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: September 18, 2019

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

Definition 1. 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'll now briefly discuss basic operations on sets.

Definition 2. 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 $Y \neq X$.

Warning. I tend to use $\subset$ instead of $\subseteq$. I will do this, even if there is no proper inclusion (so it makes sense to write $X \subset X$). This is the same notation used by Judson.

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 on 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: $A \times B = \{(a, b) : a \in A, b \in B\}$

Warning. Set difference is sometimes denoted with a minus sign ($-$) instead of a backslash ($\backslash$).

Proposition 1. 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. Exercise. □

Warning. When I leave proofs as exercises, it's not because I'm being lazy[1]. These are proofs that I think you're capable of doing on your own and are good practice. I strongly encourage you to work through these exercises and talk to me about them. It's a good way to get feedback on your proof writing and check your understanding of concepts without the pressure of grades.

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) below and leave (2) as an exercise:

$$\begin{aligned}(A \cup B)' &= \{x \in U : x \notin (A \cup B)\} \\ &= \{x \in U : x \notin A \text{ and } x \notin B\} \\ &= \{x \in U : x \in A' \text{ and } x \in B'\} \\ &= \{x \in U : x \in A' \cap B'\}.\end{aligned}$$

□

Next we'll discuss equivalence relations on sets.

Definition 3. 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 $[x] = \{y \in X : (x, y) \in R\}$.

Warning. 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. Let's check the properties.

- (reflexive) Let $x \in \mathbb{Z}$, then $x - x = 0$ and 0 is divisible by n. Thus $(x, x) \in R$.
- (symmetric) Suppose $(x, y) \in R$. Thus, $x - y = nk$ for some integer k. Then $y - x = n(-k)$ and so $y - x$ is divisible by n and $(y, x) \in R$.
- (transitive) Suppose $(x, y), (y, z) \in R$. 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 and $(x, z) \in R$.

Thus, R is an equivalence relation on $\mathbb{Z}$. We write $x \equiv y \mod n$ if $(x, y) \in R$. 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.

[1] OK, I'm being a *little* lazy.

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 4. 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. 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 $\bigcup_{k \in X} [x_k] = X$. □

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 and 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 5. Let A and B be sets. A function (or mapping) $f \subset A \times B$ 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 $f(A) = \{f(a) : a \in A\} \subset B$.

Warning. This is not the definition of a function that one sees in a calculus course. Instead, one might say that 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. Note the well-defined and one-to-one are not the same thing. For f to be 1-1, a value in the codomain cannot have more that one pre-image.

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). Clearly, every input has an output. We must show that each input has a unique output. In other words, the output is *independent of the choice of equivalence class representative.*

Let $a, a', b, b' \in \mathbb{Z}$ such that $[a] = [a']$ and $[b] = [b']$. We claim $[a] + [b] = [a'] + [b']$. Since $[a] = [a']$, then $a' = a + kn$. Similarly, $b' = b + \ell n$. Thus,

$$a' + b' = (a + kn) + (b + \ell n) = (a + b) + (k + \ell)n.$$

Therefore, $a' + b' \in [a + b]$ so $[a + b] = [a' + b']$.

Definition 6. 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.

Definition 7. Let $f : A \to B$ and $g : B \to C$ be functions. The composition $g \circ f : A \to C$ is defined by the rule $(g \circ f)(a) = g(f(a))$ for all $a \in A$.

Example. Let $X = \{1, 2, 3\}$. The function $f : X \to X$ given by $f(1) = 2$, $f(2) = 1$, and $f(3) = 3$ is bijective. As f is a bijective function from a set to itself, it is called a permutation.

Exercise. 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). Be careful with sides! Remember that composition of functions is not a commutative operation.

Theorem 4. 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.

Proof. We will prove (1) and (3). Property (2) is left as an exercise. Property (4) follows from (2) and (3).

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.

For (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. □

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.

Definition 8. 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 said to be 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 map, denoted f^{-1}.

Warning. The inverse of a function is unique. We will prove this soon in higher generality. For now you should think about why it is true but may take it as a given.

Theorem 5. 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. Then for every $a \in A$, there is exactly one element $b \in B$ such that $f(a) = b$. (There is one because f is surjective and no more than one because f is injective). Thus, define $f^{-1} : B \to A$ by the rule that $f^{-1}(b) = a$ if $f(a) = b$. It is easy to check that f^{-1} is well-defined. □

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

Example.

- Addition and multiplication on the integers (or $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) are binary operations.
- Addition on $\mathbb{N}$ is a binary operation but subtraction is not.
- Division is not a binary operation on $\mathbb{Z}$ or $\mathbb{Q}$, but it is on $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$.
- Addition mod n is a binary operation.

3. Induction, the well-ordering principle, and the division algorithm

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 commonly 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 $n \geq 0$.

Definition 10. A nonempty subset S of $\mathbb{Z}$ is well-ordered if S contains a least element.

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 f 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 $q = q'$. □

The proof of the next theorem is 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 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 $s = 88$.

We will often use the notation $a \mid b$ in place of a divides b. The proofs of the following results are left as exercises.

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

(1) Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
(2) Identity: there exists $e \in G$ such that $a \cdot e = e \cdot a$ 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.

Warning. 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.

- $(\mathbb{Z}, +)$ is a group. One can also replace $\mathbb{Z}$ by $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ (but not $\mathbb{N}$).
- For any positive integer n, $(\mathbb{Z}_n, +)$ is a group.
- $(\mathbb{Q}^\times, \cdot)$ is a group. One can also replace $\mathbb{Q}^\times$ by $\mathbb{R}^\times$ (but not $\mathbb{Z}^\times$).
- Let $M_2(\mathbb{R})$ denote the set of 2×2 matrices with entries in $\mathbb{R}$. Then $(M_2(\mathbb{R}), +)$ is a group, where $+$ is the operation of matrix addition.
- Let $\mathrm{GL}_2(\mathbb{R}) \subset M_2(\mathbb{R})$ denote the set of 2×2 *invertible* matrices. Then $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ is a group where $\cdot$ is the operation of matrix multiplication (This follows from the fact that $\det(A)\det(B) = \det(AB)$ for all $n \times n$ matrices A, B).

Because for a group $(G, \cdot)$, G is a set and so it makes sense to write $|G| = n$ for the number of elements in the group/set G (so $|\mathbb{Z}_n| = n$). We call n the order of the group and say a group is finite if $n < \infty$. Otherwise the group is said to be infinite.

Definition 12. A Cayley Table records all compositions in a group (like a multiplication table).

Example. The Cayley table for $(\mathbb{Z}_4, +)$ is printed below. We drop the [ ] notation and recognize the operation as addition mod n.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

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

Definition 13. For any positive integer n, let $U(n)$ denote the set of invertible elements (units) in $\mathbb{Z}_n$. Then $U(n)$ is a group under the operation of multiplication mod n.

Exercise. Check that multiplication mod n is indeed a binary operation.

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

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition 14. 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. The Cayley table is printed below.

	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_2	μ_3	μ_1
ρ_2	ρ_2	id	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	id	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	id	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	id

Warning. 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. 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 $a, b, c \in G$,

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

Proof. (1) Let $e, e' \in G$ be identity elements. Because e is an identity element, then $e = ee'$. Because e' is an identity element, $ee' = e$. Thus, $e = ee' = e'$.

(2) Fix $g \in G$ and let $g', g'' \in G$ be inverses of G. Then

$$e = gg' \Rightarrow g''e = g''gg' \Rightarrow g'' = eg' \Rightarrow g'' = g'.$$

(3) By (2), it suffices to show that $h^{-1}g^{-1}$ is *the* inverse of gh. But this is a straightforward verification,

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e.$$

One verifies similarly that $(h^{-1}g^{-1})(gh) = e$. Or see the next exercise.

(4) Multiply on the left or right by a^{-1} and use the associativity axiom. □

It's important to note that (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

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

On the other hand, 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 12. 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: $m(g + h) = mg + mh$.

Proof. Easy exercise. □

6. Subgroups

Definition 15. A subgroup H of a group G is a subset such that H is a group with respect to the operation associated to G.

Example. (1) Let G be a group. Then G is a subgroup of itself. If $e \in G$ is the identity element, then $\{e\}$ is a subgroup called the trivial subgroup. A subgroup of G that is not G and not the trivial subgroup is called proper.

(2) $2\mathbb{Z}$, the set of even numbers, is a subgroup of $\mathbb{Z}$ (under addition). The set of odd numbers is not a subgroup.

(3) $\mathbb{R}^\times$ is a group under multiplication and $\mathbb{Q}^\times$ is a subgroup.

(4) $\mathrm{GL}_2(\mathbb{R})$ is a subset of $M_2(\mathbb{R})$ but not a subgroup because $M_2(\mathbb{R})$ is a group under matrix addition and $\mathrm{GL}_2(\mathbb{R})$ a group under matrix multiplication.

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,

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

The Cayley Table for this group is given below.

	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

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 are $\{(0,0)\}$, $\{(0,0),(1,0)\}$, $\{(0,0),(1,0)\}$, $\{(0,0),(1,1)\}$, and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note that this group has more subgroups than $\mathbb{Z}_4$. Thus, even though they have the same order, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are different groups.

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) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$;
(3) $h \in H \Rightarrow h^{-1} \in H$.

Proof. ($\Rightarrow$) Suppose H is a subgroup. We will verify that the three conditions hold.

(1) As H is a group, it has an identity element, say e_H. We must show that $e_H = e$. Since $e_H \in H$ and $H \subset G$, then $e_H \in G$. Thus, $e_H \cdot e_H = e_H$ and $e_H \cdot e = e_H$. Thus, $e_H \cdot e_H = e_H \cdot e$. By left cancellation, $e_H = e$.

(2,3) These follows because H is a group and therefore closed under multiplication and inverses.

($\Leftarrow$) Suppose (1),(2), and (3) hold. We must show that H is a group. The operation is associative because G is a group and H is a subset of G. (2) says that the operation is a binary operation on H (closure). (1) says that H has an identity. (3) says that H is closed under inverses. Thus, H is a group. □

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 $a, b \in H$, $ab^{-1} \in H$.

Proof. ($\Rightarrow$) Assume H is a subgroup. Then $H \neq \emptyset$ because $e \in H$. If $a, b \in H$, then $b^{-1} \in H$ by closure under inverses and by closure of multiplication $ab^{-1} \in H$.

($\Leftarrow$) Assume $H \neq \emptyset$ and $a, b \in H$ implies $ab^{-1} \in H$. We will verify (1), (2), and (3) from the previous proposition.

(1) Let $a \in H$ (this exists because H is non-empty). Then $e = aa^{-1} \in H$. (2) Since $e \in H$ by (1), then for any $a \in H$ we have $a^{-1} = ea^{-1} \in H$. (3) Given $a, b \in H$, we have $b^{-1} \in H$ by (2) and so $ab = a(b^{-1})^{-1} \in H$. Thus, H is a subgroup. □

Example 15. Let $\mathrm{SL}_2(\mathbb{R})$ denote the subset of determinant one matrices in $\mathrm{GL}_2(\mathbb{R})$. Since $\det(I_2) = 1$, then $I_2 \in \mathrm{SL}_2(\mathbb{R})$ and so $\mathrm{SL}_2(\mathbb{R}) \neq \emptyset$. Now suppose $A, B \in \mathrm{SL}_2(\mathbb{R})$. Then

$$\det(AB^{-1}) = \det(A)\det(B)^{-1} = 1,$$

so $AB^{-1} \in \mathrm{SL}_2(\mathbb{R})$. Thus, $\mathrm{SL}_2(\mathbb{R})$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. (The subgroup $\mathrm{SL}_2(\mathbb{R})$ is known as the *special linear group*.)

Families of Groups

1. Cyclic groups

Recall the group $(\mathbb{Z}_n, +)$ that we studied previously. Note that any element in this group 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 use this fact to determine all subgroups of $\mathbb{Z}$.

Theorem 1. 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.

Proof. Since $a \in \langle a \rangle$, then $\langle a \rangle \neq \emptyset$. Let $g, h \in \langle a \rangle$, then $g = a^k$ and $h = a^\ell$ for some $k, \ell \in \mathbb{Z}$. Then $gh^{-1} = (a^k)(a^{-\ell}) = a^{k-\ell} \in \langle a \rangle$ and so $\langle a \rangle$ is a subgroup.

Let H be another subgroup of G containing a. Because H is a group, every power of a lives in H. Thus, $\langle a \rangle \subset H$, proving the second claim. □

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

Definition 1. Let G be a group. For $a \in G$, $\langle a \rangle$ is called the cyclic subgroup of G generated by a. If there exists $a \in G$ such that $\langle a \rangle = G$, then G is said to be a cyclic group and a a generator of G. The order of a is the smallest positive integer such that $a^n = e$ ($na = 0$ in additive notation) and we write $|a| = n$. If no such n exists then we say the order is infinite and write $|a| = \infty$.

Example.

- $\mathbb{Z}$ is a cyclic group generated by either 1 or -1. Note that $|1| = |-1| = \infty$.
- $\mathbb{Z}_6$ is a cyclic group generated by 1 or 5. Note that $\langle 2 \rangle = \langle 2, 4, 0 \rangle$.
- $U(9)$ is a cyclic group generated by 2.
- The group D_3 is not cyclic but every proper subgroup is cyclic.

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: September 18, 2019

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 2. Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$, a cyclic group, and H a subgroup of G. If $H = \langle e \rangle$ or $H = G$, then this is trivial so assume H is a proper subgroup. Note that, because H is a subgroup of G, every element of H has the form a^n for some $n \in \mathbb{Z}$.

Let m be the smallest positive integer such that $a^m \in H$. Such an m exists because H is proper and by the Well-Ordering Principle. We claim $h = a^m$ is a generator for H. Let $h' \in H$. Then $h' = a^k$ for some integer $k > 0$. By the Division Algorithm, there exists some integers q, r such that $k = mq + r$ with $0 \leq r < m$. Now

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

But then $a^r = a^k h^{-q} \in H$, contradicting the minimality of m. Thus, $r = 0$ and $a^k = h^q \in \langle h \rangle$, so h is a generator of H. □

Corollary 3. The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

Proposition 4. Let $G = \langle a \rangle$ is a cyclic group of order n. Then $a^k = e$ if and only if $n \mid k$.

Proof. If $n \mid k$, then $k = n\ell$ for some positive integer ℓ and

$$a^k = a^{n\ell} = (a^n)^\ell = e^\ell = e.$$

Now suppose $a^k = e$. This is similar to the proof of the previous theorem. By the Division Algorithm there exists integers q, r such that $k = nq + r$ with $0 \leq r < n$. Hence,

$$e = a^k = a^{nq+r} = (a^n)^q a^r = ea^r = a^r.$$

This contradicts the definition of order since n is the smallest positive integer such that $a^n = e$. Thus, $r = 0$ and so $n \mid k$. □

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

Theorem 5. Let $G = \langle a \rangle$ be a cyclic group of order n. If $b = a^k$, then $|b| = n/d$ where $d = \gcd(k, n)$.

Proof. Set $m = |b|$. This is the smallest integer such that $e = b^m = a^{km}$. By the previous proposition, this implies that n divides km. Equivalently, n/d divides $m(k/d)$. Since $d = \gcd(k, n)$, then n/d and k/d are relatively prime. Hence, n/d divides m.

On the other hand, k/d is an integer and so n divides $(k/d)n$. Hence, $b^{n/d} = a^{kn/d} = a^{(k/d)n} = e$. But m is the order of b so by Proposition 4, m divides n/d. □

Corollary 6. 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 $\{A, B, C\}$, D_4 does not for the set of $\{A, B, C, D\}$.

Exercise. Find a rearrangement (bijective function) of the set $\{A, B, C, D\}$ that does not correspond to an element of D_4.

Definition 2. A permutation is a bijective function on the set X (from X to itself). The set of permutations on X is denoted $\mathcal{S}_X$. If X is finite we write $X = \{1, \ldots, n\}$ and denote $\mathcal{S}_X$ by $\mathcal{S}_n$ and call it the symmetric group on n letters. A subgroup of $\mathcal{S}_n$ is said to be a permutation group.

Theorem 7. S_n is a group of order $n!$ under composition.

Proof. The composition of two bijective functions is again a bijective function (see Chapter 1). Moreover, the operation of composition is associative (check!). The identity function is given by $\mathrm{id}(x) = x$ for all $x \in X$ and a bijective function is invertible.

The last part of the theorem is left as an exercise. □

There are two standard types of notation to represent elements of $\mathcal{S}_n$: two-line and cycle. Two-line is in some ways easier to use at first but much clumsier. We will learn both but as we go on we will use cycle notation much more frequently.

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. 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:

	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	τ	μ	id
τ	τ	μ	id	σ
μ	μ	id	σ	τ

This Cayley table is equivalent to one we've seen before. Where?

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

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

Then

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

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

Definition 3. 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, one *could* translate back to two-line notation but I strongly advise against that. Instead, 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

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

Then

$$\sigma\tau = (1\ 4\ 3\ 2)(1\ 3)(2\ 4) = (2\ 3\ 4\ 1) = (1\ 2\ 3\ 4) = \mu.$$

Definition 4. Two cycles $\sigma = (a_1\ a_2\ \cdots\ a_k)$ and $\tau = (b_1\ b_2\ \cdots\ b_\ell)$ are said to be 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 $(1\ 3\ 5)(3\ 4\ 7) = (3\ 4\ 7\ 5\ 1)$.

Proposition 8. Disjoint cycles in $\mathcal{S}_n$ commute.

Proof. Let $\sigma, \tau \in \mathcal{S}_n$ be disjoint. Write $\sigma = (a_1\ a_2\ \cdots\ a_k)$ and $\tau = (b_1\ b_2\ \cdots\ b_\ell)$. We claim $(\sigma\tau)(x) = (\tau\sigma)(x)$ for all $x \in \{1, \ldots, n\}$.

Suppose $x \notin \{a_1, \ldots, a_k\}$ and $x \notin \{b_1 \ldots, b_\ell\}$. By definition of a cycle, $(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$ and similarly $(\tau\sigma)(x) = \tau(\sigma(x)) = \tau(x) = x$.

Now suppose $x \in \{a_1, \ldots, a_k\}$ (so $x \notin \{b_1, \ldots, b_\ell\}$). Then $\sigma(x) \in \{a_1, \ldots, a_k\}$ and so $\sigma(x) \notin \{b_1, \ldots, b_\ell\}$. Thus $(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x)$ and $(\tau\sigma)(x) = \tau(\sigma(x)) = \sigma(x)$.

The proof for $x \in \{b_1, \ldots, b_\ell\}$ is similar. □

The next theorem gives an algorithm for decomposing cycles.

Theorem 9. Every element in $\mathcal{S}_n$ can be written as the product of disjoint cycles.

Proof. Set $X = \{1, \ldots, n\}$. First we will decompose X into disjoint pieces and use these to define the cycles. Choose $\sigma \in \mathcal{S}_n$ and define $X_1 = \{1, \sigma(1), \sigma^2(1), \ldots\}$. Then X_1 is finite because σ has finite order. Choose $k \in X \backslash X_1$ and define $X_2 = \{k, \sigma(k), \sigma^2(k), \ldots\}$. Continue in this way. Note that the process *must* end because X is finite. Write $X = X_1 \cup X_2 \cup \cdots \cup X_r$.

Define a cycle σ_i by

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i. \end{cases}$$

Then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$. Note that the σ_i are disjoint because the X_i are. □

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.

Starting with 1 we have $\sigma_1 = (1\ 3)$. We choose a value, say 2, that is not yet accounted for and continue, $\sigma_2 = (2)$. Next we choose 4 and continue, $\sigma_3 = (4\ 5\ 6)$. This exhausts $\{1, \ldots, 6\}$ and so $\sigma = \sigma_1 \sigma_2 \sigma_3 = (1\ 3)(2)(4\ 5\ 6)$. Note that (2) is equivalent to the identity so it is appropriate to omit it.

Example. We will compute the Cayley table for $\mathcal{S}_3$ using cycle notation. As a set (in cycle notation), $\mathcal{S}_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. The Cayley Table is

	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

Note the similarities between this table and that of D_3. Can you match up the permutations and the symmetries?

3. The Alternating Group

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

Definition 5. A transposition is a cycle of length 2.

Proposition 10. 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.

Proof. The first part is easy. We must exhibit a single decomposition. One is given below,

$$(a_1\ a_2\ a_3\ \cdots\ n) = (a_1\ a_n)(a_1\ a_{n-1})\cdots(a_1\ a_3)(a_1\ a_2).$$

The second is much harder and we will not cover this proof. The interested and motivated student is referred to the textbook for the argument. □

We say a permutation is even if it can expressed as the product of n transpositions and odd otherwise.

Theorem 11. The set of all even permutations in $\mathcal{S}_n$ is a subgroup of $\mathcal{S}_n$.

Proof. Let $\sigma, \tau \in \mathcal{S}_n$ be even permutations. Write, $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ and $\tau = \tau_1\tau_2\cdots\tau_\ell$ with k, ℓ even. Then

$$\sigma\tau^{-1} = (\sigma_1\sigma_2\cdots\sigma_k)(\tau_\ell\tau_{\ell-1}\cdots\tau_1),$$

which is an even permutation. □

Definition 6. The alternating group on n letters, denoted A_n, is the subgroup of $\mathcal{S}_n$ generated by all even permutations.

Proposition 12. The order of A_n is $n!/2$.

Proof. Let A_n and B_n denote the sets of even and odd permutations in $\mathcal{S}_n$, respectively. We will define a bijection between them, implying $|A_n| = |B_n|$. Fix a transposition $\sigma \in \mathcal{S}_n$ and define $\lambda_\sigma : A_n \to B_n$ by $\lambda_\sigma = \sigma\tau$ for all $\tau \in A_n$. Clearly this is well-defined.

If $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$, then $\sigma\tau = \sigma\mu$ so $\tau = \mu$. Thus λ_σ is 1-1. If $\eta \in B_n$, then $\sigma^{-1}\eta \in A_n$ and $\lambda_\sigma(\sigma^{-1}\eta) = \eta$, so λ_σ is surjective. □

4. Dihedral Groups

Throughout this section, $n \geq 3$. Recall that the dihedral group D_n (sometimes denoted D_{2n}) 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 13. There exist (at least) $2n$ distinct rigid motions of a regular n-gon.

Proof. There are n rotations (counterclockwise) by $\left(\frac{360 \cdot k}{n}\right)^\circ$, $k = 0, \ldots, n-1$. These are all clearly distinct from each other. Also note that there are no fixed vertices by these rotations. In fact, the only fixed point on the n-gon is the center. For reflections, we have to split into two cases.

If there are an odd number of vertices, then for each vertex there is a reflection through a point and the midpoint of the side opposite that vertex. If there are even number of vertices, the there are $n/2$ reflections through opposite vertices and $n/2$ reflections through opposite midpoints on sides. In either case there are two points fixed by the reflection (the intersection points between the lines of reflection and the n-gon). Thus, no reflection is a rotation. □

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

Theorem 14. The order of D_n is $2n$.

Proof. Choose two adjacent vertices, A and B in the regular n-gon. Let $g \in D_n$. There are n choices for the position of $g(A)$. Since g must preserve adjacency of vertices, then $g(A)$ and $g(B)$ are adjacent. Thus, given the position of $g(A)$, there are 2 choices for the position of $g(B)$. Also recall that g must preserve distances between points. Thus, given any other point P, the position of $g(P)$ is determined by the choice of location for $g(A)$ and $g(B)$. This gives $2n$ *rearrangements of the vertices.* By the Lemma 13, each such rearrangement is a rigid motion and hence $|D_n| = 2n$. □

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

Proof. First note that these are all distinct from each other since $r^k s = r^\ell s$ implies $r^k = r^\ell$. Suppose one of the above is a rotation, that is $sr^k \neq r^\ell$ for some k, ℓ. But then $s = r^{\ell - k}$, which implies that s is a rotation, a contradiction. Thus, sr^k is a reflection for all k. □

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

Proof. Let A be a vertex fixed by s with adjacent vertices B, B' where B is counterclockwise of A. Then

$$(srs)(A) = (sr)(s(A)) = s(r(A)) = s(B) = B' \quad \text{and} \quad r^{-1}(A) = B.$$
$$(srs)(B) = (sr(s(B)) = s(r(B')) = s(A) = A \quad \text{and} \quad r^{-1}(B) = A.$$

Thus, since the relation holds for an arbitrary pair of adjacent vertices, it holds for all vertices. □

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 1. Let G be a group and H a subgroup of G. A left coset of H with representative in G is the set

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

A right coset of H with representative 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

$$(1)K = (1\ 2)K = \{(1), (1\ 2)\}$$
$$(1\ 3)K = (1\ 2\ 3)K = \{(1\ 3), (1\ 2\ 3)\}$$
$$(2\ 3)K = (1\ 3\ 2)K = \{(2\ 3), (1\ 3\ 2)\}$$

The right cosets are

$$K(1) = K(1\ 2) = \{(1), (1\ 2)\}$$
$$K(1\ 3) = K(1\ 3\ 2) = \{(1\ 3), (1\ 3\ 2)\}$$
$$K(2\ 3) = K(1\ 2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$$

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

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

$$0 + H = \{0, 3\} = 3 + H$$
$$1 + H = \{1, 4\} = 4 + H$$
$$2 + H = \{2, 5\} = 5 + H.$$

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: October 18, 2019

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

$$(1)L = (1\ 2\ 3)L = (1\ 3\ 2)L = L$$
$$(1\ 2)L = (1\ 3)L = (2\ 3)L = \{(1\ 2), (1\ 3), (2\ 3)\}$$

The right cosets are

$$L(1) = L(1\ 2\ 3) = L(1\ 3\ 2)$$
$$L(1\ 2) = L(1\ 3) = L(2\ 3) = \{(1\ 2), (1\ 3), (2\ 3)\}$$

In this case, the left and right cosets are the same.

Lemma 1. Let H be a subgroup of G and suppose $g_1, g_2 \in G$. The following are equivalent.

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

Proof. (1) $\Rightarrow$ (2) Assume $g_1H \subset g_2H$. We claim the opposite inclusion holds. Let $g_2h \in g_2H$ for some $h \in H$. Since $g_1 \in g_1H \subset g_2H$, then $g_1 = g_2h'$ for some h'. But then $g_2 = g_1(h')^{-1}$ and so

$$g_2h = g_1(h')^{-1}h = g_1((h')^{-1}h) \in g_1H.$$

(2) $\Rightarrow$ (3) Assume $g_1H = g_2H$. Let $hg_1^{-1} \in Hg_1^{-1}$ with $h \in H$. Note that $g_1 \in g_1H = g_2H$, so $g_1 = g_2h'$ for some $h' \in H$. Then $g_1^{-1} = (h')^{-1}g_2^{-1}$ and so

$$hg_1^{-1} = h((h')^{-1}g_2^{-1}) = (h(h')^{-1})g_2^{-1} \in Hg_2^{-1}.$$

Thus, $Hg_1^{-1} \subset Hg_2^{-1}$. A similar proof shows the reverse inclusion and the result follows.

(3) $\Rightarrow$ (4) Assume $Hg_1^{-1} = Hg_2^{-1}$. Then $g_2^{-1} \in Hg_2^{-1} = Hg_1^{-1}$ so $g_2^{-1} = hg_1^{-1}$ for some $h \in H$. Thus, $g_2 = g_1h^{-1} \in g_1H$.

(4) $\Rightarrow$ (5) Assume $g_2 \in g_1H$. Then $g_2 = g_1h$ for some $h \in H$. Thus, $g_1^{-1}g_2 = h \in H$.

(5) $\Rightarrow$ (1) Assume $g_1^{-1}g_2 \in H$. Let $g_1h \in g_1H$ for some $h \in H$. By our assumption, $g_1^{-1}g_2 = h'$ for some $h' \in H$. Thus, $g_1 = g_2(h')^{-1}$ and $g_1h = g_2((h')^{-1}h) \in g_2H$. Therefore $g_1H \subset g_2H$. $\square$

Warning. Remember when we proved that the equivalence classes under some equivalence relation partition the set. This is when we need that result.

Theorem 2. Let H be a subgroup of a group G. The left cosets of H in G partition G.

Proof. Define an equivalence relation $\sim$ on G by $g_1 \sim g_2$ if (and only if) $g_2 \in g_1 H$. Clearly $\sim$ is reflexive because $g_1 = g_1 e \in g_1 H$, so $g_1 \sim g_1$. Suppose $g_1 \sim g_2$. Then $g_2 \in g_1 H$. By the previous lemma, this implies $g_1 H = g_2 H$ and so $g_1 = g_1 e \in g_1 H = g_2 H$. Thus, $g_2 \sim g_1$ and so $\sim$ is reflexive. Finally, suppose $g_1 \sim g_2$ and $g_2 \sim g_3$. Then $g_2 \in g_1 H$ and $g_3 \in g_2 H$. Again using the above lemma, $g_1 H = g_2 H$ and $g_2 H = g_3 H$, so $g_1 H = g_3 H$. Thus, $g_3 \in g_1 H$ so $g_1 \sim g_3$.

The equivalence classes under this relation *are the cosets* and therefore a partition of G. □

Note that the above result holds if we replace 'left' with 'right'. One could prove it similarly or apply the lemma (exercise).

Definition 2. Let G be a group and H a subgroup. The index of H in G is the number of left cosets in G, denoted $[G : H]$.

We will show momentarily that the number of left cosets is equal to the number of right cosets.

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. Let H be a subgroup of G. The number of left cosets of H in G is the same as the number of right cosets.

Proof. Denote by $\mathcal{L}_H$ the set of left cosets of H in G and by $\mathcal{R}_H$ the set of right cosets of H in G. We will establish a bijection between these sets, which shows that $|\mathcal{L}_H| = |\mathcal{R}_H|$.

Define a map

$$\begin{aligned} \phi : \mathcal{L}_H &\to \mathcal{R}_H \\ gH &\mapsto Hg^{-1}. \end{aligned}$$

First we need to show that this map is well-defined. Suppose $g_1 H = g_2 H$. By the lemma, $\phi(g_1 H) = Hg_1^{-1} = Hg_2^{-1} = \phi(g_2 H)$. Thus, ϕ is well-defined.

Suppose $\phi(g_1 H) = \phi(g_2 H)$, then $Hg_1^{-1} = Hg_2^{-1}$. Again, the lemma implies $g_1 H = g_2 H$, so ϕ is injective. Let $Hg \in \mathcal{R}_H$. Then $\phi(g^{-1} H) = H(g^{-1})^{-1} = Hg$, so ϕ is surjective.

Thus, ϕ is bijective and so the result holds. □

2. Lagrange's Theorem

The next lemma proves a fact we observed in the examples.

Lemma 4. Let H be a subgroup of G. For all $g \in G$, $|H| = |gH|$.

Proof. Fix $g \in G$ and define a map $\phi : H \to gH$ by $h \mapsto gh$. It is clear that ϕ is well-defined. We will show that it is bijective. It will then follow immediately that $|H| = |gH|$.

Suppose $\phi(h) = \phi(h')$ for $h, h' \in H$. Then $gh = gh'$ and so by left cancellation, $h = h'$. Thus ϕ is injective. Next let $gh \in gH$ for some $h \in H$, then $\phi(h) = gh$ so the map is surjective. □

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.

Proof. The group G is partitioned into $[G : H]$ distinct left cosets. Each coset has exactly $|H|$ elements by the previous lemma. Hence, $|G| = |H|[G : H]$. □

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

Corollary 6. Suppose G is a finite group and $g \in G$. Then the order of g divides $|G|$, and $g^{|G|} = e$.

Proof. Note that $|g| = \langle g \rangle$. Thus, for the first statement we simply apply Lagrange's Theorem with $H = \langle g \rangle$. Now set $d = |G|$. Then $|g| = k \mid d$ by the above Thus, $d = k\ell$ for some integer ℓ. Then $g^d = g^{k\ell} = (g^k)^\ell = e^\ell = e$. □

Corollary 7. 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.

Proof. Let $g \in G$, $g \neq e$. Then $|g| \mid |G|$ by the previous corollary, so $|g| = 1$ or p. But $g \neq e$ so $|\langle g \rangle| > 1$, so $|\langle g \rangle| = p$. Thus, $\langle g \rangle = G$. □

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

Proof. We have by Lagrange's Theorem,

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K].$$ □

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 3. The Euler ϕ-function is defined as $\phi : \mathbb{N} \to \mathbb{N}$ with $\phi(1) = 1$ and

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

This next theorem formalizes something we discussed much earlier.

Theorem 9. Let $n \in \mathbb{N}$.

(1) $|U(n)| = \phi(n)$.
(2) (Euler's Theorem) Let a, n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \mod n$.
(3) (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 $b \in \mathbb{Z}$, $b^p \equiv b \mod p$.

Proof. (1) By definition, $|U(n)|$ is the set of integers m, $1 \leq m < n$ that are invertible (under multiplication) mod n. We need only show that any such number is relatively prime to n. Suppose $mk \equiv 1 \mod n$ for some integer k. Then $mk = n\ell + 1$, or $mk + n(-\ell) = 1$ for some integer ℓ. Thus, by the Euclidean Algorithm, $\gcd(m, n) = 1$.

(2) Since $|U(n)| = \phi(n)$, then $a^{\phi(n)} = 1$ for all $a \in U(n)$. This is equivalent to $a^{\phi(n)} \equiv 1 \mod n$.

(3) Apply Euler's Theorem with $n = p$. □

3. Normal subgroups and factor groups

Warning. We are deviating from the structure of the book at this point. I make no apologies.

On one hand, normality encapsulates the idea of left and right cosets being the same, but more importantly they lead to the idea of *factor groups*. The motivation for this is simply that subgroups do not give a full sense of the structure of the groups. The factor groups give the complementary hidden structure.

Definition 4. A subgroup N of a group G is normal if $gN = Ng$ for all $g \in G$.

Example. (1) If G is abelian, then *every* subgroup is normal.
(2) $L = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ is normal in $\mathcal{S}_3$.
(3) $K = \{(1), (1\ 2)\}$ is *not* normal in $\mathcal{S}_3$.

Theorem 10. Let G be a group and N a subgroup. The following are equivalent.

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

Proof. (1) $\Rightarrow$ (2) Assume N is normal and fix $g \in G$. Let $n \in N$, then by the definition of normal, $gN = Ng$ so $gn = n'g$ for some $n' \in N$. Thus, $gng^{-1} = (n'g)g^{-1} = n'(gg^{-1}) = n' \in N$, so $gNg^{-1} \subset N$.

(2) $\Rightarrow$ (3) Assume $gNg^{-1} \subset N$ for all $g \in G$. We claim the opposite inclusion holds (for all $g \in G$). Let $n \in N$ and fix $g \in G$. By our assumption, $g^{-1}ng \subset N$ (since it holds for all $g \in G$). Thus, $g^{-1}ng = n'$ for some $n' \in N$, so $n = gn'g^{-1} \in gNg^{-1}$. Therefore, $N \subset gNg^{-1}$.

(3) $\Rightarrow$ (1) Assume $gNg^{-1} = N$ for all $g \in G$. We will show $gN \subset Ng$. The proof that $Ng \subset gN$ is similar. Let $g \in G$ and $n \in N$. Then $gng^{-1} = n'$ for some $n' \in N$. Thus, $gn = n'g \in Ng$. □

Let N be a normal subgroup of a group G. We define a binary operation on the cosets by

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

Before we proceed, we should verify that this operation is actually well-defined. Said another way, we must verify that the product is independent of choice of coset representative.

Let $aN = cN$ and $bN = dN$. We claim $(aN)(bN) = (cN)(dN)$. Since $c \in aN$ and $d \in bN$, then there exists $n_1, n_2 \in N$ such that $c = an_1$ and $d = bn_2$. Thus

$$(cd)N = (an_1)(bn_2)N = (an_1)b(n_2N) = (an_1)(bN) = (an_1)(Nb) = a(n_1N)b = aNb = (ab)N.$$

Note that $bN = Nb$ by normality.

Warning. The operation for additive cosets is equivalent,

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

We denote by G/N the set of cosets of N in G.

Theorem 11. 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 $[G:N]$.

Proof. We have already shown that the operation is binary. We verify the group axioms. Throughout, let $aN, bN, cN \in G/N$. The operation is associative since

$$(aN)[(bN)(cN)] = (aN)(bcN) = (a(bc))N = ((ab)c)N = (abN)(cN) = [(aN)(bN)](cN).$$

For all $aN \in G/N$, $(eN)(aN) = (ea)N = aN$, so $eN = N$ is the identity in G/N. Similarly, for all $aN \in G/N$, $(aN)(a^{-1}N) = (aa^{-1})N = eN$, so $a^{-1}N$ is the inverse of aN. □

Definition 5. 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 (we have already verified this) and the cosets are N and $(1\ 2)N$. The Cayley Table is given by

	N	(1 2)N
N	N	(1 2)N
(1 2)N	(1 2)N	N

Observe that this table is equivalent to that of $\mathbb{Z}_2$.

Example. Consider the subgroup $H = 3\mathbb{Z}$ in $\mathbb{Z}$. There are 3 cosets: $0+H$, $1+H$, $2+H$. Write out the Cayley Table for $\mathbb{Z}/H$ and observe how it is equivalent to that of $\mathbb{Z}_3$.

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. Then R_n is normal in D_n because $srs = r^{-1} \in R_n$. Note that

$$|D_n/R_n| = [D_n : R_n] = |D_n|/|R_n| = 2n/n = 2.$$

Thus, the Cayley Table is equivalent to $\mathbb{Z}_2$.

4. Homomorphisms

Our next goal will be to explain how normal subgroups and factor groups arise naturally in the study of groups. In particular, a normal subgroups can be thought of as the *kernel*, or left over, part of a map between two groups.

Definition 6. 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.

One should think of a homomorphism as a *structure preserving map*, that is, it preserves the structure of the groups G and H. In fact, whenever you see the word *morphism*, this is generally what is meant.

Example.
(1) The function $\phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ given by $\phi(M) = \det(M)$ is a homomorphism. Note that in this case ϕ is surjective but not injective.
(2) The function $\phi : M_2(\mathbb{R}) \to \mathbb{R}$ given by $\phi(M) = \det(M)$ is *not* a homomorphism because $\det(M + N) \neq \det(M) + \det(N)$ in general.
(3) The function $\phi : \mathbb{Z}_2 \mapsto \mathbb{Z}_4$ by $\phi(0) = 0$ and $\phi(1) = 2$. This map is injective but not surjective.
(4) Choose $g \in G$, G a group, and define $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. Then ϕ is a homomorphism and $\operatorname{im} \phi = \langle g \rangle$.
(5) Let $C = (\{1, -1\}, \times)$. Define $\phi : \mathcal{S}_n \to C$ by $\sigma(\sigma) = \operatorname{sgn} \sigma$ where $\operatorname{sgn} \sigma = 1$ if σ is even and -1 is σ is odd. (We say $\operatorname{sgn} \sigma$ is the sign of σ).

Proposition 12. 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.

Proof. (1) Let $g \in G$, then

$$\phi(g)e_H = \phi(g) = \phi(ge_G) = \phi(g)\phi(e_G).$$

By left cancellation, $e_H = \phi(e_G)$.

(2) Let $g \in G$, then by (1),

$$e_H = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}).$$

Hence, $\phi(g)^{-1} = \phi(g^{-1})$.

(3) Let K be a subgroup of G. Since $e_G \in K$, then $K \neq \emptyset$. Let $a, b \in \phi(K)$, so there exists $k_1, k_2 \in K$ such that $\phi(k_1) = a$ and $\phi(k_2) = b$. Then $ab^{-1} = \phi(k_1)\phi(k_2)^{-1} \in K$ because K is a subgroup of G. Thus, $\phi(K)$ is a subgroup of H.

(4) Let L be a subgroup of H. Since $e_G \in \phi^{-1}(L)$, then $\phi^{-1}(L) \neq \emptyset$. Choose $c, d \in \phi^{-1}(L)$, so $\phi(c), \phi(d) \in L$. Then by (2) $\phi(cd^{-1}) = \phi(c)\phi(d^{-1}) = \phi(c)\phi(d)^{-1} \in L$ because L is a subgroup of H. Thus, $cd^{-1} \in \phi^{-1}(L)$ and so $\phi^{-1}(L)$ is a subgroup of G.

Finally, suppose L is normal in H. Let $g \in H$. We claim $g\phi^{-1}(L)g^{-1} \in \phi^{-1}(L)$. Let $a \in \phi^{-1}(L)$, then $\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in L$ because L is normal. Thus, $gag^{-1} \in \phi^{-1}(L)$ for all $a \in \phi^{-1}(L)$, so $\phi^{-1}(L)$ is normal in G. □

Definition 7. The kernel of a homomorphism $\phi : G \to H$ is $\ker \phi = \{g \in G : \phi(g) = e_H\}$.

Theorem 13. Let $\phi : G \to H$ be a group homomorphism. Then $\ker \phi$ is a normal subgroup of G.

Proof. The trivial group $\{e_H\}$ is a normal subgroup of H and $\ker \phi = \phi^{-1}(\{e_H\})$. The result now follows from Proposition 12 (4). □

Example. (1) $\phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ given by $\phi(M) = \det(M)$. Then $\ker \phi = \mathrm{SL}_2(\mathbb{R})$.

(2) $\phi : \mathbb{Z}_2 \mapsto \mathbb{Z}_4$ by $\phi(0) = 0$ and $\phi(1) = 2$. We can check directly that $\ker \phi = \{0, 2\}$.

(3) Choose $g \in G$, G a group, and define $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. If $|g| = \infty$ then $\ker \phi = \{0\}$. If $|g| = k$, then $\ker \phi = k\mathbb{Z}$.

(4) Let $\phi : \mathcal{S}_n \to C$ by $\sigma(\sigma) = \operatorname{sgn} \sigma$. Then $\ker \phi = A_n$.

Example. Let G be a group and N a normal subgroup. The quotient map $\phi : G \to G/N$ is given by $\phi(g) = gN$. This is a homomorphism since for all $g, h \in G$,

$$\phi(g)\phi(h) = (gN)(hN) = (gh)N = \phi(gh).$$

The quotient map is *always* surjective (the preimage of gN is g). The kernel of the quotient map is $\ker \phi = N$ and so the quotient map is injective if and only if N is the trivial group.

The previous example illustrates the idiom: *Kernels are normals and normals are kernels.*

5. Isomorphisms

Definition 8. 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. (1) Let H be a cyclic group of order 3 generated by h (so $H = \{e, h, h^2\}$). The map $\phi : \mathbb{Z}_3 \to H$ is an isomorphism. Note that we have already verified that this map is an isomorphism, we need only verify that it is injective and surjective, but this is an easy exercise in this case.

(2) The groups D_3 and $\mathcal{S}_3$ are isomorphic. One possible map is $\phi : D_3 \to \mathcal{S}_3$ given by setting $\phi(r) = (123)$ and $\phi(s) = (12)$.

Theorem 14. 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.

Proof. (1) By standard results on functions, ϕ^{-1} exists and is bijective (see the book's introductory chapter). We need only verify that it is a homomorphism, but this is easy. Since $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$, then $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$ for all $a, b \in G$.

(2) This follows because ϕ is bijective.

(3) Assume G is abelian. Let $h_1, h_2 \in H$, then there exist (unique) elements $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1) = h_2 h_1.$$

Thus, H is abelian.

(4) Exercise.

(5) Let K be a subgroup of G of order n. Then $\phi(K)$ is a subgroup of H because ϕ is a homomorphism. Moreover, $|\phi(K)| = n$ because ϕ is bijective. □

Proposition 15. A surjective group homomorphism $\phi : G \to H$ is an isomorphism if and only if $\ker \phi = \{e_H\}$.

Proof. Assume ϕ is an isomorphism. Because it is a homomorphism, $e_H \in \ker \phi$. Because it is 1-1, then $\ker \phi = \{e_H\}$.

Assume $\ker \phi = \{e_H\}$. We claim ϕ is 1-1. Suppose $\phi(g_1) = \phi(g_2)$ for some $g_1, g_2 \in G$. Then $e = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1 g_2^{-1})$. Thus, by our assumption, $g_1 g_2^{-1} = e$ so $g_1 = g_2$. It follows that G is 1-1 and thus an isomorphism. □

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

Theorem 16. 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 $G \cong \mathbb{Z}_n$.

Proof. Define a map $\phi : \mathbb{Z} \to G$ by $\phi(n) = a^n$. Note that we have already verified that ϕ is a homomorphism. We verify in (1) that ϕ is bijective and leave (2) as an exercise.

It is clear that ϕ is surjective. We will show that it is injective and thus an isomorphism. Let $k, \ell \in \mathbb{Z}$ such that $\phi(k) = \phi(\ell)$. Then $a^k = a^\ell$ and so $a^{k-\ell} = e$. Since $|a| = \infty$, this implies $k - \ell = 0$, so $k = \ell$. Thus, ϕ is injective and the result follows. □

Corollary 17. If $|G| = p$, p prime, then $G \cong \mathbb{Z}_p$.

Proof. Let $a \in G$, $a \neq e$. Then by Lagrange's Theorem, $|a| \mid p$. Since $|a| \neq 1$ then $|a| = p$. Thus, $G = \langle a \rangle$. By the previous theorem, $G \cong \mathbb{Z}_p$. □

The next result tells us that every group is (isomorphic to) a subgroup of $\mathcal{S}_n$.

Theorem 18 (Cayley's Theorem)**.** Every group is isomorphic to a group of permutations.

Proof. Let G be a group and for each $g \in G$ define a map $\lambda_g : G \to G$ by $\lambda_g(a) = ga$ for all $a \in G$. Note that if $h \in G$, then $\lambda_g(g^{-1}h) = g(g^{-1}h) = h$, so λ_g is surjective. If $a, b \in G$ such that $\lambda_g(a) = \lambda_g(b)$, then $ga = gb$ so $a = b$ by left cancellation. Thus, λ_g is injective and hence bijective[1] It follows that λ_g is a permutation of (the set) G.

Now set $\overline{G} = \{\lambda_g : g \in G\}$. We claim that $\overline{G}$ is a group under function composition. Of course, function composition is associative so we need only check closure under the operation, existence of an identity, and closure under inverses. First claim that for $\lambda_g \lambda_h = \lambda_{gh}$ for all $g, h \in G$. These are functions, so it suffices to check this by evaluating both sides at some $a \in G$:

$$\lambda_{gh}(a) = (gh)a = g(ha) = g(\lambda_h a) = \lambda_g(\lambda_h a) = (\lambda_g \lambda_h)(a).$$

Now it is clear that λ_e is the identity of $\overline{G}$ and that $\lambda_{g^{-1}}$ is the inverse of λ_g for all $g \in G$. Thus, $\overline{G}$ is a group.

Finally, we define a map $\Phi : G \to \overline{G}$ by $g \mapsto \lambda_g$. By the previous paragraph, Φ is a homomorphism. We claim that Φ is an isomorphism. It is clear that Φ is surjective. For injectivity, let $g, h \in G$ such that $\Phi(g) = \Phi(h)$, so $\lambda_g = \lambda_h$. Now if $a \in G$, then $ga = \lambda_g(a) = \lambda_h(a) = ha$, so $g = h$ by right cancellation. Thus, Φ is bijective and further an isomorphism. □

[1] Note that λ_g is not a homomorphism in general.

6. Direct products

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 $\star$ below,

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

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

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

Proposition 19. 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 9. 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. The cyclic group $\mathbb{Z}_6$ has subgroups $A = \langle 2 \rangle \cong \mathbb{Z}_3$ and $B = \langle 3 \rangle \cong \mathbb{Z}_2$. By the above proposition, $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Thus, $\mathbb{Z}_6$ is the external direct product of A and B.

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. The next proposition gives a criteria where it is.

Proposition 20. Let G be a group with subgroups H, N. If N is normal, then HN is a subgroup of G.

Proof. Clearly $e \in HN$ because $e \in H \cap N$. Let $h_1n_1, h_2n_2 \in HN$. Then $(h_1n_1)(h_2n_2)^{-1} = (h_1n_1)(n_2^{-1}h_2)$. Because N is normal, $Nh_2 = h_2N$. Thus, $n_2^{-1}h = hn_3$ and $n_1h = hn_4$ for some $n_3, n_4 \in N$. We therefore have

$$(h_1n_1)(h_2n_2)^{-1} = (h_1n_1)(n_2^{-1}h_2) = (h_1n_1)(h_2n_3) = h_1(h_2n_4)n_3 = (h_1h_2)(n_4n_3) \in HN.$$

Thus, HN is a subgroup of G. □

Warning. In additive notation, HN is $H + N = \{h + n : h \in H, n \in N\}$. Recall that subgroups of abelian groups are always normal and so $H + N$ is always a subgroup of G.

Exercise. Let H, N be subgroups of a group G with N normal. Prove that N is normal subgroup of HN and $H \cap N$ is a normal subgroup of H.

Definition 10. A group G is the interal direct product of subgroups H and K provided

$$(1)\ G = HK \text{ (as sets)}, \quad (2)\ H \cap K = \{e\}, \text{ and } \quad (3)\ hk = kh \text{ for all } h \in H,\ k \in K.$$

Example. Let $G = U(8)$, $H = \{1, 3\}$, $K = \{1, 5\}$. Then $G = HK$ (because $3 \cdot 5 \equiv 7 \mod 8$). Clearly $H \cap K = \{1\}$, and because G is abelian we have $hk = kh$ for all $h \in H$, $k \in K$. Thus, G is the internal direct product of H and K.

Example. $\mathcal{S}_3$ is *not* an internal direct product of its subgroups. Since $|\mathcal{S}_3| = 6$ then without loss of generality we need subgroups H, K with $|H| = 3$ and $|K| = 2$. But then $H \cong \mathbb{Z}_3$ and $K \cong \mathbb{Z}_2$. The condition $hk = kh$ for all $h \in H$, $k \in K$ now implies that $\mathcal{S}_3$ is abelian, a contradiction.

Lemma 21. 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 $h \in H$, $k \in K$.

Proof. Let $g \in G$. By the first condition of internal direct products, $G = HK$, and so $g = hk$ for some $h \in H$, $k \in K$. We claim this decomposition is unique. Suppose $g = h'k'$ for some $h' \in H$, $k' \in K$. By the second condition, $hk = h'k'$ and so $(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\}$. Thus, $(h')^{-1}h = e$ and $k'k^{-1} = e$, so $h = h'$ and $k' = k$. □

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

Proof. Define a map $\phi : H \times K \to G$ by $(h, k) \mapsto hk$. By the lemma, ϕ is bijective. We need only show that it is a homomorphism. Let $(h_1, k_1), (h_2, k_2) \in H \times K$. Then by the third condition of internal direct products,

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = (h_1h_2)(k_1k_2) = (h_1k_1)(h_2k_2) = \phi(h_1, k_1)\phi(h_2, k_2).$$

Thus, ϕ is a homomorphism and therefore an isomorphism. □

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

Here is a result that is helpful in checking the internal direct product properties above.

Proposition 23. Let H and K be subgroups of a group G. Then $|HK| = |H||K|/|H \cap K|$.

Proof. Let $C = H \cap K$ and note that C is a subgroup of K. By Lagrange's Theorem $n = [K : C] = |K|/|H \cap K|$. Thus, K is the disjoint union of n right cosets: $Ck_1 \cup Ck_2 \cup \cdots Ck_n$ for $k_i \in K$. But $HC = C$ so then HK is the disjoint union $Hk_1 \cup Hk_2 \cup \cdots Hk_n$. Thus,

$$|HK| = |H| \cdot n = |H||K|/|H \cap K|.$$ □

Example. Let $G = \mathbb{Z}_{mn}$ with $\gcd(m, n) = 1$. Set $H = \langle m \rangle$ and $K = \langle n \rangle$ so $|H| = n$ and $|K| = m$. Clearly $hk = kh$ for all $h \in H$, $k \in K$ because G is abelian. Let $g \in H \cap K$, then $|g|$ divides n and m by Lagrange's Theorem. But then $|g| = 1$ because $\gcd(m, n) = 1$. Thus, $g = 0$ and so $H \cap K = \{0\}$. Hence, by the previous proposition $|HK| = |H||K| = nm = |G|$, so $G = HK$.

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 24 (First Isomorphism Theorem)**.** Let $\phi : G \to H$ be a homomorphism and $K = \ker \phi$. There exists an isomorphism

$$\begin{aligned} \psi : G/K &\to \phi(G) \\ gK &\mapsto \phi(g). \end{aligned}$$

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

Proof. First recall that by an earlier exercise, K is a normal subgroup and thus G/K is well-defined. However, ψ is a map defined on a set of cosets and therefore we must check that it is well-defined.

Suppose $g_1K = g_2K$ for some $g_1K, g_2K \in G/K$. We must show that $\psi(g_1K) = \psi(g_2K)$. Because K is normal, our hypothesis implies that $g_2^{-1}g_1 \in K$. Therefore, $\psi(g_2^{-1}g_1) = e$, so $\psi(g_2) = \phi(g_1)$. But then $\psi(g_1K) = \phi(g_2K)$. Thus, ψ is well-defined.

We now check that ψ is a homomorphism. Let $g_1K, g_2K \in G/K$. Then

$$\psi((g_1K)(g_2K)) = \psi((g_1g_2)K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \psi(g_1K)\psi(g_2K).$$

It is left to show that ψ is bijective. Clearly ψ is surjective since for all $\phi(g) \in \phi(G)$, $\psi(gK) = \phi(g)$. To show injectivity we reverse the argument above for well-definedness. Suppose $\psi(g_1K) = \psi(g_2K)$ for some $g_1K, g_2K \in G/K$. Then $\phi(g_1) = \phi(g_2)$ so $g_2^{-1}g_1 \in K$. Because K is normal, $g_1K = g_2K$, so ψ is injective. □

Example. Consider the map $\phi : \mathbb{Z} \mapsto \mathbb{Z}_3$ given by $\phi(k) = k \mod 3$. This map is a surjective homomorphism (check!) and $\ker \phi = 3\mathbb{Z}$. By the first isomorphism theorem, $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$.

Exercise. Generalize the previous example (and carefully check all steps) to show that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ for all positive integers n.

Theorem 25 (Second Isomorphism Theorem)**.** Let H, N be subgroups of a group G with N normal. Then $H/H \cap N \cong HN/N$.

Proof. By an earlier exercise, N is a normal subgroup of HN and $H \cap N$ is a normal subgroup of H. Thus, the given factor groups are well-defined.

Define a map

$$\phi : H \to HN/N$$
$$h \mapsto hN.$$

We claim this map is a surjective homomorphism. Let $h_1, h_2 \in H$. Then by the normality of N,

$$\phi(h_1h_2) = (h_1h_2)N = h_1(h_2N) = h_1(Nh_2) = (h_1N)(Nh_2) = (h_1N)(h_2N) = \phi(h_1)\phi(h_2).$$

Thus, ϕ is a homomorphism. Let $hnN \in HN/N$, then clearly $hnN = hN = \phi(h)$, so ϕ is surjective.

By the first isomorphism theorem, $H/\ker\phi \cong HN/N$, so we need only show that $\ker\phi = H \cap N$. Let $x \in H \cap N$, then $\phi(x) = xN = N$ because $x \in N$, so $H \cap N \subset \ker\phi$. On the other hand, if $y \in \ker\phi$, then $yN = \phi(y) = N$, so $y \in N$. Thus, $\ker\phi \subset H \cap N$ so the sets are equal. □

Warning. In additive notation, the theorem is rephrased as $H + N$ instead of HN.

Example. Let $H = 2\mathbb{Z}$ and $N = 3\mathbb{Z}$ be subgroups of $\mathbb{Z}$. Clearly N is normal because $\mathbb{Z}$ is abelian. Then $H \cap N = 6\mathbb{Z}$ and $H + N = \mathbb{Z}$. Thus, by the second isomorphism theorem, $2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_3$.

The next two results are also important, but in the interest of time and sanity I will leave the proofs as reading exercises. However, I suspect that the third isomorphism theorem is one that you can prove once you fully understand the proofs above, especially that of the second isomorphism theorem.

Theorem 26 (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. Consider the group $G = \mathbb{Z}_{12}$ and let $N = \langle 4 \rangle$. Note that $G/N \cong \mathbb{Z}_4$. Then we can identify the subgroups of G containing N with the subgroups of G/N.

$$\text{subgroups of } G \text{ containing } N \mapsto \text{subgroups of } G/N$$
$$N \mapsto \{N\}$$
$$\{0, 2, 4, 6, 8, 10, 12\} \mapsto \{N, 2 + N\}$$
$$G \mapsto \{N, 1 + N, 2 + N, 3 + N\}.$$

Theorem 27 (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. By the third isomorphism theorem, $\mathbb{Z}/3\mathbb{Z} \cong (\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z})$

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 $m, n \in \mathbb{Z}$.

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:

(1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
(3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$
(4) $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
(5) $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
(6) $\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$

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: January 24, 2020

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

Definition 2. The groups $\mathbb{Z}_2$ $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are all 2-groups, as is D_4. The group $\mathbb{Z}_{27}$ is a 3-group.

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 an easy exercise.

Lemma 1. 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 2. 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

Proof. The proof is by strong induction. The case $n = 1$ is trivial so assume the lemma holds for all groups of order k, $1 \leq k \leq n$, and suppose p is a prime dividing n. If G has no proper nontrivial subgroups, then $G = \langle a \rangle$ for any $e \neq a \in G$ and n must be prime (exercise). Thus, $|a| = p$.

Suppose G contains a nontrivial proper subgroup H. Because G is abelian, then H is a normal subgroup and $|G| = |H| \cdot |G/H|$. Thus, $p \mid |G|$ or $p \mid |G/H|$. Suppose $|H| = r$, so $1 < r < n$.

If $p \mid r$, then $p \mid |H|$ and so H contains an element h of order p by the inductive hypothesis and $h \in G$. For the other case, $p \nmid r$ and so p divides $|G/H|$. By the inductive hypothesis, G/H contains an element aH of order p. Then $H = (aH)^p = a^p H$ and so $a^p \in H$ but $a \notin H$. We claim $|a^r| = p$.

Because $a^p \in H$, then $e = (a^p)^r = (a^r)^p$. Thus, $|a^r| \mid p$ so $|a^r| = 1$ or p. Therefore it suffices to show that $a^r \neq e$. Since p and r are relatively prime, there exist integers r, s such that $sp + tr = 1$. If $a^r = e$, then

$$a = a^{sp+tr} = a^{sp} a^{tr} = (a^p)^s (a^r)^t = (a^p)^s \in H.$$

This contradicts $a \notin H$. Thus, $a^r \neq e$ so $|a^r| = p$. □

Lemma 3. A finite abelian group is a p-group if and only if its order is a power of p.

Proof. If $|G|$ is a power of p, then by Lagrange's theorem, so is every element of G. Conversely, if $|G|$ is not a power of p, then there exists a prime $q \mid |G|$ and by the previous lemma, G contains an element of order q, a contradiction. □

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

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 4. 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 $|h| = p$.

Proof. Let $g \in G$ be of maximal order in G, say $|g| = p^m$ for some $m \leq n$. Since G is not cyclic, $G \neq \langle g \rangle$. Choose $h \in G \backslash \langle g \rangle$ where h has smallest possible order, say $|h| = p^\ell$. Since $e \in \langle g \rangle$, then $h \neq e$ and so $\ell > 0$. But $|h^p| = p^{\ell - l}$ (exercise) and so $|h^p|$ has smaller order than $|h|$, whence $h^p \in \langle g \rangle$. That is, $h^p = g^r$ for some r. By the above,

$$(g^r)^{p^{\ell-1}} = (h^p)^{p^{\ell-1}} = h^{p^\ell} = e.$$

Then $|g^r| \leq p^{\ell-1} < p^m$ and so g^r is not a generator for $\langle g \rangle$. Write $r = p^s$ and define $a = g^{-s}h$, so $a \notin \langle g \rangle$. Then

$$a^p = g^{-sp}h^p = g^{-r}h^p = h^{-p}h^p = e.$$

Since a has minimal non-trivial order and $a \notin \langle g \rangle$, then $|h| = p$. □

Lemma 5. 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.

Proof. First note that if $a \in G$ has order m, then $(aN)^m = a^m N = N$ and so $|aN|$ divides m. That is, the order of a coset aN is at most the order of a.

Now if $g \in G$ has maximal order n in G, then $|gN| \leq |g|$ by the above. On the other hand, if $|gN| = k$, then $N = (gN)^k = g^k N$ and so $k \in N$. Thus, $g^k \in N$ and so $g^k = e$ by hypothesis. That is, $|g|$ divides k and so $|gN| = |g|$. By the above argument, no element of G/N has order greater than the maximal order in G and so the conclusion follows. □

Proposition 6. 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.

Proof. By Lemma 3, $|G| = p^n$ for some $n \in \mathbb{N}$. The case $n = 1$ (or $n = 0$) implies G is cyclic in which case this result is trivial. Assume now that $n > 1$ and that G is not cyclic. We inductively assume that the lemma holds for all k such that $1 \leq k < n$.

Let $g \in G$ be of maximal order in G, say $|g| = p^m$ for some $m \leq n$. Choose $h \notin \langle g \rangle$ where h has smallest possible order and set $H = \langle h \rangle$. By Lemma 4, $|H| = |h| = p$. Thus, $|G/H| = |G|/|H| = p^n/p = p^{n-1}$ and so we can apply the inductive hypothesis to G/H.

Since H has no nontrivial subgroups, then $\langle g\rangle \cap H = \{e\}$. By Lemma 5, gH is an element of G/H of maximal order. By the inductive hypothesis, G/H is the internal direct product of $\langle gH\rangle$ and some subgroup K' of G/H. The Correspondence Theorem now implies that $K' = K/H$ for some subgroup K of G containing H. We claim that G is the internal direct product of $\langle g\rangle$ and K.

Let $b \in G$. Then $bH = (gH)^t y = g^t H y$ for some $t \in \mathbb{N}$ and $y \in K$. Then there exists $h, h' \in H$ such that $bh = g^t h' y$ and since $H \subset K$, $b = g^t(h' y h^{-1}) \in \langle g\rangle K$. Thus, $G = \langle g\rangle K$.

The group G is abelian so it is left only to prove that $\langle g\rangle \cap K = \emptyset$. Suppose there exists $b \in \langle g\rangle \cap K$. Then $bH \in \langle gH\rangle \cap K/H = H$, so $b \in H$. But this implies that $b \in \langle g\rangle \cap H = \{e\}$. It follows that G is the internal direct product of $\langle g\rangle$ and K. □

Corollary 7. Let G be a finite abelian p-group and suppose that $g \in G$ has maximal order. Then G is isomorphic to $\langle g\rangle \times K$ for some subgroup K.

3. Proof of the Fundamental Theorem (Part II)

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 3. 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 8. If a group G is the internal direct product of subgroups $H_1, H_2, \ldots, H_n$, then $G \cong H_1 \times H_2 \times \cdots \times H_n$ and each $g \in G$ can be written uniquely as $h_1h_2\cdots h_n$, $h_i \in H_i$.

Lemma 9. Let G be a finite abelian group. Then G is the internal direct product of p-groups.

Proof. Write $|G| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ with the p_i distinct primes. By Lemma 1, the sets G_i are subgroup of G. We will show that G is an internal direct product of the G_i.

If $g \in G$, then by Lagrange's Theorem, $|g| = p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ where $0 \leq \beta_i \leq \alpha_i$ for all i. Let $a_i = |g|/p^{\beta_i}$. The a_i are relatively prime so there exist b_i such that $a_1b_1 + a_2b_2 + \cdots + a_nb_n = 1$. Then

$$g = g^{a_1b_1+a_2b_2+\cdots+a_nb_n} = g^{a_1b_1}g^{a_2b_2}\cdots g^{a_nb_n}.$$

For each i, we have

$$\left(g^{a_ib_i}\right)^{p^{\beta_i}} = g^{b_i|g|} = e.$$

Thus, $g^{a_ib_i} \in G_i$ for all i. It follows that $G = G_1G_2\cdots G_n$.

Let $h \in G_i \cap \langle \bigcup_{j\neq i} G_j \rangle$. Because $h \in G_i$, $h = p_i^k$ for some $k \in \mathbb{Z}$. But if $h \in \langle \bigcup_{j\neq i} G_j \rangle$, then h is the product of elements whose orders are not divisible by p_i. Hence, $|h|$ is not divisible by p_i (because the G_i are all abelian). Thus, $k = 0$, so $h = e$. □

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.

Proof. Let G be a finite abelian group. By Lemma 9, G is the internal (and hence the external) direct product of the G_i, which are all p-groups by Lemma 3. Applying Corollary 7, inductively, we get that each of the G_i decompose (isomorphically) into the direct product of cyclic groups. The result follows. □

4. Finitely generated abelian groups

Definition 4. 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. (1) If G is generated by X and $|X| = 1$, then G is cyclic.

(2) D_n is generated by $X = \{r, s\}$.

(3) Finite groups are finitely generated, just take $X = G$.

(4) $\mathbb{Q}$ is not finitely generated. To see this, let $X = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n} \right\}$ be a generating set for G with all fractions written in lowers terms. Choose $p \in \mathbb{Z}$ such that $p \nmid q_i$ for all i. Then $p \notin \langle X \rangle$.

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 finite 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 $\alpha_i \in \mathbb{N}$.

We won't prove this theorem here.

Group actions

1. Group actions on sets

There are two (primary) motivations for studying group actions. On one hand, this generalizes our original motivation for studying groups (symmetries). On the other hand, this provides us with the tools to classify (nonabelian) finite groups. Using tools in these notes, we will be able to classify groups of order up to 12. Note that groups of order 1, 2, 3, 4, 5, 7, and 11 can be classified by other means. In the case that the order is prime, every such group is cyclic. Only groups of order 4 need special attention.

Exercise. Every group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition 1. Let X be a set and G a group. A (left) action of G on X is a map $G \times X \to X$ given by $(g, x) \mapsto gx$ where

(1) $ex = x$ for all $x \in X$;
(2) $(g_1 g_2)x = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

We call X a G-set.

Example.
(1) If G is a group and X any set, then G acts on X by the trivial action $(g, x) \mapsto x$.
(2) Let $G = \mathrm{GL}_2(\mathbb{R})$ and $X = \mathbb{R}^2$. Then G acts on X by left multiplication.
(3) Let $G = \{(1), (13), (14), (1\ 4\ 3\ 2), (1\ 2\ 3\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(24)\} \subset \mathcal{S}_4$. Then $G \cong D_4$. If $X = \{1, 2, 3, 4\}$ is the set of vertices of the square, then D_4 acts on the set X according to the permutations.
(4) If X is any set and G a subgroup of $\mathcal{S}_X$, then G acts on X by the rule $(\sigma, x) \mapsto \sigma(x)$.
(5) Let G be a group and $X = G$ (as a set). Then G acts on itself by left multiplication $(g, x) \mapsto \lambda_g(x)$. This is known as the (left) regular representation of G.
(6) Again let G be a group and $X = G$ (as a set). Let H be a subgroup of G, then G is an H-set under conjugation, $(h, g) \mapsto hgh^{-1}$.
(7) Conjugation also defines an action of a group G on the set S of subgroups of G. That is, for $K \in S$, the action is given by the map $(g, K) \mapsto gKg^{-1}$. Note that if K is normal then $(g, K) \mapsto K$ for all $g \in G$.
(8) Let H be a subgroup of a group G and $\mathcal{L}_H$ the set of left cosets of H. The set $\mathcal{L}_H$ is a G-set under the action $(g, xH) \mapsto (gx)H$.

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapters 14 and 15. Some parts are borrowed from *Algebra* by Thomas Hungerford, Contemporary Abstract Algebra by Joseph Gallian(5ed), as well as Keith Conrad's notes on classification of small groups. Last Updated: October 31, 2019

Exercise. Let G be a group and X a G-set. If $gx = y$, then $g^{-1}y = x$.

Definition 2. If a group G acts on a set X and $x, y \in X$, then x is said to be G-equivalent to y if there exists a $g \in G$ such that $gx = y$. We write $x \sim_G y$ (or just $x \sim y$ if the group G is implied).

Proposition 1. Let G be a group. Then G-equivalence is an equivalence relation on a G-set X.

Proof. Since $ex \sim x$ for all $x \in X$, then $\sim$ is reflexive. Assume $x \sim y$, then there exists $g \in G$ such that $gx = y$. But then $x = g^{-1}y$, so $y \sim x$ and $\sim$ is symmetrix. Finally, assume $x \sim y$ and $y \sim z$. Then there exists $g, h \in G$ such that $gx = y$ and $hy = z$. But then $(hg)x = h(gx) = hy = z$, so $x \sim z$ and $\sim$ is transitive. □

Definition 3. Let G be a group and X a G-set. The partitions of X under $\sim_G$ are called the orbits of X under G. We denote the orbit of $x \in X$ by $\mathcal{O}_x$.

Example. Let G be the permutation group $\{(1), (1\ 2\ 3), (1\ 3\ 2), (4\ 5), (1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\}$. Let $X = \{1, 2, 3, 4, 5\}$, so X is a G-set with orbits $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ and $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$.

Proposition 2. Let G be a group and X a G-set. For $x \in X$, the set $G_x = \{g \in G : gx = x\}$ is a subgroup of G.

Proof. By the axioms of G-sets, $ex = x$ and so $e \in G_x$. Let $g, h \in G_x$, then $(gh)x = g(hx) = gx = x$, so $gh \in G_x$. Finally, if $g \in G_x$, then $gx = x$ implies $x = g^{-1}x$ and so $g^{-1} \in G_x$. Thus, G_x is a subgroup. □

Definition 4. Let G be a group and X a G-set. For $x \in X$, the stabilizer subgroup of x is $G_x = \{g \in G : gx = x\}$. For $g \in G$, the fixed point set of g is the set $X_g = \{x \in X : gx = x\}$.

Warning. Note that the fixed point set X_g is a subset of X but does not have any additional structure.

Example. Let $X = \{1, 2, 3, 4, 5, 6\}$ and suppose G is the permutation group

$$\{(1), (1\ 2)(3\ 4\ 5\ 6), (3\ 5)(4\ 6), (1\ 2)(3\ 6\ 5\ 4)\}.$$

Then the fixed point sets are

$$X_{(1)} = X, \qquad X_{(3\ 5)(4\ 6)} = \{1, 2\}, \qquad X_{(1\ 2)(3\ 4\ 5\ 6)} = X_{(1\ 2)(3\ 6\ 5\ 4)} = \emptyset.$$

The stabilizer subgroups are

$$G_1 = G_2 = \{(1), (3\ 5)(4\ 6)\}, \qquad G_3 = G_4 = G_5 = \{(1)\}.$$

Now we see how all of these sets are connected.

Theorem 3 (The Orbit-Stabilizer Theorem)**.** Let G be a finite group and X a finite G-set. If $x \in X$, then $|\mathcal{O}_x| = [G : G_x]$.

Proof. We will establish a bijection between $\mathcal{O}_x$ and the set of left cosets $\mathcal{L}_{G_x}$ of G_x in G. Define

$$\phi : \mathcal{L}_{G_x} \to \mathcal{O}_x$$
$$gG_x \mapsto gx.$$

We claim ϕ is well-defined. Suppose $gG_x = hG_x$, then $h^{-1}g \in G_x$ so $(h^{-1}g)x = x$. Thus, $gx = hx$. and so ϕ is well-defined. Reversing the argument shows that $gx = hx$ implies $gG_x = hG_x$, so ϕ is injective. Finally, let $y \in \mathcal{O}_x$. Then there exists $g \in G$ such that $gx = y$ and $\phi(gG_x) = gx = y$, thus, ϕ is surjective and hence bijective. □

Example. Recall the earlier example of $X = \{1, 2, 3, 4, 5\}$ and G the permutation group

$$\{(1), (1\ 2\ 3), (1\ 3\ 2), (4\ 5), (1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\}.$$

We have $G_1 = \{(1), (4\ 5)\}$, so

$$|\mathcal{O}_1| = 3 = \frac{6}{2} = \frac{|G|}{G_1} = [G : G_1].$$

Similarly, $G_4 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$, so

$$|\mathcal{O}_4| = 2 = \frac{6}{3} = \frac{|G|}{G_4} = [G : G_4].$$

2. The Class Equation

The Orbit-Stabilizer Theorem gives rise to the *class equation* that we will see shortly. This equation has many applications. The first one that we will see is that every group of order p^2 is abelian.

Let X be a finite G-set. The set of fixed points in X is $X_G := \{x \in X : gx = x \text{ for all } g \in G\}$. Thus, for any $x \in X_G$, $\mathcal{O}_x = \{x\}$. Since the orbits of the action of G partition X, then

$$|X| = |X_G| + \sum_{i=1}^{k} |\mathcal{O}_{x_i}| \tag{1}$$

where $x_1, \ldots, x_k$ are representatives from distinct nontrivial orbits of X.

When G acts on itself by conjugation, then $X_G = \mathcal{Z}(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$, the center of G. The nontrivial orbits of G are called the conjugacy classes of G. If $x_1, \ldots, x_k$ are representatives from distinct nontrivial conjugacy classes G and $|\mathcal{O}_{x_i}| = n_i$, then by (1),

$$|G| = |\mathcal{Z}(G)| + n_1 + \cdots + n_k.$$

The stabilizer subgroup G_{x_i} is just the centralizer subgroup $C(x_i) = \{g \in G : gx_i = x_i g\}$ of x_i. Thus, by the Orbit-Stabilizer Theorem, we have the class equation:

$$|G| = |\mathcal{Z}(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)]. \tag{2}$$

Example. (1) If G is abelian, then $G = \mathcal{Z}(G)$. Hence, every conjugacy class has size 1.

(2) The center of D_4 is $\{(1), (1\ 3)(2\ 4)\}$, and the conjugacy classes are

$$\{(1\ 3), (2\ 4)\}, \quad \{(1\ 4\ 3\ 2), (1\ 2\ 3\ 4)\}, \quad \{(1\ 2)(3\ 4), (1\ 4)(2\ 3)\}.$$

(3) The conjugacy classes of $\mathcal{S}_3$ are $\{(1)\}$, $\{(1\ 2\ 3), (1\ 3\ 2)\}$, and $\{(1\ 2), (1\ 3), (2\ 3)\}$.

Example 4. We will show that the conjugacy classes of $\mathcal{S}_n$ are determined by cycle type.

First we show that if two cycles $\tau, \mu \in \mathcal{S}_n$ have the same length if and only if they are conjugate. Write $\tau = (a_0\ a_1\ \ldots\ a_{k-1})$ and $\mu = (b_0\ b_1\ \ldots\ b_{k-1})$. Let $\sigma \in \mathcal{S}_n$ be defined by $\sigma(a_i) = b_i$ for $i = 0, \ldots, k-1$ (and $\sigma(i) = i$ for $i \notin \{a_0, a_1, \ldots, a_{k-1}\}$). Then

$$\sigma\tau\sigma^{-1}(b_i) = \sigma\tau(a_i) = \sigma(a_{i+1 \bmod k}) = b_{i+1 \bmod k} = \mu(b_i).$$

Hence, $\mu = \sigma\tau\sigma^{-1}$.

On the other hand, let $\rho \in \mathcal{S}_n$. Set $\rho(a_i) = b$ and $\rho(a_{i+1 \bmod k}) = b'$ (note that $b \neq b'$ because ρ is injective). Then

$$\rho\tau\rho^{-1}(b) = \rho\tau(a_i) = \rho(a_{i+1 \bmod k}) = b'.$$

It follows that $\rho\tau\rho^{-1} = (\rho(a_0)\ \rho(a_1)\ \cdots\ \rho(a_{k-1}))$ and our claim is proved.

It is left as an exercise now to show that this extends to arbitrary permutations. Once shown, it follows that the number of conjugacy classes of $\mathcal{S}_n$ is equal to partitions of n.

Next we'll look at some consequences of the class equation.

Theorem 5. Let G be a group of order p^n where p is prime. Then G has a nontrivial center.

Proof. By the class equation (1), $|G| = |\mathcal{Z}(G)| + n_1 + \cdots + n_k$, where $n_i = |\mathcal{O}_{x_i}| > 1$. Since $n_i = [G : G_{x_i}]$, then $n_i \mid G$. Consequently, p divides each n_i. But $p \mid |G|$ and so $p \mid |\mathcal{Z}(G)|$. Since $|\mathcal{Z}(G)| \geq 1$, then $|\mathcal{Z}(G)| \geq p$. □

Corollary 6. Let G be a group of order p^2 where p is prime. Then G is abelian.

Proof. By the previous theorem and Lagrange's Theorem, $|\mathcal{Z}(G)| = p$ or p^2. If $|\mathcal{Z}(G)| = p^2$, then $\mathcal{Z}(G) = G$ and we are done. Suppose $|\mathcal{Z}(G)| = p$, then $|G/\mathcal{Z}(G)| = p$. Thus $G/\mathcal{Z}(G)$ is cyclic. By a homework exercise, G is abelian. □

The previous corollary gives us an alternate proof (along with the Fundamental Theorem of Finite Abelian Groups) that every group of order 4 is abelian and hence isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Similarly, every group of order 9 is isomorphic to $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Example. Let G be a group of order 8. Then $|\mathcal{Z}(G)| = 2, 4, 8$. If $|\mathcal{Z}(G)| = 8$, then clearly G is abelian. Moreover, if $|\mathcal{Z}(G)| = 4$, then since $\mathcal{Z}(G)$ is a normal subgroup of G, $G/\mathcal{Z}(G)$ is defined and $|G/\mathcal{Z}(G)| = 2$. Thus, $G/\mathcal{Z}(G)$ is cyclic and so G is abelian. Thus, if G is non-abelian, then we must have $\mathcal{Z}(G) = 2$.

3. The Sylow Theorems

The Sylow Theorems give us information on the existence of subgroups of prime (power) order, thereby allowing us to classify groups of small order.

Theorem 7 (Cauchy's Theorem)**.** Let G be a finite group and p a prime such that $p \mid |G|$. Then G contains a subgroup of order p.

Proof. Set $|G| = n \geq p$. By hypothesis, $p \mid n$. If $n = p$, then this theorem is trivial. We proceed inductively. Suppose the theorem holds for all groups of order k, $p \leq k < n$. By the class equation,

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

By Lagrange's Theorem, $|G| = |C(x_i)|[G : C(x_i)]$ for each i. Thus, for each i, either p divides $|C(x_i)|$ or it divides $[G : C(x_i)]$. If p divides some $C(x_i)$, then we are done by our inductive hypothesis since $|C(x_i)| < |G|$. Otherwise, p divides no $C(x_i)$ and so p divides each $[G : C(x_i)]$. Hence, p also divides $|\mathcal{Z}(G)|$ and so the result follows from the Fundamental Theorem of Finite Abelian Groups (since any subgroup of $\mathcal{Z}(G)$ is a subgroup of G). □

Corollary 8. Let G be a finite group. Then G is a p-group if and only if $|G| = p^n$.

Example. Consider A_4. Since $|A_4| = 12 = 2^2 \cdot 3$, then A_4 has subgroups of order 2 and 3. Note that the theorem does not tell us that A_4 has a subgroup of order 6 (it does not).

Example. Let G be a group of order 6. Clearly if G is cyclic, then $G \cong \mathbb{Z}_6$. Suppose G is not cylic. We will show that $G \cong D_3 (\cong S_3)$. By Cauchy's Theorem, G has (cyclic) subgroups of order 2 and 3. Let a be an element of order 3 and b an element of order 2. Note that $b \notin \langle a \rangle$. Thus, the elements of G are $\{e, a, a^2, b, ba, ba^2\}$[1]. Because G is not cyclic, then every element has order 2 or 3. It follows that ba and ba^2 have order 2. Thus, $e = (ba)^2 = baba$, so $bab = a^2 = a^{-1}$. Similarly, $ba^2b = a$. Define a map $\phi : D_3 \to G$ by $\phi(r) = a$ and $\phi(s) = b$.

Theorem 9 (First Sylow Theorem)**.** Let G be a finite group and p a prime such that p^r divides $|G|$. Then G contains a subgroup of order p^r.

Proof. Set $|G| = n \geq p$ and fix $r \in \mathbb{N}$. By hypothesis, $p \mid n$. If $n = p$, then this theorem is trivial. We proceed inductively. Suppose the theorem holds for all groups of order k, $p \leq k < n$. By the class equation,

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

By Lagrange's Theorem, $|G| = |C(x_i)|[G : C(x_i)]$ for each i. Thus, for each i, either p divides $|C(x_i)|$ or it divides $[G : C(x_i)]$. If p does not divide $[G : C(x_i)]$ for some i, then p^r divides $C(x_i)$. We may then apply the inductive hypothesis to $C(x_i)$ since $|C(x_i)| < |G|$.

[1] To see this, note that $ba \neq b$ (else $a = e$), $ba \neq a$ (else $b = e$) and $ba \neq a^2$ (else $b = e$). One can similarly show that ba^2 is a genuinely new element.

Otherwise, p divides each $[G : C(x_i)]$ and so p also divides $|\mathcal{Z}(G)|$. Because $\mathcal{Z}(G)$ is abelian it then contains an element of order p, say g. Let $N = \langle g \rangle$. Because N is a subgroup of $\mathcal{Z}(G)$, then N is normal in G. But then $|G/N| < n$ and so by the induction hypothesis, G/N has a subgroup H of order p^{r-1}. By the Correspondence Theorem, G then has a subgroup of order p^r. □

Definition 5. Let p be a prime, G and group, and H a subgroup. A Sylow p-subgroup of G is a maximal p-subgroup of G. Two Sylow p-subgroups P and Q are said to be conjugate if there exists $g \in G$ such that $gPg^{-1} = Q$. The set $N(H) = \{g \in G : gHg^{-1} = H\}$ is a subgroup of G called the normalizer of H in G.

Exercise. Let H be a subgroup of a group G. Show that $N(H)$ is a normal subgroup of G.

Lemma 10. Let P be a Sylow p-subgroup of a finite group G and let x have as its order a power of p. If $x^{-1}Px = P$, then $x \in P$.

Lemma 11. Let H and K be subgroups of G. The number of distinct H-conjugates of K is $[H : N(K) \cap H]$.

Theorem 12 (The Second Sylow Theorem)**.** Let G be a finite group and p a prime dividing $|G|$. Then all Sylow p-subgroups of G are conjugate. That is, if P_1 and P_2 are two Sylow p-subgroups, then there exists $g \in G$ such that $gP_1g^{-1} = P_2$.

Theorem 13 (Third Sylow Theorem)**.** Let G be a finite group and let p be a prime dividing the order of G. Then the number of Sylow p-subgroups is congruent to 1 mod p and divides $|G|$.

Corollary 14. A Sylow p-subgroup of a finite group G is a normal subgroup if and only if it is the only Sylow p-subgroup of G.

Example. Consider the Sylow 2-subgroups of $\mathcal{S}_3$. They are $P_1 = \{(1), (1\ 2)\}$, $P_2 = \{(1), (1\ 3)\}$, $P_3 = \{(1), (2\ 3)\}$. Note that $3 \equiv 1 \mod 2$. By the Third Sylow Theorem, these are all conjugate. Indeed, $(2\ 3)P_1(2\ 3) = P_2$ and $(1\ 3)P_1(1\ 3) = P_3$.

Corollary 15. Let G be a group of order pq with p and q prime, $p < q$. If $q \not\equiv 1 \mod p$, then G is cyclic. Otherwise, there are (up to isomorphism) exactly two groups of order pq, the cyclic group of order pq and a nonabelian group.

Proof. We will prove the first part. By Cauchy's Theorem, G has a subgroup K of order p and a subgroup H of order q. The number of conjugates of H divides pq and is equal to $1 + kq$ for some nonnegative integer k. Thus, $k = 0$ and so H is normal in G. Similarly, the number of conjugates of K divides pq and is equal to $1 + kp$ for some nonnegative integer k. Thus, $1 + kp = q$ or $1 + kp = 1$. Since $q \not\equiv 1 \mod p$, then $1 + kp = 1$ and K is also normal in G.

We claim that G is the internal direct product of H and K. Since both groups are cyclic of different prime orders, then $H \cap K = \{e\}$. Moreover, $G = HK$ since $|G| = |H||K|/|H \cap K|$. Write $H = \langle h \rangle$

and $K = \langle k \rangle$. It is sufficient to show that $hk = kh$. By normality, $hkh^{-1} \in K$ and so $hkh^{-1} = k^m$ for some positive integer m. Inductively one may show that $h^q k h^{-q} = (k^m)^q$ and so $k = (k^m)^q$. Thus, $(k^m)^q \equiv 1 \mod p$. It follows that m has order 1 or q in $U(p)$. If the order is q, then $q \mid (p-1)$, contradicting our assumption. Thus $m \equiv 1 \mod q$ and $hkh^{-1} = k^m = k$.

Thus, $G \cong K \times H \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. □

Example. (1) Any group of size 15 is cyclic.

(2) There are (up to isomorphism) two groups of order 6: $\mathbb{Z}_6$ and D_3.

(3) There are (up to isomorphism) two groups of order 10: $\mathbb{Z}_{10}$ and D_5.

Note that the quaternion group Q is the set $\{\pm 1, \pm i, \pm j, \pm k\}$ under multiplication. The element -1 acts as one would expect: $(-1)^2 = 1$, $(-1)i = -i$, etc. Additionally, we have the relations $i^2 = j^2 = k^2 = ijk = -1$.

Corollary 16. The groups D_4 and Q are the only non-abelian groups of order 8.

Proof. Let G be a non-abelian group of order 8. Then G has no element of order 8 (else G would be cyclic). By the First Sylow Theorem, G has a subgroup of order 4 and by an earlier exercise, this group is either cyclic or isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Also, G cannot have the property that every non-identity element is of order 2 (exercise). Hence, G contains an element a of order 4. Since $[G : \langle a \rangle] = 2$, then $\langle a \rangle$ is normal. Let $b \in G$ with $g \notin \langle a \rangle$. But then $b^2 \in \langle a \rangle$. It then follows that either $b^2 = a^2$ or $b^2 = e$ (exercise). By normality, $bab^{-1} \in \langle a \rangle$, and so $bab^{-1} = a^3 = a^{-1}$. Thus, every element of G has the form $b^i a^j$. The two possibilities are

- Q: $|a| = 4$, $b^2 = a^2$, $ba = a^{-1}b$.
- D_4: $|a| = 4$, $|b| = 2$, $ba = a^{-1}b$. □

4. Groups of order 12

The classification of groups of order 12 is a bit more involved, but it is do-able. The first step is to list groups we know.

There are two finite abelian groups of order 12: $\mathbb{Z}_{12}$ and $\mathbb{Z}_2 \times \mathbb{Z}_6$. The dihedral group D_6 has order 12, as does A_4. There is one more: a subgroup T of the direct product $\mathcal{S}_3 \times \mathbb{Z}_4$. This group T is generated by two elements, a and b, with the properties that $|a| = 6$, $a^3 = b^2$, and $ba = a^{-1}b$.

Exercise. Verify that T is indeed a group of order 12 (write out its Cayley Table). Show that D_6, A_4, and T are all nonisomorphic.

Lemma 17. Let H be a subgroup of G and let $\mathcal{L}_H$ be the set of left cosets of H in G. Then G acts on $\mathcal{L}_H$ by left translation. That is, for $g \in G$, there is a map $\tau_g : \mathcal{L}_H \to \mathcal{L}_H$ given by $xH \mapsto (gx)H$.

Proof. Fix $g \in G$. Suppose $xH = yH$ for some $xH, yH \in \mathcal{L}_H$. Then $y^{-1}x \in H$ so $y^{-1}xH = H$. Then τ_g is well-defined since

$$\tau_g(yH) = (gy)H = (gy)(y^{-1}x)H = (gx)H = \tau_g(xH).$$

Let $aH \in \mathcal{L}_H$. Then clearly, $\tau_e(aH) = (ea)H = aH$. Moreover, for $g_1, g_2 \in G$,

$$\tau_{g_1}(\tau_{g_2}(aH)) = \tau_{g_1}((g_2a)H) = (g_1(g_2a))H = ((g_1g_2)a)H = \tau_{g_1g_2}(aH). \qquad \square$$

Exercise. The set of such τ_g from the previous lemma form a group under function composition. In fact, this is just the group of permutations $\mathcal{S}(\mathcal{L}_H)$ of $\mathcal{L}_H$. Verify this and show that the group is isomorphic to S_n where $n = [G : H]$.

Lemma 18. Let H be a subgroup of G and let $\mathcal{L}_H$ be the set of left cosets of H in G. The map $\phi : G \to \mathcal{S}(\mathcal{L}_P)$ given by $g \mapsto \tau_g$ is a homomorphism and $\ker \phi \subset H$.

Proof. That ϕ is a homomorphism follows from the last computation in the previous lemma. Suppose $g \in \ker \phi$. Then $\phi(g) = \tau_e$ so $g(xH) = (gx)H = xH$ for all $xH \in \mathcal{L}_H$. Setting $x = e$ we get $gH = H$, so $g \in H$. $\square$

Theorem 19. Let G be a nonabelian group of order 12. Then G is isomorphic to exactly one of D_6, A_4, or T.

Proof. Let P be a Sylow 3-subgroup of G. Such a subgroup exists by Cauchy's Theorem. Then $|P| = 3$ and $[G : P] = 4$. By Lemma 18, there is a homomorphism $\phi : G \to \mathcal{S}(\mathcal{L}_P)$ given by $g \mapsto \tau_g$. and $K = \ker \phi \subset P$. Thus, $K = \langle e \rangle$ or $K = P$. If $K = \langle e \rangle$, then ϕ is injective and so G is isomorphic to a subgroup of $\mathcal{S}(\mathcal{L}_P) \cong \mathcal{S}_4$ order 12, whence K is isomorphic to A_4. (See remark after the theorem.)

Otherwise, $K = P$ and so P is normal in G. Consequently, P is the unique Sylow 3-subgroup of G. Therefore, G has exactly two elements of order 3. Call one of them c. Then $[G : C_G(c)] = 1$ or 2 since $[G : C_G(c)]$ is the number of conjugates of c and every conjugate of c has order 3. Hence, $C_G(c)$ is a group of order 12 or 6. In either case, by Cauchy's Theorem, there exists $d \in C_G(c) \subset G$ of order 2.

It is left as an exercise to show that $|cd| = 6$. Let $a = cd$. Then $[G : \langle a \rangle] = 2$ so $\langle a \rangle$ is normal in G. Hence, there is an element $b \in G$ such that $b \notin \langle a \rangle$, $b^2 \in \langle a \rangle$, and $bab^{-1} \in \langle a \rangle$. Since G is nonabelian and $|a| = 6$, we must have $bab^{-1} = a^5 = a^{-1}$. That is, $ba = a^{-1}b$. There are six possibilities for $b^2 \in \langle a \rangle$.

(1) $b^2 = e$: In this case we get $G \cong D_6$.
(2) $b^2 = a$: This implies $|b| = 12$ and so G is cyclic, whence abelian.
(3) $b^2 = a^2$: Using the above relations we get $bb^2b^{-1} = ba^2b^{-1}$, so $a^2 = b^2 = (bab^{-1})(bab^{-1}) = a^{-2}$, but this implies $a^4 = e$, a contradiction.
(4) $b^2 = a^3$: In this case we get $G \cong T$.
(5) $b^2 = a^4$: Similar to (3)
(6) $b^2 = a^5$: Similar to (2). □

Remark. To see that A_n is the *unique* subgroup of order $n/2$ in $\mathcal{S}_n$, one must show that A_n is generated by all the 3-cycles in $\mathcal{S}_n$ and that any subgroup of index 2 contains the 3-cycles.

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 1. 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 $a, b, c \in R$,

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

Example. The following are rings:

(1) $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ under addition and multiplication.
(2) $M_n(\mathbb{R})$ under matrix addition and matrix multiplication.
(3) $\mathbb{Z}_n$ under addition and multiplication mod n.

Example. Let $[a, b] \subset \mathbb{R}$ be an interval and denote by $\mathcal{C}([a, b])$ the set of continuous real-valued functions on $[a, b]$. We will show that $\mathcal{C}([a, b])$ is a function under pointwise addition and multiplication. That is, for $f, g \in \mathcal{C}([a, b])$ and $x \in [a, b]$,

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x).$$

Let $\mathcal{C} = \mathcal{C}([a, b])$. First we will show that $(\mathcal{C}, +)$ is an abelian group. The sum of two real numbers is a real number, so $+$ is a binary operation on $\mathcal{C}$. Let $f, g, h \in \mathcal{C}$ and $x \in [a, b]$, then by associativity of real numbers,

$$\begin{aligned}((f + g) + h)(x) &= (f + g)(x) + h(x) = (f(x) + g(x)) + h(x) \\ &= f(x) + (g(x) + h(x)) = f(x) + (g + h)(x) \\ &= (f + (g + h))(x).\end{aligned}$$

Thus, $(f + g) + h = f + (g + h)$ and so $+$ is associative. The identity element is the function e defined by $e(x) = 0$ and the inverse of $f \in \mathcal{C}$ is the function g defined by $g(x) = -f(x)$. Thus,

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: December 4, 2019

$(\mathcal{C}, +)$ is an abelian group. A similar computation as above shows that multiplication is associative. Let $f, g, h \in \mathcal{C}$ and $x \in [a, b]$, then

$$(f(g+h))(x) = f(x)(g+h)(x) = f(x)(g(x)+h(x)) = f(x)g(x) + f(x)h(x) = (fg+fh)(x).$$

Thus, $f(g+h) = fg + fh$ so the left distributive property holds. Multiplication of real numbers is commutative so the right distributive property also holds. Thus, $\mathcal{C}([a, b])$ is a ring.

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

Definition 2. 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.

Remark. The definition of a division ring is to says $(R\backslash\{0\}, \cdot)$ is a group.

Example. (1) $2\mathbb{Z}$ is a ring without unity.
(2) $\mathbb{Z}$ is an integral domain but not a field.
(3) $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are fields.
(4) $M_n(\mathbb{R})$ is not a domain.

Example. The ring $\mathbb{Z}_n$ is an integral domain if and only if n is prime. In particular, for a prime p, $\mathbb{Z}_p$ is a field.

Example. Recall the quaternions are the group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ under multiplication with identity element 1 satisfying $(-1)^2 = 1$, $i^2 = j^2 = k^2 = -1$, and

$$ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j.$$

Let $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, so $\mathbb{H}$ is a real vector space with basis $\{1, i, j, k\}$ Define addition and multiplication on $\mathbb{H}$ as follows. Let $a_1 + b_1 i + c_1 j + d_1 k, a_2 + b_2 i + c_2 j + d_2 k \in \mathbb{H}$, then

$$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

$$(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) = \alpha + \beta i + \gamma j + \delta k$$

where

$$\alpha = a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \qquad \beta = a_1b_2 + a_2b_1 + c_1d_2 - d_1c_2$$

$$\gamma = a_1c_2 - b_1d_2 + c_1a_2 - d_1b_2 \qquad \delta = a_1d_2 + b_1c_2 - c_1b_2 - d_1a_2.$$

Thus, $\mathbb{H}$ is a ring with identity. The multiplication operation is noncommutative (since $ij \neq ji$). One can now check that for $a + bi + cj + dk \neq 0$,

$$(a + bi + cj + dk)\left(\frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}\right) = 1.$$

Thus, $\mathbb{H}$ is a (noncommutative) division ring.

Warning. Because $(R, +)$ is assumed to be an (additive) abelian group, we denote the additive inverse of an element $a \in R$ by $(-a) = (-1)a$.

Proposition 1. Let R be a ring with $a, b \in R$. Then

(1) $a0 = 0a = 0$.
(2) $a(-b) = (-a)b = -(ab)$.
(3) $(-a)(-b) = ab$.

Proof. For (1), we have $a0 = a(0 + 0) = a0 + a0$, so $a0 = 0$. Now by (1) and the (left) distributive property, $ab + a(-b) = a(b - b) = a0 = 0$. Thus, $a(-b) = -(ab)$. Similarly $(-a)b = -(ab)$, proving (2). It now follows that $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, proving (3). □

Proposition 2. 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.

Proof. (1) is left as an exercise. For (2), let a^{-1} be an inverse of a and suppose $ba = 0$. Then $0 = (ba)a^{-1}b(aa^{-1}) = b$. Similarly, $ab = 0$ implies $b = 0$. Finally, for (3) suppose that b, c are multiplicative inverses of a. Then $ba = 1 = ca$, so $(b - c)a = 0$. Thus, by (2), $b - c = 0$, or $b = c$. □

Definition 3. 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 $s_1 - s_2 \in S$.

Proof. Let S be a nonempty subset of R and let $s_1, s_2 \in S$. By the subgroup test, $(S, +)$ is an abelian group if and only if $s_1 - s_2 \in S$. If S is a subring, then $s_1 s_2 \in S$ by closure. Conversely, if $s_1 s_2 \in S$, then multiplication is a binary operation with inherited associativity. □

Example. We already know that $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$. Clearly the product of two even numbers is even and hence $2\mathbb{Z}$ and so $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Example. Let T be the set of 2×2 real upper-triangular matrices, a subset of $M_2(\mathbb{R})$. Clearly, $I_2 \in T$ so $T \neq \emptyset$. Let $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in T$. Then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & c-c' \end{pmatrix} \in T$$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \in T.$$

Thus, T is a subring of $M_2(\mathbb{R})$.

Example. The Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ are a subring of $\mathbb{C}$.

2. Homomorphisms and ideals

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

Definition 4. A map $\phi : R \to S$ of rings is a (ring) homomorphism if

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

The image of ϕ is the set $\operatorname{im}\phi = \{\phi(a) : a \in R\}$ and the kernel of ϕ is the set $\ker\phi = \{x \in R : \phi(x) = 0_s\}$. An isomorphism (of rings) is a bijective homomorphism.

Example. The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(a) = a \mod n$ is a surjective homomorphism with $\ker\phi = n\mathbb{Z}$.

Example. Recall the ring $\mathcal{C}([a,b])$. For $\alpha \in [a,b]$, define the evaluation map by

$$\begin{aligned} \phi_\alpha : \mathcal{C}([a,b]) &\to \mathbb{R} \\ f &\mapsto f(\alpha). \end{aligned}$$

We claim this map is a ring homomorphism.

Let $f, g \in \mathcal{C}([a,b])$ and $\alpha \in [a,b]$. Then

$$\begin{aligned} \phi_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g), \\ \phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g). \end{aligned}$$

Proposition 4. 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.

Proof. (1) Let $x, y \in \phi(R)$. Then there exists $a, b \in R$ such that $\phi(a) = x$ and $\phi(b) = y$. Thus,

$$xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = yx,$$

so $\phi(R)$ is commutative.

(2) We have $\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R)$, so $\phi(0_R) = 0_S$.

(3) Assume ϕ is surjective. Then there exists $r \in R$ such that $\phi(r) = 1_s$. Then,

$$1_s = \phi(r) = \phi(1_R r) = \phi(1_R)\phi(r) = \phi(1_R)1_s = \phi(1_R).$$

(4) Homework exercise. □

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 5. 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. (1) Every ring R has two ideals: $\{0\}$ (called the trivial ideal) and R itself. An ideal I of R that is not one of these is called a proper ideal.

(2) We showed previously that $2\mathbb{Z}$ is a subring of $\mathbb{Z}$. If $r \in \mathbb{Z}$ and $x \in 2\mathbb{Z}$, then $rx = xr \in 2\mathbb{Z}$ because it is even, and so $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

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

Proof. First we show that $\langle a \rangle$ is a subring. Clearly $a \in \langle a \rangle$ so $\langle a \rangle \neq \emptyset$. If $x, y \in \langle a \rangle$, then $x = ar$ and $y = ar'$ for some $r, r' \in R$. Thus, $x - y = ar - ar' = a(r - r') \in \langle a \rangle$. Moreover, by associativity, $xy = (ar)(ar') = a(rar') \in \langle a \rangle$. Thus, $\langle a \rangle$ is a subring.

Now let $x = ar \in \langle a \rangle$ and $s \in R$. Then $xs = (ar)s = a(rs) \in \langle a \rangle$ and by commutativity, $sx = s(ar) = a(sr) \in \langle a \rangle$. Thus, $\langle a \rangle$ is an ideal. □

Definition 6. The set $\langle a \rangle$ in the previous proposition is called the principal ideal generated by a.

Theorem 7. Every ideal in $\mathbb{Z}$ is principal.

Proof. Since the trivial ideal is principal, assume I is a nontrivial ideal in $\mathbb{Z}$. The set $I \cap \mathbb{N} \subset \mathbb{N}$ is nonempty[1] and so has a least element n by the Well-Ordering Principle. We claim $I = \langle n \rangle = n\mathbb{Z}$. Clearly $n\mathbb{Z} \subset I$ so we need only show the opposite inclusion.

Let $a \in I$ be positive. By the division algorithm we have $a = nq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Then $r = a - nq \in I$, a contradiction unless $r = 0$, so $a \in \langle n \rangle$. If $b \in I$ is negative, then $-b \in \langle n \rangle$ by the above argument so $b = (-1)(-b) \in \langle n \rangle$. □

Theorem 8. Let $\phi : R \to S$ be a homomorphism of rings. Then $\ker \phi$ is an ideal of R.

Proof. Homework exercise. □

[1] If $x \in I$ is negative, then $-x = (-1)x \in I \cap \mathbb{N}$ because I is a subring and hence closed under taking additive inverses.

Warning. 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.

Theorem 9. Let I be an ideal of a ring R. The factor group R/I is a ring with multiplication defined by

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

Proof. We know that R/I is an abelian group under addition. It is only left to show that the multiplication operation is well-defined, that it is associative, and that the distributive properties hold. Let $r + I, s + I \in R/I$. Suppose $r + I = r' + I$ and $s + I = s' + I$ for some $r', s' \in R$. We will show that $r's' + I = rs + I$.

Our hypothesis implies that $r' \in r + I$ so $r' = r + a$ for some $a \in I$. Similarly, $s' = s + b$ for some $b \in I$. Then

$$r's' = (r + a)(s + b) = rs + rb + as + ab.$$

Since I is an ideal, $rb + as + ab \in I$, whence $r's' \in rs + I$. Thus, because cosets are either equal or disjoint, $r's' + I = rs + I$.

Checking associativity and the distributive properties are left as an exercise. □

Definition 7. Let I be an ideal of a ring R. The ring R/I is called the factor ring (or quotient ring) of R by I.

Theorem 10. Let I be an ideal of a ring R. The map $\phi : R \to r/I$ given by $r \mapsto r + I$ is a ring homomorphism of R onto R/I with kernel I.

Proof. It is clear that ϕ is a surjective group homomorphism. We need only show that it respects multiplication. Let $r, s \in R$. Then

$$\phi(r)\phi(s) = (r + I)(s + I) = rs + I = \phi(rs).$$ □

We are now ready to state the isomorphism theorems (for rings). The proofs, especially for the First Isomoprhism Theorem, are very similar to proofs of the corresponding group theorems. Their proofs are left as an exercise.

Theorem 11 (First Isomorphism Theorem (for rings))**.** Let $\phi : R \to S$ be a ring homomorphism. Then $R/\ker\phi \cong \phi(R)$.

Theorem 12 (Second Isomorphism Theorem (for rings))**.** 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

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

Theorem 13 (Third Isomorphism Theorem (for rings))**.** Let R be a ring with ideals $J \subset I$. Then

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

Polynomial rings

1. Polynomials

Throughout this section, R is a commutative ring with identity

Definition 1. 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 set of such polynomials is denoted $R[x]$.

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.

Let $p(x), q(x) \in R[x]$ be nonzero polynomials 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 $R[x]$. Suppose $n \geq m$ and set $b_i = 0$ for $i > m$. Then

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

This is similar if $m > n$. Now

$$p(x)q(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n},$$

where

$$c_i = \sum_{k=0}^{i} a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0.$$

Theorem 1. Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.

Proof. Above we showed that addition and multiplication are binary operations. It is easy to check that $(R[x], +)$ is an abelian group where the zero polynomial is the (additive) identity. The multiplicative identity is the constant polynomial 1. Associativity of multiplication and the distributive property are easy (albeit annoying) proofs. The details are left as an exercise. □

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: November 20, 2019

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 $\deg(q(x)) = 4$. Then

$$p(x) + q(x) = (3 + 2) + (0 + 0)x + (0 - 1)x^2 + (2 + 0)x^3 + (0 + 4)x^4 = 5 - x^2 + 2x^3 + 4x^4$$

and

$$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7.$$

Example. Let $p(x) = 3+3x^3$ and $q(x) = 4+4x^2+4x^4$ be polynomials in $\mathbb{Z}_{12}[x]$. Then $p(x)+q(x) = 7 + 4x^2 + 3x^3 + 4x^4$ and $p(x)q(x) = 0$.

Proposition 2. If R be an integral domain, then $R[x]$ is an integral domain.

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

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Then the leading term of $p(x)q(x)$ is $a_nb_mx^{n+m}$. By hypothesis, $a_n, b_m \neq 0$ and because R is an integral domain, $a_nb_m \neq 0$ so $p(x)q(x) \neq 0$. □

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 $\deg(0) = -\infty$.

So far we've discussed polynomials in one variable, but it is relatively straightforward, albeit very tedius, to define polynomials in two or more variables. By the above theorem, if R is a commutative ring with identity then so is $R[x]$. If y is another indeterminate, then it makes sense to define $(R[x])[y]$. One could then show that this ring is isomorphic to $(R[y])[x]$. 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 $R[x_1, \ldots, x_n]$.

Theorem 3. Let S be a commutative ring with identity and R a subring of S containing 1. Let $\alpha \in S$. If $p(x) = a_0 + a_1x + \cdots + a_nx^n$, then we define $p(\alpha)$ to be

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

Then there is a ring homomorphism $R[x] \to S$ given by $p(x) \mapsto p(\alpha)$.

Definition 2. The map in the previous theorem 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 4. Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $f(x), r(x) \in F(x)$ such that

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

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

Proof. For simplicity throughout we will write $f = f(x), g = g(x), etc.$ Set $\deg f = n$ and $\deg g = m$. If $n < m$, then let $q = 0$ and $r = f$. Note that this may happen if $f = 0$.

Now suppose $m \leq n$. Write

$$f = a_0 + a_1 x + \cdots + a_n x^n$$
$$g = b_0 + b_1 x + \cdots + b_m x^m.$$

Because $b_m \neq 0$ and F is a field, b_m^{-1} exists.

If $n = 0$, then $m = 0$ so $f = c_0$ and $g = b_0$. Set $q = a_0 b_0^{-1}$ and $r = 0$.

We proceed inductively. That is, assume the division algorithm holds when $\deg f < n$. Note that $f - a_n b_m^{-1} x^{n-m} g$ has degree strictly less than n. Hence, there exists q_0, r such that $f - a_n b_m^{-1} x^{n-m} g = q_0 g + r$ with $\deg r < \deg g$. This implies that

$$f = (q_0 + a_n b_m^{-1} x^{n-m}) g + r.$$

Setting $q = q_0 + a_n b_m^{-1} x^{n-m}$ completes the existence part of the proof.

For uniqueness, assume there exists $q, q', r, r' \in F[x]$ such that $f = qg + r = q'g + r'$ with $\deg r, \deg r' < \deg g$. Then $g(q - q') = r' - r$. If $q \neq q'$, then because $g \neq 0$ we have

$$\deg(r' - r) = \deg(g(q - q')) \geq \deg g.$$

This is a contradiction since both r' and r have degrees less than $\deg g$. Thus, $q = q'$ and so $r = r'$. □

Corollary 5. 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 (is a factor of) $p(x)$.

Proof. By the division algorithm, $p(x) = (x - \alpha)q(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $\deg r(x) < \deg(x - \alpha) = 1$. Applying the evaluation homomorphism we get $p(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha)$. If $x - \alpha$ divides $p(x)$, then $r(x) = 0$ so $p(\alpha) = 0$ and α is a root of $p(x)$. Conversely, if α is a root, then $r(\alpha) = 0$. But $\deg r < 1$ and since $r(x)$ cannot be a nonzero constant, then $r(x) = 0$. □

Corollary 6. Let F be a field. A nonzero polynomial $p(x) \in F[x]$ of degree n can have at most n distinct roots.

Proof. First note that a polynomial of degree 0 has no roots. Let $p(x) \in F[x]$ have degree n. If $n = 1$, then $p(x)$ has 1 root. We proceed by induction on $\deg p(x)$. Suppose all polynomials of degree m, $m \geq 1$, have at most m distinct roots. Let $\deg p(x) = m + 1$ and let α be a root of $p(x)$. By the previous corollary, $p(x) = (x - \alpha)q(x)$ for some $q(x)$ with $\deg q(x) = m$. Thus, m has at most m distinct roots and so $p(x)$ has at most $m + 1$ distinct roots. □

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

Corollary 7. Let F be a field. Every ideal in $F[x]$ is principal.

Proof. Let I be a nonzero ideal in $F[x]$. Set $S = \{\deg p(x) : p(x) \in I, p(x) \geq 0\}$. Since $I \neq 0$, then $S \neq \emptyset$ and $S \subset \mathbb{N}$. Thus, by the Well-Ordering Principal, S has a least element, d. Let $g(x) \in I$ be a polynomial of degree d. We claim $I = \langle g(x) \rangle$. It is clear that $\langle g(x) \rangle \subset I$ and so it is left only to prove the reverse inclusion.

Let $f(x) \in I$. If $\deg f(x) = d$, then either $f(x) = ag(x)$ for some $a \in F$ or else $\deg(f(x) - g(x)) < d$, a contradiction since $f(x) - g(x) \in I$. Now assume $\deg f(x) > d$. By the division algorithm, $f(x) = g(x)q(x) + r(x)$ for some $q(x), r(x) \in I$ with $\deg r(x) < \deg g(x)$. But then $r(x) = f(x) - g(x)q(x) \in I$. If $\deg r(x) \geq 0$, then this contradicts the minimality of d. Thus, $r(x) = 0$ and $f(x) \in \langle g(x) \rangle$ □

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

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

(3) $p(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3$. To see this, just note that $p(0) = 2$, $p(1) = 1$, and $p(2) = 2$, so $p(x)$ does not have a root in $\mathbb{Z}_3$.

Lemma 8. Let $p(x) \in \mathbb{Q}[x]$. Then

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n),$$

where $r, s, a_0, \ldots, a_n \in \mathbb{Z}$, the a_i relatively prime, and r, s relatively prime.

Proof. Write, $a_i = b_i/c_i$ with $b_i, c_i \in \mathbb{Z}$. Then

$$p(x) = \frac{1}{c_0 \cdots c_n}\left(d_0 + d_1 x + \cdots + d_n x^n\right),$$

where the d_i are integers. Set $d = \gcd\{d_0, \ldots, d_n\}$. Set $a_i = d_i d^{-1}$ and let $\frac{r}{s} = \frac{d}{c_0 \cdots c_n}$ written in lowest terms. The result follows. □

Theorem 9 (Gauss' Lemma)**.** If a non-constant monic polynomial $p(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$.

Proof. We will prove the contrapositive. Let $p(x) \in \mathbb{Z}[x]$ be a non-constant polynomial and suppose it factors over $\mathbb{Q}$. We will show that it factors over $\mathbb{Z}$.

Write $p(x) = \alpha(x)\beta(x)$ for some monic polynomials $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ with $\deg \alpha(x), \deg \beta(x) < \deg p(x)$. By the previous lemma,

$$\alpha(x) = \frac{c_1}{d_1}(a_0 + a_1 x + \cdots + a_m x^m) = \frac{c_1}{d_1}\alpha_1(x) \quad (a_m \neq 0),$$
$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1 x + \cdots + b_n x^n) = \frac{c_2}{d_2}\beta_1(x) \quad (b_n \neq 0),$$

where the a_i are relatively prime and the b_i are relatively prime. Then

$$p(x) = \frac{c_1 c_2}{d_1 d_2}\alpha_1(x)\beta_1(x).$$

Set $\frac{c}{d} = \frac{c_1 c_2}{d_1 d_2}$ expressed in lowest terms. Thus, $dp(x) = c\alpha_1(x)\beta_1(x)$. We now consider several cases.

Case 1: ($d = 1$) Because $p(x)$ is monic, then $ca_m b_n = 1$. As all three factors are integers, so then $c, a_m, b_n \in \{\pm 1\}$. Suppose $c = a_m = b_n = 1$, then $p(x) = \alpha_1(x)\beta_1(x)$ and this proves the claim. If $c = 1$ and $a_m = b_n = -1$, then $p(x) = (-\alpha_1(x))(-\beta_1(x))$. The remaining cases are left as an exercise.

Case 2: ($d \neq 1$) Since $\gcd(c, d) = 1$, there exists a prime p such that $p \mid d$ and $p \nmid c$. The coefficients of $\alpha_1(x)$ are relatively prime and so there exists a coefficient a_i of $\alpha_1(x)$ such that $p \nmid a_i$. Similarly, there exists a coefficient b_j of $\beta_1(x)$ such that $p \nmid b_j$. Let $\alpha_1'(x)$ and $\beta_1'(x)$ be the images of $\alpha_1(x)$ and $\beta_1(x)$ in $\mathbb{Z}_p[x]$. Since $p \mid d$, $\alpha_1'(x)\beta_1'(x) = 0$. But this is impossible since neither $\alpha_1'(x)$ or $\beta_1'(x)$ are the zero polynomial and $\mathbb{Z}_p[x]$ is an integral domain. Therefore, $d = 1$. □

Corollary 10. 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.

Proof. Let $p(x)$ have a zero $a \in \mathbb{Q}$. Then $p(x)$ has a linear factor $x - a \in \mathbb{Q}[x]$. By Gauss' Lemma, $p(x)$ has a factorization with a linear factor in $\mathbb{Z}[x]$. Hence, for some $\alpha \in ZZ$,

$$p(x) = (x - \alpha)(x^{n-1} + \cdots - a_0/\alpha).$$

Thus, $a_0/\alpha \in \mathbb{Z}$ and so $\alpha \mid a_0$. □

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

Case 1: Suppose $p(x)$ has a linear factor in $\mathbb{Q}[x]$, so $p(x) = (x-a)q(x)$ for some $q(x) \in \mathbb{Q}[x]$. Then $p(x)$ has a zero in $\mathbb{Z}$ (by Gauss' Lemma) and $\alpha \mid 1$ (by the corollary), so $\alpha = \pm 1$. But $p(1) = 1$ and $p(-1) = 3$, so $p(x)$ has no linear factors.

Case 2: Suppose $p(x)$ is the product of two (irreducible) quadratic factors. By Gauss's Lemma, $p(x)$ factors over $\mathbb{Z}[x]$ and so

$$p(x) = (x^2 + ax + b)(x^2 + cx + d)$$
$$x^4 - 2x^3 + x + 1 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.$$

where $a, b, c, d \in \mathbb{Z}$. Thus, $bd = 1$ so $b = d = \pm 1$. Then

$$1 = ad + bc = (a + c)b = -2b.$$

This implies $1 = \pm 2$, a contradiction. Hence, $p(x)$ is irreducible.

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

Theorem 11 (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 $\mathbb{Q}$.

Proof. If suffices by Gauss' Lemma to prove that $f(x)$ does not factor over $\mathbb{Z}[x]$. Let

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

be such a factorization with $b_r, c_s \neq 0$ and $r, s < n$. Since $p^2 \nmid a_0 = b_0 c_0$, either b_0 or c_0 is not divisible by p. Suppose $p \nmid b_0$ and $p \mid c_0$ (the other case is similar). Since $p \nmid a_n$ and $a_n = b_r c_s$, neither b_r nor c_s is divisible by p. Let m be the smallest value of k such that $p \nmid c_k$. Then

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$$

is not divisible by p since all but one of the terms $(b_0 c_m)$ is divisible by p. Therefore, $m = n$ since a_i is divisible by p for $m < n$. Hence, $f(x)$ cannot be factored and is therefore irreducible. $\square$

Example. Let $f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$ and set $p = 3$. Then clearly p divides all coefficients except for that of x^5 and $p^2 \nmid 21$. Thus, $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion.

Integral Domains

1. Localization

The intent of this section is to make formal the process of forming the rationals $\mathbb{Q}$ from the integers $\mathbb{Z}$. This process, known as localization, is applicable to a large class of rings. We will define $\mathbb{Q}(x)$, the ring of rational functions in one variable (over $\mathbb{Q}$), using this process. Another goal here is to extend notions of divisibility and factorization in $\mathbb{Z}$ to integral domains.

One can associate any rational number $p/q \in \mathbb{Q}$ with the ordered pair $(p, q) \in \mathbb{Z}\times\mathbb{Z}\backslash\{0\}$. This is not a bijection of sets, however, because $1/2 = 2/4$ but $(1, 2) \neq (2, 4)$. Thus, we place an equivalence relation on the latter set. Recall that $a/b = c/d$ if and only if $ad = bc$. Hence, we say $(a, b) \sim (c, d))$ if $ad = bc$.

Lemma 1. Let D be any integral domain and define the set

$$S = \{(a, b) : a, b \in D \text{ and } b \neq 0\}.$$

The relation $\sim$ on S given by $(a, b) \sim (c, d)$ if $ad = bc$ is an equivalence relation.

Proof. Let $(a, b) \in S$. Then $ab = ba$ because D is an integral domain (and hence commutative). Thus, $(a, b) \sim (a, b)$ and so $\sim$ is reflexive. Let $(a, b), (c, d) \in S$ such that $(a, b) \sim (c, d)$. Then $ad = bc$ and so $cb = da$ because D is an integral domain. Thus, $(c, d) \sim (a, b)$ and so $\sim$ is symmetric. Finally, suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ in S. Then $ad = bc$ and $cf = de$. Since D is an integral domain without zero divisors, then $ade = bce$ so $acf = bce$. Thus, $af = be$ so $(a, b) \sim (e, f)$ and $\sim$ is transitive. □

Let $[a, b]$ denote the equivalence class of $(a, b) \in S$ under $\sim$. The set of such equivalence classes is denoted F_D. We will prove that F_D is in fact a field, justifying the name *field of fractions* of D. The operations on F_D are defined to mimic the operations of adding and multiplying fractions. For $[a, b], [c, d] \in F_D$, define

$$[a, b] + [c, d] = [ad + bc, bd] \quad \text{and} \quad [a, b] \cdot [c, d] = [ac, bd].$$

Lemma 2. The operations of addition and multiplication above are binary operations on F_D.

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapter 18. Hungerford's *Algebra* was also consulted. Last Updated: December 6, 2019

Proof. That F_D is closed under these operations is clear. We need only show that they are well-defined (independent of equivalence class).

Let $[a_1, b_1], [a_2, b_2], [c_1, d_1], [c_2, d_2] \in F_D$ with $[a_1, b_1] = [a_2, b_2]$ and $[c_1, d_1] = [c_2, d_2]$. Thus, $a_1 b_2 = b_1 a_2$ and $c_1 d_2 = d_1 c_2$. We claim $[a_1, b_1] + [c_1, d_1] = [a_2, b_2] + [c_2, d_2]$. Equivalently,

$$[a_1 d_1 + b_1 c_1, b_1 d_1] = [a_2 d_2 + b_2 c_2, b_2 d_2]$$

or

$$(a_1 d_1 + b_1 c_1)(b_2 d_2) = (b_1 d_1)(a_2 d_2 + b_2 c_2).$$

We have

$$\begin{aligned}(a_1 d_1 + b_1 c_1)(b_2 d_2) &= (a_1 d_1)(b_2 d_2) + (b_1 c_1)(b_2 d_2) = (a_1 b_2)(d_1 d_2) + (b_1 b_2)(c_1 d_2) \\ &= (b_1 a_2)(d_1 d_2) + (b_1 b_2)(d_1 c_2) = (b_1 d_1)(a_2 d_2 + b_2 c_2).\end{aligned}$$

Checking the operation of multiplication is left as an (easier) exercise. □

Lemma 3. The set F_D with the above binary operations is a field.

Proof. We claim the additive identity is $[0, 1]$. Let $[a, b] \in F_D$, then

$$[a, b] + [0, 1] = [a \cdot 1 + b \cdot 0, b \cdot 1] = [a, b].$$

Associativity is left as an exercise. We claim the additive inverse of $[a, b]$ is $[-a, b]$ (note $-a \in D$ because D is a ring). One checks that $[a, b] + [-a, b] = [ab + b(-a), b^2] = [0, b^2] = [0, 1]$. (Note that this last equality follows because $0 \cdot 1 = b^2 \cdot 0$.) Thus, $(F_D, +)$ is an abelian group.

Associativity and commutivity of multiplication are left as an exercise. We check the left distributive property. Let $[a, b], [c, d], [e, f] \in F_D$. Then

$$\begin{aligned}[a, b][c, d] + [a, b][e, f] &= [ac, bd] + [ae, bf] = [acbf + bdae, bdbf] \\ &= [acf + dae, bdf] = [a, b][cf + de, df] = [a, b]([c, d] + [e, f]).\end{aligned}$$

By commutivity, the right distributive property also holds. Hence, F_D is a commutative ring.

The multiplicative identity in F_D is $[1, 1]$. This is an easy check: $[a, b][1, 1] = [a, b]$. Moreover, the multiplicative inverse of $[a, b]$ is $[b, a]$ as $[a, b][b, a] = [ab, ba] = [1, 1]$. Thus, F_D a field. □

Definition 1. The field F_D defined above is the field of fractions of D.

We next aim to show that, in some sense, F_D is the *smallest* field containing D.

Lemma 4. Let D be an integral domain and F_D its field of fractions. There is an injective homomorphism $\phi : D \to F_D$ defined by $\phi(a) = [a, 1]$.

Proof. Let $a, b \in D$, then

$$\phi(a) + \phi(b) = [a, 1] + [b, 1] = [a + b, 1] = \phi(a + b)$$
$$\phi(a)\phi(b) = [a, 1][b, 1] = [ab, 1] = \phi(ab).$$

Thus, ϕ is a ring homomorphism. Now suppose $\phi(a) = 0$, then $[a, 1] = [0, 1]$, so $a = 0$. Thus, $\ker \phi = \{0\}$ and ϕ is injective. □

As a consequence of this lemma, D is isomorphic to a subring of F_D. The next theorem is an example of a *universal property*.

Theorem 5. Let D be an integral domain and F_D its field of fractions. If E is any field containing D, then there exists a unique injective homomorphism $\psi : F_D \to E$ such that $\psi(\phi(a)) = a$ for all $a \in D$.

Proof. Let E be any field containing D. Define a map $\psi : F_d \to E$ by $[a, b] \mapsto ab^{-1}$. We must show that ψ is well-defined. Suppose $[a_1, b_1], [a_2, b_2] \in F_D$ with $[a_1, b_1] = [a_2, b_2]$. Then $a_1 b_2 = b_1 a_2$. Thus, in E, $a_1 b_1^{-1} = a_2 b_2^{-1}$ and so $\psi(a_1 b_1^{-1}) = \psi(a_2 b_2^{-1})$.

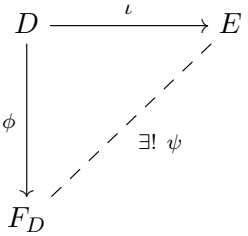
Now we claim ψ is an injective homomorphism. Let $[a, b], [c, d] \in F_D$. Then

$$\psi([a, b] + [c, d]) = \psi([ad + bc, bd]) = (ad + bc)(bd)^{-1} = ab^{-1} + cd^{-1} = \psi([a, b]) + \psi([c, d])$$
$$\psi([a, b][c, d]) = \psi([ac, bd]) = (ac)(bd)^{-1} = (ab^{-1})(cd^{-1}) = \psi([a, b])\psi([c, d]).$$

For injectivity, suppose $\psi([a, b]) = 0$. Then $ab^{-1} = 0$. Multiplying both sides by b gives $a = 0$. Thus, $[a, b] = [0, 1]$, the additive identity in F_D, so ψ is injective. Moreover,

$$\psi(\phi(a)) = \psi([a, 1]) = a1^{-1} = a.$$ □.

The previous theorem can be visualized using the following *commutative diagram* where ϕ and ψ are as in the theorem and ι is the inclusion map:



Remark. It is possible to localize in noncommutative rings but there are several technical hurdles.

Example. The field of fractions of $\mathbb{Q}[x]$, denoted $\mathbb{Q}(x)$, is the set of rational expressions $p(x)/q(x)$ for polynomials $p(x), q(x) \in \mathbb{Q}[x]$ with $q(x) \neq 0$.

2. Factorization

Definition 2. Let R be a commutative ring with identity and let $a, b \in R$. We say a divides b, denoted $a \mid b$, if there exists $c \in R$ such that $b = ac$. If there exists a unit $u \in R$ such that $b = au$, then a and b are said to be associates.

Example. (1) The elements 2 and -2 are associates in $\mathbb{Z}$. In fact, since the only units in $\mathbb{Z}$ are ± 1, then $a, b \in \mathbb{Z}$ are associates if and only if $a = \pm b$.

(2) The elements 2 and 1 are associates in $\mathbb{Q}$ since $1 = 2 \cdot (1/2)$. In fact, if $p, q \in \mathbb{Q}$ are nonzero, then $p = q \cdot (p/q)$ and so *any* two nonzero elements in $\mathbb{Q}$ are associates.

Definition 3. Let D be an integral domain. A nonzero element $p \in D$ that is not a unit is irreducible provided that whenever $p = ab$, either a or b is a unit. Furthermore, p is prime whenever $p \mid ab$ either $p \mid a$ or $p \mid b$.

Example. Let R be the subring of $\mathbb{Q}[x, y]$ generated by x^2, y^2, and xy. Then each element is irreducible in R, however xy is not prime because xy divides x^2y^2 but not x^2 or y^2.

Definition 4. An integral domain D is a unique factorization domain (UFD) if any nonzero, nonunit element $a \in D$ can be written as $a = p_1 \cdots p_k$ for irreducible elements $p_i \in D$ and if $a = q_1 \cdots q_\ell$ for irreducibles $q_j \in D$ then $k = \ell$ and, up to reordering p_i and q_i are associates for all i.

Example. (1) The integers are a UFD by the Fundamental Theorem of Arithmetic.

(2) The subring $\mathbb{Z}[i\sqrt{3}]$ of $\mathbb{C}$ is an integral domain (exercise) and the only units are ± 1 (also an exercise). The element $4 \in \mathbb{Z}[i\sqrt{3}]$ has two factorizations: $4 = 2 \cdot 2 = (1 - i\sqrt{3})(1 + i\sqrt{3})$. One can show that $2, 1 \pm i\sqrt{3}$ are irreducible. Hence $\mathbb{Z}[i\sqrt{3}]$ is not a UFD.

Lemma 6. Let D be an integral domain and let $a, b \in D$. Then

(1) $a \mid b$ if and only if $\langle b \rangle \subset \langle a \rangle$.
(2) a and b are associates if and only if $\langle b \rangle = \langle a \rangle$.
(3) a is a unit in D if and only if $\langle a \rangle = D$.

Proof. (1) We have $a \mid b$ if and only if there exists $x \in D$ such that $ax = b$ if and only if $b \in \langle a \rangle$ if and only if $\langle b \rangle \subset \langle a \rangle$.

(2) Suppose a and b are associates. Then there exists a unit $y \in D$ such that $b = ay$, thus $a \mid b$ and so $\langle b \rangle \subset \langle a \rangle$. Because y is a unit, $a = by^{-1}$ and so $\langle a \rangle \subset \langle b \rangle$. Thus, $\langle b \rangle = \langle a \rangle$. Conversely, suppose $\langle b \rangle = \langle a \rangle$. Then $a = bx$ and $b = ay$ for some $x, y \in D$. Thus, $a = bx = ayx$ so $yx = 1$ because D is an integral domain. It follows that x and y are units so a and b are associates.

(3) An element $a \in D$ is unit if and only if it is an associate of 1 if and only if $\langle a \rangle = \langle 1 \rangle = D$. □

We will now see how divisibility is related to the idea of maximal ideals.

Definition 5. A proper ideal M in a ring R is a maximal ideal of R if M is not a proper subset of any ideal of R except R itself.

Theorem 7. Let R be a commutative ring with identity and M an ideal in R. Then M is a maximal ideal of R if and only if R/M is a field.

Proof. Let M be a maximal ideal in R. Since R is commutative ring with identity, it follows that R/M is a commutative ring with identity $1 + M$. It suffices to prove that for all $a \in R$, $a \notin M$, $a + M$ has a multiplicative inverse.

Set $I = \{ra + m : r \in R, m \in M\}$. We claim I is an ideal in R. Since $0a + 0 = 0 \in I$, then $I \neq \emptyset$. Let $r_1a + m_1, r_2a + m_2 \in I$. Then

$$(r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in I$$

since M is an ideal. Let $r \in R$, then

$$r(r_1a + m_1) = (rr_1)a + (rm_1) \in I$$

again because M is an ideal. Thus, I is an ideal. Since $M \subset I$ and $M \neq I$, then $I = R$. Thus, there exists $m \in M$ and $b \in R$ such that $ba + m = 1$. Thus

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

Conversely, suppose R/M is a field, so R/M contains the elements $0 + M$ and $1 + M$. Hence, M is a proper ideal of R. Let I be an ideal properly containing M. We claim $I = R$. Let $a \in I \backslash M$. Since $a + M$ is a nonzero element in the field R/M, it has an inverse $b + M$ such that $(a + M)(b + M) = ab + M = 1 + M$. Thus, there exists an element $m \in M$ such that $ab + m = 1$ and so $1 \in I$. It follows that $I = R$. □

Definition 6. A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Example. We have already shown that $\mathbb{Z}$ and $F[x]$ (F a field) are PIDs.

Theorem 8. Let D be a PID and $\langle p \rangle$ a nonzero ideal in D. Then $\langle p \rangle$ is a maximal ideal if and only if p is irreducible.

Proof. Assume $\langle p \rangle$ is a maximal ideal and $a \in D$ divides p. Then $\langle p \rangle \subset \langle a \rangle$. By maximality, either $D = \langle a \rangle$ or $\langle p \rangle = \langle a \rangle$. In the first case, a is a unit. In the second, a and p are associatives. Thus, p is irreducible.

Assume p is irreducible and $\langle a \rangle$ an ideal such that $\langle p \rangle \subset \langle a \rangle \subset D$. Thus, $a \mid p$ and by irreducibility, either a is a unit or a and p are associates. It follows that either $D = \langle a \rangle$ or $\langle p \rangle = \langle a \rangle$. □

Definition 7. Let R be a commutative ring. An ideal P in R is a prime ideal if whenever $ab \in P$ for some elements $a, b \in R$, $a \in P$ or $b \in P$.

Note that R is always a prime ideal of itself.

Exercise. Let R be a commutative ring with identity. Prove that P is a prime ideal of R if and only if R/P is an integral domain. Conclude that every maximal ideal in a commutative ring with identity is also a prime ideal

Proposition 9. Let D be a PID and $p \in D$. If p is irreducible, then p is prime.

Proof. Let $p \in D$ be irreducible and suppose that $p \mid ab$. Then $\langle ab \rangle \subset \langle p \rangle$, so $ab \in \langle p \rangle$. Since $\langle p \rangle$ is maximal, it is prime and so $a \in \langle p \rangle$ or $b \in \langle p \rangle$. Thus, $p \mid a$ or $p \mid b$ and so p is prime. □

Definition 8. A collection of sets $\mathcal{A}$ is said to satisfy the ascending chain condition (ACC) if for all ascending chain of subsets $A_1 \subset A_2 \subset \cdots$ there exists an integer N such that $A_n = A_N$ for all $n \geq N$. A commutative R is said to be noetherian if it satisfies the ACC on ideals.

Lemma 10. A PID is noetherian.

Proof. Let $I_1 \subset I_2 \subset \cdots$ be an ascending chain of ideals in a PID D. Set $I = \bigcup_{k=1}^{\infty} I_k$. We claim I is an ideal.

Since $I_1 \subset I$, $I \neq \emptyset$. Let $a, b \in I$, then $a \in I_k$ and $b \in I_\ell$ for some $i, \ell \in \mathbb{N}$. WLOG, we may assume $k \leq \ell$. Thus, $a, b \in I_\ell$ so $a - b \in I_\ell \subset I$. Finally, let $a \in I$ and $r \in D$. Then as before, $a \in I_k$ for some $k \in \mathbb{N}$. Thus, $ra \in I_k \subset I$. It follows that I is an ideal.

Since D is a PID, then $I = \langle a \rangle$ for some $a \in I$. Since $a \in I_N$ for some $N \in \mathbb{N}$, then $I_N = I = \langle a \rangle$. Thus, $I_n = I_N$ for all $n \geq N$. □

Theorem 11. Every PID is a UFD.

Proof. Let D be a PID and $a \in D$ such that $a \neq 0$ and not a unit. If a is irreducible then there is nothing to prove, so we may assume $a = a_1 b_1$ for some non-units $a_1, b_1 \in D$. Hence, $\langle a \rangle \subset \langle a_1 \rangle$. This inclusion is proper because otherwise a and a_1 would be associates and b_1 a unit. Now either a_1 is irreducible or there exists non-units $a_2, b_2 \in D$ such that $a_1 = a_2 b_2$. Then $\langle a_1 \rangle \subset \langle a_2 \rangle$ and this inclusion is proper. This process continues to obtain an ascending chain of ideals

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$$

Because D is a PID, it is noetherian and so there exists a positive integer N such that $\langle a_n \rangle = \langle a_N \rangle$ for all $n \geq N$. Thus, a_N is irreducible.

Set $p_1 = a_N$, then $a = c_1 p_1$ for some $c_1 \in D$. If c_1 is not a unit, then we can repeat the above process to show that $c_1 = c_2 p_2$ for some $c_2, p_2 \in D$ such that p_2 is irreducible. Continuing in this way we obtain an ascending chain of ideals

$$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots$$

Again because D is noetherian, this chain stabilizes and therefore $a = p_1 p_2 \cdots p_r$ for some irreducible elements $p_1, \ldots, p_r$.

It is left to show that this factorization is unique (up to permutation of the factors). Suppose

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

for some irreducible elements p_i, q_i. WLOG, we may assume $r < s$. Since $p_1 \mid a$, $p_1 \mid q_1 q_2 \cdots q_s$. Thus, p_1 divides one of the q_i. After reordering, we may assume $p_1 \mid q_1$. Thus, $q_1 = u_1 p_1$ for some unit $u_1 \in D$. Therefore,

$$a = p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s.$$

Because D is an integral domain, we can cancel the p_1 to obtain

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

Continuing in this manner, we find,

$$1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s,$$

but this implies that $q_{r+1} \cdots q_s$ is a unit, contradicting the fact that the q_i are irreducible. Thus, $r = s$ and the factorization is unique. $\square$

3. Noetherian rings

Recall that a commutative ring is noetherian if it satisfies the ACC on ideals[1]. The noetherian property is an extremely important property in the study of rings. We will justify this statement, and then prove a fundamental result related to noetherian rings: The Hilbert Basis Theorem.

Definition 9. For X a nonempty subset of R, we denote by $\langle X \rangle$ the smallest ideal of R containing X. If I is an ideal of a ring R and $X \subset I$ such that $\langle X \rangle = I$, then we say I is generated by X. If $|X| < \infty$, then we say I is finitely generated.

This generalizes the notion of a principal ideal, that is, an ideal generated by one element.

Theorem 12. Let R be a commutative ring with identity. R is noetherian if and only if every ideal is finitely generated.

Proof. Suppose R is noetherian and let I be an ideal of R. If $I = 0$ or $I = R$, then this is trivial (since $R = \langle 1 \rangle$), so suppose I is a proper, nontrivial ideal. Then there exists $a_1 \in I$, $a_1 \neq 0$. If $I = \langle a_1 \rangle$, then we are done. Otherwise, choose $a_2 \in I \backslash \langle a_1 \rangle$, $a_2 \neq 0$. Continue in this way to obtain an ascending chain of ideals

$$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset \cdots$$

Since R is noetherian, there exists an N such that $\langle a_1, \ldots, a_n \rangle = \langle a_1, \ldots, a_N \rangle$ for all $n \geq N$. But this implies that $I \backslash \langle a_1, \ldots, a_N \rangle = \emptyset$, so $I = \langle a_1, \ldots, a_N \rangle$ and I is finitely generated.

Conversely, suppose R is not noetherian. Then there exists an infinitely ascending chain of ideals,

$$0 = I_0 \subset I_1 \subset I_2 \subset I_3 \subset \cdots$$

where each inclusion is proper. For each $k \geq 1$, we can choose an element $x_k \in I_k \backslash I_{k-1}$. It follows that the ideal $\langle x_1, x_2, x_3, \ldots \rangle$ is not finitely generated. □

Lemma 13. Let R be a commutative ring with identity and let J be an ideal of $R[x]$. The set L_n of leading coefficients of polynomial in J of degree at most n is an ideal of R.

Proof. Let $a, b \in L_n$. Then there exists polynomials $p(x), q(x) \in J$ of degree at most n with leading coefficients a and b, respectively. Since J is an ideal, $x^k p(x) \in J$ for all integers $k \geq 1$. Hence, we may assume that $p(x)$ has degree n and similarly for $q(x)$. Because J is an ideal, $p(x) - q(x) \in J$ with leading coefficient $a - b$. As $\deg(p(x) - q(x)) \leq n$, then $a - b \in L_n$. Now let $r \in R$. Since $r \in R[x]$ (as a constant polynomial), then $rp(x) \in J$ with leading coefficient ra. Since $\deg(rp(x)) \leq n$, then $ra \in L_n$. □

[1]For noncommutative rings there is a notion of *left noetherian* and *right noetherian* for the ACC on left ideals and right ideals, respectively. A noncommutative ring is called noetherian if it is simultaneously left and right noetherian

Theorem 14 (Hilbert Basis Theorem)**.** Let R be a commutative ring with identity. If R is noetherian, then $R[x]$ is noetherian.

Proof. Let J be a nonzero ideal of $R[x]$. We will show that J is finitely generated. For each $n \in \mathbb{N}$, define L_n to be the set of leading coefficients of polynomials in J of degree at most n. Then each L_n is an ideal of R and $L_n \subset L_{n+1}$ by Lemma 13. Thus, there exists $N \in \mathbb{N}$ such that $L_n = L_N$ for all $n \geq N$. Each L_n is finitely generated, say by $\{a_{n1}, \ldots, a_{nk}\}$. Then $L = L_N$ is finitely generated by the a_{ij}. For each n, choose $f_{ij} \in J$ of degree n with leading coefficient a_{ij}. Let I be the ideal in $R[x]$ (finitely) generated by the f_{ij} (so clearly $I \subset J$). We claim $I = J$.

Let $m \geq 0$ be the least (nonnegative) degree of a polynomial in J. If $p(x) \in J$ with $\deg p(x) = m$ and leading coefficient a. Then $a \in L_m$ and so there exist $r_1, \ldots, r_k \in R$ such that $r_1 a_{m1} + \cdots + r_k a_{mk} = a$. Thus, $p(x) - \sum r_i f_{mi} \in J$ and $\deg\left(p(x) - \sum r_i f_{mi}\right) < m$, contradicting the minimality of m *unless* $p(x) = \sum r_i f_{mi}$. That is, $p(x) \in I$.

We proceed by induction. Assume that for some degree $d \geq m$, all polynomials in J of degree less than d are in I. Let $q(x) \in J$ with $\deg(q) = d$ and leading coefficient b. We have two cases, though the difference between their proofs is subtle.

(Case 1:) If $d \leq N$, then we can proceed as above. We have that $b \in L_d$ and so there exist $s_1, \ldots, s_\ell \in R$ such that $s_1 a_{d1} + \cdots + s_\ell a_{d\ell} = b$. Note that the corresponding f_{di} will have degree e *at most* d, but by multiplying by x^{d-e} we may assume that all have degree d. Thus, $q(x) - \sum s_i f_{di}$ has degree less than d and so is an element of I by our inductive hypothesis. Since $\sum s_i f_{di} \in I$, then $q(x) \in I$.

(Case 2:) If $d \geq N$, then $b \in L$ and so it is generated by the a_{ij}. That is, there exists $r_{ij} \in R$ such that $b = \sum r_{ij} a_{ij}$. Again, the f_{ij} will have degree e *at most* N, but by multiplying by x^{d-e} we may assume they have degree d. Thus, $q - \sum s_i f_{di}$ has degree less than d and so is an element of I by our inductive hypothesis. Since $\sum s_i f_{di} \in I$, then $q \in I$. □