Fall 2018

Connecting High School Mathematics and Abstract Algebra

Abbey Scupin

Connecting High School Mathematics and Abstract Algebra

by

Abbey Scupin

B.A., Eastern Illinois University, 2014

Thesis

Submitted in partial fulfillment of the requirements

for the Degree of Master of Science with a Major in Mathematics

Governors State University

University Park, IL 60484

2018

Table of Contents

List of Figures

Abstract

This thesis focuses on the connections between the content covered in college level abstract algebra and high school mathematics courses. The purpose of studying and understanding these connections is in hopes to improve the way concepts are presented at the high school level to give students a deeper understanding of the mathematics. High school mathematics teachers are required to take specific college courses such as abstract algebra before they can teach high school mathematics. However, many teachers do not believe they can use the complex ideas learned in college to teach their students. On the surface, the content from courses like abstract algebra may seem unrelated, but recognizing important links and altering instruction could make college level mathematical ideas seem accessible to the high school students. We will not only study the connections in content, but also examine different ways to teach the content and how this can be beneficial to students.

Keywords: Abstract Algebra, High School Mathematics, Mathematical Connections, Mathematics Teachers

Chapter 1: Proof Methods

1.1 Why Proof Skills are Important for High School Mathematics Teachers

According to Knuth (2002), "proof is considered to be central to the discipline of mathematics and the practice of mathematicians." With such a prominent role in the study of mathematics, it is surprising that there has not always been more emphasis on the practice of proofs in high school. Many students have not had enough, if any, experience with proofs prior to taking an abstract algebra course in college. In high school, proofs should be used as part of the learning process to help students understand not just whether a conjecture is correct, but the reason why it is correct (Knuth, 2002). When a student recognizes why a statement must be true, then they truly comprehend the mathematical theory. This is the level of understanding that all teachers want their students to have, and exposing them to a variety of proofs is an important part of this development. Additionally, attempting to prove a conjecture may cause students to gain a deeper appreciation and knowledge of the underlying mathematical concepts involved. (Goldberger, 2002).

The importance of proofs in high school mathematics is continually supported throughout *The Common Core State Standards for Mathematics* (2018). One of the Standards for Mathematical Practices states that mathematically proficient students can construct viable arguments and critique the reasoning of others, which describes the skills required to create a valid mathematical proof. *The Common Core State Standards for Mathematics* (2018) requires students to have the ability to prove conjectures about various topics, such as polynomial identities, system of equations, and trigonometric identities, as well as many geometric theorems.

High school teachers can effectively incorporate the idea of proofs by fostering an environment that encourages students to defend and explain their reasoning with others (Knuth, 2002). Presenting and evaluating mathematical arguments will help students begin to develop basic ideas of proof writing. According to Lalonde (2013), there are two fundamental aspects of proof writing: logic and style. There are many different ways to prove a statement, and we will discuss the main proof methods in the following sections.

1.2 Proof by Contradiction

In a proof by contradiction, we assume the hypothesis and logical negation of the result we are trying to prove, and then reach a contradiction. When a contradiction is reached, we conclude that the logical negation of the statement is false, which must mean the statement we are trying to prove is true. In other words, the proof by contradiction of the statement "If A, then B" would be to assume A and not B, and then arrive at some kind of contradiction.

Example 1.2.1 Show that there are infinitely many integers.

Proof. Assume there are finitely many integers. Then, there must be a greatest integer. Let n be the number of integers, listed as $x_1, x_2, ..., x_n$ with $x_1 < x_2 < ... < x_n$. This means there is a greatest integer, x_n. Let $N = x_n + 1$. N is an integer because it is the sum of integers and $N > x_n$ since $N = x_n + 1$. Thus, x_n is not the greatest integer. We can conclude, by contradiction, that there are infinitely many integers. □

1.3 Proof by Induction

Mathematical induction is a method used to prove statements about integers. For example, if we need to prove a statement $P(n)$, with $n \in \mathbb{N}$, is true for all $n \geq n_0$ with n_0 the starting point. To do this, we prove that the base case $P(n_0)$ is true, assume that $P(k)$ is true, then show that $P(k+1)$ must be true. A fundamental axiom about the positive integers, called the Well-Ordering Property, validates mathematical induction.

The Well-Ordering Principle tells us that we can assume every nonempty subset of the set of positive integers has a least element.

Theorem. The Well-Ordering Principle implies mathematical induction.

Proof. Let $C = \{n \in \mathbb{Z} \mid \neg P(n)\}$, with $C \neq \varnothing$. In other words, C is the set of number of counterexamples to the statement $\forall n \in \mathbb{Z}, P(n)$ is true. By the well-ordering property, C has a least element. Mathematical induction shows that the base case $P(1)$ is true, so the least element in C must be greater than 1. Let $k+1$ be the least element in C. Then, $P(1), P(2), ..., P(k)$ must be true. However, $P(1), P(2), ..., P(k)$ implies $P(k+1)$, so if $P(1), P(2), ..., P(k)$ are true, then $P(k+1)$ must be true. This contradicts the assumption that $k+1 \in C$. Thus, $P(k+1)$ is true and $k+1 \notin C$, so $C = \varnothing$ and $\forall n \in \mathbb{Z}, P(n)$ is true. □

Example 1.3.1 (De Moivre's Theorem) Show that for any integer $n \geq 1$,

$$[r(\cos\theta + i\sin\theta)]^n = r^n[\cos(n\theta) + i\sin(n\theta)].$$

Proof. We will prove by induction on n.

Base Case: If $n = 1$, then $[r(\cos\theta + i\sin\theta)] = r[\cos(\theta) + i\sin(\theta)]$ is obviously true.

Inductive Step: Assume that for $n = k$ the formula is true. So,

$[r(\cos\theta + i\sin\theta)]^k = r^k[\cos(k\theta) + i\sin(k\theta)]$. Then,

$$\begin{aligned}[r(\cos\theta + i\sin\theta)]^{k+1} &= [r(\cos(\theta) + i\sin(\theta))]^k r[\cos(\theta) + i\sin(\theta)] \\ &= r^k[\cos(k\theta) + i\sin(k\theta)]r[\cos(\theta) + i\sin(\theta)] \\ &= r^{k+1}[\cos(k+1)\theta + i\sin(k+1)\theta].\end{aligned}$$

Thus, by induction, $[r(\cos\theta + i\sin\theta)]^n = r^n[\cos(n\theta) + i\sin(n\theta)]$ is true for all integers $n \geq 1$. □

1.4 Proof by Exhaustion

Proof by Exhaustion is a straightforward proof method that checks each possible case.

Example 1.4.1 Show that among any three consecutive integers, exactly one of them is divisible by 3.

Proof. Let n be the first of the consecutive integers. Then, they are $n, n+1,$ and $n+2$. The integer n must have a remainder of either 0, 1, or 2 when divided by 3. Thus, n can be written as $3k, 3k+1,$ or $3k+2$. We will look at each case.

Case 1: If $n=3k$, then $n+1=3k+1$ and $n+2=3k+2$. This means that only n is divisible by 3.

Case 2: If $n=3k+1$, then $n+1=3k+2$ and $n+2=3k+3$. This means that only $n+2$ is divisible by 3.

Case 3: If $n=3k+2$, then $n+1=3k+3$ and $n+2=3k+4$. This means that only $n+1$ is divisible by 3.

Thus, by checking each case, exactly one of three consecutive integers is divisible by 3. □

1.5 Proof by Construction

In number theory, to show that there exists an n such that the statement $P(n)$ is true, the method of proof by construction uses a case $n=a$, and proves that $P(a)$ is true.

Example 1.5.1 Show that if $n \in \mathbb{N}$ is not prime, then there is a prime divisor p of n such that $p \le \sqrt{n}$.

Proof. By the Fundamental Theorem of Arithmetic (Childs, p.54), construct p to be the least prime divisor of $n>1$. Since n is not prime, then $n=pd$ with $p, d \in \mathbb{N}$ and $1<p<d<n$. Since $n=pd \ge p^2$, $p \le \sqrt{n}$. □

Example 1.5.2 Show that there is a unique quadratic function $f(x)$ such that its graph contains three points $(0,1), (1,3),$ and $(-1,1)$.

Proof. We will prove the claim by construction. Let $f(x) = ax^2 + bx + c$. Then

$f(0) = 1,\ f(1) = 3,\ f(-1) = 1$, which gives the following system of three linear equations:

$$\begin{aligned} &c = 1 \\ &a + b + c = 3 \\ &a - b + c = 1 \end{aligned}$$

Solving the system of equations gives the unique solution $a = 1,\ b = 1,$ and $c = 1$. Thus, $f(x)$ is a unique quadratic function that contains the three points $(0,1),\ (1,3),$ and $(-1,1)$. □

1.6 Proof by Contrapositive

To prove the statement that A implies B, we can use a proof by contrapositive and show that not B implies not A. This is a valid method of proof since a statement is true if and only if its contrapositive is true.

Example 1.6.1 Prove for any $n \in \mathbb{Z}$, if $3n + 1$ is even, then n is odd.

Proof. We will prove the contrapositive, for any $n \in \mathbb{Z}$, if n is not odd, then $3n + 1$ is not even. In other words, for any $n \in \mathbb{Z}$, if n is even, then $3n + 1$ is odd. So, let n be an even integer. Then, $n = 2k$ for some $k \in \mathbb{Z}$. Then, $3n + 1 = 3(2k) + 1 = 2(3k) + 1$. Since $k \in \mathbb{Z},\ 3k \in \mathbb{Z}$. Thus, $3n + 1$ must be odd. So if $3n + 1$ is even, then n is odd. □

Chapter 2: Mappings and Functions

For mathematics majors, the concept of a function, or mapping, is taught as a preliminary topic in most abstract algebra courses and books. In K-12 mathematics education in the United States, students are introduced to functions in 8^{th} grade and continue to build on their knowledge of functions throughout high school. Although students learn continuously about functions for years, the ideas of functions in abstract algebra seem foreign to most of them. High school students are usually only exposed to functions that are mappings from the real numbers to itself, so certain aspects and notations used in abstract algebra are not needed and, therefore, not taught.

2.1 Classifying Functions

In abstract algebra, a function of mapping f from set S to set T is defined as a rule in which for each element $s \in S$, there is a unique element $t \in T$ assigned by this rule f. This mapping is denoted as $f: S \rightarrow T$ and for the $t \in T$ we write $t = f(s)$ (Herstein, 1996). The mapping $f: S \rightarrow T$ has domain S and range $f(S) = \{f(s) \in T, s \in S\}$. While the definition of a function is the same in high school algebra, the unfamiliar notation may prevent some from seeing the connections. The concepts of domain and range are essential to understanding functions in both high school math and abstract algebra, but there are other significant characteristics of functions used in abstract algebra that are often introduced for the first time. Injections, surjections, and bijections are fundamental properties of mappings that relate to other important concepts in abstract algebra. A mapping $f: S \rightarrow T$ is injective, or one-to-one, if for $x \neq y \in S$, $f(x) \neq f(y) \in T$. Equivalently, $f(x) = f(y)$ implies that $x = y$. In other words, for each $t \in f(S)$, there exists a unique $s \in S$ such that $f(s) = t$. A mapping $f: S \rightarrow T$ is surjective, or onto, if $f(S) = T$. In other words, for each $t \in T$, there exists an $s \in S$ such that $f(s) = t$. A function that is both an injection and surjection is bijective. These classifications could certainly be taught in high school math to give students a deeper understanding of functions and provide them with examples that go beyond the commonly studied functions.

When students are introduced to functions, they use a mapping diagram to decide if a relation is a function, as shown in Figure 2.1.

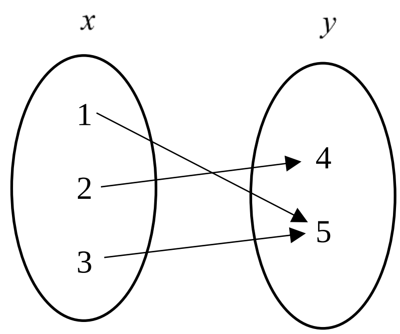
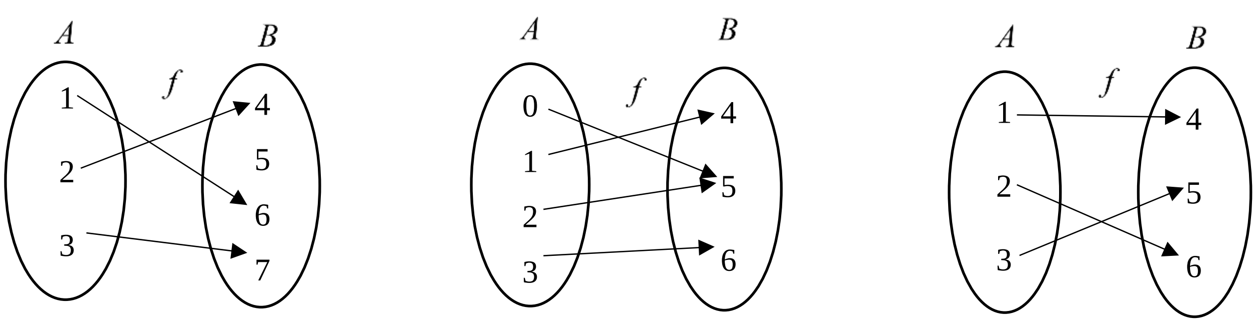


Figure 2.1. A mapping diagram example of a function.

This initial introduction to functions, unfortunately, is the only time a high school student relates a function to a mapping. A mapping diagram allows students to visualize a function as a relation of elements in a set, rather than only a relation between x and y on a Cartesian plane. Having students learn more about functions as mappings could be added into the high school curriculum to give students the ability to explore various types of functions. Using a mapping diagram, for example, is a great way to understand the concept of a function being one-to-one, onto, or bijective. Figure 2.2 shows an example of each.



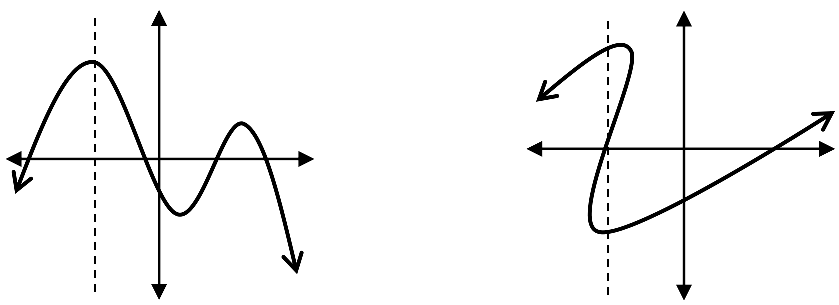
Injective or One-to-One Function

Surjective or Onto Function

Bijective Function

Figure 2.2. Mapping diagram examples of one-to-one, onto, and bijective functions.

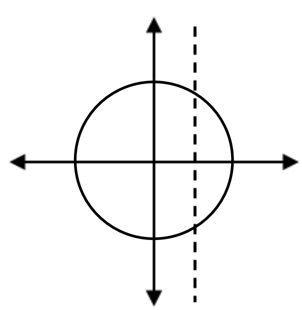
These important function properties could also be determined graphically, which is more familiar to high school students. To determine if a graphed relation represents a function, students are taught to use the Vertical Line Test. If we can draw a vertical line that intersects the graph at more than one point, then there is a specific x value is assigned to more than one y value, which would make the relation not a function.



Function Not a Function

Figure 2.3. Vertical Line Test used to determine if a relation is a function

Example 2.1.1 Consider the unit circle equation $x^2 + y^2 = 1$, where x, y are real numbers. Since for all values x in the open interval $(-1,1)$, y has two different values, this equation does not define y as a function of x. From its graph, we can see that the vertical line $x = a$, $-1 < a < 1$, intersects the graph at two distinct points.



Much like the Vertical Line Test students learn in high school, a Horizontal Line Test can be used to determine if a graphed function is injective, surjective, or bijective. If we can draw a horizontal line that intersects the graph at more than one point, then there are at least two different x values are assigned to the same y value, which would make the function not injective. If we can draw a horizontal line that does not intersect the graph at all, then there is at least one y value to which no x values are assigned, which would make the function not surjective. An example of each is shown in Figure 2.4.

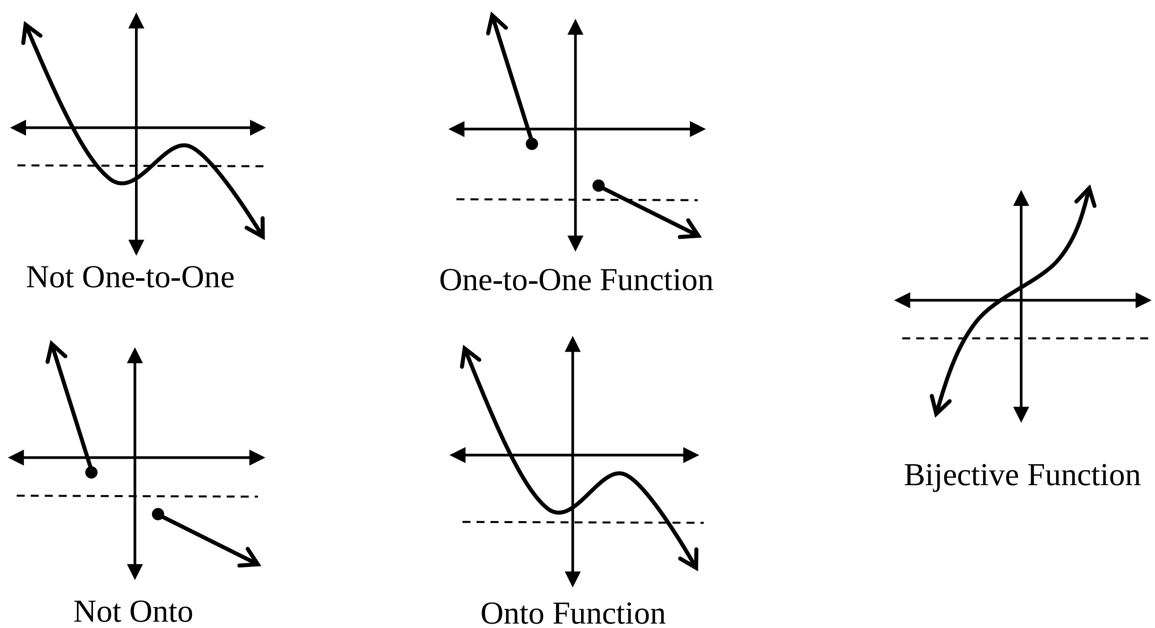


Figure 2.4. Horizontal Line Test examples used to determine if a function is one-to-one, onto, or bijective

The following is a linear algebra example of proving a mapping is one-to-one and onto.

Example 2.1.2 Let A be the 2×2 matrix

$$A=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},$$

and $T_A:\mathbb{R}^2\to\mathbb{R}^2$ defined by

$$T_A(x,y)=(x+y,x-y)\ .$$

which is the matrix multiplication

$$\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}x+y\\ x-y\end{pmatrix}$$

Prove that T_A, which is called a linear transformation, is a bijection.

Proof. Injection: Let $T_A(x,y) = T_A(x',y')$. Then,

$$\begin{pmatrix} x+y \\ x-y \end{pmatrix} = \begin{pmatrix} x'+y' \\ x'-y' \end{pmatrix}$$

and

$$\begin{aligned} x+y &= x'+y' \\ x-y &= x'-y' \end{aligned}$$

or

$$\begin{aligned} (x-x')+(y-y') &= 0 \\ (x-x')-(y-y') &= 0 \end{aligned}$$

which gives $x = x'$ and $y = y'$. Thus, $T_A(x,y) = T_A(x',y') \Rightarrow (x,y) = (x',y')$, so T is injective.

Surjection: Let $c,d \in \mathbb{R}$ such that

$$\begin{aligned} c &= x+y \\ d &= x-y \end{aligned}$$

Then,

$$\begin{aligned} x &= \frac{1}{2}(c+d) \\ y &= \frac{1}{2}(c-d) \end{aligned}$$

Thus, arbitrary $c,d \in \mathbb{R}$ has a solution $x,y \in \mathbb{R}$, so T is surjective. Since T is both an injection and surjection, it is a bijection. □

2.2 Composition of Functions

The composition of functions is another topic covered in high school math that is an essential idea used in abstract algebra. Given the mappings $g: S \to T$, $f: T \to U$, consider an element $g(s) \in T$ that is then assigned an element in U by f. Thus $f(g(s)) \in U$ is a mapping from S to U, which is defined by the composition process as follows.

Definition. Let $g: S \to T$, $f: T \to U$. Then the composition, or product, is the mapping $f \circ g: S \to U$ defined by $(f \circ g)(s) = f(g(s))$ for $s \in S$.

In high school math, students may find composite functions similar to the following example.

Example 2.2.1 Let $f(x) = 3x - 5$ and $g(x) = x^2 + 4$, then the composite functions

$$(f \circ g)(x) = f(g(x)) = 3(x^2 + 4) - 5 = 3x^2 + 7$$

and

$$(g \circ f)(x) = g(f(x)) = (3x - 5)^2 + 4 = 9x^2 - 30x + 29 \ . \qquad \square$$

As in the above example, $f \circ g \neq g \circ f$ for most functions. In abstract algebra, students learn essential properties of composition of mappings.

Theorem 2.1. Let $f: S \to T$, $g: T \to U$ and $h: U \to V$. Then The composition of mappings is associative; that is, $(h \circ g) \circ f = h \circ (g \circ f)$.

Theorem 2.2. Let $f: S \to T$, $g: T \to U$. If f and g are both one-to-one, then the mapping $g \circ f: S \to U$ is one-to-one.

Proof. Let $x, y \in S$ with $(f \circ g)(x) = (f \circ g)(y)$. Then $f(g(x)) = f(g(y))$. Since f is one-to-one, this gives $g(x) = g(y)$. Since g is also one-to-one, $x = y$. Thus, $(f \circ g)(x) = (f \circ g)(y)$ implies $x = y$, so $f \circ g$ is one-to-one. $\square$

Theorem 2.3. Let $g: S \to T$, $f: T \to U$. If f and g are both onto, then the mapping $f \circ g$ is onto.

Proof. Let $u \in U$. Since f is onto, there exists $t \in T$ such that $f(t) = u$. Since g is onto, there exists $s \in S$ such that $g(s) = t$ for $t \in T$. Thus, for $u \in U$, there exists an $s \in S$ such that $f(g(s)) = u$, so $f \circ g$ is onto. □

Combining Theorem 2.2 and 2.3, we have Theorem 2.4.

Theorem 2.4. Let $g : S \to T,\ \ f : T \to U$. If f and g are bijective, then so is $f \circ g$.

2.3 Inverse Functions

Another important concept of mappings in abstract algebra is the existence of inverses.

Definition. A mapping $f^{-1} : T \to S$ is called an inverse mapping of $f : S \to T$ if

$(f^{-1} \circ f)(s) = f^{-1}(f(s)) = s$, $\forall s \in S$ and $(f \circ f^{-1})(t) = f(f^{-1}(t)) = t$, $\forall t \in T$.

Inverse functions are presented in high school math, but the importance and explanation of inverse functions is often not explored or understood. The following theorem used in abstract algebra allows us to identify when inverse mappings exist.

Theorem 2.5. The mapping $f : S \to T$ is one-to-one and onto if and only if the inverse f^{-1} exists.

Proof. $(\Rightarrow)$ Let the mapping $f : S \to T$ be one-to-one and onto. Let $t \in T$. Since f is onto, there exists an $s \in S$ such that $f(s) = t$ and because f is one-to-one, s is unique. Thus, the mapping defined by $f^{-1}(t) = s$, is the inverse of f and is a mapping of T onto S.

$(\Leftarrow)$ Let the mapping $f : S \to T$ have inverse $f^{-1} : T \to S$. Then, $f^{-1}(f(s)) = s\ \ \forall s \in S.$ Let $s_1, s_2 \in S$ with $f(s_1) = f(s_2)$, then $s_1 = f^{-1}(f(s_1)) = f^{-1}(f(s_2)) = s_2$. Thus, f is one-to-one. To show f is onto, let $t \in T$ and show there exists an $s \in S$ such that $f(s) = t$. Since $f(f^{-1}(t)) = t$ with $f^{-1}(t) \in S,$ let $s = f^{-1}(t)$, then $f(s) = t$. Thus, f is onto. □

If we refer back to Example 2.1, we can now make a general theorem used in linear algebra.

Theorem 2.6. Let $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ be a transformation defined by $T(x, y) = A\begin{pmatrix} x \\ y \end{pmatrix}$ where

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

If $\det(A) = a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0$, then the inverse matrix A^{-1} exists. Therefore, the inverse mapping $T_A^{-1} = T_{A^{-1}}$ exists and T_A is a bijection.

The following examples show how we can connect the ideas of inverse functions used in abstract algebra with functions taught in high school math.

Example 2.3.1 Let $f(x) = x^2$. Consider the function $f : \mathbb{R} \to \mathbb{R}$. Then, f is neither injective nor surjective and the inverse function does not exist. □

Example 2.3.2 Let $g(x) = x^2$. Consider the function $g : S \to S$, where S is the set of non-negative real numbers. Then, g is a bijection and the inverse function g^{-1} exists with $g^{-1}(x) = \sqrt{x}$. □

Example 2.3.3 Let $h(x) = x^2$. Consider the function $h : T \to T$, where T is the set of nonnegative integers. Then, h is neither injective nor surjective and the inverse function does not exist. □

From the examples, we can generalize that the function $f(x) = x^{2n}$ is a bijection and has an inverse only when $f : S \to S$, $S = \mathbb{R}^+$.

Example 2.3.4 Let $f(x) = x^3$ with $f : \mathbb{R} \to \mathbb{R}$. Then, f is a bijection and the inverse function f^{-1} exists with $f^{-1}(x) = \sqrt[3]{x}$. In general, the function $f(x) = x^{2n+1}$, $f : \mathbb{R} \to \mathbb{R}$ with n a nonnegative integer, is a bijection and the inverse f^{-1} exists. □

Example 2.3.5 The function $f(x) = \sin x$ with $f : \mathbb{R} \to [-1,1]$ is not injective, but surjective. However, with $f : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1,1]$, the function is a bijection and the inverse $f^{-1}(x) = \arcsin x$ exists. □

These examples show that a function is defined not only by a rule, but also by its domain. This is an idea that is fully recognized in abstract algebra, yet is not often acknowledged in high school math.

It is clear that there are many connections between abstract algebra and high school math on the topic of mappings and functions. Most high school students, however, are restricted to learning only a few types of functions. Exposing these students to function properties such as being injective, surjective, or bijective, would give them a deeper understanding of functions and inverse functions, which would better prepare them for more abstract concepts.

Chapter 3: Group Theory and Operations

Group theory, like many topics in abstract algebra, helps connect and explain concepts learned throughout high school math classes. The connections we will discuss are how group theory can be used to justify solutions to equations, and how it is linked to symmetry studied in geometry.

3.1 Group Axiom and Solving Linear Equations

Definition. A binary operation, denoted $*$, on a non-empty set S is a mapping $S \times S \to S$ that assigns each pair $(a,b) \in S \times S$ a unique element $a * b \in S$.

Example 3.1.1 The operations of addition and multiplication are binary operations on the set of real numbers, and division is a binary operation on the set of non-zero real numbers (Kiang, 1988).

Definition. A nonempty set G, is considered a group if there is a defined operation $*$ that follows the following four axioms:

1. Closure: If $a,b \in G$ then $a * b \in G$.
2. Associativity: If $a,b,c \in G$ then $(a*b)*c = a*(b*c)$.
3. Identity: There exists an element $e \in G$ such that for any element $a \in G$, $a*e = e*a = a$.
4. Inverses: For any element $a \in G$, $\exists a^{-1} \in G$ such that $a*a^{-1} = a^{-1}*a = e$.

Groups with commutative operations are called Abelian groups. For Abelian groups, if $a,b \in G$, then $a*b = b*a$.

Example 3.1.2 Let $G = \mathbb{Z}$ be the set of all integers under the operation of addition. If $a,b \in G$ then $a+b \in G$ (G is closed under addition). If $a,b,c \in G$ then $(a+b)+c = a+(b+c)$ (it is associative). For any $a \in G$, $a+0 = 0+a = a$ (0 is the identity element). For any

$a \in G,\ a+(-a)=(-a)+a=0$ (the inverse of any element is its negative). Thus, G forms an additive group. Additionally, if $a,b \in G$, then $a+b=b+a$, which makes the integers under addition an Abelian group. □

Similarly, the set of real numbers and set of complex numbers form abelian groups under addition.

Example 3.1.3 Let $G=\mathbb{Z}$ be the set of all integers, with $\bullet$ the ordinary product of integers. If $a,b \in G$ then $a \bullet b = ab \in G$ (G is closed under multiplication). If $a,b,c \in G$ then $(ab)c=a(bc)$ (it is associative). For any $a \in G,\ a \bullet 1 = a1 = a = 1a = 1 \bullet a$ (1 is the identity element). Three of the axioms hold true for the integers under multiplication, but the fourth axiom fails. For example, $5 \in G$ does not have an integer $a \in G$ such that $5 \bullet a = 1$ because this would require $a=\frac{1}{5} \notin \mathbb{Z}$. Therefore, the integers do not form a group under multiplication. □

The study of group theory allows us to expand on our perception of solutions to equations that we learned in high school. The Common Core State Standards in High School: Algebra states the importance for students to recognize that "some equations have no solutions in a given number system, but have a solution in a larger system." For example, the solution to the equation $2x=5$ depends on the domain: if $x \in \mathbb{Z}$, there is no solution; if $x \in \mathbb{Q}$, the solution is $x=\frac{5}{2}$; and if $x \in \mathbb{Z}_7$, then $x=6$ is a solution. With group theory, we use a more abstract approach that allows us to deal with many mathematical systems at once (Dogfrey, 1998).

Example 3.1.4 Let G be a group with $a,b \in G$. Find the solution of $a*x=b$.

Using the four group axioms,

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

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

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

$$e * x = a^{-1} * b$$

$$x = a^{-1} * b \qquad \square$$

Thus, we can solve the equation for x without being concerned with what $a, b, x,$ or the operation $*$ represent.

Group theory relates to several Common Core State Standards for high school algebra. One example is the following standard in the domain of Reasoning with Equations & Inequalities that requires students to "understand solving equations as a process of reasoning and explain the reasoning" (*Common Core State Standards for Mathematics*, 2018). The standard states,

> "Explain each step in solving a simple equation as following from the equality of numbers asserted at the previous step, starting from the assumption that the original equation has a solution. Construct a viable argument to justify a solution method."

Though the concepts of groups are not taught in high school, the group axioms can be used to justify steps in solving equations, as shown in the following examples.

Example 3.1.5 Find the solution to the equation $x + 9 = 16$. Justify each step.

Proof. Since the integers form a group under addition, we can use the group axioms.

$(x+9)+(-9) = 16+(-9)$ (Closure and Addition Property of Equality)

$x+(9+(-9)) = 16+(-9)$ (Associativity)

$x+0 = 16+(-9)$ (Inverse axiom)

$x = 16+(-9)$ (Identity axiom)

$x = 7$ (Closure) $\square$

Example 3.1.6 Find the solution to the equation $9x = 16$. Justify each step.

Proof. Since the set of nonzero rational numbers form a group under multiplication, we can use the group axioms.

$$\frac{1}{9}\cdot(9x) = \frac{1}{9}\cdot 16 \qquad \text{(Closure and Multiplication Property of Equality)}$$

$$\left(\frac{1}{9}\cdot 9\right)x = \frac{1}{9}\cdot 16 \qquad \text{(Associativity)}$$

$$1\cdot x = \frac{1}{9}\cdot 16 \qquad \text{(Inverse axiom)}$$

$$x = \frac{1}{9}\cdot 16 \qquad \text{(Identity axiom)}$$

$$x = \frac{16}{9} \qquad \text{(Closure)}$$

□

Example 3.1.7 The set of the primitive nth roots of unity

$$U = \left\{ z_n = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right),\ k = 0,1,\ldots,(n-1) \right\}$$

is a multiplicative group and cyclic group generated by z_1.

Definition. Let $GL(n,\mathbb{R})$ be the set of all invertible $n\times n$ matrices with entries in $\mathbb{R}$, then it is a group with the operation of matrix multiplication, called the general linear group of degree n over $\mathbb{R}$.

Note that $I_n + (-I_n) = 0 \notin GL(n,\mathbb{R})$, where I_n is the identity matrix, so $GL(n,\mathbb{R})$ is not a group with the operation of matrix addition. Additionally, $GL(n,\mathbb{R})$ is not an Abelian group since matrix multiplication is not commutative.

Example 3.1.8 Given the system of two linear equations $x+3y=22$ and $2x-y=2$, solve for (x, y) by using matrices, if possible.

Proof. We can write $x+3y=22$ and $2x-y=2$ in the matrix form $AX=b$, so

$$\begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 22 \\ 2 \end{pmatrix}.$$

The determinant of A is $-1-6=-7$. Since $\det(A)=-7\neq 0$, the inverse A^{-1} exists with

$$A^{-1}=-\frac{1}{7}\begin{pmatrix} -1 & -3 \\ -2 & 1 \end{pmatrix}.$$

Then,

$$\begin{aligned} X &= A^{-1}b \\ &= -\frac{1}{7}\begin{pmatrix} -1 & -3 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 22 \\ 2 \end{pmatrix} \\ &= -\frac{1}{7}\begin{pmatrix} -28 \\ -42 \end{pmatrix} \\ &= \begin{pmatrix} 4 \\ 6 \end{pmatrix}. \end{aligned}$$

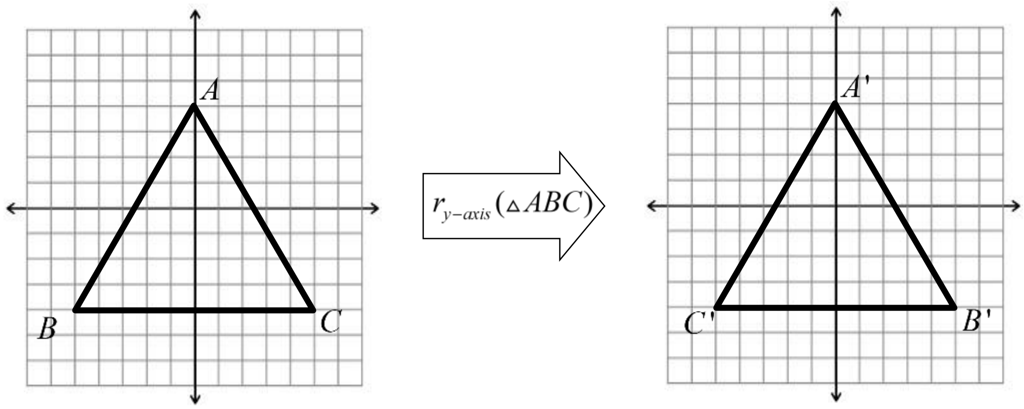
Thus, the solution to the system is $(4,6)$. □

3.2 Symmetry

All high school students study geometry and the concepts of symmetry and transformations in the plane. Students learn that an isometry is a transformation that preserves length, or Euclidean distance. The isometries in $\mathbb{R}^2$ explored in high school are rotations, reflections, translations, or any combination of them.

Example 3.2.1 Given $\triangle ABC$ graphed below, graph the image $r_{y-axis}(\triangle ABC)$.

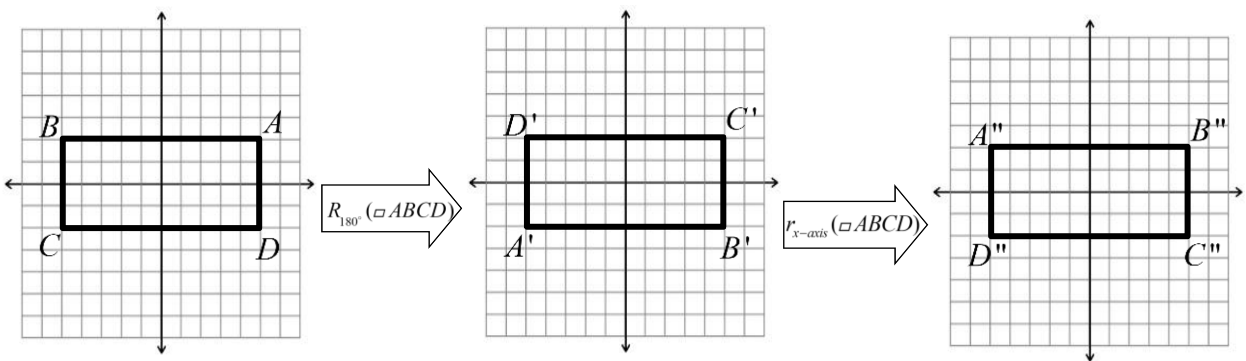
Solution.



□

Example 3.2.2 Given $\square ABCD$ graphed below, graph the image $r_{x-axis}(R_{180^\circ}(\square ABCD))$.

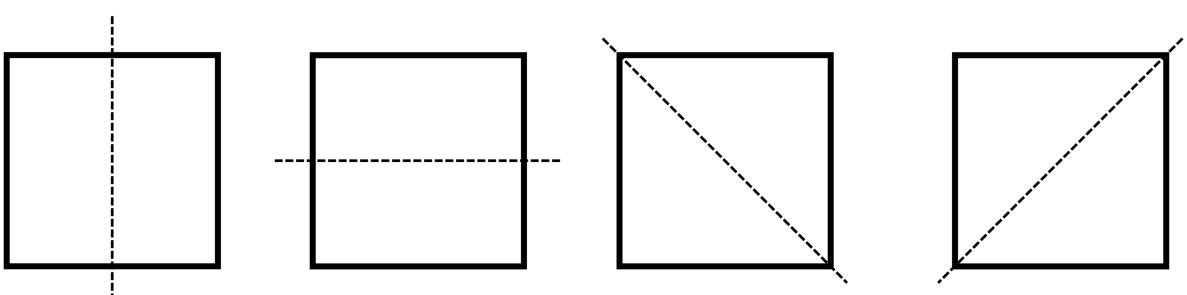
Solution:



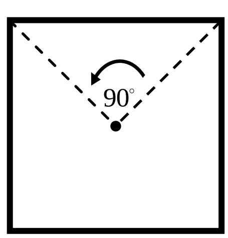
□

Example 3.2.3 Find the lines of symmetry and rotational symmetry of a square.

Solution: A square has four lines of symmetry, as shown below.



A square has rotational symmetry of 90°.



□

These concepts of isometries and symmetries are explored further in abstract algebra. Judson (2010) describes the symmetry of a geometric figure as "a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles," and a rigid motion as "a map from the plane to itself that preserves the symmetry of an object." In abstract algebra, we find that the rigid motions of a figure form a group, called the symmetry groups. Before introducing the symmetry groups, let us first discuss permutations.

Definition. A permutation is a one-to-one map of a set S onto itself.

If σ is a permutation of the set $S = \{x_1, x_2, x_3\}$ with $\sigma : x_1 \to x_3,\ x_2 \to x_2,\ x_3 \to x_1$, we denote as

$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}$. The product of permutations is defined as the composition of maps.

Example 3.2.4 Let σ and τ be permutations of the set $S = \{1,2,3,4,5,6\}$, with

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 1 & 3 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

Then,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}.$$

Here, $\sigma\tau$ is the composition of σ and τ. □

Theorem. Let S be a set of n elements. Then the set of all permutations of S, denoted S_n, forms a group with the operation of composition of maps. This group is called the symmetric group and has $n!$ elements.

Proof. We will first prove each of the four axioms to be true for S_n :

- Let $\sigma, \tau \in S_n$. Then $\sigma\tau$ means we perform the permutation τ on S and then perform the permutation σ. This result is another permutation on S, so by Theorem 2.4, $\sigma\tau \in S_n$.
- Let $\sigma, \tau, \mu \in S_n$, then $\sigma(\tau\mu) = (\sigma\tau)\mu$ since the composition of maps is associative.
- The permutation $e = \begin{pmatrix} 1 & 2 & 3 \ldots n \\ 1 & 2 & 3 \ldots n \end{pmatrix}$ that maps each element of S to itself is the identity and $e \in S_n$.
- Let $\sigma \in S_n$. Since permutations are one-to-one and onto, σ^{-1} exists by Theorem 2.5. The inverse of a permutation is also a permutations, so $\sigma^{-1} \in S_n$

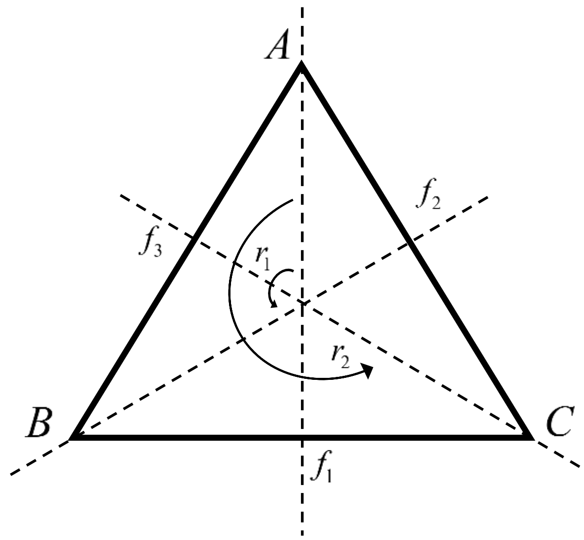
Thus, S_n forms a group under the operation composition of maps. We will now prove that S_n has $n!$ elements:

Let $\sigma \in S_n$ where $S = \{x_1, x_2, ..., x_n\}$. σ can send x_1 to any of the elements in S, so it has n elements to choose from. Since σ is one-to-one, $\sigma(x_1) \neq \sigma(x_2)$. Thus, σ can send x_2 to $(n-1)$ different elements, x_3 to $(n-2)$ different elements, and so on. Therefore, the number of different permutations of S is $n(n-1)(n-2)\cdots 1 = n!$ □

The symmetries of a figure can be thought of as permutations of the vertices. Thus, all the symmetries of a figure form a symmetry group.

Example 3.2.5 Prove the symmetries of an equilateral triangle form a group.

Proof. Let $\triangle ABC$ be an equilateral triangle. An equilateral has three lines of reflections, as shown below. We will denote the symmetry from the line of reflection through the top vertices A as f_1, the left vertices B as f_2, and the right vertices C as f_3. $\triangle ABC$ has rotational symmetry of 120° counterclockwise we will denote as r_1, and 240° counterclockwise we will denote as r_2.



The identity symmetry would be not performing any transformation on $\triangle ABC$. The symmetries of an equilateral triangle $\triangle ABC$ can be represented by the following permutations on the vertices $A, B,$ and C.

$$f_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \qquad f_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \qquad f_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

$$r_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \qquad r_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \qquad e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

The composition of any two symmetries of $\triangle ABC$ is another symmetry. For example, $f_1 r_2 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$ which is the same as the reflective symmetry f_3. Each symmetry of $\triangle ABC$ has an inverse, which is another symmetry that "undoes" the transformation. For example, $r_1 r_2 = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} = e$, so r_2 is the inverse of r_1. It is clear that the symmetries of an equilateral triangle form a group. In fact, they form the symmetric group S_3. A set with three elements has

$3! = 6$ permutations, so every permutation of a set with three elements corresponds to a symmetry of an equilateral triangle. □

3.3 Applications

Group theory is a mathematical tool that allows us to understand the underlying structure objects in nature like molecules and designed works like sculptures, so it has countless applications. Group theory resulted from mathematicians trying to find the roots of polynomials, but it is now an essential part of coding theory and the study of symmetries, and it is used in areas of biology, chemistry, and physics (Judson, 2010). One example where chemists use group theory is when they analyze crystals by using the study of symmetries (Roney-Dougal, 2006).

Example 3.3.1. The symmetries of the molecule PF_5 form a group.

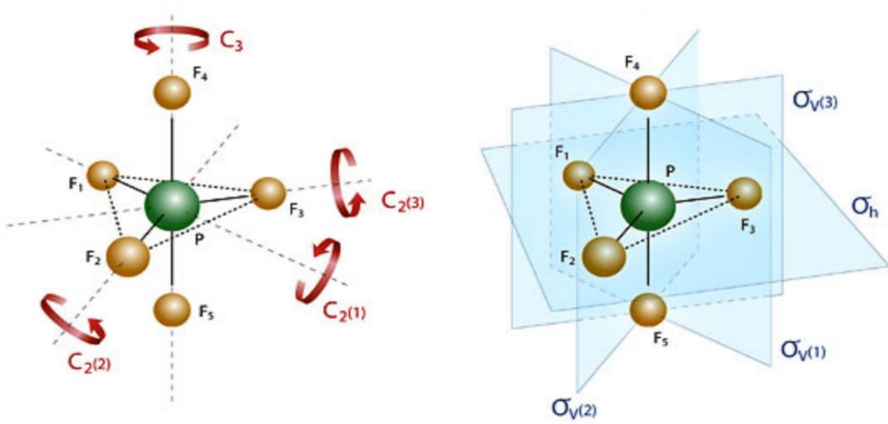


Figure 3.1 The symmetry operations of the molecule PF_5. Reprinted from "Through the Looking Glass," by R. Thomas, 2003, Retrieved from https://plus.maths.org/content/os/issue24/features/symmetry/index

Proof. As shown in Figure 3.1, PF_5 has rotational symmetries $C_2(1), C_2(2), C_2(3), C_3$ and reflection symmetries $\sigma_v(1), \sigma_v(2), \sigma_v(3), \sigma_h$. We will denote a 360° rotation as C_1, a 120° rotation around C_3 as $C_3(1)$, and a 240° rotation around C_3 as $C_3(2)$. $C_2(1), C_2(2),$ and $C_2(3)$ are all 180° rotations. The identity symmetry would be C_1. Rotating the molecule 360° does not change the molecule at all, so the composition of any symmetry with C_1 is just the original symmetry. The composition of any two symmetries of PF_5 results in another symmetry. For example, the resulting molecule after a 240° rotation around C_3 and then a reflection over the plane $\sigma_v(2)$ is equivalent to reflecting the molecule over the plane $\sigma_v(1)$. In other words,

$$\sigma_v(2) \circ C_3(2) = \sigma_v(1) .$$

The composition of the symmetries of PF_5 is associative. For example,

$$\sigma_v(2) \circ (C_3(2) \circ C_2(1)) = (\sigma_v(2) \circ C_3(2)) \circ C_2(1) .$$

For each symmetry, there is another symmetry in which the composition of the symmetries results in the original molecule, or C_1. For example, reflecting over a symmetry plane twice always results in the original molecule. This means that each symmetry of PF_5 has an inverse symmetry. Thus, the symmetries of PF_5 form a group. $\square$

Another well-known application of group theory is the Rubik's Cube. The permutations that can be performed on a Rubik's Cube form a group, so group theory can be used to solve a Rubik's Cube (Freiberger, 2007). Additionally, group theory has many applications in physics. For applications in physics, see Dr. Mildred Dresselhaus' book "Applications of Group Theory to the Physics of Solids."

References

Common Core State Standards for Mathematics[PDF]. (2018). Common Core State Standards Initiative.

Dogfrey, A. (1998). Introduction to Group Theory. Retrieved from http://dogschool.tripod.com/index.html.

Dresselhaus, M. (2002). *Applications of Group Theory to the Physics of Solids*. Retrieved from http://web.mit.edu/course/6/6.734j/www/group-full02.pdf

Farlow. (n.d.). Section 4.2 Injections, Surjections, and Bijections. Retrieved from http://www.math.umaine.edu/~farlow/sec42.pdf.

Freiberger, M. (2007, June 5). Rubik Success in Twenty-Six Steps. Retrieved from https://plus.maths.org/content/rubik-success-twenty-six-steps

Goldberger, A. (2002). *What Are Mathematical Proofs and Why Are They Important?* Retrieved from http://www.math.uconn.edu/~hurley/math315/proofgoldberger.pdf.

Herstein, I. N. (1996). *Abstract Algebra* (3rd ed.). New Jersey: Prentice-Hall.

Hutchings, M. (n.d.). *Introduction to Mathematical Arguments*. Lecture. Retrieved from https://math.berkeley.edu/~hutching/.

Judson, T. W. (2010). *Abstract Algebra: Theory and Applications*. Boston, MA: PWS Pub.

Kiang, L. (1988, September 5). *Axioms and Algebraic Systems*. Speech presented at Singapore Mathematical Society Workshop. Retrieved from https://sms.math.nus.edu.sg/smsmedley/Vol-17-1/Axioms and algebraic systems(YK Leong).pdf.

Lalonde, S. (2013). *Notes on Abstract Algebra*. Lecture. Retrieved from https://math.dartmouth.edu/archive/m31x13/public_html/Notes on Abstract Algebra 2013.pdf.

Roney-Dougal, C. (2006, June 1). The Power of Groups. Retrieved from https://plus.maths.org/content/os/issue39/features/colva/index

Thomas, R. (2003, March 1). Through the Looking-Glass. Retrieved from https://plus.maths.org/content/os/issue24/features/symmetry/index