MATH 7720 Intro to Abstract Algebra 1
Notes and Selected Exercises

Krishna Chebolu
University of Missouri-Columbia

Abstract Algebra: Theory and Applications
Free Online Textbook by Thomas W. Judson

Contents

1 PRELIMINARIES

That basic stuff before the hard part begins.

1.1 Sets and Equivalence Relations

[1]

SET THEORY
A set is a well-defined collection of objects; that is, it is defined s.t. that we can determine for any given object x whether or not x belongs to the set.

- A set A is a **subset** of B (denoted $A \subset B$ if every element of A is in B.
- Furthermore, if $A \neq B$ but $A \subset B$, then A is a **proper subset** of B.
- If not a subset, use $\not\subset$.
- Two sets are **equal** if $A \subset B$ and $B \subset A$.
- **Union** is defined as $A \cup B = \{x : X \in A \text{ OR } x \in B\}$
- **Intersection** is defined as $A \cup B = \{x : X \in A \ \& \ x \in B\}$
- We generally work within a **universal** set U. So for any arbitrary set A, $A \subset U$.

[1] This subsection corresponds to section 1.2 in the textbook

- **Complement** is defined as $A' = \{x : x \in U \ \& \ x \notin A\}$
- **Difference** of two sets is defined as $A \backslash B = \{x : x \in A \ \& \ x \notin B\} = A \cap B'$

CARTESIAN PRODUCTS and MAPPINGS

Given sets A and B, we can define a new set A x B called the **cartesian product** of A and B. We get a set of ordered pairs:

$$\text{A x B}=\{(a, b) : a \in A \ \& \ b \in B\}$$

We can generalize this idea to n sets. So the ordered pairs would become n-tuples. Subsets of A x B are called **relations**. We define a **mapping** or **function** $f \subset$ A x B from set A to set B. The mapping is special in the sense that element $a \in A$ has a unique element $b \in B$ s.t. $(a, b) \in f$. We denote this as $f : A \to B$.

The set A is the **domain** (or input values) of f and $f(A) = \{f(a) : a \in A\} \subset B$ is the **range** or **image** (or output values) of f. A relation is **well-defined** if each element in the domain is assigned to a unique element in the range.

If $f : A \to B$ is a map and the image(f) = B (f(A)=B), then f is **onto** or **surjective**. A map is **one-to-one** (1-1) or **injective** if $a_1 \neq a_2$ implies that $f(a_1) \neq f(a_2)$; converse is also true. A map is **bijective** if it is 1-1 and onto.

Let $f : A \to B$ and $g : B \to C$. Define a new map from A to C as a **composition**, $(f \circ g)(x) = g(f(x))$. In $f, A \to B$, so B is inputted into g leading to C. Order of composition matters so $(f \circ g) \neq (g \circ f)$.

EQUIVALENCE RELATIONS and PARTITIONS

An important notion in maths is **equality**, which we generalize to equivalence relations and equivalence classes.

Definition 1.1. *An **equivalence relation** on a set X is a relation $R \subset X$ x X such that*

- $(x, x) \in \mathbb{R}$ $\forall x \in X$*:* ***reflexive property***
- $(x, y) \in \mathbb{R}$ $\Rightarrow (y, x) \in \mathbb{R}$*:* ***symmetric property***
- (x, y) *and* $(y, z) \in \mathbb{R}$ $\Rightarrow (x, z) \in \mathbb{R}$*:* ***transitive property***

*We denote this equivalence relation R on a set X using a **tilde**, so we write $x \sim y$ rather than $(x, y) \in \mathbb{R}$.*

A **partition** P of a set X is a collection of nonempty sets $X_1, X_2, ...$ s.t. $X_i \cap X_j = \emptyset$ for $i \neq j$ and $\cup_k X_k = X$. Let $\sim$ be an equivalence relation on a set X and let $x \in X$. Then $[x] = \{y \in X : y \sim x\}$ is called the **equivalence class** of x. When a partition of a set exists, there is some natural underlying equivalence relation, as the following theorem demonstrates.

Theorem 1.2. *Given an equivalence relation $\sim$ on a set X, the equivalence classes of X form a partition of X. Conversely, if $P = \{X_i\}$ is a partition of a set X, then there is an equivalence relation on X with equivalence class X_i*

Furthermore, we can also say that two classes of an equivalence relation are either disjoint or equal.

1.2 Reading Questions

[2]

1.3/1-2 What do relations and mappings have in common? What makes relations and mapping different?
A mapping or a function requires that for each value x in the domain, one and only one value y exists in the codomain s.t. y=f(x). A relation, however, is a general assignment of values from one set to another, regardless of assignment uniqueness. Every mapping is a relation, but not vice-versa.

1.3/3 State carefully the three defining properties of an equivalence relation. In other words, do not just name the properties, give their definitions.
There are three properties: reflexive– when an element can map to itself; symmetric– when one element x maps to another y, it implies that y maps to x as well; transitive– if element x maps to y and y maps to z, this implies that x maps to z.

1.3/4 What is the big deal about equivalence relations? (Hint: Partitions.)
Each equivalence relation divides the underlying set into disjoint equivalence classes. Two elements of the given set are equivalent to each other if and only if they belong to the same equivalence class.

1.3/5 Describe a general technique for proving that two sets are equal.
If two sets are equal, say A = B. Then A must be a subset of B, and B must be a subset of A; showing these two properties is sufficient.

1.3 Select Exercises

[3]

1.4/18 Determine which of the following functions are one-to-one and which are onto. If the function is not onto, determine its range.

[2] Section 1.3 in the textbook
[3] Section 1.4 in the textbook

(a) $f : \mathbb{R} \to \mathbb{R}$ **defined by** $f(x) = e^x$
We see that $\forall x, e^x > 0$; so, f(x) is not onto; also, $e^x = 0$ has no solution. The range is all positive real numbers defined as range(f)=$\{x \in \mathbb{R} \mid x > 0\}$. If $e^{x_1} = e^{x_2} \implies ln(e^{x_1} = e^{x_2}) \implies x_1 = x_2$, so 1-1.

(b) $f : \mathbb{Z} \to \mathbb{Z}$ **defined by** $f(n) = n^2 + 3$
Consider $f(-2) = f(2) \neq > -2 = 2$, not 1-1. Consider $f(n) = 2 \implies n^2 = -1 \notin \mathbb{Z}$, so not onto.

(c) $f : \mathbb{R} \to \mathbb{R}$ **defined by** $f(x) = sinx$
Not onto; consider f(x)=2. The range is given by $[-1, 1]$. Also, $sin(\pi) = sin(0) = 0$, not 1-1.

(d) $f : \mathbb{Z} \to \mathbb{Z}$ **defined by** $f(x) = x^2$
Consider $f(-2) = f(2) \neq > -2 = 2$, not 1-1. Consider $f(x) = -1 \implies x^2 = -1 \notin \mathbb{Z}$, so not onto. The range is given by $\mathbb{Z}^+$, or $[0, \infty)$.

1.4/19 Let $f : A \to B$ **and** $g : B \to C$ **be invertible mappings; that is, mappings such that** f^{-1} **and** g^{-1} **exists. Show that** $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
Define a new mapping $h : C \to A = (g \circ f)^{-1}$. So, $(g \circ f) \circ h = I_C$. We know that function composition is associative, so: $g \circ (f \circ h) = I_C$. We also have $f \circ h = I_B \circ (f \circ h) = (g^{-1} \circ g) \circ (f \circ h) = g^{-1} \circ (g \circ (f \circ h)) = (g^{-1} \circ I_C = g^{-1}$.
So, we can write $(g \circ f)^{-1} = h = I_A \circ h = (f^{-1} \circ f) \circ h) = f^{-1} \circ (f \circ h) = f^{-1} \circ g^{-1}$

1.4/20
(a) Define a function $f : \mathbb{N} \to \mathbb{N}$ **that is 1-1 but not onto.**
Consider $f(x) = x + 1$. The range is given by the interval $[2, \infty)$, assuming $\mathbb{N}$ starts with 1. 1-1 is trivial.

(b) Define a function $f : \mathbb{N} \to \mathbb{N}$ **that is onto but not 1-1.**
Consider the function $f(n) = 0$ if $n = 0$ and $n - 1$ if $n > 0$. $f(n) = y = n - 1$ when $n > 0$, so $y + 1 = n$; showing that for every n, there is a y in the codomain. It is not 1-1 since f(0)=f(1)=0.

1.4/21 Prove the relation defined on $\mathbb{R}^2$ **by** $(x_1, y_1) \sim (x_2, y_2)$ **if** $x_1^2 + y_1^2 = x_2^2 + y_2^2$ **is an equivalence relation.**
To show equivalence, we need to show the following three properties.

1. **Reflexivity:** We observe that $(x_1, y_1) \sim (x_1, y_1) \implies x_1^2 + y_1^2 = x_1^2 + y_1^2$
2. **Symmetry:** Consider $(x_1, y_1) \sim (x_2, y_2) \implies x_1^2 + y_1^2 = x_2^2 + y_2^2 \implies x_2^2 + y_2^2 = x_1^2 + y_1^2 \implies (x_2, y_2) \sim (x_1, y_1)$
3. **Transitivity:** Let $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. Then $x_1^2 + y_1^2 = x_2^2 + y_2^2$ and $x_2^2 + y_2^2 = x_3^2 + y_3^2$. We obtain $x_1^2 + y_1^2 = x_3^2 + y_3^2 \implies (x_1, y_1) \sim (x_3, y_3)$

1.4/22 Let $f : A \to B$ and $g : B \to C$ be maps.
(a) If f and g are both 1-1, show that $g \circ f$ is 1-1

Proof. Let f and g be 1-1. To show $g \circ f$ is 1-1, we need to show $g(f(x_1) = g(f(x_2) \implies x_1 = x_2$. Assume $g(f(x_1) = g(f(x_1)$ for some $x_1, x_2 \in A$. Since g is 1-1, we get $f(x_1) = f(x_2)$. Since f is 1-1, we get $x_1 = x_2$. Hence, proved. □

(b) If $g \circ f$ is onto, show g is onto

Proof. Let $g \circ f$ be onto. So we have $g(f(x))$ is onto, which is a map $A \to C$. So, $\forall c \in C, \exists a \in A$ s.t. $(g \circ f)^{-1}(c) = a \implies (f^{-1} \circ g^{-1})(c) = a \implies g^{-1}(c) = f(a) \implies g^{-1}(c) = b$, showing that $\forall c \in C, \exists b \in B$ s.t. $g(b) = c$. Hence, proved. □

(c) If $g \circ f$ is 1-1, show f is 1-1

Proof. Let $g \circ f$ be 1-1. Then $g(f(x_1)) = g(f(x_2)) \implies x_1 = x_2$. Suppose, for contradiction, that f is not 1-1. Then $\exists x_1, x_2$ s.t. $x_1 \neq x_2$ and $f(x_1) = f(x_2)$. Then $g \circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g \circ f(x_2)$, showing that $g \circ f$ is not 1-1– a contradiction. Thus, f is 1-1. □

(d) If $g \circ f$ is 1-1 and f is onto, show g is 1-1

Proof. Let $g \circ f$ be 1-1 and f be onto. To show g is 1-1, we need to show $g(b_1) = g(b_2) \implies b_1 = b_2$. So, choose $b_1, b_2 \in B$ s.t. $g(b_1) = g(b_2)$.
Since f is onto, we know $\exists a_1, a_2 \in A$ s.t. $f(a_1) = b_1$ and $f(a_2) = b_2$. Also, since $g \circ f$ is 1-1, we get: $(g \circ f)(a_1) = g(f(a_1)) = g(b_1) = g(b_2) = g(f(a_2)) = (g \circ f)(a_2)$, so we note that $a_1 = a_2$. Since f is well-defined, $f(a_1) = f(a_2) \implies b_1 = b_2$. Hence, proved. □

(e) If $g \circ f$ is onto and g is 1-1, show f is onto

Proof. Let $g \circ f$ be onto and g be 1-1. To show f is onto, we need to show that $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$. Since $g \circ f$ is onto, we know $\exists a \in A$ s.t. $\forall c \in C, (g \circ f)^{-1}(c) = a$, or can also be written as $g(f(a)) = c$. Since g is 1-1, there exists a unique b s.t. g(b)=c. Thus, f(a)=b, showing f is onto. □

1.4/23 Define a function on $\mathbb{R}$ by $f(x) = (x + 1)/(x - 1)$

(a) What are the domain and range of f?
Since the denominator cannot equal 0, we can input all values but 1; thus, the domain of $f = \mathbb{R} - \{1\}$. The range of f is $\mathbb{R}$.

(b) What is the inverse of f?
Let $y = (x+1)/(x-1) \implies yx - y = x + 1 \implies yx - x = y + 1 \implies x = (y+1)/(y-1)$. So $f^{-1} = f$.

(c) Compute $f \circ f^{-1}$
We see that f and its inverse are the same, thus $f \circ f^{-1} = I$.

(d) Compute $f^{-1} \circ f$
We see that f and its inverse are the same, thus $f^{-1} \circ f = I$.

1.4/24 Let $f : X \to Y$ be a map with $A_1, A_2 \subset X$ and $B_1, B_2 \subset Y$

(a) Prove $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

Proof. ($\leftarrow$) Consider $y \in f(A_1) \cup f(A_2)$, then $\exists x$ s.t. $x \in A_1$ or $x \in A_2$ s.t. f(x)=y. So $y \in f(A_1)$ or $y \in f(A_2)$, giving that $y \in f(A_1) \cup f(A_2)$. Thus, $f(A_1 \cup A_2) \leq f(A_1) \cup f(A_2)$.
($\rightarrow$) Consider $y \in f(A_1 \cup A_2)$, then $y \in f(A_1)$ or $y \in f(A_2)$. Then $\exists x$ s.t. $x \in A_1$ or $x \in A_2$, s.t. $f(x_1) = y$ or $f(x_2) = y$. In either case, we have $x \in (A_1 \cup A_2)$ s.t. f(x)=y. So $y \in f(A_1 \cup A_2)$. Thus, $f(A_1 \cup A_2) \geq f(A_1) \cup f(A_2)$.
Combining both directions, we get the desired result. □

(b) Prove $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$**. Give an example in which equality fails.**

Proof. Consider an element $y \in f(A_1 \cap A_2)$. Then, $\exists x$ s.t. $x \in A_1 \cap A_2$ where f(x)=y. Since x is in A_1 and A_2, y must be in $f(A_1)$ and $f(A_2)$. Thus, $y \in f(A_1) \cap f(A_2)$. If X is $\mathbb{N}$, A_1 contains all odd numbers, and A_2 contains all even numbers except 0. Define f s.t. a number is multiplied by 2 when odd and added 1 when even. We see that equality is not held. □

(c) Prove $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$**, where** $f^{-1}(B) = \{x \in A : f(X) \in B\}$

Proof.

$$\begin{aligned} \text{Let } x \in f^{-1}(B_1 \cup B_2) &\iff f(x) \in B_1 \cup B_2 \\ &\iff f(x) \in B_1 \text{ or } f(x) \in B_2 \\ &\iff x \in f^{-1}(B_1) \text{ or } x \in f^{-1}(B_2) \\ &\iff x \in f^{-1}(B_1) \cup f^{-1}(B_2) \end{aligned}$$

□

(d) Prove $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

Proof.

$$\begin{aligned} \text{Let } x \in f^{-1}(B_1 \cap B_2) &\iff f(x) \in B_1 \cap B_2 &&\iff f(x) \in B_1 \text{ and } f(x) \in B_2 \\ &\iff x \in f^{-1}(B_1) \text{ and } x \in f^{-1}(B_2) &&\iff x \in f^{-1}(B_1) \cap f^{-1}(B_2) \end{aligned}$$

□

(e) Prove $f^{-1}(Y \backslash B_1) = X \backslash f^{-1}(B_1)$

Proof.

$$\begin{aligned} \text{Let } x \in f^{-1}(Y \backslash B_1) &\iff f(x) \in Y \backslash B_1 &&\iff f(x) \in Y \text{ and } f(x) \notin B_1 \\ &\iff x \in f^{-1}(Y) \text{ and } x \notin f^{-1}(B_1) &&\iff x \in X \text{ and } x \notin f^{-1}(B_1) \\ &\iff x \in X \backslash f^{-1}(B_1) \end{aligned}$$

□

1.4/25 Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalence relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.

(a) $x \sim y$ **in** $\mathbb{R}$ **if** $x \geq y$

Consider counter example x = 2 and y = 1. The relation is not symmetric, and thus, not in equivalence.

(b) $m \sim n$ **in** $\mathbb{Z}$ **if** $mn > 0$

Consider counter example m = 0. The relation is not reflexive, and thus, not in equivalence.

(c) $x \sim y$ **in** $\mathbb{R}$ **if** $|x - y| \leq 4$

Consider counter example x = 1, y = 5, and z = 9. We see that the relation is not transitive, and thus, not in equivalence.

(d) $m \sim n$ **in** $\mathbb{Z}$ **if** $m \equiv n \pmod 6$

Proof. We need to show the following three properties:

1. **Reflexive**: $m \equiv m \pmod n \iff m - m \equiv 0 \pmod 6 \iff 0 \equiv 0 \pmod 6$
2. **Symmetric**: $m - n \equiv 0 \; mod \; 6 \implies n - m = 0 \; mod \; 6 \implies n \equiv m \; mod \; 6$
3. **Transitive**: $(m - n) + (n - p) = m - p \equiv 0 \; mod \; 6 \implies m \equiv p \; mod \; 6$

(mod 6) has six equivalence classes given by $[0], [1], [2], [3], [4], [5]$. We see that $[6] \equiv [0]$, and so on. □

1.4/26 Define a relation $\sim$ **on** $\mathbb{R}^2$ **by stating that** $(a, b) \sim (c, d)$ **iff** $a^2 + b^2 \leq c^2 + d^2$**. Show that** $\sim$ **is reflexive and transitive but not symmetric.**

Proof. Reflexive: Consider $(a, b) \sim (a, b)$, then $a^2 + b^2 \leq a^2 + b^2$. We see that this inequality will always hold true since $a^2 + b^2 = a^2 + b^2$.

Transitive: Consider $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $a^2 + b^2 \leq c^2 + d^2$ and $c^2 + d^2 \leq e^2 + f^2 \implies a^2 + b^2 \leq c^2 + d^2 \leq e^2 + f^2 \implies a^2 + b^2 \leq e^2 + f^2$, showing that $(a, b) \sim (e, f)$.

NOT symmetric: Consider counter example (1,2) and (3,4). We see that $1^2 + 2^2 = 5 \leq 25 = 3^2 + 4^2$, but $25 \not\leq 5$.

□

1.4/27 Show that an $m \times n$ **matrix gives rise to a well-defined map from** $\mathbb{R}^n \to \mathbb{R}^m$**.**

Proof. Consider an $m \times n$ matrix $A \in \mathbb{R}^{m \times n}$. Define $f : \mathbb{R}^n \to \mathbb{R}^m$ by, for some $v \in \mathbb{R}^n, f(v) = Av = u \in \mathbb{R}^m$. To show a map is well-defined, we need two things:

1. The output is in the codomain: We know that $Av = u \in \mathbb{R}^m$, so u is an $m \times 1$ vector. Since $A \in \mathbb{R}^{m \times n}$ and $v \in \mathbb{R}^n$, all the entries of u are in $\mathbb{R}$. Thus, $u \in \mathbb{R}^m$.

2. There is only output per input: Suppose $v_1, v_2 \in \mathbb{R}^n$, s.t. $v_1 = v_2$. Then $Av_1 = Av_2 \implies f(v_1) = f(v_2) \implies u_1 = u_2$.

□

1.4/28 Find the error in the following argument by providing a counterexample. "The reflexive property is redundant in the axioms for an equivalence relation. If $x \sim y$, then $y \sim x$ by the symmetric property. Using the transitive property, we can deduce that $x \sim x$. "
Consider the counter-example: Let $X = \mathbb{N} \cup \{\pi\}$ and define $x \sim y$ if $x + y \in \mathbb{N}$.
We see that this would not work for $x = \pi$, since $\pi + \pi = 2\pi \notin \mathbb{N}$.

2 INTEGERS

The integers are the building blocks of mathematics.

2.1 Mathematical Induction

[4] Instead of attempting to verify a statement about some subset $S \subset \mathbb{N}$ on a case-by-case basis (an impossible task if S is an infinite set), we give a specific proof for the smallest integer being considered, followed by a generic argument showing that if the statement holds for a given case, then it must also hold for the next case in the sequence. We summarize mathematical induction in the following axiom.

Theorem 2.1. ***First Principle of Mathematical Induction****. Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If, for all, $k \in \mathbb{Z}$ with $k \geq n_0$, $S(k) \implies S(k+1)$ is True, then $S(n)$ is true for all $n \geq n_0, n \in \mathbb{Z}$.*

We also sometimes use an equivalent form of the principle above:

Theorem 2.2. ***Second Principle of Mathematical Induction****. Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If $S(n_0), S(n_0 + 1), ..., S(k) \implies S(k+1)$ $\forall k \geq n_0$, then $S(n)$ is true for all $n \geq n_0, n \in \mathbb{Z}$.*

A nonempty subset $S \subset \mathbb{Z}$ is **well-ordered** if S contains a least element.

NOTE 2.3. *$\mathbb{Z}$ is not well-ordered since it does not contain a smallest element. However, $\mathbb{N}$ is well-ordered.*

[4] Section 2.1 in the textbook

From the note above, we can infer the following:

Theorem 2.4. ***Principle of Well-Ordering*** *Every nonempty subset of the natural numbers is well-ordered.*

aaaand another:

Theorem 2.5. *The Principle of Mathematical Induction implies the Principle of Well-Ordering, i.e., every nonempty subset of* $\mathbb{N}$ *contains a least element.*

2.2 Division Algorithm

[5] A direct application of the Principle of Well-Ordering is the following division algorithm.

Theorem 2.6. ***Division Algorithm*** *Let* $a, b \in \mathbb{Z}, b > 0$. *Then* $\exists! q, r \in \mathbb{Z}$ *s.t.* $a = bq + r$, *where* $0 \leq r < b$.

Proof. Consider the set $S = \{a - bq \mid q \in \mathbb{Z},\ a - bq \geq 0\}$. Since S contains all non-negative differences of the form $a - bq$, S is non-empty.

By the well-ordering principle, S contains a smallest element, say $r = a - bq_0$ for some integer q_0. Thus,

$$a = bq_0 + r, \quad \text{where} \quad r \geq 0.$$

We need to show that $r < b$. Assume, for contradiction, that $r \geq b$. Then, we could write:

$$r - b \geq 0.$$

But then

$$a = bq_0 + r = bq_0 + (r - b + b) = b(q_0 + 1) + (r - b),$$

implying $r - b$ is a smaller non-negative element in S than r, which contradicts the minimality of r. Therefore, $r < b$.

To show uniqueness, suppose there exist q_1 and r_1 such that:

$$a = bq_1 + r_1 \quad \text{with} \quad 0 \leq r_1 < b.$$

Then,

$$bq_0 + r = bq_1 + r_1.$$

Rearranging, we get:

$$b(q_0 - q_1) = r_1 - r.$$

Since $0 \leq r, r_1 < b$, the right-hand side must satisfy $|r_1 - r| < b$. However, since $b(q_0 - q_1)$ is a multiple of b, the only possibility is $q_0 = q_1$ and $r = r_1$, proving the uniqueness. □

Theorem 2.7. *Let a and b be nonzero integers. Then, integers r and s exist, such that gcd(a,b) = ar + bs. Furthermore, the gcd of a and b is unique.*

Corollary 2.8. *If a and b are relatively prime, then ar + bs = 1.*

We can find the most common divisor of two numbers using the division algorithm.

[5] Section 2.2 in the textbook

The Euclidean Algorithm is a method to find the greatest common divisor (GCD) of two integers a and b (with $a \geq b$). The steps are as follows:

1. Divide a by b to obtain the quotient q and remainder r:

$$a = bq + r, \quad \text{where } 0 \leq r < b.$$

2. Replace a with b and b with r.

3. Repeat the process until $r = 0$; replacing r with r', and so on.

Lemma 2.9. ***Euclid*** *Let $a, b \in \mathbb{Z}$ and p be prime. If $p|ab$, then either $p|a$ or $p|b$.*

Proof. Suppose $p \nmid a$, we must show $p|b$. Since $gcd(a, p) = 1$, $\exists r, s$ s.t. $ar + ps = 1$. So, $b = b(ar + ps) = ab(r) + p(bs)$. Since $p|ab$ and $p|p(bs) \implies p|(ab(r) + p(bs)) \implies p|b$. □

Theorem 2.10. ***Euclid*** *There exists an infinite number of primes.*

Theorem 2.11. ***Fundamental Theorem of Arithmetic*** *Every integer greater than 1 can be uniquely factored into prime numbers, up to the order of the factors. That is, if n is an integer with $n > 1$, then n can be expressed as:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $p_1, p_2, \ldots, p_k$ are primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. Moreover, this factorization is unique except for the order of the prime factors.

2.3 Reading Questions

[6]

2.3/3 Find $r, x \in \mathbb{Z}$ s.t. $r(84) + s(52) = gcd(84, 52)$.

[6] Section 2.3 in the textbook

First, we find the GCD of 84 and 52 using the Euclidean Algorithm:

$$84 = 52 \times 1 + 32,$$

$$52 = 32 \times 1 + 20,$$

$$32 = 20 \times 1 + 12,$$

$$20 = 12 \times 1 + 8,$$

$$12 = 8 \times 1 + 4,$$

$$8 = 4 \times 2 + 0.$$

Therefore, $\gcd(84, 52) = 4$.
Now, we work backwards using the Extended Euclidean Algorithm to express 4 as a linear combination of 84 and 52:

$$4 = 12 - 8,$$

$$4 = 12 - (20 - 12) = 2(12) - 20,$$

$$4 = 2(32 - 20) - 20 = 2(32) - 3(20),$$

$$4 = 2(32) - 3(52 - 32) = 5(32) - 3(52),$$

$$4 = 5(84 - 52) - 3(52) = 5(84) - 8(52).$$

Thus, the integers $r = 5$ and $s = -8$ satisfy the equation:

$$5(84) + (-8)(52) = 4.$$

2.3/4 Explain the use of the term "induction hypothesis."
The term "induction hypothesis" is used in the context of mathematical induction, a proof technique that establishes the truth of an infinite sequence of statements. The induction hypothesis is a crucial step in the process, where we assume the statement to be true for a particular case $n = k$ (for some integer k) to prove it for the next case, $n = k + 1$.

2.3/5 What is Goldbach's Conjecture? And why is it called a "conjecture"?
Goldbach's Conjecture is a famous unsolved problem in number theory. It states: *Every even integer greater than 2 can be expressed as the sum of two prime numbers.* Despite being tested for very large numbers and appearing true in all cases examined, no one has yet been able to prove it for all even integers, nor has anyone found a counterexample. The term **conjecture** is used in mathematics to describe a statement or proposition that is believed to be true based on observations or evidence but has not been proven rigorously.

2.4 Select Exercises

[7]

DO

3 GROUPS

The theory of groups occupies a central position in mathematics. Modern group theory arose from an attempt to find the roots of a polynomial in terms of its coefficients. Groups now play a central role in such areas as coding theory, counting, and studying symmetries; many areas of biology, chemistry, and physics have benefited from group theory.

3.1 Integer Equivalence Classes and Symmetries

[8]

An important set of equivalence classes are the integers mod n. These sets partition $\mathbb{Z}$ into equivalence classes denoted $\mathbb{Z}_n$. Some important properties are given by:

Theorem 3.1. *Let $\mathbb{Z}_n$ be the set of equivalence classes of the integers mod n and $a, b, c, \in \mathbb{Z}$.*

1. *Addition and multiplication are commutative:* $a + b \equiv b + a \pmod{n}$ *and* $ab \equiv ba \pmod{n}$
2. *Addition and multiplication are associative:* $(a+b)+c \equiv a+(b+c \pmod{n}$ *and* $(ab)c \equiv a(bc) \pmod{n}$
3. *There are both additive and multiplicative identities:* $a + 0 \equiv a \pmod{n}$ *and* $a \cdot 1 \equiv a \pmod{n}$
4. *Multiplication distributes over addition:* $a(b + c) \equiv ab + ac \pmod{n}$
5. *For every integer a there is an additive inverse -a:* $a + (-a) \equiv 0 \pmod{n}$
6. *Let a be a nonzero integer. Then gcd(a,n) = 1 iff there exists a multiplicative inverse b for a* $\pmod{n}$*, i.e., a nonzero integer b s.t.* $ab \equiv 1 \pmod{n}$

Commutativity is a type of symmetry on operations since, regardless of arrangement of the elements undergoing the operation, the result is preserved. This notion of symmetry can be applied to geometric figures (well, the idea of symmetry is *from* geometric figures). A **symmetry** of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles. A map from the plane to itself preserving the symmetry of an object is called a **rigid motion**.

These rigid motions that preserve the original shape, so to speak, can be represented by numbers. Consider an equilateral triangle, we can denote its original position of vertices by (1 2 3), which is, now, the identity position– our reference position for future rigid motion.

[7] Section 2.4 in the textbook
[8] Section 3.1 in the textbook

If we rotate this triangle clockwise, we get (1 2 3) $\to$ (3 1 2). We would represent this as a matrix, but shorthanded, we just write (3 1 2). This specific action gives rise to a **permutation** in the position. We have three points, so we have $3! = 6$ permutations for a triangle. These permutations can be achieved using rotation and reflection actions.

3.2 Definitions and Examples

[9]

The integers mod n and the symmetries of a triangle or a rectangle are examples of groups. A **binary operation** or **law of composition** on a set G is a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$, or ab in G, called the composition of a and b. A **group** $(G, \circ)$ is a set G together with a law of composition $(a, b) \mapsto a \circ b$ that satisfies the following axioms.

- Law of composition is **associative**.
- There exists an element referred to as the **identity element**, s.t. $\forall a \in G,\ e \circ a = e = a \circ e$.
- For each element a, there is an inverse in G, denoted by a^{-1} s.t. $a \circ a^{-1} = a^{-1} \circ a = e$.

Furthermore, a group G is **abelian** if it is **commutative**, i.e., $a \circ b = b \circ a,\ \forall a, b \in G$. If this property does not hold, then a group is **nonabelian** or **noncommutative**.

Above, I mentioned that we denote the composition by $\circ$, but if the operation is something common like addition, we use that symbol. Instead of writing $a \circ b$, when it is obvious, we can observe that ab is used.

From the axioms of groups, we can also observe that groups are closed. So, $\forall a, b \in G,\ a * b \in G$. This property indicates that for finite groups, we can form a **Cayley table**; a convenient way to describe a group in terms of an addition or multiplication table. Speaking of finite, a group is **finite** if it contains a finite number of elements, otherwise it is an **infinite group**. The number of elements in a group is its **order**.

Let us talk more about the basic properties of groups.

Theorem 3.2. *The following are true*

1. *The identity element in a group G is unique; that is, there exists only one element $e \in G$ s.t. $eg = ge = g\ \forall g \in G$.*
2. *If g is any element in a group G, then the inverse of g, denoted by g^{-1}, is unique.*
3. *Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.*
4. *Let G be a group. $\forall a \in G,\ (a^{-1})^{-1} = a$.*
5. *Let G be a group and a and b be any two elements in G. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.*

[9] Section 3.2 in the textbook

6. *If G is a group and $a, b, c \in G$, then $ba = ca \implies ab = ac \implies b = c$. So,* ***right*** *and* ***left cancellation*** *laws are true in groups.*

Now, some basic types of groups that we will encounter in the future.

- **Group of units**, denoted $U(n)$. $\forall k \in \mathbb{Z}\backslash\{0\}$ has an inverse in $\mathbb{Z}_n$ if k is relatively prime to n. So, for example, $U98) = \{1, 3, 5, 7\}$.
- $M_2(\mathbb{R})$ denotes the set of all 2×2 matrices.
- The set of invertible matrices forms a group called the **general linear group**, denoted $GL(\mathbb{R}, n)$, where n is the matrix dimension.
- $SL(\mathbb{R}, n)$ is a subset of $GL(\mathbb{R}, n)$ and is called the **special linear group**. This subset contains all $n \times n$ matrices with determinant 1.
- **Quaternion group**

3.3 Subgroups

[10]

Sometimes we wish to investigate smaller groups sitting inside a larger group. We define a **subgroup** H of a group G to be a subset H of G such that when the group operation of G is restricted to H, H is a group in its own right. Observe that every group G with at least two elements will always have at least two subgroups, the subgroup consisting of the identity element alone and the entire group itself. The subgroup $H = \{e\}$ of a group G is called the **trivial subgroup**. A subgroup that is a proper subset of G is called a **proper subgroup**.

We can formally describe a subgroup in the following theorem.

Theorem 3.3. *A subset H of G is a subgroup iff satisfies the following conditions*

1. *The identity e of G is in H. (identity)*
2. *If $h_1, h_2 \in H$, then $h_1 h_2 \in H$. (closure)*
3. *If $h \in H$, then $h^{-1} \in H$. (inverse)*

We can combine the three properties from above to do a one-shot proof;so, we can also describe a subgroup in the following manner.

Theorem 3.4. *Let H be a subset of a group G. Then H is a subgroup of G iff $H \neq \emptyset$, and whenever $g, h \in H$, then $gh^{-1} \in H$.*

[10] This subsection corresponds to section 3.3 in the textbook

3.4 Reading Questions

[11]

3.4/1 In the group $\mathbb{Z}_8$ compute, (a) 6 + 7, and (b) 2^{-1}.
(**a**) $6 + 7 \pmod 8 \equiv 13 \pmod 8 \equiv 5 \pmod 8$
(**b**) 2^{-1} does not exist.

3.4/2 In the group $U(16)$ compute, (a) $5 \cdot 7$, and (b) 3^{-1}.
(**a**) $5 \cdot 7 \pmod{16} \equiv 35 \pmod{16} \equiv 3 \pmod{16}$
(**b**) $3^{-1} \equiv 11 \pmod{16}$

3.4/3 State the definition of a group.
A **group** $(G, \circ)$ is a set G together with a law of composition $(a, b) \mapsto a \circ b$ that satisfies the following axioms.

- Law of composition is **associative**.
- There is an **identity element**, so $\forall a \in G,\ e \circ a = e = a \circ e$.
- For each element, there is an inverse in G.

3.4/4 Explain a single method that will decide if a subset of a group is itself a subgroup.
Whenever $g, h \in H \implies gh^{-1} \in H$, and $H \subset G \implies H < G$.

3.4/5 Explain the origin of the term *abelian* for a commutative group.
An abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written. That is, the group operation is commutative. With addition as an operation, the integers and the real numbers form abelian groups, and the concept of an abelian group may be viewed as a generalization of these examples. Abelian groups are named after Niels Henrik Abel.

3.4/6 Give an example of a group you have seen in your previous mathematical experience, but that is not an example in this chapter.
The ways a shape can be reflected or rotated.

3.5 Select Exercises

[12]

3.5/10 Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

[11] Section 3.4 in the textbook
[12] Section 3.5 in the textbook

is a group under matrix multiplication. This group, known as the Heisenberg group, is important in quantum physics. Matrix multiplication in the Heisenberg group is defined by

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & c+c' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix}$$

Proof. To show that Heisenberg group is a group under multiplication, we need to show the following four properties:

1. **Closure**: Given two matrices $M_1 = \begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}$, their product is:

$$M_1 \cdot M_2 = \begin{pmatrix} 1 & a_1+a_2 & c_1+a_1b_2+c_2 \\ 0 & 1 & b_1+b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

   This product is also in the Heisenberg form, hence the set is closed under multiplication.

2. **Associativity**: Matrix multiplication is associative by definition, so for any M_1, M_2, M_3 in the Heisenberg group:

$$(M_1 \cdot M_2) \cdot M_3 = M_1 \cdot (M_2 \cdot M_3)$$

3. **Identity elemtent**: The identity element in this group is:

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

   For any matrix M in the Heisenberg group, $I \cdot M = M \cdot I = M$.

4. **Inverse**: For any matrix $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$, the inverse is:

$$M^{-1} = \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$

   which satisfies $M \cdot M^{-1} = M^{-1} \cdot M = I$.

□

3.5/13 Show that $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ is a group under the operation of multiplication.

Proof. Similar to the previous problem, to show the claim is a group, we need to show the following properties:

1. **Closure**: For any $a, b \in \mathbb{R}^*$, the product ab is also in $\mathbb{R}^*$ since $ab \neq 0$. Hence, $\mathbb{R}^*$ is closed under multiplication.

2. **Associativity**: Since $\mathbb{R}^* \subset \mathbb{R}$, multiplication in $\mathbb{R}^*$ is associative: for all $a, b, c \in \mathbb{R}^*$,
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
Thus, associativity holds.

3. **Identity elemtent**: The identity element in $\mathbb{R}^*$ is 1, as for any $a \in \mathbb{R}^*$,
$$1 \cdot a = a \cdot 1 = a$$

4. **Inverse**: For every $a \in \mathbb{R}^*$, there exists an inverse $a^{-1} \in \mathbb{R}^*$ such that
$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$
This inverse $a^{-1} = 1/a > 0$, since $a \neq 0$, so $1/a \subset \mathbb{R}^*$.

□

3.5/15 Prove or disprove that every group containing six elements is abelian.
Proof. Consider the counter-example S_3, a.k.a., the dihedral group. This group is not abelian ($s_{12} * s_{13} \neq s_{13} * s_{12}$, for $s_{ij} \in S_3$, where $i, j = \{1, 2, 3\}$). Thus, every group containing six elements is not abelian. □

3.5/27 Prove that the inverse of $g_1 g_2 ... g_n$ is $g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}$.
Proof. By the definition of inverse, we must show that $g * g^{-1} = g^{-1} * g = I$:

1. Consider $(g_1 g_2 ... g_n) * (g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}) = g_1 g_2 ... g_n * g_n^{-1} g_{n-1}^{-1} ... g_1^{-1} = g_1 ... g_{n-1} * g_{n-1}^{-1} ... g_1^{-1} = ... = g_1 * g_1^{-1} = I$

2. Consider $(g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}) * (g_1 g_2 ... g_n) = g_n^{-1} g_{n-1}^{-1} ... g_1^{-1} * g_1 g_2 ... g_n = g_n^{-1} ... g_2^{-1} * g_2 ... g_n = ... = g_1^{-1} * g_1 = I$

Thus, the inverse of $g_1 g_2 ... g_n$ is $g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}$. □

3.5/31 Show that if $a^2 = e$ for all elements a in a group G, then G must be abelian.
Proof. We know that $x^2 = e,\ \forall x \in G \implies x = x^{-1},\ \forall x \in G$. Consider $a, b \in G \implies ab \in G$, then $|ab| = 2 \implies (ab)^2 = abab = e \implies ba = a^{-1}b^{-1} = ab$ (left and right multiplication of $abab$ with a^{-1} and b^{-1}, respectively; then we know that $a^{-1} = a$ and $b^{-1} = b$). Thus, G is abelian. □

3.5/41 Prove that $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}$ and a and b are both nonzero$\}$ is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

Proof. Choose $a = 1, b = 1$, then we get $1+1\sqrt{2} \in G$, showing that G is nonempty. Suppose two elements $g_1, g_2 \in G$, then $g_1 = a_1 + b_1\sqrt{2}$ and $g_2 = a_2 + b_2\sqrt{2}$, for some $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Note that the inverse of g_2 can be written as $g_2^{-1} = \frac{1}{a_2+b_2\sqrt{2}} = \frac{1}{a_2+b_2\sqrt{2}} \cdot \frac{a_2-b_2\sqrt{2}}{a_2-b_2\sqrt{2}} = \frac{a_2-b_2\sqrt{2}}{a_2^2-2b_2^2} = \frac{a_2}{a_2^2-2b_2^2} - \frac{b_2\sqrt{2}}{a_2^2-2b_2^2}$, where $c = \frac{a_2}{a_2^2-2b_2^2} \in \mathbb{Q}$ and $d = \frac{b_2}{a_2^2-2b_2^2} \in \mathbb{Q}$. Then, consider $g_1 g_2^{-1} = (a_1 + b_1\sqrt{2})(c + d\sqrt{2}) = a_1c + a_1d\sqrt{2} + b_1c\sqrt{2} + 2b_1d = (a_1c+2b_1d) + (a_1d+b_1c)\sqrt{2} \in G$, since $(a_1c+2b_1d) \in \mathbb{Q}$ and $(a_1d+b_1c) \in \mathbb{Q}$. Thus, $G < \mathbb{R}^*$. □

3.5/47 Prove or disprove: If H and K are subgroups of G, then $HK = \{hk : h \in H$ and $k \in K\}$ is a subgroup of G. What if G is abelian?

1. **Is $H < G$?**
   Consider the group $G = S_3$, the symmetric group on 3 elements, and let H and K be subgroups defined by:

   $$H = \{e, (12)\}, \quad K = \{e, (23)\}$$

   Then HK contains elements such as $(12)(23) = (123)$. However, HK is not closed under multiplication, as $(12)(123) = (13) \notin HK$. Thus, HK is not a subgroup of S_3.

2. **What if G is abelian?**
   Now, suppose G is abelian and $x, y \in HK$. Then, for any $h_1, h_2 \in H$ and $k_1, k_2 \in K$:

   $$xy = (h_1k_1)(h_2k_2) = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2) \in HK$$

   The identity e of G is in HK since $e = e \cdot e$ with $e \in H$ and $e \in K$. Moreover, for any $x = hk \in HK$, its inverse $x^{-1} = k^{-1}h^{-1}$ also belongs to HK since $k^{-1} \in K$ and $h^{-1} \in H$. So, if G is abelian, then $HK < G$

4 CYCLIC GROUPS

4.1 Cyclic Subgroups

[13]

Often a subgroup will depend entirely on a single element of the group; that is, knowing that particular element will allow us to compute any other element in the subgroup.

Theorem 4.1. *Let G be a group and $a \in G$. Then the set $< a >= \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G. Furthermore, $< a >$ is the smallest subgroup of G that contains a.*

For $a \in G$, we call $< a >$ the **cyclic subgroup** generated by a. If G contains some element a s.t. $G =< a >$, then G is a **cyclic group**. In this case, a is its **generator**. The

[13] Section 4.1 in the textbook

order of a is defined as the smallest +ve integer n s.t. $a^n = e$, written as $|a| = n$. If no such n exists, the order is ∞.

Theorem 4.2. *Every subgroup of a cyclic group is cyclic.*

Theorem 4.3. *Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = gcd(k, n)$.*

4.2 Circle Group and Roots of Unity

[14]

The multiplicative group of complex numbers, $\mathbb{C}^*$, possesses some interesting subgroups of finite order. First, we consider the **circle group**.

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}.$$

Theorem 4.4. *The circle group is a subgroup of $\mathbb{C}^*$.*

Though the circle group has infinite order, it has many interesting finite subgroups, one of them is $H = \{1, -1, i, -i\}$. Note that for $z \in H$, $z^4 = 1$, called the 4th roots of unity. For any $z^n = 1$, the complex number z are called the **nth roots of unity**.

Theorem 4.5. *If $z^n = 1$, then the nth roots of unity are*

$$z = exp(\frac{2k\pi}{n}),$$

where $k = 0, 1, ..., n-1$. Furthermore, the nth roots of unity form a cyclic subgroup of $\mathbb{T}$ of order n.

A generator for the group of the nth roots of unity is called a **primitive nth root of unity**.

4.3 Reading Questions

[15]

4.4/1 What is the order of the element 3 in $U(20)$?
Since $gcd(3, 20) = 1$, $|3| = 1$.

4.4/2 What is the order of the element 5 in $U(23)$?
Similar to above, $|5| = 1$.

4.4/3 Find three generators of $\in \mathbb{Z}_8$.
All generators are coprime to 8 $\implies$ generators are $\{1, 3, 5, 7\}$.

[14] Parts of section 4.2 in the textbook
[15] Section 4.4 in the textbook

4.4/4 Find three generators of the 5th roots of unity.
The 5th roots of unity are the complex numbers that satisfy the equation:

$$z^5 = 1$$

These roots are given by:

$$z_k = e^{2\pi ik/5} \quad \text{for } k = 0, 1, 2, 3, 4$$

Explicitly, they are:

$$1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}$$

The elements that generate the cyclic group of 5th roots of unity are those whose exponents are relatively prime to 5, namely:

$$e^{2\pi i/5}, e^{4\pi i/5}, e^{8\pi i/5}$$

Thus, the generators of the 5th roots of unity are:

$$e^{2\pi i/5}, e^{4\pi i/5}, e^{8\pi i/5}$$

4.4 Select Exercises

[16]

4.5/1 Prove or disprove each of the following statements.

[16] Section 4.5 in the textbook

1. **All of the generators of $\mathbb{Z}_{60}$ are prime**.
   Consider counter example 49. Since gcd(49, 60) = 1, 49 is a generator. Thus, the claim is false.

2. $U(8)$ **is cyclic.**

   Proof. $U(8) = \{1, 3, 5, 7\}$. We have $|1| = 1$ and the order of the remaining elements is 2. Thus, $U(8)$ is not cyclic. □

3. $\mathbb{Q}$ **is cyclic.**

   Proof. Suppose, for contradiction, $\mathbb{Q}$ is cyclic. Then it would be generated by $\frac{a}{b} \in \mathbb{Q}$ s.t. $a, b \in \mathbb{Z}$, and $gcd(a, b) = 1$ and $a, b \neq 0$. Then the set $< \frac{a}{b} >$ contains all integral multiples of a/b. Consider the rational number $a/2b \implies z \times a/b = 1/2b,\ z \in \mathbb{Z}$. Then $z = 1/2 \notin \mathbb{Z}$, a contradiction. Thus, $\mathbb{Q}$ is not cyclic. □

4. **If every proper subgroup of a groupG is cyclic, then G is a cyclic group.**
   The claim is not true. Consider the counter example $U(8)$. The group has four subgroups, the cyclic groups generated by each element.

5. **A group with a finite number of subgroups is finite.**

   Proof. Note that each $a \in G$ generates a subgroup $< a >$. Noting that

   $$G = \bigcup_{a \in G} \langle a \rangle$$

   and any elements of infinite order produce a subgroup isomorphic to $\mathbb{Z}$, so that this subgroup has infinitely many subgroups, i.e., if $< a >$ is infinite, then $< a^n >$, $\forall n \in \mathbb{N}$ is an infinite family of subgroups, a contradiction. Then G is a finite union of finite sets, making it a finite set. □

4.5/2 Find the order of each of the following elements.

1. $5 \in \mathbb{Z}_{12}$
   Since $gcd(5, 12) = 1$, 5 is generator of $\mathbb{Z}_{12} \implies |5| = 12$.

2. $\sqrt{3} \in \mathbb{R}$
   So in the case of additive $\mathbb{R}$ we are looking at solutions to $n\sqrt{3} = 0$. Since $\sqrt{3} > 0$ then by induction $n\sqrt{3} > 0$ and so this only works for $n = 0$. Hence $|\sqrt{3}| = \infty$. .

3. $\sqrt{3} \in \mathbb{R}^*$
   Similar to above, we are looking for solutions to $\sqrt{3}n = 1$, however $\sqrt{3}^n > 1, \ \forall n \in \mathbb{N}$. Thus, $|\sqrt{3}| = \infty$.

4. $-i \in \mathbb{C}^*$
   We are looking for $-i^n = 1$, we see that $n = 2 \implies |-i| = 2$.

5. $72 \in \mathbb{Z}_{240}$
   $gcd(240, 72) = 24$. Thus, $|72| = 240/24 = 10$.

6. $312 \in \mathbb{Z}_{471}$
   $gcd(312, 471) = 3$. Thus, $|312| = 471/3 = 157$.

4.5/7 What are all of the cyclic subgroups of the quaternion group, Q_8.
The Quaternion group is given by $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. By Lagrange's theorem, all possible proper subgroups have order 2 or 4. Since all groups of order 2 are cyclic, examination of subgroups of order 4 are necessary, so we are left with

$$< i >= \{\pm 1, \pm i\}$$

which is generated by i or $-i$; cyclic by definition. Similarly, we can say the same for subgroups generated by $< j >$ and $< k >$. These are all the cyclic subgroups of the quaternion group.

4.5/22 Calculate each of the following.

1. $292^{3171} \pmod{582}$
   We can write $3171 = 2^{11} + 2^{10} + 2^6 + 2^5 + 2^1 + 2^0$. Solving for each $292^{2^i}, \ i \in \{0, 1, 5, 6, 10, 11\}$ and multiplying the result, we get 292.

2. $2557^{341} \pmod{5681}$
   Done similarly to above.

3. $2071^{9521} \pmod{4724}$
   Done similarly to above.

4. $971^{321} \pmod{765}$
   Done similarly to above.

4.5/23 Let $a, b \in G$. Prove the following statements.

1. **The order of a is the same as the order of a^{-1}.**

   Proof. Let $a^n = e$, then $e = (aa^{-1})^n = a^n(a^{-1})^n = e(a^{-1})^n = (a^{-1})^n$. Now, let $(a^{-1})^n = e$, then $e = (aa^{-1})^n = a^n(a^{-1})^n = a^n e = a^n$. So, $a^n = e \iff (a^{-1})^n = e$. □

2. $\forall g \in G,\ |a| = |g^{-1}ag|$.

   Proof. Let $|a| = n \implies a^n = e$. Then

   $$(g^{-1}ag)^n = g^{-1}agg^{-1}ag...g^{-1}ag = g^{-1}a^n g = g^{-1}eg = g^{-1}g = e,$$

   giving $|a| \leq |g^{-1}ag|$. For the other side, consider $b = g^{-1}ag$ and $h = g^{-1}$, then we get $|h^{-1}bh| = |(g^{-1})^{-1}g^{-1}agg^{-1}| = |a| \leq |b| = |g^{-1}ag|$. Hence, proved. □

3. **The order of ab is the same as the order of ba.**

   Proof. Let $|ab| = n$. Then consider $(ba)^{n+1} = b(ab)^n a = ba \implies (ba)^n = e$. So, $|ab| \leq |ba|$. Suppose $|ba| = m$ and consider $(ab)^{m+1} = a(ba)^m b = ab \implies (ab)^m = e$, showing $|ab| \geq |ba|$. □

4.5/26 Prove that $\mathbb{Z}_p$ has no trivial subgroups if p is prime.
Proof. Suppose a nontrivial subgroup $H < \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is cyclic, H must be cyclic too; let $H =< b >,\ b \in \mathbb{Z}_p$. Then $|b| = \frac{p}{gcd(p,b)} = p$. Then $H = \mathbb{Z}_p$. So the only subgroups of $\mathbb{Z}_p$ are $\{0\}$ and itself. □

4.5/31 Let G be an abelian group. Show that the elements of finite order in G form a subgroup, called the *torsion subgroup* of G.
Proof. We know that the identity has finite order in any group G, thus the subgroup is nonempty. Let $g, h \in G$ have orders m and n. Since $(g^{-1})^m = e$ and $(gh)^{mn} = e$, the elements of finite order in G form a subgroup of G. □

4.5/37 Prove that if G has no proper nontrivial subgroups, then G is a cyclic group.
Proof. Suppose G has no proper nontrivial subgroups. Take an element $a \in G$ for which $a \neq e$. Consider the cyclic subgroup $< a >$. This subgroup contains at least e and a, so it is not trivial. But G has no proper subgroups, so it must be that $< a >= G$. Thus G is cyclic, by definition of a cyclic group. □

4.5/39 Prove that if G is a cyclic group of order m and $d|m$, then G must have a subgroup of order d.
Proof. Since $d|m \implies m = dk,\ k \in \mathbb{Z}$. Let a be a generator of G and consider a^k. Clearly, $(a^k)^d = a^{kd} = e$. So $|a^k| \geq d$. If $|a^k| < d \implies |a^{kc}| = e,\ c < d$ which gives us $kc < m$, with kc as the new order of a, a contradiction. Thus, a subgroup $|a^k| = d$ proving the claim. □

4.5/44 Let $\alpha \in \mathbb{T}$. Prove that $\alpha^m = 1$ and $\alpha^n = 1 \iff \alpha^d = 1$ for $d = gcd(m, n)$.
Proof. ($\rightarrow$) Since $d = gcd(m, n)$, we can write $d = rm + sn$, for some $r, s \in \mathbb{Z}$. So, consider $a^d = a^{rm+sn} = a^{rm} \cdot a^{sn} = (a^m)^r \cdot (a^n)^s = 1 \implies 1^r \cdot 1^s = 1$.
($\leftarrow$) Suppose $a^d = 1$. We know that $d = gcd(m, n) \implies d|m$ and $d|n \implies m = dk$ and $n = dl$, $k, l \in \mathbb{Z}$. Thus, $a^m = a^{dk} = 1$ and $a^n = a^{dl} = 1 \implies a^m = 1$ and $a^n = 1$. □

5 PERMUTATION GROUPS

Permutation groups are central to the study of geometric symmetries and to Galois theory, the study of finding solutions to polynomial equations. They also provide abundant examples of nonabelian groups.

5.1 Definitions and Notation

[17]

The set of permutations of a finite set forms a group, denoted S_n for a set of n elements, called the **symmetric group** on n letters.

Theorem 5.1. *The symmetric group S_n is a group with $n!$ elements, where the binary operation is composition of maps. The identity element is the identity map, and every permutation has an inverse since it is one-to-one and onto.*

A subgroup of S_n is called a **permutation group**. Permutations are often composed from right to left, meaning we apply the second permutation first.

A permutation is a **cycle of length** k if there exists $a_1\, a_2\, \ldots\, a_k \in X$ s.t.

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_k) &= a_1 \end{aligned}$$

and $\sigma(x) = x$ for all other elements. We write $(a_1\, a_2\, \ldots\, a_k)$ to denote the cycle.

Two cycles are **disjoint** if $a_i \neq b_j\ \forall i, j$ when $\sigma = (a_1\, a_2\, \ldots\, a_k)$ and $\tau = (b_1\, b_2\, \ldots\, b_l)$.

Theorem 5.2. *Let σ and τ be two disjoint cycles in S_X. Then $\sigma\tau = \tau\sigma$.*

Proof. Let $\sigma = (a_1\ a_2\ \ldots\ a_k)$ and $\tau = (b_1\ b_2\ \ldots\ b_m)$ be two disjoint cycles in the symmetric group S_X, where σ and τ are permutations acting on a finite set X.

Since σ and τ are disjoint, the elements moved by σ are distinct from the elements moved by τ. In other words:

$$\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_m\} = \emptyset.$$

[17] Section 5.1 in the textbook

This implies that $\sigma(x) = x$ for all $x \in \{b_1, b_2, \ldots, b_m\}$, and similarly, $\tau(x) = x$ for all $x \in \{a_1, a_2, \ldots, a_k\}$.

Now, we want to show that $\sigma\tau = \tau\sigma$, meaning that the two permutations commute. Let $x \in X$. We consider two cases:

Case 1: $x \in \{a_1, a_2, \ldots, a_k\}$

In this case, $\tau(x) = x$ because τ fixes all elements in the support of σ. Hence:

$$\sigma(\tau(x)) = \sigma(x).$$

On the other hand:

$$\tau(\sigma(x)) = \tau(y),$$

where $y = \sigma(x)$, and since $y \in \{a_1, a_2, \ldots, a_k\}$, $\tau(y) = y$. Thus:

$$\tau(\sigma(x)) = \sigma(x).$$

Therefore, $\sigma(\tau(x)) = \tau(\sigma(x))$.

Case 2: $x \in \{b_1, b_2, \ldots, b_m\}$

In this case, $\sigma(x) = x$ because σ fixes all elements in the support of τ. Hence:

$$\tau(\sigma(x)) = \tau(x).$$

On the other hand:

$$\sigma(\tau(x)) = \sigma(z),$$

where $z = \tau(x)$, and since $z \in \{b_1, b_2, \ldots, b_m\}$, $\sigma(z) = z$. Thus:

$$\sigma(\tau(x)) = \tau(x).$$

Therefore, $\sigma(\tau(x)) = \tau(\sigma(x))$.

In both cases, we have $\sigma(\tau(x)) = \tau(\sigma(x))$ for all $x \in X$. Hence, $\sigma\tau = \tau\sigma$, which completes the proof.

$$\boxed{\sigma\tau = \tau\sigma}.$$

□

Theorem 5.3. *Every permutation in S_n can be written as a product of disjoint cycles.*

Proof. We can assume that

$$X = \{1, 2, \ldots, n\}.$$

If $\sigma \in S_n$ and we define X_1 to be

$$X_1 = \{\sigma(1), \sigma^2(1), \ldots\},$$

then the set X_1 is finite since X is finite. Now let i be the first integer in X that is not in X_1, and define X_2 by

$$X_2 = \{\sigma(i), \sigma^2(i), \ldots\}.$$

Again, X_2 is a finite set. Continuing in this manner, we can define finite disjoint sets $X_3, X_4, \ldots$. Since X is finite, this process must terminate, meaning that X is the finite union of disjoint finite sets, which correspond to the orbits of the permutation σ.

□

A **transposition** is a cycle of length 2. Any permutation can be written as a product of transpositions.

Lemma 5.4. *If the identity is written as the product of r transpositions, then r is an even number.*

Theorem 5.5. *Suppose a permutation can be expressed as the product of an even (or odd) number of transpositions. In that case, any other product of transpositions equal to that permutation must also contain an even (or odd) number of transpositions.*

The set of all even permutations in S_n forms a subgroup called the **alternating group** A_n. Half the elements of S_n are even, and half are odd.

Theorem 5.6 (Theorem 5.16)**.** *The alternating group A_n is a subgroup of S_n.*

The order of A_n is half the order of S_n. So, we have

$$|A_n| = \frac{|S_n|}{s} = \frac{n!}{s}$$

NOTE 5.7 (Historical Note)**.** *Cauchy developed the basic theorems and notation for permutations, introducing cycle notation.*

5.2 Dihedral Groups

[18]

Another special type of group is the **dihedral group**. It is defined as the group of rigid motions of a regular n-gon, denoted D_n.

Theorem 5.8. *The dihedral group D_n is subgroup of S_n of order $2n$.*

Notice that there are exactly n choices to replace the first vertex. If we replace the first vertex by k, then the second vertex must be replaced either by vertex $k+1$ or by vertex $k-1$; hence, there are $2n$ possible rigid motions of the n-gon.

Theorem 5.9. *The dihedral group D_n, $n \geq 3$ consists of all products of the two elements r and s, where r has order n and s has order 2, and these two elements satisfy the relation $srs = r^{-1}$.*

5.3 Reading Questions

[19]

[18] Section 5.2 in the textbook
[19] Section 5.3 in the textbook

5.3/1 Express $(134)(354)$ **as a cycle, or a product of disjoint cycles.**
To express $(134)(354)$ as a cycle, we compose the permutations as follows:

- Start with 1: (134) sends 1 to 3, and then (354) sends 3 to 3 (no change). So, 1 maps to 3.
- Start with 3: (134) sends 3 to 4, and then (354) sends 4 to 5. So, 3 maps to 5.
- Start with 5: (134) sends 5 to 5 (no change), and then (354) sends 5 to 4. So, 5 maps to 4.
- Start with 4: (134) sends 4 to 1, and then (354) sends 1 to 1 (no change). So, 4 maps to 1.

The resulting permutation is $(1\,3\,5\,4)$. Therefore,

$$(134)(354) = (1\,3\,5\,4).$$

5.3/2 What is a transposition?
A transposition is a permutation that swaps exactly two elements and leaves all other elements unchanged. In cycle notation, it is written as $(a\,b)$, where a and b are the two elements being swapped.

5.3/3 What does it mean for a permutation to be even or odd?
A permutation is classified as **even** or **odd** based on the number of transpositions (2-cycles) needed to express it:

- A permutation is **even** if it can be expressed as a product of an even number of transpositions.
- A permutation is **odd** if it can be expressed as a product of an odd number of transpositions.

The parity (evenness or oddness) of a permutation is determined by the number of transpositions in its decomposition.

5.3/4 Describe another group that is fundamentally the same as A_3**.**
The group A_3 is the alternating group on 3 elements, which consists of the identity permutation and the 3-cycles of S_3. It is isomorphic to the cyclic group of order 3, denoted by C_3, which is the group with three elements under multiplication.

5.3/5 Write the elements of the symmetry group of a pentagon using permutations in cycle notation.

The symmetry group of a pentagon is the dihedral group D_5. It consists of:

- **Rotations**:
  - e (the identity, no rotation)
  - (12345) (rotation by 72 degrees)
  - (13524) (rotation by 144 degrees)
  - (14253) (rotation by 216 degrees)
  - (15432) (rotation by 288 degrees)
- **Reflections**:
  - Reflection over a line through a vertex and the midpoint of the opposite side: (12)(34), (13)(25), (14)(23), (15)(24)
  - Reflection over a line through the midpoints of opposite sides: (12)(35), (13)(24), (14)(25), (15)(23)

Combining these, the full symmetry group D_5 has 10 elements.

5.4 Select Exercises

[20]

5.4/1 Write the following permutations in cycle notation (answers only)

1. (12453)
2. (14)(35)
3. (13)(25)
4. (24)

5.4/3 Express the following permutations as products of transpositions and identify them as even or odd.

1. (14356) = (16)(15)(13)(14); even
2. (156)(234) = (16)(15)(24)(23); even
3. (1426)(142) = (1624) = (14)(12)(16); odd
4. (17254)(1423)(154632) = (14672)=(12)(17)(16)(14); even
5. (142637) = (17)(13)(16)(12)(14); odd

5.4/6 Find all of the subgroups in A_4. What is the order of each subgroup?

[20] Section 5.4 in the textbook

To find all subgroups of A_4, recall that A_4 has order 12. The possible subgroups are:

1. Trivial Subgroup $\{e\}$
2. Subgroups of Order 2 $e, (12)(34)\}$
3. Subgroups of Order 3 $\langle(123)\rangle = \{e, (123), (132)\}$ There are 4 such subgroups, each generated by one of the 3-cycles.
4. Subgroup of Order 4$\{e, (12)(34), (13)(24), (14)(23)\}$

5.4/7 Find all possible orders of elements in S_7 and A_7.
Since S_7 consists of permutations of cycles, and the order of a product of cycles is their least common multiple, we can have the following orders: {1, 2, 3,4,5,6,7,10,12}. All even permutations can be in A_7, so we get {1,3,5,7}.

5.4/10 Find an element of largest order in S_n for $n = 3, ..., 10$.
We get, for

1. S_3: 3
2. S_4: 3
3. S_5: 6
4. S_6: 6
5. S_7: 12
6. S_8: 15
7. S_9: 20
8. S_{10}: 24

5.4/17 Prove that S_n is nonabelian for $n \geq 3$.
Proof. Consider the case when $n = 3$, then we find $(13)(12) = (123) \neq (132) = (12)(13)$ showing S_3 is not abelian. Now, we have $S_3 < S_n$ when we fix n for $\{4, 5, 6, ...\}$. Showing S_3 is a subgroup is easy, (i) if we compose two cycles that fix all letters $n > 4$, they remain fixed, and (ii) taking the inverse of fixed letters results in the same fixed letters. Thus, we can always find two elements in $S_3 < S_n$ that do not commute, provided they are not the identity element. □

5.4/18 Prove that A_n is nonabelian for $n \geq 4$.
Proof. Consider the case when $n = 4$, then we find $(14)(23)(124) = (132) \neq (234) = (124)(14)(23)$ showing A_4 is not abelian. Similar to the proof above, we can find that $A_4 < A_n$, for $n = \{5, 6, ...\}$. We can fix all letters for $n > 5$, and find that A_4 is a subgroup. So, the claim is true. □

5.4/22 If σ can be expressed as an odd number of transpositions, show that any other product of transpositions equaling σ must also be odd.

Proof. Let $\sigma = \sigma_1 \dots \sigma_k$, where k is odd. Let σ also be represented by an alternate product of transpositions, $\sigma = \tau_1 \dots \tau_l$; we must show that l is odd as well. Consider

$$\sigma^{-1} = \sigma_k \dots \sigma_1,$$

so we can write

$$e = \sigma\sigma^{-1} = \sigma(\sigma_k \dots \sigma_1) = (\tau_1 \dots \tau_l)(\sigma_k \dots \sigma_1).$$

From a previous result, we know that the identity can only be written as a product of an even number of transpositions, so $k + l = r$ must be even. Then, $l = n - k$ must be odd. Hence, proved. □

5.4/24 Show that a 3-cyle is an even permutation.

Proof. Consider a 3-cycle (a, b, c). Then we can write $(a, b, c) = (a, c)(a, b)$, a product of two transpositions, which by definition is an even permutation. □

5.4/30 Let $\tau = (a_1, ..., a_k)$ be a cycle of length k.

1. Prove that if σ is any permutation, then $\sigma\tau\sigma^{-1} = (\sigma(a_1), ..., \sigma(a_k))$ is a cycle of length k.

   Proof. Consider $\sigma\tau\sigma^{-1}(\sigma(1)) = \sigma(\tau(1)) = \sigma(2)$. Similarly, $\sigma\tau\sigma^{-1}(\sigma(2)) = \sigma(\tau(2)) = \sigma(3)$. Finally, $\sigma\tau\sigma^{-1}(\sigma(k)) = \sigma(\tau(k)) = \sigma(1)$, since $\tau(k) = 1$. So, $\sigma\tau\sigma^{-1} = (\sigma(a_1), ..., \sigma(a_k))$, showing cycle length is k. □

2. Let μ be a cycle of length k. Prove that there is a permutation σ s.t. $\sigma\tau\sigma^{-1} = \mu$.

   Proof. Let $\tau = (a_1, a_2, \ldots, a_k)$ and $\mu = (b_1, b_2, \ldots, b_k)$, where both τ and μ are cycles of length k, permuting the sets $\{a_1, a_2, \ldots, a_k\}$ and $\{b_1, b_2, \ldots, b_k\}$, respectively.

   Define the permutation $\sigma \in S_n$ such that:

   $$\sigma(a_i) = b_i \quad \text{for all} \quad i = 1, 2, \ldots, k$$

   and let σ act as the identity on all other elements (i.e., $\sigma(x) = x$ for all $x \notin \{a_1, a_2, \ldots, a_k\}$).

   Now, we check that conjugating τ by σ gives μ.

   1. *Apply σ^{-1} to $b_1, b_2, \ldots, b_k$:*

      $$\sigma^{-1}(b_1) = a_1, \quad \sigma^{-1}(b_2) = a_2, \quad \ldots, \quad \sigma^{-1}(b_k) = a_k$$

   2. *Apply τ to $a_1, a_2, \ldots, a_k$:*

      $$\tau(a_1) = a_2, \quad \tau(a_2) = a_3, \quad \ldots, \quad \tau(a_k) = a_1$$

   3. *Apply σ to the result of τ:*

      $$\sigma(a_2) = b_2, \quad \sigma(a_3) = b_3, \quad \ldots, \quad \sigma(a_1) = b_1$$

   Therefore:

   $$\sigma\tau\sigma^{-1}(b_1) = b_2, \quad \sigma\tau\sigma^{-1}(b_2) = b_3, \quad \ldots, \quad \sigma\tau\sigma^{-1}(b_k) = b_1$$

   This shows that:

   $$\sigma\tau\sigma^{-1} = (b_1, b_2, \ldots, b_k) = \mu$$

   Thus, we have constructed a permutation $\sigma \in S_n$ such that conjugating τ by σ transforms τ into μ, as required. Therefore, we have proved the statement:

   $$\boxed{\exists \sigma \in S_n \text{ such that } \sigma\tau\sigma^{-1} = \mu}$$

   □

6 COSETS and LAGRANGE'S THEOREM

Lagrange's Theorem, one of the most important results in finite group theory, states that the order of a subgroup must divide the order of the group. This theorem provides a powerful tool for analyzing finite groups; it gives us an idea of exactly what type of subgroups we might expect a finite group to possess. Central to understanding Lagranges's Theorem is the notion of a coset.

6.1 Cosets

[21]

Definition 6.1. *Let $H < G$. Define a **left coset** of H with **representative** $g \in G$ to be the set*

$$gH = \{gh : h \in H\}$$

***Right cosets** are defined similarly*

$$Hg = \{hg : h \in H\}$$

Some properties are as follows.

Lemma 6.2. *Let $H < G$ and $g_1, g_2 \in G$. Then*

1. $g_1 H = g_2 H$;
2. $H g_1^{-1} = H g_2^{-1}$;
3. $g_1 H \subset g_2 H$;
4. $g_2 \in g_1 H$;
5. $g_1^{-1} g_2 \in H$

Theorem 6.3. *Let $H < G$. Then the left cosets of H in G partition G. That is, the group G is the disjoint union left cosets of H in G.*

Proof. Let $g_1 H$ and $g_2 H$ be two cosets of H in G. We must show that either $g_1 H \cap g_2 H = \emptyset$ or $g_1 H = g_2 H$. Suppose $g_1 H \cap g_2 H \neq \emptyset$ and $a \in g_1 H \cap g_2$. Then by the definition of a left coset, $a = g_1 h_1 = g_2 h_2$ for some elements h_1 and $h_2 \in H$. Hence, $g_1 = g_2 h_2 h_2^{-1}$ or $g_1 \in g_2 H$. By properties above, $g_1 H = g_2 H$. □

The above theorem is also true for right cosets. So, we can also infer that the no. of left cosets is the same as the no. of right cosets.

Definition 6.4. *Let $H < G$. Define the **index** of H in G to be the number of left (or right) cosets of H in G. We will denote the index by [G:H].*

[21] Section 6.1 in the textbook

6.2 Lagrange's Theorem

[22]

Theorem 6.5. *Let $H < G$, $g \in G$ and define a map $\phi : H \to gH$ by $\phi(h) = gh$. The map is bijective; hence, the no. of elements in H is the same as the number of elements in gH.*

Theorem 6.6 (Lagrange's Theorem)**.** *Let $H < G$. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.*

Proof. The group G is partitioned into [G:H] distinct left cosets. Each left coset $|H|$ has; elements; therefore, $|G| = [G : H]|H|$. □

Note the converse of Lagrange's theorem is not true. The theorem above states that the orders of subgroups of a group G must divide G's order. So, if we have $|A_4| = 12$, Lagrange's theorem states that we could have subgroups of order $1, 2, 3, 4, 6, 12$. However, there is no subgroup of order 6. So the theorem cannot guarantee the existence of a subgroup of a particular order.

Corollary 6.7. *Suppose G is a finite group. Then the order of any $g \in G$ must divide the order of G, i.e., the number of elements in G.*

Corollary 6.8. *Let $|G| = p$, where p is prime. Then G is cyclic and any $g \in G$ s.t. $g \neq e$ is a generator.*

Theorem 6.9. *Two cycles τ and $\mu \in S_n$ have the same length $\iff$ $\exists \sigma \in S_n$ s.t. $\mu = \sigma\tau\sigma^{-1}$.*

Proof. Suppose

$$\tau = (a_1, a_2, ..., a_k) \text{ and } \mu = (b_1, b_2, ..., b_k)$$

Define a permutation

$$\sigma(a_1) = b_1, \sigma(a_2) = b_2, ..., \sigma(a_k) = b_k$$

Then $\mu = \sigma\tau\sigma^{-1}$. Conversely, suppose that $\tau = (a_1, a_2, ..., a_k)$ is a k-cycle and $\sigma \in S_n$. If $\sigma(a_i) = b$ and $\sigma(a_{(i \bmod k)+1} = b' \implies \mu(b)$'_. hence,

$$\mu = (\sigma(a_1), \sigma(a_2), ..., \sigma(a_k))$$

Since σ is onto and 1-1, it is a cycle of the same length as τ. □

[22] Section 6.2 in the textbook

6.3 Reading Questions

[23]

6.4/1 State Lagrange's Theorem in your own words.
Lagrange's Theorem states that if G is a finite group and H is a subgroup of G, then the order (number of elements) of H divides the order of G. In other words, the size of any subgroup must be a divisor of the size of the whole group.

6.4/2 Determine the left cosets of $< 3 >$ in $\mathbb{Z}_9$.
The subgroup generated by 3 in $\mathbb{Z}_9$ is $< 3 >= \{0, 3, 6\}$. The left cosets of $< 3 >$ in $\mathbb{Z}_9$ are found by adding elements of $\mathbb{Z}_9$ to each element of the subgroup:
$0 + < 3 >= \{0, 3, 6\}$, $1 + < 3 >= \{1, 4, 7\}$, $2 + < 3 >= \{2, 5, 8\}$
So the left cosets are $\{0, 3, 6\}$, $\{1, 4, 7\}$, and $\{2, 5, 8\}$.

6.4/4 Suppose G is a group of order 29. Describe G.
Since 29 is a prime number, by a well-known result in group theory, any group of prime order is cyclic and isomorphic to the group of integers modulo 29, denoted $\mathbb{Z}_{29}$. This means that G is cyclic and every element of G can be written as powers of a single generator element. Therefore, G is isomorphic to $\mathbb{Z}_{29}$ and is cyclic.

6.4 Select Exercises

[24]

6.5/1 Suppose G is a finite group with an element of order 5 and another element of order 7. Why must $|G| \geq 35$?
Since element orders must divide the order of the group and $gcd(5, 7) = 1$, $5||G|$ and $7||G| \implies 35||G| \implies |G| \geq 35$.

6.5/2 Suppose G is a finite group with 60 elements. What are the orders of possible subgroups of G?
All subgroup orders must divide $|G|$. Thus, all factors of 60 can be the order of subgroups of G; $\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$.

6.5/9 Show that the integers have infinite index in the additive group of rational numbers.
Proof.
DO

□

6.5/11 Let $H < G$ and $g_1, g_2 \in G$. Then prove

[23] Section 6.4 in the textbook
[24] Section 6.5 in the textbook

DO

1. $g_1H = g_2H$;
2. $Hg_1^{-1} = Hg_2^{-1}$;
3. $g_1H \subset g_2H$;
4. $g_2 \in g_1H$;
5. $g_1^{-1}g_2 \in H$

6.5/14 Suppose that $g^n = e$. Show that the order of g divides n.
Proof. Suppose $|g| = d$. Suppose, for contradiction, $d \nmid n \implies n = dk + r,\ 0 < r < d$. Then $g^n = g^{dk}g^r = eg^r \implies g^r = e$, contradicting the fact that d is the order of g. Thus, $d|n$. □

6.5/16 If $|G| = 2n$, prove that the number of elements of order 2 is odd. Use this result to show that G must contain a subgroup of order 2.
Proof. Let G be a group of order $|G| = 2n$. We will show that the number of elements of order 2 is odd. First, observe that the identity element e is of order 1 and can be paired with itself. For elements of order greater than 2, every such element $g \in G$ has a distinct inverse g^{-1}, where $g \neq g^{-1}$. These elements can be paired off as $\{g, g^{-1}\}$. This pairing accounts for all elements of G except for those of order 2, as an element g of order 2 is equal to its own inverse, i.e., $g = g^{-1}$. Hence, elements of order 2 cannot be paired with distinct inverses and remain unpaired.
If the number of elements of order 2 were even, then, when combined with the identity element, the total number of unpaired elements would be even, which contradicts the fact that the total number of elements in G is $2n$, an even number. Therefore, the number of elements of order 2 must be odd.

To show that G contains a subgroup of order 2, note that if $g \in G$ is an element of order 2, the subgroup generated by g is $\langle g \rangle = \{e, g\}$, which has order 2. Since we have shown that there is at least one element of order 2, G must contain a subgroup of order 2.

□

6.5/17 Suppose $[G : H] = 2$. If a and $b \notin H$, show that $ab \in H$.

Proof. Since $[G : H] = 2$, G has exactly two cosets: H and $G \setminus H$. In other words, every element of G is either in H or in $G \setminus H$, and $G \setminus H$ is the coset aH for any $a \notin H$.

Now, suppose $a, b \notin H$. Since H and $G \setminus H$ are the only two cosets, both a and b must lie in $G \setminus H$. Consider the product ab. If $ab \notin H$, then $ab \in G \setminus H$. However, this would imply that H and $G \setminus H$ are closed under multiplication, which contradicts the fact that H is a subgroup, and subgroups are closed under multiplication.

Therefore, it must be the case that $ab \in H$.

□

6.5/18 If $[G : H] = 2$. prove that $gH = Hg$.
Proof. To show that $gH = Hg$ for all $g \in G$, we need to demonstrate that gH and Hg are the same coset. Since H is a subgroup, we know that $eH = H$ for the identity element e. Additionally, because $[G : H] = 2$, there are only two cosets of H in G: H and $G \setminus H$. In particular, $G = H \cup gH$ for some $g \in G \setminus H$.

Now, for any $g \in G$, consider two cases:

1. If $g \in H$, then $gH = H = Hg$ since H is a subgroup, and subgroups are closed under multiplication.

2. If $g \notin H$, then gH must be the coset $G \setminus H$. Since H is normal in G, we have $gH = Hg$ by definition of a normal subgroup.

Thus, in either case, we conclude that $gH = Hg$ for all $g \in G$, meaning H is normal in G.

□

6.5/21 Let G be a cyclic group of order n. Show that there are exactly $\phi(n)$ generators for G.
Proof. Let $G = \langle g \rangle$ be a cyclic group of order n, which means that every element of G is a power of g. That is, $G = \{g^0, g^1, g^2, \ldots, g^{n-1}\}$. We want to show that the number of generators of G is $\phi(n)$, where ϕ is Euler's totient function, which counts the number of integers less than or equal to n that are coprime to n.

An element $g^k \in G$ is a generator if and only if the order of g^k is n. The order of g^k is the smallest positive integer d such that $(g^k)^d = e$. Since g has order n, we have $(g^k)^d = g^{kd}$. Thus, $g^{kd} = e$ if and only if kd is a multiple of n, i.e., $kd = mn,\ m \in \mathbb{Z}$. This implies that the order of g^k is $\frac{n}{\gcd(k,n)}$.

For g^k to have order n, we must have $\gcd(k, n) = 1$. Therefore, g^k is a generator if and only if k is coprime to n. The number of integers k such that $1 \leq k < n$ and $\gcd(k, n) = 1$ is precisely $\phi(n)$ by definition of Euler's totient function.

□

7 ISOMORPHISMS

7.1 Definitions and Examples

[25]

Two groups G and H are *isomorphic* if there exists a one-to-one and onto map $\varphi : G \to H$ such that the group operation is preserved; that is, $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. If G is isomorphic to H, we write $G \cong H$. The map φ is called an isomorphism.

Example: To show that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, define a map $\varphi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by $\varphi(k) = (k \mod 2, k \mod 3)$. We must show that φ is bijective and preserves the group operation. The map is one-to-one and onto because φ maps elements uniquely and covers all elements of the product group. Moreover,

$$\varphi(k_1 + k_2) = ((k_1 + k_2) \mod 2, (k_1 + k_2) \mod 3) = \varphi(k_1) + \varphi(k_2).$$

Thus, the group operation is preserved.

Example: We can define an isomorphism $\varphi : \mathbb{R} \to \mathbb{R}_+$ from the additive group of real numbers to the multiplicative group of positive real numbers with the exponential map $\varphi(x) = e^x$. This is one-to-one and onto, as can be shown using calculus.

Example: The integers are isomorphic to the subgroup of $\mathbb{R}$ consisting of elements of the form $e^{2\pi it}$. Define a map $\varphi : \mathbb{Z} \to S^1$ by $\varphi(n) = e^{2\pi in}$. The map is onto the subset of S^1, and it is injective since $\varphi(n) = \varphi(m)$ implies $n = m$.

Example: The groups $\mathbb{Z}_4$ and V_4 cannot be isomorphic since they have different structures; however, $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V_4$.

Example: Even though $\mathbb{S}_3$ and D_3 possess the same number of elements, they are not isomorphic because $\mathbb{S}_3$ is nonabelian while D_3 is abelian.

Theorem 7.1. *Let $\varphi : G \to H$ be an isomorphism of two groups. Then the following statements are true:*

- *$\varphi^{-1} : H \to G$ is an isomorphism.*
- *G is abelian if and only if H is abelian.*
- *G is cyclic if and only if H is cyclic.*
- *If G has a subgroup of order n, then H has a subgroup of order n.*

Theorem 7.2. *All cyclic groups of infinite order are isomorphic to $\mathbb{Z}$.*

Theorem 7.3. *If G is a cyclic group of order n, then $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Corollary 7.4. *If G is a group of prime order p, then $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Theorem 7.5. *The isomorphism of groups determines an equivalence relation on the class of all groups.*

[25] Section 9.1 in the textbook

CAYLEY'S THEOREM

Theorem 7.6. *Cayley. Every group is isomorphic to a group of permutations.*

Example: Consider the group $\mathbb{Z}_4$. The Cayley table for $\mathbb{Z}_4$ suggests that it is the same as the permutation group V_4. The isomorphism is $\varphi : \mathbb{Z}_4 \to V_4$, defined by $\varphi(0) = (1), \varphi(1) = (12), \varphi(2) = (13), \varphi(3) = (14)$.

7.2 Direct Products

[26]

Given two groups G and H, it is possible to construct a new group from the Cartesian product $G \times H$. Conversely, given a large group G, it is sometimes possible to decompose the group; that is, G may be isomorphic to the direct product of smaller groups. Studying the components of G can simplify the analysis.

EXTERNAL DIRECT PRODUCTS

If G and H are groups, we can form the Cartesian product $G \times H$, where the set consists of ordered pairs (g, h) with $g \in G$ and $h \in H$. The binary operation on $G \times H$ is defined as:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2),$$

which uses the operations in G and H respectively.

Theorem 7.7. *Let G and H be groups. The set $G \times H$ is a group under the operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.*

The operation is closed, and the identity element is (e_G, e_H). The inverse of (g, h) is (g^{-1}, h^{-1}), and associativity follows from the associativity of G and H.

Example: Let $\mathbb{R}$ be the group of real numbers under addition. The Cartesian product $\mathbb{R} \times \mathbb{R}$ is also a group, with the group operation given by addition in each coordinate: $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. The identity is $(0, 0)$ and the inverse of (x, y) is $(-x, -y)$.

The group $G \times H$ is called the **external direct product** of G and H. We can generalize this to multiple groups $G_1, G_2, \ldots, G_n$, forming the group $G_1 \times G_2 \times \cdots \times G_n$.

Theorem 7.8. *Let $G = G_1 \times G_2$. If G_1 and G_2 have finite orders n_1 and n_2, the order of an element $(g_1, g_2) \in G$ is the least common multiple of n_1 and n_2.*

Corollary 7.9. *Let $G = G_1 \times G_2$. If an element $g \in G$ has finite order n, the order of g in G is the least common multiple of the orders of its components.*

Example: Let $G = \mathbb{Z}_4 \times \mathbb{Z}_6$. The order of $(1, 2)$ is the least common multiple of the orders of $1 \in \mathbb{Z}_4$ and $2 \in \mathbb{Z}_6$, which is $\text{lcm}(4, 3) = 12$.

[26] Section 9.2 in the textbook

Theorem 7.10. *The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $gcd(m, n) = 1$.*

Corollary 7.11. *Let $n_1, n_2, \ldots, n_k$ be positive integers. Then*

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

is cyclic if and only if $gcd(n_i, n_j) = 1$ for all $i \neq j$.

Corollary 7.12. *If $G = \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$, where the p_i are distinct primes, then G is isomorphic to $\mathbb{Z}_{p_1^{k_1} \cdot p_2^{k_2} \cdots\cdots p_m^{k_m}}$.*

INTERNAL DIRECT PRODUCTS

The external direct product builds a large group from smaller groups. We would like to reverse this process to decompose a group into direct product components. Let G be a group with subgroups H and K such that:

- $H \cap K = \{e\}$,
- Every element of G can be written as hk for some $h \in H$ and $k \in K$,
- $hk = kh$ for all $h \in H$ and $k \in K$.

Then G is the internal direct product of H and K.
Example: The group $\mathbb{Z}_6$ is the internal direct product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

Example: The dihedral group D_6 is the internal direct product of its subgroups $H = \langle r \rangle$ and $K = \langle s \rangle$.

Not every group can be written as the internal direct product of two of its proper subgroups.

Theorem 7.13. *Let G be the internal direct product of subgroups H and K. Then $G \cong H \times K$.*

Example: The group $\mathbb{Z}_6$ is an internal direct product isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$.

We can extend the definition of the internal direct product to a collection of subgroups $H_1, H_2, \ldots, H_n$ of G, provided:

- $H_i \cap H_j = \{e\}$ for all $i \neq j$,
- Every element of G can be written as a product of elements from the H_i.

Theorem 7.14. *Let G be the internal direct product of subgroups $H_1, H_2, \ldots, H_n$. Then $G \cong H_1 \times H_2 \times \cdots \times H_n$.*

7.3 Reading Questions

[27]

9.3/1 Determine the order of $(1,2) \in \mathbb{Z}_4 \times \mathbb{Z}_8$.
To determine the order of the element $(1,2) \in \mathbb{Z}_4 \times \mathbb{Z}_8$, we find the least common multiple of the orders of its components.
1. The order of $1 \in \mathbb{Z}_4$ is 4 because the smallest positive integer k such that $k \cdot 1 \equiv 0 \mod 4$ is 4.
2. The order of $2 \in \mathbb{Z}_8$ is 4 because the smallest positive integer k such that $k \cdot 2 \equiv 0 \mod 8$ is also 4.
Thus, the order of the element $(1,2)$ is given by:

$$\text{order}((1,2)) = \text{lcm}(4,4) = 4.$$

9.3/2 List three properties of a group that are preserved by an isomorphism.

1. Order of the group: If G is isomorphic to H, then the order of G is equal to the order of H.

2. Structure of subgroups: The subgroups of G correspond to the subgroups of H in a one-to-one manner.

3. Abelian property: If G is abelian, then H is also abelian, and vice versa.

9.3/3 Find a group isomorphic to $\mathbb{Z}_{15}$ that is an external direct product of two non-trivial groups.
A group isomorphic to $\mathbb{Z}_{15}$ that can be expressed as an external direct product of two non-trivial groups is $\mathbb{Z}_3 \times \mathbb{Z}_5$.
Since 3 and 5 are coprime, by the Chinese Remainder Theorem, we have:

$$\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}.$$

9.3/4 Explain why we can now say "the infinite cyclic group"?
We can refer to "the infinite cyclic group" because there is a unique up to isomorphism infinite cyclic group, which is isomorphic to the group of integers $\mathbb{Z}$. Any infinite cyclic group can be generated by a single element, and thus it has the same structure as $\mathbb{Z}$, making it well-defined to refer to it as "the infinite cyclic group."

9.3/5 Compare and contrast external direct products and internal direct products.

[27] Section 9.3 in the textbook

- External Direct Product: Given groups G and H, the external direct product $G \times H$ is the Cartesian product of the two sets, where the group operation is defined component-wise. It creates a new group that is the "product" of the two groups.
- Internal Direct Product: A group G is said to be the internal direct product of subgroups A and B if G can be expressed as the product of A and B, where A and B are normal subgroups of G that intersect trivially. In this case, G retains its original structure while being decomposed into its components.

7.4 Select Exercises

[28]

9.4/1 Prove that $\mathbb{Z} \simeq n\mathbb{Z},\ n \neq 0$.
Proof: Define a map $\phi(x) = nx, n \in \mathbb{N}, z \in \mathbb{Z}$.

(a) 1-1: Consider $\phi(x_1) = \phi(x_2) \implies nx_1 = nx_2 \implies x_1 = x_2$. So, 1-1.

(b) Onto: Let $\phi(x) = y \implies nx = y \implies x = y/n$. Then $\phi(y/n) = ny/n = y$. So every image has a pre-image.

(c) Homomorphism: $\phi(a + b) = n(a + b) = na + nb = \phi(a) + \phi(b)$.

■

9.4/2 Prove that $\mathbb{C}^*$ is isomorphic to the subgroup of $GL_2(\mathbb{R})$ consisting of matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$
Proof: Define a map $\phi(a + bi) = M, a, b \in \mathbb{Z}^*$, where M is of the form shown in the question.

(a) 1-1: Consider $\phi(a + bi) = \phi(c + di) \implies \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \implies a = c, b = d \implies a + bi = c + di$. So, 1-1.

(b) Onto: Choose an element of the image $x = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ Then $\phi^{-1}(x) = (x + yi)$.

(c) Homomorphism: $\phi((a+bi)(c+di)) = \begin{pmatrix} ac - bd & ad - bc \\ bc - ad & ac - bd \end{pmatrix} = \phi(a + bi) + \phi(c + di)$.

■

9.4/3 Prove that $U(8) \simeq \mathbb{Z}_4$.

[28] Section 9.4 in the textbook

Proof: Draw a Cayley table.

■

9.4/5 Show that $U(5) \simeq U(10)$, but not to $U(12)$.

Proof: For the first part, define the map $\phi(1) = 1, \phi(2) = 3, \phi(3) = 7, \phi(4) = 9$. It is 1-1 and onto be definition. Draw Cayley table to show similarity.

For second part, there is an element $2 \in U(5)$ and $|2| = 3$. However, there is no element of order 3 in $U(12)$.

■

9.4/6 Show that nth roots of unity are isomorphic to $\mathbb{Z}_n$.

Proof: Define a map $\phi : \mathbb{Z}_n \to n$th roots of unity by $k \mapsto e(2k\pi/n)$.

(a) 1-1: Consider $\phi(x_1) = \phi(x_2) \implies e(2x_1\pi/n) = e(2x_2\pi/n) \implies \ln(e(2x_1\pi/n) = e(2x_2\pi/n)) \implies 2x_1\pi/n = 2x_2\pi/n \implies x_1 = x_2$. So, 1-1.

(b) Onto: Let $\phi(k) = y \in Im(k)$. Then $k = n \ln y/2\pi$. Plug it back in and confirm that we receive y.

(c) Homomorphism: $\phi(a+b) = e(2\pi(a+b)/n) = e(2\pi a/n)e(2\pi b/n)hi = \phi(a)\phi(b)$.

■

9.4/11 Find five non-isomorphic groups of order 8.

We start with the known groups $D_4, Q_8,$ and $\mathbb{Z}_8$. Then we also have $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, which are direct products.

9.4/12 Prove that $\S_4 \not\simeq D_{12}$.

Note that D_{12} is the group consisting of all the rigid motions on an octagon. Naturally, we can rotate the figure 12 times to get back its original position, so we have an element of order 12. S_4 has no such element.

9.4/14 Show that the set of all matrices of the form $\begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix}$ is a group isomorphic to D_n, where are entries in the matrix are in Z_n.

Proof: Let's begin with showing a group is formed. Define the Set: Let

$$G = \left\{ \begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix} : k \in \mathbb{Z}_n \right\}.$$

This set consists of matrices where the first entry can be 1 or -1 and the second entry can take any value in $\mathbb{Z}_n$. **Group Operation**: The operation on G is matrix multiplication. For any two elements

$$A = \begin{pmatrix} a & k_1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} b & k_2 \\ 0 & 1 \end{pmatrix} \in G,$$

the product AB is given by

$$AB = \begin{pmatrix} ab & ak_2 + k_1 \\ 0 & 1 \end{pmatrix}.$$

Here, ab will be 1 or -1, depending on whether a and b are 1 or -1, and $ak_2 + k_1$ is in $\mathbb{Z}_n$. **Identity Element**: The identity element in G is

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Inverses: Each element $\begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix}$ has an inverse given by $\begin{pmatrix} \pm 1 & -k \\ 0 & 1 \end{pmatrix}$, since

$$\begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pm 1 & -k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Isomorphism: We need to check that $\phi(AB) = \phi(A)\phi(B)$ for all $A, B \in G$. Let $A = \begin{pmatrix} a & k_1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} b & k_2 \\ 0 & 1 \end{pmatrix}$. Compute AB:

$$AB = \begin{pmatrix} ab & ak_2 + k_1 \\ 0 & 1 \end{pmatrix}.$$

Depending on the signs of a and b: If both are 1, $\phi(AB) = r^{ak_2+k_1} = r^{k_1+k_2} = \phi(A)\phi(B)$. If $a = 1$ and $b = -1$, $\phi(A) = r^{k_1}$ and $\phi(B) = s \cdot r^{k_2}$, leading to:

$$\phi(AB) = s \cdot r^{k_2} = \phi(A)\phi(B).$$

The other combinations can be similarly checked to show that the mapping respects the group operation.

Injectivity: Assume $\phi(A) = \phi(B)$. If both are rotations, $k_1 = k_2$ implies $A = B$. If one is a rotation and the other is a reflection, they cannot be equal. Thus, the mapping is injective.

Surjectivity: For every element in D_n (both rotations and reflections), there exists a corresponding matrix in G. This ensures that every element of D_n is covered by the mapping ϕ.

■

9.4/24 Prove or disprove: There is a noncyclic abelian group of order 51.

Proof: **(Disproving)** We know that all abelian groups of finite order is isomorphic to the form

$$\mathbb{Z}_{p_i^{k_1}} \times \ldots \mathbb{Z}_{p_n^{k_n}},\ n \in \mathbb{Z}$$

So, we have we can write, for the group in the question: $\mathbb{Z}_{51}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_{17}$. Both are cyclic.

■

8 NORMAL SUBGROUPS and FACTOR GROUPS

8.1 Factor Groups and Normal Subgroups

[29]

NORMAL SUBGROUPS

A subgroup $H < G$ is **normal** in G if $gH = Hg,\ \forall g \in G$. So, the right and left cosets are the same.

Theorem 8.1. *Let G be a group and N be a subgroup of G. Then the following statements are equivalent.*

1. *The subgroup N is normal in G.*
2. $\forall g \in G,\ gNg^{-1} \subset N$
3. $\forall g \in G,\ gNg^{-1} = N$

FACTOR GROUPS

If $N \triangleleft G$, then the cosets of N in G form a group G/N under the operation $(aN)(bN) = abN$. This group is called the **factor** or **quotient group** of G and N.

Theorem 8.2. *Let $N \triangleleft G$. The cosets of N in G form a group G/N of order [G:N].*

[29] Section 10.1 in the textbook

Proof: The operation of G/N is given by $(aN)(bN) = abN$. We must show this operation is well-defined– so the group multiplication must be independent of the choice of closet representative. Let $aN = bN$ and $cN = dN$, so we must show

$$(aN)(cN) = acN = bdN = (bN)(dN)$$

Then $a = bn_1$ and $c = dn_2$ for some $n_1, n_2 \in N$. Hence,

$$\begin{aligned} acN &= bn_1dn_2N \\ &= bn_1dN \\ &= bn_1Nd \\ &= bNd \\ &= bdN \end{aligned}$$

We also note that $eN = N$ and the identity $g^{-1}N$ is the inverse of gN. The order of G/N is, of course, the number of cosets of N in G.

■

NOTE 8.3. *Elements in a factor group are* ***sets of elements*** *in the original group.*

8.2 The Simplicity of the Alternating Group

[30]

A group with no nontrivial normal subgroups is called **simple groups**; examples are $\mathbb{Z}_p$ where p is prime.

Theorem 8.4. *The alternate group A_n is generated by 3-cycles for $n \geq 3$.*

Proof: To show that 3-cycles generate A_n, we need only show that any pair of transpositions can be written as the product of 3-cycles. Since $(a, b) = (b, a)$, every pair of transpositions must be one of the following:

$$(a, b)(a, b) = e$$

$$(a, b)(c, d) = (a, c, b)(a, c, d)$$

$$(a, b)(a, c) = (a, c, b)$$

■

Theorem 8.5. *Let $N \triangleleft A_n$, where $n \geq 3$. If N contains a 3-cycle, then $N = A_n$.*

Theorem 8.6. *For $n \geq 5$, every nontrivial normal subgroup N of A_n contains a 3-cycle.*

Theorem 8.7. *The alternating group, A_n, is simple for $n \geq 5$.*

[30] Section 10.2 in the textbook

Proof: Let $N \triangleleft A_n$. By the previous lemma/theorem, N contains a 3-cycle. Then by the theorem/lemma before the previous, $N = A_n$; therefore, A_n contains no proper nontrivial normal subgroups for $n \geq 5$.

■

8.3 Reading Questions

[31]

10.3/1 Let G be the group of symmetries of an equilateral triangle, expressed as permutations of the vertices numbered $1, 2, 3$. Let $H < G$ s.t. $H =< (12) >$. Build the left and right cosets of H in G.
We compute the left cosets of H in G:

$$eH = \{e, (12)\}, \quad (23)H = \{(23), (132), \quad (13)H = \{(13), (123)\}$$

Next, we compute the right cosets of H in G:

$$He = \{e, (12)\}, \quad H(13) = \{(13), (132)\}, \quad H(23) = \{(23), (123)\}$$

Thus, the left and right cosets are the same.

10.3/2 Based on your answer to the previous question, is H normal in G? Explain why or why not.
Not normal $\Longleftarrow$ $(13)H \neq H(13)$

10.3/3 The subgroup $8\mathbb{Z}$ is normal in $\mathbb{Z}$. In the factor group $\mathbb{Z}/8\mathbb{Z}$ perform the computation $(3 + 8\mathbb{Z}) + (7 + 8\mathbb{Z})$.
$(3 + 8\mathbb{Z}) + (7 + 8\mathbb{Z}) \implies ((3 + 7) + 8\mathbb{Z}) \implies (10 + 8\mathbb{Z}) \implies (2 + 8\mathbb{Z})$

10.3/4 List two statements about a group G and a subgroup H that are equivalent to H *is normal in* G.

1. For all $g \in G$, $gH = Hg$ (i.e., the left and right cosets of H in G are the same).

2. For all $g \in G$ and $h \in H$, $ghg^{-1} \in H$ (i.e., H is closed under conjugation by elements of G).

10.3/5 In your own words, what is a factor group?
A factor group (or quotient group) is a group formed by dividing a group G by one of its normal subgroups H. The elements of the factor group are the cosets of H in G, and the group operation is defined as the product of cosets. Factor groups allow us to study the structure of groups by "collapsing" a normal subgroup to the identity element.

[31] Section 10.3 in the textbook

8.4 Select Exercises

[32]

10.4/1 For each of the following groups G, determine whether $H \triangleleft G$. If $H \triangleleft G$, write out a Cayley table for the factor group G/H.

1. $G = S_4$ and $H = A_4$:
   $H = A_4$ is a normal subgroup of $G = S_4$. The factor group S_4/A_4 is isomorphic to $\mathbb{Z}_2$. The Cayley table for S_4/A_4 is:

$\cdot$	A_4	$(12)A_4$
A_4	A_4	$(12)A_4$
$(12)A_4$	$(12)A_4$	A_4

2. $G = A_5$ and $H = \{(1), (123), (132)\}$:
   $H \not\triangleleft A_5$. Consider $(12)(34)(123) \neq (123)(12)(34)$.

3. $G = S_4$ and $H = D_4$:
   $D_4 \not\triangleleft S_4$.

4. $G = \mathbb{Q}_8$ and $H = \{1, -1, i, -i\}$:
   Yes, H is a normal subgroup of $\mathbb{Q}_8$. The factor group $\mathbb{Q}_8/H$ is isomorphic to $\mathbb{Z}_2$. The Cayley table for $\mathbb{Q}_8/H$ is:

$\cdot$	H	jH
H	H	jH
jH	jH	H

5. $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$:
   Yes, $H = 5\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. The factor group $\mathbb{Z}/5\mathbb{Z}$ is isomorphic to $\mathbb{Z}_5$. The Cayley table for $\mathbb{Z}/5\mathbb{Z}$ is:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

10.4/2 Find all the subgroups of D_4. Which subgroups are normal? What are all the factor groups of D_4 up to isomorphism?

[32] Section 10.4 in the textbook

The group D_4, the dihedral group of order 8, has the following subgroups:

1. $\{e\}$
2. $\langle r \rangle = \{e, r, r^2, r^3\}$ (the cyclic group of rotations)
3. $\langle s \rangle = \{e, s\}$ (a reflection)
4. $\langle rs \rangle = \{e, rs\}$ (a reflection)
5. $\langle r^2 \rangle = \{e, r^2\}$ (a 180-degree rotation)
6. D_4 itself

The normal subgroups of D_4 are:

- $\{e\}$
- $\langle r^2 \rangle = \{e, r^2\}$
- $\langle r \rangle = \{e, r, r^2, r^3\}$
- D_4

The factor groups of D_4 up to isomorphism are:

- $D_4/\langle r^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
- $D_4/\langle r \rangle \cong \mathbb{Z}_2$
- $D_4/D_4 \cong \{e\}$

10.4/4 Let T be the group of nonsingular upper triangular 2×2 matrices with entries in $\mathbb{R}$; that is, matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

where $a, b, c \in \mathbb{R}$ and $ac \neq 0$. Let U consist of matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

where $x \in \mathbb{R}$.

1. Show $U < T$.
   U is a subgroup of T because the product of two matrices in U is still in U:
   $$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$
   which is of the form required for U.

2. Prove U is abelian.
   For any two matrices in U, say $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$, we have:
   $$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y+x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$
   Therefore, U is abelian.

3. Prove $U \triangleleft T$.
   Let $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in T$ and $u = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in U$. Then,
   $$gug^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}b/c \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \frac{x}{c^2} \\ 0 & 1 \end{pmatrix} \in U$$
   showing that U is normal in T.

4. Show T/U is abelian.
   Since $U \triangleleft T$, the factor group T/U is abelian because the commutator of any two elements in T becomes trivial modulo U.

5. Is $T \triangleleft GL_2(\mathbb{R})$?
   No, T is not normal in $GL_2(\mathbb{R})$ because conjugation by certain elements in $GL_2(\mathbb{R})$ can take upper triangular matrices to matrices that are not upper triangular.

10.4/7 Prove or disprove: if $H \triangleleft G$ such that both H and G/H are abelian, then G is abelian.
Disprove. Consider the group $G = D_4$, the dihedral group of order 8. The subgroup $H = \langle r^2 \rangle$ is abelian (isomorphic to $\mathbb{Z}_2$), and the factor group $D_4/\langle r^2 \rangle$ is also abelian (isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$). However, D_4 itself is not abelian. This shows that H and G/H being abelian does not imply that G is abelian.

10.4/12 Define the centralizer of an element $g \in G$ to be the set
$$C(g) = \{x \in G : xg = gx\}$$
Show that $C(g) \triangleleft G$. If g generates a normal subgroup of G, prove that $C(g) \triangleleft G$.

Proof: To show that $C(g) \triangleleft G$, let $x \in C(g)$ and $h \in G$. We want to show that $hxh^{-1} \in C(g)$. Since $xg = gx$, we have:

$$hxh^{-1}g = hxh^{-1}g = hxh^{-1}g = hgxh^{-1} = ghxh^{-1}$$

so $hxh^{-1} \in C(g)$, proving that $C(g) \triangleleft G$.
If g generates a normal subgroup, then for any $x \in G$, we have $xgx^{-1} \in \langle g \rangle$.
Since the centralizer is closed under conjugation, $C(g)$ is normal in G.

■

9 HOMOMORPHISMS

9.1 Group Homomorphism

[33]

Definition 9.1. *A **homomorphism** between groups G and G' is a map $f : G \to G'$ such that*

$$f(xy) = f(x)f(y) \quad \textit{for all } x, y \in G.$$

The range of f in G' is called the homomorphic image of G.

Example: Let $G = \mathbb{Z}$ be a group and $n \in \mathbb{Z}$. Define a map $f : \mathbb{Z} \to \mathbb{Z}_n$ by $f(k) = k \mod n$. Then f is a group homomorphism, since

$$f(k_1 + k_2) = (k_1 + k_2) \mod n = (k_1 \mod n) + (k_2 \mod n) = f(k_1) + f(k_2).$$

This homomorphism maps $\mathbb{Z}$ onto the cyclic subgroup of $\mathbb{Z}_n$ generated by $1 \mod n$.

Example: Let $G = GL_2(\mathbb{R})$, the group of all 2×2 invertible matrices with real entries. If $A \in GL_2(\mathbb{R})$, then the determinant is nonzero; that is, $\det(A) \neq 0$. Also, for any two elements A and B in $GL_2(\mathbb{R})$,

$$\det(AB) = \det(A)\det(B).$$

Using the determinant, we can define a homomorphism $\det : GL_2(\mathbb{R}) \to \mathbb{R}^*$ by $\det(A) = \det(A)$.

[33] Section 11.1 in the textbook

Example: Recall that the circle group S^1 consists of all complex numbers z such that $|z| = 1$. We can define a homomorphism $f : \mathbb{R} \to S^1$ from the additive group of real numbers $\mathbb{R}$ to S^1 by

$$f(t) = e^{2\pi it}.$$

Indeed,

$$f(t_1 + t_2) = e^{2\pi i(t_1+t_2)} = e^{2\pi it_1}e^{2\pi it_2} = f(t_1)f(t_2).$$

Geometrically, we are simply wrapping the real line around the circle in a group-theoretic fashion.

Theorem 9.2. *Let $f : G \to G'$ be a homomorphism of groups. Then:*

- *If e_G is the identity of G, then $f(e_G)$ is the identity of G'.*
- *For any element $g \in G$, $f(g^{-1}) = (f(g))^{-1}$.*
- *If H is a subgroup of G, then $f(H)$ is a subgroup of G'.*
- *If K is a subgroup of G', then $f^{-1}(K)$ is a subgroup of G. Furthermore, if K is normal in G', then $f^{-1}(K)$ is normal in G.*

Proof: **Proof of (1):** Suppose that e_G and $e_{G'}$ are the identities of G and G', respectively; then

$$f(e_G e_G) = f(e_G) = f(e_G)f(e_G) = e_{G'}f(e_G).$$

By cancellation, $f(e_G) = e_{G'}$.
Proof of (2): This statement follows from the fact that

$$f(gg^{-1}) = f(e_G) = e_{G'} = f(g)f(g^{-1}).$$

Proof of (3): The set $f(H)$ is nonempty since the identity of H is in H. Suppose that H is a subgroup of G and let $f(h_1), f(h_2) \in f(H)$. There exist elements $h_1, h_2 \in H$ such that $f(h_1), f(h_2)$. Since

$$f(h_1 h_2^{-1}) = f(h_1)f(h_2)^{-1},$$

$f(H)$ is a subgroup of G' by closure and inverses.
Proof of (4): Let K be a subgroup of G' and define $f^{-1}(K)$ to be the set $\{g \in G \mid f(g) \in K\}$. The identity is in $f^{-1}(K)$ since $f(e_G) = e_{G'} \in K$. If $g_1, g_2 \in f^{-1}(K)$, then $f(g_1), f(g_2) \in K$ since K is a subgroup of G'. Therefore, $g_1 g_2^{-1} \in f^{-1}(K)$, and $f^{-1}(K)$ is a subgroup of G. If K is normal in G', we must show that $f^{-1}(K)$ is normal in G; that is, $gf^{-1}(K)g^{-1} \subseteq f^{-1}(K)$ for all $g \in G$. But

$$f(gf^{-1}(K)g^{-1}) = f(g)f(K)f(g^{-1}) \subseteq K,$$

since K is a normal subgroup of G'. Therefore, $f^{-1}(K)$ is normal in G.

■

KERNELS
The **kernel** of a group homomorphism $f : G \to G'$ is the set of all elements in G that map to the identity element in G'. Formally, the kernel is defined as

$$\ker(f) = \{g \in G \mid f(g) = e_{G'}\},$$

where $e_{G'}$ is the identity element of G'. The kernel plays a fundamental role in group theory as it measures how far the homomorphism is from being injective. If the kernel consists only of the identity element of G, then the homomorphism is injective (one-to-one). Additionally, the kernel is always a normal subgroup of G, which means it remains invariant under conjugation by elements of G.

Theorem 9.3. *Let $f : G \to G'$ be a group homomorphism. Then the kernel of f is a normal subgroup of G.*

9.2 The Isomorphism Theorems

[34]

FACTOR GROUPS and HOMOMORPHIC IMAGES Although it is not evident at first, factor groups correspond exactly to homomorphic images, and we can use factor groups to study homomorphisms. We already know that with every group homomorphism $\varphi : G \to H$ we can associate a normal subgroup of G, namely $\ker(\varphi)$. The converse is also true; that is, every normal subgroup of a group G gives rise to a homomorphism of groups.

Let $N \triangleleft G$ be a normal subgroup of G. Define the **natural** or **canonical homomorphism**

$$\phi : G \to G/N$$

by

$$\phi(g) = gN.$$

The kernel of this homomorphism is N.

Theorem 9.4 (**First Isomorphism Theorem**)**.** *If $\varphi : G \to H$ is a group homomorphism with $\ker(\varphi) = K$, then K is normal in G. Let $\phi : G \to G/K$ be the canonical homomorphism. Then there exists a unique isomorphism $\eta : G/K \to Im(\varphi)$ such that $\varphi = \eta \circ \phi$.*

Example: Let $G = \mathbb{Z}/n\mathbb{Z}$ be a cyclic group with generator g. Define a map $\varphi : \mathbb{Z} \to G$ by $\varphi(m) = g^m$. This map is a surjective homomorphism since

$$\varphi(m + n) = g^{m+n} = g^m g^n = \varphi(m)\varphi(n).$$

Clearly, φ is onto. If $\varphi(m) = e$, then $g^m = e$. Hence, m is divisible by n, and $\ker(\varphi) = n\mathbb{Z}$. On the other hand, if the order of g is infinite, then $\ker(\varphi) = \{0\}$ and φ is an isomorphism of $\mathbb{Z}$ and $\mathbb{Z}$. Hence, two cyclic groups are isomorphic exactly when they have the same order. Up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

[34] Section 11.2 in the textbook

Theorem 9.5 (**Second Isomorphism Theorem**). *Let H be a subgroup of a group G (not necessarily normal in G) and $N \triangleleft G$ a normal subgroup of G. Then $H \cap N \triangleleft H$, $HN/N \leq G/N$, and*

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

Theorem 9.6 (**Correspondence Theorem**). *Let N be a normal subgroup of a group G. Then there is a one-to-one correspondence between the set of subgroups of G containing N and the set of subgroups of G/N. Furthermore, the normal subgroups of G containing N correspond to normal subgroups of G/N.*

Theorem 9.7 (**Third Isomorphism Theorem**). *Let G be a group and let $N \triangleleft G$ and $K \triangleleft G$ with $K \subseteq N$. Then*

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

9.3 Reading Questions

[35]

11.3/1 Consider the function $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ defined by $\phi(x) = x + x$. Prove that ϕ is a group homomorphism.

Proof: Consider $x, y \in \mathbb{Z}_{10}$. Then $\phi(x+y) = (x+y)+(x+y) = (x+x)+(y+y) = \phi(x) + \phi(y)$. Hence, proved.

■

11.3/3 Compare and contrast isomorphism and homomorphisms.

Homomorphisms vs Isomorphisms

A **homomorphism** is a map between two groups $f : G \to G'$ that preserves the group operation, i.e., for all $g_1, g_2 \in G$,

$$f(g_1 g_2) = f(g_1) f(g_2).$$

An **isomorphism** is a bijective homomorphism. It implies that the two groups G and G' have the same structure, and there exists an inverse $f^{-1} : G' \to G$.

Key Differences:

- Every isomorphism is a homomorphism, but not all homomorphisms are isomorphisms.
- Isomorphisms require bijectivity (one-to-one and onto), while homomorphisms do not.
- Homomorphisms may map a group onto a smaller or different group; isomorphisms indicate structural equivalence between two groups.

11.3/4 Paraphrase the First Isomorphism Theorem using *only words.* No symbols allowed *at all.*

[35] Section 11.3 in the textbook

If there is a homomorphism between two groups, then the original group is divided into disjoint parts based on which elements are mapped to the same result. The group formed by these parts behaves in the same way as the group formed by the outputs of the homomorphism. This means that the original group, when split in this way, is structurally identical to the image of the homomorphism.

11.3/5 "For every normal subgroup there is a homomorphism, and for every homomorphism there is a normal subgroup." Explain the (precise) basis for this (vague) statement.

The statement "For every normal subgroup there is a homomorphism, and for every homomorphism there is a normal subgroup" refers to two fundamental concepts in group theory:

1. *For every normal subgroup there is a homomorphism*: This part is based on the fact that given a normal subgroup N of a group G, we can define a natural homomorphism from G to the quotient group G/N. This homomorphism is called the quotient map and sends each element of G to its corresponding coset in G/N. Thus, the existence of a normal subgroup gives rise to a natural homomorphism.
2. *For every homomorphism there is a normal subgroup*: This part refers to the fact that given a group homomorphism φ from a group G to another group H, the kernel of φ, which consists of all elements in G that map to the identity element in H, is always a normal subgroup of G. Therefore, any homomorphism defines a normal subgroup of the original group, known as the kernel.

This explains the precise basis for the statement, which connects normal subgroups and homomorphisms through the concepts of quotient maps and kernels.

9.4 Select Exercises

[36]

11.4/2 Which of the following maps are homomorphisms? If the map is a homomorphism, what is the kernel?

(a) $\mathbb{R}^* \to GL_2(\mathbb{R})$ defined by $\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$

It is easy to see that this map is a homomorphism. To find the kernel, we must find all the real numbers that map to $e \in GL_2(\mathbb{R})$. The identity matrix demands that $a = 1 \implies \ker \phi = \{1\} \in \mathbb{R}^*$.

11.4/3 Let A be an $m \times n$ matrix. Show that matrix multiplication, $x \mapsto Ax$, defines a homomorphism $\phi : \mathbb{R}^n \to R^m$.

Proof: Consider a matrix A and two elements $x, y \in \mathbb{R}^n$. Since $A \in \mathbb{R}^{m \times n}$, we have $Ax \in \mathbb{R}^m$. So, $\phi(x + y) = A(x + y) = Ax + Ay = \phi(x) + \phi(y)$, where $Ax, Ay \in \mathbb{R}^m$.

■

[36] Section 11.4 in the textbook

11.4/5 Describe all of the homomorphisms from $\mathbb{Z}_{24} \to \mathbb{Z}_{18}$.
Let ϕ be a homomorphism. Suppose $\phi(1) = k$, $k \in \mathbb{Z}_{18}$. Then $\phi(m) = m\phi(1) = mk$. So $\phi(1)$ can give us $\phi(m)$, $\forall m \in \mathbb{Z}_{24}$. Since $24 \equiv 0 \pmod{24} \implies 24k = \phi(24) = \phi(0) = 0 \implies 24k \equiv 0 \pmod{18} \implies 8k \equiv 0 \pmod{18} \implies 4k \equiv 0 \pmod{3} \implies k \equiv 0 \pmod{3}$. So, possible values of k are given by $\{0, 3, 6, 9, 12, 15\}$.

So homomorphisms $\phi(m) = mk \pmod{18}$ for $k = \{0, 3, 6, 9, 12, 15\}$.

11.4/8 If G is an abelian group and $n \in \mathbb{N}$, show that $\phi : G \to G$ defined by $g \mapsto g^n$ is also a group homomorphism.
Proof: Consider $a, b \in G$. Then $\phi(ab) = (ab)^n = a^n b^n$ (since G is abelian) $= \phi(a)\phi(b)$.

■

11.4/9 If $\phi : G \to H$ is a group homomorphism and G is abelian, prove that $\phi(G)$ is also abelian.
Proof: Since G is abelian, we have $ab = ba \implies \phi(ab) = \phi(ba) \implies \phi(a)\phi(b) = \phi(b)\phi(a)$, showing that $\phi(G)$ is abelian.

■

11.4/10 If $\phi : G \to H$ is a group homomorphism and G is cyclic, prove that $\phi(G)$ is also cyclic.
Proof: Since G is cylic, we have $g \in G$ s.t. $< g >= G \implies g^k = G, k \in \mathbb{N}$. Then $\phi(g^k) = (\phi(g))^k \implies < \phi(g) >= \phi(G)$, showing that $\phi(G)$ is cyclic. (generators map to generators)

■

11.4/12 If G has exactly one subgoup H of order k, prove that $H \triangleleft G$.
Proof: $\forall g \in G$, define a map $\phi : G \to G$ by $x \mapsto gxg^{-1}$. Observe that, for $x, y \in G$ $\phi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \phi(x)\phi(y)$. So the map is homomorphic.

Note that the map is bijective: $\varphi_{g^{-1}}(\varphi_g(x)) = \varphi_{g^{-1}}(gxg^{-1}) = g^{-1}gxg^{-1}(g^{-1})^{-1} = x$ and similarly, $\varphi_g(\varphi_{g^{-1}}(x)) = x$. //
Thus, the ϕ is a subgroup of G (by homomorphism) with the same cardinality as H (by bijectivity), so it is normal.

■

11.4/13 Prove or disprove: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$.
Proof:

■

11.4/14 Let G be a finite group and N a normal subgroup of G. If H is a subgroup

of G/N prove that $\phi^{-1}(H)$ is a subgroup in G of order $|H| \cdot |N|$, where $\phi : G \to G/N$ is the canonical homomorphism.

Proof: 1. The homomorphism $\phi : G \to G/N$ is defined by $\phi(g) = gN$ and has kernel $\ker(\phi) = N$.

2. The preimage $\phi^{-1}(H)$ is given by:

$$\phi^{-1}(H) = \{g \in G : gN \in H\}.$$

3. To show $\phi^{-1}(H)$ is a subgroup of G: - **Identity**: Since $N \in H$, the identity $e_G \in \phi^{-1}(H)$. - **Closure**: For $g_1, g_2 \in \phi^{-1}(H)$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \in H$, hence $g_1 g_2 \in \phi^{-1}(H)$. - **Inverses**: For $g \in \phi^{-1}(H)$, $\phi(g^{-1}) = \phi(g)^{-1} \in H$, thus $g^{-1} \in \phi^{-1}(H)$.

4. Therefore, $\phi^{-1}(H)$ is a subgroup of G.

5. To determine the order:

$$|G| = |N| \cdot |G/N| \quad \text{and} \quad |G/N| = |H| \implies |G| = |N| \cdot |H|.$$

The subgroup $\phi^{-1}(H)$ consists of all lifts of elements in H with each lift corresponding to $|N|$ elements, leading to:

$$|\phi^{-1}(H)| = |H| \cdot |N|.$$

Thus, we conclude that $\phi^{-1}(H)$ is a subgroup of G with the desired order.

■

11.4/16 If H and K are normal subgroups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of $G/H \times G/K$.

Proof: 1. Define a map $\phi : G \to G/H \times G/K$ by

$$\phi(g) = (gH, gK).$$

2. ϕ is a well-defined homomorphism:

$$\phi(g_1 g_2) = (g_1 g_2 H, g_1 g_2 K) = (g_1 H, g_1 K)(g_2 H, g_2 K) = \phi(g_1)\phi(g_2).$$

3. The kernel of ϕ is

$$\ker(\phi) = \{g \in G : gH = H \text{ and } gK = K\} = H \cap K = \{e\}.$$

Thus, ϕ is injective.

4. The image $\mathrm{Im}(\phi)$ is a subgroup of $G/H \times G/K$, and since ϕ is injective, we have

$$G \cong \mathrm{Im}(\phi) \subseteq G/H \times G/K.$$

Therefore, G is isomorphic to a subgroup of $G/H \times G/K$.

■

10 STRUCTURE of GROUPS

10.1 Finite Abelian Groups

[37]

All cyclic groups of prime order are isomorphic to $\mathbb{Z}_p$, where p is prime. Also, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ when $\gcd(m,n) = 1$. Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order; that is, every finite abelian group is isomorphic to a group of the type

$$\mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_n}^{\alpha_n}$$

where each p_k is prime (not necessarily distinct).

Definition 10.1. *If there exists a set such that $\{g_i : i \in I\}$ generates G and it is finite, then G is **finitely generated**. I is the set of indices.*

Theorem 10.2. *Let $H < G$ generated by $\{g_i \in G : i \in I\}$. Then $h \in H$ exactly when it is a product of the form*

$$h = g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n},$$

where the g_{i_1}s are not necessarily distinct.

We can express any finite abelian group as a finite direct product of cyclic groups.

Definition 10.3. *Define a group G to be a P-**group** if every element in G has as its order a power of p, where p is prime.*

Theorem 10.4 (**Fundamental Theorem of Finite Abelian Groups**)**.** *Every finite abelian group G is isomorphic to a direct product of cyclic groups of the form*

$$\mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_n}^{\alpha_n}$$

here the p_i's are primes and not necessarily distinct.

Lemma 10.5. *Let G be a finite abelian group, and $|G| = n$. If $p|n \implies \exists g \in G$ s.t. $|g| = p$.*

Lemma 10.6. *A finite abelian group is a p-group if and only if its order is a power of p.*

Lemma 10.7. *Let G be a finite abelian group of order $n = p_1^{\alpha_1} \dots p_n^{\alpha_n}$. Then G is the internal direct product of subgroups $G_1, \dots, G_k$, where G_i is the subgroup of G consisting of all elements of order $p_i^r, r \in \mathbb{Z}$.*

Lemma 10.8. *Let G be a finite abelian p-group and suppose that $g \in G$ has maximal order. Then G is ormorphic to $< g > \times H$ for some $H < G$.*

[37] Section 13.1 in the textbook

10.2 Reading Questions

[38]

13.3/1 How many abelian groups are there of order $200 = 2^3 \cdot 5^2$
For $200 = 2^3 \cdot 5^2$, we find the following: - For the factor 2^3, the partitions of 3 are: - (3) - $(2, 1)$ - $(1, 1, 1)$ There are 3 partitions of 3. - For the factor 5^2, the partitions of 2 are: - (2) - $(1, 1)$ There are 2 partitions of 2.
Thus, the number of abelian groups of order 200 is the product of the partitions for each prime factor, i.e., $3 \times 2 = 6$.
So, there are 6 distinct abelian groups of order 200.

13.3/2 How many abelian groups are there of order $729 = 3^6$
The number of abelian groups of order 3^6 is determined by the partitions of 6: - (6) - $(5, 1)$ - $(4, 2)$ - $(4, 1, 1)$ - $(3, 3)$ - $(3, 2, 1)$ - $(3, 1, 1, 1)$ - $(2, 2, 2)$ - $(2, 2, 1, 1)$ - $(2, 1, 1, 1, 1)$ - $(1, 1, 1, 1, 1, 1)$
There are 11 partitions of 6, so there are 11 distinct abelian groups of order 729.

13.3/3 Find a subgroup of order 6 in $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
The order of $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ is $8 \cdot 3 \cdot 3 = 72$. A subgroup of order 6 can be found by taking elements whose orders are 2 and 3.
Consider the subgroup generated by: - The element of order 2 in $\mathbb{Z}_8$: $(4, 0, 0)$ (since 4 has order 2 in $\mathbb{Z}_8$). - The element of order 3 in $\mathbb{Z}_3 \times \mathbb{Z}_3$: $(0, 1, 0)$.
Thus, the subgroup generated by $(4, 1, 0)$ has order 6, as the least common multiple of 2 and 3 is 6.

13.3/4 It can be shown that an abelian group of order 72 contains a subgroup of order 8. What are the possibilities for this subgroup?
The order of the abelian group is $72 = 2^3 \cdot 3^2$. A subgroup of order 8 must involve only the 2-part of the group, i.e., the Sylow 2-subgroup.
The Sylow 2-subgroup is of order $2^3 = 8$. The possible subgroups of order 8 are the abelian groups whose orders divide 8. These are $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

11 GROUP ACTIONS

11.1 Groups Acting on Sets

[39]

Definition 11.1. *Let X be a set and G be a group. A **left action** of G on X is a map $G \times X \to X$ given by $(g, x) \mapsto gx$, where*

- $ex = x, \ \forall x \in X$
- $(g_1 g_2)x = g_1(g_2 x), \ \forall x \in X$ *and* $g_1, g_2 \in G$

[38] Section 13.3 in the textbook
[39] Section 14.1 in the textbook

Under these considerations X is called a ***G-set****.*

In general, if X is any set and $G < S_X$, the group of all permutations acting on X, then X is a $G - set$ under the group action $(\sigma, x) \mapsto \sigma(x),\ \sigma \in G$ and $x \in X$.

Definition 11.2. *Let G be a group and suppose that $X = G$. If $H < G \implies G$ is an H-set under* ***conjugation****; that is, we can define an action of H on G, $H \times G \to G$, via $(h, g) \mapsto hgh^{-1},\ h \in H$ and $g \in G$.*

If G acts on a set X and $x, y \in X$, then x is said to be G**-equivalent** to y if there exists a $g \in G$ such that $gx = y$. We write $x \sim y$ if two elements are G-equivalent.

Theorem 11.3. *Let X be a G-set. Then G-equivalence is anequivalence relation on X.*

Definition 11.4. *If X is a G-set, then each partition of X associeated with the G-equivalence is clled an* ***orbit*** *of X under G. We will denote the ordbit that contains an element $x \in X$ by $\mathcal{O}_x$ or O_x.*

Now suppose that G is a group acting on a set X and let $g \in G$. The **fixed point set** of g in X, denoted X_g, is the set of all $x \in X$ s.t. $gx = x$. We can also study the group elements g that fix a given $x \in X$. This set is a subgroup called the **stabilizer subgroup** or **isotropy subgroup** of x. We denote this using G_x.

Theorem 11.5. *Let G be a finite group and X a finite G-set. If $x \in X$, then $|O_x| = [G : G_x]$.*

11.2 The Class Equation

[40]

Let X be a finite G-set and

$$X_G = \{x \in X : gx = x \quad \forall g \in G\}$$

(the set of fixed points in X). Since the orbits of the action partition X, we have

$$|X| = |X_G| + \sum_{i=k}^{n} |O_{x_i}|,$$

where $x_k, \ldots, x_n$ are representatives from the distinct nontrivial orbits of X.

Consider the special case in which G acts on itself by **conjugation**, $(gx) \mapsto gxg^{-1}$. The **center of** G is given by

$$Z(G) = \{x : xg = gx \quad \forall g \in G\}$$

which represents the set of points fixed by conjugation. The nontrivial orbits of htis action are called the **conjugacy classes** of G.

From theorem 11.5 in this document, we obtain the following **class equation**

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)]$$

The stabilizer subgroups of each x_i is $C(x_i) = \{g \in G : gx_i = x_i g\}$.

One of the consequences of the class equation is that the order of each conjugacy class must divide the order of G.

[40] Section 14.2 in the textbook

Theorem 11.6. *Let G be a group of order p^n. Then G has a nontrivial center.*

Corollary 11.7. *Let G be a group of order p^2. Then G is abelian.*

12 SYLOW THEOREMS

12.1 The Sylow Theorems

[41]

Definition 12.1. *A group G is a **p-grouo** if every element in G has as its order a power of p, where p is a prime number. A subgroup of a group G is a $p-$subgroup if it is a p-group.*

Theorem 12.2 (**Cauchy**). *Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.*

Corollary 12.3. *Let G be a finite group. Then G is a p-group if and only if $|G| = p^n$.*

Theorem 12.4 (**First Sylow Theorem**). *Let G be a finite group and p a prime such that p^r divides $|G|$. Then G contains a subgroup of order p^r.*

A **Sylow p- subgroup** P of a group G is a maximal p-subgroup of G.

Definition 12.5. *The **normalizer** of H in G is given by*

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

H is a normal subgroup of N(H); it is the largest subgroup of G in which H is normal.

Lemma 12.6. *Let P be a Sylow p-group of a finite grou pG and let x have as its order a power of p. If $x^{-1}Px = P$, then $x \in P$.*

Theorem 12.7 (**Second Sylow Theorem**). *Let G be a finite group and p a prime dividing $|G|$. Then all Sylow p-subgroups of G are conjugate. That is, if P_1 and P_2 are two Sylow p-subgroups, $\exists g \in G$ s.t. $gP_1g^{-1} = P_2$.*

Theorem 12.8 (**Third Sylow Theorem**). *Let G be a finite group and p a prime dividing $|G|$. The number of Sylow p-subgroups is congruent to $1 \pmod p$ and divides $|G|$.*

12.2 Examples and Applications

[42]

Theorem 12.9. *If p and q are distinct primes with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence, G cannot be simple. Furthermorem if $q \not\equiv 1 \pmod p$, then G is cyclic.*

[41] Section 15.1 in the textbook
[42] Section 15.2 in the textbook

Theorem 12.10. *Let $G' =< aba^{-1}b^{-1} : a, b \in G >$ be the subgroup consisting of all finite products of elements of the form $aba^{-1}b^{-1} \in G$. Then $G' \triangleleft G$ and G/G' is abelian.*

The subgroup G' is called the **commutator subgroup** of G.

Lemma 12.11. *Let H and K be finite subgroups of a group G. Then*

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

12.3 Reading Questions

[43]

15.3/1 State Sylow's First Theorem.
Sylow's First Theorem states that if G is a finite group and p is a prime dividing the order of G, then G has at least one subgroup of order p^k for each k such that p^k divides the order of G (where p^k is the highest power of p dividing the order of G).

15.3/2 How many groups are there of order 69? Why?
There are exactly two groups of order 69. By the Sylow theorems, the number of Sylow 3-subgroups n_3 must divide 23 and satisfy $n_3 \equiv 1 \mod 3$. The possible values are 1 or 23. If $n_3 = 1$, there is a normal Sylow 3-subgroup, making the group a semidirect product of this normal subgroup and the Sylow 23-subgroup (which is cyclic). If $n_3 = 23$, all Sylow 3-subgroups are conjugate and non-normal, leading to a different structure. Thus, we can conclude there are two distinct groups.

15.3/3 Give two descriptions, fundamentally different in character, of the normalizer of a subgroup.
1. The normalizer $N_G(H)$ of a subgroup H in a group G is defined as $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$; it consists of all elements in G that commute with H under conjugation.
2. The normalizer can also be described as the largest subgroup of G in which H is normal. It reflects the structure of H within G by identifying the symmetries of H that preserve its subgroup structure.

15.3/4 Suppose that G is an abelian group. What is the commutator subgroup of G, and how do you know?
The commutator subgroup $[G, G]$ of an abelian group G is the trivial subgroup, i.e., $[G, G] = \{e\}$. This is because in an abelian group, every element commutes with every other element, so for any $g, h \in G$, the commutator $[g, h] = g^{-1}h^{-1}gh$ equals the identity element e.

15.3/5 What's all the fuss about Sylow's Theorems?

[43] Section 15.3 in the textbook

Sylow's Theorems provide crucial information about the structure of finite groups by detailing the existence and properties of p-subgroups for each prime p dividing the group order. They establish the relationship between group order and subgroup structure, allowing mathematicians to classify groups, understand their composition, and analyze their actions.

13 RINGS

13.1 Rings

[44]

Definition 13.1. *A nonempty set R is a **ring** if it has two closed binary operations, addition, and multiplication, satisfying the following conditions.*

1. $a + b = b + a \quad a, b \in R$
2. $(a + b) + c = a + (b + c) \quad a, b, c \in R$
3. *There is an element* $0 \in R$ *such that* $a + 0 = a \quad \forall a \in R$
4. *For every element* $a \in R$*, there exists an element* $-a \in R$ *such that* $a + (-a) = 0$
5. $(ab)c = a(bc) \quad a, b, c \in R$
6. *For* $a, b, c \in R : a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$

14 POLYNOMIALS

14.1 Polynomial Rings

We assume all rings R is a commutative ring with an identity. A **polynomial ring** is of the form with **indeterminate** x

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

where $a_i \in R$ and $a_n \neq 0$. The a_i's are **coefficients**. The coefficient a_n is the **leading** coefficient. Additionally, a polynomial is **monic** if the leading coefficient is 1. If n is the largest nonnegative number for which $a_n \neq 0$, we say that the **degree** of f of n and write $f(x) = n$. If no such n exists, the polynomial is a 0 one, and its degree is $-\infty$.

Two polynomials are equal when all of their corresponding coefficients are equal.

Theorem 14.1. *Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.*

[44] Section 16.1 in the textbook

Theorem 14.2. *Let $p, q \in R[x]$, where R is an integral domain. Then* $\deg p + \deg q = \deg(pq)$. *Furthermore, $R[x]$ is an integral domain.*

We can also subsequently define a ring with more than one indeterminate (variable). So we can have $R[x_1, \ldots, x_n]$. We also have $(R[x])[y] \cong (R[y])[x]$.

14.2 The Division Algorithm

Like for whole numbers, we can define the division algorithm for polynomials as follows.

Theorem 14.3 (**Division Algorithm**). *Let $f, g \in F[x]$, where F is a field and g is a nonzero polynomial. Then there exists unique polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x)$$

where either $\deg r < \deg g$ *or r is the zero polynomial.*

We have a **zero** of a polynomial $p(x)$ if $p(\alpha) = 0$.

Corollary 14.4. *Let F be a field. An element $\alpha \in F$ is a zero of $p(x) \in F[x] \iff x - \alpha$ is a factor of $p(x) \in F[x]$.*

Corollary 14.5. *Let F be a field. A nonzero polynomial $p(x)$ of degree n in F[x] can have at most n distinct zeros in F.*

Since we can have the division algorithm for polynomials, we can naturally have the greatest common divisor as well. We define it as follows.

Theorem 14.6. *Let F be a field and suppose that d(x) is a GCD of two polynomials p(x) and q(x) in F[x]. Then there exists polynomials r(x) and s(x) such that*

$$d(x) = r(x)p(x) + s(x)q(x).$$

Furthermore, the GCD of two polynomials is unique.

14.3 Irreducible Polynomials

A nonconstant polynomial f in F[x] is **irreducible** over a field F if f cannot be expressed as a product of two polynomials g and $h \in F[x]$, where the degrees of g and h are smaller than the degree of f.

Irreducible polynomials function analogous to prime numbers.

Lemma 14.7. *Let $p \in \mathbb{Q}[x]$. Then*

$$p(x) = \frac{r}{s}(a_0 + \cdots + a_n x^n)$$

where r, s, a_i's are integers, and all the coefficients are relatively prime, and r and s are relatively prime.

Theorem 14.8 (**Gauss's Lemma**). *Let $p(x) \in \mathbb{Z}[x]$ be a monic polynomial such that p factors into a product of two polynomials α and $\beta \in \mathbb{Q}[x]$, where the degrees of the factors are less than p. Then $p = a(x)b(x)$, where a and b are monic polynomials in $\mathbb{Z}[x]$ with $\deg \alpha = \deg a$ and $\deg \beta = \deg b$.*

Corollary 14.9. *Let $p = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Z}$ and $a_0 \neq 0$. If p has a zero in $\mathbb{Q}$, then p has a zero α in $\mathbb{Z}$. Furthermore, $\alpha | a_0$.*

Theorem 14.10 (**Eisenstein's Criterion**). *Let p be a prime and suppose that*

$$f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x].$$

If $p | a_i$, for $i = 1, \ldots, n-1$, but $p \nmid a_n$ and $p^2 \nmid a_o$, then f is irreducible over $\mathbb{Q}$.

IDEALS in $F[x]$ Recall that a principal ideal in $F[x]$ is an ideal $< p(x) >$ generated by some polynomial $p(x)$; that is,

$$< p(x) >= \{p(x)q(x) : q(x) \in F[x]\}.$$

Theorem 14.11. *If F is a field, then every ideal in $F[x]$ is a principal ideal.*

Theorem 14.12. *Let F be a field and suppose that $p(x) \in F[x]$. Then the ideal generated by $p(x)$ is maximal $\iff$ $p(x)$ is irreducible.*

14.4 Select Exercises

[45]

17.5/6 Find all units in $\mathbb{Z}[x]$.
In $\mathbb{Z}[x]$, a polynomial $p(x)$ is a unit if there exists $q(x) \in \mathbb{Z}[x]$ such that $p(x) \cdot q(x) = 1$. The constant terms of $p(x)$ and $q(x)$ must multiply to 1. Hence, $p(x)$ and $q(x)$ must have constant terms ± 1.
Since $p(x)$ must divide 1 in $\mathbb{Z}[x]$, the only such polynomials are $p(x) = \pm 1$.

17.5/7 Find a unit $p(x)$ in $\mathbb{Z}_4[x]$ such that $\deg p(x) > 1$.
An element $p(x) \in \mathbb{Z}_4[x]$ is a unit if there exists another element $g(x) \in \mathbb{Z}_4[x]$ such that $p \cdot g = 1$ in $\mathbb{Z}_4[x]$. Consider $p(x) = 2x^2 + 1$. Then $g = p = 2x^2 + 1 \implies p \cdot g = (2x^2 + 1)(2x^2 + 1) = 4x^4 + 4x^2 + 1 = 1$. Note that $\deg p = 2 > 1$.

17.5/8 Which of the following are reducible over $\mathbb{Q}[x]$.

[45] Section 17.5 in the textbook

(a) $x^4 - 2x^3 + 2x^2 + x + 4$
Similar to part (b), there are no linear factors. So proceeding, we get $a + c = -2,\ ac + b + d = 2,\ ad + bc = 1,\ bd = 4$. So $b = d = \pm 2$. Since $b = d \implies b(a + c) = 1 \implies -2b = 1 \implies b \notin \mathbb{Z}$. Thus, irreducible.

(b) $x^4 - 5x^3 + 3x - 2$
No linear factors, so

$$\begin{aligned} p(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd, \end{aligned}$$

By Gauss's Lemma, we can say that $a + c = -5,\ ac + b + d = 0,\ ad + bc = 3,\ bd = -2$. Since $bd = -2 \implies b, d = \pm 1, \mp 2$. So $b+d = 1-2, -1+2 = \pm 1$. So $ac = \pm 1$. If $ac = 1 \implies a = c = 1$; if $ac = -1 \implies a, c = \pm 1, \mp 1$. In either case, $a + c \neq 5$. Thus, irreducible.

(c) $3x^5 - 4x^3 - 6x^2 + 6$
Irreducible by Eisenstein's criterion.

(d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$
Irreducible by Eisenstein's criterion.

17.5/9 Find all irreducible polynomials of degrees 2 and 3 in $\mathbb{Z}_2[x]$.
A polynomial $p(x)$ of degree 2 or 3 is reducible if and only if it has a linear factor. So, for a linear factor to exist, we must have that $p(0) = 0$ or $p(1) = 0$, since $\mathbb{Z}_2 = \{0, 1\}$. In other words, $p(x)$ has no linear factor if and only if $p(0) = p(1) = 1$. In $\mathbb{Z}_2[x]$, $p(0) = 1$ only when the constant term is 1, so we must have 1 in all irreducible polynomials. Also, $p(1) = 1$ when we have an odd number of terms in the polynomial; if even, then $p(1) = 2m \equiv 0 \pmod 2$, for some $m \in \mathbb{N}$.

We see that the only polynomial of degree 2 to meet this criteria is $x^2 + x + 1$. For degree 3, we have $x^3 + x^2 + 1$ and $x^3 + x + 1$.

17.5/10 Give two different factorizations of $x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$.
We can rewrite $x^2 + x + 8$ as $x^2 + x - 2$, which can be factored into $(x - 1)(x + 2)$ which is the same as $(x + 9)(x + 2)$. Similarly, we have $x^2 + x + 8 = x^2 + x - 12$, which can be factored into $(x - 3)(x + 4) = (x + 7)(x + 4)$.

17.5/11 Prove or disprove: There exists a polynomial $p(x)$ in $\mathbb{Z}_6[x]$ of degree n with more than n distinct zeros.
Consider the polynomial $p(x) = 3x$. Observe that its degree is 1, but $p(0) = p(2) = 0 \pmod 6$.

17.5/12 If F is a field, show that $F[x_1, \ldots, x_n]$ is an integral domain.

Proof: Assume $p, q \in F[x_1, \ldots, x_n]$ are nonzero polynomials. We must show that $p \cdot q \neq 0$. Each polynomial has a *total degree*, which is the highest degree among its monomials when expressed in standard form. The total degree of the product $p \cdot q$ is equal to the sum of the total degrees of p and q, since the product of the highest-degree terms of p and q dominates in the expansion of $p \cdot q$. Therefore, $p \cdot q$ is a polynomial of positive degree and cannot be the zero polynomial.

■

17.5/13 Show that the division algorithm does not hold for $\mathbb{Z}[x]$. Why does it fail?
Consider two polynomials $f(x) = x^2$ and $g(x) = 2x$. Dividing the leading terms, we get $x/2 \notin \mathbb{Z}[x]$. Thus, the division algorithm does not work.

17.5/14 Prove or disprove: $x^p + a$ is irreducible for any $a \in \mathbb{Z}_p$, where p is prime.
Consider the case $a = 0$, then $x^p + a = x^p = x^{p-1}x$. Thus, it is reducible.

17.5/20 The polynomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

is called the cyclotomic polynomial. Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ for any prime p.
Proof: The roots of $\Phi_p(x)$ are the primitive p-th roots of unity, given by:

$$\zeta = e^{2\pi i k/p}, \quad k = 1, 2, \ldots, p-1,$$

where ζ satisfies $\zeta^p = 1$ but $\zeta^m \neq 1$ for $1 \leq m < p$. Therefore, $\Phi_p(x)$ is the minimal polynomial of the primitive p-th roots of unity over $\mathbb{Q}$.
To prove that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$, consider the polynomial $\Phi_p(x+1)$ obtained by substituting $x = y+1$. Expanding this substitution, we have:

$$\Phi_p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1.$$

Using the binomial theorem, each term can be written as:

$$(x+1)^k = \sum_{j=0}^{k} \binom{k}{j} x^j.$$

In $\Phi_p(x+1)$, all coefficients except the leading term are divisible by p, and the constant term is exactly p. Thus, $\Phi_p(x+1)$ satisfies Eisenstein's Criterion at p, ensuring that $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}$. Therefore, $\Phi_p(x)$ is also irreducible over $\mathbb{Q}$.

■

17.5/21 If F is a field, show that there are infinitely many irreducible polynomials

in $F[x]$.

Proof: Suppose there are only finitely many irreducible polynomials in $F[x]$, say $p_1(x), p_2(x), \ldots, p_n(x)$. Consider the polynomial:

$$q(x) = p_1(x)p_2(x)\cdots p_n(x) + 1.$$

Clearly, $q(x) \not\equiv 0$ because the constant term of $q(x)$ is 1. Moreover, $q(x)$ is not divisible by any of the $p_i(x)$, since dividing $q(x)$ by $p_i(x)$ leaves a remainder of 1. Thus, $q(x)$ is not reducible in terms of $p_1(x), p_2(x), \ldots, p_n(x)$, contradicting the assumption that these are the only irreducible polynomials in $F[x]$.
Hence, $F[x]$ must contain infinitely many irreducible polynomials.

■

17.5/24 Show that $x^p - x$ has p distinct zeros in $\mathbb{Z}_p$, for any prime p. Conclude that

$$x^p - x = x(x-1)\ldots(x-(p-1)).$$

Proof: $\mathbb{Z}_p = \{1, \ldots, p-1\}$ and $f(x) = x^p - x$.

Using Fermat's little theorem, we have, for $a \in \mathbb{Z}_p$ and a is nonzero, that $a^p \equiv a \pmod{p} \implies a^p - a \equiv 0 \pmod{p}$. Thus, $\forall a \in \mathbb{Z}_p$, we have $f(a) \equiv 0$. Since $|\mathbb{Z}_p| = p$, we have p distinct roots (all elements of $\mathbb{Z}_p$) for $f(x)$.

Since $\mathbb{Z}_p$ is a field, we know that if $\alpha \in \mathbb{Z}_p$ is a root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$. Thus, $(x - \alpha)$ divides $f(x)$ for all $\alpha \in \mathbb{Z}_p$:

$$f(x) = x^p - x = (x-0)(x-1)\ldots(x-(p-1)) = x(x-1)\ldots(x-(p-1))$$

■

17.5/26 Let F be a field. Show that $F[x]$ is never a field.

Proof: Let F be a field. Consider a polynomial $f(x) = x \in F[x]$. Note that $\deg f(x) = 1$. For $F[x]$ to be a field, there must exists a polynomial $g(x) \in F[x]$ s.t. $f \cdot g = 1 \implies x \cdot g(x) = 1$.

For $x \cdot g(x) = 1$, $g(x)$ would have to be a polynomial whose product with x gives the constant polynomial 1. Observe that $\deg x \cdot g(x) = \deg x + \deg g(x) \geq 1$. However $\deg 1 = 0$. So $\deg g(x)$ must equal -1, which is not possible.

So $f(x) = x$ has no multiplicative inverse in $F[x]$. Thus, $F[x]$ is not a field.

■

15 INTEGRAL DOMAINS

15.1 Fields of Fractions

15.2 Factorization in Integral Domains

15.3 Select Exercises

[46]

18.4/1 Let $z = a + b\sqrt{3}i$ be in $\mathbb{Z}[\sqrt{3}i]$. If $a^2 + 3b^2 = 1$, show that z must be a unit. Show that the only units of $\mathbb{Z}[\sqrt{3}i]$ are 1 and -1.

(a) **Show z is unit.**

Proof: We have $z = a + b\sqrt{3}i$. Note that $a + b\sqrt{3}i \cdot \frac{1}{a+b\sqrt{3}i} = 1$. So $z^{-1} = \frac{1}{a+b\sqrt{3}i} = \frac{1}{a+b\sqrt{3}i} \cdot \frac{a-b\sqrt{3}i}{a-b\sqrt{3}i} = \frac{a}{a^2+3b^2} - \frac{b\sqrt{3}i}{a^2+3b^2}$. Since $a^2 + 3b^2 = 1$, we have $z^{-1} = a - b\sqrt{3}i = a + c\sqrt{3}i$ where $-b = c \in \mathbb{Z}$ and $a \in \mathbb{Z}$. Thus $z^{-1} \in \mathbb{Z}[\sqrt{3}i]$. Thus, z is a unit.

■

(b) **Show 1 and -1 are the only units.**

Proof: Clearly, $a = \pm 1, b = 0$ satisfy $a^2 + 3b^2 = 1 \implies a^2 = 1 - 3b^2$. Suppose there are other solutions. Then $b^2 \geq 1 \implies 1 - 3b^2 \leq -2 \implies a \notin \mathbb{Z}$. Thus, other solutions are not possible.

■

18.4/2 The Gaussian integers, $\mathbb{Z}[i]$, are a UFD. Factor each of the following elements into a product of irreducibles.

(a) 5

Observe that $5 = 2^2 + 1^2 = (2 - i)(2 + i) = -i(1 + 2i)(2 + i)$.

(b) 1+3i

We need solutions for $a^2 + b^2 = 1$. We see that with $a = 1, b = 3$, there are no such solutions. So $1 + 3i$ is irreducible.

18.4/4 Prove or disprove: Any subring S of a field F containing 1 is an integral domain.

Proof: Since S is a subring of a field F, we know that S also has no zero-divisors. If S had zero-divisors, then F has zero-divisors, but that is not possible since F is a field. Since S also contains 1, the identity, it is an integral domain.

■

18.4/6 Let F be a field of characteristic zero. Prove that F contains a subfield

[46] Section 18.4 in the textbook

isomorphic to $\mathbb{Q}$.

Proof: Since F has characteristic zero, we know that the set $\mathbb{Z} = \{0, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots\} \subseteq F$ is a subring of F. This follows from the fact that the characteristic of F is zero, meaning that no positive integer n satisfies $n \cdot 1_F = 0$.

Elements of $\mathbb{Q}$ are of the form $\frac{a}{b}$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$.

For each $\frac{a}{b} \in \mathbb{Q}$, we can define an element $\frac{a}{b}$ in F by taking $a \in F$ and $b \in F$ (since $\mathbb{Z} \subseteq F$) and using the multiplicative inverse $b^{-1} \in F$ (since $b \neq 0$ and F is a field). This gives the element $a \cdot b^{-1} \in F$.

Thus, the map

$$\varphi : \mathbb{Q} \to F, \quad \varphi\left(\frac{a}{b}\right) = a \cdot b^{-1},$$

is well-defined, injective, and preserves both addition and multiplication, making it an isomorphism of fields. Therefore, the subfield of F generated by $\mathbb{Z}$ is isomorphic to $\mathbb{Q}$.

■

Well-defined: If $\frac{a}{b} = \frac{c}{d}$, then $a \cdot d = b \cdot c$. Therefore: $a \cdot b^{-1} = c \cdot d^{-1}$, which shows that $\varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{c}{d}\right)$, proving that φ is well-defined.
Injectivity: Suppose $\varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{c}{d}\right)$. Then: $a \cdot b^{-1} = c \cdot d^{-1} \implies a \cdot d = b \cdot c$.
Addition: We have:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \implies \varphi\left(\frac{a}{b} + \frac{c}{d}\right) = (ad + bc) \cdot (bd)^{-1} = \frac{ad + bc}{bd}.$$

On the other hand:

$$\varphi\left(\frac{a}{b}\right) = a \cdot b^{-1}, \quad \varphi\left(\frac{c}{d}\right) = c \cdot d^{-1}, \implies \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right) = \frac{ad + bc}{bd}.$$

Thus, φ preserves addition.
Multiplication: We have:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \implies \varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = (ac) \cdot (bd)^{-1}.$$

On the other hand:

$$\varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{c}{d}\right) = (a \cdot b^{-1}) \cdot (c \cdot d^{-1}) = ac \cdot (bd)^{-1}.$$

Thus, φ preserves multiplication.

18.4/8 Let p be prime and denote the field of fractions of $\mathbb{Z}_p[x]$ by $\mathbb{Z}_p(x)$. Prove that $\mathbb{Z}_p(x)$ is an infinite field of characteristic p.

Proof: First, we must show that $\mathbb{Z}_p$ is infinite. The ring $\mathbb{Z}_p[x]$ contains polynomials of arbitrary degree, and there are infinitely many such polynomials since the degree of such polynomials can grow without bounds. For example, x^n, $n \in \mathbb{N}$. Since there are infinitely many polynomials $f(x), g(x) \in \mathbb{Z}_p[x]$, there are infinitely many rational functions of the form $h(x) = f/g \in \mathbb{Z}_p(x)$.

Note that the characteristic of $\mathbb{Z}_p$ is p since $p \cdot 1 = 0 \pmod{p}$. The ring $\mathbb{Z}_p[x]$ inherits this characteristic which implies that for any polynomial $f(x) \in \mathbb{Z}_p[x]$, we have $p \cdot f(x) = 0 \in \mathbb{Z}_p[x]$. Then, consider a rational function $f/g \in \mathbb{Z}_p(x)$:

$$p \cdot \frac{f}{g} = \frac{p \cdot f}{g} = \frac{0}{g} = 0$$

. Thus, $\mathbb{Z}_p(x)$ has characteristic p as well.

■

18.4/11 Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

(a) **Prove it is an integral domain.**

Proof: If we choose $a = 1, b = 0 \implies 1 \in \mathbb{Z}[\sqrt{2}]$, so the identity is contained. Choose two elements and let their product be 0:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2} = 0$$

Then $ad = -bc \implies a = -bc/d$. Also, $ac + 2bd = 0 \implies -bc^2 + 2bd^2 = 0 \implies c = \sqrt{2}d \implies c = d = 0$. So $(c + d\sqrt{2}) = 0$. If we substituted for d, we would get $(a + b\sqrt{2}) = 0$. Thus, it is an integral domain.

■

(b) **Find all the units.**
We are looking for solutions to $a^2 + 2b^2 = 1$. It is evident that ± 1 are valid units. Suppose, for contradiction, there are other units, then $b \neq 0 \implies b^2 \geq 1 \implies a^2 = 1 - 2b^2 \leq 1 - 2 = -1$. Then $a^2 \in \mathbb{C} \implies a \notin \mathbb{Z}$. So the only units are ± 1.

(c) **Determine the field of fractions**.
The field of fractions is given by $\mathbb{Q}[\sqrt{2}]$.

(d) **Prove that $\mathbb{Z}[\sqrt{2}i]$ is an Euclidean domain under the Euclidean valuation $v(a + b\sqrt{2}i) = a^2 + 2b^2$.**

Proof:

- $v(a) \leq v(ab)$
  Choose two nonzero elements. Then $v(a + b\sqrt{2}i) = a^2 + 2b^2$. Also $v((a + b\sqrt{2}i)(c + d\sqrt{2}i)) = v(ac + 2bd + (ad + bc)\sqrt{2}) = (ac + 2bd)^2 + 2(ad + bc)^2$. After expanding, we have $a^2 + 2b^2 \leq a^2c^2 + 2b^2c^2 + \ldots$. Thus, criteria one is met.

- Show there exists $q, r \in \mathbb{Z}[\sqrt{2}i]$ such that $a = bq + r$ and either $r = 0$ or $v(r) < v(b)$.
  Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$. Consider the division of x by y in the field of fractions $\mathbb{Q}[\sqrt{2}]$:

$$\frac{x}{y} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}}.$$

  This quotient can be written as $q + r$, where q is the closest approximation of $\frac{x}{y}$ in $\mathbb{Z}[\sqrt{2}]$, and $r = x - yq$. By construction, r satisfies the inequality $v(r) < v(y)$ or $r = 0$, since the Euclidean valuation v decreases when dividing x by y and rounding to the nearest element in $\mathbb{Z}[\sqrt{2}]$.

■

18.4/16 Show that $\mathbb{Z}[\sqrt{5}i]$ is not a unique factorization domain.

Proof: Consider $21 = 7 \cdot 3 = (4+\sqrt{5}i)(4-\sqrt{5}i)$. Suppose 3 is reducible. Then $3 = zw$ where $v(z) = v(w) = 3$. Since $a^2 + 5b^2 = 3, 7$ has no integer solutions, there is no such element with $v(z) = 3$. Thus, they are irreducible. A similar argument can be made for $(4 + \sqrt{5}i)$ and $(4 - \sqrt{5}i)$.

■

18.4/17 Prove or disprove: Every subdomain of a UFD is also a UFD.

Proof: Not true. We just showed above that $\mathbb{Z}[\sqrt{5}i]$ is not a UFD. It is clear that it is contained in $\mathbb{C}$, the field of the complex numbers.

■

16 FIELDS

16.1 Extensions Fields

16.2 Splitting Fields

16.3 Select Exercises

21.5/1 Show that each of the following are algebraic over $\mathbb{Q}$ by finding the minimal polynomial of the number over $\mathbb{Q}$.

(a) $\sqrt{1/3 + \sqrt{7}}$: Let $x = \sqrt{1/3 + \sqrt{7}} \implies (x^2 - 1/3)^2 = 7 \implies x^4 - 62/9 - 2x^2/3 = 0$.

(c) $\sqrt{3}+\sqrt{2}i$: let $x = \sqrt{3}+\sqrt{2}i \implies x^2 = 3-2+2\sqrt{6}i \implies (x^2-1)^2+24 = 0$.

21.5/2 Find a basis for each of the following field extensions. What is the degree of each extension?

(a) $\mathbb{Q}(\sqrt{3}, \sqrt{6})$ over $\mathbb{Q}$: Degree is 4. The basis for the former is given by $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

21.5/12 Prove or disprove: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})$

Proof: They are not isomorphic. Suppose for contradiction that there existed an isomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Then $\phi(\sqrt{2}) = a + b\sqrt{3} \implies \phi(2) = a^2 + 2ab\sqrt{3} + 3b^2$. But also $\phi(2) = 2\phi(1) = 2$, and $2 \neq a^2 + 2ab\sqrt{3} + 3b^2$, since $a, b \in \mathbb{Q}$ and $a^2 + 2ab\sqrt{3} + 3b^2 \notin \mathbb{Q}$.

■

21.5/13 Prove that the fields $\mathbb{Q}(\sqrt[4]{3}) \cong \mathbb{Q}(\sqrt[4]{3}i)$, but are not equal.

Proof: Define a map $\phi : \mathbb{Q}(\sqrt[4]{3}) \to \mathbb{Q}(\sqrt[4]{3}i)$ by $\phi(\sqrt[4]{3}) = \sqrt[4]{3}i$. So,

$$\phi(a + b(\sqrt[4]{3}) + c(\sqrt[4]{3})^2 + d(\sqrt[4]{3})^3) = a + b(\sqrt[4]{3}i) + c(\sqrt[4]{3}i)^2 + d(\sqrt[4]{3}i)^3$$

Due to being entirely linear, we can clearly see that ϕ preserves addition. Similarly, it preserves multiplication. So ϕ is a homomorphism. Since the coefficients do not change, we can see that $a \to a, b \to b, \ldots$, the map is 1-1 and onto. So, it is isomorphic.

However, since the image of ϕ also adjoins i, they are not equal.

■

21.5/15 Prove or disprove: $\mathbb{Z}[x]/ < x^3 - 2 >$ is a field.

Proof: If $< x^3 - 2 >$ is maximal, then the claim is proved. To show it is maximal, we must show that $x^3 - 2$ is irreducible. Suppose, for contradiction, that it is reducible. Then $x^3 - 2$ but have a linear factor of form $(x - \alpha)$, for some $\alpha \in \mathbb{Z}$. However, $x^3 = 2$ does not have any solutions in $\mathbb{Z}$, thus, there is no such linear factor. So, the polynomial is irreducible. The claim is proved.

■

21.5/16 Let F be a field with characteristic p. Prove that $p(x) = x^p - a$ either is irreducible over F or splits in E.

Proof: Let F be a field with characteristic $p > 0$. Consider the polynomial $p(x) = x^p - a$ over F. By Fermat's Little Theorem, for any $c \in F$, we have $c^p = c$. This implies that any root of $x^p - a$ in F satisfies $(c^p - c) = 0$, which is equivalent to $c^p = a$. Thus, c is a root of $p(x)$ if and only if $c^p = a$. If $p(x)$ has a root c in F, then $x^p - a = (x - c)^p$ in $F[x]$. This means $p(x)$ splits completely into linear factors. If $p(x)$ has no root in F, it must be irreducible over F, as it is of degree p. Therefore, the polynomial $p(x)$ is either irreducible over F or splits completely in F.

■

21.5/20 Show that the set of all elements in $\mathbb{R}$ that are algebraic over $\mathbb{Q}$ forms field extension of $\mathbb{Q}$ that is not finite.

Proof: Suppose, for contradiction, that the given field extension, denoted E, can be written as $E = F(\alpha_1, \ldots, \alpha_n), n \in \mathbb{N}$. Then let $[E : Q] = N$. N is a natural number because the $\mathbb{Q}$ is the product of the degree of n finite field extensions. Now, we know that there is no irreducible polynomial in Q of highest order, for we can construct one of arbitrary order using Eisenstein's criterion. Let $p(x)$ be an irreducible polynomial in Q of degree $N+1$, and let α be a root. Then $[Q(\alpha) : Q] = N+1$. Because the degree of $Q(\alpha)$ is greater than the degree of E, the dimension of $Q(\alpha)$ when viewed as a vector space over Q is greater than that of E, so $Q(\alpha) \notin E$. Therefore there exists an element of $Q(\alpha)$ that is not in E, and because both of those sets contain $\mathbb{Q}$, this element is irrational. Therefore there is an algebraic real that is not in E, and the contradiction is reached.

■

21.5/22 Show that $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{7})$. Extend your proof to show that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, $a \neq b$ and neither a nor b is a perfect square.
Proof: Consider $\alpha = \sqrt{3} + \sqrt{7}$. Then:

$$\alpha^2 = (\sqrt{3} + \sqrt{7})^2 = 10 + 2\sqrt{21}.$$

Rearranging, we get:

$$\sqrt{21} = \frac{\alpha^2 - 10}{2}.$$

Since $\sqrt{21} \in \mathbb{Q}(\alpha)$, it follows that $\sqrt{3} = \frac{\alpha+\sqrt{21}}{2}$ and $\sqrt{7} = \frac{\alpha-\sqrt{21}}{2}$ are also in $\mathbb{Q}(\alpha)$. Thus:

$$\mathbb{Q}(\sqrt{3}, \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3} + \sqrt{7}).$$

Conversely, $\sqrt{3} + \sqrt{7} \in \mathbb{Q}(\sqrt{3}, \sqrt{7})$, so:

$$\mathbb{Q}(\sqrt{3} + \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{7}).$$

Therefore, $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{7})$.
The argument generalizes to $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$ for $a \neq b$, provided a, b are not perfect squares. A similar computation shows that $\sqrt{ab} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$, which suffices to establish the equality of fields.

■

17 FINITE FIELDS

17.1 Structure of a Finite Field

[47]

[47] Section 22.1 in the textbook

17.2 Select Exercises

[48]

22.4/5 Construct a finite field of order 27.
To construct such a finite field, we use the fact that any finite field has order p^n for some prime p and $n \in \mathbb{N}$. We need a field of order 27 which is 3^3. We can construct such a field as an extension field of degree over $\mathbb{Z}_3 = \{0, 1, 2\}$. We choose an irreducible polynomial over $\mathbb{Z}_3$: $f(x) = x^3 + 2x^2 + 1$, which has no roots in $\mathbb{Z}_3 (f(0) = 1, f(1) = 4 \equiv 1, f(2) = 17 \equiv 2)$.

Thus, the quotient ring $\mathbb{Z}_3[x]/(x^3 + 2x^2 + 1)$ is a field which has $3^3 = 27$ elements.

22.4/6 Prove or disprove: $\mathbb{Q}*$ is cyclic.
FALSE.
Proof: Suppose, for contradiction, that $\mathbb{Q}*$ is cyclic, then consider an element $p/q \in \mathbb{Q}*$ that is a generator. Take p, q to be relatively prime. So $< p/q >= \mathbb{Q}*$. Consider element $p/q + 1 = (p + q)/q \neq (p/q)^m \ \forall m \in \mathbb{Z}$.

■

22.4/7 Factor each of the following polynomials in $\mathbb{Z}_2[x]$.
(a) $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ in $\mathbb{Z}_2[x]$

(b) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)$

(c) $x^9 - 1 = (x + 1)(x^6 + x^3 + 1)(x^2 + x + 1)$

(d) $x^4 + x^3 + x^2 + x + 1$ is irreducible.

22.4/8 Prove or disprove: $\mathbb{Z}_2[x]/ < x^3 + x + 1 > \cong \mathbb{Z}_2[x] < x^3 + x^2 + 1 >$.
Proof: Since both polynomials are irreducible in $\mathbb{Z}_2[x]$ and have degree 3, both $\mathbb{Z}_2[x]/ < x^3 + x + 1 >$ and $\mathbb{Z}_2[x] < x^3 + x^2 + 1 >$ have order 8. They both contain polynomials of the form $\{a + bx + cx^2 \mid a, b, c \in \mathbb{Z}_2\}$, thus, they must be isomorphic.

■

22.4/12 Prove or disprove: There exists a finite field that is algebraically closed.
Not true. Suppose K is finite and write $K = \{\alpha_1, \ldots, \alpha_n\}$. Now take the polynomial $p(x) = (x - \alpha_1) \ldots (x - \alpha_n) + 1 \in K[x]$. Observe that there are no roots in K, thus, K is not algebraically closed.

22.4/16 Let E and F be subfields of a finite field K. If $E \cong F$, show that $E = F$.

[48] Section 22.4 in the textbook

Proof: Suppose $E \cong F$. Since E and F are finite fields, their orders must be powers of the same prime p. Let $|E| = p^m$ and $|F| = p^n$. If $E \cong F$, then $m = n$ because finite fields of different orders cannot be isomorphic. Thus, $|E| = |F|$, which implies that both contains roots of $x^m - x = 0$. Thus, $E = F$.

■