example, 1_G and $\cdot_G$).
- Nested products of group elements will no longer be written with parentheses. The requirement of associativity guarantees that $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, so we may write $x \cdot y \cdot z$ without fear of ambiguity. We will freely and implicitly apply the associative property whenever it is required to interpret a nested product in more than one way.
- Group operations will no longer be denoted by the symbol $\cdot$, but merely by juxtaposition. What we previously wrote as $x \cdot y$ will now simply be denoted by xy.

Inverse of a Product is the Reverse Product of Inverses

Theorem: Let G be a group and $n \in \mathbb{N}$. If $x_1, \ldots, x_n \in G$, then $(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}$.

Proof: By the uniqueness of inverses, it suffices to show that $x_1 x_2 \cdots x_n x_n^{-1} \cdots x_2^{-1} x_1^{-1} = 1$. We proceed by induction on n. The base case $n = 1$ holds by the inverse property $x_1 x_1^{-1} = 1$. Supposing that the claim holds for $n = k$, we establish the claim for $n = k + 1$ by calculating as follows:
$$x_1 x_2 \cdots x_k x_{k+1} x_{k+1}^{-1} x_k^{-1} \cdots x_2^{-1} x_1^{-1} = x_1 x_2 \cdots x_k x_k^{-1} \cdots x_2^{-1} x_1^{-1} = 1$$
The first equality follows from the inverse property $x_{k+1} x_{k+1}^{-1} = 1$, and the second equality follows from the inductive hypothesis.

Definition: Left Conjugate, Right Conjugate

Let G be a group, and let $g, x \in G$. The ***left conjugate*** of x by g is the element ${}^g x \in G$ defined by
$${}^g x \coloneqq g x g^{-1}.$$
Similarly, the ***right conjugate*** of x by g is the element $x^g \in G$ defined by
$$x^g \coloneqq g^{-1} x g.$$

Properties of Conjugation

Theorem: Let G be a group. For all $g, h, x \in G$, we have:

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

Proof: Let $g, h, x \in G$ be given.

$$ {}^{1}x = 1x1^{-1} = x1 = x = 1x = 1^{-1}x1 = x^{1} $$

$$ {}^{g^{-1}}x = g^{-1}x(g^{-1})^{-1} = g^{-1}xg = x^{g} $$

$$ x^{g^{-1}} = (g^{-1})^{-1}xg^{-1} = gxg^{-1} = {}^{g}x $$

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

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

Definition: Normal Subgroup, $N \trianglelefteq G$

Let G be a group. A ***normal subgroup*** of G is a subgroup $N \leq G$ that satisfies the following additional requirement:

- ***Closed under conjugation***: If $g \in G$ and $x \in N$, then $x^{g} \in N$.

We write $N \trianglelefteq G$ to denote that N is a normal subgroup of G.

Definition: Abelian Group

An ***abelian group*** is a group G that satisfies the following additional requirement:

- ***Commutative property***: $xy = yx$ for all $x, y \in G$.

When a group is abelian, it is customary to adopt a different notational convention. Instead of the ***multiplicative notation*** $\langle G; 1, {}^{-1}, \cdot \rangle$, for abelian groups we use the ***additive notation*** $\langle G; 0, -, + \rangle$.

Definition: Integer Powers of Group Elements, x^{n}

Let $\langle G; 1_G, {}^{-1}, \cdot \rangle$ be a group, $x \in G$, and $n \in \mathbb{Z}$. We denote by x^{n} the element of G defined as follows:

- If $n = 0$, then we define $x^{0} \coloneqq 1_G$.
- For $n > 0$, we define x^{n} inductively as $x^{n} \coloneqq x^{n-1} \cdot x$.
- For $n < 0$, we define x^{n} inductively as $x^{n} \coloneqq x^{n+1} \cdot x^{-1}$.

For example, $x^{2} \coloneqq x \cdot x$ and $x^{-3} \coloneqq x^{-1} \cdot x^{-1} \cdot x^{-1}$. This definition can create ambiguities

with the notation x^g for right conjugation if we do not carefully distinguish between group elements and integers. Thankfully, the potentially-problematic case x^1 causes no issues, as $x^1 = x$ regardless of whether we interpret x^1 as x raised to the first power or the right conjugate of x by 1.

Definition: Cyclic Group, Generator

A ***cyclic group*** is a group G containing an element $x \in G$ such that every element $y \in G$ can be written as $y = x^n$ for some $n \in \mathbb{Z}$. Such an element x is called the ***generator*** of the group G, and we write $G = \langle x \rangle$ to denote that G is generated by x.

Chapter 2

Ring Theory

In this chapter, we introduce a new class of algebraic structures, called rngs and rings, whose study is collectively called ***ring theory***. Rngs and rings are more complicated than groups because their definition involves not one, but two binary operations.

Definition: Rng

A ***rng*** (pronounced as "*rung*") is an algebraic structure $\langle R; 0, -, +, \cdot \rangle$ consisting of:

- a set R, called the ***underlying set***;
- a distinguished element $0 \in R$, called the ***zero element***;
- a unary operation $- : R \to R$, written as $x \mapsto -x$, called ***negation***;
- a binary operation $+ : R \times R \to R$, written as $(x, y) \mapsto x + y$, called ***addition***;
- a binary operation $\cdot : R \times R \to R$, written as $(x, y) \mapsto x \cdot y$, called ***multiplication***;

satisfying the following requirements:

- ***Additive structure***: $\langle R; 0, -, + \rangle$ is an abelian group.
- ***Associativity***: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in R$.
- ***Left distributivity***: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ for all $x, y, z \in R$.
- ***Right distributivity***: $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ for all $x, y, z \in R$.

The key ingredient present in the definition of a rng is ***distributivity***, which establishes a link between two different binary operations. We begin our study of rngs by proving a simple (but important) result to demonstrate the utility of the distributive property.

Multiplying by Zero Yields Zero

Theorem: Let $\langle R; 0, -, +, \cdot \rangle$ be a rng. For any $x \in R$, we have $0 \cdot x = x \cdot 0 = 0$.

Proof: Let $x \in R$ be given. Because 0 is the identity element of the abelian group $\langle R; 0, -, + \rangle$, we have $0 = 0 + 0$. Using left distributivity, it follows that $0 \cdot x = (0 + 0) \cdot x = (0 \cdot x) + (0 \cdot x)$, and by canceling one copy of $0 \cdot x$ on both sides, we conclude that $0 \cdot x = 0$. We similarly apply

right distributivity to the expression $x \cdot 0 = x \cdot (0+0) = (x \cdot 0) + (x \cdot 0)$ to conclude that $x \cdot 0 = 0$.

Definition: Subrng, $S \leq R$

Let $\langle R; 0, -, +, \cdot \rangle$ be a rng. A ***subrng*** of $\langle R; 0, -, +, \cdot \rangle$ is a subgroup $S \leq \langle R; 0, -, + \rangle$ that satisfies the following additional requirement:

- ***Closed under products***: If $x, y \in S$, then $x \cdot y$ in S.

We write $S \leq R$ to indicate that S is a subrng of R.

Definition: Zero Rng, Trivial Rng, Nonzero Rng, Nontrivial Rng

The ***zero rng*** or ***trivial rng*** is the rng $\langle \{0\}; 0, -, +, \cdot \rangle$ whose underlying set is a singleton containing the distinguished element 0, and whose operations are defined by $-0 = 0 + 0 = 0 \cdot 0 = 0$. A rng is ***nonzero*** or ***nontrivial*** if its underlying set contains more than one element.

The zero rng is a subrng of every rng.

Definition: Rng Homomorphism

Let $\langle R; 0_R, -_R, +_R, \cdot_R \rangle$ and $\langle S; 0_S, -_S, +_S, \cdot_S \rangle$ be rngs. A ***rng homomorphism*** is a function $f : R \to S$ that satisfies the following requirements:

- ***Preserves additive structure***: f is a group homomorphism between the abelian groups $\langle R; 0_R, -_R, +_R \rangle$ and $\langle S; 0_S, -_S, +_S \rangle$.
- ***Preserves products***: $f(x \cdot_R y) = f(x) \cdot_S f(y)$ for all $x, y \in R$.

Every rng homomorphism is also a group homomorphism, so the theory and terminology of group homomorphisms is immediately applicable to rng homomorphisms. For example, the kernel of a rng homomorphism $f : R \to S$ is still defined to be the set

$$\ker f \coloneqq \{x \in R : f(x) = 0_S\}.$$

As with groups, we will often refer to a rng $\langle R; 0, -, +, \cdot \rangle$ by the name of its underlying set R and denote the multiplication operation $\cdot$ by juxtaposition. We will never denote addition, subtraction, or negation by juxtaposition, so the symbols $+$ and $-$ will always be used.

Definition: Ideal, Left Ideal, Right Ideal, One-Sided Ideal, Two-Sided Ideal, $I \trianglelefteq R$

Let R be a rng.

- A ***left ideal*** of R is a subrng $I \leq R$ that satisfies the following additional requirement:
  - ***Absorbs left multiplication***: $rx \in I$ for all $r \in R$ and $x \in I$.
- A ***right ideal*** of R is a subrng $I \leq R$ that satisfies the following additional requirement:
  - ***Absorbs right multiplication***: $xr \in I$ for all $x \in I$ and $r \in R$.
- A ***one-sided ideal*** of R is a subrng $I \leq R$ that is a left ideal or a right ideal (possibly both).
- A ***two-sided ideal*** of R, or simply an ***ideal*** of R, is a subrng $I \leq R$ that is both a left ideal

and a right ideal.

We write $I \trianglelefteq R$ to denote that I is a (two-sided) ideal of R.

Every two-sided ideal is also a one-sided ideal, but the converse is not true.

Kernels are Ideals

Theorem: If $f : R \to S$ is a rng homomorphism, then $\ker f \trianglelefteq R$.

Proof: By definition, a rng homomorphism $f : R \to S$ is also a group homomorphism, so we already know that $\ker f$ is a subgroup of R. To prove that $\ker f$ is an ideal, we must show that it absorbs multiplication. Let $r \in R$ and $x \in \ker f$ be given. It follows that

$$f(rx) = f(r)f(x) = f(r)0 = 0 \qquad \text{and} \qquad f(xr) = f(x)f(r) = 0f(r) = 0,$$

so we conclude that $rx \in \ker f$ and $xr \in \ker f$.

Definition: Zero Divisor, Left Zero Divisor, Right Zero Divisor, Two-Sided Zero Divisor

Let R be a rng.

- A ***left zero divisor*** is an element $x \in R$ for which there exists a nonzero element $y \in R \setminus \{0\}$ such that $xy = 0$.
- A ***right zero divisor*** is an element $x \in R$ for which there exists a nonzero element $y \in R \setminus \{0\}$ such that $yx = 0$.
- A ***zero divisor*** is an element $x \in R$ that is a left zero divisor or a right zero divisor.
- A ***two-sided zero divisor*** is an element $x \in R$ that is both a left zero divisor and a right zero divisor.

Note that the terms "ideal" and "zero divisor" have opposite usage conventions. Unless otherwise specified, the lone term "ideal" means "two-sided ideal," whereas the lone term "zero divisor" does *not* mean "two-sided zero divisor."

Definition: Ring

A ***ring*** is an algebraic structure $\langle R; 0, 1, -, +, \cdot \rangle$ consisting of a rng $\langle R; 0, -, +, \cdot \rangle$ and a distinguished element $1 \in R$, called the ***identity element***, satisfying the following requirement:

- ***Identity***: $1 \cdot x = x \cdot 1 = x$ for all $x \in R$.

In order to distinguish the identity element 1 from the zero element 0, we sometimes call 1 the ***multiplicative identity element*** and 0 the ***additive identity element***. These elements need not be distinct; in fact, there is one ring in which $0 = 1$ holds.

$0 \neq 1$ in any Nontrivial Ring

Theorem: Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a ring. If $0 = 1$, then $R = \{0\}$.

Proof: For any $x \in R$, we have $x = 1 \cdot x = 0 \cdot x = 0$.

Definition: Subring

Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a ring. A ***subring*** of $\langle R; 0, 1, -, +, \cdot \rangle$ is a subrng $S \leq \langle R; 0, -, +, \cdot \rangle$ that satisfies the following additional requirement:

- ***Contains the identity***: $1 \in S$.

In these notes, we will only use the notation $S \leq R$ for *subrngs*, not *subrings*. This ensures consistency with the notation $I \trianglelefteq R$ for ideals (i.e., $I \trianglelefteq R \implies I \leq R$), since an ideal is always a subrng, but not necessarily a subring.

The distinction between subrngs and subrings is subtle and can easily lead to confusion if these terms are not used carefully. For example, if R is a ring and $S \leq R$ is a subrng, it is possible for S to be a ring in its own right without being a *subring* of R. Consider $\mathbb{Z} \times \{0\} \leq \mathbb{Z} \times \mathbb{Z}$; both of these rngs are rings, with identity elements $(1, 0) \in \mathbb{Z} \times \{0\}$ and $(1, 1) \in \mathbb{Z} \times \mathbb{Z}$. However, $\mathbb{Z} \times \{0\}$ is *not* a subring of $\mathbb{Z} \times \mathbb{Z}$ because $(1, 1) \notin \mathbb{Z} \times \{0\}$. A subring *must* contain the identity element of the original ring.

Definition: Inverse, Left Inverse, Right Inverse, Two-Sided Inverse, Invertible, Unit

Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a ring, and let $x \in R$.

- A ***left inverse*** of x is an element $y \in R$ such that $y \cdot x = 1$. If such an element exists, then we say that x is ***left-invertible***.
- A ***right inverse*** of x is an element $y \in R$ such that $x \cdot y = 1$. If such an element exists, then we say that x is ***right-invertible***.
- A ***two-sided inverse*** of x, or simply an ***inverse*** of x, is an element $y \in R$ such that $y \cdot x = x \cdot y = 1$. If such an element exists, then we say that x is ***invertible***, and we call x a ***unit***.

In ring theory, the word "inverse" used without further elaboration usually means "two-sided inverse."

Left and Right Invertibility Imply Two-Sided Invertibility

Theorem: Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a ring. If $x \in R$ has both a left inverse $y \in R$ and a right inverse $z \in R$, then $y = z$, and x is invertible.

Proof: Using the associativity of multiplication, observe that

$$y = y \cdot 1 = y \cdot (x \cdot z) = (y \cdot x) \cdot z = 1 \cdot z = z.$$

Hence, $y = z$ is a two-sided inverse of x.

Inverses are Unique and Invertible

Corollary: Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a ring. If an element $x \in R$ is invertible, then it has a unique inverse. Moreover, that inverse is itself invertible, and x is its unique inverse.

Proof: Let $y, z \in R$ be (two-sided) inverses of x. In particular, y is a left inverse of x, and z is a right inverse of x, so we can apply the preceding result to conclude that $y = z$.

Observe that the relation $x \cdot y = y \cdot x = 1$ that defines inverses is symmetric in x and y. Hence, if y is an inverse of x, then x is also an inverse of y.

This result allows us to speak unambiguously of *the* inverse of an invertible element of a ring.

Definition: $R^\times$, x^{-1}

Let $\langle R; 0, 1, -, +, \cdot \rangle$ be a ring. The set of all units in R is denoted by $R^\times$. For each $x \in R^\times$, we denote by x^{-1} the unique inverse of x. Thus, we regard the map $x \mapsto x^{-1}$ as a unary operation $^{-1} : R^\times \to R^\times$.

Using this notation, we can restate the preceding result as $x = (x^{-1})^{-1}$ for all $x \in R^\times$.

$R^\times$ is a Group

Theorem: If $\langle R; 0, 1, -, +, \cdot \rangle$ is a ring, then $\langle R^\times; 1, ^{-1}, \cdot \rangle$ is a group.

In the Absence of Zero Divisors, $xy = 1 \implies yx = 1$

Theorem: Let R be a ring, and let $x, y \in R$. If $xy = 1$, and at least one of the following conditions holds:

- x is not a left zero divisor.
- y is not a right zero divisor.

then $yx = 1$.

Proof: Observe that $xy = 1$ implies $xy - 1 = 0$, and hence that

$$0 = (xy - 1)x = xyx - x = x(yx - 1).$$

If x is not a left zero divisor, then we can conclude that $yx = 1$. Similarly, we also have

$$0 = y(xy - 1) = yxy - y = (yx - 1)y.$$

If y is not a right zero divisor, then we can conclude that $yx = 1$.

An Ideal that Contains a Unit Contains Everything

Theorem: Let R be a ring. If $I \leq R$ is a one-sided ideal that contains a unit, then $I = R$.

Definition: Commutative Ring

A ***commutative ring*** is a ring R that satisfies the following additional requirement:

- ***Commutativity***: $xy = yx$ for all $x, y \in R$.

Definition: Domain

A ***domain*** is a nontrivial ring in which there are no zero divisors except 0 itself.

Definition: Integral Domain

An ***integral domain*** is a nontrivial commutative ring in which there are no zero divisors except 0 itself.

Definition: Principal Ideal, Generator

Let R be a commutative ring, and let $r \in R$. The ***principal ideal*** generated by r, denoted by $\langle r \rangle$, is the subset of R consisting of all multiples of r.

$$\langle r \rangle \coloneqq \{rx : x \in R\}$$

An ideal $I \trianglelefteq R$ is ***principal*** if there exists an element $r \in I$ such that $R = \langle r \rangle$. In this case, we say that r ***generates*** the ideal I, and we call r the ***generator*** of I.

Definition: Principal Ideal Domain, PID

A ***principal ideal domain*** is an integral domain in which every ideal is principal.

Definition: Divides, Divisibility Relation

Let R be a commutative rng. An element $a \in R$ ***divides*** an element $b \in R$ if there exists an element $q \in R$ such that $b = qa$. We write $a \mid b$ to denote that a divides b, and we call this relation $\mid \subseteq R \times R$ the ***divisibility relation*** on R.

The divisibility relation $\mid$ is always reflexive in a ring, but can fail to be reflexive in a rng. Note that 0 does not divide any element of a rng except 0, but every element of a rng divides 0.

Divisibility is Transitive

Theorem: The divisibility relation on any rng is transitive.

Proof: Let R be a rng, and let $a, b, c \in R$. If $a \mid b$ and $b \mid c$, then there exist $x, y \in R$ such that $b = xa$ and $c = yb$. It follows that $c = yxa$, which proves that $a \mid c$.

Definition: Prime Element

Let R be a commutative ring. An element $p \in R$ is ***prime*** if $p \neq 0$, $p \notin R^\times$, and for all $a, b \in R$, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Definition: Irreducible Element

Let R be a ring. An element $r \in R$ is ***irreducible*** if $r \notin R^\times$ and for all $a, b \in R$, if $r = ab$, then $a \in R^\times$ or $b \in R^\times$.

Note that 0 is never an irreducible element of a ring, since $0 = 0 \cdot 0$.

Definition: Euclidean Valuation

A ***Euclidean valuation*** on a commutative rng R is a function $\nu : R \setminus \{0\} \to W$ into a well-ordered set $(W, \leq)$ that has the following property: for all $a, b \in R$, if $b \neq 0$, then there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\nu(r) < \nu(b)$.

Definition: Euclidean Domain, ED

A ***Euclidean domain***, or ***ED***, is an integral domain on which there exists a Euclidean valuation.

This complicated definition formalizes a simple idea: a Euclidean domain is a set in which it is possible to divide two elements with remainder. In any commutative ring, it is possible to define a completely unhelpful division-with-remainder operation by declaring a divided by b to have quotient 0 and remainder a. In order for this operation to make useful progress, the remainder r has to be, in some sense, "smaller" than the divisor b.

A Euclidean valuation formalizes this notion by requiring that $r = 0$ or $\nu(r) < \nu(b)$. The actual values taken by the function ν are completely unimportant, as long as they exist in a set that does not contain an infinite descending chain $\nu(x_1) > \nu(x_2) > \cdots$. This guarantees that repeated division with remainder (as performed in the Euclidean algorithm) always terminates in a finite number of steps.

Euclidean Valuation Implies Existence of Identity

Theorem: Let R be a commutative rng. If R admits a Euclidean valuation, then R contains a multiplicative identity element.

Proof: If $R = \{0\}$, then 0 is a multiplicative identity. Otherwise, let $\nu : R \setminus \{0\} \to W$ be a Euclidean valuation on R for some well-ordered set W, and choose an element $a \in R \setminus \{0\}$ that minimizes $\nu(a)$. (The well-ordering of W guarantees that such an element exists.)

We claim that every element of R is a multiple of a. Indeed, let $x \in R$ be given. By definition, $a \neq 0$, so there exist $q, r \in R$ such that $x = qa + r$ and either $r = 0$ or $\nu(r) < \nu(a)$. The latter would contradict the minimality of $\nu(a)$, so it must be the case that $r = 0$. Hence, $x = qa$ is a multiple of a.

Having established that every element of R is a multiple of a, it follows that a itself is a multiple of a. Thus, there exists $i \in R$ such that $a = ia$. We claim that i is the desired multiplicative identity. To see this, let $x \in R$ be arbitrary, and write $x = ra$ for some $r \in R$. It follows that $ix = ira = ria = ra = x$, as desired.

Every ED is a PID

Theorem: Every Euclidean domain is a principal ideal domain.

Proof: Let R be a Euclidean domain, and let an ideal $I \trianglelefteq R$ be given. If $I = \{0\}$, then I is the principal ideal generated by 0. Otherwise, let $\nu : R \setminus \{0\} \to W$ be a Euclidean valuation on R for some well-ordered set W. Choose an element $b \in I \setminus \{0\}$ that minimizes $\nu(b)$. (The well-ordering of W guarantees that such an element exists.)

We claim that $I = \langle b \rangle$. It is clear that $\langle b \rangle \subseteq I$, since an ideal I must contain all multiples of an element $b \in I$. To see that $I \subseteq \langle b \rangle$, take an arbitrary element $a \in I$. Either $b \mid a$, in which case $a \in \langle b \rangle$, or there exist $q, r \in R$ with $r \neq 0$ and $\nu(r) < \nu(b)$ such that $a = qb + r$. Since $a \in I$ and $b \in I$, it follows that $qb \in I$, and hence that $a - qb = r \in I$. This is impossible, as the condition $\nu(r) < \nu(b)$ would contradict the minimality of $\nu(b)$. Hence, it must be the case that $a \in \langle b \rangle$.

Chapter 3

Field Theory

Definition: Field

A ***field*** is a commutative ring $\langle K; 0, 1, -, +, \cdot \rangle$ that satisfies the following additional requirements:

- ***Nontriviality***: $0 \neq 1$.
- ***Invertibility***: Every element of $K \setminus \{0\}$ has a (two-sided) inverse, i.e., $K^\times = K \setminus \{0\}$.

Definition: Field of Fractions, $\mathrm{Frac}(R)$, Numerator, Denominator, a/b, $\frac{a}{b}$

Let R be an integral domain. The ***field of fractions*** of R, denoted by $\mathrm{Frac}(R)$, is the set of equivalence classes of the relation $\sim$ defined on $R \times (R \setminus \{0\})$ as follows: $(a, b) \sim (c, d)$ if and only if $ad = bc$. We denote by a/b or $\frac{a}{b}$ the equivalence class of the pair $(a, b) \in R \times (R \setminus \{0\})$.

For this definition to make sense, we need to verify that $\sim$ is an equivalence relation on $R \times (R \setminus \{0\})$. Reflexivity and symmetry are straightforward consequences of the commutativity of R. Indeed, let $a, c, e \in R$ and $b, d, f \in R \setminus \{0\}$ be arbitrary. Then

$$ab = ba \implies (a, b) \sim (a, b)$$

shows that $\sim$ is reflexive, and

$$(a, b) \sim (c, d) \implies ad = bc \implies cb = da \implies (c, d) \sim (a, b)$$

shows that $\sim$ is symmetric. Establishing transitivity requires us to invoke the lack of zero divisors in R. Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$; this means that $ad - bc = 0$ and $cf - de = 0$. It follows that

$$0 = (ad - bc)f + b(cf - de) = adf - bcf + bcf - bde = adf - bde = d(af - be).$$

Since $d \neq 0$ by hypothesis, we know that d is not a zero divisor, and hence that $af - be = 0$. This proves that $(a, b) \sim (e, f)$, completing the proof that $\sim$ is transitive.

Field of Fractions is a Field

Theorem: If $\langle R; 0_R, 1_R, -_R, +_R, \cdot_R \rangle$ is an integral domain, then $\langle \mathrm{Frac}(R); 0, 1, -, +, \cdot \rangle$, is a field, where the distinguished elements $0, 1 \in \mathrm{Frac}(R)$, the unary operation $- : \mathrm{Frac}(R) \to \mathrm{Frac}(R)$, and the binary operations $+, \cdot : \mathrm{Frac}(R) \times \mathrm{Frac}(R) \to \mathrm{Frac}(R)$ are defined as follows:

$$0 \coloneqq \frac{0_R}{1_R} \qquad 1 \coloneqq \frac{1_R}{1_R}$$

$$-\frac{a}{b} \coloneqq \frac{-_R a}{b} \qquad \frac{a}{b} + \frac{c}{d} \coloneqq \frac{(a \cdot_R d) +_R (b \cdot_R c)}{b \cdot_R d} \qquad \frac{a}{b} \cdot \frac{c}{d} \coloneqq \frac{a \cdot_R c}{b \cdot_R d}$$

Definition: Field Homomorphism

A ***field homomorphism*** is a ring homomorphism $f : K \to L$ where the domain K and codomain L are both fields.

Note that field homomorphisms are defined as *ring* homomorphisms, not *rng* homomorphisms, so they are required to map 1 to 1.

We now prove a crucial fact that markedly distinguishes field theory from group theory and ring theory.

Fields Have Two Ideals

Theorem: Let K be a field. If $I \leq K$ is a one-sided ideal, then either $I = \{0\}$ or $I = K$.

Proof: A one-sided ideal $I \leq K$ must contain 0 by definition. If I contains any other element of K, then I contains a unit, and hence contains every element of K.

Every Field Homomorphism is a Monomorphism

Theorem: Every rng homomorphism $f : K \to R$ from a field K to a rng R is either injective or trivial (i.e., $f(x) = 0$ for all $x \in K$).

Proof: Either $\ker f = \{0\}$, in which case f is injective, or $\ker f = K$, in which case f is trivial.

In field theory, it is conventional to regard a monomorphism $f : K \hookrightarrow L$ as an *embedding* of K into L. Under this interpretation, the preceding result shows that the only possible relationship between two fields (via a field homomorphism) is for one to be contained inside the other. For this reason, field theory does not adopt the language of homomorphisms that permeates group theory and ring theory. Instead, field theory is written in the language of *subfields* and *field extensions*.

Definition: Subfield

Let K be a field. A ***subfield*** of K is a subring $L \leq K$ that satisfies the following additional requirement:

- ***Closed under inversion***: If $x \in L \setminus \{0\}$, then $x^{-1} \in L$.

Not every subring of a field is a subfield. For example, $\mathbb{Z}$ is a subring but not a subfield of $\mathbb{Q}$.

Definition: Field Extension, L/K

Let L be a field. If K is a subfield of L, then we say that L is an ***extension*** of K, and we say that L/K (pronounced as "L *over* K") is a ***field extension***.

Somewhat confusingly, the notation L/K is not intended to represent a quotient of any kind. It is simply a strange (but historically traditional) notation for an ordered pair (L, K) of fields, carrying the additional information that the second field is contained in the first. Field theory has no use for quotients, since fields have no nontrivial proper ideals.

Definition: Degree, $[L : K]$, Finite Extension

The ***degree*** of a field extension L/K, denoted by $[L : K]$, is the dimension of L as a vector space over K. If $[L : K]$ is finite, then we call L/K a ***finite extension***.

Note that the individual fields K and L involved in a finite extension L/K are allowed to have infinite cardinality. The phrase "finite extension" specifies that the *extension* is finite, not that the *fields* are finite.

Definition: Algebraic Element, Transcendental Element

Let L/K be a field extension. We say that an element $\alpha \in L$ is ***algebraic*** over K if there exists a polynomial $p \in K[x]$ such that $p(\alpha) = 0$. If no such polynomial exists, then we say that α is ***transcendental*** over K.

Definition: Algebraic Extension, Transcendental Extension

An ***algebraic extension*** is a field extension L/K in which every element of L is algebraic over K. On the other hand, a ***transcendental extension*** is a field extension L/K in which L contains an element that is transcendental over K.

Minimal Polynomials Exist

Theorem: Let L/K be a field extension. If $\alpha \in L$ is algebraic over K, then there exists a unique monic polynomial in $K[x]$ of minimal degree satisfying $p(\alpha) = 0$.

Proof: The existence of such a polynomial is clear, since by the hypothesis that α is algebraic over K, there exists a polynomial $p \in K[x]$ satisfying $p(\alpha) = 0$. (This polynomial can be made monic by dividing it by its leading coefficient.) Because the degrees of monic polynomials (i.e., natural numbers) are well-ordered, we can conclude that there exists a minimal-degree monic polynomial having this property.

We verify uniqueness by contradiction. Suppose that there exist two distinct monic polynomials $p, q \in K[x]$ of minimal degree that satisfy $p(\alpha) = q(\alpha) = 0$. It follows that $p - q \in K[x]$ is a polynomial of strictly smaller degree that satisfies $(p - q)(\alpha) = p(\alpha) - q(\alpha) = 0 - 0 = 0$, contradicting the minimality of p and q.

Definition: Minimal Polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. The ***minimal polynomial*** of α over K is the unique monic polynomial $p \in K[x]$ of minimal degree satisfying $p(\alpha) = 0$.

Minimal Polynomials are Irreducible

Theorem: Let L/K be a field extension. If $p \in K[x]$ is the minimal polynomial of an algebraic element $\alpha \in L$, then p is irreducible in $K[x]$.

Proof: If p could be written as the product of two non-constant polynomials $q, r \in K[x]$, then $0 = p(\alpha) = q(\alpha)r(\alpha)$ would imply that $q(\alpha) = 0$ or $r(\alpha) = 0$, contradicting the minimality of p.

Definition: Annihilator Ideal

Let L/K be a field extension. The ***annihilator ideal*** of an element $\alpha \in L$ over K is the subset of $K[x]$

Minimal Polynomial Divides Every Other Polynomial

Definition: Finite Field

A ***finite field*** is a field whose underlying set has finite cardinality.

Finite Fields have Cyclic Multiplicative Groups

Theorem: If K is a finite field, then $K^\times$ is a cyclic group.

Definition: Simple Extension, Primitive Element

A field extension L/K is called a ***simple extension*** if there exists an element $\alpha \in L$ such that $L = K(\alpha)$, i.e., every element of L can be expressed as a rational function of α with coefficients in K. Such an element α is called a ***primitive element*** of L over K.

Primitive Element Theorem

Theorem: Let K be a field. A finite extension L/K is simple if and only if there exist finitely many intermediate subfields F satisfying $K \leq F \leq L$.

Proof: We first consider the case of a finite base field K. In this case, the extension field L, being a finite extension of a finite field, is also finite. This implies that both sides of the desired "if and only if" statement are true. In particular, L has finitely many subfields, and $L^\times$ is a cyclic group, so its generator is a primitive element.

Now suppose that the base field K is infinite. There are two implications that need to be proven.

- Suppose L/K is a simple extension with primitive element $\alpha \in L$,

- Suppose there are finitely many intermediate subfields F satisfying $K \leq F \leq L$.

Definition: (Algebraic) Number Field

An ***algebraic number field***, or simply a ***number field***, is a finite extension of $\mathbb{Q}$.

Definition: Ring of Integers

Let K be an algebraic number field. An element $\alpha \in K$ is an ***algebraic integer*** if there exists a monic polynomial $p \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. The set of all algebraic integers in K is called the ***ring of integers*** of K, denoted by $\mathcal{O}_K$.

Chapter 4

Differential Algebra

Definition: Derivation

A ***derivation*** on a rng $\langle R; 0, -, +, \cdot \rangle$ is a unary operation $\mathrm{d} : R \to R$ that satisfies the following requirements:

- ***Additivity***: $\mathrm{d}(x + y) = \mathrm{d}(x) + \mathrm{d}(y)$ for all $x, y \in R$.
- ***Leibniz rule***: $\mathrm{d}(x \cdot y) = \mathrm{d}(x) \cdot y + x \cdot \mathrm{d}(y)$ for all $x, y \in R$.

Definition: Constant

Let R be a rng, and $\mathrm{d} : R \to R$ be a derivation on R. An element $x \in R$ is ***constant*** with respect to d if $\mathrm{d}(x) = 0$.

Definition: Differential Rng

A ***differential rng*** is an algebraic structure $\langle R; 0, -, \mathrm{d}, +, \cdot \rangle$ consisting of a rng $\langle R; 0, -, +, \cdot \rangle$ and a derivation $\mathrm{d} : R \to R$ on $\langle R; 0, -, +, \cdot \rangle$.

Definition: Subrng of Constants, $\mathrm{const}(R)$

Let R be a differential rng. The ***subrng of constants*** of R, denoted by $\mathrm{const}(R)$, is the set of constants in R.

$$\mathrm{const}(R) \coloneqq \{x \in R : \mathrm{d}(x) = 0\}$$

Constants Form a Subrng

Theorem: If R is a differential rng, then $\mathrm{const}(R) \leq R$.

Proof: It suffices to show that $\mathrm{const}(R)$ is closed under sums and products. Let $x, y \in \mathrm{const}(R)$.

$$\mathrm{d}(x + y) = \mathrm{d}(x) + \mathrm{d}(y) = 0 + 0 = 0 \implies x + y \in \mathrm{const}(R)$$

$$\mathrm{d}(x \cdot y) = \mathrm{d}(x) \cdot y + x \cdot \mathrm{d}(y) = 0 \cdot y + x \cdot 0 = 0 \implies x \cdot y \in \mathrm{const}(R)$$

Definition: Antiderivative, Integrable

Let R be a differential rng, and let $f \in R$. An ***antiderivative*** of f is an element $F \in R$ such that $\mathrm{d}(F) = f$. If f has an antiderivative, then we say that f is ***integrable***.

Definition: Differential Subrng, Differential Rng Extension

Let R be a differential rng. A ***differential subrng*** of R is a subrng $S \leq R$ that satisfies the following additional requirement:

- ***Closed under derivation:*** If $x \in S$, then $\mathrm{d}(x) \in S$.

If S is a differential subrng of R, then we say that R is a ***differential extension*** of S, and say that R/S (pronounced as "*R over S*") is a ***differential rng extension***.

Note that in a differential rng extension R/S, the derivation on R is required to coincide with the derivation on S when restricted to S. This distinguishes a differential rng extension R/S from a rng extension R/S where R happens to be a differential rng.

Definition: Differential Ring

A ***differential ring*** is an algebraic structure $\langle R; 0, 1, -, \mathrm{d}, +, \cdot \rangle$ consisting of a ring $\langle R; 0, 1, -, +, \cdot \rangle$ and a derivation $\mathrm{d} : R \to R$ on $\langle R; 0, -, +, \cdot \rangle$.

The terms ***differential integral domain***, ***differential PID***, ***differential field***, etc. are defined analogously.

1 is a Constant

Theorem: In any differential ring, $\mathrm{d}(1) = 0$.

Proof: We apply the Leibniz rule to $1 = 1 \cdot 1$.

$$\mathrm{d}(1) = \mathrm{d}(1 \cdot 1) = \mathrm{d}(1) \cdot 1 + 1 \cdot \mathrm{d}(1) = \mathrm{d}(1) + \mathrm{d}(1)$$

By cancellation, this implies that $\mathrm{d}(1) = 0$.

This result implies that the *subrng* of constants of a differential ring is, in fact, a *subring*. Hence, when R is a differential ring, we will refer to $\mathrm{const}(R)$ as its ***subring of constants***.

Algebraic Extensions Don't Create Antiderivatives

Theorem: Let K be a differential field of characteristic zero. If $f \in K$ does not have an antiderivative in K, then f cannot have an antiderivative in any algebraic differential extension of K.

Proof: We proceed by contraposition. Suppose that there exists an algebraic differential extension L/K having an element $g \in L$ for which $f = \mathrm{d}(g)$. Let $\mathrm{Tr} : K[g] \to K$ denote the trace map, and recall that Tr commutes with d. Since $f \in K$, we have $\mathrm{Tr}(f) = nf$, where

$n \coloneqq [K[g] : K]$. It follows that

$$\mathrm{d}\left(\frac{\mathrm{Tr}(g)}{n}\right) = \frac{1}{n}\mathrm{d}(\mathrm{Tr}(g)) = \frac{1}{n}\,\mathrm{Tr}(\mathrm{d}(g)) = \frac{1}{n}\,\mathrm{Tr}(f) = f$$

which shows that $\mathrm{Tr}(g)/n \in K$ is an antiderivative of f.