Math 403 Summary and Examples

Dr. Ebrahimian

Contents

If you see any typos, feel free to message me. No typos are too small to report!

Notations

- $\mathbb{N} = \{0, 1, 2, \ldots\}$, the set of natural numbers.
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$, the set of integers.
- $\mathbb{Z}^+ = \{1, 2, \ldots\}$, the set of positive integers.
- $\mathbb{Q}$, the set of rational numbers.

- $\mathbb{Q}^c$, the set of irrational numbers.
- $\mathbb{R}$, the set of real numbers.
- $\mathbb{C}$, the set of complex numbers.
- $\in$, belongs to.
- $\forall$, for all.
- $\exists$, there exists or for some.
- $\overline{z}$, the conjugate of the complex number z.
- $|z|$, the absolute value of z.
- $A \backslash B$, the difference of sets A and B.
- $|S|$, the size of a set S.
- e or e_G, the identity element of a group G.
- a^{-1}, the inverse of a group element a.
- $|a|$, the order of a group element a.
- $H \leq G$, H is a subgroup of G.
- $M_n(\mathbb{R})$, the set of all $n \times n$ matrices with real entries.
- $GL_n(\mathbb{R})$, the set of all $n \times n$ invertible matrices with real entries.
- $SL_n(\mathbb{R})$, the set of all $n \times n$ matrices with real entries and determinant 1.
- $n\mathbb{Z}$, the set of all multiples of n in $\mathbb{Z}$.
- $U(n)$, the multiplicative group of $\mathbb{Z}_n$.
- $Sym(X)$, the symmetric group on a set X.
- S_n, the symmetric group of degree n.
- A_n, the alternating group of degree n.

1 Week 1

1.1 Methods of Proof

Many mathematical statements are in the "if-then" form. To prove such statements we often use the method of direct proof or proof by contradiction. Suppose we want to prove " if p, then q".

Direct proof: We start by assuming p. Then by taking logical steps we obtain the desired conclusion q. Note that all steps must be justified by referring to a theorem, a definition, an axiom, or an assumption.

Example 1.1. The sum of every two even integers is even.

Solution. Suppose a, b are two even integers. Then, by definition of "even", there are integers m, n for which $a = 2n, b = 2m$. Therefore, $a + b = 2(n + m)$, which is even since $n + m$ is an integer. □

Proof by contradiction: We start by assuming p is true but q is false. By taking logical steps we obtain a contradiction, i.e. something that cannot be true. This means the initial assumption that q is false may not be true.

Example 1.2. There are infinitely many primes.

Solution. On the contrary assume $p_1 = 2, p_2 = 3, \ldots, p_n$ is the list of all primes. Note that the integer $p_1 p_2 \cdots p_n + 1$ is more than one and thus has a prime divisor. Since the list $p_1 = 2, p_2 = 3, \ldots, p_n$ consists of all primes, p_i must divide $p_1 \cdots p_n + 1$ for some i, however p_i divides $p_1 \cdots p_n$, which means p_i must divide their difference of 1, which is impossible. This contradiction proves the claim. □

Proof by mathematical induction: Suppose we want to prove the statement $P(n)$ that depends of a natural number n is true for all n. In this method we prove this statement as follows:
Basis step. $P(0)$ is true.
Inductive step. If $P(n)$ holds for some natural number n, then $P(n + 1)$ holds as well.

Example 1.3. Prove that for every positive integer n, we have $n < 2^n$.

Solution. Basis step. We see that $1 < 2^1$, which proves the basis step.
Inductive step. Suppose $n < 2^n$ for some positive integer n. We have $n + 1 < 2^n + 1$, by the inductive step. Since $1 < 2^n$ we have $n + 1 < 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$, as desired. □

Well-Ordering Principle states that any nonempty subset of $\mathbb{Z}^+$ has a smallest element. This can be proved using mathematical induction.

1.2 Elementary Number Theory

Definition 1.1. We say an integer a **divides** an integer b, denoted by $a \mid b$, if there is an integer c for which $b = ac$. In that case we say b is a **multiple** of a.

Theorem 1.1 (Quotient-Remainder Theorem)**.** *Let a, b be two integers and $b \neq 0$. Then, there are unique integers q, r satisfying both of the following:*

- *$a = bq + r$, and*
- *$0 \leq r < |b|$.*

Definition 1.2. Given two integers a and b, not both zero, the **greatest common divisor of a and b** is the largest integer d dividing both a and b. This integer is denoted by $\gcd(a, b)$. We also define $\gcd(0, 0) = 0$. When $\gcd(a, b) = 1$ we say a and b are **relatively prime** or **co-prime**.

Definition 1.3. Let a and b be two integers. When both a and b are non-zero, the **least common multiple of a and b** is the smallest positive integer m that is divisible by both a and b. This integer is denoted by $\operatorname{lcm}(a, b)$. We also define $\operatorname{lcm}(a, 0) = \operatorname{lcm}(0, a) = a$ for every integer a. The greatest common divisor and the least common multiple of any number of integers is defined similarly.

Theorem 1.2 (Bezout's Lemma)**.** *Suppose a and b are two integers. Then, there are integers x and y for which $\gcd(a, b) = ax + by$.*

Corollary 1.1. Two integers a and b are relatively prime if and only if there are integers x, y for which $ax + by = 1$.

Theorem 1.3. *Suppose a, b, c are integers for which $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Definition 1.4. An integer p more than 1 is called a **prime** if its only divisors are 1 and p.

Theorem 1.4 (Euclid's Lemma)**.** *If p is a prime number, a, b are two integers for which $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Theorem 1.5 (Fundamental Theorem of Arithmetic)**.** *Any integer more than 1 can uniquely be written as a product of primes. In other words, if n is an integer more than 1, then there are primes $p_1 < \cdots < p_k$ and positive integers $a_1, \ldots, a_k$ for which $n = p_1^{a_1} \cdots p_k^{a_k}$. Furthermore if $p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_\ell^{b_\ell}$, where $q_1 < \cdots < q_\ell$ are primes and $b_1, \ldots, b_\ell$ are positive integers, then $k = \ell$, $p_i = q_i$, and $a_i = b_i$ for all i.*

Theorem 1.6. *Given two positive integers a and b with prime factorizations $a = p_1^{a_1} \cdots p_k^{a_k}$ and $b = p_1^{b_1} \cdots p_k^{b_k}$, where $p_1, \ldots, p_k$ are distinct primes and a_i, b_i's are non-negative integers, we have the following:*

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdots p_k^{\min(a_k, b_k)}, \text{ and } \operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_k^{\max(a_k, b_k)}.$$

Similar results hold for the greatest common divisor and least common multiple of several positive integers.

Definition 1.5. Given two integers a, b and a positive integer n we say "a is congruent to b modulo n", written as $a \equiv b \mod n$, if $n \mid (a - b)$.

Example 1.4. Let n be a positive integer. Every integer is congruent to one of $0, 1, \ldots, n-1$ modulo n.

Theorem 1.7 (Properties of Congruences)**.** *Suppose a, b, c, d are integers, and m, n are positive integers.*

(a) If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$, $ac \equiv bd \mod n$, and $a^m \equiv b^m \mod n$.

(b) If $a \equiv b \mod n$, then $ac \equiv bc \mod n$ and $a + c \equiv b + c \mod n$.

(c) If $ac \equiv bc \mod n$ and $\gcd(c, n) = 1$, then $a \equiv b \mod n$.

Example 1.5. Prove that the sum of every three consecutive perfect cubes is always divisible by 9.

1.3 Complex Numbers

Definition 1.6. The set of **complex numbers** $\mathbb{C}$ is defined as

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\},$$

where i is a solution of the equation $i^2 = -1$. Addition and multiplication on $\mathbb{C}$ are defined naturally taking into consideration that $i^2 = -1$. The real numbers a and b are called **real** and **imaginary** parts of the complex number $z = a + bi$. The **complex conjugate** of $z = a + bi$, denoted by $\overline{z}$, is given by $a - bi$. The **absolute value** (or **norm**) of z is given as $|z| = \sqrt{a^2 + b^2}$.

Theorem 1.8 (Properties of complex conjugate and norm)**.** *For every two complex numbers z and w, we have*

- $\overline{zw} = \overline{z}\,\overline{w}$.
- $|z|^2 = z\,\overline{z}$.
- $|wz| = |z|\,|w|$.

Each complex number $z = a + bi$ can be plotted on a plane called the complex plane. The horizontal component of point corresponding to z is the real part a and the vertical component is the imaginary part b. If θ is the angle between $0z$ and the positive real axis, then $z = |z|(\cos\theta + i\sin\theta)$.

Writing the Taylor series we can see that for every real number θ we have $e^{i\theta} = \cos\theta + i\sin\theta$. Therefore, we can write $z = |z|e^{i\theta}$. Some of the usual properties of exponent such as $e^{i\theta}e^{i\alpha} = e^{i(\theta+\alpha)}$ hold. The one below is particularly important.

Theorem 1.9 (De Moivre's Formula)**.** *For every real number θ and every integer n we have $(e^{i\theta})^n = e^{in\theta}$.*

1.4 Sets and Relations

Definition 1.7. A set A is a **subset** of a set B if every element of A is an element of B.

Definition 1.8. A **partition** of a non-empty set A is a collection $\{A_i\}_{i\in I}$ of non-empty subsets of A for which they are pairwise disjoint and their union is A. In other words, both of the following holds:

- $A_i \neq \emptyset$ for every $i \in I$, and
- $A_i \cap A_j = \emptyset$ for all distinct $i, j \in I$, and
- $\bigcup\limits_{i\in I} A_i = A$.

Example 1.6. $\mathbb{Q}$, and $\mathbb{Q}^c$ partition $\mathbb{R}$.

Definition 1.9. A **relation** on a set A is a subset R of the Cartesian product $A \times A$. Instead of $(x, y) \in R$ we often write xRy.

Definition 1.10. A relation R on a set A is called an **equivalence relation** if it satisfies the following properties:

- (Reflexive property) xRx, for all $x \in A$.
- (Symmetric property) For all $x, y \in A$, if xRy, then yRx.
- (Transitive property) For all $x, y, z \in A$, if xRy and yRz, then xRz.

Example 1.7. Prove that "equality" is an equivalence relation on $\mathbb{R}$.

Example 1.8. Prove that "inclusion" is not an equivalence relation on the set consisting of all subsets of the set $\mathbb{R}$.

Solution. This relation is not symmetric, since $\{1\} \subseteq \{1, 2\}$, but $\{1, 2\} \not\subseteq \{1\}$. □

Definition 1.11. Suppose $\sim$ is an equivalence relation on a set A. For every $a \in A$, the **equivalence class of** a, denoted by $[a]$, is defined by $[a] = \{x \in A \mid a \sim x\}$.

Theorem 1.10. *Let $\sim$ be an equivalence relation on a non-empty set A. Then, the collection of equivalence classes of $\sim$ partition A. In other words, every two equivalence classes are either disjoint or equal.*

Example 1.9. Let n be a positive integer. Prove that "$\equiv \mod n$" is an equivalence relation on $\mathbb{Z}$, and identify its equivalence classes.

1.5 Formal Definition of Groups

We will first look at some examples of structures that appear in different parts of mathematics and then we will unify them with a formal definition.

Example 1.10. Consider the set of integers $\mathbb{Z}$ along with addition. We know this operation satisfies the following properties for all $a, b, c \in \mathbb{Z}$:

- $(a+b)+c = a+(b+c)$.
- $a+0 = 0+a = a$.
- $a+(-a) = (-a)+a = 0$.
- $a+b = b+a$.

Example 1.11. Consider all symmetries of a square. We see there are four rotations, and four reflections that are symmetries of this square. We also have an "operation" called composition between each two symmetries. This operation turns every two symmetries into another symmetry. Let D_4 be the set of these eight symmetries. We see that for every $\sigma, \tau, \delta \in D_4$ we have the following:

- $\sigma \circ \tau$ is also a symmetry.
- $(\sigma \circ \tau) \circ \delta = \sigma \circ (\tau \circ \delta)$.
- $\sigma \circ id = id \circ \sigma = \sigma$.
- The inverse of any symmetry is also a symmetry.
- It is not always the case that $\sigma \circ \tau = \tau \circ \sigma$.

Example 1.12. Consider the set of all permutations (i.e. bijections) of $\{1, \ldots, n\}$. Composing every two permutations yields another permutation. These permutations can also be thought as "symmetries" of the set $\{1, \ldots, n\}$, which is to say they preserve the structure of the set, i.e. any two distinct elements are mapped to distinct integers. The permutations along with the composition operation also satisfy the same properties as the ones in the previous example.

Definition 1.12. Let G be a set. A **binary operation** on G is a function that assigns an element of G to each ordered pair of elements of G.

Example 1.13. The following are examples of binary operations:

(a) $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ that assigns to every pair (a, b) the integer $a + b$. Note that $+(a, b)$ is denoted by $a + b$.

(b) $\times : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ that assigns to every pair (a, b) the integer ab. Note that $\times(a, b)$ is denoted by $a \times b$ or ab.

Remark. The fact that for a binary operation the image of every pair of elements is in the set is often stated as "the set is **closed** under the binary operation".

Example 1.14. The following examples are *not* binary operations:

(a) The function $f(a, b) = \dfrac{1}{a-b}$ from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$ is not a binary operation, because $f(a, a)$ is not a real number.

(b) The subtraction function defined by $f(a,b) = a - b$ over $\mathbb{N}$ is not a binary operation. For example $1 - 2$ is not a natural number.

Remark. We often denote the element of G associated to the pair $(a,b) \in G \times G$ under a binary operation by $a \circ b$, $a \star b$, or ab.

Definition 1.13. Let G be a non-empty set together with a binary operation $\circ$. We say G is a **group** if it satisfies the following properties:

(a) (Associativity) For all $a, b, c \in G$ we have $(a \circ b) \circ c = a \circ (b \circ c)$,

(b) (Identity) There exists $e \in G$ for which for every $a \in G$ we have $a \circ e = e \circ a = a$.

(c) (Inverse) For every $a \in G$, there is $b \in G$ for which $a \circ b = b \circ a = e$.

If there is an ambiguity about the binary operation we write $(G, \circ)$ is a group. A group is called **Abelian** if in addition to the above properties we have $a \circ b = b \circ a$ for all $a, b \in G$.

Example 1.15. Prove that the set $\mathbb{Z}$ along with addition is a group.

Solution. We will check all the properties:
Non-empty. $0 \in \mathbb{Z}$ and thus it is non-empty.
Closed. For every $a, b \in \mathbb{Z}$ we have $a + b \in \mathbb{Z}$.
Associativity. For every $a, b, c \in \mathbb{Z}$ we have $(a + b) + c = a + (b + c)$.
Identity. For every integer a we have $a + 0 = 0 + a = a$.
Inverse. For every $a \in \mathbb{Z}$ we have $a + (-a) = (-a) + a = 0$.
All of these properties follow from the properties of integers and thus $\mathbb{Z}$ along with integer addition is a group. □

Example 1.16. These are all examples of Abelian groups: $(\mathbb{R}, +), (\mathbb{Q}, +), (M_n(\mathbb{R}), +), (\mathbb{Z}_n, +), (U(n), \cdot)$. The following are examples of non-Abelian groups: $(GL_n(\mathbb{R}), \cdot), (S_n, \circ), (D_n, \circ)$.

1.6 Warm-ups

Example 1.17. Prove that for every positive integer n we have $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Solution. We will prove this by induction.
Basis step. For $n = 1$, the two sides are 1 and $\dfrac{1(1+1)}{2} = 1$, hence they are equal.
Inductive step. Suppose $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$, for some n. Adding $n + 1$ to both sides we obtain:

$$1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2} + 1\right) = \frac{(n+1)(n+2)}{2}, \text{as desired.}$$

This completes the proof by induction. □

Example 1.18. Find three integers that are 7 modulo 13.

Solution. We would need to add multiples of 13 to 7. So, anything of the form $7 + 13k$ is one such integer. Some examples are $7, -6, -19$, and 20. □

Example 1.19. Using the Quotient-Remainder theorem prove that every integer is either odd or even but not both.

Solution. Let a be an integer. By the Quotient-Remainder Theorem with $b = 2$, there exist integers q and r for which $a = 2q + r$ and $0 \leq r < 2$. Therefore, $a = 2q$ or $a = 2q + 1$. This proves that every integer is either even or odd.

Now assume an integer a is both even and odd. Thus, $a = 2k = 2\ell + 1$ for integers k, ℓ. This violates the uniqueness in the Quotient-Remainder Theorem. □

Example 1.20. Let $z = 2 + i, w = 1 - 3i$. Write down the complex numbers $z + w, z - w, zw$, and z/w in standard form.

Solution. $z+w = 3-2i$, $z-w = 1+4i$, $zw = 2+i-6i-3i^2 = 5-5i$. $z/w = z\overline{w}/|w|^2 = (2+i+6i+3i^2)/(1+9) = -0.1 + 0.7i$. □

1.7 More Examples

Example 1.21. Evaluate $(1 + i)^{1000}$

Solution. Since we are finding large exponents of a complex number, De Moiver's formula would be helpful. So, we write $1 + i = \sqrt{2}e^{i\pi/4}$. Therefore, $(1 + i)^{1000} = 2^{500}e^{i250\pi} = 2^{500}$. □

Example 1.22. Let $C(\mathbb{R})$ be the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$. Define a relation $\sim$ on $C(\mathbb{R})$, by $f \sim g$ if and only if $f - g$ is a constant function. Prove that $\sim$ is an equivalence relation and identify its equivalence classes.

Example 1.23. Prove that for every two positive integers a, b we have $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Solution. In order to show the two sides of the equality are the same we need to show the exponent of every prime in their prime factorizations is the same. Let p be a prime and let k and ℓ be the exponents of p in the prime factorizations of a and b, respectively. We know the exponent of p in the prime factorizations of $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are $\min(k, \ell)$ and $\max(k, \ell)$, repectively. Therefore, the power of p in the prime factorization of $\gcd(a, b) \cdot \operatorname{lcm}(a, b)$ is $\min(k, \ell) + \max(k, \ell) = k + \ell$, which is the exponent of p in the prime factorization of ab. Therefore, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$. □

Example 1.24. Given a group G and an element $g \in G$, prove that the function $f : G \to G$ defined by $f(x) = gx$ is a bijection.

Solution. Suppose $f(x) = f(y)$, for some $x, y \in G$. By definition of f we have $gx = gy$. Suppose h is an inverse of g. Multiplying both sides from the left by h yields $h(gx) = h(gy)$, which by associativity is equivalent to $(hg)x = (hg)y$. By inverse and identity properties we get $ex = ey$ and $x = y$. Therefore, f is one-to-one.

Let h be an inverse of g. For every $x \in G$, we have $f(hx) = g(hx) = (gh)x = ex = x$, by associativity, inverse, and identity. Therefore, f is onto.

Therefore, f is a bijection. □

Example 1.25. Let S be a finite set of size n, with n a positive integer.

(a) Prove that there are n^{n^2} binary operations on S.

(b) Prove that there are $n^{\frac{n^2+n}{2}}$ commutative binary operations on S.

(c) Prove that there are n^{n^2-2n+2} binary operations on S that have an identity element?

(d) Prove that there are $n^{\frac{n^2-n+2}{2}}$ commutative binary operations on S that have an identity element?

(e) For $n = 2$ find the number of associative binary operations on S. The number of associative binary operations for every n is much more difficult to find.

Example 1.26. True or false? If false, make an adjustment to get a true statement.

If for integers a, b, c we have $a \mid bc$, then either $a \mid b$ or $a \mid c$.

1.8 Exercises

All students are expected to do all of the exercises listed in the following two sections.

1.8.1 Problems for Grading

The following problems must be submitted by Friday 2/5/2021 before the class starts. The submission will be on Gradescope via Elms. **Late submission will not be accepted.**

Instructions for submission: To submit your solutions please note the following:

- Each problem must go on a separate page.
- It is highly recommended (but not required) that you LaTeX your homework.
- If you are not typing your work (which is fine) please make sure your work is legible.
- To submit your homework go to Elms. Hit "Gradescope" on the left panel. That should allow you to upload a PDF file of your homework.

- You could use the (free) DocScan app to scan and upload your homework.
- Sometime in the next few days run a test and make sure this all works out so you do not face any issues right before the deadline.
- Homework must be submitted before the class starts on the due date. GradeScope will not allow late submissions.
- You can read more about submitting homework on Gradescope here.
- All proofs must be complete and solutions must be fully justified.
- Read and follow the directions carefully.
- Numbered problems are from the textbook

Exercise 1.1 (10 pts)**.** *Prove that for any three positive integers a, b, c we have* $\gcd(ab, bc, ca) \cdot \operatorname{lcm}(a, b, c) = abc$*.*

Hint: See Example 1.23.

Exercise 1.2 (10 pts)**.** *Define a relation $\sim$ on $\mathbb{R}^2$ by*

$$(x_1, y_1) \sim (x_2, y_2) \text{ iff } x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Prove that $\sim$ is an equivalence relation and geometrically describe its equivalence classes.

Exercise 1.3 (10 pts)**.** *Problem 28, page 25.*

Exercise 1.4 (10 pts)**.** *Problem 34, page 25.*

Definition 1.14. A **symmetry** of a subset $\mathcal{D}$ of $\mathbb{R}^2$ is a bijection from $\mathcal{D}$ to $\mathcal{D}$ that preserves distance. In other words $f : \mathcal{D} \to \mathcal{D}$ is a symmetry, if f is bijective and that for every two $\mathbf{x}, \mathbf{y} \in \mathcal{D}$ we have $|\mathbf{x} - \mathbf{y}| = |f(\mathbf{x}) - f(\mathbf{y})|$.

Exercise 1.5 (10 pts)**.** *Let $A_1 A_2 \cdots A_n$ be a regular n-gon. Prove that it has precisely $2n$ symmetries.*

Hint: First note that there are n reflections and n rotations. Next, note that every vertex must be mapped to another vertex. (You don't need to prove these two facts.) Using the fact that A_1, A_2 must be mapped to two adjacent vertices prove that there are at most $2n$ symmetries.

Exercise 1.6 (10 pts)**.** *Problem 22, page 39.*

Exercise 1.7 (20 pts)**.** *Let $\mathcal{D}$ be a region in $\mathbb{R}^2$. Prove that the set of symmetries of $\mathcal{D}$ along with composition is a group.*

1.8.2 Practice Problems

Exercise 1.8. *Let a and b be two positive integers. Prove that both a and b are perfect squares if and only if both* $\gcd(a, b)$ *and* $\operatorname{lcm}(a, b)$ *are perfect squares.*

Exercise 1.9. *Let $n > 2$ be a positive integer. Find the necessary and sufficient condition for positive integers $a_1, a_2, \ldots, a_n$ for which*

$$\gcd(a_1, a_2, \ldots, a_n) \cdot \operatorname{lcm}(a_1, a_2, \ldots, a_n) = a_1 a_2 \cdots a_n.$$

p.24-27: 15, 16, 38, 60, 65.
p. 37: 5, 7.

Exercise 1.10. *Prove that for every n integers $a_1, \ldots, a_n$, there are integers $b_1, \ldots, b_n$ for which*

$$a_1 b_1 + \cdots + a_n b_n = \gcd(a_1, \ldots, a_n).$$

1.8.3 Challenge Problems

Exercise 1.11. *For every four positive integers m, n, r, and s, denote the following statement by $P(m, n, r, s)$:*

$$\forall a, b \in \mathbb{N}, a^m \mid b^n \Rightarrow a^r \mid b^s$$

Prove that $P(m, n, r, s)$ is true if and only if $nr \leq ms$.

1.9 Summary

- Let p be a prime and $k_1, \ldots, k_n$ be the exponents of p in the prime factorizations of positive integers $a_1, \ldots, a_n$, respectively. Then, the exponents of p in the prime factorizations of $\gcd(a_1, \ldots, a_n)$ and $\operatorname{lcm}(a_1, \ldots, a_n)$ are $\min(k_1, \ldots, k_n)$ and $\max(k_1, \ldots, k_n)$, respectively.

- If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

- $\gcd(a, b) = ax + by$ for some integers x, y.

- Given two sets A and B, to prove $A \subseteq B$, we need to prove " if $x \in A$, then $x \in B$." To prove $A = B$, we need to show $A \subseteq B$ and $B \subseteq A$.

- To prove a function $f : A \to B$ is one-to-one we start from $f(x) = f(y)$ and prove $x = y$, for every $x, y \in A$.

- To prove a function $f : A \to B$ is onto, we start from $b \in B$ and prove there is an element $a \in A$ for which $f(a) = b$.

- To prove a set along with an operation is a group you must prove it satisfies five properties: non-empty, closed, associative, identity, and inverse.

2 Week 2

The following table lists some of the most common groups that we often use.

Set	Operation	Identity	Elements	Inverse	Abelian?
$\mathbb{Z}$	Addition	0	n	$-n$	Yes
$\mathbb{Q}$	Addition	0	n/m	$-n/m$	Yes
$\mathbb{R}$	Addition	0	x	$-x$	Yes
$\mathbb{Q}^+$	Multiplication	1	m/n	n/m	Yes
$\mathbb{R}^+$	Multiplication	1	x	$1/x$	Yes
$\mathbb{R}^*$ or $\mathbb{C}^*$	Multiplication	1	x	$1/x$	Yes
$\mathbb{Z}_n$	Addition mod n	0	$k \mod n$	$-k \mod n$	Yes
$GL_n(\mathbb{R})$ or $GL_n(\mathbb{C})$	Matrix multiplication	The identity matrix I	$n \times n$ matrix A with $\det A \neq 0$	A^{-1}	No
D_n	Composition	R_0	$R_{\frac{2\pi k}{n}}$, and Reflections L	$R_{-\frac{2\pi k}{n}}$, L	No
$U(n)$	Multiplication mod n	1	$k \mod n$ with $\gcd(k, n) = 1$	solution to $kx \equiv 1 \mod n$	Yes
$M_n(\mathbb{R})$ or $M_n(\mathbb{C})$	Matrix Addition	The zero matrix	$n \times n$ matrix A	$-A$	Yes
$\mathbb{R}^n$ or $\mathbb{C}^n$	Vector Addition	The zero vector	$(x_1, \dots, x_n)$	$(-x_1, \dots, -x_n)$	Yes
S_n	Composition	The identity function ϵ	Permutations of $\{1, \dots, n\}$	Inverse function	No

Table of some common groups.

2.1 Properties of Groups

Theorem 2.1. *In every group G the following statements are true.*

(a) The identity element is unique.

(b) Every element has a unique inverse.

(c) The inverse of inverse of every element of G is itself.

Notation. The identity of a group G is denoted by e_G or e. The inverse of an element a is denoted by a^{-1}.

Theorem 2.2 (Shoes-Socks Property)**.** *For every two elements a, b of a group G, we have $(ab)^{-1} = b^{-1}a^{-1}$.*

Theorem 2.3 (Left and Right Cancellation Properties)**.** *Let a, b, c be group elements. Then,* *(a) (Right Cancellation Property) If $ba = ca$, then $b = c$.*

(b) (Left Cancellation Property) If $ab = ac$, then $b = c$.

Definition 2.1. Let a be an element of a group G. Given an integer n, we define a^n recursively as follows:

- $a^0 = e$.
- $a^{n+1} = aa^n$, for all $n \geq 0$.
- If $n < 0$, then let $a^n = (a^{-n})^{-1}$. In other words, a^n is the inverse of a^{-n}

Clearly, the above definition gives us $a^1 = aa^0 = ae = a$, which means $a^1 = a$, as expected. Also note that by the above definition a^{-1} is the inverse of a^1, which means a^{-1} is the same as the inverse of a, which matches the notation that we used for the inverse of an element a.

Theorem 2.4. *Let a be a group element and $m, n \in \mathbb{Z}$. Then*

(a) $a^n a^m = a^{n+m}$.

(b) $(a^n)^m = a^{nm}$.

Proof. (a) Since the definition relies on the sign of the exponents we need to take several cases.
Case I. $n = 0$.

$$\begin{aligned} a^n a^m &= ea^m && \text{By definition of } a^0. \\ &= a^m && \text{By the identity property.} \\ &= a^{n+m} && \text{Since } n+m = m. \end{aligned}$$

Case II. $m = 0$. This is similar to the first case except that we need to use $a^n e = a^n$.

Case III. $n, m > 0$. We will prove this by induction on n.
Basis Step: If $n = 1$, then by definition of exponents $a^n a^m = aa^m = a^{m+1}$, as desired.
Inductive Step: Suppose $a^n a^m = a^{n+m}$ for some $n > 0$ and for all $m > 0$. Then, we have

$$\begin{aligned} a^{n+1} a^m &= (aa^n)a^m && \text{By definition of } a^k. \\ &= a(a^n a^m) && \text{By associativity.} \\ &= aa^{n+m} && \text{By inductive hypothesis.} \\ &= a^{1+n+m} && \text{By definition of } a^k. \\ &= a^{(n+1)+m} && \text{Since } 1+n = n+1. \end{aligned}$$

This completes the proof for this case.

Case IV. $n, m < 0$.
By Case III we know $a^{-m}a^{-n} = a^{-m-n}$. Evaluating the inverse of both sides and using shoes-socks property we obtain $(a^{-n})^{-1}(a^{-m})^{-1} = (a^{-m-n})^{-1}$. By definition of a^k we have $a^n a^m = a^{n+m}$, as desired.
Case V. $n > 0$ and $m < 0$. We need to prove $a^n(a^{-m})^{-1} = a^{n+m}$. By the Cancellation property from

the right it is enough to prove $a^n(a^{-m})^{-1}a^{-m} = a^{n+m}a^{-m}$. This is equivalent to $a^n = a^{n+m}a^{-m}$. This follows from Cases I and III if $n+m$ is zero or positive. If $n+m$ is negative then we can re-write it as $a^n = (a^{-n-m})^{-1}a^{-m}$. Again using the cancellation property from the left it is enough to prove $a^{-n-m}a^n = a^{-m}$, which follows from Case III.

Case VI. $n < 0$ and $m > 0$. This case is similar to Case V. (b) Exercise. □

Example 2.1. Evaluate $2^{2021} \mod 15$.

Solution. We notice that $2^4 \equiv 1 \mod 15$. Therefore, powers of 2 cycle through 1, 2, 4, 8 and back to 1. This can be used to find the answer as follows:

$$2^{2021} \equiv (2^4)^{505} \cdot 2 \equiv 1^{505} \cdot 2 = 2 \mod 15$$

□

The above example motivates the following definition:

Definition 2.2. Given a group element a, the **order** of a is the smallest positive integer n for which $a^n = e$, in which case we write $|a| = n$. If no such n exists, we say a has infinite order and we write $|a| = \infty$.

Example 2.2. Here are a few examples of order:

(a) The order of 2 in $U(15)$ is 4.

(b) The order of 2 in $\mathbb{Z}_{15}$ is 15.

(c) 1 has infinite order in $\mathbb{Z}$.

2.2 Subgroups

Example 2.3. Consider the group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Show that $\{0, 2\}$ itself is a group with the same addition of $\mathbb{Z}_4$.

Definition 2.3. A subset H of a group G is said to be a **subgroup** if H along with the operation of G is a group. This is denoted by $H \leq G$.

Example 2.4. The following are examples of subgroups.

(a) $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$.

(b) $\mathbb{Q}$ is a subgroup of $\mathbb{R}$.

(c) $\mathbb{R}^*$ is a subgroup of $\mathbb{C}^*$.

(d) $\mathbb{R}^n$ is a subgroup of $\mathbb{C}^n$.

(e) $M_n(\mathbb{R})$ is a subgroup of $M_n(\mathbb{C})$

Example 2.5. The following are not examples of subgroups.

(a) $\mathbb{R}^*$ is not a subgroup of $\mathbb{R}$.

(b) $M_2(\mathbb{R})$ is not a subgroup of $M_4(\mathbb{R})$.

(c) $U(n)$ is not a subgroup of $\mathbb{Z}_n$.

(d) $\mathbb{Z}_n$ is not a subgroup of $\mathbb{Z}$.

(e) $GL_n(\mathbb{R})$ is not a subgroup of $M_n(\mathbb{R})$.

Theorem 2.5 (Compatibility Theorem)**.** *Let H be a subgroup of a group G. Then*

(a) $e_G = e_H$.

(b) If $a \in H$, then the inverse of a in H is the same as the inverse of a in G.

At first, it might seem that part (a) follows from the uniqueness of the identity element but that is not the case, because we don't know if e_G is even an element of H, or e_H is an identity of G. we have to find a different approach. Similar for part (b).

Proof. (a)

$$\begin{aligned} e_G e_H &= e_H && \text{(Since } e_G \text{ is the identity of } G.) \\ &= e_H e_H && \text{(Since } e_H \text{ is the identity of } H.) \end{aligned}$$

Applying the cancellation property of G to the equality $e_G e_H = e_H e_H$ we obtain $e_G = e_H$.
(b) Suppose $a \in H$, and b, c are the inverses of a in G and H, respectively, and let e be the identity of G (and H). By assumption $ab = e = ac$. Applying the cancellation property in G we obtain $b = c$. □

Question. Given a group G, how do we check if H is a subgroup of G? Is there any shortcut or do we need to go through all of the properties listed in Definition 1.13?

Theorem 2.6 (Two-step Subgroup Test)**.** *Let G be a group. A non-empty subset H of G is a subgroup of G if and only if H is closed under the binary operation of G and its inverse. In other words if the following hold:*

(a) For all $a, b \in H$ we have $ab \in H$.

(b) For all $a \in H$ we have $a^{-1} \in H$.

Theorem 2.7 (One-step Subgroup Test)**.** *Let G be a group. A non-empty subset H of G is a subgroup of G if and only if for all $a, b \in H$ we have $ab^{-1} \in H$.*

Example 2.6. Prove that $SL_n(\mathbb{R})$ defined as the set of all matrices in $GL_n(\mathbb{R})$ with determinant 1 is a subgroup of $GL_n(\mathbb{R})$.

Theorem 2.8 (Finite Subgroup Test)**.** *Suppose H is a non-empty, finite subset of a group. Then, H is a subgroup if and only if H is closed under the group operation.*

2.3 Important Subgroups

Theorem 2.9. *Suppose a is an element of a group G. Then, the set $\{a^n \mid n \in \mathbb{Z}\}$ is the smallest subgroup of G containing a.*

Definition 2.4. For every group element a, the subgroup **generated** by a is defined and denoted as follows:

$$\langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, \ldots\}.$$

Definition 2.5. The **centralizer** of an element a of a group G is defined and denoted by

$$C_G(a) = \{g \in G \mid ag = ga\}.$$

Similarly when S is a subset of G, then its **centralizer** is defined and denoted by

$$C_G(S) = \{g \in G \mid sg = gs \text{ for all } s \in S\}.$$

When the underlying group G is clear from the context, we often use $C(a)$ and $C(S)$ instead of $C_G(a)$ and $C_G(S)$. The **center** of a group G is defined and denoted below

$$Z(G) = \{a \in G \mid ag = ga \text{ for all } g \in G\}.$$

Theorem 2.10. *Let G be a group, S be a subset of G, and a be an element of G. Then $C(S), C(a)$ and $Z(G)$ are subgroups of G.*

Example 2.7. Suppose G is an Abelian group. Prove that the set of all elements of finite order in G is a subgroup of G. Is this true for non-Abelian groups?

2.4 Warm-ups

Example 2.8. Prove that in any group and for every integer n we have $e^n = e$.

Solution. We will prove this by taking cases.
Case I. $n \geq 0$. We will prove this by induction on n.
Basis step. $e^0 = e$, by definition.
Inductive step. Suppose $e^n = e$ for some non-negative integer n. We have $e^{n+1} = ee^n = ee = e$, by inductive hypothesis and the identity property.

Case II. $n < 0$. $e^n = (e^{-n})^{-1}$, by definition. By Case I, we have $e^{-n} = e$, and since $e^{-1} = e$ we are done. □

Example 2.9. Suppose G is a group and x is an element of G for which $xa = a$ (i.e. x is a left identity) for all $a \in G$. Prove that x is the identity of G.

Solution. We see that $xa = a = ea$. By the right cancellation property we have $x = e$. □

Example 2.10. In a group G assume $abc = e$. Prove that $cab = e$.

Solution. Multiplying by c^{-1} from the right and using the identity and inverse properties, we obtain $ab = c^{-1}$. Multiplying by c from the left and using the inverse and identity properties, we obtain $cab = e$. $\square$

2.5 More Examples

Example 2.11 (Important)**.** Let a, b be two elements of a group for which $ab = ba$, and let n be an integer. Prove that $(ab)^n = a^n b^n$.

Solution. First note that since $a \in C(b)$ by Theorems 2.9 and 2.10 we have $a^n \in C(b)$ and similarly $b^n \in C(a)$ for all integers n.

We will now take two cases.

Case I. For $n \geq 0$, we will prove the result by induction.
Basis step. For $n = 0$ we have $(ab)^0 = e$, $a^0 = b^0 = e$. Since $ee = e$ we are done.
Inductive step. Suppose $(ab)^n = a^n b^n$ for some non-negative integer n. By definition we have

$$\begin{array}{rcll} (ab)^{n+1} & = & (ab)(ab)^n & \text{Definition of } a^k. \\ & = & (ab)(a^n b^n) & \text{Inductive hypothesis.} \\ & = & aa^n bb^n & \text{Associativity and } ba^n = a^n b. \\ & = & a^{n+1} b^{n+1} & \text{Definition of } a^k. \end{array}$$

Case II. $n < 0$. By definition we have $(ba)^n = ((ba)^{-n})^{-1}$. By Case I, we know $(ba)^{-n} = b^{-n} a^{-n}$. By shoes-socks theorem we obtain $((ba)^{-n})^{-1} = (a^{-n})^{-1}(b^{-n})^{-1}$. By definition of a^k this is equal to $a^n b^n$. Since $ab = ba$ we obtain $(ab)^n = a^n b^n$, as desired. $\square$

Definition 2.6. An element a of $\mathbb{Z}_n$ is said to have a **multiplicative inverse** b if $ab \equiv 1 \mod n$.

Example 2.12. Prove that the only elements of $\mathbb{Z}_n$ that have a multiplicative inverse are those relatively prime to n. In other words, show that the congruence $kx \equiv 1 \mod n$ has a solution for x if and only if $\gcd(k, n) = 1$.

Solution. Suppose $\gcd(k, n) = 1$. By Bezout's Lemma, there are integers x, y for which $kx + ny = 1$. Taking both sides modulo n yields $kx \equiv 1 \mod n$, and thus k has a multiplicative inverse x modulo n.
Now, suppose $kx \equiv 1 \mod n$ for some integer x. Thus, $kx - 1$ is divisible by n, which implies $kx - 1 = ny$ for some integer y. Hence $kx + ny = 1$. Now, by Corollary 1.1 we conclude that $\gcd(k, n) = 1$, as desired. $\square$

Example 2.13. Prove that $U(n)$ along with multiplication modulo n is a group.

Solution. First, note that $1 \in U(n)$, and thus $U(n)$ is non-empty. Note also that if k and ℓ are relatively prime to n, then $k\ell$ and n are also relatively prime. Suppose on the contrary p is a prime dividing $k\ell$ and n. Since p is a prime, by Euclid's Theorem p divides k or ℓ, but since p divides n we obtain a contradiction. Thus, $U(n)$ is closed under multiplication modulo n. Associativity follows from the associativity of multiplication in $\mathbb{Z}$. The integer $1 \mod n$ is an identity element. By the previous example if $\gcd(k,n) = 1$, then there is an integer x for which $kx \equiv 1 \mod n$. Also note that $\gcd(x,n) = 1$ by the same example, and thus $x \in U(n)$. This shows $U(n)$ is a group. □

Example 2.14. Suppose in a group G, we have $(ab)^2 = a^2b^2$ for all $a, b \in G$. Prove that G is Abelian.

Solution. Re-writing $(ab)^2 = a^2b^2$, we get $abab = aabb$. By cancellation property from both sides we obtain $ba = ab$, which implies G is Abelian. □

Example 2.15. Define an operation $\circ$ on the set $\mathbb{R}\backslash\{1\}$ by $a \circ b = a + b - ab$. Prove that this produces an Abelian group.

Solution. We will show all the conditions of an Abelian group is satisfied by $G = \mathbb{R}\backslash\{1\}$.

First, note that the set is non-empty.

Closed. Suppose $a, b \in G$. Since $\mathbb{R}$ is closed under addition, multiplication and subtraction $a \circ b$ is also a real number. We need to show $a \circ b \neq 1$. Suppose on the contrary $a \circ b = 1$. Thus, $a + b - ab - 1 = 0$, which implies $(a-1)(1-b) = 0$, and hence $a = 1$ or $b = 1$, which is a contradiction, since $a, b \in G$.

Commutative. (We will check this first, so we do not have to check the identity and inverse properties for both sides.) $a \circ b = a + b - ab = b + a - ba = b \circ a$.

Identity. We need to find e for which $e + a - ea = a$ for all a. This holds if and only if $e(1-a) = 0$ which holds when $e = 0$. Thus 0 is an identity.

Inverse. For every a we need to find b for which $a + b - ab = 0$. This holds if and only if $b = a/(a-1)$. Note that since $a \neq 1$, b is a real number. Note also that $b = 1$ implies $a = a - 1$ or $0 = -1$, which is a contradiction. Thus, $a/(a-1)$ is an inverse of a.

This completes the proof. □

Example 2.16. Give an example of a nonempty set G along with an associative binary operation such that:

- (Right identity) There is $e \in G$ for which for all $a \in G$ we have $ae = a$, and
- (Left inverse) For every $a \in G$, there is $b \in G$ for which $ba = e$,

but G is not a group.

Solution. Consider the set $\mathbb{Z}$ along with the operation $\star$ given by $x \star y = x$. Note that $x \star (y \star z) = x \star y = x$, and $(x \star y) \star z = x \star z = x$. Thus, $\star$ is associative.

We see that 1 is a right identity, since $x \star 1 = x$ for all $x \in \mathbb{Z}$.

Note also that $1 \star x = 1$, which means 1 is a left inverse of x. However this set is not a group, as it doesn't satisfy the right cancellation property. (e.g. $1 \star 0 = 1 \star 1$ but $1 \neq 0$.) □

Example 2.17. Let $a_1, \ldots, a_n$ be group elements. Prove that $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

Solution. We will prove this by induction on n.
Basis step. For $n = 1$ the statement is $a_1^{-1} = a_1^{-1}$.
Inductive step. Suppose $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$. By Socks-shoes property we have $(a_1 \cdots a_n a_{n+1})^{-1} = a_{n+1}^{-1}(a_1 \cdots a_n)^{-1}$. By inductive hypothesis this is equal to $a_{n+1}^{-1} a_n^{-1} \cdots a_1^{-1}$. This completes the proof. □

Example 2.18. Find the order of each element in the given group.

(a) 1 in $\mathbb{R}$.

(b) 1 in $\mathbb{C}^*$.

(c) 3 is $U(8)$.

Solution. (a) We note that if we add 1 any positive number of times, we end up with a positive real numbers which is not zero. Thus, the order of 1 in $\mathbb{R}$ is infinity.
(b) We see $1^1 = 1$, and thus the order of 1 is 1.
(c) 3 is not equal to 1 mod 8, but $3^2 = 9$ is 1 mod 8. Thus, the order of 3 in $U(8)$ is 2. □

Example 2.19 (Important)**.** Prove that the intersection of every two subgroups of a group G is itself a subgroup.

Solution. We will use the one-step subgroup test.
Suppose H and K are subgroups of G. By the Compatibility Theorem, we know both $e \in H$ and $e \in K$, and thus $H \cap K$ is non-empty.
Let a, b be elements of $H \cap K$. By definition of intersection a, b are in both H and K. Since both H and K are groups, ab^{-1} is in both H and K. Thus, $ab^{-1} \in H \cap K$, which completes the proof by the one-step subgroup test. □

Example 2.20. Prove that each of the following is a group:

(a) $x \star y = \dfrac{xy}{2}$ over $\mathbb{R}^*$.

(b) $x \star y = x + y + 3$ over $\mathbb{Z}$.

(c) $x \star y = \dfrac{x+y}{1+xy}$ over $(-1, 1)$.

Example 2.21. Let S be a set and $\mathcal{P}(S)$ be the set consisting of all subsets of S. Define the binary operation Δ on $\mathcal{P}(S)$ by $X \Delta Y = (X \cup Y) \backslash (X \cap Y)$. ($X \Delta Y$ is called the symmetric difference of X and Y.) Prove that $(\mathcal{P}(S), \Delta)$ is an Abelian group.

Example 2.22. Let G be a finite Abelian group. Prove that the product of the squares of all elements of G is the identity element. What can be said about the product of all elements of G?

Example 2.23. Let n be a positive integer. Prove that the set of all upper triangular $n \times n$ matrices in $GL_n(\mathbb{R})$ with non-zero diagonal entries is a subgroup of $GL_n(\mathbb{R})$.

Example 2.24. Suppose H is a subgroups of a group G such that every element of H commutes with every element of $G \backslash H$. Prove that $H \subseteq Z(G)$.

2.6 Exercises

All students are expected to do all of the exercises listed in the following two sections.

2.6.1 Problems for Grading

The following problems must be submitted by Friday 2/12/2021 before the class starts. The submission will be on Gradescope via Elms. **Late submission will not be accepted.**

Instructions for submission: To submit your solutions please note the following:

- Each problem must go on a separate page.
- It is highly recommended (but not required) that you LaTeX your homework.
- If you are not typing your work (which is fine) please make sure your work is legible.
- To submit your homework go to Elms. Hit "Gradescope" on the left panel. That should allow you to upload a PDF file of your homework.
- You could use the (free) DocScan app to scan and upload your homework.
- Sometime in the next few days run a test and make sure this all works out so you do not face any issues right before the deadline.
- Homework must be submitted before the class starts on the due date. GradeScope will not allow late submissions.
- You can read more about submitting homework on Gradescope here.
- All proofs must be complete and solutions must be fully justified.
- Read and follow the directions carefully.
- Numbered problems are from the textbook

Exercise 2.1 (10 pts)**.** *Suppose G is an Abelian group and n is an integer. Prove that the set*

$$H = \{g^n \mid g \in G\}$$

is a subgroup of G.

Hint: Use Example 2.11.

Exercise 2.2 (10 pts). *Prove the second part of Theorem 2.4: For every two integers m, n and every group element a we have $(a^n)^m = a^{nm}$.*

Hint: You may need to take cases.

Exercise 2.3 (10 pts). *Let G be a non-empty set along with a binary operation that is associative. Suppose the following hold.*

- *(Left identity) There is an element $e \in G$ for which $ea = a$, and*
- *(Left inverse) For every $a \in G$ there is $b \in G$ for which $ba = e$.*

Prove that G is a group.

Hint: Prove that $(ab)^2 = ab$. Then use the left inverse of ab. Then, use $ae = aba$.

Exercise 2.4 (10 pts). *Let H_i with $i \in I$ be a collection of subgroups of a group G. Prove that $\bigcap\limits_{i \in I} H_i$ is a subgroup of G.*

Hint: See Example 2.19

Exercise 2.5 (10 pts). *Problem 11, Page 55.*

Exercise 2.6 (10 pts). *Problem 27, Page 56.*

Hint: Use the definition of a^n as given in class.

Exercise 2.7 (10 pts). *Problem 11, Page 69.*

Exercise 2.8 (10 pts). *Prove that for every two group elements a and b, we have $|a| = |bab^{-1}|$. Deduce that $|ab| = |ba|$.*

2.6.2 Practice Problems

p. 54-58: 1, 5, 15, 17, 25, 37, 39

p. 69-71: 11, 15, 19, 46, 56, 72, 73, 77

Exercise 2.9. *Suppose m and n are two relatively prime integers. Let a, b be elements of a group for which $(ab)^n = (ba)^n$, and that $(ab)^m = (ba)^m$. Prove that $ab = ba$.*

Hint: Use Bezout's Lemma.

Exercise 2.10. *Suppose $G = \{g_1, \ldots, g_n\}$ is a group of size n that contains precisely m elements $a_1, \ldots, a_m$ satisfying the equation $x^2 = e$. Prove that $g_1 \cdots g_n = a_1 \cdots a_m$. Use this to prove the Wilson's Theorem from number theory: $(p-1)! \equiv -1 \mod p$, for every prime p.*

Exercise 2.11. *Let G be a non-empty set equiped with an associative binary operation with identity e. Suppose G has the property that for every $a \in G$ there is $b \in G$ with $ab = e$ or $ba = e$. Prove that G is a group.*

2.6.3 Challenge Problems

Exercise 2.12. *Prove that if for two group elements x, y we have $xy^2 = y^3x$ and $yx^2 = x^3y$, then $x = y = e$.*

Exercise 2.13. *Let a be an element of a group G. Prove that the equation $x^2ax = a^{-1}$ has a solution for $x \in G$ if and only if $a = b^3$ for some $b \in G$.*

Exercise 2.14. *Find the center of each of the groups $GL_n(\mathbb{R}), SL_n(\mathbb{R})$, and $SL_n(\mathbb{C})$.*

Exercise 2.15. *Let G be a group, m, n be relatively prime integers such that for all $a, b \in G$ we have $(ab)^n = a^nb^n$, and $(ab)^m = a^mb^m$. Prove that G is Abelian.*

Exercise 2.16. *Suppose S is a set with an associative binary operation and an identity element. Suppose further that S has n elements. Prove that S^n defined by*

$$S^n = \{s_1 \cdots s_n \mid s_j \in S \textit{ for all } j\}$$

is a group.

Exercise 2.17. *Suppose G is a non-empty set along with an associative binary operation for which $x^2y = y = yx^2$ for all $x, y \in G$. Prove that $xy = yx$ for all $x, y \in G$.*

2.7 Summary

- Make sure you are familiar with the usual examples of groups.
- Identity element, and inverse of each element are unique.
- A subgroup is a subset that is a group under the same operation.
- To check if a non-empty set is a subgroup we should use the one-step or two-step subgroups tests.
- A finite subset of a group is a subgroup if it is closed.
- $\langle a \rangle, C(a), Z(G)$ and $C(S)$ are some examples of subgroups.

2.8 Other Algebraic Structures (optional)

Definition 2.7. A non-empty set along with an associative binary operation is called a **semigroup**. A semigroup that has an identity is called a **monoid**.

Example 2.25. Here are some examples of monoids and semigroups.

(a) $(\mathbb{Z}^+, +)$ is a monoid with no identity.

(b) $(\mathbb{N}, +)$ is a semigroup with 0 as its identity.

(c) $(\mathbb{Z}, \cdot)$ is a semigroup with 1 as its identity.

Theorem 2.11. *The identity of a monoid is unique. If an element of a monoid has an inverse then, this inverse is unique.*

3 Week 3

3.1 Cyclic Groups

Definition 3.1. A group is called **cyclic** if it can be generated by one element.

Example 3.1. Determine if each of the following groups is cyclic.

(a) $\mathbb{Q}$.

(b) $\mathbb{Q}^\star$.

(c) $(2\mathbb{Z}, +)$.

(d) $\mathbb{Z}_8$.

(e) $U(7)$.

Theorem 3.1. *Suppose a is a group element and m, n are two integers.*

(a) If $|a| = \infty$, then $a^m = a^n$ if and only if $m = n$.

(b) If $|a| = k$ is finite, then $a^n = a^m$ if and only if $n \equiv m \mod k$.

As a result of the above theorem when $|a| = k$, then $\langle a \rangle$ has precisely k distinct elements: $e, a, \ldots, a^{k-1}$, and when $|a| = \infty$, the group $\langle a \rangle$ has infinitely many elements: $e, a^{\pm 1}, a^{\pm 2}, \ldots$. This motivates the following definition and theorem.

Definition 3.2. The **order** of a group G, denoted by $|G|$, is defined to be the size of it as a set.

Theorem 3.2. *The order of every cyclic group equals the order of its generator.*

Theorem 3.3. *Suppose a is a group element of finite order, and k is an integer. Then, $a^k = e$ if and only if $|a|$ divides k.*

Theorem 3.4. *If a and b are group elements of finite order for which $ab = ba$, then ab also has finite order, and $|ab|$ divides* $\operatorname{lcm}(|a|, |b|)$.

Theorem 3.5. *Suppose a is a group element of finite order $|a| = n$. Then, for every integer k we have*

$$|a^k| = \frac{n}{\gcd(n,k)}, \text{ and } \langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle.$$

Theorem 3.6. *Let a be a group element of finite order $|a| = n$, and let j, k be two integers. Then, the following are equivalent:*

(a) $\langle a^j \rangle = \langle a^k \rangle$

(b) $|a^j| = |a^k|$.

(c) $\gcd(n, j) = \gcd(n, k)$.

Example 3.2. Find all generators of $\mathbb{Z}_n$.

Theorem 3.7 (Fundamental Theorem of Cyclic Groups)**.** *Let G be a cyclic group. Then,*

(a) Every subgroup of G is cyclic.

(b) If $G = \langle a \rangle$ is finite and of order n, then the order of every subgroup of G divides n. Furthermore, for every divisor d of n, the only subgroup of G of order d is $\langle a^{n/d} \rangle$.

Definition 3.3. For every positive integer n the number of positive integers not exceeding n that are relatively prime to n is denoted by $\varphi(n)$. This function φ is called the **Euler's Totient Function**.

Example 3.3. Find $\varphi(1), \varphi(2)$, and $\varphi(p)$ for every prime p.

Theorem 3.8. *Let a be a group element of finite order n and d be a divisor of n. The number of elements of order d in $\langle a \rangle$ is $\varphi(d)$.*

Theorem 3.9. *Let n be a positive integer and G be a finite group. Then, the number of elements of order n in G is a multiple of $\varphi(n)$.*

Definition 3.4. Given a finite group G its **subgroup lattice** is a graph with all subgroups of G as its vertices. Two subgroups are connected by an edge if one is a subgroup of the other and there is no subgroup lying between them.

Example 3.4. Draw the subgroup lattice of $\mathbb{Z}_{12}$.

3.2 Symmetric Groups

Definition 3.5. Given a set X, the group consisting of all bijections $\sigma : X \to X$ under composition is called the **symmetric group on** X. This group is denoted by $Sym(X)$. Every element of $Sym(X)$ is called a **permutation**. If $X = \{1, 2, \ldots, n\}$ we denote this group by S_n. This group is called the **symmetric group of degree** n. The identity of a symmetric group is generally denoted by ε.

Notation. An element α of S_n is often denoted by

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

Definition 3.6. A **cycle of length** m (or an m**-cycle**) is a permutation σ in S_n for which, there are distinct integers $a_1, \ldots, a_m$ such that

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, a_{m-1} = a_m, \sigma(a_m) = a_1, \text{ and } \sigma(k) = k \text{ for every } k \neq a_1, \ldots, a_m.$$

This cycle is denoted by $(a_1 \cdots a_m)$. Two cycles $(a_1 \cdots a_m)$ and $(b_1 \cdots b_k)$ are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

Example 3.5. Write down the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$ as a product of disjoint cycles.

Theorem 3.10 (Cycle Decomposition)**.** *Every permutation in S_n, with $n \geq 2$, can be written as a product (i.e. composition) of pairwise disjoint cycles. Furthermore this representation is unique up to the order of cycles. In other words, if $c_1 \cdots c_k$ and $d_1 \cdots d_\ell$ are decompositions of a permutation σ into disjoint cycles of length more than 1, then $k = \ell$ and for each c_i there is a unique d_j for which $c_i = d_j$.*

Theorem 3.11. *Disjoint cycles commute.*

Theorem 3.12. *Suppose $\sigma = c_1 \cdots c_m$ is a cycle decomposition of a permutation $\sigma \in S_n$. Then, the order of σ is the least common multiple of the length of cycles $c_1, \ldots, c_m$.*

Example 3.6. Find the order of the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$

Example 3.7. Determine the number of elements of order 3 in S_5.

Theorem 3.13. *Every permutation in S_n can be written as a product of 2-cycles. Furthermore, if a permutation is written as a product of an odd number of 2-cycles, then it cannot be written as a product of an even number of 2-cycles. Similarly,if a permutation is written as a product of an even number of 2-cycles, then it cannot be written as a product of an odd number of 2-cycles.*

Definition 3.7. An element of S_n (with $n \geq 2$) is said to be an **even** permutation if it can be written as a product of an even number of 2-cycles of S_n. Otherwise we say the permutation is **odd**.

Example 3.8. Write (1 2 3 4) as a product of 2-cycles.

Theorem 3.14. *The subset of S_n consisting of all even permutations is a subgroup of S_n.*

Definition 3.8. The subgroup of S_n consisting of all even permutations is called the **alternating group of degree** n and is denoted by A_n.

Theorem 3.15. *For $n \geq 2$ we have $|A_n| = n!/2$.*

3.3 Warm-ups

Example 3.9. Given an integer n is $\{kn \mid k \in \mathbb{Z}\}$ a cyclic group under addition?

Solution. Yes. This is a subgroup of $\mathbb{Z}$ generated by n. (why?) □

Example 3.10. Prove that:

(a) $|e| = 1$.

(b) For every group element a we have $|a| = |a^{-1}|$.

Solution. (a) Note that $e^1 = e$ and 1 is the smallest such positive integer. Thus $|e| = 1$.
(b) If a is of infinite order but a^{-1} has a finite order n, then $(a^{-1})^n = e$ which implies $a^{-n} = e$ which means

$a^n = e$, by inverting both sides. This is a contradiction.

If a has finite order then we use Theorem 3.5 to obtain $|a^{-1}| = \dfrac{|a|}{\gcd(|a|, -1)} = |a|$, as desired. □

Example 3.11. List all elements of $\langle 2 \rangle$ in $U(17)$.

Solution. Powers of 2 mod 17 are: 2, 4, 8, 16, 15, 13, 9, 1. Thus, these are all the elements of $\langle 2 \rangle$. □

Example 3.12. For a group element a we know $|a| = 1200$. Find the order of a^{70}.

Solution. By a theorem $|a^{70}| = \dfrac{1200}{\gcd(1200, 70)} = \dfrac{1200}{10} = 120$. □

Example 3.13. For an element α of S_n prove that $\alpha(1) + \cdots + \alpha(n) = \dfrac{n(n+1)}{2}$.

Solution. Since α is a permutation of $\{1, \ldots, n\}$, the values $\alpha(1), \ldots, \alpha(n)$ are the same as $1, \ldots, n$ perhaps in a different order. Therefore, $\alpha(1) + \cdots + \alpha(n) = 1 + \cdots + n = \dfrac{n(n+1)}{2}$. □

Example 3.14. Show that every 1-cycle in S_n is the identity.

Solution. By definition, a 1-cycle (a) maps a to a and every other element k to itself. This is precisely the definition of the identity permutation. □

Example 3.15. Prove that the only finite subgroup of an infinite cyclic group is the trivial subgroup $\{e\}$.

Solution. Suppose $\langle a \rangle$ is an infinite cyclic group. We know every subgroup of this group must be of the form $\langle a^k \rangle$ for some integer k. If $k = 0$, then this subgroup is the trivial subgroup, as desired. Otherwise, the order of $(a^k)^n = a^{kn} \neq e$ for every $n \in \mathbb{Z}^+$, since the order of a is infinity. Therefore, $\langle a^k \rangle$ is an infinite subgroup. This completes the proof. □

Example 3.16. Is it possible for a finite group to have an element of infinite order?

Solution.

□

3.4 More Examples

Example 3.17. Determine if each of the following groups are cyclic.

(a) $GL_2(\mathbb{R})$.

(b) $U(8)$.

Solution. (a) Note that this group is not Abelian (why?), and thus not cyclic.

(b) We see that $1 \equiv 3^2 \equiv 5^2 \equiv 7^2 \mod 8$, which means all elements of $U(8)$ have order 1 or 2, but $U(8)$ has four elements, and thus since it contains no element of order 4 it is not cyclic. □

Example 3.18. Let a, b be two group elements. Prove or disprove:

(a) If a and b are of finite order, then ab also has finite order.

(b) If $ab = ba$, then $|ab| = \operatorname{lcm}(|a|, |b|)$.

Solution. (a) This is false. For example consider the following matrices in $GL_2(\mathbb{R})$:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \text{ and } B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

We see that

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

and thus $A^2 = B^2 = I$. Therefore, A and B both have finite orders. Note that

$$(AB)^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

We can see by induction (how?) that

$$(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

Thus AB has infinite order.

(b) This is false. If we take $b = a^{-1}$ we will have $aa^{-1} = a^{-1}a$, but $|aa^{-1}| = |e| = 1$, however if we take a to be non-identity $\operatorname{lcm}(|a|, |a^{-1}|)$ is more than 1. □

Example 3.19. Show that $\mathbb{C}^*$ has a unique subgroup of order 4.

Solution. For a subgroup of $\mathbb{C}^*$ to be of order 4, we need an element of order 4, which means we need a solution of $x^4 = 1$ that is not a solution to $x^2 = 1$. (Recall that if $x^4 = 1$, then the order of x must divide 4.) Such elements in $\mathbb{C}^*$ are only $\pm i$. So, $\langle i \rangle = \langle -i \rangle = \{\pm 1, \pm i\}$ is the only subgroup of order 4 in $\mathbb{C}^*$. □

Example 3.20. How many elements of order 3 does S_{10} have?

Solution. We know σ has order 3 if and only if the cycles that appear in its cycle decomposition are all of length 3. We will solve the problem based on how many cycles appear in the cycle decomposition of σ.

If σ is a 3-cycle, then we have to select 3 numbers between 1 and 10. For any three integers a, b, c we have two cycles $(a\ b\ c)$ and $(a\ c\ b)$. Therefore, we have $\binom{10}{3} \cdot 2$ such permutations.

If $\sigma = c_1c_2$ then we will select two disjoint cycles and multiply them. By the same argument as the one above the number of possibilities of c_1 is $\binom{10}{3} \cdot 2$. The number of possibilities of c_2 is $\binom{7}{3} \cdot 2$. Since $c_1c_2 = c_2c_1$ we need to divide the result by 2. So, the number of such σ's is $2\binom{10}{3}\binom{7}{3}$.

For when $\sigma = c_1c_2c_3$, where c_j's are pairwise disjoint we repeat the same argument: There are $2\binom{10}{3}$ possibilities for c_1, and $2\binom{7}{3}$ possibilities for c_2 and $2\binom{4}{3}$ possibilities for c_3. Since we can rearrange c_j's the answer is $8\binom{10}{3}\binom{7}{3}\binom{4}{3}/6$.

Therefore the answer is

$$2\binom{10}{3} + 2\binom{10}{3}\binom{7}{3} + 4\binom{10}{3}\binom{7}{3}\binom{4}{3}/3 = 3140.$$

□

Example 3.21. Prove that a permutation in S_n is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

3.5 Exercises

3.5.1 Problems for Grading

Exercise 3.1 (10 pts)**.** *Problem 26, Page 87.*

Exercise 3.2 (10 pts)**.** *Problem 34, Page 87.*

Exercise 3.3 (10 pts)**.** *Problem 34, Page 114.*

Exercise 3.4 (10 pts)**.** *Problem 57, Page 115.*

Exercise 3.5 (10 pts)**.** *Prove that for every positive integer n, $\mathbb{C}^*$ has a unique cyclic subgroup of order n.*

Hint: See Example 3.19.

Exercise 3.6 (10 pts)**.** *Let n be a positive integer and a be a group element for which $a^n = e$. Prove that $|a| = n$ if and only if for every prime p dividing n we have $a^{n/p} \neq e$.*

Exercise 3.7 (10 pts)**.** *Determine the number of elements of order 2 in A_8.*

Hint: Use cycle decomposition. See Example 3.20.

Exercise 3.8 (10 pts)**.** *For the following permutation find its cycle decomposition, its order, and determine if it is even or odd:* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 1 & 4 & 6 & 3 \end{pmatrix}$

3.5.2 Problems for Practice

Definition 3.9. Let $a_1, \dots, a_n$ be elements in a group G. The intersection of all subgroups of G containing $a_1, \dots, a_n$ is called the **group generated by** $a_1, \dots, a_n$. This group is denoted by $\langle a_1, \dots, a_n \rangle$. A group G is said to be **finitely generated** if there finitely many elements $a_1, \dots, a_n$ in G for which $G = \langle a_1, \dots, a_n \rangle$.

Exercise 3.9. *Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.*

Exercise 3.10. *Let $m \leq n$ be two positive integers more than 1. How many m-cycles are there in S_n?*

Exercise 3.11. *Let p be a prime. How many elements of order p does S_p have?*

Exercise 3.12. *Draw the subgroup lattice of $\mathbb{Z}_{18}$.*

Pages 86-90: 7, 17, 21, 38, 65, 70.

Pages 112-116: 3, 43, 44, 61.

3.5.3 Challenge Problems

Exercise 3.13. *Prove that every element of finite order in $GL_n(\mathbb{C})$ is diagonalizable.*

Exercise 3.14. *Prove that every finite subgroup of $\mathbb{C}^*$ is cyclic.*

Exercise 3.15. *A finite group G is said to be almost Abelian if G can be written as a finite union $G = \bigcup_{i=1}^{m} H_i$, where $H_i \leq G$ in which H_i's intersect trivially, i.e. $H_i \cap H_j = \{e\}$, for all $i \neq j$. Find all integers n for which S_n is almost Abelian.*

3.6 Summary

- Groups of the form $\langle a \rangle$ are called cyclic.
- $|a^k| = \dfrac{|a|}{\gcd(|a|, k)}$.
- $a^m = e$ iff $|a|$ divides m.
- Subgroups of cyclic groups are cyclic.
- A cyclic group $\langle a \rangle$ of order n has precisely one subgroup of order d for every positive divisor d of n. This subgroup is $\langle a^{n/d} \rangle$. These are all subgroups of $\langle a \rangle$.
- $\langle a \rangle$ has precisely $\varphi(d)$ elements of order d for every divisor d of $|a|$.
- Every permutation can be written as a product of disjoint cycles.
- The order of a permutation is the least common multiple of the length of its disjoint cycles.
- Every permutation can be written as a product of transpositions (i.e. 2-cycles).

- A_n, the set of all even permutations of S_n is a subgroup of S_n.

- To find the order of a permutation write down its cycle decomposition and find the least common multiple of the lengths of the cycles.

- Use $(a_1\ a_2\ \cdots a_n) = (a_1\ a_2)(a_2 a_3)\cdots(a_{n-1}a_n)$ to determine if a permutation is odd or even.

4 Week 4

4.1 Group Isomorphisms

Two groups with the "same" multiplication tables (these tables are called **Cayley tables**) are considered isomorphic. For example consider the Cayley tables of the groups $\mathbb{Z}_4$ and the subgroup $\langle i \rangle$ of $\mathbb{C}^*$.

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

Cayley Table of $\mathbb{Z}_4$

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

Cayley Table of $\langle i \rangle$

As shown above, if we do the following replacements we get the Cayley table of $\langle i \rangle$ from the Cayley table of $\mathbb{Z}_4$.

$$0 \to 1, \qquad 1 \to i, \qquad 2 \to -1, \qquad 3 \to -i$$

We say the two groups $\mathbb{Z}_4$ and $\langle i \rangle$ are isomorphic and we write $\mathbb{Z}_4 \simeq \langle i \rangle$. The definition can mathematically be stated as follows:

Definition 4.1. We say two groups G_1 and G_2 are **isomorphic** if there is a bijection $\phi : G_1 \to G_2$ for which $\phi(xy) = \phi(x)\phi(y)$ for every $x, y \in G_1$. The function ϕ is called an **isomorphism**. When two groups G_1 and G_2 are isomorphic we write $G_1 \simeq G_2$.

When a function $\phi : G_1 \to G_2$ satisfies $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G_1$ we say ϕ is **operation-preserving.**

Theorem 4.1. *Isomorphism is an equivalence relation. In other words if G, H and K are groups, then*

(a) $G \simeq G$. Furthermore, $id : G \to G$ is an isomorphism.

(b) If $G \simeq H$, then $H \simeq G$. Furthermore, if $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is also an isomorphism.

(c) If $G \simeq H$, and $H \simeq K$, then $G \simeq K$. Furthremore, if $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms, then $\psi \circ \phi : G \to K$ is an isomorpshim,

Proof. (a) Note that the identity function is bijective. Also $id(xy) = xy = id(x)id(y)$. Thus, it is an isomorphism.
(b) Since ϕ is bijective, ϕ^{-1} exists and is a bijection. Suppose $x, y \in H$. We will need to show $\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y)$. By definition of inverse function it is enough to show $xy = \phi(\phi^{-1}(x)\phi^{-1}(y))$. Since ϕ is an isomorphism we have

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

(c) Since ϕ and ψ are bijective, their composition $\psi \circ \phi$ is also bijective. Let $x, y \in G$. We have $\psi \circ \phi(xy) = \psi(\phi(x)\phi(y))$, since ϕ is an isomorphism. Since ψ is an isomorphism we have

$$\psi \circ \phi(xy) = \psi(\phi(x))\psi(\phi(y)) = (\psi \circ \phi(x))(\psi \circ \phi(y)).$$

Thus $\psi \circ \phi$ is an isomorphism. □

Example 4.1. Every two cyclic groups are isomorphic if and only if they have the same order.

Proof. Suppose $G = \langle a \rangle$ and $H = \langle b \rangle$ are two cyclic groups of the same order. By a theorem we have $|a| = |b|$. For simplicity let n be this common order. Note that $G = \{e, a, \ldots, a^{n-1}\}$ and $H = \{e, b, \ldots, b^{n-1}\}$. Define $\phi : G \to H$ by $\phi(a^k) = b^k$ for each k with $0 \leq k \leq n-1$. By definition ϕ is onto and one-to-one.

Note also that $\phi(a^k a^\ell) = \phi(a^{k+\ell})$. If $k + \ell \equiv m \mod n$ with $0 \leq m \leq n-1$, then $a^{k+\ell} = a^m$ and $b^{k+\ell} = b^m$. Therefore, $\phi(a^{k+\ell}) = \phi(a^m) = b^m$, and $\phi(a^k)\phi(a^\ell) = b^k b^\ell = b^{k+\ell} = b^m$. This completes the proof. □

Example 4.2. The following are some examples of isomorphic groups:

(a) $U(7) \simeq \mathbb{Z}_6$.

(b) $2\mathbb{Z} \simeq \mathbb{Z}$.

(c) $\langle e^{2\pi i/n} \rangle \simeq \mathbb{Z}_n$ for every positive integer n.

Solution. We will use Example 4.1.
(a) $U(7) = \langle 2 \rangle$ is a cyclic group of order 6.
(b) $2\mathbb{Z} = \langle 2 \rangle$ is an infinite cyclic group.
(c) $(e^{2\pi i} n)^k = 1$ if and only if $\cos(2\pi k/n) = 1$, and $\sin(2\pi k/n) = 0$, which is equivalent to $2\pi k/n$ being an integer multiple of 2π. This means k must be a multiple of n. Therefore the order of $e^{2\pi i/n}$ is n. □

Theorem 4.2 (Cayley's Theorem)**.** *If G is a group, then G is isomorphic to a subgroup of $Sym(G)$.*

Theorem 4.3 (Properties of Isomorphisms and Isomorphic Groups)**.** *Let $\phi : G_1 \to G_2$ be an isomorphism. Then, for every $a, b \in G_1$ and every integer n we have:*

(a) $\phi(e) = e$. (Note: The first e is the identity of G_1 and the second e is the identity of G_2.)

(b) $\phi(a^n) = (\phi(a))^n$.

(c) $\phi(\langle a\rangle) = \langle\phi(a)\rangle$.

(d) $|a| = |\phi(a)|$.

(e) a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute. Thus, G_1 is Abelian if and only if G_2 is Abelian.

(f) $\phi(Z(G_1)) = Z(G_2)$.

(g) G_1 and G_2 have the same number of elements of each specific order.

(h) If H is a subgroup of G_1, then $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of G_2.

(i) If K is a subgroup of G_2, then $\phi^{-1}(K) = \{g \in G_1 \mid \phi(g) \in K\}$ is a subgroup of G_1.

Definition 4.2. An **automorphism** of a group G is an isomorphism from G to G. The set of all automorphisms of G is denoted by $Aut(G)$.

Theorem 4.4. *For every group G, the set $Aut(G)$ is a subgroup of $Sym(G)$.*

Definition 4.3. Given an element a of a group G, an **inner automorphism** of G is a function $\phi_a : G \to G$ given by $\phi_a(g) = aga^{-1}$. The set consisting of all inner automorphisms of G is denoted by $Inn(G)$.

Theorem 4.5. *For every group G, $Inn(G)$ is a subgroup of $Aut(G)$.*

Understanding the structure of $Aut(G)$ is not easy in general, but in some cases we can identify this group.

Example 4.3. Let n be an integer more than 1. Prove that $Aut(\mathbb{Z}_n) \simeq U(n)$.

Example 4.4. Suppose H is a subgroup of a group G and a is an element of G. Prove that $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ is a subgroup of G and that $H \simeq aHa^{-1}$.

4.2 Cosets

Let us first take a look at an example:

Example 4.5. We know the set $3\mathbb{Z}$, consisting of integer multiples of 3, is a subgroup of $\mathbb{Z}$. This set can be seen as the set of all integers that are $0 \mod 3$. However, those integers that are 1 or $2 \mod 3$ do not form a group. But we could think about those sets as "translations" of $3\mathbb{Z}$. In other words, every integer belongs to precisely one of $3\mathbb{Z}, 3\mathbb{Z}+1$, or $3\mathbb{Z}+2$. Similarly $n\mathbb{Z}$ could be translated to partition $\mathbb{Z}$. Each of these translations $n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+(n-1)$ is called a coset as defined below.

Definition 4.4. Let S be a nonempty subset of a group G and a be an element of G. The set $\{as \mid s \in S\}$ is denoted by aS. Similarly we set $Sa = \{sa \mid s \in S\}$. When H is a subgroup of G and a is an element of G, the set aH is called the **left coset** of H containing a. The set Ha is called the **right coset** of H containing a. The set $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ is called the **conjugate** of H by a. For two nonempty subsets S and T of a group G we define $ST = \{st \mid s \in S, \text{ and } t \in T\}$.

Remark. For three nonempty subsets S, T, U of a group G and elements a, b of G we can easily see that

$$eS = Se = S,\ (ab)S = a(bS),\ S(ab) = (Sa)b,\ (aS)b = a(Sb), S(aT) = (Sa)T, \text{ and } (ST)U = S(TU).$$

Example 4.6. Consider the subgroup $H = \langle(1\ 2\ 3)\rangle = \{\varepsilon, (1\ 2\ 3), (1\ 3\ 2)\}$ of S_3. This subgroup has two right cosets H and $H(1\ 2)$, and two left cosets H and $(1\ 2)H$. This can be manually checked by finding Hg and gH for all $g \in S_3$. Clearly this is too computational and we would like to minimize such computations. In this example we will see that S_3 can be partitioned into right cosets of H, and also into left cosets of H. Also note that despite the fact that S_3 is not Abelian, $H(1\ 2) = (1\ 2)H$.

Theorem 4.6 (Properties of Cosets)**.** *Let H be a subgroup of G, and a, b be elements of G. Then,*

(a) $|aH| = |Ha| = |aHb| = |H|$.

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

(c) $aH = bH$ *or* $aH \cap bH = \emptyset$.

(d) $aH = bH$ *if and only if* $Ha^{-1} = Hb^{-1}$.

Corollary 4.1. Let H be a subgroup of a group G. Then, the number of distinct left cosets of H in G is the same as the number of distinct right cosets of H in G.

Definition 4.5. The number of distinct left (or right) cosets of a subrgoup H of a group G is called the **index** of H in G and is denoted by $[G : H]$.

Example 4.7. The index of $n\mathbb{Z}$ in $\mathbb{Z}$ is n.

Theorem 4.7 (Lagrange's Theorem)**.** *Let H be a subgroup of a finite group G. Then, $|G| = |H|[G : H]$, and thus the order of H divides the order of G.*

Corollary 4.2. Every group of a prime order p is isomorphic to $\mathbb{Z}_p$.

Corollary 4.3. The order of an element a in a finite group G divides the order of the group. Therefore, $a^{|G|} = e$.

Example 4.8 (Fermat's Little Theorem)**.** Prove that for every prime p and every integer a we have $a^p \equiv a$ mod p.

4.3 Warm-ups

Example 4.9. Suppose G is an Abelian group. Prove that for every two subsets S and T of G we have $ST = TS$. Is it true that if for every two subsets S and T of a group G we have $ST = TS$, then G must be Abelian?

Solution. By definition we have $ST = \{st \mid s \in S, t \in T\} = \{ts \mid s \in S, t \in T\}$, since $st = ts$. Therefore, $ST = TS$.

The answer to the question is also positive. Let $a, b \in G$ and take $S = \{a\}, T = \{b\}$. We have $ST = \{ab\}$, and $TS = \{ba\}$. Since $ST = TS$ we must have $ab = ba$, and hence G is Abelian. □

Example 4.10. Prove that a finite group of order n, does not have a subgroup whose order strictly lies between $n/2$ and n.

Solution. Suppose m is the order of a subgroup of a group of order n. We know $n = mk$ for some positive integer k. Since k is a positive integer, $n = m$ or $n \geq 2m$ which means either $m = n$ or $m \leq n/2$, as desired. □

Example 4.11. Show that every group of order 11 is cyclic.

Solution. Since 11 is prime by Corollary 4.2 any group of order 11 is isomprhic to $\mathbb{Z}_{11}$ and therefore it is cyclic. □

Example 4.12. Let H be a subgroup of a finite group G. Prove that the size of every coset of H divides the order of G.

Solution. By Theorem 4.6 the size of every coset of H is the same as the order of H. By Lagrange's Theorem the order of H divides the order of G. Therefore, the size of every coset of H divides the order of G. □

4.4 More Examples

Example 4.13. Find all integers n for which they satisfy the following property:

"For every group G, the map $f : G \to G$, defined by $f(x) = x^n$ is an automorphism."

Solution. Note that if $n = 1$, then f is an isomorphism. If $n > 1$, then taking $G = \mathbb{Z}_n$, gives us $f(k) = nk = 0$, for all k, which means f is not one-to-one and thus not an isomorphism.
If $n < -1$, similarly consider $G = \mathbb{Z}_{-n}$. This again shows that f is not one-to-one.
If $n = 0$, then taking $G = \mathbb{Z}_2$ (or any non-trivial group) we get that $f(1) = 0$, and thus f is not one-to-one.
If $n = -1$, then for f to be an isomorphism we need to have $(xy)^{-1} = x^{-1}y^{-1}$, which means $xy = (x^{-1}y^{-1})^{-1} = yx$. Thus, G must be Abelian, which is not true for all G, e.g. $G = S_3$.
The answer is $n = 1$. □

Example 4.14. Prove that a group G is Abelian if and only if the function $f : G \to G$ defined by $f(x) = x^{-1}$ is an automorphism.

Solution. First, note that $x^{-1} = y^{-1}$ implies $x = y$, by taking the inverse of both sides, and thus f is always one-to-one.
Now, note that $f(x^{-1}) = (x^{-1})^{-1} = x$ and thus f is onto. Therefore, f is always a bijection.

Suppose f is an isomorphism of a group G. We must have $f(xy) = f(x)f(y)$ for all $x, y \in G$. Therefore, $(xy)^{-1} = x^{-1}y^{-1}$. By taking the inverse of both sides and applying the shoes-socks property and the fact that $(a^{-1})^{-1} = a$ we obtain $xy = yx$, which implies G is Abelian.

If G is Abelian, then $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$. Here we used the shoes-socks property and the fact that G is Abelian. Thus, if G is Abelian, then f is an isomorphism, as desired. □

Example 4.15. Find all integers $n > 2$ for which $S_n \simeq D_{n!/2}$.

Sketch. First note that both groups have order $n!$, so we should look at the structure of the groups. $D_{n!/2}$ has a rotation of order $n!/2$. We know how to find order of elements of S_n. So, we need a cycle decomposition with the least common multiple of the lengths equal to $n!/2$. This doesn't happen when n is "large".

Solution. Note that $D_3 \simeq S_3$, as each group is the group of permutations of a set of size 3. We claim that for every $n \geq 4$, the groups S_n and $D_{n!/2}$ are not isomorphic. For S_4 and D_{12} note that D_{12} has an element of order 12, but all possible lengths of cycle decompositions of elements of S_4 are $4, 3, 2+2, 2$, which means the maximum order of elements of S_4 is 4. So, $S_4 \not\simeq D_{12}$.

Note that $D_{n!/2}$ has an element of order $n!/2$. The order of an element of S_n does not exceed the product $a_1 \cdots a_k$, where $a_1 + \cdots + a_k = n$. (Least common multiple does not exceed the product.) We will inductively (on n) show that if $a_1 + \cdots + a_k = n$ for positive integers $a_1, \ldots, a_k$ with $n \geq 4$, then $a_1 \cdots a_k < n!/2$. We already proved this for $n = 4$. If $a_1 + \cdots + a_k = n + 1$, then $a_2 + \cdots + a_k \leq n$ and thus $a_2 \cdots a_k < n!/2$ by inductive hypothesis. Since $a_1 \leq n + 1$ we obtain the result.

Therefore $S_n \simeq D_{n!/2}$ if and only if $n = 3$. □

Example 4.16. Prove that if G and H are isomorphic groups, then $Aut(G) \simeq Aut(H)$ and that $Inn(G) \simeq Inn(H)$.

Solution. Suppose $\phi : G \to H$ is an isomorphism. We define $T : Aut(G) \to Aut(H)$ by $T(f) = \phi \circ f \circ \phi^{-1}$. We will prove that T is an isomorphism.
First, we need to show $T(f)$ is an automorphism of H. Note that by Theorem 4.1, $\phi^{-1} : H \to G$ is an isomorphism. Applying the same theorem we conclude that $\phi \circ f \circ \phi^{-1}$ is an automorphism of H.

Next, we will show T is one-to-one: Suppose $T(f) = T(g)$. We have $\phi \circ f \circ \phi^{-1} = \phi \circ g \circ \phi^{-1}$. After composing both sides by ϕ and ϕ^{-1} from the right and left we obtain $f = g$.

Now, we will show T is onto: Let $g \in Aut(H)$. Note that $f = \phi^{-1} \circ g \circ \phi$ is an automorphism of G by Theorem 4.1. $T(f) = \phi \circ g \circ \phi^{-1} = f$.

We will show T is operation preserving: Suppose f and g are automorphisms of G. $T(f)T(g) = \phi f \phi^{-1} \phi g \phi^{-1} = \phi f g \phi^{-1} = T(fg)$. (Note that here the operation is composition.) This completes the proof. □

Example 4.17. Suppose S and T are two finite sets of the same size. Prove that $Sym(S) \simeq Sym(T)$.

Solution. Let $f : S \to T$ be a bijection between S and T. Define an isomorphism $\phi : Sym(S) \to Sym(T)$ by $\phi(\sigma) = f \circ \sigma \circ f^{-1}$. Note that since $\sigma : S \to S$ and $f^{-1} : T \to S$ are bijections, $f \circ \sigma \circ f^{-1} : T \to T$ is also a bijection and thus $f \circ \sigma \circ f^{-1} \in Sym(T)$. The rest of the proof is similar to the above proof. □

Example 4.18. Is it possible for a finite group G to have a proper subgroup H for which $G \simeq H$? How about when G is an infinite group?

Solution. The answer to the first part is negative. If G and H are isomorphic, then they must have the same order. However if G is finite then since $H \subseteq G$ we must have $G = H$, which is a contradiction.

The answer to the second part is positive. Consider $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$. Both of these groups are infinite cyclic groups and thus they are isomorphic by Example 4.1. □

Example 4.19. Let H be a subgroup of a group G and aH be a coset of H in G. Prove that if K is a subgroup of G containing aH, then K must also contain H.

Solution. Since K contains aH, we must have $a = ae \in K$. Since $ah \in aH$ for every $h \in H$ we must have $ah \in K$. Therefore, $a^{-1}ah \in K$ which means $h \in K$. This shows every element of H must be in K, and thus H is a subset of K, as desired. □

Example 4.20. Prove that $\mathbb{R} \simeq \mathbb{R}^+$.

Sketch. We need to find an isomorphism between $\mathbb{R}$ and $\mathbb{R}^+$. In other words, we are looking for a bijection $f : \mathbb{R} \to \mathbb{R}^+$ for which $f(x + y) = xy$. We realize that exponential functions satisfy this property. This leads to the following solution:

Solution. Define $f : \mathbb{R} \to \mathbb{R}^+$ by $f(x) = e^x$. Note that e^x is always positive and thus the function is well-defined. $f(x) = f(y)$ implies $e^x = e^y$ or $x = y$. Thus, f is one-to-one. We also note that for every positive real number x we have $f(\ln x) = e^{\ln x} = x$, and thus f is onto. Also, note that $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$. Therefore $\mathbb{R} \simeq \mathbb{R}^+$. □

Example 4.21. Let H be a subgroup of finite index n in a group G. Prove that for every $a \in G$ there is a positive integer $k \leq n$ for which $a^k \in H$.

Solution. Consider the cosets $H, Ha, \ldots, Ha^n$. Since the index of H in G is n, there are two integers $0 \leq k < \ell \leq n$ for which $Ha^k = Ha^\ell$. Therefore, $a^\ell a^{-k} \in H$ which implies $a^{\ell - k} \in H$, as desired. □

4.5 Exercises

4.5.1 Problems for Grading

Exercise 4.1 (10 pts)**.** *Page 133, Problem 24.*

Exercise 4.2 (10 pts)**.** *Page 135, Problem 55.*

Exercise 4.3 (10 pts)**.** *Page 136, Problem 63.*

Exercise 4.4 (10 pts)**.** *Page 151, Problem 11.*

Exercise 4.5 (10 pts)**.** *Determine which of these groups are isomorphic and why: $U(8), U(10), U(12)$.*

Exercise 4.6 (10 pts)**.** *Let H be a subgroup of a group G, and $a, b, x, y \in G$ such that $aHb = xHy$. Prove that $b^{-1}Ha^{-1} = y^{-1}Hx^{-1}$.*

Exercise 4.7 (10 pts)**.** *Let $n \geq 2$ be an integer. Consider the set $H = \{\sigma \in S_{n+1} \mid \sigma(n+1) = n+1\}$. Prove that H is a subgroup of S_{n+1} and that $H \simeq S_n$.*

Exercise 4.8 (10 pts)**.** *Find all automorphisms of $\mathbb{Q}$ and determine which well-known group* Aut($\mathbb{Q}$) *is isomorphic to.*

Hint: Follow a proof similar to that of $Aut(\mathbb{Z}_n) \simeq U(n)$. Be aware that there are significant differences, since $\mathbb{Q}$ is not cyclic.

4.5.2 Problems for Practice

Exercise 4.9. *Find two groups G and H for which $G \not\simeq H$, but $Aut(G) \simeq Aut(H)$.*

Exercise 4.10. *Let G and H be two groups. Is the set of isomorphisms $\phi : G \to H$ under composition a group? Justify your answer.*

Exercise 4.11. *Prove that $Aut(\mathbb{Z}) \simeq \mathbb{Z}_2$.*

Page 133-136, Problems 23, 40, 41, 50, 65, 66.
Pages 150-151, Problems 7, 10, 14, 17.

4.5.3 Challenge Problems

Exercise 4.12. *Find all groups G (up to isomorphism) whose group of automorphisms is the trivial group $\{e\}$.*

Exercise 4.13. *This question is regarding the automorphism group of the additive group $\mathbb{R}$.*

(a) Describe all automorphisms of $\mathbb{R}$, and prove $Aut(\mathbb{R})$ is uncountable.

(b) Prove that for every finite group G, $Aut(\mathbb{R})$ has a subgroup isomorphic to G.

4.6 Summary

- To prove $\phi : G \to H$ is an isomorphism, we would have to show ϕ is a bijection and operation-preserving, i.e. $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.
- Isomorphism is an equivalence relation.
- Usual group properties of two isomorphic groups are the same.
- $Inn(G) \leq Aut(G) \leq Sym(G)$.
- $aH = bH$ iff $a^{-1}b \in H$, and $Ha = Hb$ iff $ba^{-1} \in H$.
- Left cosets of a subgroup H of a group G partition G.
- $|G| = |H|[G : H]$, where $[G : H]$ is the number of left cosets of H.

5 Week 5

Theorem 5.1. *Suppose G is a group and $H \leq K \leq G$ for which indices of K in G and H is K are both finite. Then, $[G : H] = [G : K][K : H]$.*

Theorem 5.2. *Let H and K be two subgroups of a group G. Then, HK is a subgroup of G if and only if $HK = KH$.*

Theorem 5.3. *Suppose H and K are finite subgroups of a group. Then, $|HK| = \dfrac{|H||K|}{|H \cap K|}$.*

Example 5.1. Consider the subgroups $H = \langle(1\ 2)\rangle$ and $K = \langle(1\ 2\ 3\ 4)\rangle$ of S_4. Is HK a subgroup of S_4? What is the size of HK?

Theorem 5.4. *Let p be an odd prime. Every group of order $2p$ is either isomorphic to $\mathbb{Z}_{2p}$ or D_p. Every group of order 4 is either isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Definition 5.1. A **group of permutations** of a nonempty set S is a subgroup of $Sym(S)$. Let G be a group of permutations on a set S and let $i \in S$. The **stabilizer** of i in G is $stab_G(i) = \{\sigma \in G \mid \sigma(i) = i\}$. The **orbit** of i under G is given by $orb_G(i) = \{\sigma(i) \mid \sigma \in G\}$

Example 5.2. Consider the subgroup $G = \langle(1\ 2 \cdots n)\rangle$ of S_n. Find the orbit and stabilizer of 1 in G.

Theorem 5.5 (Orbit-Stabilizer)**.** *Let G be a finite group of permutations on a set S. Then, for any $i \in S$ we have $|G| = |orb_G(i)||stab_G(i)|$.*

Example 5.3. How many rotations does a cube have?

5.1 External Direct Products (or Cartesian Products)

Definition 5.2. Given groups $G_1, \dots, G_n$ their **External Direct Product**, denoted by $G_1 \times \cdots \times G_n$ or $\prod_{k=1}^{n} G_k$, is the set of n-tuples $(g_1, \dots, g_n)$ with $g_j \in G_j$ for every j. The group operation of $\prod_{k=1}^{n} G_k$ is componentwise. Similarly for any collection of groups G_i indexed by a set I, i.e. $i \in I$, their external direct product, denoted by $\prod_{i \in I} G_i$, is the set of all sequences $(g_i)_{i \in I}$, where each g_i is in G_i. Similarly, the operation is componentwise.

Example 5.4. $\mathbb{Z}_3 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$ is a group with 6 elements. The first components are added mod 3 and the second components are added mod 2. For example $(2,1)+(1,1) = (0,0)$ and $(2,0) + (2,1) = (1,1)$.

Theorem 5.6. *For every three groups G, H, K we have $G \times H \simeq H \times G$, and $(G \times H) \times K \simeq G \times (H \times K)$.*

Theorem 5.7. *The group $\prod_{k=1}^{n} G_k$ is Abelian if and only if every G_k is Abelian.*

Theorem 5.8. *Suppose $(g_1, \dots, g_n) \in G_1 \times \cdots \times G_n$, where G_j's are groups. Then, $|(g_1, \dots, g_n)| = \operatorname{lcm}(|g_1|, \dots, |g_n|)$, if all g_i's are of finite order. If the order of at least one g_i is infinity, then the order of $(g_1, \dots, g_n)$ is infinity.*

Example 5.5. Prove that $\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_9$ is cyclic but $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_6$ is not.

Example 5.6. Prove that $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ is cyclic if and only if $n_1, \dots, n_k$ are pairwise relatively prime.

Theorem 5.9. *Suppose $G_1, \dots, G_n$ are finite groups. Then, $\prod_{i=1}^{n} G_i$ is cyclic if and only if every G_i is cyclic and the orders of G_i's are pairwise relatively prime.*

Example 5.7. Determine if each of the following is cyclic.

(a) $\mathbb{Z}_7 \times \langle(1\ 2\ 3)\rangle$.

(b) $\mathbb{Z} \times \mathbb{Z}$.

Theorem 5.10. *Suppose m and n are relatively prime integers. Then $U(mn) \simeq U(m) \times U(n)$.*

Corollary 5.1. If m and n are relatively prime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Theorem 5.11. *Let p be a prime and n be a positive integer. Then,*

(a) If p is odd, then $U(p^n) \simeq \mathbb{Z}_{p^n - p^{n-1}}$.

(b) $U(2) = \{1\}$ is a trivial group with 1 element.

(c) $U(4) \simeq \mathbb{Z}_2$.

(d) If $n \geq 3$, *then* $U(2^n) \simeq \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$.

Combining Theorems 5.10 and 5.11 we can understand the structure of groups of units $U(n)$ for each n.

Example 5.8. Determine if the groups $U(630)$ and $U(540)$ are isomorphic.

5.2 Warm-ups

Example 5.9. Give an example of an Abelian group of size 12 that is not cyclic.

Solution. $\mathbb{Z}_2 \times \mathbb{Z}_6$ is Abelian since both $\mathbb{Z}_2$ and $\mathbb{Z}_6$ are Abelian. Since 2 and 6 are not relatively prime, this group is not cyclic. □

Example 5.10. Prove that if H and K are two subgroups of an Abelian group, then HK is also a group.

Solution. Note that for every $h \in H$ and $k \in K$ we have $hk = kh$ and thus $HK = KH$. Therefore, by Theorem 5.2, HK is a group. □

5.3 More Examples

Example 5.11. Suppose G is a group, H is a subgroup of G and a is an element of G for which $aH = Ha$. Prove that $\langle a\rangle H$ is a subgroups of G.

Solution. Note that by Theorem 5.2 we need to prove $\langle a\rangle H = H\langle a\rangle$.

First, we will prove by induction on n that $a^nH = Ha^n$ for all $n \geq 0$.
Basis step. $a^0H = eH = H = He = Ha^0$.
Inductive step. Suppose $a^nH = Ha^n$ for some nonnegative integer n. By definition of a^k we have $a^{n+1}H = aa^nH = aHa^n$, by inductive hypothesis. By assumption $aH = Ha$ and thus $aHa^n = Haa^n = Ha^{n+1}$, as desired.
Now, note that $aH = Ha$ implies $a^{-1}aHa^{-1} = a^{-1}Haa^{-1}$ or $Ha^{-1} = a^{-1}H$. Therefore, replacing a by a^{-1} we conclude that $a^{-n}H = Ha^{-n}$ for every positive integer n. Therefore, $a^mH = Ha^m$ for every integer m.

By definition

$$\langle a\rangle H = \bigcup_{n=-\infty}^{\infty} a^nH = \bigcup_{n=-\infty}^{\infty} Ha^n = H\langle a\rangle.$$

Therefore, $\langle a\rangle H$ is a subgroup of G. □

Example 5.12. Let G be a group of order 28, H and K be two subgroups G of orders 4 and 7, respectively. Prove that $G = HK$.

Solution. By Theorem 5.3, we have $|HK| = \dfrac{|H||K|}{|H \cap K|}$. By Lagrange's Theorem, since $H \cap K$ is a subgroup of both H and K, its order must divide both 4 and 7, which means $|H \cap K| = 1$. Therefore, $|HK| = 4 \cdot 7 = 28$. However HK is a subset of G with 28 elements. Since G also has 28 elements we have $HK = G$. □

Example 5.13. Suppose G and H are two groups. Find the necessary and sufficient condition for the group $G \times H$ to be cyclic.

Sketch. First, note that if $G \times H$ is cyclic, then $G \simeq G \times \{e\}$ and $H \simeq \{e\} \times H$ must also be cyclic. Next, note that if both G and H are finite, then the condition is given in Theorem 5.9. So, we are left with the case where G or H is infinite. If one of G or H is the trivial group, then $G \times H$ would be cyclic. Now, assume $G = \langle g \rangle$ is infinite and H is nontrivial. Let $e \neq h \in H$. We will use that to show $G \times H$ cannot be cyclic.

Solution. We claim that $G \times H$ is cyclic if and only if one of the following holds:

(a) $|G| = 1$ and H is cyclic.

(b) G is cyclic and $|H| = 1$.

(c) G and H are finite cyclic groups and $\gcd(|G|, |H|) = 1$.

First note that if (a) or (b) hold then $G \times H \simeq H$ or G, which implies $G \times H$ is cyclic. Also note that Theorem 5.9 implies that if (c) holds then $G \times H$ is cyclic.

Now, suppose $G \times H$ is cyclic. Therefore, by Theorem 3.7, G and H must both be cyclic.

If G and H are both finite, then by Theorem 5.9, the orders of G and H must be relatively prime.

Suppose G or H is infinite. If the other has order 1, then (a) or (b) holds. Otherwise G or H must be infinite and the other must be more than 1 elements.

Suppose $G = \langle a \rangle$ is infinite and H is nontrivial. Let (g, h) be a generator of $G \times H$. There is an integer n for which $(g, h)^n = (e, h)$. Thus, $g^n = e$ and $h^n = e$. Since G has no element of finite order, $g = e$. However this means $(g, h) = (e, h)$ does not generate any element of form (a, h), since $(e, h)^m = (e, h^m)$, and $e \neq a$. □

Example 5.14. Is there a non-trivial group G for which $G \times G \simeq G$?

Solution. Clearly G cannot be finite, otherwise $|G \times G| = |G|$ implies $|G| = 1$, which means G is a trivial group. For infinite groups this is possible. For example let $G = \prod_{n=1}^{\infty} \mathbb{Z}$. Then, $\phi : G \times G \to G$ defined by $\phi(a_1, a_2, \ldots, b_1, b_2, \ldots) = (a_1, b_1, a_2, b_2, \ldots)$ is an isomorphism. (Why?) □

Example 5.15. Describe all right cosets of $SL_n(\mathbb{R})$ in $GL_n(\mathbb{R})$ and find one representative for each one of these coset.

Solution. Each coset is of the form $SL_n(\mathbb{R})A$ for a matrix $A \in GL_n(\mathbb{R})$. Note that every element of $SL_n(\mathbb{R})A$ is of the form BA for some matrix $B \in SL_n(\mathbb{R})$, and hence $\det(BA) = \det(A)$. This means all elements of a coset have the same determinant. So, we need to find one matrix of a given determinant r for each $r \neq 0$.

We will prove that all cosets of $SL_n(\mathbb{R})$ in $GL_n(\mathbb{R})$ are of the form

$$SL_n(\mathbb{R})A_r, \text{ where } A = \begin{pmatrix} r & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \text{ with } r \in \mathbb{R}^*.$$

First note that if $\det X = r$, then $\det(A_r) = \det(X)$ and thus $\det(XA_r^{-1}) = 1$, which implies $SL_n(\mathbb{R})X = SL_n(\mathbb{R})A_r$. Furthermore, if $r \neq s$ then $\det(A_r A_s^{-1}) \neq 1$ and thus $SL_n(\mathbb{R})A_r \neq SL_n(\mathbb{R})A_s$. This completes the proof of the claim. □

Example 5.16. Let n be a positive integer. Give an example of an infinite group that has precisely n elements of finite order.

Solution. Consider the group $\mathbb{Z} \times \mathbb{Z}_n$. If (a, b) is an element of finite order, then a must have finite order and thus $a = 0$. Furthermore $n(0, b) = (0, 0)$ for every $b \in \mathbb{Z}_n$. Thus, this groups has precisely n elements of finite order. □

Example 5.17. Given groups $G_1, \ldots, G_n$, prove that for every k,

$$H_k = \{(e, \ldots, e, g_k, e, \ldots, e) \in \prod_{j=1}^{n} G_j \mid g_k \in G_k\}$$

is a subgroup of $\prod_{j=1}^{n} G_j$, and that $H_k \simeq G_k$.

Solution. Clearly H_k contains the identity of $\prod_{j=1}^{n} G_j$ and thus is non-empty.
Let $(e, \ldots, e, g_k, e, \ldots, e)$ and $(e, \ldots, e, h_k, e, \ldots, e)$ be in H_k. Then,

$$(e, \ldots, e, g_k, e, \ldots, e)(e, \ldots, e, h_k, e, \ldots, e)^{-1} = (e, \ldots, e, g_k h_k^{-1}, e, \ldots, e) \in H_k.$$

Therefore, by the two-step subgroup test H_k is a subgroup of $\prod_{j=1}^{n} G_j$.

Define $\phi : H_k \to G_k$ by $\phi(e, \ldots, e, g_k, e, \ldots, e) = g_k$. This is an isomorphism (why?) and thus $G_k \simeq H_k$. □

Example 5.18. Let G, H, K be groups. Is it true that if $G \times H \simeq G \times K$, then $H \simeq K$?

Solution. This is false. For example if we take $G = \prod_{j=1}^{\infty} \mathbb{Z}$, then $G \times G \simeq G \simeq G \times \{0\}$, but $G \not\simeq \{0\}$. See Example 5.14 for details. □

5.4 Exercises

5.5 Problems for Grading

Exercise 5.1 (10 pts)**.** *Problem 25, Page 151.*

Exercise 5.2 (10 pts)**.** *Problem 48, Page 153.*

Exercise 5.3 (10 pts)**.** *Problem 36, Page 169.*

Exercise 5.4 (10 pts)**.** *Problem 78, Page 171.*

Exercise 5.5 (15 pts)**.** *Suppose H and K are finite subgroups of a group G for which* $\gcd(|H|, |K|) = 1$.

(a) Prove that $H \cap K = \{e\}$.

(b) Prove that $|HK| = |H||K|$.

(c) Deduce that if $|G| = |H||K|$, then $G = HK$.

Hint: For the first part, use Lagrange's Theorem. For the other two parts use the formula for $|HK|$.

Exercise 5.6 (10 pts)**.** *Let $G = \langle (1\ 2\ 3\ 4) \rangle \leq S_{10}$. Find $orb_G(i)$ and $stab(i)$ for $i = 1$ and $i = 5$.*

Exercise 5.7 (10 pts)**.** *Determine which of the following are isomorphic:* $U(800), U(1200), U(1320)$.

5.6 Problems for Practice

Exercise 5.8. *Suppose H and K are subgroups of a group G for which $|H| > \sqrt{|G|}$, and $|K| > \sqrt{|G|}$. Prove that $|H \cap K| > 1$.*

Page 151-154: 16, 21, 22, 47.

Page 167-171: 2, 10, 13, 37, 62, 72

5.7 Challenge Problems

Exercise 5.9. *Let m, n be two positive integers. Find the necessary and sufficient condition on m and n for which there is a group G that has n elements of finite order and m elements of order* 2.

(This problem may or may not be difficult! I am not sure, as I have not tried it.)

6 Week 6

6.1 Exercises

6.1.1 Problems for Grading

Definition 6.1. Let $a_1, \dots, a_n$ be elements in a group G. The intersection of all subgroups of G containing $a_1, \dots, a_n$ is called the **group generated by** $a_1, \dots, a_n$. This group is denoted by $\langle a_1, \dots, a_n \rangle$. A group G is said to be **finitely generated** if there are finitely many elements $a_1, \dots, a_n$ in G for which $G = \langle a_1, \dots, a_n \rangle$.

Exercise 6.1 (10 pts)**.** *Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic. Prove that $\mathbb{Q}$ is not finitely generated.*

Solution. Let G be a subgroup of $\mathbb{Q}$ generated by $r_1 = \dfrac{a_1}{b_1}, \dots, r_n = \dfrac{a_n}{b_n} \in \mathbb{Q}$, with a_j, b_j integers, and let m be the least common multiple of $b_1, \dots, b_n$. Since m/b_j is an integer, $\dfrac{a_j}{b_j} = \dfrac{a_j m}{b_j} \dfrac{1}{m} \in \langle \dfrac{1}{m} \rangle$. Since every subgroup of a cyclic group is cyclic, G is cyclic. □

Exercise 6.2 (10 pts)**.** *Draw the subgroup lattice of $\mathbb{Z}_{18}$.*

Exercise 6.3 (10 pts)**.** *Suppose G is a finite group of order n. Let m be an integer relatively prime to n and $g \in G$ be an element for which $g^m = e$. Prove that $g = e$.*

Exercise 6.4 (10 pts)**.** *Let S be a set and $\mathcal{P}(S)$ be the set consisting of all subsets of S. Define the binary operation Δ on $\mathcal{P}(S)$ by $X \Delta Y = (X \cup Y) \backslash (X \cap Y)$. ($X \Delta Y$ is called the symmetric difference of X and Y.) Prove that $(\mathcal{P}(S), \Delta)$ is an Abelian group.*

7 Week 7

7.1 Normal Subgroups

Example 7.1. Recall that $n\mathbb{Z}$ has n cosets in $\mathbb{Z}$: $n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$. These cosets can be added the same way that elements of $\mathbb{Z}_n$ are added. For example adding $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ can be thought of as adding a and b mod n.

We would like to see if we can replicate this idea for a subgroup of an arbitrary group. In other words, given a subgroup H of a group G we would like to define a "natural" operation on the left cosets of H such that this operation turns the set of all left cosets of G into a group. The most natural operation is perhaps $(aH)(bH) = abH$, however we need to see if this is well-defined, and satisfies properties of a group. Clearly there is at least one coset and thus the set of all left cosets is non-empty.

Well-defined: In order for the operation to be well-defined we need to have $abH = xyH$ if $aH = xH$ and $bH = yH$. In other words, we need know the following:

$$\text{If } a^{-1}x \in H, \text{ and } b^{-1}y \in H, \text{ then } (ab)^{-1}xy \in H.$$

On the other hand,

$$(ab)^{-1}xy \in H \iff b^{-1}a^{-1}xy = (b^{-1}y)(y^{-1}a^{-1}xy) \in H \iff y^{-1}(a^{-1}x)y \in H.$$

The last implication holds because $b^{-1}y \in H$. We know $aH = xH$ holds if $a = e$ and $x \in H$, which implies $a^{-1}x = x$. This means $a^{-1}x$ could be any arbitrary element of H. Therefore, in order for this operation to be well-defined we need $y^{-1}Hy \subseteq H$ for all $y \in G$. So, we have no choice but to assume $y^{-1}Hy \subseteq H$ for all $y \in G$. Once we have this, the rest automatically follows.

Associativity: $[(aH)(bH)](cH) = (abH)(cH) = (ab)cH = a(bcH) = (aH)[(bH)(cH)]$.

Identity: $(eH)(aH) = aH = (aH)(eH)$ for all $a \in H$.

Inverse: $(aH)(a^{-1}H) = eH = (a^{-1}H)(aH)$ for all $a \in H$.

Theorem 7.1. *Suppose H is a subgroup of a group G. The following are equivalent:*

(a) $a^{-1}Ha \subseteq H$ (or $Ha \subseteq aH$) for all $a \in G$.

(b) $aHa^{-1} \subseteq H$ (or $aH \subseteq Ha$) for all $a \in G$.

(c) $aHa^{-1} = H$ (or $aH = Ha$) for all $a \in G$.

(d) $a^{-1}Ha = H$ for all $a \in G$.

Definition 7.1. A subgroup N of a group G is said to be **normal**, denoted by $N \lhd G$, if it satisfies one of the equivalent properties of Theorem 7.1.

Putting these together, we proved the following:

Theorem 7.2. *Suppose N is a subgroup of a group G. Then the set of all left cosets of N in G along with the operation $(aN)(bN) = abN$ form a group if and only if $N \lhd G$.*

Definition 7.2. Let N be a normal subgroup of G. The group consisting of all cosets of N in G with operation $(aN)(bN) = abN$ is called the **factor group** or the **quotient group** of G by N. This group is denoted by G/N or $\dfrac{G}{N}$.

Example 7.2. Here are some examples of normal subgroups:

(a) Every subgroup of an Abelian group is a normal subgroup.

(b) Let G be a group. Every subgroup of $Z(G)$ is a normal subgroup of G.

(c) $A_n \lhd S_n$ for all $n \geq 2$.

(d) $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$ for all n.

Example 7.3. The following are examples of subgroups that are not normal.

(a) $\langle(1\ 2)\rangle \ntriangleleft S_n$ for all $n \geq 3$.

(b) $GL_2(\mathbb{R}) \ntriangleleft GL_2(\mathbb{C})$.

(c) $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}$ is not a normal subgroup of $GL_2(\mathbb{R})$.

Example 7.4. Which well-known group is S_n/A_n isomorphic to?

Theorem 7.3. *Let G be a group for which $G/Z(G)$ is cyclic, then G is Abelian.*

Theorem 7.4. *In every group G we have $G/Z(G) \simeq Inn(G)$.*

Theorem 7.5. *Let p be a prime dividing the order of a finite Abelian group G. Then, G contains an element of order p.*

7.2 Internal Direct Products

We learned before that from two given groups G and H we can create a new group called the external direct product $G \times H$. This allows us to create new groups. Now, given a group K we are interested in decomposing it as $K \simeq G \times H$. Extracting G and H from the given group K requires understanding of the way G and H are related to $G \times H$.

It is not difficult to see the following properties hold:

- $G \times \{e\} \triangleleft G \times H$ and $\{e\} \times H \triangleleft G \times H$,
- $(G \times \{e\}) \cap (\{e\} \times H) = \{(e, e)\}$, and
- $G \times H = (G \times \{e\})(\{e\} \times H)$.

It turns out that these three properties are enough for a group to be decomposed as $G \times H$. In fact this can be done for any number of subgroups.

Definition 7.3. A group G is said to be an **internal direct product** of its subgroups $N_1, \ldots, N_n$ if all of the following hold:

(a) $N_j \triangleleft G$ for every j,

(b) $N_{j+1} \cap (N_1 \cdots N_j) = \{e\}$ for all j.

(c) $G = N_1 \cdots N_n$, and

Theorem 7.6. *Let G be an internal direct product of subgroups $N_1, \ldots, N_n$. Then $G \simeq N_1 \times \cdots \times N_n$.*

Theorem 7.7. *Let p be a prime. Any group of order p^2 is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.*

7.3 Group Homomorphisms

Relaxing one of the conditions of an isomorphism we obtain a homomorphism.

Definition 7.4. Let G and H be two groups. A function $\phi : G \to H$ is said to be a **group homomorphism** if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. When it is clear from the context we simply say ϕ is a "homomorphism" instead of a "group homomorphism".

Example 7.5. The following are examples of homomorphisms:

(a) $f : \mathbb{Z} \to \mathbb{Z}_n$ given by $f(a) = a \mod n$ is a homomorphism.

(b) $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism.

(c) $f : G \to H$ defined by $f(e) = e$ is a homomorphism for every two groups G and H.

(d) Every isomorphism is a homomorphism.

Example 7.6. The following are examples of functions that are not homomorphisms:

(a) $f : G \to G$ given by $f(x) = x^2$ is not a homomorphism if G is not Abelian.

(b) Given a group G and an element $a \in G$ the function $f : G \to G$ given by $f(g) = ag$ is not a homomorphism unless $a = e$.

Theorem 7.8. *Suppose $\phi : G \to H$ be a group homomorphism, and $g \in G$. Then,*

(a) $\phi(e) = e$.

(b) $\phi(a^n) = (\phi(a))^n$ *for all* $n \in \mathbb{Z}$.

(c) $\ker \phi = \{g \in G \mid \phi(g) = e\}$ *is a normal subgroup of* G.

(d) $\phi(a) = \phi(b)$ *if and only if* $a \ker \phi = b \ker \phi$.

(e) ϕ *is one-to-one if and only if* $\ker \phi = \langle e \rangle$.

(f) If $|a|$ *is finite, then* $|\phi(a)|$ *divides* $|a|$.

Theorem 7.9. *Suppose $\phi : G_1 \to G_2$ is a group homomorphism and H is a subgroup of G_1. Then,*

(a) $\phi(H)$ *is a subgroup of* G_2.

(b) If H *is cyclic, then so is* $\phi(H)$.

(c) If H *is Abelian, then so is* $\phi(H)$.

(d) If $H \lhd G_1$, *then* $\phi(H) \lhd \phi(G_1)$.

(e) If $|H| = n$ *is finite, then* $|\phi(H)|$ *divides* n.

(f) If K *is a subgroup of* G_2, *then* $\phi^{-1}(K)$ *is a subgroup of* G_1.

(g) If $K \lhd G_2$, then $\phi^{-1}(K) \lhd G_1$.

Example 7.7. Find the kernel of each of the following:

(a) $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\star$.

(b) $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(a) = a \mod n$.

7.4 Warm-ups

Example 7.8. Prove that each of the following is a homomorphism:

(a) $f : \mathbb{R}^* \to \mathbb{R}^+$ defined by $f(x) = |x|$.

(b) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $f(x, y) = x + y$.

Solution. (a) $f(xy) = |xy| = |x||y| = f(x)f(y)$, by properties of absolute value.
(b) $f((a, b) + (x, y)) = f(a + x, b + y) = (a + x) + (b + y) = (a + b) + (x + y) = f(a, b) + f(x, y)$. □

Example 7.9. Prove that for every group G, $\dfrac{G}{\langle e\rangle} \simeq G$.

Solution. Define $f : G \to G/\langle e\rangle$ by $f(g) = g\langle e\rangle$. We will prove f is an isomorphism.
One-to-one: If $f(g) = f(h)$, then $g\langle e\rangle = h\langle e\rangle$, hence $g^{-1}h \in \langle e\rangle$, which implies $g^{-1}h = e$, i.e. $g = h$.
Onto: Every element of $G/\langle e\rangle$ is of the form $a\langle e\rangle$ and thus $f(a) = a\langle e\rangle$ is in the image of f.
Operation-preserving: $f(ab) = ab\langle e\rangle = (a\langle e\rangle)(b\langle e\rangle) = f(a)f(b)$. □

7.5 More Examples

Example 7.10. Suppose a is an element of order 2 in a group G for which $\langle a\rangle \lhd G$. Prove that $a \in Z(G)$.

Solution. Let $g \in G$. We need to prove $ag = ga$. Since the order of a is 2, we have $\langle a\rangle = \{e, a\}$, and thus $g\langle a\rangle g^{-1} = \{e, gag^{-1}\}$. Since $\langle a\rangle \lhd G$ we must have $a = gag^{-1}$ and thus $ag = ga$, as desired. □

Example 7.11. Let G be a group, N be a normal subgroup of G and H be a subgroup of G. Then, NH is a subgroup of G. If H is normal in G, then $NH \lhd G$.

Solution. Note that $NH = \bigcup\limits_{h\in H} Nh$ and $HN = \bigcup\limits_{h\in H} hN$. Since N is a normal subgroup we have $hN = Nh$ and therefore, $HN = NH$. Theorem 5.2 implies that NH is a subgroup of G.

Now, assume $H \lhd G$, and let $g \in G$. We have $NHg = NgH = gNH$, since both N and H are normal subgroups. Therefore, $NH \lhd G$, as desired. □

Example 7.12. Let G be a finite group. Suppose $f : G \to G$ is a homomorphism with the property that $f(x) = x$ if and only if $x = e$. Prove that $G = \{g^{-1}f(g) \mid g \in G\}$.

Solution. Since G is finite, in order to prove the claim we need to show if g, h are two distinct elements of G, then $g^{-1}f(g) \neq h^{-1}f(h)$. This would prove both G and the given set have the same number of elements and since the gives set is a subset of G, the two sets must be the same.

Suppose $g^{-1}f(g) = h^{-1}f(h)$. We have $hg^{-1} = f(h)(f(g))^{-1}$. By properties of homomorphism we obtain $hg^{-1} = f(h)f(g^{-1}) = f(hg^{-1})$. By assumption, since $hg^{-1} = f(hg^{-1})$ we have $hg^{-1} = e$ which implies $h = g$, as desired. □

Example 7.13. Is it true that if N is a normal subgroup of a group G, then $G \simeq N \times \dfrac{G}{N}$?

Solution. This is false. Consider $2\mathbb{Z}$ as a subgroup of $\mathbb{Z}$. We know $\mathbb{Z}$ only has one element of finite order. However $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ has two elements of finite order and thus $\mathbb{Z} \not\simeq 2\mathbb{Z} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$. □

Example 7.14. Suppose N, H are normal subgroups of a group G for which $N \cap H = \langle e \rangle$. Prove that $ab = ba$ for all $a \in N, b \in H$.

Solution. We need to prove $aba^{-1}b^{-1} = e$. Note that since N is a normal subgroup $ba^{-1}b^{-1} \in N$ and thus $aba^{-1}b^{-1} \in N$. Similarly, since H is a normal subgroup of G, $aba^{-1} \in H$ and thus $aba^{-1}b^{-1} \in H$. Therefore, $aba^{-1}b^{-1} \in N \cap H$ and thus $aba^{-1}b^{-1} = e$, which implies $ab = ba$, as desired. □

Example 7.15. Let H be a subgroup of a group G. Prove that the normalizer of H in G, defined by $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$, is the largest subgroup of G for which H is normal.

Solution. First note $H \subseteq N_G(H)$ and thus $N_G(H)$ contains H and hence is non-empty. Next, assume $a, b \in N_G(H)$. We have $abH(ab)^{-1} = a(bHb^{-1})a^{-1} = aHa^{-1} = H$, and thus $ab \in N_G(H)$. On the other hand since $aHa^{-1} = H$ we obtain $a^{-1}aHa^{-1}a = a^{-1}Ha$, which implies $H = a^{-1}Ha$ and hence $a^{-1} \in N_G(H)$. Therefore, $N_G(H)$ is a subgroup of G containing H.

By definition of $N_G(H)$, H is normal in $N_G(H)$. If H is normal in K, then for every $x \in K$ we have $xHx^{-1} = H$ and thus $x \in N_G(H)$, which means $K \subseteq N_G(H)$, as desired. □

Example 7.16. In the definition of internal direct product we assume $N_{j+1} \cap (N_1 \cdots N_j) = \langle e \rangle$. Can we replace this assumption by $N_i \cap N_j = \langle e \rangle$, for every $i \neq j$?

7.6 Exercises

7.6.1 Problems for Grading

Exercise 7.1 (10 pts)**.** *List all subgroups of S_3 and determine which ones are normal subgroups.*

Exercise 7.2 (10 pts)**.** *Prove that if $\phi : G \to H$ is a group homomorphism, g is an element of G and n is an integer, then $\phi(g^n) = (\phi(g))^n$. Deduce that if N be a normal subgroup of G and $g \in G$ and $n \in \mathbb{Z}$ we have $(aN)^n = a^n N$.*

Hint: For the second part use $\phi : G \to G/N$ defined by $\phi(a) = aN$.

Exercise 7.3 (10 pts)**.** *Let G be a group.*

(a) Prove that if $Inn(G)$ is cyclic, then $Inn(G)$ must be a trivial group.

(b) Suppose N is a subgroup of $Z(G)$ for which G/N is cyclic. Prove that G is Abelian.

Hint: See the proof of Theorem 7.4.

Exercise 7.4 (10 pts)**.** *Suppose N is a subgroup of index 1 or 2 in a group G. Prove that $N \lhd G$. Prove that the result does not hold if the index is 3.*

Exercise 7.5 (10 pts)**.** *Page 188, Problem 7.*

Exercise 7.6 (10 pts)**.** *Page 190, Problem 50.*

Exercise 7.7 (20 pts)**.** *Page 191, Problem 62.*

Exercise 7.8 (10 pts)**.** *Page 206, Problem 8.*

Exercise 7.9 (10 pts)**.** *Page 207, Problem 32.*

7.6.2 Problems for Practice

Exercise 7.10. *Suppose a group G is a union of a family of proper normal subgroups each two of which only intersect trivially. Prove that G is Abelian.*

Exercise 7.11. *Consider the group $G = \dfrac{\mathbb{Q}}{\mathbb{Z}}$. Prove that*

(a) Every element of G has finite order.

(b) For every positive integer n, the group G has a unique subgroup of order n.

Page 189: 23, 38, 43, 66, 69, 72.
Page 206: 24, 10, 33, 35.

7.6.3 Challenge Problems

Exercise 7.12. *By an example show that there is a group G, an element $g \in G$, and a subgroup H of G for which $gHg^{-1} \subsetneqq H$. How do you reconcile this with Theorem 7.2?*

Exercise 7.13. *Prove that if a group is a union of three of its proper subgroups if and only if G has a normal subgroup N for which $G/N \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.*

7.7 Summary

- To prove a subgroup N is normal in a group G we need to show $gNg^{-1} \subseteq G$ for all $g \in G$.
- To prove a subgroup N is not normal in a group G we need to show there exist $a \in N, g \in G$ for which $gag^{-1} \notin N$.
- If $N \lhd G$, then $Ng = gN$ and G/N becomes a group under the operation $(aN)(bN) = abN$.
- If $G/Z(G)$ is cyclic, then G is Abelian, i.e. $G = Z(G)$ and thus $G/Z(G)$ is the trivial group.
- Every group of order p^2, where p is a prime, is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$, and thus it is Abelian.
- Any operation-preserving map is called a homomorphism.
- Homomorphisms map the identity element to the identity element.
- Homomorphisms map every subgroup to a subgroup.
- Kernel of every homomorphism is a normal subgroup.
- A homomorphism is one-to-one if and only if its kernel is trivial.

8 Week 8

8.1 Isomorphism Theorems

Theorem 8.1 (First Isomorphism Theorem)**.** *Suppose $\phi : G \to H$ is a group homomorphism. Then,* $\dfrac{G}{\ker \phi} \simeq \phi(G)$.

Example 8.1. Prove that for every integer n we have $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n$.

Example 8.2. Prove that $\dfrac{GL_n(\mathbb{R})}{SL_n(\mathbb{R})} \simeq \mathbb{R}^\star$.

Example 8.3. Every normal subgroup of a group G is the kernel of some homomorphism from G to some group.

Theorem 8.2. *Let N be a normal subgroup of a group G.*

(a) Every subgroup of G/N is of the form H/N, where H is a subgroup of G containing N. Furthermore if H is a subgroup of G containing N, then H/N is a subgroup of G/N.

(b) Every normal subgroup of G/N is of the form K/N, where K is a normal subgroup of G containing N. Furthermore if K is a subgroup of G containing N, then K/N is a subgroup of G/N.

Example 8.4. Suppose H is a subgroup of a group G. Define $\phi : N_G(H) \to Aut(H)$ by $\phi(a) = f_a$, where $f_a(x) = axa^{-1}$. Use this to prove that $N_G(H)/C_G(H)$ is isomorphic to a subrgoup of $Aut(H)$.

Theorem 8.3 (Second Isomorphism Theorem)**.** *Suppose K is a subgroup of a group G, and N is a normal subgroup of G. Then, $K \cap N$ is a normal subgroup of K, and*

$$\frac{KN}{N} \simeq \frac{K}{K \cap N}.$$

Theorem 8.4 (Third Isomorphism Theorem)**.** *Suppose M and N are normal subgroups of a group G, and $N \leq M$. Then,*

$$\frac{(G/N)}{(M/N)} \simeq \frac{G}{M}.$$

8.2 Fundamental Theorem of Finite Abelian Groups

The purpose of this section is to classify all finite Abelian groups.

Theorem 8.5 (Fundamental Theorem of Finite Abelian Groups)**.** *Every finite Abelian group G is isomorphic to a direct product of cyclic groups of prime-power order. Furthermore, the number of terms and the order of these cyclic groups is uniquely determined by G.*

Before we prove the theorem, let's look at some of its applications.

Example 8.5. List all Abelian groups of order 120 up to isomorphism.

Theorem 8.6. *If G is an Abelian group of order n, and d is a positive divisor of n, then G has a subgroup of order d.*

The idea of the proof of the Fundamental Theorem of Finite Abelian Groups is to break up the group into groups of prime-power order and then break those up into cyclic subgroups,

8.3 Rings

Definition 8.1. A **ring** is a set R along with two binary operations, usually denoted by $+$, and $\cdot$ for which all of the following hold:

- $(R, +)$ is an Abelian group.
- $(R, \cdot)$ is associative.
- The binary operation $\cdot$ distributes over $+$. In other words, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$, for all $a, b, c \in R$.

A ring is said to be a ring with **unity** if $(R, \cdot)$ has a non-zero identity element. In other words, there is $0 \neq e \in R$ for which $a \cdot e = e \cdot a = a$ for all $a \in R$. A ring is said to be **commutative** if $(R, \cdot)$ is Abelian, i.e. $a \cdot b = b \cdot a$ for all $a, b \in R$. A ring is said to be **trivial** if it has only one element, i.e. $R = \{0\}$.

Remark. $a \cdot b$ is often written as ab. The additive identity, i.e. the identity of $(R, +)$, is typically denoted by 0. The additive inverse of an element a is usually denoted by $-a$. We will also use the same order of operations that we use for real numbers. For example $ab + ac$ is the same as $(ab) + (ac)$.

Example 8.6. Here are some examples of rings.

(a) $\mathbb{Z}$ under integer addition and multiplication is a commutative ring with unity.

(b) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ under the usual addition and multiplication are all commutative rings with unity.

(c) $\mathbb{Z}_n$ under addition and multiplication mod n is a commutative ring with unity.

(d) $M_n(\mathbb{R})$ under matrix addition and matrix multiplication is a non-commutative ring with unity, if $n \geq 2$.

(e) $n\mathbb{Z}$ under integer addition and multiplication is a commutative ring without a unity if $n \geq 2$.

(f) $C(\mathbb{R})$, the set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, under the usual addition and multiplication of functions is a commutative ring with unity.

Example 8.7. The following examples are not rings.

(a) Even though S_n is a group, we cannot turn it into a ring under any natural operation because it is not Abelian.

(b) $C(\mathbb{R})$ under addition and composition is not a ring. For it to be a ring we need $f \circ (g+h) = f \circ g + f \circ h$ for all $f, g, h \in C(\mathbb{R})$. This is not true for example if we take $f(x) = x^2, g(x) = h(x) = x$.

Theorem 8.7 (Properties of Rings)**.** *Let a, b, c be elements of a ring R. Then,*

(a) $a0 = 0a = 0$.

(b) $a(-b) = (-a)b = -(ab)$.

(c) $(-a)(-b) = ab$.

(d) $a(b-c) = ab - ac$, *and* $(b-c)a = ba - ca$.

If R has a unity element 1, then

(e) $(-1)a = a(-1) = -a$.

(f) $(-1)(-1) = 1$.

Theorem 8.8. *If a ring has a unity then this unity is unique. If a ring element has a multiplicative inverse then this inverse is unique.*

Remark. The unity of a ring with unity is denoted by 1. The multiplicative inverse of an element a in a ring is denoted by a^{-1}.

Definition 8.2. In a ring with unity an element a is called a **unit** if it has a multiplicative inverse.

Theorem 8.9. *Let R be a ring with unity. Then, the set of all units of R along with the ring multiplication forms a group.*

Definition 8.3. Let R be a ring with unity. The multiplicative group consisting of all units of R is called the **group of units** of R and is denoted by $U(R)$.

Example 8.8. The following are some examples of groups of unity.

(a) $U(\mathbb{R}) = \mathbb{R}^\star$.

(b) $U(\mathbb{Z}_n) = U(n)$.

(c) $U(M_n(\mathbb{R})) = GL_n(\mathbb{R})$.

(d) $U(\mathbb{Z}) = \{1, -1\}$.

Definition 8.4. A subset S of a ring R is called a **subring** of R if S is a ring with the operation of R.

Theorem 8.10 (Subring Test)**.** *A non-empty subset S of a ring R is a subring if and only if for every $x, y \in S$ we have $x - y \in S$, and $xy \in S$.*

Definition 8.5. The **centralizer** of an element a of a ring R is defined and denoted by

$$C_R(a) = \{r \in R \mid ra = ar\}.$$

Similarly when S is a subset of R, then its **centralizer** is defined and denoted by

$$C_R(S) = \{r \in R \mid sr = rs \text{ for all } s \in S\}.$$

When the underlying ring R is clear from the context, we often use $C(a)$ and $C(S)$ instead of $C_R(a)$ and $C_R(S)$. The **center** of a ring R is defined and denoted below

$$Z(R) = \{r \in R \mid ra = ar \text{ for all } a \in R\}.$$

Theorem 8.11. *Let R be a ring, S be a subset of R, and a be an element of R. Then $C(a), C(S)$ and $Z(R)$ are subrings of R.*

8.4 Warm-ups

Example 8.9. Prove that all subgroups of $\mathbb{Z}$ are also subrings.

Solution. We know every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some integer n. This set is closed under subtraction, since $na - nb = n(a - b) \in n\mathbb{Z}$. Therefore, it is a subring of $\mathbb{Z}$. □

Example 8.10. Let u be an element of a commutative ring with identity R. Prove that u is a unit if and only if $\langle u \rangle = R$.

Solution. Suppose u is a unit. If $r \in R$, then $r = uu^{-1}r \in \langle u \rangle$. Thus, every element of R is in $\langle u \rangle$. Therefore, $\langle u \rangle = R$.

Suppose $\langle u \rangle = R$. Thus, $1 = uv$ for some $v \in R$, i.e. u is a unit. □

8.5 More Examples

Example 8.11. Suppose m, n are two positive integers. Prove that $\dfrac{n\mathbb{Z}}{mn\mathbb{Z}} \simeq \mathbb{Z}_m$.

Solution. Define $\phi : n\mathbb{Z} \to \mathbb{Z}_m$ by $\phi(na) = a \mod m$.

Onto: Since a could be any integer, ϕ is onto.

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

$\ker \phi = \{na \mid a \equiv 0 \mod m\} = nm\mathbb{Z}$.

Therefore, by the First Isomorphism Theorem $\dfrac{n\mathbb{Z}}{nm\mathbb{Z}} \simeq \mathbb{Z}_m$. □

Example 8.12. Consider an Abelian group G. Prove that $D = \{(g, g) \mid g \in G\}$ is a normal subgroup of $G \times G$, and $\dfrac{G \times G}{D} \simeq G$.

Solution. Define $\phi : G \times G \to G$ by $\phi(x, y) = xy^{-1}$.

Onto: If $g \in G$, then $\phi(g, e) = g$ and thus ϕ is onto.

Homomorphism: $\phi(x_1x_2, y_1y_2) = x_1x_2(y_1y_2)^{-1} = x_1x_2y_2^{-1}y_1^{-1} = x_1y_1^{-1}x_2y_2^{-1} = \phi(x_1, y_1)\phi(x_2, y_2)$. Here we use the fact that G is Abelian.

$\ker \phi = \{(x, y) \in G \times G \mid xy^{-1} = e\} = \{(x, y) \in G \times G \mid x = y\} = D$.

Therefore, $D \lhd G \times G$. Furthermore, by the First Isomorphism Theorem, $\dfrac{G \times G}{D} \simeq G$. □

Example 8.13. Prove that for every positive integer n, $\dfrac{\mathbb{C}^\star}{\langle e^{2\pi i/n} \rangle} \simeq \mathbb{C}^\star$.

Solution. Define $\phi : \mathbb{C}^\star \to \mathbb{C}^\star$ by $\phi(z) = z^n$.

Onto: If $z \in \mathbb{C}^\star$, then we know the equation $x^n = z$ has a root, and thus ϕ is onto,

Homomorphism: Follows from the fact that $(zt)^n = z^n t^n$ for every $z, t \in \mathbb{C}^\star$.

$\ker \phi = \{z \in \mathbb{C}^\star \mid z^n = 1\} = \{e^{2\pi ik/n} \mid k = 0, 1, \ldots, n - 1\} = \langle e^{2\pi i/n} \rangle$. The result then follows from the First Isomorphism Theorem. □

Example 8.14. Suppose G, H, K are finite Abelian groups for which $G \times H \simeq G \times K$. Prove that $H \simeq K$.

Solution. First, write down G, H, and K as products of cyclic groups of prime-power order. Suppose p is a prime, and n is a positive integer. We need to show the number of copies of $\mathbb{Z}_{p^n}$ in H and K are the same. Suppose the number of copies of $\mathbb{Z}_{p^n}$ in G, H, K are a, b, c, respectively. Thus, there are $a + b$ and $a + c$ copies of $\mathbb{Z}_{p^n}$ in $G \times H$ and $G \times K$, respectively. By the Fundamental Theorem of Finite Abelian Groups, $a + b = a + c$ and thus $b = c$. Since this is true for all p and n we must have $H \simeq K$, as desired. □

Example 8.15. Prove that the intersection of any collection of subrings of a ring R is a subgring.

Solution. We will use the subring test.

Suppose $R_i, i \in I$ is a collection of subrings of R. We know $0 \in R_i$ for all $i \in I$ and thus $\bigcap_{i\in I} R_i$ is non-empty. Assume $a, b \in \bigcap_{i\in I} R_i$. By definition of intersection, $a, b \in R_i$ for all $i \in I$. Since R_i is a subring, $a - b \in R_i$ and thus $a - b \in \bigcap_{i\in I} R_i$. This completes the proof. □

Example 8.16. Suppose R satisfies all properties of a ring, except we do not know $(R, +)$ is Abelian. Furthermore, assume R has a unity. Prove that R must be a ring.

Solution. We only need to show $a + b = b + a$ for all $a, b \in R$. Using distributive property from the left we have

$$(a + b)(1 + 1) = (a + b)1 + (a + b)1 = a + b + a + b.$$

Using distributive property from the right we obtain

$$(a + b)(1 + 1) = a(1 + 1) + b(1 + 1) = a1 + a1 + b1 + b1 = a + a + b + b.$$

Therefore, $a + b + a + b = a + a + b + b$. By the cancellation property we obtain $b + a = a + b$, as desired. □

Recall that since $(R, +)$ is a group we can recursively define na for every $a \in R$ and $n \in \mathbb{Z}$. Below we define a^n for positive n.

Definition 8.6. Let a be a ring element. We define a^n for positive integer n recursively as bellow:

- $a^1 = a$.
- $a^{n+1} = aa^n$ for every $n > 0$.

Example 8.17. Suppose a, b are ring elements and m, n are positive integers.

(a) Prove that $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

(b) Prove that if $ab = ba$, then $(ab)^n = a^n b^n$ for every positive integer n.

(c) Prove that if $ab = ba$, then for every positive integer n we have

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n-1} ab^{n-1} + b^n.$$

Solution. (a) We will prove these by induction on m.
Basis step: $a^1 a^n = aa^n = a^{n+1}$, as desired.
Inductive step: $a^{n+1} a^m = aa^n a^m = aa^{n+m} = a^{1+n+m}$, as desired. Here we use the definition of a^k and the inductive hypothesis.

Basis step: $(a^m)^1 = a^m = a^{m1}$, by definition.
Inductive step: $(a^m)^{n+1} = a^m (a^m)^n = a^m a^{mn}$. This equals a^{m+mn} by the previous part of the theorem. Therefore, $(a^n)^{m+1} = a^{n(m+1)}$.
(b) and (c) can both be proved by induction on n. □

Example 8.18. Suppose a, b are in a ring R and $m, n \in \mathbb{Z}$. Prove that:

(a) $(ma)(nb) = mnab$.

(b) If n is positive, then $(ma)^n = m^n a^n$.

Solution. (a) First, we will prove the statement for $m = 1$. We need to prove $a(nb) = nab$, for all $n \in \mathbb{Z}$. First assume $n \geq 0$.
Basis step: When $n = 0$ we have $a(0b) = a0 = 0 = 0ab$, as desired.
Inductive step: Assume $a(nb) = nab$. We have $a((n+1)b) = a(b+nb) = ab+a(nb) = ab+nab = (n+1)ab$. Here we used the definition of a^k in the group $(R, +)$, the distributive property and the inductive hypothesis.

Now, note that $a(-nb) = a(-(nb)) = -a(nb) = -nab$, if n is a positive integer. This completes the proof for $m = 1$.

Now, we will prove $(ma)(nb) = mnab$ for $m \geq 0$ by induction on m.
Basis step: For $m = 0$ we have $(0a)(nb) = 0(nb) = 0 = 0ab$, as desired.
Inductive step: Suppose $(ma)(nb) = mnab$. Then, $((m+1)a)(nb) = (a+ma)(nb) = a(nb) + (ma)(nb) = a(nb) + mnab = nab + mnab = (m+1)(nab) = (mn+n)ab$, as desired. Here we used the properties of exponents in the group $(R, +)$, the inductive hypothesis and the case where $m = 1$ proved above.

We also note that $(-ma)(nb) = -(ma)(nb) = -(mnab) = -mnab$ if m is positive. This completes the proof.

(b) We will prove this by induction on n.
Basis step: $(ma)^1 = ma = m^1 a^1$, as desired.
Inductive step: $(ma)^{n+1} = (ma)(ma)^n = (ma)(m^n a^n) = (mm^n)(aa^n) = m^{n+1}a^{n+1}$, as desired. □

Example 8.19. For a ring R and a positive integer n, let $M_n(R)$ be the ring consisting of all $n \times n$ matrices whose entries are elements of R. Prove that $M_n(R)$ along with the usual matrix addition and matrix multiplication is a ring. If R has a unity, then $M_n(R)$ also has a unity.

8.6 Exercises

8.6.1 Problems for Grading

Exercise 8.1 (10 pts)**.** *Prove the Second Isomorphism Theorem.*

Hint: Write down a homomorphism $\phi : K \to \dfrac{KN}{N}$ by $\phi(x) = xN$. Then apply the First Isomorphism Theorem.

Exercise 8.2 (10 pts)**.** *Prove the Third Isomorphism Theorem.*

Hint: Write a homomorphism $\phi : \dfrac{G}{N} \to \dfrac{G}{M}$ by $\phi(gN) = gM$. Then, apply the First Isomorphism Theorem.

Exercise 8.3 (10 pts)**.** *Suppose G is a finite Abelian group of order n such that for every prime p dividing n, there are precisely $p-1$ elements of order p in G. Prove that G is cyclic.*

Exercise 8.4 (10 pts)**.** *Page 207, Problem 34. (Note the word "onto".)*

Hint: Use the First Isomorphism Theorem and Example 5, Page 144.

Exercise 8.5 (10 pts)**.** *Page 221, Problem 18.*

Exercise 8.6 (10 pts)**.** *Page 221, Problem 23.*

Exercise 8.7 (10 pts)**.** *Page 233, Problem 23.*

Exercise 8.8 (10 pts)**.** *Page 235, Problem 50.*

8.6.2 Problems for Practice

Exercise 8.9. *Let p be a prime. Determine the number of homomorphisms $\phi : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$. Do the same for $\phi : \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ times}} \to \mathbb{Z}_p$.*

Page 208-209: 37, 38, 49, 56, 58, 64.

Page 221: 22, 24, 30, 32.

Page 233: 29, 30, 42, 43.

8.6.3 Challenge Problems

Exercise 8.10. *Prove that if in a ring R we have $x^3 = x$ for all $x \in R$, then R is commutative. Can you do this problem when 3 is replaced by 4? What about 5? What about an arbitrary integer $n \geq 2$?*

8.7 Summary

- To prove a group H is isomorphic to a factor group G/N, we often:
  - Write down a homomorphism $\phi : G \to H$.
  - Prove ϕ is both a homomorphism and onto,
  - Show $\ker \phi = N$.
  - Using the First Isomorphism Theorem we obtain the result.
- Every finite Abelian group is isomorphic to an external direct product of cyclic groups of prime-power. This group is unique.
- To check R along with two operations $+$ and $\cdot$ is a ring we need to show:
  - $(R, +)$ is an Abelian group.
  - $(R, \cdot)$ is associative.
  - Multiplication distributes over addition from both sides.

9 Week 9

We will now focus on the study of different kinds of rings.

9.1 Integral Domains

For this section we will only focus on commutative rings.

Definition 9.1. A **zero-divisor** is a nonzero element a of a commutative ring R such that $ab = 0$ for some nonzero element $b \in R$.

Definition 9.2. An **integral domain** is a commutative ring with unity that has no zero-divisors.

Example 9.1. The following are examples of integral domains:

(a) $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$.

(b) $\mathbb{Z}_p$ if p is a prime.

Example 9.2. The following are not integral domains:

(a) $M_n(\mathbb{R})$ for $n \geq 2$ is not commutative and has zero-divisors, and thus is not an integral domain.

(b) $\mathbb{Z}_6$ has zero-divisors and thus it is not an integral domain.

Theorem 9.1. *If in an integral domain we have $ab = ac$ for three elements a, b, c with $a \neq 0$, then $b = c$.*

9.2 Fields

Definition 9.3. A **field** is commutative ring with unity for which every non-zero element is a unit.

Example 9.3. $\mathbb{R}, \mathbb{Q}$ and $\mathbb{Z}_p$, where p is a prime are all fields.

Example 9.4. $\mathbb{Z}$ and $\mathbb{Z}_n$ are not fields if $n > 1$ is composite.

Theorem 9.2. *Every finite integral domain is a field.*

Definition 9.4. The **characteristic** of a ring R, denoted by char$R$, is the least positive integer n for which $na = 0$ for all $a \in R$. If no such integer exists we say the characteristic of R is 0.

Theorem 9.3. *Let R be a ring with unity 1. If the order of 1 is finite, then the characteritic of R is equal to the order of 1. If the order of 1 is infinity, then the characteristic of R is 0.*

Theorem 9.4. *Characteristic of an integral domain is 0 or prime.*

9.3 Ideals and Factor Rings

Suppose S is a subring of a ring R. Since $(R, +)$ is an Abelian group we can consider the factor group R/S. We now find the necessary and sufficient condition for this group to be a ring under a natural multiplication. We already know $(R/S, +)$ is an Abelian group. We define $(a + S)(b + S) = ab + S$. We need to see when this operation is well-defined, associative, and satisfies the distributive property.

Well-defined: Suppose $a + S = x + S$ and $b + S = y + S$. We need to have $ab + S = xy + S$. In other words we need to have the following:

$$\text{If } a - x \in S, \text{ and } b - y \in S, \text{ then } ab - xy \in S.$$

We write $a = x + s_1$, and $b = y + s_2$ for some $s_1, s_2 \in S$. Thus, we have $ab = xy + xs_2 + s_1y + s_1s_2$, which implies $ab - xy = xs_2 + s_1y + s_1s_2$. Since S is a subring, $s_1s_2 \in S$. So, we need to make sure $xs_2 + s_1y \in S$, for all $x, y \in R$ and all $s_1, s_2 \in S$. Letting $s_1 = 0$ we obtain $xs_2 \in S$ for all $s_2 \in S$ and all $x \in R$. Similarly we need to have $s_1y \in S$ as long as $s_1 \in S$. So we have to make this assumption in order to be able to proceed further.

Associative: For every $a, b \in R$ we have

$$\begin{aligned}(a + S)[(b + S)(c + S)] &= (a + S)(bc + S)\\ &= a(bc) + S\\ &= (ab)c + S\\ &= (ab + S)(c + S)\\ &= [(a + S)(b + S)](c + S),\end{aligned}$$

and thus multiplicative is associative.

Distributive: For every $a, b, c \in R$ we have

$$\begin{aligned}(a + s)[(b + S) + (c + S)] &= (a + S)[(b + c) + S]\\ &= a(b + c) + S\\ &= (ab + ac) + S = (ab + S) + (ac + S)\\ &= (a + S)(b + S) + (a + S)(c + S).\end{aligned}$$

Similarly multiplication distributes over addition from the right.

Definition 9.5. A subring I of a ring R is said to be an **ideal** (or a two-sided ideal) if for every $a \in I$ and every $r \in R$ both ar and ra are in I.

In the above discussion we proved the following:

Theorem 9.5. *Let S be a subring of a ring R. Then, R/S under the operations*

$$(a + S) + (b + S) = (a + b) + S; \; (a + S)(b + S) = ab + S$$

is a ring if and only if S is an ideal of R.

Theorem 9.6 (Ideal Test)**.** *A non-empty subset I of a ring R is an ideal if and only if the following are satisfied:*

- $a - b \in I$ *for all* $a, b \in I$.
- $ar, ra \in I$ *for all* $r \in R$ *and* $a \in I$.

Example 9.5. The following are examples of ideals:

(a) All subrings of $\mathbb{Z}$ are ideals.

(b) If a is an element of a commutative ring R with unity, then $\langle a \rangle = \{ar \mid r \in R\}$ is an ideal of R. This ideal is called the **ideal generated by** a.

Example 9.6. The following are not ideals:

(a) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$, but is not an ideal.

(b) $\{(a, a) \mid a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$, but is not an ideal.

We will now explore the properties of factor rings.

Question. When is a factor ring R/I an integral domain? When is it a field?

For a factor ring to be an integral domain we need the following:

- R/I must be a commutative ring. To fulfill this we will assume R is commutative. Note that this assumption is not necessary, but it is sufficient.
- R/I must have a unity. To fulfill this we will assume R has a unity. Similar to above this assumption is only sufficient but not necessary.
- R/I must have no zero-divisors. This means we need to have the following

  $$(a + I)(b + I) = 0 + I \Rightarrow a + I = 0 + I \text{ or } b + I = 0 + I.$$

  This is equivalent to

  $$ab \in I \Rightarrow a \in I \text{ or } b \in I.$$

Similar to above, in order for R/I to be a field we need R/I to be a commutative ring with unity. For this to be fulfilled we will assume R is a commutative ring with unity. We also need every non-zero element of R/I to have an inverse. In other words we need to make sure if $a \notin I$, then $(a + I)(b + I) = 1 + I$ for some $b \in R$. This means for every $a \notin I$ there must exist b for which $1 - ab \in I$. This means, $a + I$ has an inverse if and only if

$$1 \in \{x + ab \mid x \in I, \text{ and } b \in R\}.$$

Note that the set $J = \{x + ab \mid x \in I, \text{ and } b \in R\}$ is an ideal of R. It is not difficult to see 1 belongs to an ideal J if and only if that ideal is the entire ring R. Therefore, in essense this condition is equivalent to saying there is no ideal J for which $I \subsetneq J \subsetneq R$. Such ideals are called maximal.

Definition 9.6. Let I be an ideal of a commutative ring R.

- We say I is **prime** if it satisfies the following: If $ab \in I,$ then $a \in I$ or $b \in I$.
- We say I is **maximal** if $I \neq R$, and there is no ideal J for which $I \subsetneq J \subsetneq R$.

In the above discussion, we proved the following:

Theorem 9.7. *Let I be an ideal in a commutative ring R with unity .*

- *R/I is an integral domain if and only if I is prime.*
- *R/I is a field if and only if I is a maximal ideal of R.*

Since every field is an integral domain an immediate consequence of the above theorem is the following:

Corollary 9.1. A maximal ideal of a commutative ring with unity is prime.

Example 9.7. Some examples of maximal and prime ideals are listed below:

(a) $\{0\}$ is a prime ideal of $\mathbb{Z}$, but is not maximal.

(b) If p is a prime integer, then $p\mathbb{Z}$ is a maximal and prime ideal of $\mathbb{Z}$.

9.4 Ring Homomorphisms and Ring Isomorphisms

Definition 9.7. Let R and S be two rings. A function $\phi : R \to S$ is said to be a **ring homomorphism** if $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. This homomorphism is said to be an **isomorphism** if ϕ is also bijective. When there is an isomorphism from a ring R to a ring S, then we say R and S are **isomorphic** and we write $R \simeq S$.

Theorem 9.8. *Suppose $\phi : R \to S$ is a ring homomorphism, $a, b \in R$, n is a positive integer, and m is an integer. Then,*

(a) $\phi(a^n) = (\phi(a))^n$, and $\phi(ma) = m\phi(a)$.

(b) The image of every subring of R is a subring of S, and the pre-image of every subring of S is a subring of R.

(c) The image of an ideal of R is an ideal of the range $\phi(R)$, and the pre-image of any ideal of S is an ideal of R.

(d) If R is commutative, then so is $\phi(R)$.

(e) If R has the unity 1, and $\phi(R)$ has at least two elements, then $\phi(1)$ is the unity of $\phi(R)$.

(f) $\ker\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

(g) ϕ is one-to-one if and only if $\ker\phi = \{0\}$.

Theorem 9.9. *Ring isomorphism is an equivalence relation. In other words if R, S and T are rings, then*

(a) $R \simeq R$. *Furthermore,* $id : R \to R$ *is an isomorphism.*

(b) If $R \simeq S$, *then* $S \simeq R$. *Furthermore, if* $\phi : R \to S$ *is an isomorphism, then* $\phi^{-1} : S \to R$ *is also an isomorphism.*

(c) If $R \simeq S$, *and* $S \simeq T$, *then* $R \simeq T$. *Furthremore, if* $\phi : R \to S$ *and* $\psi : S \to T$ *are isomorphisms, then* $\psi \circ \phi : R \to T$ *is an isomorpshim,*

Theorem 9.10 (First Isomorphism Theorem)**.** *Suppose* $\phi : R \to S$ *is a ring homomorphism. Then,*

$$\frac{R}{\ker \phi} \simeq \phi(R).$$

Example 9.8. For every positive integer m we have $\dfrac{\mathbb{Z}}{m\mathbb{Z}} \simeq \mathbb{Z}_m$.

Given a ring R with unity we can define a homomorphism $\phi : \mathbb{Z} \to R$, by $\phi(n) = n1$. The kernel of this homomorphism is the set of all integers n for which $n1 = 0$. If $char R = m$ is non-zero, then $\ker \phi = m\mathbb{Z}$, and thus by the First Isomorphism Theorem, $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ is isomorphic to a subring of R. Therefore, R has a subring that is isomorphic to $\mathbb{Z}_m$. If $char R = 0$, then R has a subring that is isomorphic to $\mathbb{Z}$.

Theorem 9.11. *Let F be a field. If characteristic of F is zero, then it has a subring that is isomorphic to $\mathbb{Q}$. If characteristic of F is a prime number p, then F has a subring isomorphic to $\mathbb{Z}_p$.*

When creating rational numbers we consider all fractions of integers with non-zero denominators. The same can be done for all integral domains.

9.5 Warm-ups

Example 9.9. Let R be a ring with unity. Prove that an ideal I contains 1 if and only if $I = R$.

Solution. Suppose $1 \in I$. If $r \in R$, then by definition of an ideal $r = r1 \in I$, since $1 \in I$. Therefore, I contains all elements of R and thus $I = R$.
Conversely suppose $I = R$. Then, clearly $1 \in I$. □

Example 9.10. In the definition of the unity, we assumed the unity to be non-zero. What happens if the unity is zero?

Solution. If the unity of a ring is its zero, then since $0x = 0$, and $1x = x$, and $1 = 0$. Thus $x = 0$, for all $x \in R$, which implies $R = \{0\}$ is the trivial ring. □

Example 9.11. Prove that if a ring element is a unit, then it cannot be a zero-divisor.

Solution. Suppose a is a unit. If $ab = 0$, then multiplying by a^{-1} gives $a^{-1}ab = a^{-1}0 = 0$, and thus $b = 0$. Therefore, a is not a zero-divisor. □

9.6 More Examples

Example 9.12. Is there a ring R and an ideal I for which R/I is commutative but R is not commutative? Is it possible that R/I has a unity but R does not? Is it possible that R/I has no zero-divisors but R has zero-divisors?

Solution. The answer is yes to all of the above questions. Consider a ring R and a field F. Then, $R \times \{0\}$ is an ideal of $R \times F$. We will show factor ring $\dfrac{R \times F}{R \times \{0\}}$ is a field. First, note that $(r, x) - (0, x) = (r, 0) \in R \times \{0\}$, and thus every element of this factor ring is of the form $(0, x) + R \times \{0\}$. We see that

$$((0, x) + R \times \{0\})((0, y) + R \times \{0\}) = (0, x)(0, y) + R \times \{0\} = (0, xy) + R \times \{0\}.$$

Since F is commutative, $xy = yx$ and thus this factor ring is commutative.

Now, note that $(0, 1) + R \times \{0\}$ is the unity of this ring.

Furthermore, if $(0, x) + R \times \{0\}$ and $(0, y) + R \times \{0\}$ are non-zero, then their product $(0, xy) + R \times \{0\}$ is also non-zero, since $xy \neq 0$. Therefore, this factor ring is commutative, has a unity and has no zero-divisors. If we choose $R = M_2(\mathbb{R})$, then the ring $R \times F$ is not commutative. If we choose $R = 2\mathbb{Z}$, then the ring $R \times F$ does not have a unity. Furthremore, $(2, 0)(0, 1) = (0, 0)$ and thus $R \times F$ has a zero-divisor. □

Example 9.13. Prove that if a commutative ring with unity has precisely two ideals, then it is a field.

Solution. Let F be a commutative ring with unity that has precisely two ideals. Note that $\{0\}$ and F are both ideals of F. We need to show every non-zero element of F has a multiplicative inverse. Suppose $0 \neq a \in F$, and consider the ideal $\langle a \rangle$. Since $a \in \langle a \rangle$, this ideal is non-zero, and thus $\langle a \rangle = F$. Since $1 \in F$ we need to have $1 \in \langle a \rangle$, which implies $1 = ab$ for some $b \in F$, and thus a has a multiplicative inverse. □

Example 9.14. Prove that the intersection of any collection of ideals is an ideal.

Solution. Suppose A_i with $i \in I$ is a collection of ideals of a ring R. Suppose $a, b \in \bigcap\limits_{i \in I} A_i$, and $r \in R$. By definition of intersection $a, b \in A_i$ for all $i \in I$. Since A_i is an ideal $a - b \in A_i$, and $ar, ra \in A_i$. Since this is true for all $i \in I$, we have $a - b, ar, ra \in \bigcap\limits_{i \in I} A_i$. Therefore, $\bigcap\limits_{i \in I} A_i$ is an ideal. □

Example 9.15. Suppose for elements a, b in a commutative ring, the element ab is a zero-divisor. Prove that at least one of a and b is a zero-divisors.

Solution. First, note that since ab is a zero-divisor, $ab \neq 0$ and $abc = 0$ for some non-zero element c. Note that if $a = 0$, then ab would be zero, which is a contradiction. Therefore, $a \neq 0$. Similarly $b \neq 0$. If $bc = 0$, then by definition, b would be a zero-divisor. Otherwise, $a(bc) = 0$ and $bc \neq 0$. Therefore, a is a zero-divisor, as desired. □

Definition 9.8. An element a in a ring is said to be **nilpotent** if $a^n = 0$ for some positive integer n.

Example 9.16. Prove that in a commutative ring, the set of all nilpotent elements is an ideal. By an example show this is not true in non-commutative rings.

Solution. Let I be the set of all nilpotent elements of a commutative ring. First, note that $0 \in I$, since $0^1 = 0$. Therefore, I is nonempty.
Assume $a, b \in I$. Since $ab = ba$ we can show by induction that

$$(a-b)^k = a^k + \binom{k}{1} a^{k-1}(-b) + \binom{k}{2} a^{k-2}(-b)^2 + \cdots + \binom{k}{k-1} a(-b)^{k-1} + (-b)^k.$$

Now, assume $a^n = b^m = 0$. Letting $k = m + n$ we see each $a^j(-b)^{k-j}$ is zero, because either $j \geq n$ or $k - j \geq m$. Note that since $a^n = 0$, we have $a^{n+1} = a^{n+2} = \cdots = 0$, and $b^{m+1} = b^{m+2} = \cdots = 0$. Therefore, $a - b \in I$.

Now, assume $a \in I$ and $r \in R$. We have $(ar)^n = a^n r^n = 0r^n = 0$, which means ar is nilpotent. Thus, $ar \in I$.

Therefore, I is an ideal of R.

In $M_2(\mathbb{R})$, the elements $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ satisfy $a^2 = b^2 = 0$, and thus, they are nilpotent, however their sum $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the unity, which is not nilpotent. Therefore, the set of nilpotent elements is not closed under addition and thus it is not an ideal. □

Example 9.17. Prove that if I is an ideal of a ring R, a is an element of R and n is a positive integer, then $(a + I)^n = a^n + I$.

Solution. We will prove this by induction on n.
Basis step. $(a + I)^1 = a + I = a^1 + I$, by definition of a^n.
Inductive step. Suppose $(a + I)^n = a^n + I$ for some positive integer n. Then, by definition $(a + I)^{n+1} = (a+I)(a+I)^n$. By inductive hypothesis this is equal to $(a+I)(a^n+I) = aa^n + I = a^{n+1} + I$, as desired. □

Example 9.18. Suppose N is the ideal consisting of all nilpotent elements of a commutative ring R. Then, the factor ring R/N contains no non-zero nilpotent elements.

Solution. Suppose on the contrary $a + N$ is a non-zero nilpotent element of R/N. On the other hand $(a + N)^n = 0 + N$ for some positive integer n and thus $a^n + N = 0 + N$, which implies $a^n \in N$. Since every element of N is nilpotent, $(a^n)^m = 0$ for some positive integer m. Therefore, $a^{nm} = 0$, which implies $a \in N$. This contradicts the fact that $a + N \neq 0 + N$. □,

Example 9.19. Suppose I, J are ideals of a ring R. Prove that $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal of R.

Solution. First, note that $0 + 0 \in I + J$ and thus $I + J$ is non-empty.

Assume $x, y \in I + J$, and $r \in R$. By definition of $I + J$, there are $a, a_1 \in I, b, b_1 \in J$ for which $x = a + b$, and $y = a_1 + b_1$. Thus $x - y = (a - a_1) + (b - b_1)$. Since I and J are ideals, we know $a - a_1 \in I$ and $b - b_1 \in J$. Thus $x - y \in I + J$.

Now, note that $rx = ra + rb$. Since I and J are ideals and $a \in I, b \in J$ we have $ra \in I$ and $rb \in J$. Therefore, $ra + rb \in I + J$, which means $rx \in I + J$. Similarly $xr = ar + br \in I + J$, since $ar \in I$ and $br \in J$. Therefore, by the Ideal Test, $I + J$ is an ideal. □

Example 9.20. Prove that if a is an element of a commutative ring with unity R for which $\langle a \rangle = R$, then a must be a unit.

Solution. By definition $\langle a \rangle = \{ar \mid r \in R\}$. Since this ideal is equal to R it must contain 1 and thus $ar = 1$ for some $r \in R$. Since R is commutative, $ar = ra = 1$ and thus a is a unit. □

Example 9.21. Suppose $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an ascending chain of ideals of a ring R. Prove that $\bigcup\limits_{n=1}^{\infty} I_n$ is an ideal of R.

9.7 Exercises

9.7.1 Problems for Grading

Exercise 9.1 (10 pts)**.** *Problem 39, Page 245.*

Exercise 9.2 (15 pts)**.** *Problem 49, Page 245.*

Hint: Use Example 8.17. Prove that $\binom{p}{j}$ is divisible by p, where p is prime and $0 < j < p$.

Exercise 9.3 (10 pts)**.** *Problem 16, Page 257. (See Problem 12 for the definition of AB.)*

Exercise 9.4 (10 pts)**.** *Problem 64, Page 259.*

Exercise 9.5 (10 pts)**.** *Problem 44, Page 272.*

Exercise 9.6 (10 pts)**.** *Problem 48, Page 272.*

Exercise 9.7 (25 pts)**.** *Problem 66, Page 274.*

9.7.2 Problems for Practice

Prove the Second and Third Isomorphism Theorems:

Theorem 9.12 (Second Isomorphism Theorem)**.** *Suppose S is a subring of a ring R, and I is an ideal of R. Then, $S \cap I$ is an ideal of S, and*

$$\frac{S+I}{I} \simeq \frac{S}{S \cap I}.$$

Theorem 9.13 (Third Isomorphism Theorem)**.** *Suppose I and J are ideals of a ring R, and $I \subseteq J$. Then,*

$$\frac{(R/I)}{(J/I)} \simeq \frac{R}{J}.$$

Page 246: 51, 62, 65.

Page 258-259: 41, 47, 48, 60, 63.

Page 274: 68, 69.

9.7.3 Challenge Problems

Exercise 9.8. *Prove that for every field F, the ring $M_n(F)$ has precisely two ideals.*

9.8 Summary

- A zero-divisor is a non-zero element a for which $ab = 0$ for some non-zero b.
- An integral domain is a commutative ring with unity that has no zero-divisors.
- A field is a ring whose non-zero elements form an Abelian group under multiplication.
- I is an ideal of R if I is closed under subtraction, and for every $a \in I$ and $r \in R$ we have $ar, ra \in I$.
- Much of the properties of homomorphisms from group theory remain intact if we replace subgroups by subrings, and normal subgroups by ideals.
- The First Isomorphism Theorem is valid for rings.

10 Week 10

Theorem 10.1 (Field of Quotients)**.** *Let D be an integral domain. Then, there exists a field F that satisfies both of the following:*

- *F contains a subring S that is isomorphic to D.*
- *Every element of F is of the form xy^{-1} for some $x, y \in S$ with $y \neq 0$.*

Furthermore, this field F is unique up to isomorphism.

The unique field above is called the **field of quotients of** D.

Example 10.1. Here are some examples of fields of quotients.

(a) $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$.

(b) The ring of rational functions of the form $P(x)/Q(x)$, where $P(x)$ and $Q(x)$ are polynomials with real coefficients and $Q(x) \neq 0$, is the field of quotients of $\mathbb{R}[x]$, the ring of polynomials with real coefficients.

10.1 Polynomial Rings

Definition 10.1. Let R be a ring, and define

$$R[x] = \{a_n x^n + \cdots + a_1 x + a_n \mid n \in \mathbb{N}, \text{ and } a_j \in R \text{ for all } j = 0, \dots, n\},$$

where x is a symbol. Two elements $a_n x^n + \cdots + a_1 x + a_0$ and $b_m x^m + \cdots + b_1 x + b_0$, with $n \leq m$, are said to be equal if $a_j = b_j$ for all $j = 0, \dots, n$ and $b_{n+1} = \cdots = b_m = 0$.
We define two binary operations $+$ and $\cdot$ on $R[x]$ as follows:
If $p(x) = a_n x^n + \cdots + a_1 x + a_0$, and $q(x) = b_m x^m + \cdots + b_1 x + b_0$, then

$$p(x) + q(x) = (a_s + b_s)x^s + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

where $s = \max(n, m)$ and $a_j = 0$ if $j > n$ and $b_j = 0$ if $j > m$. Two polynomials are multiplied in the usual way:

$$p(x)q(x) = a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)x^{n+m-1} + \cdots .$$

Theorem 10.2. *Suppose R is a ring. Then $R[x]$ along with the above addition and multiplication is a ring. If R is commutative, then $R[x]$ is also commutative. If R has a unity, then $R[x]$ has a unity.*

Definition 10.2. Let R be a ring. The **degree** of a polynomial $p(x) \in R[x]$, denoted by $\deg p(x)$, is the largest exponent n for which x^n appears in $p(x)$ with a non-zero coefficient. In other words,

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \; a_j \in R \text{ for all } j, \text{ and } a_n \neq 0.$$

We define the degree of the zero polynomial as $-\infty$. The coefficient a_n is said to be the **leading coefficient** of $p(x)$. A polynomial of degree less than 1 is said to be a **constant**. A polynomial of degree 1 is said to be **linear**.

Theorem 10.3. *Let D be an integral domain. Then, $D[x]$ is also an integral domain. Furthermore, for every two polynomials $p(x), q(x) \in D[x]$ we have*

$$\deg(p(x)q(x)) = \deg p(x) + \deg q(x).$$

Theorem 10.4 (Division Algorithm)**.** *Suppose R is a ring with unity, $f(x), g(x)$ are elements of $R[x]$ for which the leading coefficient of $g(x)$ is a unit. Then, there are unique polynomials $q(x), r(x) \in R[x]$ for which the following are both satisfied:*

- *$f(x) = g(x)q(x) + r(x)$, and*
- $\deg r(x) < \deg g(x)$.

Corollary 10.1. Since every non-zero element of a field is a unit, the division algorithm is valid in $F[x]$, where F is a field, for every non-zero polynomial $g(x)$.

Corollary 10.2 (Remainder Theorem)**.** Let F be a field, and let $f(x) \in F[x]$. If $a \in F$, then

$$f(x) = (x - a)q(x) + f(a)$$

for some $q(x) \in F[x]$.

Definition 10.3. Let F be a field and $f(x) \in F[x]$. We say an element $a \in F$ is a root of $f(x)$ if $f(a) = 0$.

Corollary 10.3 (Factor Theorem)**.** Suppose F is a field, and $f(x) \in F[x]$. Suppose further that $a_1, \ldots, a_k$ are distinct roots of $f(x)$. Then, there is $q(x) \in F[x]$ for which

$$f(x) = (x - a_1) \cdots (x - a_k)q(x).$$

Corollary 10.4. Let F be a field. Then, every non-zero polynomial of degree n in $F[x]$ has at most n roots.

Recall that since $\mathbb{Z}$ is a cyclic group, all ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. The proof of this fact uses the division algorithm is valid in $\mathbb{Z}$. A similar strategy allows us to prove this fact in $F[x]$.

Definition 10.4. An ideal I of a commutative ring R is said to be a **principal ideal** if

$$I = \langle a \rangle = \{ar \mid r \in R\},$$

for some $a \in R$.

Definition 10.5. An integral domain is said to be a **principal ideal domain** or **PID** if all of its ideals are principal.

Theorem 10.5. *Suppose F is a field. Then $F[x]$ is PID. Furthermore, if I is a non-zero ideal of $F[x]$, then $I = \langle f(x) \rangle$ if and only if $f(x)$ is a non-zero polynomial in I with the lowest degree.*

10.2 Divisibility and Factorization

Definition 10.6. Let D be an integral domain. We say an element a divides an element b, written as $a \mid b$, if $b = ac$ for some $c \in D$.

Definition 10.7. Let D be an integral domain. Elements $a, b \in D$ are said to be **associates** if $a = bu$ for some unit $u \in D$. We say a non-zero element $a \in D$ is **reducible** if $a = bc$ for two non-unit elements $b, c \in D$. Otherwise, we say a is **irreducible**. Note that the element 0 and units are neither reducible nor irreducible. We say a is **prime** if a is non-zero, and is not a unit and $a \mid bc$ for $b, c \in D$ implies $a \mid b$ or $a \mid c$.

The following example determines all units of polynomial rings over integral domains.

Example 10.2. Prove that if D is an integral domain, then $U(D[x]) = U(D)$.

Example 10.3. Here are some examples of irreducible and prime elements.

(a) Any prime number in $\mathbb{Z}$ is both a prime and irreducible.

(b) Any linear polynomial in $\mathbb{R}[x]$ is irreducible.

(c) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$.

Theorem 10.6. *Let F be a field. A polynomial $f(x) \in F[x]$ of degree 2 or 3 is irreducible if and only if it does not have a root in F.*

Definition 10.8. Let D be an integral domain. We say a polynomial $f(x)$ is irreducible over D if $f(x)$ is irreducible as an element of $D[x]$.

Example 10.4. Prove that for every prime p the polynomial $x^3 - 2px^2 + p$ is irreducible over $\mathbb{Q}$.

For polynomials of higher degree, simple irreducibility tests are rare, but over some domains irreducibility tests exist.

We will now focus on polynomials with integer coefficients. The objective is to show that if a polynomial with integer coefficients can be factored over $\mathbb{Q}$, then it can also be factored over $\mathbb{Z}$.

Definition 10.9. The **content** of a non-zero polynomial $f(x)$ in $\mathbb{Z}[x]$ is the greatest common divisor of its coefficients. The content of $f(x)$ is denoted by $c(f(x))$ or simply $c(f)$.

Theorem 10.7. *Let $f(x), g(x) \in \mathbb{Z}[x]$. Then, $c(fg) = c(f)c(g)$.*

Theorem 10.8. *Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.*

Theorem 10.9. *Let p be a prime and suppose $f(x) \in \mathbb{Z}[x]$ has degree at least 1. Let $\overline{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by taking all coefficients of f mod p. If $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p[x]$ and $\deg f(x) = \deg \overline{f}(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Example 10.5. Prove that the polynomial $x^3 + 7x^2 + 4x + 979$ is irreducible over $\mathbb{Q}$.

Theorem 10.10 (Eisenstein's Criterion)**.** *Let p be a prime and the coefficients of*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

satisfy the following properties:

$$p \nmid a_n, p \mid a_{n-1}, \ldots, p \mid a_1, p \mid a_0, p^2 \nmid a_0.$$

Then, $f(x)$ is irreducible over $\mathbb{Q}$.

Example 10.6. Prove that the polynomial is $7x^5 + 9x^2 + 15x + 12$. irreducible over $\mathbb{Q}$.

Solution. Consider prime 3 and note that

$$3 \nmid 7, 3 \mid 9, 3 \mid 15, 3 \mid 12, 3^2 \nmid 12$$

Therefore, by the Eisenstein's Criterion this polynomial is irreducible over $\mathbb{Q}$. □

10.3 Warm-ups

Example 10.7. Prove that if for a ring R, the polynomial ring $R[x]$ is commutative, then R must also be commutative.

Solution. Since $R \subseteq R[x]$ and every two elements of $R[x]$ commute, every two elements of R also commute, and thus R is commutative. □

Example 10.8. Prove that every cubic polynomial is reducible over $\mathbb{R}$.

Solution. From calculus we know that every cubic polynomial has a real root, and thus it is reducible. □

Example 10.9. Suppose a and b are two elements of a commutative ring with unity R. Prove that if a and b are associates, then $\langle a \rangle = \langle b \rangle$.

Solution. Suppose a and b are associates. By definition $a = bu$ for some unit u. Thus, $a \in \langle b \rangle$, which implies $\langle a \rangle \subseteq \langle b \rangle$. Similarly $b = au^{-1} \in \langle a \rangle$. Thus $\langle b \rangle \subseteq \langle a \rangle$. Therefore, $\langle a \rangle = \langle b \rangle$, as desired. □

Example 10.10. Suppose a and b are elements of an integral domain R. Prove that a and b are associates if and only if $\langle a \rangle = \langle b \rangle$.

Solution. The forward direction was proved in the above example.

Suppose $\langle a \rangle = \langle b \rangle$. We have $a = br$, and $b = as$ for some $r, s \in R$. This yields, $a = asr$. Thus, $a = 0$ or $1 = sr$.

Case I. $a = 0$. Thus, $b = 0s = 0$, which means $a = b$, and thus they are associates.
Case II. $rs = 1$. Thus, r is a unit, and since $a = br$, the elements a and b are associates, by definition. □

10.4 More Examples

Example 10.11. Prove that if for a ring R, the polynomial ring $R[x]$ has a unity, then R must also have a unity.

Solution. Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is the unity of $R[x]$. Thus, for every $r \in R$ we must have

$$f(x) = rf(x) = ra_n x^n + \cdots + ra_1 x + ra_0.$$

By comparing the constant terms we obtain $a_0 = ra_0$. Similarly $a_0 = a_0 r$, and thus a_0 is the unity of R. □

Example 10.12. Let F be a field. Prove that $\langle x \rangle$ is a maximal ideal of $F[x]$.

Solution. Define $\phi : F[x] \to F$ by $\phi(f(x)) = f(0)$. If $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$, then the constant terms of $f(x) + g(x)$ and $f(x)g(x)$ are $a_0 + b_0$ and $a_0 b_0$, respectively. Therefore, $\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x))$ and $\phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$, and thus ϕ is a ring homomorphism. Note that if $r \in F$ then $\phi(r) = r$, and thus ϕ is onto. Also, $\phi(f(x)) = 0$ if and only if $a_0 = 0$, if and only if $f(x) = xh(x)$ for some polynomial $h(x)$. Therefore, $\ker \phi = \langle x \rangle$. By the First Isomorphism Theorem $\dfrac{F[x]}{\langle x \rangle} \simeq F$ is a field, which by a theorem we conclude that $\langle x \rangle$ is a maximal ideal of $F[x]$. □

Example 10.13. Check if each of the following polynomials are irreducible over $\mathbb{Q}$.

(a) $x^3 + 15x^2 - x + 2$.

(b) $x^3 - 3x + 2$.

(c) $5x^8 - 21x^7 + 24x^5 + 42x^2 + 9x + 6$.

Solution. (a) Taking this polynomial mod 3 we obtain $p(x) = x^3 - x + 2 \in \mathbb{Z}_3[x]$. We notice that $p(0) = p(1) = p(2) = 2 \neq 0$ and thus $p(x)$ has no roots in $\mathbb{Z}_3$. Since this polynomial is of degree 3, by a theorem it is irreducible over $\mathbb{Z}_3$ and thus the origian polynomial is irreducible over $\mathbb{Q}$.
(b) This polynomial has a root $x = 1$ and thus it is reducible.
(c) This is irreducible by the Eisenstein's Criterion with $p = 3$. □

Example 10.14. Let n be a positive integer. Prove that there are infinitely many polynomials of degree n that are irreducible over $\mathbb{Q}$.

Solution. Consider the polynomial $x^n - 2a$, where a is an odd integer. This polynomial satisfies the conditions of Eisenstein's Criterion with $p = 2$, since $2 \nmid 1, 2 \mid 2a$ and $4 \nmid 2a$. Since a could be any odd integer, we obtain infinitely many polynomials of degree n that are irreducible. □

Example 10.15. Is it true that if a polynomial is reducible over $\mathbb{Z}$ then it must be reducible over $\mathbb{Q}$?

Solution. No. 6 is reducible over $\mathbb{Z}$, since $6 = 2 \times 3$, and neither 2 nor 3 are units in $\mathbb{Z}[x]$. However, 6 is a unit in $\mathbb{Q}[x]$, and thus is not reducible. □

Example 10.16. Let a, b be two elements of a field F with $a \neq 0$, and let $f(x) \in F[x]$ be a polynomial of degree at least 1. Prove that $f(x)$ is irreducible if and only if $f(ax + b)$ is irreducible.

Solution. We will prove that $f(x)$ is reducible if and only if $f(ax + b)$ is reducible.

Suppose $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ have degree at least 1. Then, $f(ax+b) = g(ax+b)h(ax+b)$. Note that $g(ax+b)$ is not a constant, since otherwise, $g(x) = g(a(a^{-1}x - a^{-1}b) + b) = g(x)$ would also be a constant polynomial, which is not the case. Similarly $h(ax+b)$ is also a non-constant polynomial. Therefore, $f(ax+b)$ is reducible,

Now, note that if $f(ax+b)$ is reducible, by what we proved above $f(a(a^{-1}x - a^{-1}b) + b) = f(x)$ must also be reducible, as desired. □

Example 10.17. Let p be an odd prime. Prove that $x^p + px + 1$ is irreducible over $\mathbb{Q}$.

Solution. By Example 10.16 it is enough to show $(x-1)^p + p(x-1) + 1$ is irreducible. Expanding we have

$$(x-1)^p + p(x-1) + 1 = x^p - \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x - 1 + px - p + 1.$$

The leading coefficient of this polynomial is 1 which is not a multiple of p. Since $\binom{p}{k}$ for $k = 1, \ldots, p-1$ is divisible by p, all other coefficients are multiples of p. The constant term is $-p$ which is not a multiple of p^2, and thus by Eisenstein's Criterion this polynomial is irreducible. □

10.5 Exercises

10.5.1 Problems for Grading

Exercise 10.1 (10 pts)**.** *Problem 15, Page 284.*

Exercise 10.2 (10 pts)**.** *Problem 34, Page 285.*

Exercise 10.3 (10 pts)**.** *Problem 35, Page 286.*

Exercise 10.4 (25 pts)**.** *Problem 14, Page 301.*

Exercise 10.5 (10 pts)**.** *Problem 15, Page 301.*

Exercise 10.6 (10 pts)**.** *Problem 23, Page 302.*

10.5.2 Problems for Practice

Pages 284-287: 8, 24, 33, 52, 57, 61.
Pages 302-303: 24, 34, 38.

Example 10.18. Prove that $\langle x+1, 2\rangle$ is a maximal ideal of $\mathbb{Z}[x]$.

Example 10.19. Let F be a field and let $a, b \in F$. Prove that:

1. $\langle x - a\rangle$ is a maximal ideal of $F[x]$.

2. $\langle x - a, y - b\rangle$ is a maximal ideal of $F[x, y]$.

10.6 Summary

- Polynomials with coefficients in a given ring form a ring with the usual polynomial addition and multiplication.
- Division algorithm in polynomial rings is valid as long as the divisor has a unit as its leading coefficient.
- A polynomial of degree n over a field has at most n roots.
- Polynomial rings over fields are PID, i.e. every ideal is generated by an element of the lowest degree inside the ideal.
- The following irreudicibility tests can be used. (F is a field.)
  - A polynomial of degree 2 or 3 over F is irreducible iff it has no roots.
  - A polynomial $f(x)$ is irreducible over F iff $f(ax+b)$ is irreducible for some $a, b \in F$, with $a \neq 0$.
  - For a polynomial with integer coefficients we can use Eisenstein's Criterion: (1) Find a prime p that divides all coefficients, except for the leading coefficient, and (2) Make sure p^2 does not divide the constant term.

11 Week 11

Example 11.1. For every prime number p, the polynomial $1 + x + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}$.

Theorem 11.1. *In an integral domain, every prime element is also irreducible.*

Example 11.2. In $\mathbb{Z}[\sqrt{-3}]$ the element $1 + \sqrt{-3}$ is irreducible but it is not prime.

Definition 11.1. Given a non-square integer d we set

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

This is a subring of $\mathbb{C}$. We define

$$N(a + b\sqrt{d}) = |(a + b\sqrt{d})(a - b\sqrt{d})| = |a^2 - b^2 d|.$$

It can easily be seen that $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[\sqrt{d}]$.

Theorem 11.2. *In every principal ideal domain an element is prime if and only if it is irreducible.*

Theorem 11.3. *A non-zero element a in a principal ideal domain is irreducible if and only if $\langle a \rangle$ is a maximal ideal.*

Another important property of integers is the ability to uniquely prime factorize all non-zero integers. We will now study domains that satisfy this property.

Definition 11.2. An integral domain D is called a **unique factorization domain** or a **UFD** if every non-zero, non-unit element of D is a product of irreducible elements. Furthermore, this factorization is unique up to associates and the order in which the factors appear.

Example 11.3. Here are a few examples of UFD's.

(a) $\mathbb{Z}$ is a UFD.

(b) $\mathbb{C}[x]$ is a UFD.

Example 11.4. $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

Theorem 11.4. *In any UFD an element is prime if and only if it is irreducible.*

In order to understand the concept of UFD we repeat the argument that proves every positive integer can be written as a product of primes.

To obtain the prime factorization of an integer n, we see if n is prime, if so we are done. Otherwise we write $n = ab$ for some integers $a, b > 1$. We then factor a and b into product of integers, repeat this and we will have the prime factorization of n. This idea cannot be replicated in all integral domains, because this process may never terminate. What that means is that in a ring it could be the case that $n = a_1b_1$, then $a_1 = a_2b_2$, $a_2 = a_3b_3$, etc, and this factorization never ends. In the language of ideals this can be interpreted as follows:

$$\langle n\rangle \subsetneq \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots .$$

In other words, we are looking for rings that do not have any sequence of ideals of the above form. Such a sequence above is called an **ascending chain of ideals**.

Definition 11.3. A ring R is said to satisfy the **ascending chain condition** or **ACC** if for any sequence of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

there is a positive integer n for which $I_n = I_{n+1} = I_{n+2} = \cdots$. A ring that satisfies ACC is sometimes called a **Noetherian ring**.

Theorem 11.5. *Any principal ideal domain satisfies the ascending chain condition.*

Theorem 11.6. *Every PID is a UFD.*

Corollary 11.1. For every field F, the polynomial ring $F[x]$ is a UFD.

Definition 11.4. An integral domain D is called a **Euclidean domain** if there is a function $d : D^* \to \mathbb{N}$ that assigns to any non-zero element a of D a non-negative integer $d(a)$ that satisfies the following:

(a) $d(a) \leq d(ab)$ for all $a, b \in D^*$, and

(b) For every $a, b \in D$ with $b \neq 0$, there are $q, r \in D$ for which $a = bq + r$, and either $r = 0$ or $d(r) < d(b)$.

The function d is called a **measure** for D.

Example 11.5. The following are two examples of Euclidean domains:

(a) $\mathbb{Z}$ along with the measure $d(a) = |a|$.

(b) $F[x]$ along with $d(f(x)) = \deg f$, where F is a field.

Theorem 11.7. *Every Euclidean domain is a PID, and hence a UFD.*

Example 11.6. $\mathbb{Z}[i]$ is a Euclidean domain.

Theorem 11.8. *If D is a UFD, then so is $D[x]$.*

11.1 Warm-ups

Example 11.7. Prove that being associate in a commutative ring with unity is an equivalence relation.

Solution. Reflexive. $a = a1$, and thus a is an associate of a.
Symmetric. If $a = ub$ with u a unit, then $b = u^{-1}a$, and thus b is an associate of a.
Associative. If $a = ub$ and $b = vc$, where u, v are units, then $a = uvc$. Since u and v are units, uv is also a unit. Thus, a is an associate of c. □

Example 11.8. In an integral domain prove that:

(a) An associate of a prime is prime.

(b) An associate of an irreducible element is irreducible.

Solution. (a) Suppose a is a prime and b is an associate of a. By definition $a = bu$. First, note that since a is non-zero and non-unit, b is also non-zero and not a unit. If b divides xy for elements, x, y we have $xy = bz$. This implies $xy = auz$, and thus a divides x or y. If $x = at$, then $x = bu^{-1}t$ or b divides x. Therefore b divides x or y. Thus, b is prime.
(b) Suppose a is irreducible and b is an associate of a. By definition $a = bu$. First, note that since a is non-zero and non-unit, b is also non-zero and not a unit. Now, assume $b = xy$ for some elements x, y. Thus, $a = u^{-1}xy$. Since a is irreducible, $u^{-1}x$ or y must be a unit. Since u is a unit, this implies x or y is a unit. Therefore, b is irreducible. □

11.2 More Examples

Example 11.9. Determine all units of $\mathbb{Z}[i]$.

Solution. Suppose $a + ib \in \mathbb{Z}[i]$ is a unit. Thus, $(a + ib)(c + id) = 1$ for integers a, b, c, d. Taking absolute values we obtain $(a^2 + b^2)(c^2 + d^2) = 1$, or $a^2 + b^2 = 1$. This means $a + ib = \pm 1, \pm i$, all of which are units. Therefore, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. □

Example 11.10. Let d be a non-square integer, and let

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

Prove that $\mathbb{Z}[\sqrt{d}]$ is a subring of $\mathbb{C}$. Also show that the representation $a + b\sqrt{d}$ is unique.

Solution. We will show this set is closed under subtraction and multiplication. Let $x, y \in \mathbb{Z}[\sqrt{d}]$. We have $x = a + b\sqrt{d}, y = m + n\sqrt{d}$ for integers a, b, m, n. Thus,

$$x - y = (a - m) + (b - n)\sqrt{d} \in \mathbb{Z}[\sqrt{d}], \text{ and } xy = (am + bnd) + (an + bm)\sqrt{d} \in \mathbb{Z}[\sqrt{d}].$$

As for the uniqueness, assume $a + b\sqrt{d} = m + n\sqrt{d}$. This gives us $(a - m)^2 = (n - b)^2 d$. If $a = m$, then $b = n$ and we are done. Otherwise, since $a - m$ and $n - b$ are both non-zero integers, by comparing the exponent of each prime on both sides of this equality we conclude that the exponent of each prime in the prime factorization of d must be even. Thus, d must be a perfect suquare, which contradicts the assumption. □

Example 11.11. Suppose we change the definition of UFD to assume every non-zero element has a unique factorization as a product of *prime* elements (instead of irreducible elements). Prove that this definition is equivalent to the one given.

Solution. Since in a UFD, every irreducible is prime and every prime is irreducible, the unique factorization into products of primes exist.

Suppose an integral domain satisfied the unique prime factorization property. We know every prime is irreducible in any integral domain. We will now show every irreducible is also a prime. Suppose an element a is irreducible. Thus, a can be written as a product of primes. Since a is irreducible, all of the factors must be unit except for one that is prime. Thus, a is associate to a prime and thus it is a prime. Therefore, in every such ring irreducibles and primes coincide, and thus every element has a unique irreducible factorization or the ring id a UFD. □

Example 11.12. Let u be an element of a Euclidean domain with measure d. Prove that u is a unit if and only if $d(u) = d(1)$.

Solution. First, note that $d(1) \leq d(1a) = d(a)$ for every element a.

Assume u is a unit. $d(u) \leq d(uu^{-1}) = d(1)$. Therefore, by what we showed above we must have $d(u) = d(1)$.

Assume $d(u) = d(1)$. Since we are working in a Euclidean domain, $1 = uq + r$ for some elements q, r for which $r = 0$ or $d(r) < d(u)$. If $r = 0$, then $uq = 1$ and thus u is a unit. Otherwise, $d(r) < d(u) = d(1)$, which contradicts what we proved in the beginning. □

Example 11.13. Prove that $\mathbb{Z}[2i]$ is not a UFD.

Solution. Note that 2 and $2i$ are not associated, because $i \notin \mathbb{Z}[i]$.
Now, we will show that 2 and $2i$ are both irreducible. If $2 = xy$, then $4 = N(x)N(y)$. If $N(x) = 1$ then x must be a unit. Similar for y. Thus, we must have $N(x) = N(y) = 2$. However $N(a + 2bi) = a^2 + 4b^2$ can never be 2. □

Example 11.14. Prove that for every two integers a, b we have $\dfrac{\mathbb{Z}[i]}{\langle a - bi\rangle} \simeq \dfrac{\mathbb{Z}[i]}{\langle a + bi\rangle}$.

Solution. Define $\phi : \mathbb{Z}[i] \to \dfrac{\mathbb{Z}[i]}{\langle a + bi\rangle}$ by $\phi(z) = \overline{z} + \langle a + bi\rangle$. By properties of complex conjugate, it can be shown that ϕ is a ring homomorphism.

$$\ker \phi = \{z \in \mathbb{Z}[i] \mid \overline{z} + \langle a + bi\rangle = \langle a + bi\rangle\} = \{z \in \mathbb{Z}[i] \mid \overline{z} \in \langle a + bi\rangle\}.$$

The above condition is equivalent to $\overline{z} = (a + bi)u$ for some $u \in \mathbb{Z}[i]$. Taking complex conjugate of both sides we obtain $z = (a - bi)\overline{u}$. Since this all can be reveresed we obtain $\ker \phi = \langle a - bi\rangle$. By the First Isomorphism Theorem we conclude $\dfrac{\mathbb{Z}[i]}{\langle a - bi\rangle} \simeq \dfrac{\mathbb{Z}[i]}{\langle a + bi\rangle}$. □

Example 11.15. Prove that for every field F an every integer n the polynomial ring $F[x_1, \dots, x_n]$ is a UFD.

Solution. We will prove this by induction on n. For $n = 1$, the polynomial ring $F[x_1]$ is a PID and thus a UFD.
Suppose $F[x_1, \dots, x_n]$ is a UFD. By Theorem 11.8, the polynomial ring $F[x_1, \dots, x_n][x_{n+1}] = F[x_1, \dots, x_{n+1}]$ is a UFD. □

Example 11.16. Prove that if F is a field and $n \geq 2$ then the polynomial ring $F[x_1, \dots, x_n]$ is not a PID.

Solution. We will prove $\langle x_1, x_2\rangle$ is not a principal ideal. On the contrary assume $\langle x_1, x_2\rangle = \langle f\rangle$ for some polynomial f on n variables $x_1, \dots, x_n$. By assumption, $x_1 = fg$ and $x_2 = fh$ for polynomials g and h. Considering f as a polynomial of x_j with $j \neq 1$ the equality $x_1 = fg$, we conclude that degree of f with respect to x_j must be zero. Similarly degree of f with respect to x_1 must be zero by looking at $x_2 = fh$. Thus, f must be a constant. Since $x_1 = fg$, f cannot be zero, and thus f must be a unit. Therefore, $1 \in \langle x_1, x_2\rangle$, and thus $1 = x_1 a + x_2 b$ for polynomials a, b. This is impossible since substituting $x_1 = x_2 = 0$ yields $1 = 0$. □

Example 11.17. Suppose $f(x) \in \mathbb{Z}[x]$ is a non-constant polynomial. Prove that $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $f(ax + b)$ is irreducible over $\mathbb{Q}$ for some non-zero integers a and some integer b.

Solution. Suppose $f(x)$ is reducible over $\mathbb{Q}$. By Theorem 10.8 there must be non-constant polynomials $g(x), h(x) \in \mathbb{Z}[x]$ for which $f(x) = g(x)h(x)$. Thus, $f(ax + b) = g(ax + b)h(ax + b)$ is also irreducible, since

$\deg f(x) = \deg f(ax+b)$ and $\deg g(x) = \deg g(ax+b)$, as a is non-zero.

Now, assume $f(ax+b)$ is reducible over $\mathbb{Q}$. This implies $f(a(x-b)/a+b)$ is also reducible over $\mathbb{Q}$ by Example 10.16. Thus, $f(x)$ is reducible over $\mathbb{Q}$. □

Example 11.18. Show that even though the polynomial x^4+x+1 is irreducible over $\mathbb{Q}$, the Eisenstein's Criterion along with Example 11.17 cannot prove this.

Solution. First, we will prove $f(x) = x^4+x+1$ is irreducible over $\mathbb{Q}$. Suppose on the contrary $f(x)$ is reducible. By Theorem 10.8 there are non-constant polynomials $g(x), h(x)$ with integer coefficients for which $f(x) = g(x)h(x)$. By comparing the coefficients of both sides we conclude that the product of the leading coefficients of g and h is 1. If necessary we will consider $f(x) = (-g(x))(-h(x))$ and thus we may assume both g and h are monic. Looking at the degrees of both sides we obtain $\deg g + \deg h = 4$. Assuming $\deg g \leq \deg h$ we have two cases:

Case I. $\deg g = 1, \deg h = 3$. In that case $f(x) = (x+a)h(x)$, and thus $f(-a) = 0$, which implies $a^4 - a + 1 = 0$. Thus $a(a^3-1) = -1$, and hence a divides 1. This means $a = \pm 1$. This implies $f(\pm 1) = 0$, which is not true.

Case II. $\deg g = \deg h = 2$. In which case we have the following:

$$x^4+x+1 = (x^2+ax+b)(x^2+mx+n) = x^4+(m+a)x^3+(n+am+b)x^2+(an+bm)x+bn$$

This implies $m+a = n+am+b = 0$, $an+bm = 1$, and $bn = 1$. The last equation implies $b = n = \pm 1$. Substituting this into $an+bm = 1$ we obtain $b(a+m) = 1$, which contradicts $m+a = 0$. Therefore, this case is also impossible.
Thus, x^4+x+1 is irreducible over $\mathbb{Q}$.

Now we will prove that the above cannot be proved by applying a linear transformation and an application of Eisenstein's Criterion.

Assume that is not the case. In other words, assume the polynomial satisfied the conditions of the Eisenstein's Criterion:

$$(ax+b)^4 + (ax+b) + 1 = a^4x^4 + 4a^3bx^3 + 6a^2b^2x^2 + (4ab^3+a)x + (b^4+b+1).$$

Thus, there is a prime p for which

$$p \nmid a^4, p \mid 4a^3b, p \mid 6a^2b^2, p \mid a(4b^3+1), p \mid (b^4+b+1), \text{ and } p^2 \nmid (b^4+b+1).$$

Since p is a prime from the first condition we obtain $p \nmid a$. Since $p \mid 4a^3b$ and $p \mid a(4b^3+1)$ we have $p \mid 4b$ and $p \mid 4b^3+1$. This means p must divide $4b^3+1-4b\cdot b^2 = 1$, which is a contradiction. □

11.3 Exercises

11.3.1 Problems for Grading

Exercise 11.1 (10 pts)**.** *Let d be a non-square integer. Prove that $a+b\sqrt{d}$ with $a, b \in \mathbb{Z}$, is a unit of $\mathbb{Z}[\sqrt{d}]$ if and only if $N(a+b\sqrt{d})=1$.*

Hint: $N(a+b\sqrt{d})=|(a+b\sqrt{d})(a-b\sqrt{d})|$.

Exercise 11.2 (10 pts)**.** *Let D be a Euclidean domain with measure d. Suppose a is an element of D for which $d(a)$ is the smallest element in the range of d that is larger than $d(1)$. Prove that a is irreducible.*

Hint: See Example 11.12.

Exercise 11.3 (10 pts)**.** *Prove that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.*

Hint: Use the same method that we used to prove $\mathbb{Z}[i]$ is a Euclidean domain.

Exercise 11.4 (10 pts)**.** *Problem 18, Page 319.*

Exercise 11.5 (10 pts)**.** *Problem 37, Page 320.*

Exercise 11.6 (10 pts)**.** *Problem 39, Page 320.*

11.3.2 Problems for Practice

Exercise 11.7. *Suppose $f(x)$ is a non-constant polynomial in $\mathbb{Z}[x]$. Prove that $\langle f(x)\rangle$ is not a maximal ideal of $\mathbb{Z}[x]$.*

Pages 320-321: 26, 29, 33, 36, 42, 47.

11.3.3 Challenge Problems

Exercise 11.8. *Prove that if D is an integral domain that is not a field, then $D[x]$ is not a Euclidean domain.*

Exercise 11.9. *Prove that the set of primes of $\mathbb{Z}[i]$ are those elements that are associated to one of the following:*

- *Primes in $\mathbb{Z}$ that are 3 modulo 4, i.e. 3, 7, 11, 19, etc.*
- *Elements of the form $a \pm bi$ where a, b are integers and a^2+b^2 is a prime in $\mathbb{Z}$.*

11.4 Summary

- In integral domains: Prime $\Rightarrow$ Irreducible.
- In PID: Prime=Irreducible.
- ED $\Rightarrow$ PID $\Rightarrow$ UFD.
- In every PID any ascending chain of ideals eventually terminates.

12 Week 12: Review

12.1 Exercises

12.1.1 Problems for Grading

Exercise 12.1 (10 pts)**.** *Suppose a group G is a union of a family of proper normal subgroups each two of which only intersect trivially. Prove that G is Abelian.*

Exercise 12.2 (10 pts)**.** *Let p be a prime. Determine the number of group homomorphisms $\phi : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$. Do the same for $\phi : \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ times}} \to \mathbb{Z}_p$.*

Exercise 12.3 (10 pts)**.** *Suppose $f(x)$ is a non-constant polynomial in $\mathbb{Z}[x]$. Prove that $\langle f(x) \rangle$ is not a maximal ideal of $\mathbb{Z}[x]$.*

13 Week 13

We will now revisit some topics in Group Theory.

13.1 Sylow Theorems

Definition 13.1. Two elements a, b of a group G are said to be **conjugate** if $a = gbg^{-1}$ for some $g \in G$. The **conjugacy class** of an element a is given by $\text{cl}(a) = \{gag^{-1} \mid g \in G\}$.

Theorem 13.1. *Given a group G the relation $\sim$ defined by*

$$a \sim b \textit{ if and only if } a \textit{ and } b \textit{ are conjugates}$$

is an equivalence relation.

Example 13.1. Find all conjugacy classes of S_3.

Theorem 13.2. *Let a be an element of a group G. Then $|\text{cl}(a)| = [G : C(a)]$. Hence in a finite group the size of each conjugacy class divides the order of the group.*

Theorem 13.3. *Let G be a finite group, and let S be a set consisting of one element from each conjugacy class of G that contains at least two elements. Then,*

$$|G| = |Z(G)| + \sum_{a \in S} [G : C(a)].$$

The above theorem can be used to understand p-groups, those groups whose orders are prime-powers.

Definition 13.2. Let p be a prime. We say a finite group is a **p-group** if its order is of the form p^n for some positive integer n.

Theorem 13.4. *The center of every p-group is non-trivial.*

Corollary 13.1. Let p be a prime. Every group of order p^2 is Abelian.

13.2 The Sylow's Theorems

Theorem 13.5 (Sylow's First Theorem)**.** *Let G be a finite group, p be a prime, and k a positive integer for which p^k divides $|G|$. Then, G has a subgroup of order p^k.*

Definition 13.3. Let G be a finite group, and p be a prime dividing $|G|$. Suppose n is the largest positive integer for which p^n divides $|G|$. Any subgroup of G of order p^n is called a **Sylow p-subgroup**.

Corollary 13.2 (Cauchy's Theorem)**.** Let G be a finite group and p be a prime dividing $|G|$. Then, G has an element of order p.

Theorem 13.6 (Sylow's Second Theorem)**.** *If H is a p-subgroup of a finite group G, then H is contained in some Sylow p-subgroup of G.*

Definition 13.4. Two subgroups H and K of a group G are said to be **conjugate** if $H = gKg^{-1}$ for some $g \in G$.

Similar to what we saw before, "being conjugate" is an equivalence relation.

Theorem 13.7 (Sylow's Third Theorem)**.** *Let p be a prime, and let G be a group of order $p^n m$, where n and m are positive integers and p does not divide m. Then, the number of Sylow p-subgroups of G is 1 modulo p and divides m. Furthermore, any two Sylow p-subgroups of G are conjugate.*

Notation: The number of Sylow p-subgroups of a group G is denoted by $n_p(G)$. When the group is clear from the context this is often shortened as n_p.

Corollary 13.3. A Sylow p-subgroup of a finite group G is a normal subgroup of G if and only if it is the only Sylow p-subgroup of G.

Example 13.2. Any group of order 33 is cyclic.

Example 13.3. Suppose $p < q$ are primes for which p does not divide $q - 1$. Then, every group of order pq is cyclic.

Example 13.4. Let p be an odd prime, and n be a positive integer. Find all Sylow p-subgroups of D_{p^n}.

Example 13.5. Let $p < q$ be two primes for which p does not divide either $q - 1$ or $q + 1$. Prove that every group of order pq^2 is Abelian.

Check out more examples in the textbook.

13.3 Finite Simple Groups

Definition 13.5. A group is said to be **simple** if it has no non-trivial proper normal subgroups.

Example 13.6. For every prime p, the group $\mathbb{Z}_p$ is simple.

Theorem 13.8 (Sylow's Simplicity Criterion)**.** *Let n be a positive integer and let p be a prime dividing n. Suppose n is not a power of p. If 1 is the only integer dividing n that is 1 modulo p, then there are no simple groups of order n.*

Theorem 13.9. *Let $n > 1$ be an odd integer. Then, any group of order $2n$ has a normal subgroup of order n. Hence, there are no simple groups of order $2n$.*

Theorem 13.10. *Let H be a subgroup of a group G, and let S be the group of all permutations of the left cosets of H in G. Then, there is a homomorphism from G to S whose kernel lies in H and contains every normal subgroup of G that is contained in H.*

Corollary 13.4 (Index Theorem)**.** If G is a finite group and H is a proper subgroups of G such that $|G|$ does not divide $[G : H]!$, then H contains a non-trivial normal subgroup of G. In particular, G is not simple.

Corollary 13.5 (Embedding Theorem)**.** If a finite non-Abelian simple group G has a subgroup of index n, then G is isomorphic to a subgroup of A_n.

For every integer $n \geq 5$ the group A_n is simple,
The group $SL_n(\mathbb{R})/Z(SL_n(\mathbb{R}))$ is simple for every integer $n \geq 2$.

13.4 Warm-ups

Example 13.7. Prove that for a group element a we have $\text{c}l(a) = \{a\}$ if and only if a is in the center.

Solution. If a is in the center then, $gag^{-1} = a$ for every g and thus $\text{c}l(a) = \{a\}$.

If $\text{c}l(a) = \{a\}$, then for every group element g we must have $gag^{-1} = a$ and thus $ga = ag$, i.e. a is in the center. □

13.5 More Examples

Example 13.8. Prove there are no non-Abelian simple groups of order less than 60.

Solution. Suppose G be a non-Abelian simple group of order n. Since G is not cyclic n cannot be 1 or prime.

By Theorem 13.9, n cannot be double an odd integer. This leaves us with the following integers:

$$4, 8, 9, 12, 15, 16, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 39, 40, 44, 45, 48, 49$$

The integers 4, 8, 9, 16, 25, 27, 32, and 49 are of the form p^n, where p is prime and $n > 1$. By Theorem 13.4, $Z(G)$ is non-trivial, since $Z(G)$ is a normal subgroup, $Z(G) = G$, which is a contradiction.

This leaves us with the following integers:

$$12, 15, 20, 21, 24, 28, 33, 35, 39, 40, 44, 45, 48$$

Now we will use Sylow's Criterion to eliminate some more possibilities:

The only positive integer dividing 15 that is 1 mod 5 is 1.

The only positive integer dividing 20 that is 1 mod 5 is 1.

The only positive integer dividing 21 that is 1 mod 7 is 1.

The only positive integer dividing 28 that is 1 mod 7 is 1.

The only positive integer dividing 33 that is 1 mod 11 is 1.

The only positive integer dividing 35 that is 1 mod 5 is 1.

The only positive integer dividing 39 that is 1 mod 11 is 1.

The only positive integer dividing 40 that is 1 mod 5 is 1.

The only positive integer dividing 44 that is 1 mod 11 is 1.

The only positive integer dividing 45 that is 1 mod 5 is 1.

We are left with the following integers:

$$12, 24, 48$$

For 12, 24, and 48 let H be a Sylow 2-subgroup with $[G : H]! = 3!$ is not divisible by 12 (or 24 or 48) and thus by the Index Theorem, G is not simple. This completes the proof. □

Example 13.9. Let p, q, r be three distinct primes. Prove that any group of order pqr has a non-trivial proper cyclic normal subgroup.

Solution. First, WLOG assume $p < q < r$, and let G be a group of order pqr. We will prove one of the Sylow subgroups of G is normal. Since Sylow subgroups are of order p, q or r they are all cyclic.

Assume to the contrary that none of the Sylow subgroups is normal. Therefore, n_p, n_q, n_r are all more than 1. We will now obtain a contradiction by counting the number of elements of G and showing it must contain too many elements.

First, note that n_r must divide pq and must be 1 modulo r. Since $1 < p, q < r$ neither p nor q is 1 modulo r. Thus, $n_r = pq$. Asume $H_1, \ldots, H_{pq}$ are all distinct Sylow r-subgroups of G. Since H_j's are of prime order the order of $H_j \cap H_k$ is 1 and thus the union $\bigcup_{j=1}^{pq} H_j$ has $(r-1)pq = pqr - pq$ non-identity elements.

Now, we will look at the Sylow q-subgroups of G. By Sylow's Theorem n_q must divide pr. Since $1 < p < q$, we have $n_q \neq p$. Thus, we obtain $n_q = r$ or pr. Similar to above the union of these Sylow q-subgroups has $(q-1)r$ or $(q-1)pr$ non-identity elements. Therefore,

$$|G| \geq 1 + pqr - pq + qr - r > pqr - pq + r(q-1) \geq pqr - pq + rp > pqr,$$

which is a contradiction. Therefore, either $n_q = 1$ or $n_r = 1$ and thus G has a normal subgroups of order q or r. □

Example 13.10. Let $p < q$ be two odd primes for which $q \not\equiv \pm 1 \mod p$. Prove that every group of order p^2q^2 is Abelian.

Solution. Suppose G is a group of order p^2q^2. Let H be a Sylow p-subgroup of G. By Sylow's Theorem n_p divides q^2 and $n_p \equiv 1 \mod p$. Thus $n_p = 1, q$ or q^2. Since $q \not\equiv 1 \mod p$, we know $n_p \neq q$. If $n_p = q^2$, then p must divide $q^2 - 1 = (q-1)(q+1)$ and thus p must either divide $q - 1$ or $q + 1$.Hence, $q \equiv \pm 1 \mod p$, which is a contradiction. Therefore, $n_p = 1$. Thus, $H \lhd G$.
Similarly let K be a Sylow q-subgroup. Note that since p and q are odd and $p < q$ we have $1 < p-1 < p+1 < q$, and thus $p \not\equiv \pm 1 \mod q$. With a similar argument to above, $n_q = 1$. Therefore, $K \lhd G$.
Now, since $H \cap K$ is a subgroup of both H and K, its order must divide both p^2 and q^2. Therefore, $|H \cap K| = 1$.

Therefore, G is an internal direct product of H and K. By Theorem 7.6 $G \simeq H \times K$. By Theorem 7.7 both H and K are Abelian. Therefore, G is Abelian. □

13.6 Exercises

13.6.1 Problems for Grading

Definition 13.6. Suppose a permutation σ of S_n can be written as a product of disjoint cycles (including 1-cycles) of length $a_1, \ldots, a_k$, where $a_1 \leq a_2 \leq \cdots \leq a_k$. The sequence $a_1, a_2, \ldots, a_k$ is called the **cycle type of** σ.

Exercise 13.1 (20 pts)**.** *Let $n \geq 2$ be a positive integer. Prove that two elements of S_n are conjugates if and only if they have the same cycle type.*

Hint: First prove that $\sigma(a_1 \cdots a_k)\sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k))$.

Exercise 13.2 (10 pts)**.** *Let H be a subgroup of a group G. Prove that the number of conjugates of H in G is $[G : N(H)]$.*

Exercise 13.3 (10 pts)**.** *Let p be a prime and n, m be positive integers for which $1 < m < p$. Prove that there is no group of order $p^n m$ that is simple.*

Exercise 13.4 (10 pts)**.** *Page 399, Problem 26.*

Exercise 13.5 (10 pts)**.** *Page 401, Problem 62.*

Exercise 13.6 (10 pts)**.** *Page 416, Problem 19.*

Exercise 13.7 (10 pts)**.** *Page 417, Problem 31. (Assume the group has more than 2 elements.)*

13.6.2 Problems for Practice

Page 400-401: 50, 51, 54.

Page 415-417: 1, 2, 3, 4, 5, 16, 30.

13.6.3 Challenge Problems

Exercise 13.8. *Suppose p is a prime. Prove that every group of order $p^2 + p$ either has a normal subgroup of order p or a normal subgroup of order $p + 1$.*

13.7 Summary

- The center of any finite p-group is non-trivial.
- If p^k is a prime-power divisor of the order of a group G, then G has a subgroup of order p^k.
- For any prime dividing the order of a group, subgroups of the largest possible prime-power order are called Sylow subgroups.
- Sylow subgroups of the same order are conjugates.
- To prove groups of a certain order n are not simple:
  - Find a prime p dividing n for which the only divisor of n that is 1 mod p is 1.
  - Show $n/2$ is an odd integer.
  - Show there is a subgroup of order m for which n does not divide $(n/m)!$ A good candidate of such a subgroup is one of the Sylow subgroups.
  - Assume for each prime p dividing the order there are at least two Sylow p-subgroups. By counting the number of elements, show the group must have more than n elements.

14 Week 14

14.1 Generators and Relations (optional)

Let $S = \{a, b, c, \ldots\}$ be a set of distinct symbols and let $S^{-1} = \{a^{-1}, b^{-1}, \ldots\}$. A **word** from S is a finite string $x_1 \cdots x_n$ of symbols from $S \cup S^{-1}$. The string with no symbols is called the **empty word**. The set of all words from S is denoted by $W(S)$. We define a binary operation on $W(S)$ by concatenation. We say two words in $W(S)$ are equivalent if and only if one can be turned into another by a finite sequence of insertions or deletions of words of form xx^{-1} or $x^{-1}x$ with $x \in S$.

Example 14.1. The two words $abb^{-1}c^{-1}ca^{-1}$ and the empty word are equivalent.

Theorem 14.1. *Let S be a set of distinct symbols. For any word u in $W(S)$, let $\overline{u}$ denote the set of all words in $W(S)$ equivalent to u. Then, the set of all equivalence classes of elements of $W(S)$ is a group under the operation $\overline{u} \cdot \overline{w} = \overline{uv}$.*

Definition 14.1. The group in the above theorem is called the **free group on** S and is denoted by $F(S)$.

Theorem 14.2 (Universal Mapping Property)**.** *Every group is a homomorphic image of a free group, and thus every group is isomorphic to a factor group of a free group.*

Definition 14.2. Let G be a group generated by some set $A = \{a_1, \ldots, a_n\}$ and let F be the free group on A. Let $W = \{w_1, \ldots, w_m\}$ be a subset of F and let N be the smallest normal subgroup of F containing W. We say G is given by the generators $a_1, \ldots, a_n$ and the relations $w_1 = \cdots = w_m = e$ if there is an isomorphism from F/N onto G for which each a_iN is mapped to a_i.

A notation for the above is

$$G = \langle a_1, \ldots, a_n \mid w_1 = \cdots = w_m = e\rangle.$$

Example 14.2. Prove that $D_4 = \langle a, b \mid a^4 = b^2 = (ab)^2 = e\rangle$.

Example 14.3 (Dyck's Theorem)**.** Let

$$G = \langle a_1, \ldots, a_n \mid w_1 = \cdots = w_m = e\rangle$$

and let

$$\overline{G} = \langle a_1, \ldots, a_n \mid w_1 = \cdots = w_{m+k} = e\rangle$$

Then, $\overline{G}$ is a homomrphic image of G.

Theorem 14.3. *Let G be a finite group defined by a set of relations. If K is a group satisfying the defining relations of G and $|K| \geq |G|$, then $K \simeq G$.*

Example 14.4. Consider the subgroup of $GL_2(\mathbb{C})$ generated by $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Prove that this group is isomorphic to

$$\langle a, b \mid a^2 = b^2 = (ab)^2\rangle.$$

Note that here by a relation $x = y$ we mean $xy^{-1} = e$.

Example 14.5. For every $n \geq 2$ prove that:

$$D_n \simeq \langle a, b \mid a^n = b^2 = (ab)^2 = e\rangle.$$

The above example motivates the following definition.

Definition 14.3. A group is called **dihedral** if it is isomorphic to D_n for some $n \geq 2$ or it is isomorphic to the **infinite dihedral group** given below:

$$D_\infty = \langle a, b \mid a^2 = b^2 = e\rangle.$$

Theorem 14.4. *Any group generated by a pair of elements of order 2 is a dihedral group.*