Chris Hayduk
Math A4900
Course Summary
10/27/2020

1. Introduction

Algebra has been a prominent field of study within mathematics for thousands of years. Its origins date back to the Babylonians of the 1st millennium BCE, who used formulas to solve problems which were typically solved geometrically in other civilizations of the time [5]. The algebraic concepts introduced in Babylonia continued to be developed in Greece, India, and the the Islamic world over the next two thousand years [5]. During the Renaissance, much interest was given to the solutions of polynomial equations, with general solutions found for quadratic, cubic, and quartic polynomials [2, 5]. However, solutions for quintic polynomials eluded mathematicians for centuries after this [2, 5].

This push towards a general solution for quintic polynomials culminated in significant developments from Neils Abel and Évariste Galois in the 19th century [2, 5]. After hundreds of years of searching for a general solution for quintic polynomials, in 1824 Abel showed that no such solution exists [2]. Meanwhile in France, Évariste Galois pushed this result even further, developing what we now know as Galois Theory in order to answer the question: which polynomials of degree 5 or higher have solutions? [2]. His results were published in 1847, 15 years after his untimely death, and represented a significant departure from the work of previous algebraists. While previous scholars viewed algebra as the theory of equations, it began to become clear that algebra could be defined in a much more general sense [2, 5, 6]. Algebra gradually tended towards this more general, axiomatic approach until in 1930, Bartel van der Waerden published *Moderne algebra*. This two-volume book synthesized the advances in algebra over the past century and thus formed the basis for today's "modern algebra" [6]. Hence, this book demarcated the change in algebra "from the theory of equations to the theory of algebraic structures" [6].

With this historical context in mind, we now turn our attention to studying this theory of algebraic structures. We start by examining groups, an algebraic structure which forms the foundation of much of algebra [1, 2]. Our foray into algebraic structures begins by examining the properties that arise from groups and their axioms. We learn about subgroups, which allow us to characterize subsets of groups which retain the group structure [1, 2, 3]. We then move onto homorphisms and isomorphisms. These functions and their properties aid us in talking about similarities between groups [1]. In particular, homomorphisms allow us to describe the notion of quotient groups, which describes the group that is yielded when dividing a group by one of its normal subgroups [1, 3]. We then examine group actions, in which we allow a group to act on a set [1]. The properties of the set and the action on this set can inform us of the group's properties, and this forms a fundamental part of Galois Theory [1]. Lastly, we switch gears to rings, which provide an extension of the material we learn about in regards to groups.

2. Topics

2.1. **Groups.** As mentioned in our introduction, groups are foundational to the modern study of algebra [1, 6]. Groups are a quite general notion of an algebraic structure, consisting simply of a set with a binary operation on this set [7]. Informally, a group consists of a set of elements and a method for combining those elements into new elements contained within the set [2, 3]. We can visualize the concept of a basic group using a Rubik's cube, as shown in *Visual Group Theory* [3, §1.1, p. 4]:

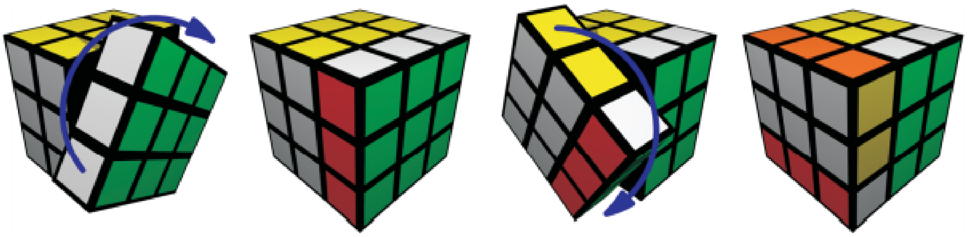
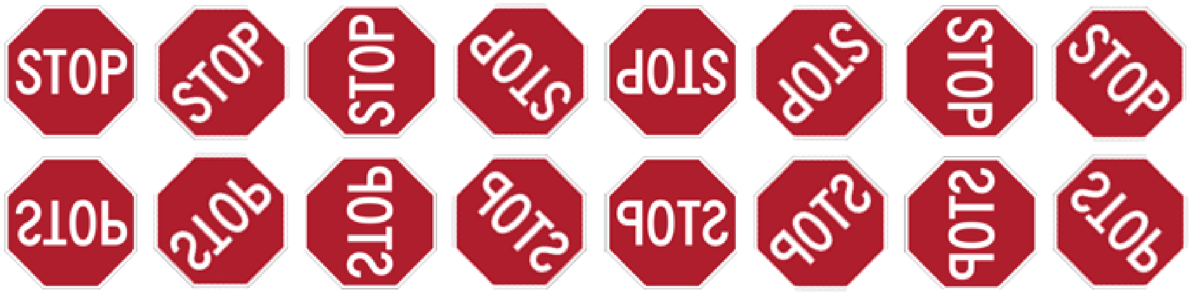


Figure 1.2. The leftmost cube shows the green face rotating 90 degrees clockwise; the next cube shows the result of that move. The third cube shows the white face rotating 90 degrees clockwise; the final cube shows the result of that move.

The cube provides a set of elements, namely any possible move that we can apply to the Rubik's cube. In addition, we see that we can combine actions in order to yield a new possible action within the set. For example, two 90° rotations of a particular face will yield a 180° rotation of that face. Moreover, the reverse rotation can be made so that we return to the original cube configuration [3]. Hence, we see that we can combine moves to form new, valid moves and that each valid move has a reverse move on the cube. This provides an intuitive notion of a group and its structure.

Another clear and intuitive example of a group structure is given by the dihedral group, which describes the rotations and reflections of a regular polygon [1, 11]. We can see a visual example of the D_8, the dihedral group on a polygon with 8 sides, by looking at the rotations and reflections of a stop sign [11]:



Each rotation and reflection changes the configuration of our stop sign, and we can combine these rotations and reflections in order to yield even more new configurations. In total, we have that there are 16 unique moves that we can on the stop sign make by taking any possible sequence of rotations and reflections [11].

Now that we have an intuitive sense of what groups are and how they work, let us formally define what a group is [1, §1.1, p. 16]:

Definition

(1) A *group* is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:

  (i) $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$, i.e. $*$ is *associative*

  (ii) there exists an element e in G called an *identity* of G, such that for all $a \in G$, we have $a * e = e * a = a$

  (iii) for each $a \in G$ there is an element a^{-1} of G called an *inverse* of a such that $a * a^{-1} = a^{-1} * a = e$

(2) The group $(G, *)$ is called *abelian* (or *commutative*) if $a * b = b * a$ for all $a, b \in G$.

(1) in the above definition provides a formalization of the intuitive notion of groups that we introduced with the Rubik's cube and dihedral groups. We see that grouping of operations on elements does not matter due to associativity. In addition, we have that there must exist an identity element in the group. In the case of the Rubik's cube, we can consider the identity element as not rotating any of the faces. Equivalently, rotating a specific face 4 times (or some multiple of 4) will result in the same configuration. Lastly, we have that every element must have an inverse. As we just discussed, in the Rubik's cube example, if we rotate any face a multiple of 4 times, we end up the identity element. Hence, any rotation of a face has an inverse element represented by the number of additional rotations needed in order to reach a multiple of 4 [3].

(2) in the above definition introduces a new notion – that of an abelian group. This type of group satisfies all of the axioms of definition (1), with the addition that the binary operation defined on the group's elements must also be commutative. That is, performing action a then action b is equivalent to performing action b then action a.

Now equipped with this formal notion of groups, let us now discuss some of the properties of groups [1, §1.1, p. 18]:

Proposition 1. If G is a group under the operation $*$, then

(1) the identity of G is unique

(2) for each $a \in G$, a^{-1} is uniquely determined

(3) $(a^{-1})^{-1} = a$ for all $a \in G$

(4) $(a * b)^{-1} = (b^{-1}) * (a^{-1})$

(5) for any $a_1, a_2, \cdots, a_n \in G$, the value of $a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed (this is called the *generalized associative law.*

This proposition gives us quite a bit of machinery to work with in regards to groups. We now have the ability to assert that both the identity element and all inverse are unique. In addition, we can take inverse of inverses, as well as inverses of the combination of two elements. Lastly, we can extend associativity to any finite combination of elements in G. Note that operations on elements of groups are often written without the $*$. Hence, in many definitions and theorems from now on, we may see ab instead of $a * b$. In addition, in additive groups, note that ab is meant to denote $a + b$.

In some of our above discussion on groups, we noted that multiple applications of the same element in a group can yield the identity element. For example, 4 rotations of a particular face of the Rubik's cube gives us the original configuration for the cube. This notion of repeatedly applying an element of the group yielding the identity can be captured by the definition of the "order" of an element [1, §1.1, p. 20]:

Definition For G a group and $x \in G$, define the *order* of x to be the smallest positive integer n such that $x^n = 1$ (where $1 = e$ from our earlier discussions), and the denote this integer by $|x|$. In this case, x is said to be of order n. If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

Note that $|x|$ represents the smallest positive integer such that $x^n = 1$, while $|G|$ denotes the number of unique elements contained in G. This definition of the order of elements leads us naturally into a discussion of cyclic groups. These types of groups can be thought of as being constructed out of a single element and its "iterates". That is, if G is a cyclic group, then there exists an element $x \in G$ such that every element $y \in G$ can be written as $x^k = y$ for some $k \in \mathbb{N}_0$. This is described formally as follows [1, §2.3, p. 54]:

Definition A group H is cyclic if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where as usual the operation is multiplication)

In this case, we can write $H = \langle x \rangle$ and say that "H is generated by x". As an example of a cyclic group, let us consider $\mathbb{Z}/3\mathbb{Z}$ (that is, the integers modulo 3). The elements of this group are $\bar{0}, \bar{1}, \bar{2}$. Observe that, if we iteratively add $\bar{1}$, we get the following results,

$$\begin{aligned} \bar{1} &= \bar{1} \\ \bar{1} + \bar{1} &= \bar{2} \\ \bar{1} + \bar{1} + \bar{1} &= \bar{3} = \bar{0} \end{aligned}$$

From the above derivation, we have that $\mathbb{Z}/3\mathbb{Z} = \langle \bar{1} \rangle$. Hence, $\mathbb{Z}/3\mathbb{Z}$ is a cyclic group generated by $\bar{1}$. Now let us discuss some of the properties that these cyclic groups have [1, §2.3, p. 55]:

Proposition 2. If $H = \langle x \rangle$, the $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically

(1) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \cdots, x^{n-1}$ are all distinct elements of H

(2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$

Hence, in the case where $|H|$ is finite, we have that every power of x with the exponents in different equivalence classes of $\mathbb{Z}/n\mathbb{Z}$ are distinct. In the case where $|H|$ is infinite, every power of x is distinct.

In addition, this discussion of cyclic groups and the order of elements leads to the following conclusions [1, §2.3, p.57]:

Proposition 5. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

(1) If $|x| = \infty$, then $|x^a| = \infty$

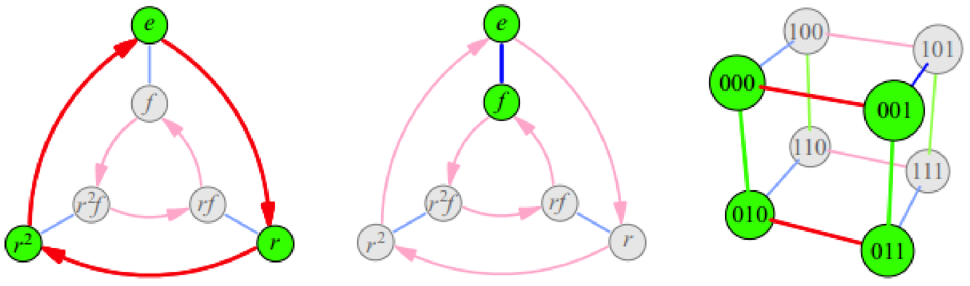
(2) If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$

(3) In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$

Hence, Proposition 5 tells us that we can use the order of an element x in order to reason about the orders of the powers of x.

2.2. **Subgroups.** Let us now shift our focus to subgroups. Consider a subset S of a group G with operation $*$. It may be true that S is closed under multiplication, closed under inverses, and contains the identity element. That is, for any $a, b \in S$, we have $a * b \in S$, $a^{-1}, b^{-1} \in S$, and $1 \in S$ [2]. If this is the case, we say that S is a *subgroup* of G. An example of such a structure would be the even integers under addition (i.e. $(2\mathbb{Z}, +)$), which is contained within the integers under addition (i.e. $(\mathbb{Z}, +)$). Note that in order to talk about a subgroup of another group, it must be a subset of the group *and* have the same operation as the group.

We can examine a visual representation of this subgroup structure using Cayley diagrams [3, §6.2, p. 100]:



A copy of C_3 in the group S_3

A copy of C_2 in the group S_3

A copy of V_4 in the group $C_2 \times C_2 \times C_2$

Figure 6.3. Three Cayley diagrams highlighting easy-to-spot subgroups.

As shown in the image above, a subgroup is a subset of a group which retains a group structure under the same operation. For example, in the example on the left, we see a subset of the dihedral group (in this notation it is called S_3, whereas in Dummit & Foote it would be denoted as D_6). We see that this subset of D_6 includes the elements generated by rotations of the polygon. Hence, we can see that this subset is closed under multiplication since $rr^2 = e = r^2r$, $rr = r^2$, $er = r = re$, and $r^2e = r^2 = er^2$. Lastly, we also have $ee = e$. In addition, we have shown that this subset is closed under inverses: $r = r^{2^{-1}}$, $r^2 = r^{-1}$, and $e = e^{-1}$. And finally, we see that e, the identity element, is contained in this subset. Thus, we can see that sometime of group structure has been retained here. Let us make this notion formal through the following definition [1, §2.1, p. 46]:

Definition Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses (i.e. $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leqslant G$.

Note that $e \in H$ was not included here because it follows directly from the facts that H is nonempty, closed under inverses, and closed under products. Since H is nonempty, we have some element $a \in H$. Since H is closed under inverses, we have $a^{-1} \in H$. And since H is closed under products, we have $aa^{-1} = e \in H$ as required.

Just as we condensed the subgroup criteria by removing the statement requiring the existence of e in the group (since its existence is implied by the other properties), we can actually further condense the conditions that we need to check. In particular, we get the following proposition [1, §2.1, p. 47]:

Proposition 1. (*The Subgroup Criterion*) A subset H of a group G is a subgroup if and only if

(1) $H \neq \varnothing$

(2) for all $x, y \in H$, $xy^{-1} \in H$

Furthermore, if H is finite then it suffices to check that H is nonempty and closed under multiplication.

Hence, we can now show that a subset of a group G is a subgroup if it satisfies just two properties – it is nonempty and for every elements x, y in the subset, we have xy^{-1} in the subset as well.

Now let us consider some specific families of subgroups [**?**, §2.2, p. 49-50]dummit:

Definitions:

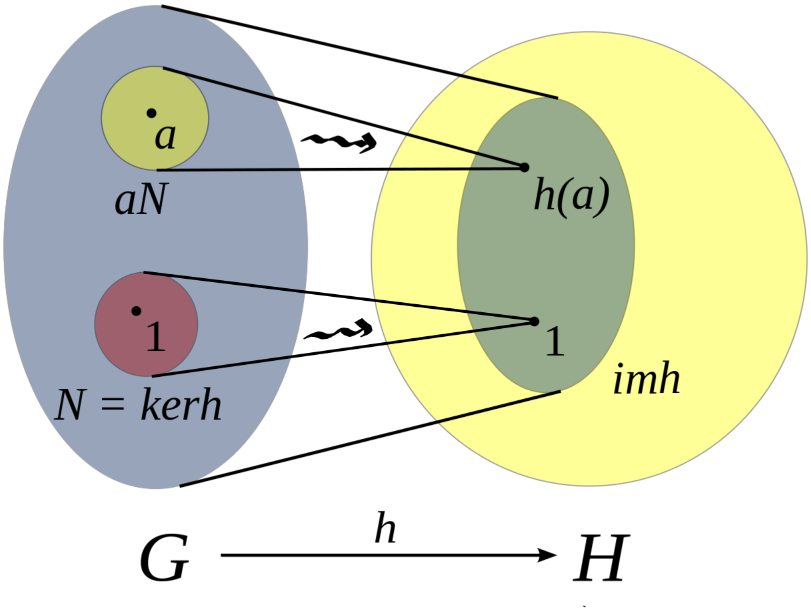
(1) Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A

(2) Define $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G. This subset of G is called the *center* of G

(3) Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$

These special subgroups will be quite important throughout our discussions of homomorphisms and quotient groups.

2.3. **Homomorphisms & Isomorphisms.** Now we turn our attention to functions between groups. We first start with homomorphisms, which describes a function from one group to another which maintains a portion of the group structure in some sense. The following image gives us an intuitive sense of what a homomorphism between groups can look like [9]:



As we can see, the above homomorphism maps elements of G into elements of H. However, note that the image of the homomorphism h in H is a proper subset of H. That is, there are elements in H which h does not map any element of G to. In addition, note that every element of G in the circle around a maps to $h(a)$ in H. In other words, multiple elements of G can map to a single element of H under a homomorphism h. These will be the key differences between homomorphisms and isomorphisms when we turn to defining these concepts rigorously.. We will give the following definition for a homomorphism [**?**, §1.6, p. 36]dummit:

Definition Let $(G, *)$ and $(H, \diamond)$ be groups. A map $\varphi : G \to H$ such that

$$\varphi(x * y) = \varphi(x) \diamond \varphi(y)$$

is called a *homomorphism*. We will usually omit the operation signs and write $\varphi(xy) = \varphi(x)\varphi(y)$, but remember that the operation on the left of the equation is not necessarily the same operation on the right of the equation.

Hence, we can see that a homomorphism preserves the group operation in some sense – the image of the product of x and y is the same as the product of the images of x and y. Isomorphisms extend this group preservation in the following way [1, §1.6, p. 37]:

Definition The map $\varphi : G \to H$ is called an *isomorphism* and G and H are said to be *isomorphic* or of the same *isomorphism* type, written $G \cong H$, if

(1) φ is a homomorphism (i.e. $\varphi(xy) = \varphi(x)\varphi(y)$), and

(2) φ is a bijection

Thus, the homomorphism part of this definition ensures that the group operation is preserved (in the sense defined above), and the bijection part of the definition ensures that the groups G and H are the same size. Hence, two isomorphic groups can in some sense be considered the "same" group, just with potentially different names for the elements and operation.

As we transition towards quotient groups, we must first discuss *fibers* of homomorphisms. Let $\varphi : G \to H$ be a homomorphism and let $a \in H$. The *fiber* of φ over a is the set of elements in G which φ maps to a. Hence, the kernel of φ over a is the same notion as the pre-image of a under φ. We pay special attention to the fiber of φ over 1 (i.e. the identity element of H), which we call the *kernel* of φ. We can define this formally as follows [1, §3.1, p. 75]:

Definition If φ is a homomorphism $\varphi : G \to H$, the *kernel* of φ is the set

$$\{g \in G \mid \varphi(g) = 1\}$$

and will be denoted by $\ker \varphi$ (here 1 is the identity of H).

Equipped with this definition of the kernel of a homomorphism, we can now assert the following properties for a homomorphism [1, §3.1, 75]:

Proposition 1. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

(1) $\varphi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H, respectively

(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$

(3) $\varphi(g^n) = \varphi(g)^n$ for all $n \in \mathbb{Z}$

(4) $\ker \varphi$ is a subgroup of G

(5) $\operatorname{im}(\varphi)$, the image of G under φ, is a subgroup of H

2.4. **Quotient Groups.** Quotient groups extend the notion of division to groups. We can think about "dividing" a group into smaller groups and studying the relations between elements in this smaller group. We can see this notion visually in the following diagram [3, §7.3, p. 133]:

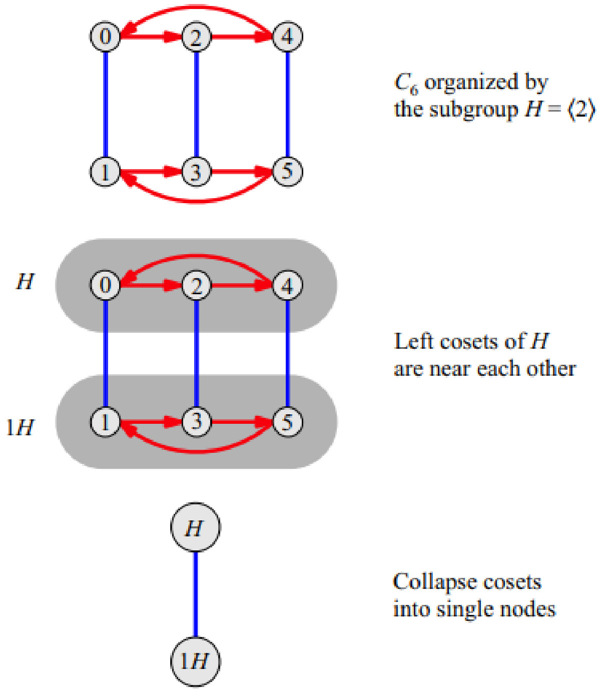


Figure 7.20. Application of the quotient process of Definition 7.5 to the group $G = C_6$ and subgroup $H = \langle 2 \rangle$, isomorphic to C_3. Notice that organizing the Cayley diagram of G by the subgroup H facilitates collapsing of the cosets of H.

We can see that G is first divided up into two groups (called "left cosets", which we will discuss soon). Then, all elements contained within each coset are collapse into a single element. Lastly, we preserve the relationship between these two subgroups of G. Hidden within this intuitive sense of quotient groups is the fact that studying quotient groups and homomorphisms is actually equivalent [1, 10]. We will see why in the following discussions,

Definition Let $\varphi : G \to H$ be a homomorphism with kernel K. The *quotient group* or *factor group*, G/K (read G *modulo* K or simply G *mod* K), is the group whose elements are the fibers of φ with group operation defined above: namely if X is the fiber above a and Y is the fiber above b then the product of X with Y is defined to be the fiber above the product ab.

Hence, the group G is divided into smaller subgroups (namely, the fibers of φ) by the kernel of φ. This connection between the kernel of φ and its fibers over other elements will be captured by our work with cosets. Let us first define what a coset is [1, §3.1, p. 77]:

Definition For any $N \leqslant G$ and any $g \in G$ let

$$gN = \{gn \mid n \in N\} \quad \text{and} \quad Ng = \{ng \mid n \in N\}$$

called respectively a *left coset* and a *right coset* of N in G. Any element of a coset is called a *representative* for the coset.

The relationship between this definition and the kernel of φ is given by the following theorem [1, §3.1, p. 77]:

Theorem 3. Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with operation defined by

$$uK \circ vK = (uv)K$$

forms a group, G/K. In particular, this operation is well defined in the sense that if u_1 is any element in uK and v_1 is any element in vK, then $u_1v_1 \in uvK$, i.e., $u_1v_1K = uvK$ so that the multiplication does not depend on the choice of representatives for the cosets. The same statement is true with "right cosets" in place of "left cosets".

Hence, we can see from this theorem that the set of left cosets of K is equivalent to the group G/K. We know that G/K is the group whose elements are the fibers of φ, and so we must have that the left cosets of K are equivalent to the fibers of φ. Hence, we see that we can actually ignore the fibers of φ other than the kernel K and simply take left cosets of K in order to obtain the other fibers.

2.5. **More on Isomorphisms.** In this section, we detail some important theorems relating quotient groups and homomorphisms. These theorems are known as "The Isomorphism Theorems" and are central to the discussion of this section. The First Isomorphism Theorem is given by the following [1, §3.3, p. 97]:

The First Isomorphism Theorem. If $\varphi : G \to H$ is a homomorphism of groups, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.

The First Isomorphism Theorem allows us to assert that the kernel of a group homomorphism is a normal subgroup of the domain. This gives us the ability to discuss the quotient group $G/\ker\varphi$, which we assert is congruent to the image of the domain under φ. The second isomorphism theorem is given by the following [1, §3.3, p. 97]:

The Diamond Isomorphism Theorem. Let G be a group, let A and B be subgroups of G and assume $A \leqslant N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $AB/B \cong A/A \cap B$.

This is called The Diamond Isomorphism Theorem due to the section of the lattice of subgroups of G that is considered. The final two isomorphism theorems are given as follows [1, §3.3, p. 98-99]:

The Third Isomorphism Theorem. Let G be a group and let H and K be normal subgroups of G with $H \leqslant K$. Then $K/H \trianglelefteq G/H$ and

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

If we denote the quotient by H with a bar, this can be written

$$\overline{G}/\overline{K} \cong G/K$$

The Lattice Isomorphism Theorem. Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leqslant G$ with $N \leqslant A$ and $N \leqslant B$.

(1) $A \leqslant B$ if and only if $\overline{A} \leqslant \overline{B}$

(2) if $A \leqslant B$, then $|B : A| = |\overline{B} : \overline{A}|$

(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$

(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$

The Third Isomorphism Theorem examines taking quotients of quotient groups, while The Lattice Isomorphism Theorem looks at the relationship between the lattice of subgroups of a quotient group (e.g. G/N) and the lattice of subgroups of the underlying group (e.g. G).

2.6. **Group Actions.** As discussed in the introduction, group actions are when groups act upon sets. We define them as follows [1, §1.7, p. 41]:

Definition A *group action* of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G, a \in A$, and

(2) $1 \cdot a = a$ for all $a \in A$

We can extend these discussions of group actions using the language of homomorphisms as follows [1, §4.1, p. 112]:

Definition

(1) The *kernel* of the action is the set of elements of G that act trivially on every element of A: $\{g \in G \mid |g \cdot a = a \text{ for all } a \in A\}$

(2) For each $a \in A$, the *stabilizer* of a in G is the set of elements of G that fix the element a: $\{g \in G \mid g \cdot a = a\}$ and is denoted by G_a

(3) An action is *faithful* if its kernel is the identity

2.7. **Direct and Semidirect Products.** Quotient groups allowed us to construct smaller groups from larger groups by "removing" unnecessary information. In this section, we will instead look at how to create larger groups from smaller groups through the use of direct and semidirect products. We will start by defining direct products in both the finite and countable cases [1, §5.1, p. 152]:

Definition.

(1) The *direct product* $G_1 \times G_2 \times \cdots \times G_n$ of the groups $G_1, G_2, \ldots, G_n$ with operation $*_1, *_2, \ldots, *_n$, respectively, is the set of n-tuples $(g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$ with operation defined componentwise:

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n)$$

(2) Similarly, the *direct product* $G_1 \times G_2 \times \cdots$ of the groups $G_1, G_2, \ldots$ with operations $*_1, *_2, \ldots$, respectively, is the set of sequences $(g_1, g_2, \ldots)$ where $g_i \in G_i$ with operation defined componentwise:

$$(g_1, g_2, \ldots) * (h_1, h_2, \ldots) = (g_1 * h_1, g_2 * h_2, \ldots)$$

The direct product of a set of groups actually preserves the information from each of the component groups. In fact, we can recover this information from the direct product group. The next proposition makes this notion formal [1, §5.1, p. 154]:

Proposition 2. Let $G_1, G_2, \ldots, G_n$ be groups and let $G = G_1 \times \cdots \times G_n$ be their direct product.

(1) For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i:

$$G_i \cong \{(1, 1, \ldots, 1, g_i, 1, \ldots 1) \mid g_i \in G_i\},$$

(here g_i appears in the i^{th} position). If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

(2) For each fixed i define $\pi_i : G \to G_i$ by

$$\pi_i((g_1, g_2, \ldots, g_n)) = g_i$$

Then π_i is a surjective homomorphism with

$$\begin{aligned} \ker \pi_i &= \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) \mid g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$

We will now introduce the notion of a semidirect product, which generalizes direct products by relaxing the constraint that the constituent groups are normal. We start with the following theorem to set the stage [1, §5.5, p. 176]:

Theorem 10. Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. Let $\cdot$ denote the (left) action of K on H determined by φ. Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

(1) This multiplication makes G into a group of order $|G| = |H||K|$

(2) The sets $\{(h, 1) \mid h \in H\}$ and $\{(1, k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1)$ for $h \in H$ and $k \mapsto (1, k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively:

$$H \cong \{(h, 1) \mid h \in H\} \text{ and } K \cong \{(1, k) \mid k \in K\}$$

Identifying H and K with their isomorphic copies in G described in (2) we have

(3) $H \trianglelefteq G$

(4) $H \cap K = 1$

(5) for all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$

Equipped with this background information, we can now precisely define what a semidirect product is [1, §5.5, p. 177]:

Definition. Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. The group described in Theorem 10 is called the *semidirect product* of H and K with respect to φ and will be denoted by $H \rtimes_\varphi K$ (when there is no danger of confusion we shall simply write $H \rtimes K$).

The following proposition and theorem provide us with useful tools for working with semidirect products [1, §5.5, p. 177, 180]:

Proposition 11. Let H and K be groups and let $\varphi : K \to \text{Aut}(H)$ be a homomorphism. Then the following are equivalent:

(1) the identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism (hence an isomorphism)

(2) φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$

(3) $K \trianglelefteq H \rtimes K$

Theorem 12. Suppose G is a group with subgroups H and K such that

(1) $H \trianglelefteq G$

(2) $H \cap K = 1$

Let $\varphi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K.

2.8. **Rings.** We now extend our study of groups to a new algebraic structure: rings. Rings are a central theme throughout many fields of algebra which include many of the same notions that we studied in groups with a few key differences. Whereas groups consisted of a set with one binary operation, rings are a set with two binary operations. Moreover, these binary operations must interact with each other in some sense, otherwise we would consider them as two different groups. We can formalize this notion with the following definition [1, §7.1, p. 223]:

Definition.

(1) A *ring* R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

  (i) $(R, +)$ is an *abelian* group

  (ii) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$

  (iii) the *distributive laws* hold in R: for all $a, b, c \in R$

$$(a + b) \times c = (a \times c) + (b \times c) \text{ and } a \times (b + c) = (a \times b) + (a \times c)$$

(2) The ring R us *commutative* if multiplication is commutative.

(3) The ring R is said to have an *identity* (or *contain a* 1) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \text{ for all } a \in R$$

Rings can be further classified based off certain attributes, such as the following [1, §7.1, p. 224]:

Definition. A ring R with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.

Commutative division rings (or fields) are extremely common throughout undergrad mathematics. For example, the real numbers and the integers equipped with our usual notions of multiplication and addition are two examples of fields.

The following proposition gives us some properties of rings [1, §7.1, p. 236]:

Proposition 1. Let R be a ring. Then

(1) $0a = a0 = 0$ for all $a \in R$

(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$ (recall $-a$ is the additive inverse of a)

(3) $(-a)(-b) = ab$ for all $a, b \in R$

(4) if R has an identity 1, then the identity is unique and $-a = (-1)a$

Hence, we can see that rings retain some the usual operations that we have seen for addition and multiplication in our more typical settings, such as the real numbers.

Definition. Let R be a ring.

(1) A nonzero element a of R is called a *zero divisor* if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$

(2) Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted $R^{\times}$.

The units in R form a group under multiplication. Rings that share certain characteristics with $\mathbb{Z}$ are defined as follows:

Definition. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

Proposition 2. Assume a, b and c are elements of any ring with a not a zero divisior. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Corollary 3. Any finite integral domain is a field.

Now, similarly to groups and subgroups, we can define a subset of a ring which retains the structure of the parent ring. We can make this notion formal through the following definition [1, §7.1, p. 228]:

Definition. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

2.9. **Ring Homomorphisms and Quotient Rings.** Ring homomorphisms are very similar in concept to group homomorphisms. However, in the case of rings, homomorphisms must retain both the additive and multiplicative structure of the domain ring. We can see this in the following definition [1, §7.3, p. 239]:

Definition. Let R and S be rings.

(1) A *ring homomorphism* is a map $\varphi : R \to S$ satisfying

  (i) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$ (so φ is a group homomorphism on the additive groups)

  (ii) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$

(2) The *kernel* of the ring homomorphism φ, denoted kerϕ, is the set of elements of R that map to 0 in S (i.e., the kernel of φ viewed as a homomorphism of additive groups).

(3) A bijective ring homomorphism is called an *isomorphism.*

Again, similarly to the case of group homomorphisms, we can relate the image of a ring homomorphism to its codomain [1, §7.3, p. 239]:

Proposition 5. Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

(1) The image of φ is a subring of S.

(2) The kernel of φ is a subring of R. Furthermore, if $\alpha \in$ kerφ then $r\alpha$ and $\alpha r \in$ kerφ for every $r \in R$, i.e., kerφ is closed under multiplication by elements from R.

Naturally, we can wonder if an analogue of normal subgroups (and by extension quotient groups) exists in the ring setting. The concept related to normal subgroups is called an ideal and is conceptualized as a subset of a ring R which is closed under multiplication on the left and on the right by elements from R. Making this definition formal yields [1, §7.3, p. 242]:

Definition. Let R be a ring, let I be a subset of R and let $r \in R$.

(1) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$

(2) A subset I of R is a *left ideal* of R if

 (i) I is a subring of R

 (ii) I is closed under left multiplication by elements from R, i.e., $rI \subset I$ for all $r \in R$

 Similarly, I is a *right ideal* if (i) holds and in place of (ii) one has

 (iii) I is closed under right multiplication by elements from R, i.e., $Ir \subset I$ for all $r \in R$

(3) A subset I that is both a left ideal and a right ideal is called an *ideal* (or, for added emphasis, a *two-sided ideal*) of R

Now we will define operations on quotient rings [1, §7.3, p. 242-243]:

Proposition 6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operation:

$$(r + I) + (s + I) = (r + s) + I \text{ and } (r + I) \times (s + I) = (rs) + I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition: When I is an ideal of R, the ring R/I with the operations in the previous proposition is called the *quotient ring* of R by I.

Thus, we now have a formal notion of normal subgroups and quotient groups in the ring context. In keeping with the theme of extending group concepts to rings, we can now discuss the Isomorphism Theorems as they apply to rings [1, §7.3, p. 243, 246]:

Theorem 7 & 8

(1) *(The First Isomorphism Theorem for Rings)* If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.

(2) If I is any ideal of R, then the map

$$R \to R/I \text{ defined by } r \mapsto r + I$$

is a surjective ring homomorphism with kernel I (this homomorphism is called the *natural projection* of R onto R/I). Thus every ideal is the kernel of a ring homomorphism and vice versa.

(3) *(The Second Isomorphism Theorem for Rings)* Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$

(4) *(The Third Isomorphism Theorem for Rings)* Let I and J be ideals of R with $I \subset J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(5) *(The Fourth or Lattice Isomorphism Theorem for Rings)* Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

2.10. **Properties of Ideals.** In this section, we will now expand on the properties of ideals. We will begin with discussing ideals generated by an element or a set of elements, just as we have seen in the case of groups. The definition is as follows [1, §7.4, p. 251]:

Definition. Let A be any subset of the ring R.

(1) Let (A) denote the smallest ideal of R containing A, called *the ideal generated by A*

(2) Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$ i.e., $RA = \{r_1a_1 + a_2r_2 + \cdots a_nr_n \mid r_i \in R, a_i \in Ann \in \mathbb{Z}^+\}$ and $RAR = \{r_1a_1r_1' + r_2a_2r_2' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$

(3) An ideal generated by a single element is called a *principal ideal.*

(4) An ideal generated by a finite set is called a *finitely generated ideal.*

Note that if R is commutative, then $RA = AR = RAR = (A)$. An element $b \in R$ belongs to an ideal (a) if and only if $b = ra$ for some $r \in R$. In other words, b is an element of (a) if and only if b is a multiple of a. It can now be useful to discuss the units of an ideal [1, §7.4, p. 253]:

Proposition 9. Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

The ideals of a ring can be ordered in such a way that we can find a "largest" ideal within the ring [1, §7.4, p. 253-254]:

Definition. An ideal M in an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.

Proposition 11. In a ring with identity every proper ideal is contained in a maximal ideal.

Proposition 12. Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Lastly, we can discuss prime ideals, which give an extension to the notion of closure under multiplication for ideals [1, §7.4, p. 255-256]:

Definition. Assume R is commutative. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

Proposition 13. Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Corollary 14. Assume R is commutative. Every maximal ideal of R is a prime ideal.

2.11. **Euclidean Domains and Principal Ideal Domains.** In this section, we examine more specialized types of rings, beginning with rings with a division algorithm. These rings are known as Euclidean Domain. In order to discuss Euclidean Domains, we must first define the idea of a norm on an integral domain R [1, §8.1, p. 270]:

Definition. Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a *norm* on the integral domain R. If $N(a) > 0$ for $a \neq 0$ define N to be a *positive norm*.

Equipped with this definition of a norm, we can now defined Euclidean Domains [1, §8.1, p. 270]:

Definition. The integral domain R is said to be a *Euclidean Domain* (or possess a *Division Algorithm*) if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$ there exist elements q and r in R with

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

The element q is called the *quotient* and the element r the *remainder* of the division.

The key point here is that Euclidean Domains allow us to make use of the *Euclidean Algorithm*, which furnishes us with a method for finding the greatest common divisor of two elements. It is now important to discuss the ideals of Euclidean Domains [1, §8.1, p. 273]:

Proposition 1. Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R, then $I = (d)$, where d is any nonzero element of I of minimum norm.

We will now define the second main type of rings, the Principal Ideal Domain [1, §8.2, p. 279]:

Definition. A *Principal Ideal Domain* (P.I.D) is an integral domain in which every ideal is principal.

3. Conclusion

This first pass into the modern form of Algebra has been enlightening, generalizing a subject which I thought I was intimately familiar with. The notions of groups, quotient groups, isomomorphisms, and more are extremely powerful, and I see them often in other mathematical contexts. For example, in Dynamics, we talk about the order of elements under a specific iterated map. This is akin to our discussion of the order of elements within a group. However, with the increased abstractedness and power of the theorems in Modern Algebra when compared with Classical Algebra, I feel that I have lost some intuition for the objects that we are working with. It is my hope that the historical context given in the main introduction as well as the informal introductions & pictures at the start of each topic will help me and potentially others to build more intuition for and understanding of the subject.

References

[1] Dummit, David Steven., and Richard M. Foote. *Abstract Algebra.* 3rd ed., John Wiley & Sons, 2004.

[2] Pinter, Charles C. *A Book of Abstract Algebra.* 2nd ed., Dover Publications, 2013.

[3] Carter, Nathan C. *Visual Group Theory.* The Mathematical Association of America, 2009.

[4] Ayres, Frank, and Lloyd R Jaisingh. *Schaum's Outlines: Abstract Algebra.* 2nd ed., McGraw-Hill, 1971.

[5] "Algebra." *Wikipedia*, Wikimedia Foundation, 16 Oct. 2020, `en.wikipedia.org/wiki/Algebra`.

[6] "Abstract Algebra." *Wikipedia*, Wikimedia Foundation, 19 Sept. 2020, `en.wikipedia.org/wiki/Abstract_algebra`.

[7] "Group (Mathematics)." *Wikipedia*, Wikimedia Foundation, 17 Oct. 2020, `en.wikipedia.org/wiki/Group_(mathematics)`.

[8] "Subgroup." *Wikipedia*, Wikimedia Foundation, 14 June 2020, `en.wikipedia.org/wiki/Subgroup`.

[9] "Group Homomorphism." *Wikipedia*, Wikimedia Foundation, 1 Oct. 2020, `en.wikipedia.org/wiki/Group_homomorphism`.

[10] "Quotient Group." *Wikipedia*, Wikimedia Foundation, 1 Oct. 2020, `https://en.wikipedia.org/wiki/Quotient_group`.

[11] Dihedral Group." *Wikipedia*, Wikimedia Foundation, 1 Oct. 2020, `https://en.wikipedia.org/wiki/Dihedral_group`.