Introduction to Groups

At its heart, Group Theory is the study of "symmetries" of objects. That is how we will approach the subject, though at times this will be obscured by abstractness. We will jump right into groups at the beginning of this course, however we will do it via examples:

- the integers
- the integers mod n (with addition or with multiplication)
- symmetries of objects
- symmetric groups

In some way all of these things will be familiar to you, even though I don't expect that any of you have seen the definition of a group yet.

One example of a group that you are already *very* familiar with is the integers with the operation of addition. I'm intentionally not defining a group here, but we'll make a few observations. The first is that the operation of addition on the integers is *associative*. Secondly, there is an identity element, 0, such that $0 + k = k$ for all $k \in \mathbb{Z}$. Finally, every number k has an *inverse* element, $-k$, such that $k + (-k) = 0$. These are the basic axioms of groups. You should try thinking of other examples on your own that are similar to this one.

Another example, and one more along the lines of symmetry, consists of rigid motions on the square. By this we mean transformations that do not change the appearance of the square but move the vertices around. There are eight such symmetries (4 counter-clockwise rotations and 4 reflections). One can compose these symmetries and that operation (composition) is associative. There is an identity element (the rotation by $0°$) and every symmetry has an inverse.

As a final example, consider bijective functions from the set $\{1, 2, 3\}$ to itself. Again, the operation here is composition and that operation is associative. There is an identity element (the identity function $e(x) = x$) and every function has an inverse (because it is bijective). We will consider many more examples but these are the prototypical ones.

Chapters 1 and 2 of Judson's book (sets, functions, and induction) will be covered minimally in the next few sections. However, you are encouraged to work through those chapters on your own and it is expected that you are familiar with this material from other courses that you have taken. In the next section we'll review some basics about integers and introduce another group that is fundamental to this course.

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapters 1-3. Last Updated: April 15, 2021

1. Sets, equivalence relations, and the integers mod n

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

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 $Y \neq X$.

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

- Union of A and B:
- Intersection of A and B:
- Complement of A in U:
- Difference:
- Cartesian Product:

Proposition 1: Set Laws

Let A, B, C be sets.

(1) $A \cup A = A$, $A \cap A = A$, $A \setminus A = \emptyset$.

(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. Exercise[1]. □

Theorem 2: DeMorgan's Laws

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

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

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

[1]When I leave proofs as exercises, it's not because I'm being lazy (OK, I'm being a *little* lazy). These are proofs that I think you're capable of doing on your own. I encourage you to work through these exercises and talk to me about them. That way you can on proof writing and check your understanding without the pressure of grades.

Definition: Relations on sets

Let X and Y be sets. A *relation* is a subset of the cartesian product $X \times Y$. An *equivalence relation* on a set X is a subset $R \subset X \times X$ such that

- $(x, x) \in R$ for all $x \in X$ (reflexive property)
- $(x, y) \in R$ implies $(y, x) \in R$ (symmetric property)
- $(x, y), (y, z) \in R$ implies $(x, z) \in R$ (transitive property)

The equivalence class of $x \in X$ is the set $[x] = \{y \in X : (x, y) \in R\}$.

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 an equivalence relation R on $\mathbb{Z}$ by the rule $(x, y) \in R$ if and only if $x - y$ is divisible by 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.

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.

Exercise. Given a partition $P = \{X_i\}$ of X, we can define a 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. Relations, functions, and the symmetric group

We'll now return to the concept of a *relation* and how it relates to functions.

Definition: Function, domain, codomain

Let A and B be sets. A *function* (or *map*) $f \subset A \times B$ is a relation such that if $(a, b), (a, c) \in f$ then $b = c$. The set A is called the *domain of* f and B the *codomain of* f. The range of f is the set $f(A) = \{f(a) : a \in A\} \subset B$.

We say a function $f : A \to B$ is *well-defined* if for every value $a \in A$ there is one and only one $b \in B$ such that $f(a) = b$. This is *not* the same as 1-1.

Example. Let n be a positive integer. Denote by $\mathbb{Z}_n$ the set of equivalence classes mod n. Define a relation $f : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by $f([a], [b]) = [a+b]$. We claim that f is a function (i.e., is well-defined).

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*.

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

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

Example. There are six permutations of the set $X = \{1, 2, 3\}$. List them all and make a table that shows the result of composing two of them (kind of like a multiplication table).

Theorem 4: Properties of composition

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

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

(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.

Definition: Identity map, invertible function

The *identity map on a set* A is the function id_A defined by $\mathrm{id}_A(a) = a$ for all $a \in A$. 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 the *inverse of* f, denoted f^{-1}.

The inverse of a function is unique. (Why?)

Theorem 5: Invertibility is equivalent to bijectivitiy

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

Example. Let $\mathcal{S}_X$ denote the set of all bijections on a set X. The identity function id_X is a bijection so $\mathrm{id}_X \in \mathcal{S}_X$. By Theorem 4, the operation of composition on $\mathcal{S}_X$ is associative. If $f \in \mathcal{S}_X$, then $f^{-1} \in \mathcal{S}_X$ by Theorem 5. Thus, $\mathcal{S}_X$ is a *group*, known as the *symmetric group* on X.

Definition: Binary operation

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

Example. The following are examples of binary operations.

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.

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 our first 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.

Theorem 6: 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 $0 \leq r < b$.

The proof of the next theorem is similar and left as a reading exercise.

Theorem 7: The Euclidean Algorithm

Let $a, b \in \mathbb{Z}$. There exist integers r, s such that $\gcd(a, b) = ar + bs$. Furthermore, the gcd of a and b is unique.

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

We will often use the notation $a \mid b$ in place of a divides b.

Lemma 8

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

Theorem 9: The Fundamental Theorem of Arithmetic

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

4. Groups

We're now ready to formally define groups and check some of the axioms more thoroughly.

Definition: Group, abelian group

A *group* is a pair $(G, \cdot)$ with G a set and $\cdot$ a binary operation on G satisfying

(1) Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.
(2) Identity: there exists $e \in G$ such that $a \cdot e = a = e \cdot a$ for all $a \in G$.
(3) Inverses: for all $a \in G$ there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$.

If in addition, $a \cdot b = b \cdot a$ for all $a, b \in G$ (commutativity) the group is said to be *abelian*.

When the operation is understood we often will only write the set to denote the group. The most common operation symbols are $+$, $\cdot$, and $\circ$. When the operation is addition, the inverse of $a \in G$ is typically denoted $-a$. For multiplication or composition, it is denoted a^{-1}.

Example. The following are examples of groups.

Note that $(\mathbb{Z}_4, \cdot)$ is *not* a group. In particular, 0 does not have an inverse.

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. The group $M_2(\mathbb{R})$ has infinite order.

A *Cayley Table* records all compositions in a group (like a multiplication table).

Example. The Cayley table for $(\mathbb{Z}_4, +)$.

Exercise. For any positive integer n, let $U(n)$ denote the set of invertible elements (units) in $\mathbb{Z}_n$. Check that multiplication mod n is indeed a binary operation on $U(n)$ and that $U(n)$ is a group under this operation.

Example. The Cayley table for the group $(U(8), \cdot)$.

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

Definition: Symmetry

A *symmetry* of an object is a rearrangement that preserves the arrangement of sides and vertices as well as distances.

Example. Denote the set of symmetries of an equilateral triangle by D_3. There are 6 such symmetries consisting of reflections and (counterclockwise) rotations. We denote these by

id: the trivial rotation	μ_1: reflection fixing the bottom left vertex
ρ_1: cc rotation of 120°	μ_2: reflection fixing the top vertex
ρ_2: cc rotation of 240°	μ_3: reflection fixing the bottom right vertex

Our binary operation is function composition, so we compose right to left. We compute the Cayley table for D_3 below.

Some people refer to this group as D_6 (because it has 6 elements) and in general the symmetries of a regular n-gon by D_{2n}. I'm not going to weigh in on the debate but I think it best that I keep my notation consistent with that of Judson.

5. Properties of groups

In this section we'll explore some of the basic properties of groups. Because we will generally treat G as an arbitrary group, we will use multiplicative notation.

Proposition 10: 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 $a, b, c \in G$,

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

Property (4) above, the cancellation property, implies that we cannot have repetitions in a row or column of the Cayley table. 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).

The next proposition is a direct corollary of Proposition 10.

Proposition 11

Let G be a group and $a, b \in G$. The equations $ax = b$ and $xa = b$ have unique solutions in G.

There are two generic operations in group theory: multiplication and addition. Almost universally, multiplicative notation is used for an arbitrary group while additive notation is used for an arbitrary *abelian* group. In multiplicative notation we use exponentials for short hand. Let $g \in G$ with G a group, then

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

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

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

The proof of the next theorem is left as an (easy) exercise.

Theorem 12: Exponential rules for groups

Let G be a group, $g, h \in G$, $m, n \in \mathbb{Z}$.

(1) mult: $g^m g^n = g^{m+n}$, add: $mg + ng = (m+n)g$;

(2) mult: $(g^m)^n = g^{mn}$, add: $m(ng) = (mn)g$;

(3) mult: $(gh)^n = (h^{-1}g^{-1})^{-n}$, add: $m(g+h) = mg + mh$.

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 examples of subgroups.

Example. The subgroups of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ are $\{0\}$, $\{0, 2\}$, and $\mathbb{Z}_4$.

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 13: The Subgroup Test

A subset H of a group G is a subgroup if and only if

(1) the identity element $e \in G$ is in H;

(2) if $h_1, h_2 \in H$, then $h_1 h_2 \in H$;

(3) if $h \in H$, then $h^{-1} \in H$.

The next proposition is a shortcut to the shortcut, but it is only useful in certain circumstances.

Proposition 14: The *Better* Subgroup Test

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

Example. Let $\mathrm{SL}_2(\mathbb{R})$ denote the subset of determinant one matrices in $\mathrm{GL}_2(\mathbb{R})$. We show that $\mathrm{SL}_2(\mathbb{R})$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

Families of Groups

1. Cyclic groups

In the group $(\mathbb{Z}_n, +)$, any element can be obtained by adding the element 1 sufficiently many times. Thus, one would say that 1 *generates* the group and we call the group *cyclic*. One should also observe that in a group, such as $(\mathbb{Z}_8, +)$, there are additional generators, namely 3, 5, and 7. On the other hand, 2, 4, 6, and 0 are not generators.

In this section we will develop the theory of cyclic groups in detail. They have the remarkable property that every subgroup is abelian and we can use this fact to determine all subgroups of $\mathbb{Z}$.

Theorem 1: The group generated by an element

Let G be a group and $a \in G$. The set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G containing a.

In additive notation, we use the notation $\langle a \rangle = \{ka : k \in \mathbb{Z}\}$.

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.

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapters 4-5. Portions are also drawn from Keith Conrad's notes on the dihedral groups. Last Updated: March 6, 2021

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

We write $|a| = n$ to denote the order of the element a (or $|a| = \infty$ if the order is infinite). In additive notation, we write $na = 0$ instead of $a^n = e$ in the above notation.

Proposition 2: Alternate definition of order of an element

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

Example. Find the order of every element of D_3.

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 and makes use of some of the techniques from the first two chapters.

Theorem 4: Every subgroup of a cyclic group is cyclic

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

Corollary 5: Subgroups of $\mathbb{Z}$

The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

Proposition 6: Powers of the generator equal to identity

Let $G = \langle a \rangle$ is a cyclic group of order n. Then $a^k = e$ if and only if $n \mid k$.

Our last result can be used to determine the generators of a cyclic group.

Theorem 7: Order of an element in a cyclic group

Let $G = \langle a \rangle$ be a cyclic group of order n. If $b = a^k$, then $|b| = n/d$ where $d = \gcd(k, n)$.

Corollary 8: Generators of $\mathbb{Z}_n$

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 9: 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 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*.

Proposition 10: Order of $\mathcal{S}_n$

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 $\mathcal{S}_4$:

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

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

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

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

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

The next theorem gives an algorithm for decomposing cycles.

Theorem 12: Cycle decomposition

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

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

3. The Alternating Group

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

Definition: Transposition

A *transposition* is a cycle of length 2.

Proposition 13: Decomposing a permutation as a transposition

Every permutation can be written as the product of (not necessarily disjoint) transpositions. Moreover, any decomposition of a given cycle contains either an even number or an odd number of transpositions.

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 14: 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*, denoted A_n, is the subgroup of $\mathcal{S}_n$ generated by all even permutations.

Proposition 15: Order of A_n

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

4. Dihedral Groups

Throughout this section, $n \geq 3$. Recall that the dihedral group D_n is the set of rigid motions (symmetries) in the plane of a regular n-gon. We will first prove that $|D_n| = 2n$ and secondly to determine the relations between reflections and rotations in D_n.

Recall that every symmetry of a regular n-gon corresponds to a rearrangement of the n vertices. Thus, we can *think* of an element of D_n as a permutation of the vertices. Since D_n is a group, it is tempting then to say that D_n is a subgroup of S_n but this isn't quite right. A better way to say this is that D_n is *isomorphic to* a subgroup of S_n. We will formalize this in coming chapters.

Lemma 16

There exist (at least) $2n$ distinct rigid motions of a regular n-gon.

Note that the above lemma does not say that these are all of the rigid motions.

Theorem 17: 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. Let $r \in D_n$ denote the rotation by $(360/n)^\circ$. Then the n rotations may be expressed as: $1, r, r^2, \ldots, r^{n-1}$ where 1 is the identity rotation. Let s denote *any reflection through a vertex.* Note that $s^2 = 1$ and $s^{-1} = s$.

Theorem 18: Presentation of D_n

The n reflections in D_n are $s, rs, r^2s, \ldots, r^{n-1}s$.

Thus, the elements of D_n are $\{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$ with $r^n = 1$ and $s^2 = 1$. We will now prove a critical defining relation in D_n.

Theorem 19: Relation on D_n

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

Cosets and Normal Subgroups

1. 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. Let $K = \{(1), (1\ 2)\}$ in $\mathcal{S}_3$. The left cosets are

The right cosets are

Note that, except for the coset of the elements in H, the left and right cosets are different.

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapters 6, and 9-11. Last Updated: April 2, 2021

Example. Let $L = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ in $\mathcal{S}_3$. The left cosets are

The right cosets are

Warning. In additive notation, we write

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

Note that additive groups are by definition abelian and so $g + H = H + g$.

Example. Let $H = \langle 3 \rangle = \{0, 3\}$ in $\mathbb{Z}_6$. The cosets are

Lemma 1: 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) $g_1^{-1} g_2 \in H$.

Theorem 2: Cosets partition a group

Let H be a subgroup of a group G. The left cosets of H in G partition G.

The above result holds if we replace 'left' with 'right'.

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 3: 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.

2. Lagrange's Theorem

Lagrange's Theorem is an important step in understanding the structure of (finite) groups.

Lemma 4: 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 5: Lagrange's Theorem

Let G be a finite group and H a subgroup of G. Then $|G|/|H| = [G : H]$. In particular, the order of H divides the order of G.

We'll now examine a host of consequence of Lagrange's Theorem.

Corollary 6: 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 $|G|$, and $g^{|G|} = e$.

Corollary 7: Prime groups are cyclic

Let G be a group with $|G| = p$, p prime. Then G is cyclic and any $g \in G$, $g \neq e$, is a generator.

Let's take a moment to consider what we have just proved. The last corollary says that *every* group of prime power order is cyclic. Thus, if G is a group of order p, p prime, then G is *essentially* the same as $\mathbb{Z}_p$. We will formalize this in coming sections.

Corollary 8: Index is multiplicative

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

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

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.

Now for a fun little diversion into number theory.

Definition: Euler ϕ-function

The *Euler ϕ-function* is defined as $\phi : \mathbb{N} \to \mathbb{N}$ with $\phi(1) = 1$ and for $n > 1$,

$$\phi(n) = |\{m \in \mathbb{N} : 1 \leq m < n \text{ and } \gcd(m, n) = 1\}|.$$

It follows that $|U(n)| = \phi(n)$ for all $n \in \mathbb{N}$.

Theorem 9: Euler's Theorem

Let a, n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \mod n$.

Theorem 10: Fermat's Little Theorem

Let p be any prime and suppose $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$. Furthermore, for any $b \in \mathbb{Z}$, $b^p \equiv b \mod p$.

3. Normal subgroups and factor groups

Factor groups are a group structure on the set of cosets of a group by certain subgroups. This is also setup for the isomorphism theorems in the last section.

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 11: 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. Note that there is no need to differentiate between left and right cosets, but we will typically work with left cosets.

Lemma 12: 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 13: 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 group G/N is the *factor group* of G by N.

Example. Let $G = \mathcal{S}_3$ and $N = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. (Note that $N = A_3$). Then N is normal in G and the cosets are N and $(1\ 2)N$. The Cayley Table of G/N is given by

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. Consider the subgroup $H=3\mathbb{Z}$ in $\mathbb{Z}$. There are 3 cosets: $0+H$, $1+H$, $2+H$. The Cayley Table of G/H is given by

Example. Consider D_n generated by r,s with

$$r^n=\mathrm{id},\quad s^2=\mathrm{id},\quad srs=r^{-1}.$$

Let R_n be the subgroup of rotational symmetries.

4. 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, image

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

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

The set $\operatorname{im} \phi = \{\phi(g) : g \in G\}$ is called the *image* of ϕ.

Example. The following are examples of homomorphisms.

Proposition 14: Properties of homomorphisms

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

(1) $\phi(e_G) = e_H$.

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

(3) If K is a subgroup of G, then $\phi(K)$ is a subgroup of H.

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

Definition: Kernel

The *kernel* of a homomorphism $\phi : G \to H$ is the set $\ker \phi = \{g \in G : \phi(g) = e\}$.

Example. The following are examples of kernels.

Theorem 15: A kernel is a normal subgroup

Let $\phi : G \to H$ be a group homomorphism. Then $\ker \phi$ is a normal subgroup of G.

The converse of the previous theorem is true in some sense. Every normal subgroup is the kernel of *some* homomorphism. This is a key component of the *First Isomorphism Theorem*.

5. Isomorphisms

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.

Lemma 16: Trivial kernel implies 1-1

A group homomorphism $\phi : G \to H$ is injective if and only if $\ker \phi = \{e_G\}$.

Proposition 17: Surjective + trivial kernel implies isomorphism

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

Theorem 18: 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.

The next theorem may be regarded as a classification of all cyclic groups (up to isomorphism).

Theorem 19: Classification of cyclic groups

Let G be a cyclic group with generator $a \in G$.

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

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

Corollary 20

If $|G| = p$, p prime, then $G \cong \mathbb{Z}_p$.

Our last goal in this section will be to prove Cayley's Theorem, which proves the "fundamentalness" of the symmetric groups in group theory.

Lemma 21: Left multiplication is a permutation

Let G be a group and $g \in G$. The map

$$\lambda_g : G \to G \qquad a \mapsto ga$$

is a permutation of G.

In general, λ_g is *not* a homomorphism.

Lemma 22: The group $\overline{G}$

For a group G, the set $\overline{G} = \{\lambda_g : g \in G\}$ is a group under composition.

Theorem 23: Cayley's Theorem

Every group is isomorphic to a group of permutations.

6. Direct products

We have previously seen one type of product group, the *external direct product*. Recall that if $(G, \cdot)$ and $(H, \circ)$ are groups, then $G \times H = \{(g, h) : g \in G, h \in H\}$ is a group under the operation $\star$:

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$$

for all $(g_1, h_1), (g_2, h_2) \in G \times H$.

Lemma 24: Order of elements in a direct product

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

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

Proposition 25: 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 $\gcd(m, n) = 1$.

Definition: External Direct Product

If G is a group and A, B subgroups of G such that $G \cong A \times B$, then G is said to be the *external direct product* of A and B.

Example. We will show that $\mathbb{Z}_6$ is the external direct product of its subgroups.

For a group G with subgroups H, N, we define the set

$$HN = \{hn : h \in H, n \in N\}.$$

Note that in general this is *not* a subgroup of G.

Lemma 26: 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. We will show that $U(8)$ is a internal direct product of two subgroups.

Example. We will show that $\mathcal{S}_3$ is *not* an internal direct product of its subgroups.

Lemma 27: Uniqueness of representation in HK

If G is the internal direct product of subgroups H and K, then every element in G can be written uniquely as hk for some $h \in H$, $k \in K$.

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 28: 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. By a previous example, $U(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

7. The isomorphism theorems

The following theorems explain how factor group structures fit into the overall picture of group structure. They are also incredibly powerful tools for proving that two groups are isomorphic.

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.

Theorem 29: First Isomorphism Theorem

Let $\phi : G \to H$ be a homomorphism and $K = \ker \phi$. There exists an isomorphism

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

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

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

Theorem 30: Second Isomorphism Theorem

Let H, N be subgroups of a group G with N normal. Then $H/H \cap N \cong HN/N$.

Example. We claim that $2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_3$.

Proofs of the following results are left as an exercise.

Theorem 31: Correspondence Theorem

Let N be a normal subgroup of a group G. Then there is a bijection from the set of all subgroups containing N and the set of subgroups of G/N. Furthermore, the normal subgroups of G containing N correspond to normal subgroups of G/N.

Example. Demonstrate the Correspondence Theorem for $G = \mathbb{Z}_{12}$ and let $N = \langle 4 \rangle$.

Theorem 32: Third Isomorphism Theorem

Let H, N be normal subgroups of a group G with $N \subset H$. Then

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

Example. Show that $\mathbb{Z}/3\mathbb{Z} \cong (\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z})$.

Finite Abelian Groups

0. Introduction

Though it might be bad form, we'll start by stating the big theorem that we want to prove. We'll then work on the proof throughout the next few sections. Ultimately, this is a generalization of the fact that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$.

Theorem 1: 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:

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapter 13. Last Updated: April 15, 2021

1. p-groups

Our goal will be to take an arbitrary finite abelian group and decompose it in a manner according to the fundamental theorem. This requires first building up the theory of p-groups.

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.

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

Lemma 2: Subgroup of prime power elements

Let G be a finite abelian group and write $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ with the p_i distinct primes. The set $G_i = \{g \in G : |g| = p_i^k, k \in \mathbb{Z}\}$ is a subgroup of G.

Lemma 3: 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

One immediate consequence of the next lemma is that each G_i is a p-group.

Lemma 4: p-group is a prime power group

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

2. Proof of the Fundamental Theorem (Part I)

In this section, we prove the Fundamental Theorem for finite p-groups. The proof will conclude in the next section wherein we decompose a finite abelian group into a direct product of p-groups.

We begin with a technical result that will help in the proof of the first proposition.

Lemma 5

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 6

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 7: 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, $G \cong \langle g \rangle \times K$.

Thus, the following definition is just a generalization of our previous one, as is the subsequent proposition whose proof 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) $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_i \in H_i\}$ (as sets),

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

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

Proposition 8: 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

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

Lemma 9: Finite abelian group is the IDP of p-groups

Let G be a finite abelian group. Then G is the internal direct product of p-groups.

Theorem 10: The Fundamental Theorem of Finite Abelian Groups

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

Definition: Subgroup generated by a subset, finitely generated group

Let G be a group and $X \subset G$. The smallest subgroup containing X is the *subgroup generated by* X, denoted $\langle X \rangle$. If $\langle X \rangle = G$, then G is said to be *generated by* X. If in addition $|X| < \infty$, then G is said to be *finitely generated*.

Example. The following are examples of finitely generated groups.

Proposition 11

If X is a set of generators for G, then every element in G can be written as a product of (powers of) the elements of X.

Theorem 12: The Fundamental Theorem of Finitely Generated Abelian Groups

Every finitely generated abelian group is isomorphic to a direct product of cyclic groups of the form

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

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

Introduction to rings

1. 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).

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:

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapter 16. Last Updated: April 21, 2021

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*.

Exercise. A ring R is a division ring if and only if $(R \backslash \{0\}, \cdot)$ is a group.

Example. Consider our examples of rings above. Let's consider what properties these rings have.

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 $\mathbb{Z}$.

2. Homomorphisms and ideals

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

$$\ker \phi = \{x \in R : \phi(x) = 0_s\}$$
$$\operatorname{im} \phi = \{\phi(a) : a \in R\}.$$

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 4: 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.

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 5: 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 6: 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 7: $\mathbb{Z}$ is a PID

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

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.

We are now ready to state the isomorphism theorems (for rings). The proofs, especially for the First Isomorphism Theorem, are very similar to proofs of the corresponding group theorems.

Theorem 10: Isomorphism Theorems for Rings

(First Isomorphism Theorem) Let $\phi : R \to S$ be a ring homomorphism. Then

$$R/\ker\phi \cong \phi(R).$$

(Second Isomorphism Theorem) Let R be a ring, S a subring of R, and I an ideal of R. Then $S \cap I$ is an ideal of S and

$$\frac{S}{S\ \cap I} \cong \frac{S+I}{I}.$$

(Third Isomorphism Theorem) Let R be a ring with ideals $J \subset I$. Then

$$R/I \cong \frac{R/J}{I/J}.$$

Polynomial rings

1. Polynomials

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

$$\begin{aligned} p(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ q(x) &= b_0 + b_1 x + \cdots + b_m x^m. \end{aligned}$$

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)

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapter 17. Last Updated: May 3, 2021

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 $p(x)q(x)$.

Example. Let $p(x) = 3 + 3x^3$ and $q(x) = 4 + 4x^2 + 4x^4$ be polynomials in $\mathbb{Z}_{12}[x]$. Compute $p(x) + q(x)$ and $p(x)q(x)$.

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*.

The next result verifies that $R[x]$ is indeed a ring.

Theorem 1: Polynomial ring and properties passed up from R

Let R be a ring.

(1) The set $R[x]$ under addition and multiplication is a ring.

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

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

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

Remark. What we actually proved in the last proposition was that for an integral domain R,

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

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

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 $R[x_1, \ldots, x_n]$.

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

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

Proposition 2: Evaluating a polynomial

Let S be a commutative ring with identity and R a subring of S containing 1. Let $\alpha \in S$. Then there is a ring homomorphism $\phi_\alpha : R[x] \to S$ given by $\phi_\alpha(p(x)) = p(\alpha)$.

Definition: Evaluation homomorphism

The map ϕ_α is called the *evaluation homomorphism* at α. We say $\alpha \in R$ is a *root* (or *zero*) of $p(x) \in R[x]$ if $\phi_\alpha(p(x)) = 0$.

2. Divisibility

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 3: 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 4: 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 5: 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 6: 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.

3. Irreducible polynomials

Definition: Irreducible

Let F be a field. A nonconstant polynomial $f(x) \in F[x]$ is *irreducible* over F if $f(x)$ cannot be written as a product of two polynomials $g(x), h(x) \in F[x]$ with $\deg g(x), \deg h(x) < \deg f(x)$.

Example. Show that the following polynomials are irreducible over the given ring.

(1) $x^2 - 2$ over $\mathbb{Q}$.

(2) $x^2 + 1$ over $\mathbb{R}$.

(3) $p(x) = x^3 + x^2 + 2$ over $\mathbb{Z}_3$.

The proof of the next two results have been omitted.

Theorem 7: Gauss' Lemma

If a non-constant monic polynomial $p(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$.

Corollary 8: Zero in $\mathbb{Q}$ implies zero in $\mathbb{Z}$

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

Example. Let $p(x) = x^4 - 2x^3 + x + 1$. We will show that $p(x)$ is irreducible over $\mathbb{Q}$.

The following actually requires a stronger version of Gauss' Lemma that we will not prove here.

Theorem 9: Eisenstein's Criterion

Let p be a prime and suppose that

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

If $p \mid a_i$ for $i = 0, 1, \ldots, n-1$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Example. Let $f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$. Show that $f(x)$ is irreducible over $\mathbb{Q}$.