Preliminaries

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Portions are also drawn from Keith Conrad's notes on the dihedral groups.

This first set of notes covers material that students should be familiar with from MTH331.

1. Basic Set Theory

Definition: Set, elements

A *set* X is a well-defined collection of objects, called *elements*. One should be able to determine membership in a set. We write $a \in X$ to say an element is in the set.

Example. Important sets to know are

(1) $\mathbb{N}$, the natural numbers $1, 2, 3, \ldots$
(2) $\mathbb{Z}$, the integers
(3) $\mathbb{Q}$, the rationals
(4) $\mathbb{R}$, the reals
(5) $\mathbb{C}$, the complex numbers
(6) $\emptyset$, the empty set.

We now briefly discuss basic operations on sets.

Definition: Subset

A *subset* of a set X is a set Y such that for all $y \in Y$, $y \in X$. We write $Y \subset X$. We say sets X and Y are *equal* and write $X = Y$ if $X \subset Y$ and $Y \subset X$. We say Y is a *proper subset* of X if $Y \subset X$ and $Y \neq X$.

Example. $\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Operations on sets: Let A and B be subsets of a (universal) set U.

- Union of A and B: $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- Intersection of A and B: $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- Complement of A in U: $A' = \{x : x \in U \text{ and } x \notin A\}$
- Difference: $A \backslash B = \{x : x \in A \text{ and } x \notin B\}$
- Cartesian Product: $A \times B = \{(a, b) : a \in A, b \in B\}$

Proposition 1: Set Laws

Let A, B, C be sets.

(1) $A \cup A = A$, $A \cap A = A$, $A \backslash A = \emptyset$.
(2) $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.
(3) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$.
(4) $A \cup B = B \cup A$, $A \cap B = B \cap A$.
(5) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
(6) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. We will prove the first statement in (3). The remainder are left as an exercise.

Let $x \in A \cup (B \cup C)$. Then $x \in A$ or $x \in B \cup C$. In the first case $x \in A$ so $x \in A \cup B$. Thus, $x \in (A \cup B) \cup C)$. In the second case, either $x \in B$ or $x \in C$. If $x \in B$ then $x \in A \cup B$. Now in either of these cases, $x \in (A \cup B) \cup C$. Hence, $A \cup (B \cup C) \subset (A \cup B) \cup C$.

Now suppose $x \in (A \cup B) \cup C$. Then either $x \in A \cup B$ or $x \in C$. In the second case $x \in B \cup C$. In the first case, either $x \in A$, or else $x \in B$, whence $x \in B \cup C$. Thus, in all cases either $x \in A$ or $x \in B \cup C$. Thus $(A \cup B) \cup C \subset A \cup (B \cup C)$. This implies that $A \cup (B \cup C) = (A \cup B) \cup C$, as desired. □

Theorem 2: DeMorgan's Laws

Let A and B be subsets of a (universal) set U.

(1) $(A \cup B)' = A' \cap B'$.
(2) $(A \cap B)' = A' \cup B'$.

Proof. We prove (1) and leave (2) as an exercise.

Suppose $x \in (A \cup B)'$. Then $x \in U$ and $x \notin A \cup B$. If $x \in A$, then $x \in A \cup B$, a contradiction. Thus, $x \notin A$. Said otherwise, $x \in A'$. By similar logic, $x \in B'$. Thus, $x \in A' \cap B'$. Thus, $(A \cup B)' \subset A' \cap B'$.

Suppose $x \in A' \cap B'$. Then $x \in A'$ and $x \in B'$. If $x \in A \cup B$, then either $x \in A$ or $x \in B$. The first case contradicts $x \in A'$ and the second contradicts $x \in B'$. We conclude that $x \notin A \cup B$, so $x \in (A \cup B)'$. Hence, $A' \cap B' \subset (A \cup B)'$, so combined with the first paragraph we have $(A \cup B)' = A' \cap B'$. □

Formally, a *relation* on sets X and Y is a subset of the Cartesian product $X \times Y$. A function is actually a special type of relation. Formally, a function is a relation $f \subset X \times Y$ satisfying if $(a, b), (a, c) \in f$ then $b = c$. (Here, X is the domain and Y is the codomain.)

For a set X, a *binary relation* is a subset $R \subset X \times X$. However, we often use different notation for binary relations. Instead of $(a, b) \in R$, we say $\sim$ is a binary relation and write $a \sim b$.

Definition: Equivalence relation, equivalence class

A binary relation $\sim$ on X is an *equivalence relation* on a set X if it satisfies the following:

- (reflexive property) $x \sim x$ for all $x \in X$;
- (symmetric property) if $x \sim y$, then $y \sim x$;
- (transitive property) if $x \sim y$ and $y \sim z$, then $x \sim z$.

The *equivalence class* of $x \in X$ is the set $[x] = \{y \in X : x \sim y\}$.

We will often write $x \sim y$ in place of $(x, y) \in R$.

Example (Congruence mod n)**.** Fix a positive integer n. We define a binary relation on $\mathbb{Z}$ by the rule $x \sim y$ if and only if $x - y$ is divisible by n. We claim that $\sim$ is an equivalence relation.

Let $x \in \mathbb{Z}$, then $x - x = 0$ and 0 is divisible by n. Thus $x \sim x$ for all $x \in X$, so the reflexive property holds.

Now suppose that $x, y \in \mathbb{Z}$ such that $x \sim y$. Then $x - y = nk$ for some integer k. Thus, $y - x = n(-k)$ and so $y - x$ is divisible by n and so $y \sim x$. Thus, the symmetric property holds.

Finally, suppose $x, y, z \in \mathbb{Z}$ such that $x \sim y$ and $y \sim z$. Then $x - y = nk$ and $y - z = n\ell$ for some integers k and ℓ. Now $x - z = (x - y) + (y - z) = nk + n\ell = n(k + \ell)$. Since $k + \ell$ is another integer (by closure under addition) then $x - z$ is divisible by n. Therefore $x \sim z$ so $\sim$ is transitive.

Thus, $\sim$ is an equivalence relation on $\mathbb{Z}$. We will often write $x \equiv y \mod n$ if $x \sim y$. (Note that by symmetry we can also write $y \equiv x \mod n$. If $x \in \mathbb{Z}$, then the equivalence class of $[x]$ is the set of integers that differ from x by a multiple of n.

Example (Congruence mod 5)**.** We have already checked that this is an equivalence relation. A complete set of equivalence classes are $[0], [1], [2], [3], [4]$. Clearly, none of these sets are the same since none of the *representatives* differ from one another by a multiple of 5. Moreover, *any other number* differs from exactly one of the above by a multiple of 5.

We can perform arithmetic on the equivalence classes above just as we would on the integers. For example, $3 + 4 = 7$ but $7 \equiv 2 \mod 5$ and so we write $3 + 4 \equiv 2 \mod 5$. Thus, $[3] + [4] = [2]$. Now observe that if we take any elements from either equivalence class, this equality still holds. For example, $13 \in [3]$ and $24 \in [4]$ but $13 + 24 = 37 \in [2]$. Moreover, this operation is associative. The element $[0]$ acts as an identity ($[0] + [k] = [k]$) and every element has an inverse ($[1] + [4] = [0]$ and $[2] + [3] = [0]$). Thus, the equivalence classes of the integers mod 5 is another example of a *group*.

Everything we've just done works perfectly well with 5 replaced by any positive number n.

Definition: Partition

A *partition* P of a set X is a collection of nonempty sets $X_1, X_2, \ldots$ such that $X_i \cap X_j = \emptyset$ for all $i \neq j$ and $\bigcup_k X_k = X$.

Theorem 3: Equivalence classes are partitions

Let $\sim$ be an equivalence relation on a set X.

(1) If $y \sim x$, then $[x] = [y]$.

(2) Given $x, y \in X$, $[x] = [y]$ or $[x] \cap [y] = \emptyset$ (equivalence classes are either equal or disjoint).

(3) The equivalence classes of X form a partition of X.

Proof. (1) Let $z \in [x]$, then $x \sim z$, so $y \sim z$ by transitivity. Thus, $z \in [y]$ and so $[x] \subset [y]$. Similarly, $[y] \subset [x]$ (exercise), so $[x] = [y]$.

(2) Choose $x, y \in X$ and suppose $[x] \cap [y] \neq \emptyset$. Then there exists $z \in [x] \cap [y]$. Thus, $z \in [x]$ and $z \in [y]$ so $x \sim z$ and $y \sim z$. By symmetry, $z \sim y$ and by transitivity, $x \sim y$. By (1), $[x] = [y]$.

(3) Since $x \sim x$, then $x \in [x]$ and so every element of X belongs to (at least) one equivalence class. By (2), we can choose $[x_1], [x_2], \ldots$, a complete set of (disjoint) equivalence classes such that $\bigcup_{k \in X} [x_k] = X$. □

We have shown that every equivalence relation determines a partition. But, in fact, the opposite is also true: every partition determines an equivalence relation. (Thus, there is a bijection between the equivalence relations and partitions of a given set X.)

Exercise. Given a partition $P = \{X_i\}$ of a set X, define a binary relation on X by the rule that $x \sim y$ if $x, y \in X_i$. Check that this rule indeed defines an equivalence relation.

2. Functions

We have seen one definition of a function in terms of relations. The following definition is independent of that.

Definition: Function, domain, codomain

Let A and B be sets. A *function* $f : A \to B$ is a rule that assigns each $a \in A$ a unique output, denoted $f(a) \in A$. The set A is called the *domain of* f and B the *codomain of* f.

So, there are two requirements for a *rule* $A \to B$ to be a *function*. First, every input must land in B. Secondly, each input must give a *unique* output. When a rule fails to follow either of these rules, we say it is not *well-defined*.

Example. (1) Define a rule $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = 2x$. Then every output has a unique output, so f is a (well-defined) function.

(2) Define a rule $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = x/2$. Then $f(1) \notin \mathbb{Z}$, so f is not well-defined.

(3) Define a rule $f : \mathbb{Q} \to QQ$ by $f(p/q) = p + q$. Then $f(1/2) = 3$ while $f(2/4) = 6$. So, while $1/2 = 2/4$, $f(1/2) \neq f(2/4)$. Hence, f is not well-defined.

Definition: Surjective, injective, bijective, permutation

Let $f : A \to B$ be a function. If $f(A) = B$, then f is said to be *surjective* (or *onto*). If for all $a_1, a_2 \in A$ such that $a_1 \neq a_2$ we have $f(a_1) \neq f(a_2)$, the f is said to be *injective* (or *one-to-one*). A function that is both injective and surjective is said to be *bijective*. A bijective function from a set to itself is a *permutation*.

Example. (1) The map $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$ is bijective.

Suppose $x, y \in \mathbb{Z}$ such that $f(x) = f(y)$. Then $x + 1 = y + 1$, so $x = y$ and thus f is injective. Now suppose $z \in \mathbb{Z}$. Then $f(z - 1) = (z - 1) + 1 = z$, so f is surjective.

(2) The map $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2x$ is injective but not surjective.

Suppose $x, y \in \mathbb{Z}$ such that $f(x) = f(y)$. Then $x + 1 = y + 1$, so $x = y$ and thus f is injective. But note that if $f(n) = 1$ then $2n = 1$, so $n = 1/2 \notin \mathbb{Z}$. Thus, f is not surjective.

(3) The map $f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(x) = \begin{cases} x & \text{if } x \text{ is odd} \\ x/2 & \text{if } x \text{ is even} \end{cases}$$

is surjective but not injective.

Let $z \in \mathbb{Z}$. Then $2z$ is even and so $f(2z) = (2z)/2 = z$. Thus, f is surjective. However, $f(1) = 1 = f(2)$ and $1 \neq 2$, so f is not injective.

Recall that if $f : A \to B$ and $g : B \to C$ are functions, then the *composition* $g \circ f : A \to C$ is defined by the rule

$$(g \circ f)(a) = g(f(a)) \quad \text{for all } a \in A.$$

Theorem 4: Properties of composition

Let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be functions.

(1) We have $(h \circ g) \circ f = h \circ (g \circ f)$. That is, function composition is associative.

(2) If f and g are injective, then $g \circ f$ is injective.

(3) If f and g are surjective, then $g \circ f$ is surjective.

(4) If f and g are bijective, then $g \circ f$ is bijective.

Proof. (1) By definition, two functions are equal if they agree at every element of their domain. Let $a \in A$. Then

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)) = h((g \circ f)(a)) = (h \circ (g \circ f))(a).$$

Hence, (1) holds.

(2) Suppose f and g are injective. We claim $g \circ f : A \to C$ is injective. Suppose there are $a, a' \in A$ such that $(g \circ f)(a) = (g \circ f)(a')$. Then $g(f(a)) = g(f(a'))$. By injectivity of g, $f(a) = f(a')$. By injectivity of f, $a = a'$. Hence, $g \circ f$ is injective.

(3) Suppose f and g are surjective. We claim $g \circ f : A \to C$ is surjective. Choose $c \in C$. Because g is surjective there exists $b \in B$ of c, so $g(b) = c$. Because f is surjective, there exists a preimage $a \in A$ of b, so $f(a) = b$. Then $(g \circ f)(a) = g(f(a)) = g(b) = c$. Thus, $g \circ f$ is surjective.

(4) This follows from properties (2) and (3). □

Property (1) from Theorem 4 says that composition of functions is associative while Property (4) says that the composition of two bijections is another bijection.

If $f : A \to B$ is a function of sets, then for any subset $C \subset B$, we define the *preimage of* C to be

$$f^{-1}(C) = \{a \in A : f(a) \in C\}.$$

Note in general that f^{-1} *is not* a function. For example, consider our previous example $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x$ if x is odd and $f(x) = x/2$ if x is even. Then $f^{-1}(1) = \{1, 2\}$ since $f(1) = f(2) = 1$. Hence, f^{-1} is not well-defined.

For every set A, there is a function $\mathrm{id}_A : A \to A$, called the *identity map on* A, defined by

$$\mathrm{id}_A(a) = a \text{ for all } a \in A.$$

Note that if $f : A \to B$ is any function (with domain A), then $f \circ \mathrm{id}_A = f$. Similarly, if $g : B \to A$ is any function (with codomain A), then $\mathrm{id}_A \circ g = g$.

Definition: Invertible function, inverse

A function $f : A \to B$ is *invertible* if there exists another function $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. In this case, the map g is called an *inverse of* f.

This next argument is one that we will see many times in this course. Recall that, generally, to prove to objects are unique we assume there are two objects with the requisite property and show that they are the same.

Theorem 5: Uniqueness of the inverse

The inverse of an invertible function is unique.

Proof. Suppose $f : A \to B$ is an invertible function with inverses g and h. Let $a \in A$. Then by the definition of an inverse function and associativity of composition,

$$h(a) = h(\mathrm{id}_A(a)) = h((f \circ g)(a)) = (h \circ (f \circ g))(a) = ((h \circ f) \circ g)(a) = \mathrm{id}_B(g(a)) = g(a).$$

Thus, $h = g$. □

Hence, if f is an invertible function, then there is no ambiguity in referring to *the* inverse of f, which we denote by f^{-1}.

Theorem 6: Invertibility is equivalent to bijectivitiy

A function $f : A \to B$ is invertible if and only if is bijective.

Proof. First assume f is invertible. By definition, there exists and inverse map f^{-1}. Let $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$. Applying f^{-1} to both sides gives $a_1 = a_2$, so f is injective. Let $b \in B$ and set $a = f^{-1}(b)$. Applying f to both sides gives $f(a) = b$, so f is surjective and hence bijective.

Now assume f is bijective. Let $b \in B$, then by surjectivity there is some $a \in A$ such that $f(a) = b$. By injectivity, a is the only element in A such that $f(a) = b$. Hence, the function $g : B \to A$ defined by $g(b) = a$ (the preimage of b) is well-defined. Then $g(f(a)) = g(b) = a$ and $f(g(b)) = f(a) = b$, so $g = f^{-1}$. □

The First Principle of Mathematical Induction

Let $S(n)$ be a statement about the integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If for all integers k with $k \geq n_0$, $S(k)$ true implies $S(k+1)$ is true, then $S(n)$ is true for all integers $n \geq n_0$. The statement $S(k)$ is referred to as the *inductive hypothesis*.

Example. Prove $10^{n+1} + 10^n + 1$ is divisible by 3.

Here we set $n_0 = 0$, so $S(0)$ is the statement that 12 is divisible by 3. That is true so assume $S(k)$ is true for some $k \geq 0$. That is, $10^{n+1} + 10^n + 1 = 3m$ for some integer m. Now $S(k+1)$ is the statement that $10^{k+2} + 10^{k+1} + 1$ is divisible by 3. By algebra we have

$$\begin{aligned} 10^{k+2} + 10^{k+1} + 1 &= 10(10^{k+1} + 10^k) + 1 \\ &= 10(3m - 1) + 1 \quad \text{by the inductive hypothesis} \\ &= 30m - 9 \\ &= 3(10m - 3). \end{aligned}$$

Thus, $S(k+1)$ is true and so by the (First) Principle of Mathematical Induction, $S(n)$ is true for all integers $n \geq 0$.

The Well-Ordering Principle

Every nonempty subset of $\mathbb{N}$ contains a least element.

Note that the First Principle of Mathematical Induction implies the Well-Ordering Principle.

The next theorem is an example of an *existence and uniqueness proof*. While this theorem is stated for integers but applies equally well to many other sets with an almost identical proof, as we will see later in the course.

Theorem 7: The Division Algorithm

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.

Proof. (Existence) Let $S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\} \subset \mathbb{N}$. If $0 \in S$, then b divides a so choose $q = a/b$ and $r = 0$. Assume $0 \notin S$. If $a \geq 0$, then $a = a - b \cdot 0 \in S$. If $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. In either case, $S \neq \emptyset$ and so we may apply the Well-Ordering Principle to find a least member of S, say r. By definition of S, there exists an integer q such that $r = a - bq$. That is, $a = bq + r$ and $r \geq 0$ by definition of S. We claim $r < b$. Suppose otherwise. Then

$$a - b(q+1) = a - bq - b = r - b > 0.$$

But then $a - b(q+1) \in S$ and $a - b(q+1) < r$, contradicting the choice of r.

(Uniqueness) Suppose there exist r, r', q, q' such that $a = bq + r$ and $a = bq' + r'$ with $0 \leq r, r' < b$. Then $bq + r = bq' + r'$. Assume $r' \geq r$. Then $b(q - q') = r - r'$ so b divides $r' - r$ and $0 \leq r' - r \leq r' < b$. Thus, $r' - r = 0$ so $r = r'$ and $q = q'$. □

We say a (nonzero) integer b divides an integer a if the (unique) r appearing the Division Algorithm is zero. We will often use the notation $b \mid a$ in place of b divides a. An integer d is a *common divisor* of integers a, b if $d \mid a$ and $d \mid b$. The *greatest common divisor* of $a, b \in \mathbb{Z}$ is a positive integer d that is a common divisor of a and b and for any other common divisor d' of a and b, $d' \mid d$. We write $d = \gcd(a, b)$.

The proof of the next theorem uses a similar idea as the Division Algorithm.

Theorem 8

Let a and b be nonzero integers. There exist integers r, s such that $\gcd(a, b) = ar + bs$. Furthermore, the gcd of a and b is unique.

Proof. Let $S = \{ar + bs : r, s \in \mathbb{Z} \text{ and } ar + bs > 0\}$. If $a, b > 0$, then $a(1) + b(1) > 0$. The other cases for a and b are similar. Thus, $S \neq 0$ and so by the Well-Ordering Principle S contains a least element, say $d = ar + bs$. We claim that $d = \gcd(a, b)$.

Write $a = dq + r'$ according to the Division Algorithm, where $0 \leq r' < d$. Suppose $r' > 0$. Then

$$r' = a - dq = a - (ar + bs)q = a(1 - rq) + b(-sq) \in S.$$

Since $r' < d$, this contradicts the minimality of d, so we must have $r' = 0$. That is $d \mid a$. A similar argument shows that $d \mid b$, so d is a common divisor of a and b.

Suppose d' is any common divisor of a and b. then $a = d'h$ and $b = d'k$ for integers h and k. Then

$$d = ar + bs = (d'h)r + (d'k)s = d'(hr + ks).$$

Thus, $d' \mid d$. It follows that d is the unique gcd of a and b. □

Note that the theorem only claims uniqueness of the gcd itself, and not the integers r and s. In fact, there are *infinitely* many integers that produce the gcd. The Division Algorithm does, however, give a methodology for producing a pair of such integers, as illustrated in the next example.

Example (Euclidean Algorithm)**.** Calculate $d = \gcd(471, 562)$ and find integers r and s such that $d = 471r + 562s$.

We repeatedly apply the division algorithm.

$$\begin{aligned} 562 &= 471 \cdot 1 + 91 \\ 471 &= 91 \cdot 5 + 16 \\ 91 &= 16 \cdot 5 + 11 \\ 16 &= 11 \cdot 1 + 5 \\ 11 &= 5 \cdot 2 + 1 \\ 5 &= 1 \cdot 5 + 0. \end{aligned}$$

Thus, $d = 1$. That is, 471 and 562 are relatively prime. Now by reversing:

$$\begin{aligned} 1 &= 11 + (-2) \cdot 5 = 11 + (-2)[16 + (-1) \cdot 11] \\ &= (3) \cdot 11 + (-2) \cdot 16 = (3) \cdot [91 + (-5) \cdot 16] + (-2) \cdot 16 \\ &= (3) \cdot 91 + (-17) \cdot 16 = (3) \cdot 91 + (-17) \cdot [471 + (-5) \cdot 91] \\ &= (88) \cdot 91 + (-17) \cdot 471 = (88) \cdot [562 + (-1) \cdot 471] + (-17) \cdot 471 \\ &= (88) \cdot 562 + (-105) \cdot 471 \end{aligned}$$

Hence, $r = -105$ and $s = 88$.

An integer $p > 1$ is *prime* if $x \mid p$ for $x > 1$ implies that $x = p$. The reason for omitting 1 as a prime becomes clear in light of the Fundamental Theorem of Arithmetic, proved below. In particular, we wish for every positive integer to have a *unique* decomposition in terms of prime numbers (e.g., $30 = 2 \cdot 3 \cdot 5$). But if we allow 1 to be prime then we lose uniqueness.

Lemma 9

Let $a, b \in \mathbb{Z}$ and p a prime number. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Suppose $p \nmid a$. We must show that $p \mid b$. Since p does not divide a, then $\gcd(a, p) = 1$. Thus, there exist integers r, s such that $ar + ps = 1$. Thus,

$$b = b \cdot 1 = b(ar + ps) = (ba)r + p(bs).$$

Since $p \mid ab$ and $p \mid p$, then p divides the right-hand sides. Consequently, p must divide the left-hand side, so $p \mid b$. □

Theorem 10: The Fundamental Theorem of Arithmetic

Let n be an integer such that $n > 1$. Then $n = p_1 p_2 \cdots p_k$ where the p_i are prime. Furthermore, if $n = q_1 q_2 \cdots q_\ell$ where the q_i are prime, then $k = \ell$ and the q_i are a rearrangement of the p_i.

Proof. (Existence) Let S be the set of all integers greater than 1 that cannot be written as the product of primes and suppose $S \neq \emptyset$. By the Well-Ordering principle, S has a least element, say a. If the only positive factors of a are a and 1, then a is prime, a contradiction. Hence we may assume $a = a_1 a_2$ where $1 < a_1, a_2 < a$. Since a is the minimal element of S, then $a_1, a_2 \notin S$. Hence, both a_1 and a_2 can be written as the product of primes:

$$a_1 = p_1 \cdots p_r$$

$$a_2 = q_1 \cdots q_s.$$

But then

$$a = a_1 a_2 = p_1 \cdots p_r q_1 \cdots q_s.$$

Thus, $a \notin S$, a contradiction.

(Uniqueness) The theorem is certainly true for $n = 2$ as 2 is prime. Suppose the theorem holds for all integers[1] m such that $1 \leq m < n$. Write

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell,$$

where $p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_\ell$. By the previous lemma, $p_1 \mid q_i$ for some q_i, $i = 1, \ldots, \ell$, and $q_1 \mid p_j$ for some $j = 1, \ldots, k$. The p_i and q_i are prime. so $p_1 = q_i$ and $q_1 = p_j$. Hence, $p_1 \leq p_j = q_1 \leq q_i = p_1$, so $p_1 = q_1$. Hence, we can divide that on both sides and obtain

$$n' = p_2 \cdots p_k = q_2 \cdots q_\ell.$$

Since $n' < n$, then by the (strong) inductive hypothesis, n' has a unique factorization. Hence, $k = \ell$ and $q_i = p_i$ for $i = 1, \ldots, k$. □

[1] In this theorem we are actually making use of *strong* induction.

Introduction to Groups

At its heart, Group Theory is the study of "symmetries" of objects. What symmetry means, and what sort of objects we will study, is a major focus of this course. Though everything we will do is directly related to symmetry in some way, the precise connection will sometimes be obscured by abstractness. This is intentional so that these ideas will apply as broadly as possible.

Most of this course is devoted to the study of *groups*. Though you may not know the definition of a group yet, you have seen them throughout most of your life. Consider the set of integers ($\mathbb{Z}$) and the operation of addition. Some observations we can make, that you know well already, are

- The sum of two integers is another integer.
- The operation of addition is associative.
- The number 0 acts as an identity, so that $0 + n = n$ for all $n \in \mathbb{Z}$.
- For every integer n, there is another integer $-n$, such that $n + (-n) = 0$.

These properties collectively make $\mathbb{Z}$ with this operation into a group[1]. It would be natural to ask whether we could choose a different operation for the integers, say multiplication. You should think about whether the above properties still hold if we replace addition by multiplication,

There are lots of other examples of groups which you have seen, including:

- the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, or the complex numbers $\mathbb{C}$ under addition;
- $n \times n$ matrices (over any of the fields mentioned above) under matrix addition;
- functions $f : \mathbb{R} \to \mathbb{R}$ under pointwise addition.

We will study all of these examples, and more, but this is not where we will begin the course. Instead, we will make the connection between groups and symmetries very clear through the study of dihedral groups.

[1]You may also note that the operation of addition on the integers is commutative, that is, $m + n = n + m$ for all $m, n \in \mathbb{Z}$. This is sort of a bonus, called the *abelian* property, which we will not require for groups

1. Symmetries of an equilateral triangle

A regular polygon is one whose sides all have equal length[2]. We will refer to such an object as a regular n-gon, where n denotes the number of sides. (Throughout, $n \geq 3$ for somewhat obvious reasons.) Here are some examples of regular n-gons:

Definition: Symmetry

A *symmetry* of a regular n-gon is a permutation of the vertices preserving adjacency.

A symmetry is an example of a *rigid motion* in the plane ($\mathbb{R}^2$). However, there are other types of rigid motions, including translations, that we do not consider. To cut down on the terminology a little bit, we will first study symmetries of an equilateral triangle.

There are a total of six symmetries: three reflections and three rotations (counterclockwise). (Note that a rotation by 360° is the same as a rotation by 0°.) These symmetries do not change the object itself, but they do permute the vertices. We record the results of these below.

[2]The definition of a regular polygon implies that all angles within the regular polygon are also congruent. You can prove this using congruent triangles.

The set of these symmetries is called[3] D_3. We can think of each one as a function and compose them just as we would compose two functions. Remember that function composition is from right-to-left.

Example. Compute each of the following compositions.

(1) $\rho_1 \circ \mu_1$

(2) $\mu_1 \circ \mu_2$

We can check all 36 compositions and record them in a multiplication-like table. More formally, this is called a *Cayley table*. We need to be careful, though, because the element in row a and column b is $a \circ b$, but this means we perform b *first* and a *second*.

[3]This group is sometimes referred to as D_6 (because it has 6 elements). Always pay attention to conventions when consulting a new text.

We make a few observations about the table above that reveal the defining properties of a group.

There are some other observations we can make that will be true for symmetries in general.

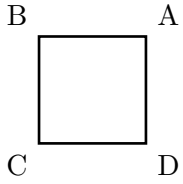
Example. (1) Identify the inverse of each element in D_3.

(2) For each element in D_3, determine how many times one would need to compose it with itself in order to obtain the identity. That is, for a in D_3, how many a's do we need to get $a \circ a \circ \cdots \circ a = \rho_0$.

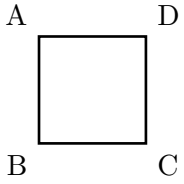
We call this the *order* of the element.

Our analysis and methods above extend easily to the symmetry group of a square, denoted D_4. There are a total of eight symmetries of a square: four rotations (including the trivial rotation) and four reflections.

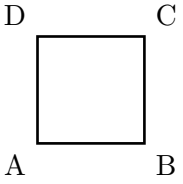
rotation 0° (ρ_0)



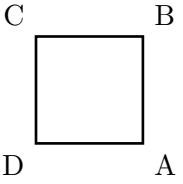
rotation 90° (ρ_1)



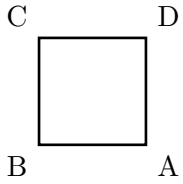
rotation 180° (ρ_2)



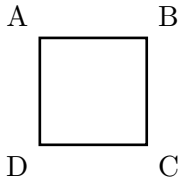
rotation 270° (ρ_3)



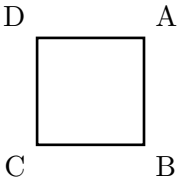
reflection about horizontal axis (μ_1)



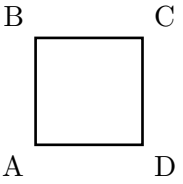
reflection about vertical axis (μ_2)



reflection about positive diagonal (μ_3)



reflection about negative diagonal (μ_4)



We will construct the Cayley table for this group.

We notice that our observations from above for D_3 all seem to hold for D_4 as well. That is, D_4 satisfies the properties of a group.

Example. (1) Find the inverse of each element in D_4.

(2) Find the order of each element in D_4.

(3) Find the elements of D_4 that commute with all other elements. (That is, find those $a \in D_4$ such that $a \circ b = b \circ a$ for all $b \in D_4$).

2. The group D_n

Here we generalize our discussion on D_3 to arbitrary regular polygons. Throughout this section, $n \geq 3$. The set of symmetries of a regular n-gon, along with the operation of composition of symmetries, is known as the *dihedral group* and is denoted D_n. Our goal here will be to develop some consistent notation for D_n, along with basic facts about this group.

Theorem 1: Order of D_n

The order of D_n is $2n$.

Next we show how to express D_n in more conventional group-theoretic notation. That is, we will replace composition with multiplication. The ability to switch between different notations will be an important skill to develop through this course.

Let $r \in D_n$ denote the rotation by $(360/n)^\circ$ and let $s \in D_n$ denote *any reflection through a vertex*. Let 1 be the identity in D_n. Note that $r^n = 1$ and $s^2 = 1$. Then it follows that the $2n$ elements of D_n are

$$\{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$$

The elements $1, r, r^2, \ldots, r^{n-1}$ are the rotations while the remaining elements $s, rs, r^2s, \ldots, r^{n-1}s$ are reflections.

We will now prove a critical defining relation in D_n.

Theorem 2: Relation on D_n

In D_n, $srs = r^{-1}$.

Example. (1) Write the Cayley table of D_3 using the r, s notation above.

(2) Write the Cayley table of D_4 using the r, s notation above.

3. The definition of a group

We now have sufficient setup to define the notion of a group. We will consider a few examples before returning to the dihedral group.

Recall that function f between sets X and Y, written $f : X \to Y$, is a rule such that for each $x \in X$, there is a unique output $f(x) \in Y$. This means that if $x_1 = x_2$ in X, then $f(x_1) = f(x_2)$.

Definition: Binary operation

A *binary operation* on a set S is a function $f : S \times S \to S$.

Often times we ignore the function itself, we will use operation notation. So instead of $f(s, s')$ we might write $s \cdot s'$. If $\cdot$ is a binary operation on S, then we say that S is *closed under* $\cdot$.

Example. The following are examples (or non-examples) of binary operations.

Definition: Group

A *group* is a pair $(G, \cdot)$ with G a set and $\cdot$ a binary operation on G satisfying
(1) for any $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity);
(2) there exists $e \in G$ such that $a \cdot e = a = e \cdot a$ for all $a \in G$ (existence of an identity element);
(3) for each $a \in G$ there exists an element $b \in G$ such that $a \cdot b = e = b \cdot a$ (closure under inverses).

To verify that a set and operation are a group actually requires checking four axioms, since we must verify that $\cdot$ is a binary operation.

Definition: Abelian group

A group $(G, \cdot)$ such that $a \cdot b = b \cdot a$ for all $a, b \in G$ is said to be *abelian*.

Example. The following are examples of groups with which you are already familiar.

Example (The group $\mathcal{S}_3$)**.**

Example (The group $\mathcal{F}$)**.**

4. The group of rotations, addition mod n, and roots of unity

Let R be the subset of D_3 consisting of rotations (though this also works for D_4 and in fact any D_n as we will see). Since the composition of two rotations is another rotation, then R is closed under composition. Furthermore,

Consequently, R is a group itself under composition of symmetries. We have now just seen our first example of a *group within a group*.

Definition: Subgroup

A *subgroup* of a group G is a subset H that is a group with respect to the operation associated to G.

Example. The following are further examples of subgroups.

Let $R_n = \{1, r, \ldots, r^{n-1}\}$ denote the subgroup of rotations of D_n (this is a subgroup by the same logic as above). Recall that $r^n = 1$. To compute a product of rotations, so that the result is an element of R_n, we must use *modular arithmetic*. For example, in D_4, $r^2 \cdot r^3 = r$ because

$$r^5 = r^4 \cdot r = 1 \cdot r = r.$$

Example. Let R_{12} be the subgroup of rotations of D_{12} (symmetries of a dodecagon)[4]. each of the following.

(1) Compute $r^4 \cdot r^3$

(2) Compute $r^8 \cdot r^7$

(3) Compute $r^3 \cdot r^9$

(4) Give an explicit formula for the inverse of a rotation r^k in R_{12}.

You should notice that doing computations in R_{12} is not altogether different than doing arithmetic on a clock[5].

The (sub)group R_n goes under many guises and has many different names. We will introduce two of them here.

Fix a positive integer n. Recall that congruence mod n is the equivalence relation[6] $\sim$ on $\mathbb{Z}$ defined by $x \sim y$ if $x - y$ is divisible by n. We typically write $x \equiv y \mod n$ in place of $x \sim y$. Let $\mathbb{Z}_n$ denote the collection of distinct equivalence classes under congruence mod n. So

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

(Recall that, since the equivalence classes partition $\mathbb{Z}$, every integer belongs to exactly one of the above equivalence classes and two given equivalence classes are either equal or disjoint.) We will show that $\mathbb{Z}_n$ is a group under addition of equivalence classes (addition mod n).

[4]Not to be confused with the hip-hop group D12 featuring Eminem and Proof, amongst others.

[5]My daughter can do this, and she's six, so you should certainly be able to do it.

[6]See preliminaries

Example. Let n be a positive integer. Define a rule $f : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by $f([a], [b]) = [a + b]$. We claim that f is a function (i.e., is well-defined). This shows that addition mod n is a binary operation on $\mathbb{Z}_n$.

Example (The group $\mathbb{Z}_n$)**.**

Exercise. Show that multiplication mod n is a binary operation but that $\mathbb{Z}_n$ is not a group under this operation.

It should (hopefully) be clear at this point the connection between addition mod n and the rotation subgroup of D_n. Just as [3] and [7] represent the same element in $\mathbb{Z}_4$, so do the rotations r^3 and r^7 in R_4. In fact, the relationship between these two groups can be made even more precise. First, we make a Cayley table for both groups.

Define a map $\phi : R_4 \to \mathbb{Z}_4$ by $r^k \mapsto [k]$. Using this map to substitute elements in the R_4 table (for example, r^3 is replaced by [3]) produces the $\mathbb{Z}_4$ table. When such a map exists between two groups and their corresponding Cayley tables, we say the groups are *isomorphic*. Essentially, they are the same group but represented in different ways. Next we will see another instance of this.

To start, note that $\mathbb{C}$ *is not* a group under multiplication. However, we can *fix* $\mathbb{C}$ so that it is a group under multiplication.

Example (The group $\mathbb{C}^*$)**.**

We can define $\mathbb{Q}^*$ and $\mathbb{R}^*$ similarly, and these are both groups under multiplication.

The group $\mathbb{C}^*$ has lots of subgroups. One you might be familiar with is $H = \{1, -1, i, -i\}$ (also known as the *group of fourth roots of unity*). We should compare this group to R_4 by constructing their Cayley tables and writing down a map between them:

We will explore roots of unity more, along with their connection the groups $\mathbb{Z}_n$. Given a complex number $z = a + bi$, the *complex conjugate* of z is $\overline{z} = a - bi$. The *modulus* of z is $|z| = \sqrt{a^2 + b^2}$. The complex number z can be represented on the Cartesian plane in polar form (r, θ) where:

Conversely, given polar coordinates (r, θ), there is a corresponding complex number $a + bi$ where

$$a = r\cos\theta \quad \text{and} \quad b = r\sin\theta.$$

Note that we require $0 \leq \theta < 2\pi$ to ensure that this representation is well-defined. Then

$$z = r(\cos\theta + i\sin\theta).$$

(Your book uses the abbreviation $\text{cis}\theta$ for $\cos\theta + i\sin\theta$ but I will avoid this.)

Theorem 3: DeMoivre's Theorem

Let $z = r(\cos\theta + i\sin\theta)$. Then for any positive integer n,

$$z^n = r^n\left(\cos(n\theta) + i\sin(n\theta)\right).$$

Definition: Roots of unity

Let n be a positive integer. The *nth roots of unity* are the complex numbers of the form

$$z = \cos(2k\pi/n) + i\sin(2k\pi/n)$$

for $k = 0, 1, \ldots, n-1$. An nth root of unity z is *primitive* if $z^m \neq 1$ for $m = 1, \ldots, n-1$.

Example. The complex number i is a fourth root of unity since $i^4 = 1$. Moreover, it is a *primitive* fourth root of unity since $i^1 = i, i^2 = -1$, and $i^3 = -i$. We see from this that i in fact *generates* all of the fourth roots of unity.

This idea of *generating* a group will be very important later when studying cyclic groups. Note that the group R_n is generated by a single rotation r (of degree $2\pi/n$). Similarly, $\mathbb{Z}_n$ is generated by [1] since added that element to itself enough times produces all the elements[7] in $\mathbb{Z}_n$.

Example (The group C_n)**.**

[7] This is not the actual definition of a generator. For example, this does not explain how 1 is a generator of $\mathbb{Z}$. The formal definition will come later.

5. Properties of groups

We now begin to study groups in more generality, including their basic properties. Throughout, we will generally treat G as an arbitrary group.

When the operation is understood we often will only write the set to denote the group. For example, the operation on $\mathbb{Z}$ is understood to be addition[8]. The most common operation symbols are $+$, $\cdot$, and $\circ$, however $+$ is almost universally reserved for groups with commutative operations (abelian groups).

When the operation is multiplication (or composition), the identity is typically denoted by 1 or e, and the inverse of an element $a \in G$ is denoted a^{-1}. When the operation is addition, the identity is typically denoted by 0, and the inverse of $a \in G$ is denoted $-a$. Because we want to treat G as an arbitrary group, we will use multiplicative notation so that there is no assumption on commutativity.

Proposition 4: Properties of groups

Let G be a group.

(1) The identity element of G is unique.

(2) For all $g \in G$, the inverse element $g^{-1} \in G$ is unique.

(3) For $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

(4) Left and right cancellation hold. That is, for all $a, b, c \in G$,

$$ba = ca \Rightarrow b = c \quad \text{and} \quad ab = ac \Rightarrow b = c.$$

[8]Recall that $\mathbb{Z}$ is *not* a group under multiplication because elements are not invertible in general.

Property (4) above, the cancellation property, implies that we cannot have repetitions in a row or column of the Cayley table[9]. To see this, just note that if $ab = ac$ in the "a row", then (left) cancellation implies that $b = c$.

The following exercise is inspired by (3) above.

Exercise. Let G be a group and $g \in G$. If $g' \in G$ satisfies $gg' = e$ or $g'g = e$, then $g' = g^{-1}$. (A left/right inverse element in a group is a two-sided inverse).

Exercise. Let G be a group and $a, b \in G$. Show that the equations $ax = b$ and $xa = b$ have unique solutions in G.

In multiplicative notation we use exponentials for short hand. Let $g \in G$ with G a group, then

$$g^0 = e, \quad g^1 = g, \quad g^n = g \cdot g \cdots g \ (n \text{ times}), \quad g^{-n} = g^{-1} \cdot g^{-1} \cdots g^{-1} \ (n \text{ times}).$$

For additive notation we use coefficients. Let $a \in A$ with A an abelian group, then

$$0a = 0, \quad 1a = a, \quad na = a + a + \cdots + a \ (n \text{ times}), \quad (-n)a = (-a) + (-a) + \cdots + (-a) \ (n \text{ times}).$$

Theorem 5: Exponential rules for groups

Let G be a group, $g, h \in G$, and $m, n \in \mathbb{Z}$. Then the following hold:

(Multiplicative notation)	(Additive notation)
(1) $g^m g^n = g^{m+n}$;	(1) $mg + ng = (m+n)g$;
(2) $(g^m)^n = g^{mn}$;	(2) $m(ng) = (mn)g$;
(3) $(gh)^n = (h^{-1}g^{-1})^{-n}$.	(3) $m(g+h) = mg + mh$.

[9] Courtesy of my Fall 2017 abstract algebra class, this is known as the *Sudoku rule*.

Definition: Order of a group, finite order, infinite order

The *order of a group* $(G, \cdot)$ is the number of elements in G, denoted $|G|$. If $|G| < \infty$, then G is said to be *finite*. Otherwise, G is *infinite*.

Example. The group $\mathbb{Z}_n$ has order n. (For the groups $\mathbb{Z}_n$, the operation is understood to be addition mod n.) On the other hand, the group $M_2(\mathbb{R})$ has infinite order. (Here the operation is understood to be matrix addition.)

Exercise. Determine all possible Cayley Tables for a group of order 4. Use this to show that every group of order 4 is abelian.

Example (The group $U(n)$)**.**

We conclude with a return to subgroups. In addition to giving a few more examples, we want to illustrate a mechanism to check more easily whether a given subset of a group is a subgroup.

Since we will use the group $\mathbb{Z}_n$ so frequently, this is a good time to declare that we will drop the equivalence class notation $[x]$ and simply denote this element by x. The understanding is that we are always working with equivalence classes and will denote elements by the preferred representatives $0, 1, \ldots, n-1$.

Example. Determine the subgroups of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

Example. Consider $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$ with addition (mod 2) in each component,

$$(a, b) + (c, d) = (a + b \mod 2, c + d \mod 2).$$

We work out the Cayley Table for this group below.

Note the similarity between this table and that of $U(8)$. They are the "same" group in a sense that we will make more explicit later.

The subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are

In general, to check that a subgroup is a group we need to verify first that it is a subset and then check that it is a group. The next proposition simplifies that process.

Proposition 6: The Subgroup Test

Let H be a nonempty subset of G. Then H is a subgroup of G if and only if whenever $a, b \in H$, $ab^{-1} \in H$.

Example (The special linear group $\mathrm{SL}_2(\mathbb{R})$)**.**

Cyclic and Symmetric Groups

1. Cyclic groups

Recall that R_n is the subgroup of rotations in D_n. The element $r \in D_n$ *generates* R_n in the sense that every element of R_n is a power of r. Similarly, every element in C_n (the group of primitive nth roots of unity) is generated by $e^{2pi/n}$. As another example, the group $\mathbb{Z}_n$ can be generated by 1 in the sense that every element of $\mathbb{Z}_n$ is a multiple of 1 (the difference here is that $\mathbb{Z}_n$ is *additive* while R_n and C_n are *multiplicative*). These are all examples of *cyclic groups*, which we study in this chapter. This also gives further insight into the *order* of elements in finite groups.

To start, we define some notation. If G is a group and $a \in G$, then we set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\} \quad \text{(multiplicative notation)}$$

$$\langle a \rangle = \{ka : k \in \mathbb{Z}\} \quad \text{(additive notation)}.$$

That is, these are the sets of powers (resp. multiples) of a given elements, including powers (resp. multiples) of the inverse. These sets (which turn out to be subgroups) are crucial to understanding the structure of a group.

Theorem 1: The group generated by an element

Let G be a group and $a \in G$. Then $\langle a \rangle$ is the smallest subgroup of G containing a.

Definition: Cyclic subgroup, cyclic group, generator

Let G be a group. For $a \in G$, $\langle a \rangle$ is the *cyclic subgroup* of G generated by a. If there exists $a \in G$ such that $\langle a \rangle = G$, then G is a *cyclic group* and a a *generator* of G.

Example. The following are examples of cyclic groups.

Definition: Order of an element

The *order* of an element a in a group G is the smallest positive integer, if it exists, such that $a^n = e$. When no such n exists then the order is infinite

In additive notation, the condition $a^n = e$ is replaced by $na = 0$.

We write $|a| = n$ to denote the order of the element a (or $|a| = \infty$ if the order is infinite).

Example. Find the order of every element of D_3.

Proposition 2: Alternate definition of order of an element

Let G be a group and $a \in G$. Then $|a| = |\langle a \rangle|$.

Proposition 3: Order of the inverse

Let G be a group and $a \in G$. Then $|a| = |a^{-1}|$.

An easy exercise is to prove that every cyclic group is abelian. The next result is much stronger.

Theorem 4: Every subgroup of a cyclic group is cyclic

If H is a subgroup of a cyclic group G. Then H is cyclic.

Recall that $\mathbb{Z}$ is a cyclic group (with generators 1 and -1). By the previous theorem, every subgroup of $\mathbb{Z}$ is cyclic and so has a generator n. This is the set $\langle n \rangle = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$. This fully classifies all subgroups of $\mathbb{Z}$.

As mentioned in the introduction, the study of cyclic groups extends beyond cyclic groups themselves. It also gives a way to understand the order of elements in groups. For example, a powerful theorem, which we will prove later, states that the order of an element in a finite group divides the order of the group. These next results will be important pieces of that theorem.

Theorem 5: Order of an element in a cyclic group

Let $G = \langle a \rangle$ be a cyclic group of order n.

(1) Then $a^k = e$ if and only if $n \mid k$.

(2) If $b = a^k$, then $|b| = n/d$ where $d = \gcd(k, n)$.

Recall that $\mathbb{Z}_n$ is cyclic (of order n). Of course 1 is a generator of $\mathbb{Z}_n$, but so is any element of order n. To see this, note that if a has order n then so does $\langle a \rangle \subset \mathbb{Z}_n$. By the Pigeonhole Principle, this implies that $\langle a \rangle = \mathbb{Z}_n$. Hence, by the theorem, the generators of $\mathbb{Z}_n$ are those integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

2. Permutation groups

Recall our example of D_3, the symmetries of a triangle with vertices A, B, C. Any symmetry may be regarded as a rearrangement of the vertices and so every symmetry is a bijective function from the set $\{A, B, C\}$ to itself. In this way we may regard D_3 as a *permutation group*. In fact, every dihedral group (group of symmetries) is a permutation group on some set. However, while D_3 captures *every* rearrangement of the vertices, D_4 does not.

Definition: Permutation

A *permutation* is a bijective function on the set X (from X to itself). The set of permutations on X is denoted $\mathcal{S}_X$.

Theorem 6: Group of permutations on a set

For any nonempty set X, $\mathcal{S}_X$ is a group under composition.

Definition: Symmetric group, permutation group

Let X be a set. The *symmetric group* on X is the set $\mathcal{S}_X$ under the operation of (function) composition. When $X = \{1, \ldots, n\}$, then $\mathcal{S}_X$ is denoted by $\mathcal{S}_n$ and is called the *symmetric group on n letters*. A subgroup of $\mathcal{S}_n$ is a *permutation group*.

The set X need not be finite, but we will focus almost exclusively on the case of $\mathcal{S}_n$. It should be relatively straightforward for you to convince yourself that the order of $\mathcal{S}_n$ is $n!$.

There are two standard types of notation to represent elements of $\mathcal{S}_n$: two-line and cycle. In two-line notation we write the elements of $\mathcal{S}_n$ as $2 \times n$ matrices. For a given element $\sigma \in \mathcal{S}_n$ we write in the first row $1, \ldots, n$ and in the second the image of each value under σ:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Warning. The elements of S_n are functions and therefore we compose right-to-left.

Example. In general, the elements of $\mathcal{S}_n$ do not commute. Consider the following elements of S_3:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Compute $\sigma\tau$ and $\tau\sigma$ using two-line notation.

Example. Consider the following elements of $\mathcal{S}_4$:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

These elements form a subgroup of $\mathcal{S}_4$ with Cayley table:

A more compact way of representing elements of $\mathcal{S}_n$ is with *cycles*.

Definition: Cycle, cycle length

A permutation $\sigma \in \mathcal{S}_n$ is a *cycle of length* k if there exists $a_1, \ldots, a_k \in \{1, \ldots, n\}$ such that

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

and $\sigma(i) = i$ for $i \notin \{a_1, \ldots, a_k\}$. We denote the cycle by $(a_1\ a_2\ \cdots\ a_k)$.

To compose cycles, we compose (from right-to-left) by tracking the image of each element through successive cycles, remembering to close cycles when we get back to where we started.

Example. In the previous example, the elements would be written in cycle notation by

$$\mathrm{id} = (1), \quad \sigma = (1\ 4\ 3\ 2), \quad \tau = (1\ 3)(2\ 4), \quad \mu = (1\ 2\ 3\ 4).$$

Example. In cyclic notation, the symmetric group on three letters is

$$\mathcal{S}_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}.$$

The Cayley Table is

Definition: Disjoint cycles

Two cycles $\sigma = (a_1\ a_2\ \cdots\ a_k)$ and $\tau = (b_1\ b_2\ \cdots\ b_\ell)$ are *disjoint* if $a_i \neq b_j$ for all i, j.

Example. (1 3 5)(2 7) are disjoint but (1 3 5)(3 4 7) are not. Note that (1 3 5)(3 4 7) = (1 3 4 7 5).

Example. Write $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$ as a product of disjoint cycles.

Proposition 7: Disjoint cycles in $\mathcal{S}_n$ commute

If σ and τ are disjoint cycles in $\mathcal{S}_n$, then $\sigma\tau = \tau\sigma$.

Theorem 8: Cycle decomposition

Let $\sigma \in \mathcal{S}_n$. Then σ is a product of disjoint cycles in $\mathcal{S}_n$.

3. The Alternating Group

In this section we will define an important subgroup of the symmetric group.

Definition: Transposition

A *transposition* is a cycle of length 2.

Example (Decomposing a cycle as a product of transpositions)**.** Any cycle can be written as the product of transpositions. There are many ways to do this. Here is one. Note that the transpositions are not disjoint in this decomposition.

Of course, the above example extends to a permutation by decomposing each cycle. The next theorem is stated here, but will actually be proved later at the end of this section.

Theorem 9: Invariance of parity in cycles

Any decomposition of a cycle contains either an even number or odd number of transpositions.

Assuming the proposition for the time being allows us to define the next terms.

Definition: Even/odd permutation

A permutation is *even* (resp. *odd*) if it can expressed as the product of an even (resp. odd) number of transpositions.

Theorem 10: Subgroup of even permuations

The set of all even permutations in $\mathcal{S}_n$ is a subgroup of $\mathcal{S}_n$.

Definition: Alternating group

The *alternating group on n letters* is the subgroup A_n of $\mathcal{S}_n$ consisting of all even permutations.

Proposition 11: Order of A_n

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

We now return to the proof of Theorem 9, which says that the notion of the *sign* of a permutation is well-defined. The individual pieces of the proof are not difficult, but there are many pieces. We prove this as a series of small lemmas which combine to form the big theorem[1].

Lemma 12: Identities in $\mathcal{S}_n$

Let a, b, c, d be distinct elements of $\{1, \ldots, n\}$. In $\mathcal{S}_n$ we have the following identities:

$$(c\ d)(a\ b) = (a\ b)(c\ d) \quad \text{and} \quad (b\ c)(a\ b) = (a\ c)(b\ c).$$

[1] Like Voltron!

Lemma 13: Decomposing the identity

If the identity $(1) \in \mathcal{S}_n$ is written as a product of transpositions $(1) = \tau_1\tau_2 \dots \tau_k$, then k is even.

Proof of Theorem 9.

Group Homomorphism

We began this course by studying a fundamental object in algebra (groups) and the corresponding sub-objects (subgroups). Now we study maps between those objects and this leads naturally to a discussion on quotient objects. This framework appears frequently in mathematics. For example, in 331 you learned about sets, subsets, and functions (between sets). In Topology, for instance, one studies topological spaces, their subspaces, and continuous functions between topological spaces.

1. Homomorphisms

One should think of a homomorphism as a *structure preserving map*, that is, a map between groups that respects the operation in each group.

Definition: Homomorphism

A *homomorphism* is a function $\phi : (G, \cdot) \to (H, \circ)$ between groups such that

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

Example. The following are examples of homomorphisms.

These properties of homomorphisms we can prove immediately. Others we will prove later.

Proposition 1: The identity and inverses are preserved

Let $\phi : G \to H$ be a homomorphism of groups.

(1) The identity of G is mapped to the identity of H under ϕ. That is, $\phi(e_G) = e_H$.

(2) For any $g \in G$, $\phi(g^{-1}) = \phi(g)^{-1}$.

There are two important subgroups relative to every homomorphism: the *image* and the *kernel*. These appear in linear algebra in the context of the column and null space of a matrix.

Definition: Image and kernel (of a homomorphism)

Let $\phi : G \to H$ be a group homomorphism. The *image* of ϕ is the set $\operatorname{Im}\phi = \{\phi(g) : g \in G\}$. The *kernel* of $\phi : G \to H$ is the set $\operatorname{Ker}\phi = \{g \in G : \phi(g) = e\}$.

Example. We compute the image and kernel in some of our examples above.

Recall that, generically, we use the notation ϕ^{-1} to refer to the *preimage* of a set. In general, the inverse of a homomorphism is not itself a homomorphism (because it may not be a function).

Proposition 2: Subgroups are mapped to subgroups (and back again)

Let $\phi : G \to H$ be a homomorphism of groups.

(1) If K is a subgroup of G, then $\phi(K) = \{\phi(k) : k \in K\}$ is a subgroup of H.

(2) If L is a subgroup of H, then $\phi^{-1}(L) = \{g \in G : \phi(g) \in L\}$ is a subgroup of G.

As we observed earlier, the kernel turns out to be a subgroup of the domain. In fact it is a *normal* subgroup, a fact we will return to later (once we have defined the term normal).

Theorem 3: Kernels are subgroups

Let $\phi : G \to H$ be a group homomorphism. Then $\text{Ker}\phi$ is a subgroup of G.

Kernels are important in detecting *injectivity* of a group homomorphism.

Lemma 4: Injective is equivalent to trivial kernel

Let $\phi : G \to H$ be a group homomorphism. Then ϕ is injective if and only if $\text{Ker}\phi = \{e_G\}$.

2. Isomorphisms

We have already seen this in practice. The groups $\mathbb{Z}_n$ (integers mod n), R_n (rotations in D_n), and C_n (nth roots of unity) all appear to be the same group in that their Cayley tables are the same up to changing notation. Isomorphisms formalize this intuition.

Definition: Isomorphic, isomorphism

Two groups $(G, \cdot)$ and $(H, \circ)$ are said to be *isomorphic* if there exists a bijective homomorphism $\phi : G \to H$. The map ϕ in this case is called an *isomorphism*.

Example. The following are examples of isomorphisms.

The following proposition is immediate from Lemma 4.

Proposition 5: Surjective + trivial kernel implies isomorphism

A group homomorphism $\phi : G \to H$ is an isomorphism if and only if it is surjective and $\text{Ker}\phi = \{e_G\}$.

Most of the properties in the next statement are easy.

Theorem 6: Properties of isomorphisms

Let $\phi : G \to H$ be an isomorphism of groups.

(1) $\phi^{-1} : H \to G$ is an isomorphism.
(2) $|G| = |H|$.
(3) If G abelian, then H is abelian.
(4) If G is cyclic, then H is cyclic.
(5) If G has a subgroup of order n, then H has a subgroup of order n.

3. Cosets

Cosets are arguably one of the strangest structures that students encounter in abstract algebra, along with factor groups, which are strongly related. Here's a motivating question for this section: if H is a subgroup of a group G, then how are $|H|$ and $|G|$ related? A partial answer to this is contained in Lagrange's Theorem.

Definition: Left and right cosets

Let H be a subgroup of a group G. A *left coset* of H with representative in $g \in G$ is the set

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

A *right coset* of H with representative in $g \in G$ is the set

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

Warning. Cosets are **NOT** subgroups in general!

Example. We compute the left and right cosets of $K = \{(1), (1\ 2)\}$ in $\mathcal{S}_3$.

Example. We compute the left and right cosets of $L = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ in $\mathcal{S}_3$.

In additive notation, we write

$$g + H = \{g + h : h \in H\}.$$

Additive groups are abelian by definition, so $g + H = H + g$, that is, the left and right cosets are equal. Hence, in this setting we will speak only of the *cosets* with no ambiguity.

Example. We compute the cosets of $H = \langle 3 \rangle = \{0, 3\}$ in $\mathbb{Z}_6$.

Lemma 7: Properties of cosets

Let H be a subgroup of G and suppose $g_1, g_2 \in G$. The following are equivalent.

(1) $g_1 H \subset g_2 H$

(2) $g_1 H = g_2 H$

(3) $H g_1^{-1} = H g_2^{-1}$

(4) $g_2 \in g_1 H$

(5) $g_1^{-1} g_2 \in H$.

4. Lagrange's Theorem

Lagrange's Theorem is an important step in understanding the structure of (finite) groups. Stated simply, it says that the order of a subgroup of a finite group divides the order of the group. The converse of Lagrange's Theorem is false in general. If $n \mid |G|$, this *does not* imply that there exists a subgroup H of G with $|H| = n$. For example, A_4 has no subgroup of order 6.

To prove Lagrange's Theorem, we first need to understand better how cosets function as equivalence classes. Here is a brief reminder of a result from the preliminary notes.

Definition: Partition

A *partition* P of a set X is a collection of nonempty sets $X_1, X_2, \ldots$ such that $X_i \cap X_j = \emptyset$ for all $i \neq j$ and $\bigcup_k X_k = X$.

Equivalence classes partition a set

Let $\sim$ be an equivalence relation on a set X. Then any two equivalence classes are either equal or disjoint. Hence, the (distinct) equivalence classes of X form a partition of X.

Theorem 8: Cosets partition a group

Let H be a subgroup of a group G. The left (or right) cosets of H in G partition G.

Definition: Index

The *index* of a subgroup H in a group G, denoted $[G : H]$, is the number of left cosets in G.

Example. In the previous examples, we have $[\mathbb{Z}_6 : H] = 3$, $[\mathcal{S}_3 : K] = 3$, and $[\mathcal{S}_3 : L] = 2$.

Theorem 9: Number of left cosets equals number of right cosets

The number of left cosets of a subgroup H in a group G equals the number of right cosets.

Lemma 10: All cosets have the same order

Let H be a subgroup of G. For all $g \in G$, $|H| = |gH|$.

The proof of Lagrange's Theorem is now simple because we've done the legwork already.

Theorem 11: Lagrange's Theorem

Let G be a finite group and H a subgroup of G. Then $|G|/|H| = [G : H]$.

One immediate consequence of Lagrange's Theorem is that the order of a subgroup divides the order of a group (when the group has finite order). This holds for order of elements as well.

Corollary 12: Order of an element divides the order of the group

Suppose G is a finite group and $g \in G$. Then the order of g divides $|G|$.

Now suppose that G is a group of prime order p. If $g \in G$ is not the identity, then $|g| > 1$ and $|g|$ divides p, so $|g| = p$. That is, g is a generator for G. Hence, *all groups of prime order are cyclic*. It follows that $G \cong \mathbb{Z}_p$ (though we have no quite proved this yet).

The last result of this section shows that index plays nicely with *towers* of subgroups.

Corollary 13: Index is multiplicative

Let H, K be subgroups of a finite group G such that $K \subset H \subset G$. Then

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

5. Normal subgroups and factor groups

Normal subgroups lead to factor groups, which reveal "hidden" structure in groups not revealed. Factor groups are a group structure on the set of cosets of a group by certain subgroups. This is also setup for several fundamental results called "isomorphism theorems". We will only prove one of these here, but this will prove immensely useful.

Definition: Normal subgroup

A subgroup N of a group G is *normal* if $gN = Ng$ for all $g \in G$.

Example. The following are examples of normal subgroups.

Theorem 14: Equivalent definitions of normality

Let G be a group and N a subgroup. The following are equivalent.

(1) The subgroup N is normal.
(2) For all $g \in G$, $gNg^{-1} \subset N$.
(3) For all $g \in G$, $gNg^{-1} = N$.

Let N be a normal subgroup of a group G. We denote by G/N the set of cosets. In this setup (because N is normal), there is no need to differentiate between left and right cosets. However, we will typically work with left cosets.

Lemma 15: Binary operation on G/N

Let N be a normal subgroup of a group G. There is a binary operation on G/N given by

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

for all $aN, bN \in G/N$.

Theorem 16: Group structure on G/N

Let N be a normal subgroup of G. The cosets of N in G form a group G/N (with the operation above) of order $[G : N]$.

Definition: Factor group

Let G be a group and N a normal subgroup. The set G/N along with the operation $(aN)(bN) = (ab)N$ is the *factor group* of G by N.

Example. We have already shown that R_n is a normal subgroup of D_n. The group D_n/R_n has the following Cayley table.

Example. We have already shown that A_n is a normal subgroup of $\mathcal{S}_n$. The group $\mathcal{S}_n/A_n$ has the following Cayley table:

For an abelian group, where cosets are denoted $a + N$, we denote the above binary operation by

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

Example. The group $\mathbb{Z}$ is abelian so the subgroup $3\mathbb{Z}$ is normal. The group $\mathbb{Z}/3\mathbb{Z}$ has the following Cayley table:

The isomorphism theorems give a more direct way of viewing the isomorphisms we just considered. There are three of them, but we will only consider the first one right now.

Our next result actually generalizes an earlier result that a homomorphism is an isomorphism if and only if its kernel is trivial. The first isomorphism theorem says that the factor group of a group by the kernel of an homomorphism is isomorphic to the image of the homomorphism. It is a powerful tool in proving that two groups are isomorphic.

Theorem 17: First Isomorphism Theorem

Let $\phi : G \to H$ be a homomorphism and $K = \text{Ker}\phi$. There exists an isomorphism

$$\psi : G/K \to \phi(G) \qquad gK \mapsto \phi(g).$$

That is, $G/K \cong \phi(G)$.

The first isomorphism tells us that in fact we should never

Example. We claim $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example. We will show that $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R}) \cong \mathbb{R}^\times$.

Finite Abelian Groups

This set of notes is dedicated to an important classification theorem in group theory. The focus will be on the statement of the theorem. The proof, however, does illustrate some of the power in using factor groups.

1. Direct products

We have seen some examples of direct products previously. For example, the *Klein-4* group $\mathbb{Z}_2 \times \mathbb{Z}_2$ where the operation is addition mod 2 in each coordinate. We will show formally two different ways to combine groups to form a new group.

Recall that for any two sets A and B, the cartesian product of two sets A and B is the set $A \times B = \{(a, b) : a \in A, b \in B\}$. Recall that the order of this set is $|A \times B| = |A| \cdot |B|$.

Proposition 1: External direct product of groups

Let $(G, \cdot)$ and $(H, \circ)$ be groups. Then $G \times H$ is a group under the operation

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2) \quad \text{for all } (g_1, h_1), (g_2, h_2) \in G \times H.$$

Definition: External direct product

The *external direct prduct* of groups $(G, \cdot)$ and $(H, \circ)$ is the set $G \times H$ with operation

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2) \quad \text{for all } (g_1, h_1), (g_2, h_2) \in G \times H.$$

The proof of the next result is left as a homework exercise.

Lemma 2: Order of elements in a direct product

Let G and H be groups and $(a, b) \in G \times H$. Then $|(a, b)| = \text{lcm}(|a|, |b|)$.

Recall that if $|G| = p$, p prime, then $G \cong \mathbb{Z}_p$. Here is a related result.

Proposition 3: Direct product of cyclic groups

Let m, n be positive integers, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

Example (Decomposing $\mathbb{Z}_6$)**.**

For a group G with subgroups H, N, let $HN = \{hn : h \in H, n \in N\}$. In general this is *not* a subgroup of G.

Lemma 4: H, N commute implies HN is a subgroup

Let G be a group with subgroups H, N. If $hn = nh$ for all $h \in H$, $n \in N$, then HN is a subgroup of G.

In additive notation, HN is $H + N = \{h + n : h \in H, n \in N\}$. It is clear from the lemma that $H + N$ is always a subgroup of G.

Definition: Internal direct product

A group G is the *interal direct product* of subgroups H and K provided

(1) $G = HK$ (as sets),

(2) $H \cap K = \{e\}$, and

(3) $hk = kh$ for all $h \in H$, $k \in K$.

Example (Decomposing $U(8)$)**.**

Example ($\mathcal{S}_3$ is not an IDP)**.**

The next theorem says that if G is the internal direct product of subgroups H and K, then it is also the external direct product of those subgroups.

Theorem 5: Internal direct product is an external direct product

If G is the internal direct product of subgroups H and K, then $G \cong H \times K$.

Example (The group $U(8)$ again)**.**

A nice corollary of the previous theorem, which we do not state formally, provides an alternative way to check property (1) in the definition of an IDP for finite groups. Suppose $|G| = n < \infty$ with subgroups H and K. Then

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

Hence, if $|H \times K| = n$ and $|H \cap K| = 1$ (this is equivalent to condition (2) in the definition), then we conclude that $|HK| = n$. By pigeonhole, $HK = G$.

All of our work thus far generalizes to more than two subgroups. The proof of the proposition below is left as an exercise.

Definition: Internal direct product (general)

A group G is the *internal direct product* of subgroups $H_1, H_2, \ldots, H_n$ provided

(1) $G = H_1H_2\cdots H_n = \{h_1h_2\cdots h_n : h_i \in H_i\}$ (as sets),

(2) $H_i \cap \langle \bigcup_{j\neq i} H_j \rangle = \{e\}$, and

(3) $h_ih_j = h_jh_i$ for all $h_i \in H_i$, $h_j \in H_j$, $i \neq j$.

Proposition 6: Internal direct product is an external direct product (general)

If a group G is the internal direct product of subgroups $H_1, H_2, \ldots, H_n$, then

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

We are now ready to state our main theorem of this set. Ultimately, this is a generalization of the fact that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$. For the proof of this theorem, we will need more technology.

Theorem 7: The Fundamental Theorem of Finite Abelian Groups

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

The Fundamental Theorem implies that every finite abelian group can be written (up to isomorphism) in the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$

with p_i prime (not necessarily distinct) and $\alpha_i \in \mathbb{N}$.

Example. Every finite abelian group of order $540 = 2^2 \cdot 3^3 \cdot 5$ is isomorphic to exactly one of the following:

2. Proof of the Fundamental Theorem (Part I)

The first part of the proof involves breaking down abelian groups into direct products of subgroups where the orders of the subgroups are relatively prime. This is a generalization of the idea used above to show that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ when $\gcd(m, n) = 1$.

Lemma 8: Decomposing abelian groups

Let G be an abelian group with $|G| = mn$ and $\gcd(m, n) = 1$. Let H be the set of elements in G whose elements have an order dividing m and define K similarly for n. Then $G \cong H \times K$.

Now suppose $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ with the p_i distinct primes. Set $G_i = \{g \in G : |g| = p_i^k, k \in \mathbb{Z}\}$. The proof above shows that each G_i is a subgroup (because the only factors of a prime power are other powers of that prime). Now as a consequence of the theorem (by induction) we have

$$G \cong G_1 \times G_2 \times \cdot \times G_n.$$

It suffices to prove the fundamental theorem for the G_i.

Definition: p-group

Let p be a prime. A group G is a *p-group* if every element in G has order a power of p.

Example. The following are examples of p-groups:

By Lagrange's Theorem, every group of order p^n, p a prime, is automatically a p-group since the order of every element must divide p^n. We will prove a converse to this for finite abelian groups.

Lemma 9: Elements of prime order

Let G be a finite abelian group of order n. If p is a prime dividing n, then G contains an element of order p

An immediate consequence of the previous lemma is that a finite p-group must have order a power of p. This follows from that fact that of G is a finite p-group and q is another prime dividing the order of G, then G has an element of order q. But this contradicts the definition of a p-group.

3. Proof of the Fundamental Theorem (Part II)

In this section, we prove the Fundamental Theorem for finite p-groups. This will conclude the proof since we have already shown that we can decompose any finite abelian group into a product of p-groups. We begin with a technical result that will help in the proof of the first proposition.

Lemma 10

Let G be a finite abelian p-group that is not cyclic. Suppose that $g \in G$ has maximal order. If $h \in G \backslash \langle g \rangle$ has smallest possible order, then $|h| = p$.

Lemma 11

Let G be a finite group, N a normal subgroup of G, and $g \in G$ an element of maximal order in G. If $\langle g \rangle \cap N = \{e\}$, then $|gN| = |g|$ and so gN is an element of maximal order in G/N.

Proposition 12: Decomposing a finite abelian p-group

Let G be a finite abelian p-group and suppose that $g \in G$ has maximal order. Then G is the internal direct product of $\langle g \rangle$ and some subgroup K. Hence, $G \cong \langle g \rangle \times K$.

By Lagrange's Theorem, the subgroup K appearing in the proposition must also be a finite abelian p-group whose order is less than that of G. That is, unless $K = \{e\}$. But in that case G is cyclic and so we conclude that $G \cong \mathbb{Z}_{p^k}$ for some k. Thus, either we are done or we proceed by induction. This concludes the proof of the fundamental theorem of finite abelian groups.

Introduction to Rings

Calling $\mathbb{Z}$ a group (under addition) obscures the fact that there are actually two well-defined (binary) operations on $\mathbb{Z}$: addition and multiplication. Moreover, these two operations play nicely together (via the distributive law). Hence, $\mathbb{Z}$ is a *ring*. We will study rings and a few families of interesting examples, drawing many parallels with our knowledge of groups.

1. Rings

Definition: Ring

A *ring* is a set R along with two binary operations (typically $+$ and $\cdot$) satisfying:

(1) $(R, +)$ is an additive abelian group;

(2) $\cdot$ is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$;

(3) the left and right distributive properties hold: for all $a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Remark. Because $(R, +)$ is assumed to be an (additive) abelian group, we denote the additive inverse of an element $a \in R$ by $-a$. If an element $a \in R$ has a multiplicative inverse we denote it by a^{-1}. Note that R need not be closed under multiplicative inverses.

Example. The following are rings:

We'll now discuss a variety of properties that a ring may or may not possess.

Definition: Ring with unity, commutative ring, left/right zero divisor, domain, integral domain, unit, division ring, field

Let R be a ring.

(1) If there exists an element $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for all $a \in R$, then R is said to be a *ring with unity* (sometimes a *ring with identity*).

(2) If $ab = ba$ for all $a, b \in R$, then R is said to be *commutative*.

(3) A nonzero element $a \in R$ is said to be a *left zero divisor* if there exists a nonzero $b \in R$ such that $ab = 0$ and a *right zero divisor* if there exists a nonzero $b \in R$ such that $ba = 0$. A ring without zero divisors is a *domain*. A commutative domain with unity is an *integral domain*.

(4) An element $u \in R$ is a *unit* if $u^{-1} \in R$. A ring with unity in which every nonzero element is a unit is a *division ring*. A commutative division ring is a *field*.

If R is a division ring, then $(R\backslash\{0\}, \cdot)$ is a group. If R is a field, then $(R\backslash\{0\}, \cdot)$ is an *abelian* group.

Example. We consider these properties for the examples discussed above.

Proposition 1: Basic properties of rings

Let R be a ring with $a, b \in R$. Then

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

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

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

Proposition 2: Basic properties of rings with unity

Let R be a ring with multiplicative identity 1.

(1) The multiplicative identity is unique.

(2) If $a \in R$ is a unit, then a is not a zero divisor.

(3) If $a \in R$ is a unit, then its multiplicative inverse is unique.

Definition: Subring

A subset S of a ring R is a *subring* if S is a ring under the inherited operations from R.

Example. $\mathbb{Z}_n$ is *not* a subring of $\mathbb{Z}$. However, $\mathbb{Z}$ is a subring of $\mathbb{R}$.

Proposition 3: Subring Test

Let R be a ring and S a nonempty subset of R. Then S is a subring of R if and only if for all $s_1, s_2 \in S$, $s_1 s_2 \in S$ and $s_1 - s_2 \in S$.

Example. Show that $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Ideals take the place of normal subgroups in ring theory in the sense that they are the right structure to allow us to define factor rings.

Definition: Ideal

An *ideal* in a ring R is a subring I of R such that if $x \in I$ and $r \in R$, then $xr \in I$ and $rx \in I$.

Example. The following are examples of ideals.

For a commutative ring, the conditions $xr \in I$ and $rx \in I$ are the same. For a noncommutative ring R, the story of ideals is a little different. A *left ideal* I is a subring satisfying $rx \in I$ for every $r \in R$, $x \in I$. A *right ideal* I is a subring satisfying $xr \in I$ for every $r \in R$, $x \in I$. A *two-sided ideal* (or just *ideal*) is both a left and right ideal.

The next proposition is a modified version of the Subring Test for Ideals. Note that we do not need to prove, separately, that I is closed under multiplication because we prove that it is closed under multiplication by *any* element of R.

Proposition 4: Ideal Test

Let R be a ring and I a nonempty subset of R. Then I is an ideal of R if and only if for all $a, b \in I$ and all $r \in R$, $a - b \in I$ and $ra, ar \in I$.

Proposition 5: Ideal generated by an element

Let R be a commutative ring and $a \in R$. The set $\langle a \rangle = \{ar : r \in R\}$ is an ideal in R.

Definition: Principal ideal, PID

The set $\langle a \rangle$ in the previous proposition is called the *principal ideal generated by* a. A integral domain R in which every ideal is principal is called a *principal ideal domain* (PID).

Theorem 6: $\mathbb{Z}$ is a PID

Let I be an ideal in $\mathbb{Z}$. Then I is principal.

3. Homomorphisms

We now extend notions of homomorphisms, cosets, and factor groups to rings.

Definition: Ring homomorphism, image, kernel, isomorphism

A map $\phi : R \to S$ of rings is a *(ring) homomorphism* if

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

An *isomorphism* (of rings) is a bijective homomorphism. The *kernel* and *image* of ϕ are defined, respectively, as the sets

$$\text{Ker}\phi = \{x \in R : \phi(x) = 0_s\}$$

$$\text{Im}\,\phi = \{\phi(a) : a \in R\}.$$

Example. Define a map $\psi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(a) = a \mod n$. Show this map is a homomorphism. Determine its image and kernel.

Example. Recall that $\mathcal{C}([a,b])$ is the ring of continuous functions $[a,b] \to \mathbb{R}$. Fix $\alpha \in [a,b]$, define the *evaluation map* $\phi_\alpha : \mathcal{C}([a,b]) \to \mathbb{R}$ by $\phi_\alpha(f) = f(\alpha)$. Show this map is a homomorphism.

Proposition 7: Properties of ring homomorphisms

Let $\phi : R \to S$ be a homomorphism of rings.

(1) If R is commutative, then $\phi(R)$ is commutative.

(2) $\phi(0_R) = 0_S$.

(3) Let R and S be rings with identity. If ϕ is surjective, then $\phi(1_R) = 1_S$.

(4) If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.

We can define "quotient objects" in rings as well. Here, again, ideals take the place of normal subgroups.

Theorem 8: Multiplication on cosets

Let I be an ideal of a ring R. The factor group R/I is a ring with multiplication defined by

$$(r+I)(s+I) = rs + I.$$

Definition: Factor ring

Let I be an ideal of a ring R. The set R/I with addition and multiplication operations defined by

$$(a+I)+(b+I) = (a+b)+I \quad \text{and} \quad (a+I)(b+I) = ab+I,$$

respectively, for all $a+I, b+I$, is called the *factor ring* of R by I.

Theorem 9: Ideals are kernels

Let I be an ideal of a ring R. The map $\phi : R \to R/I$ given by $r \mapsto r + I$ is a surjective ring homomorphism with kernel I.

The proof below is similar to the group case.

Theorem 10: First Isomorphism Theorem for Rings

Let $\phi : R \to S$ be a ring homomorphism. Then $R/\text{Ker}\phi \cong \phi(R)$.

Definition: Polynomial, coefficients, degree, leading coefficient, monic

A *polynomial over R in indeterminate x* is an expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where $a_i \in R$. The elements a_i are the *coefficients* of f. The *degree* of f is the largest m such that $0 \neq a_m$ if such an m exists. We write $\deg(f) = m$ and say a_m is the *leading coefficient*. Otherwise $f = 0$ and we set $\deg(f) = -\infty$. A nonzero polynomial with leading coefficient 1 is called *monic*.

We denote the set of polynomials over R by $R[x]$.

Let $p(x), q(x) \in R[x]$ be nonzero polynomials over R with degrees n and m, respectively. Write

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$
$$q(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

The polynomials $p(x)$ and $q(x)$ are equal ($p(x) = q(x)$) if and only if $n = m$ and $a_i = b_i$ for all i. We can define two binary operations, addition and multiplication, on $R[x]$.

(Addition)

(Multiplication)

Example. Suppose $p(x) = 3 + 2x^3$ and $q(x) = 2 - x^2 + 4x^4$ are polynomials in $\mathbb{Z}[x]$. Note that $\deg(p(x)) = 3$ and $\deg(q(x)) = 4$. Compute $p(x) + q(x)$ and $p(x)q(x)$.

Theorem 11: Polynomial ring over R

Let R be a ring. The set $R[x]$ is a ring under the operations of (polynomial) addition and (polynomial) multiplication.

Definition: Polynomial ring over R

Let R be a ring. The set $R[x]$ with the operations of (polynomial) addition and (polynomial) multiplication is called the *polynomial ring over* R.

If y is another indeterminate, then it makes sense to define $(R[x])[y]$. Note that $(R[x])[y] \cong (R[y])[x]$. Both of these rings will be identified with the ring $R[x, y]$ and call this the *ring of polynomials in two indeterminates x and y with coefficients in R*. Similarly (or inductively), one can then define the *ring of polynomials in n indeterminates with coefficients in R*, denoted $R[x_1, \ldots, x_n]$.

Proposition 12: Properties of polynomial rings

Let R be a ring.

(1) If R is commutative, then so is $R[x]$.

(2) If R has (multiplicative) identity, then so does $R[x]$.

(3) If R is an integral domain, then so is $R[x]$.

Remark. Let R be an integral domain. What we proved in part (3) of the proposition is

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)),$$

for *any* polynomials $p(x), q(x) \in R[x]$. This justifies why we set $\deg(0) = -\infty$.

5. Divisibility

Let S be a commutative ring with identity and R a subring of S containing 1. Let $\alpha \in S$. For $p(x) = a_0 + a_1x + \cdots + a_nx^n$, we set

$$p(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in S.$$

We can define a map $\phi_\alpha : R[x] \to S$ by $\phi_\alpha(p(x)) = p(\alpha)$. Then

Hence, ϕ_α is a homomorphism, called the *evaluation homomorphism* at α.

Definition: Root of a polynomial

We say $\alpha \in R$ is a *root* (or *zero*) of $p(x) \in R[x]$ if $\phi_\alpha(p(x)) = 0$.

Example.

Example.

We will now prove a version of the division algorithm for polynomials. This will be applied to determine when polynomials are irreducible over certain rings.

Theorem 13: Division algorithm for polynomials

Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

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

where $\deg r(x) < \deg g(x)$.

Now we consider some consequences of the Division Algorithm.

Definition: Factor

Let F be a field. We say $q(x)$ is a *factor* of $p(x)$ if $q(x)$ divides $p(x)$.

Corollary 14: Factors correspond to roots

Let F be a field. An element $\alpha \in F$ is a root of $p(x) \in F[x]$ if and only if $(x - \alpha)$ divides $p(x)$.

Corollary 15: Degree is less than or equal to number of roots

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

The next proof is very similar to the corresponding result for $\mathbb{Z}$.

Corollary 16: Polynomial ring over a field is a PID

Let F be a field and I an ideal in $F[x]$. Then I is principal.

Warning. The above result *does not* hold for $F[x, y]$. In particular, the ideal $\langle x, y \rangle$ is not principal.