Directed Study Article Summaries

Stewart Mitchell

Winter 2020

1 A Cohomological Viewpoint on Elementary School Arithmetic [1]

This article makes use of the familiarity of elementary school arithmetic to explain the concept of group cohomology. This is an immensely powerful set of tools in the realm of mathematics. It utilizes the study of groups and group actions to make sense of more complex mathematical structures [2].

Initially, to model addition of two-digit numbers in a group-theoretical sense, we consider the group $\mathbb{Z}_{100}$. In order to conduct addition within this group, consider the subgroup $\mathbb{Z}_{10}$ of $\mathbb{Z}_{100}$. Denote this as T for "tens," since it contains all of the multiples of 10 in $\mathbb{Z}_{100}$. To obtain the "ones," we consider the quotient group $\mathbb{Z}_{100}/T$. This is constructed from the cosets $x+T$ for any element x in $\mathbb{Z}_{100}$. These cosets "determine and are completely determined by the ones digit of x" [1]. Now, consider any element x of $\mathbb{Z}_{100}$ as $[a][b]$ such that a is the tens digit of x and b is the ones digit of x. Carrying out the process of addition between two elements is more complicated than it seems, however. Consider two arbitrary elements $[a_1][b_1]$ and $[a_2][b_2]$ in $\mathbb{Z}_{100}$. In the sum, the ones digit b need only depend on b_1 and b_2, as ones digits are only determined by ones digits. Though, the tens digit a in the sum must depend on more than just a_1 and a_2 because there is the possibility that the addition of b_1 and b_2 will create an extra ten, or carry over. To combat this issue, the carrying function $z(b_1, b_2) : O \times O \to T$ is introduced. In standard addition, this function produces only two values: 0 or 1. The output is 0 if the sum of the ones digits is less than 10, and the output is 1 if the sum of the ones digits is greater than or equal to 10. Thus, the tens digit a of the sum is determined by a_1, a_2, and $z(b_1, b_2)$. Using the associativity of addition in this group, we determine that z is a cocycle because it satisfies the cocycle condition $z(b_2, b_3) - z(b_1 + b_2, b_3) + z(b_1, b_2 + b_3) - z(b_1, b_2) = 0$ and the normalization condition $z(b, 0) = 0 = z(0, b)$.

Beyond the example of standard addition, furthermore, it is possible to construct other groups of order 100 from the subgroups T and O and from multiples of the carrying function. Namely, the cocycles $2z, 4z, 6z$, and $8z$ are involved in constructing groups that are isomorphic to $\mathbb{Z}_{50} \times \mathbb{Z}_2$; the cocycles $z, 3z, 7z$, and $9z$ are

involved in constructing groups that are isomorphic to $\mathbb{Z}_{100}$; the cocycle 0 constructs the group $\mathbb{Z}_{10} \times \mathbb{Z}_{10}$; and the cocycle $5z$ is involved in constructing a group that is isomorphic to $\mathbb{Z}_{20} \times \mathbb{Z}_5$.

Moving on from the specific example of standard addition and the multiples of the standard carrying function, the goal is to generalize this notion of cocycles. To initiate the generalization, we introduce extensions. "An extension of the group O by the group T is an abelian group E such that T is a subgroup of E and the quotient group E/T is O" [1]. It is worth noting that each element of E can be expressed uniquely as $[a][b]$ with a in T and b in O. It is also worth noting that each extension E has its own associated cocycle z, where $z : O \times O \to T$ is given by $[0][b_1] + [0][b_2] = [z(b_1, b_2)][b_1 + b_2]$. Furthermore, each cocycle z establishes a group structure on the set of all elements of the form $[a][b]$. Specifically, the set of all elements of the form $[a][b]$ is an abelian group under the operation $[a_1][b_1] + [a_2][b_2] = [a_1 + a_2 + z(b_1, b_2)][b_1 + b_2]$. Associativity follows from the cocycle condition, the identity is guaranteed by the normalization condition, and commutativity is implied from calculations with the cocycle condition.

Now we can consider a function ϕ between two extensions E and E' with respective associated cocycles z_1 and z_2. We wish to determine that ϕ is an isomorphism of these extensions. In this determination, we subtract z and z' by the hypothesis of Proposition 5.2. This difference yields a new function $\delta h : O \times O \to T : \delta h(b_1, b_2) = h(b_2) - h(b_1 + b_2) + h(b_1)$, where $h : O \to T$ is a function such that $h(0) = 0$. This δh is called a coboundary. This definition, combined with the results of Proposition 5.2, implies the following: if ϕ is an isomorphism of the extensions E and E', then the difference of the associated cocycles is a coboundary.

Now that the framework is established in regards to extensions, they can be expressed in cohomological terms. Let $Z(O;T)$ be the set of cocycles, and let $B(O;T)$ be the set of coboundaries. It is determined that both of these groups are abelian and that $B(O;T)$ is a subgroup of $Z(O;T)$. Thus, we can define the cohomology group $H(O;T)$ as the quotient group $Z(O;T)/B(O;T)$. It can now be determined that the group $H(O;T)$ is isomorphic to the set of isomorphism classes of extensions of O by T (Theorem 6.6). This is because "Definition 4.3 establishes a function from the set of extensions to the group $H(O;T)$. Proposition 5.4 tells us that the function is well-defined. Proposition 5.2 tells us that the function is [one-to-one]. Proposition 4.4 tells us that the function is [onto]" [1].

Overall, the ideas of cohomology can be extended to groups that are not necessarily O and T. This can be done by substituting T for some abelian group A and some (not necessarily abelian) group G for O. We can examine the (not necessarily abelian) extensions of G by A, but we have to assume that A is a normal subgroup of E in order to consider the quotient group E/A. This ensures that A is abelian. Rather than considering the carrying function, we can consider the actions that the extensions induce given actions of G on A to generalize the notion of cohomology groups. Just as cohomology is integral in the study of generalized mathematical concepts, it is incredibly important in our understanding of elementary

mathematics. It is a powerful tool to unlock new mathematical discoveries and reinforce familiar concepts.

2 How Many Units Can a Commutative Ring Have? [3]

This article acknowledged a problem presented by László Fuchs in 1960: "Determine whether a given abelian group can occur as the group of units in a commutative ring" [3]. This problem remains open, however, and a general solution has yet to be obtained. The authors obtained a solution to Fuch's problem for a specific set of abelian groups; namely, finite abelian groups of order p, where p is an odd prime number.

Initially, the authors set out to answer the question posed in the title for finite cardinals, with "finite cardinal" defined as finite order. In other words, the authors started by examining finite abelian groups of units of commutative rings and the conditions that arise to produce an accurate answer to the question. We began with two lemmas, stated as follows:

Lemma 2.0.1. Let $\phi : A \to B$ be a homomorphism of commutative rings. If the induced homomorphism $\phi^\times : A^\times \to B^\times$ is [onto], then there is a quotient A' of A such that $(A')^\times \equiv B^\times$.

Lemma 2.0.2. Let K and L be finite fields of characteristic 2. The tensor product $K \otimes_{\mathbf{F}_2} L$ is isomorphic as a ring to a finite direct product of finite fields of characteristic 2. [Also], as $\mathbf{F}_2$-vector spaces, $\dim(K \otimes_{\mathbf{F}_2} L) = (\dim K)(\dim L)$.

Following these lemmas was a proposition that was proven by these lemmas. This proposition defined the condition on finite abelian groups in order for them to occur as the group of units in a commutative ring. It stated that for a finite abelian group G of odd order k, k is the number of units of some commutative ring R if and only if k is the product of numbers of the form $(2^{n_i} - 1)$ for some positive integers $n_1, ..., n_t$. This proposition prompted a further condition on finite abelian groups that occur as the number of units in a commutative ring; specifically, for an odd prime number p, G is a finite p-group, where G can be expressed as the finite product of cyclic groups of order p (by the definition of finite p-groups). The corollary that followed placed a further restriction on an abelian p-group G; namely, a finite abelian p-group G can occur as the group of units of a commutative ring R if anf only if p is a Mersenne prime number (p is of the form $2^n - 1$ for some n).

Now that we have an answer to the question for finite abelian groups of odd order, it is worth mentioning the answer to the question for groups beyond finite order. These results will not be explained in detail here; nevertheless, they are important to note. It was said first that "Every even number is the number of units in a commutative ring" [3]. In other words, any group G (not necessarily abelian) of even order can occur as the group of units of a commutative ring. The final result obtained stated that a group of infinite order

can occur as the group of units of a commutative ring.

Overall, this article proved a theorem regarding the number of units of a commutative ring. In the context of the article, this makes a remark about the orders that groups (not necessarily abelian) can have to occur as the groups of units of commutative rings: for a cardinal number p that denotes the order of a group G, p can be an odd number denoted by the finite product $\prod_{i=1}^{t}(2^{n_i}-1)$, p can be an even number, or p can be an infinite cardinal number.

3 What Happens When the Division Algorithm Almost Works [4]

This article examined an immensely important topic in group theory and ring theory: the division algorithm. The authors did not, however, focus on the standard division algorithm. Rather, they identified a weaker version of the division algorithm to produce a special example under specific conditions.

The modified division algorithm, or the "almost" division algorithm, was stated as follows:

Definition 3.1. A subring R of $K[X]$, with $K \subseteq R$, has an almost division algorithm of index m (where $m \in \mathbb{N}$) if it satisfies the following property. If $f(X)$ and $g(X)$ are in R with $g(X) \neq 0$, then there exist polynomials $h(X)$ and $r(X)$ in R such that

$$f(X) = h(X)g(X) + r(X)$$

where

(d1) $r(X) = 0$

(d2) $\deg r(X) < \deg g(X)$, or

(d3) $\deg r(X) = \deg g(X) + i$ for $1 \leq i \leq m$.

This definition prompted the following theorem:

Theorem 3.0.1. Let R be a subring of $K[X]$ with an almost division algorithm index of m and I a proper ideal of R. There exist polynomials $f_1(X), ..., f_{m+1}(X)$ such that

$$I = (f_1(X), ..., f_{m+1}(X)).$$

Thus, R has the $m+1$ property on ideals.

Moving forward, we will need to define semigroups and monoids, as their definitions were excluded in this article. A semigroup is a nonempty set with a binary operation, and a monoid is a semigroup with an

identity element. Letting $\mathbb{N}_0$ denote the positive integers, it is claimed that for some additive submonoid S of $\mathbb{N}_0$, S can be generated by $n_1, ..., n_k$ where $n_1, ..., n_k$ are elements of $\mathbb{N}_0$. This generation is given by a linear combination of $x_i's$ and $n_i's$ where both x_i and n_i are elements of $\mathbb{N}_0$. Furthermore, if $n_1, ..., n_k$ are relatively prime, then S is primitive. The previous theorem and the notion of primitive semigroups prompted a propostion that ultimately showed that the rings $K[X;S]$ are made of all the polynomials $f(X)$ from $K[X]$ with exponents from the semigroup S. The notion of Frobenius numbers was introduced to prompt an important theorem that stated that for a field K and a primitive semigoup S, the ring $K[X;S]$ has an almost division algorithm index of $F(S)$ The Frobenius number, $F(S)$, of a semigroup S is the largest number that is missing from S before all of the elements of S are generated in consecutive order. Similarly to the previous proposition regarding the generator property of a ring R on ideals, furthermore, the corollary following the aforementioned theorem states that the ideals of $K[X;S]$ have at most the $F(S)+1$ generator property.

Overall, the contents of this article prompted the following proposition:

Proposition 3.0.2. Let K be a field, $n > 1$ a positive integer, and $S = \langle n, n+1, ..., 2n-1 \rangle$ a numerical semigroup. The integral domain $K[X;S]$ has the n but not the $n-1$ generator property.

The proof is centered around a $K-$vector space V generated by the linearly independent elements $X^n, ..., X^{2n+1}$.

4 On Polynomial Rings with a Goldbach Property [5]

The motivation of this article stemmed from the observations made by mathematician David Hayes in 1965. In his research, he discovered that when an integral domain $R = \mathbb{Z}$, every element of the polynomial ring $R[T]$ of degree greater than or equal to one can be expressed as the sum of two irreducible polynomials in $R[T]$ of the same degree. This property of $\mathbb{Z}$ is analogous to the conventional Goldbach conjecture, and it prompted the following definition that was used throughout the article.

Definition 4.1. ($\star$) Property: Every element of $R[T]$ of degree $n \geq 1$ can be written as the sum of two irreducible polynomials of degree n.

David Hayes only observed the ($\star$) property for the integral domain $\mathbb{Z}$. In his proof, furthermore, he showed that this property holds whenever R is the polynomial ring $F[x]$ for some field F (R has infinitely many maximal ideals). The author, however, worked to find which integral domains have the ($\star$) property in general; specifically, he wanted to loosen the requirement on R so that the ideals of R would be finitely generated.

Moving forward, it is important to note two assumptions that the author made for the duration of the article:

1. An element of $R[T]$ is irreducible if it is not a unit and cannot be factored as the product of two non-units.

2. All rings mentioned are commutative with an identity element.

The definition of the $(\star)$ Property, combined with the motivation for the article, prompted the following two theorems to be proven. It is important to note, as well, that the Noetherian condition cannot be removed because it implies that the ideals of R are finitely generated as desired.

Theorem 4.0.1. Suppose that R is an integral domain which is Noetherian and has infinitely many maximal ideals. Then R has property $(\star)$.

Theorem 4.0.2. If S is any integral domain, then $R = S[x]$ has property $(\star)$.

The argument for these theorems was developed through the use of Eisenstein's criterion and the Chinese Remainder Theorem for Rings. Both of these were used to craft another theorem to aid in the proofs of theorems 1 and 2.

Theorem 4.0.3. Suppose that R is an integral domain possessing distinct maximal ideals P and Q for which the following hold:

1. $P^2 \neq P$ and $Q^2 \neq Q$.

2. $\#R/P > 2$ and $\#R/Q > 2$.

Then R has property $(\star)$.

The proof of theorem 1 was derived through two lemmas that verified the hypotheses of theorem 5. Once R in theorem 1 was shown to satisfy the hypotheses of theorem 5, it was determined to have the property $(\star)$. The proof of theorem 2 was also derived with the use of theorem 5. Overall, it was shown that an integral domain with infinitely many, finitely generated, ideals has the property $(\star)$. Venturing beyond the scope of this article, several open problems remain in regards to cases when the structure in question is a field.

5 Finding the Finite Groups of Symmetries of the Sphere [6]

When considering a traditional sphere in three dimensions, it can be seen that its symmetry group has infinite order: any number of rotations and reflections, as long as the location of the center is maintained,

will create an identical image of the sphere. The focus of this article was to determine the finite subgroups of this infinite group of symmetries. In an effort to do so, the author, Marjorie Senechal, made use of Klein's method to determine the finite subgroups of rotations of the sphere. She used such findings to consider the behavior upon introduction of a reflection to uncover the remaining possibilities.

Senechal initially provided the intuition for her argument with an analogy to the previously-known finite subgroups of $O(2)$ (the symmetry group of a circle). I was tasked with detailing the answer that was given in the article: the two families of finite subgroups of $O(2)$ are cyclic groups of finite order n generated by rotations about the circle's center and dihedral groups with $2n$ elements generated by a rotation of order n and a reflection for some finite n. This is the conclusion that I was also able to draw, and it outlined the process that was used to find the finite subgroups of $O(3)$ (the symmetry group of a sphere); namely, first consider the finite subgroups of only the rotations of $O(3)$, the subgroup denoted $SO(3)$. Then, consider an element not in $SO(3)$ (some reflection), and note how it interacts with the rotations to determine the remaining possibilities. Although I was not able to digest all of the finer details of this article, I was able to grasp the general intuition for this process. I feel that it will serve me well moving forward. The next section is connected to this one, as it is my solution to the question posed: what are the finite subgroups of $O(2)$?

6 Finite Subgroups of O2 (my solution)

6.1 Introduction

I was posed the following question: What are the finite subgroups of $O(2)$? This $O(2)$ is defined as the "rigid symmetries of a circle." It is known that $O(2)$ is generated by rotations and reflections about a fixed center point (the center of the circle). This fixed point implies that we do not consider translations. Furthermore, I was given the following rules for the composition of operations in the group $O(2)$: a rotation composed with a rotation is a rotation; a reflection composed with a reflection is a rotation; and reflections composed with rotations (in either order) are reflections.

From [6], there are two families of finite subgroups of $O(2)$. One is the family of cyclic groups generated by a rotation about the circle's center. The second is the family of dihedral groups of regular n-gons contained in the circle, centered about the circle's center.

6.2 Claims that give us the families of the finite subgroups

From information from an online pdf that I found to help my answer this question [7], I was able to develop the following two claims to verify the statements made in [6]. My proofs were adapted from the information found in both [7] and [8]. Moving forward, furthermore, let a be a rotation and let b be a reflection.

1. Considering the group of rotations of a circle $SO(2) \subset O(2)$, any finite subgroup H of $O(2)$ is cyclic.

   Proof. Assuming H is non-empty and non-trivial, let a_θ be a rotation in H with $0 \leq \theta < 2\pi$. Since H is non-empty and non-trivial, choose an element a_ϕ in H to be the smallest possible rotation ($\phi > 0$). Then, $\theta = n\phi + \varphi$ for some n with $0 \leq \varphi < \phi$. Also, define $a_{n\phi} = (a_\phi)^n$, as is customary. Then, $a_\theta = a_{n\phi+\varphi} = (a_\phi)^n a_\varphi$.

   However, since $0 \leq \varphi < \phi$ and ϕ is the smallest angle greater than 0, φ must equal 0. So $a_\theta = a_{n\phi} = (a_\phi)^n$ since $a_\varphi = a_0$ is a trivial rotation. Thus, every rotation can be generated by a_ϕ, so $H = \langle a_\phi \rangle$, so H is cyclic. □

2. If G is a finite subgroup of $O(2)$ that is not contained in $SO(2)$, then it is a dihedral group.

   Proof. Since G is not contained in $SO(2)$, let G have a reflection b such that $b^2 = e$. If we consider $G \cap SO(2)$, we will have a cyclic group of finitely many rotations as described in (1.). Let a rotation $a \in G \cap SO(2)$ have order n for some n. Given the rules for the composition of operations (from the introduction), a reflection composed with a reflection is a rotation. Thus, for two distinct reflections b and c with $b^2 = e$ and $c^2 = e$, we have that $bc = a^k$ with $0 \leq k < n$. Then, $b = a^k c^{-1}$, so $b = a^k c$, so every new reflection in G is generated by a rotation composed with a reflection.

   Now, we have that $G = \{e, a, a^2, ..., a^{n-1}, b, ab, ..., a^{n-1}b\}$. Furthermore, since we know that a reflection composed with the same reflection is the identity and that a reflection composed with a rotation is a reflection, we have that $(ba)(ba) = e$. This implies that $ba = a^{-1}b$. Thus, G is a dihedral group with $2n$ elements, as desired. □

6.3 Final Answer

Overall, it was found that there are two classifications for the finite subgroups of $O(2)$.

1. A finite subgroup of $O(2)$ will be cyclic if it is generated by some rotation of $2\pi/n$ radians about the center of the circle for some finite number n.

2. A finite subgroup of $O(2)$ will be a dihedral group with $2n$ elements if it is generated by a rotation of order n and a reflection for some finite number n.

7 On Goldbach's Conjecture for Integer Polynomials [9]

The classic Goldbach conjecture from 1742 proposed that every even integer greater than three could be written as the sum of two prime numbers. While this conjecture currently remains open, several mathematicians have tried to prove it or formulate proofs of analogous situations to learn more about it. This article chose the latter: it began with a shortened proof of a theorem developed by Hayes in 1965 regarding integer polynomials and then moved to a more general interpretation of Hayes' theorem.

Hayes' theorem stated the following.

Theorem 7.0.1. If $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ with $\deg(f) = d \geq 1$, then there exist irreducible monic polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ with the property that $f(x) = g(x) + h(x)$.

The proof of this theorem was done using Eisenstein's Criterion for irreducibility, along with the Chinese Remainder Theorem, to provide an explicit decomposition of $f(x)$. It was briefly stated, furthermore, that this theorem holds true if it is modified to say that $f(x)$ is some arbitrary polynomial in $\mathbb{Z}[x]$ with $\deg(f) \geq 1$.

Now, we have the following theorem, the purpose of the article:

Theorem 7.0.2. If $f(x)$ in $\mathbb{Z}[x]$ is monic with $\deg(f) \geq 1$, then there exists a constant $A(f)$ depending only on d and the coefficients of $f(x)$ such that

$$\Re(f; y) > A(f)y^d$$

as $y \to \infty$. Here, $\Re(f; y)$ denotes the number of ways that a given monic polynomial $f(x)$ can be written as $f(x) = g(x) + h(x)$, with $g(x)$ and $h(x)$ being irreducible polynomials with integer coefficients g_i and h_j, respectively. These coefficients have a restriction: $|g_i| \leq y$ and $|h_j| \leq y$. Note, also, that Theorem 7.0.1 implies that $\Re(f; y) \geq 1$ as $y \to \infty$.

The proof of this theorem followed the argument from Theorem 7.0.1 as well as the following corollary:

Proposition 7.0.3. For any coprime integers a and b with $|a| < |b|$, there exist a u and v in $\mathbb{Z}$ such that $1 = au + bv$. The number of solutions (u, v) with $|u|, |v| < y$ is at least $[\frac{2y+1}{b}]$.

The conclusion was drawn from counting all of the ways to choose the two $(d-1)$-tuplets $(G_0, ..., G_{d-2})$ and $(H_0, ..., H_{d-2})$, where $pG_i + qH_i = F_i$ for prime integers p and q. Using Theorem 7.0.1 and the

Chinese Remainder Theorem, the desired result was obtained. Furthermore, $A(f)$ was found explicitly to be $\frac{2^{d-2}}{(|F_{d-1}|+2d)^d} \prod_{0\leq i\leq d-2, F_i\neq 0} \frac{1}{F_i}$. A final remark was made to obtain the overall result of the article: "The total number of monic polynomials of degree d with integer coefficients whose absolute values are bounded by y is $(2y+1)^d$. Hence, trivially $\Re(f;y) < By^d$, where B is a constant depending only on d. Thus, from [Theorem 7.0.2] we are able to deduce a Chebyshev-type estimate: $y^d \ll_f \Re(f;y) \ll_f y^d$" [9]. Here, $\ll_f$ denotes that the constant could depend on the degree and coefficients of the given polynomial $f(x)$.

There were some concluding remarks made regarding the extension of these results to Goldbach's original conjecture. The general consensus was that matters would be complicated yet not impossible. This article serves to exemplify the usefulness in making analogies in mathematics. When a posed problem seems unsolvable, it can be incredibly productive to consider a similar, more simplified problem. With the simpler solution in mind, one can begin to try to extend this solution to the broader problem. Overall, it can bring us one step closer to the overarching solution.

8 A Matrix Approach to Zero-Divisors in $R[x]$ [10]

Zero-divisors are important in the study of ring theory. In the scope of undergraduate study of ring theory, zero-divisors give us information about the invertibility of elements in rings; namely, if an element is a zero-divisor, it is not invertible. They also serve as a distinction between commutative rings and integral domains, for a commutative ring with zero-divisors cannot be an integral domain by definition. This serves an important distinction, as integral domains open the door for studying divisibility. Without zero-divisors, inverses can exist, so cancellation can occur. To highlight the importance of zero-divisors, the author of this article took an approach through linear algebra.

The following theorem served as the starting point for the matrix approach that was outlined in this article.

Theorem 8.0.1. Let R be a commutative ring, and let x be an indeterminate. If $g \neq 0$ and f in $R[x]$ are such that $gf = 0$, then there exists a nonzero r in R such that $rf = 0$.

The conventional proof was cited from author W.R. Scott and was commended for being "admirably succinct" [10]. While it is direct and short in length, this proof does not provide a great deal of visualization in regards to the reason that it works. The author of this article aimed to combat this issue by evaluating the same situation under the lens of a matrix-theoretic result. Let us start by defining the terminology in the article.

Definition 8.1. (Terminology)

1. A submatrix of an $m \times n$ matrix $A = (a_{ij})$with entries from R is a matrix obtained by deleting some (possibly none) of the rows and columns of A.

2. An order p subdeterminant of A is the determinant of a square $p \times p$ submatrix of A.

3. The columns of A are linearly dependent if there exists a nonzero $n \times 1$ column vector $\mathbf{v}$ such that $A\mathbf{v} = \mathbf{0}$.

4. The adjoint of A (adj$A$) is defined in the classical sense as the transpose of the cofactor matrix of A.

5. For an $(n-1) \times n$ matrix B, B_i is the submatrix obtained by deleting the ith column $(1 \leq i \leq n)$. Let $d_i(B) = (-1)^i \det B_i$, and let $\mathbf{d}(B) = (d_1(B), ..., d_n(B))^T$.

6. For any $1 \times n$ row vector $\mathbf{a}$, we have the $n \times n$ matrix $B_{\mathbf{a}} = \begin{pmatrix} B \\ \mathbf{a} \end{pmatrix}$

7. Expanding $\det B_{\mathbf{a}}$ by the elements of $\mathbf{a}$ gives us $\mathbf{ad}(B) = \pm \det B_{\mathbf{a}}$.

Following the abundance of terminology, we arrive at the Dependence Theorem.

Theorem 8.0.2. The columns of an $m \times n$ matrix A with $m \geq n$ are linearly dependent if and only if there exists a nonzero r in R such that r annihilates all order n subdeterminants of A.

This theorem was proven using the following three propositions:

Proposition 8.0.3. (Propositions for Dependence Theorem)

1. If $\mathbf{v}$ is an $n \times 1$ column vector satisfying $A\mathbf{v} = \mathbf{0}$, then every coordinate of $\mathbf{v}$ annihilates every order n subdeterminant of A.

2. If $m \geq n > 1$ and an element r of R annihilates all order n subdeterminants of A, then $A[r\mathbf{d}] = 0$ for each $(n-1) \times n$ submatrix B of A.

3. If A is an $m \times n$ matrix with $m \geq n > 1$ and if there exists a nonzero r in R such that r annihilates all order n subdeterminants, then there exists an $(n-1) \times n$ submatrix B of A such that $r\mathbf{d}(B)$ is a linear dependence vector for the columns of A.

There was also a short proposition following this theorem that generalized linear dependence further to the case where $m < n$ for an $m \times n$ matrix A. After the foundation was laid, the notion of diagonally constant matrices came to light. These are matrices whose diagonal entries follow the rule $a_{ij} = a_{i-1j-1}$ for $1 < i \leq m$ and $1 < j \leq n$. Introducing diagonally constant matrices is of vital importance to the purpose of

this article, as a lower triangular diagonally constant matrix is involved in multiplying two polynomials in $R[x]$. Explicitly, for

$$\begin{aligned} f &= a_0 + a_1x + ... + a_px^p \\ g &= b_0 + b_1x + ... + b_{n-1}x^{n-1} \\ fg &= c_0 + c_1x + ... + c_{n+p-1}x^{n+p-1} \\ c_0 &= a_0b_0 \\ c_1 &= a_1b_0 + a_0b_1 \\ c_2 &= a_2b_0 + a_1b_1 + a_0b_2 \\ c_3 &= ... \end{aligned}$$

we have $\mathbf{c} = A\mathbf{b}$ where A is lower triangular and diagonally constant. Furthermore, $gf = 0$ if and only if $A\mathbf{b} = \mathbf{0}$ (i.e. if and only if the columns of A are linearly dependent). From this observation, we arrive at the desired result that was outlined in the opening theorem.

Proposition 8.0.4. If f in $R[x]$ is a zero-divisor in $R[x]$, then there exists a nonzero r in R such that $rf = 0$.

This article, overall, serves to support a statement that has been cited by Professor Isaksen: all of math is counting and linear algebra. In this, case, a familiar abstract algebraic concept can be viewed in the scope of linear algebra and the concept of linear dependence. Linear algebra provided a clearer picture of the proof of the first theorem, as was the goal of the article. We were able to see explicitly how the polynomial multiplication behaved to provide the desired result. Ultimately, the idea that using an alternate branch of mathematics to revisit a familiar concept can uncover deeper insight was reinforced.

9 Groups as Unions of Proper Subgroups [11]

This topic appears to be of significance in the current study of group theory. While an impressive amount of progress has been made towards classifying the requirements for groups to be unions of proper subgroups, several open questions remain in this article. As a result, I was tasked with conducting a brief literature search within *The American Mathematical Monthly*. This literature search was devised to see which other authors' works cited this article and/or acknowledged an unanswered question from this article. The results of the literature search, as well as the subject matter of this article, will be outlined below.

The author began with a theorem derived from a relevant question in the 20th Century: when is a group

the union of two of its proper subgroups? As answered by the theorem that followed, this can never be the case. Naturally, then, a new question arose: can a group be the union of three of its proper subgroups. Unlike in the aforementioned question, this can be the case.

Theorem 9.0.1. (Scorza) A group is the union of three proper subgroups if and only if it has a quotient isomorphic to $C_2 \times C_2$, where C_2 denotes the cyclic group of order 2. This result was shown by partitioning the group G into seven parts (S_A, S_B, S_C, and all of their intersections). By claiming that $S_{AB} = S_{BC} = S_{AC} = \phi$, it was shown that S_A, S_B, S_C, and S_{ABC} form the four cosets of S_{ABC}. Thus, $G/S_{ABC} \cong C_2 \times C_2$, so G is covered by $A \cup B \cup C$ for proper subgroups A, B, C of G.

In an effort to further generalize this result, Cohn and Tomkinson presented the following theorems.

Theorem 9.0.2. (Cohn) Let $\sigma(G) = n$ denote the case where G is the union of n proper subgroups, but it is not the union of any smaller number of proper subgroups. Now, let G be a group.

1. $\sigma(G) = 4$ if and only if $\sigma(G) \neq 3$ and G has a quotient isomorphic to S_3 or $C_3 \times C_3$.
2. $\sigma(G) = 5$ if and only if $\sigma(G) \notin \{3, 4\}$ and G has a quotient isomorphic to the alternating group A_4.
3. $\sigma(G) = 6$ if and only if $\sigma(G) \notin \{3, 4, 5\}$ and G has a quotient isomorphic to the dihedral group $D_5, C_5 \times C_5$, or W, where W is the group of order 20 having two generators a and b satisfying $a^5 = b^4 = e$ and $ba = a^2b$.

Theorem 9.0.3. (Tomkinson) There is no group G such that $\sigma(G) = 7$.

It can be observed that for $n \leq 7$, G can be represented as the union of proper subgroups if it is isomorphic to a certain finite group. It was pondered whether this could be generalized to larger n. This is the case, and it was stated in the following theorem.

Theorem 9.0.4. For any positive integer n, there exists a unique minimal finite set $S(n)$ of finite groups such that $\sigma(G) = n$ if and only if $\sigma(G) \notin \{3, 4, ..., n-1\}$ and G has a quotient isomorphic to some group $K \in S(n)$.

This result is useful, but it does not provide an efficient way to determine $S(n)$. Thus, Neumann worked to prove that for an irredundant union $\bigcup_{i=1}^{n} A_i$ and a group G, $[G : \bigcap_{i=1}^{n} A_i]$ is bounded by a finite constant $f(n)$ that only depends on n. Tomkinson refined this result to create a stricter bound on the index $[G : \bigcap_{i=1}^{n} A_i]$; namely, $[G : \bigcap_{i=1}^{n} A_i] \leq n!$. Through the use of this result, it was found that for some group $K \in S(n)$, $|K| \leq n!!$. Several attempts have been made to optimize the bounds $f(n)$ for different sizes of groups in $S(n)$, but it it largely left open (for $n \geq 5$).

Since this problem becomes significantly more difficult as n increases, it was asked whether Scorza's result was properly generalized. In an attempt to specify the generalization, the attention was turned to groups as unions of proper normal subgroups. The condition of normality was implied from Scorza's initial result, so it can be added without an issue. Thus, the following theorem and proposition were born.

Theorem 9.0.5. Suppose a group G is the union of its proper normal subgroups. Then $\eta(G) = p+1$, where $\eta(G) = n$ if G is the union of n proper normal subgroups but is not the union of fewer than n proper normal subgroups. Also, p is the smallest prime such that G has a quotient isomorphic to $C_p \times C_p$, if such a prime p exists. Otherwise, $\eta(G) = \infty$.

Proposition 9.0.6. A finite group is the union of proper normal subgroups if and only if it has a quotient isomorphic to $C_p \times C_p$ for some prime p.

These results provide a classification for all anti-simple finite groups. It remains open to completely classify anti-simple infinite groups, just as the last section of the article remains largely open. This section explores finite solvable groups as conjugate unions of proper subgroup, but much work still needs to be done to refine this topic.

Overall, this article did well to present important known results of this topic, as well as underlining a number of subtopics that require further analysis. This was the driving force of my literature search in the subsection below.

9.1 Literature Search in *The American Mathematical Monthly* and Beyond

There were four relevant articles that cited the preceding article in *The American Mathematical Monthly* and other journals contained in the *Mathscinet* database.

1. "On the covering number of symmetric groups having degree divisible by 6" [12] (2016) extends the focus to finite symmetric groups, not just arbitrary finite groups.

2. "Cyclic covering of a module over an Artinian ring" [13] (2016): I am not familiar with Artinian rings, but this also narrows the focus to a specific type of covering rather than a broader, more open idea.

3. "Covering numbers of finite rings" [14] (2015) extends the ideas presented in this article to find the minimum number of subgroups to achieve a group as the union of proper subgroups. This is known as the cover of a group.

4. "Coverings of finite groups by few proper subgroups" [15] (2010) was not available to view, but it appeared that the topic was specified to finite groups only.

10 Conclusion

In the beginning of this semester, my last semester at Wayne State University, I was not sure how to feel about moving forward. This semester, along with the idea of moving on to graduate school for mathematics afterwards, contained a great deal of uncharted territory for me. I was (and still am) immensely grateful for Professor Isaksen. He was continuously enthusiastic about my learning experience, and I wholeheartedly believe that he helped me to develop my math research skills. As a result, I feel significantly more prepared for the future of my mathematics education. Learning how to navigate through *Mathscinet* and adequately summarize new information will serve me well in my future education and career, and I feel that I have made strides in writing for mathematics, which I have not had to do in length before this directed study.

More importantly, this directed reinforced an idea that I had been doubting: I can do anything that I set my mind to. I feel like I can believe in myself more because I was able to conquer uncharted territory this semester like I have never had to before. This alleviated some of the stress that I was feeling toward my future. I appreciate the boost in morale and skill more than I can say. I will be forever thankful for this opportunity. I needed it more than I could have ever thought.

References

[1] Daniel C Isaksen. A cohomological viewpoint on elementary school arithmetic. *The American mathematical monthly*, 109(9):796–805, 2002.

[2] Group cohomology. Group cohomology — Wikipedia, The Free Encyclopedia, 2020. [Online; accessed 20-January-2020].

[3] Sunil K Chebolu and Keir Lockridge. How many units can a commutative ring have? *The American Mathematical Monthly*, 124(10):960–965, 2017.

[4] Scott T Chapman. What happens when the division algorithm "almost" works. *The American Mathematical Monthly*, 125(7):643–647, 2018.

[5] Paul Pollack. On polynomial rings with a goldbach property. *The American Mathematical Monthly*, 118(1):71–77, 2011.

[6] Marjorie Senechal. Finding the finite groups of symmetries of the sphere. *The American Mathematical Monthly*, 97(4):329–335, 1990.

[7] Chapter 14. Finite subgroups of the rotation group, n.d. Accessed 02-18-2020.

[8] Unknown author. Classification of finite rotation groups, n.d. Accessed 02-19-2020.

[9] Filip Saidak. On goldbach's conjecture for integer polynomials. *The American Mathematical Monthly*, 113(6):541–545, 2006.

[10] Jack Ohm. A matrix approach to zero-divisors in r [x]. *The American Mathematical Monthly*, 114(5):444–450, 2007.

[11] Mira Bhargava. Groups as unions of proper subgroups. *The American Mathematical Monthly*, 116(5):413–422, 2009.

[12] Eric Swartz. On the covering number of symmetric groups having degree divisible by six. *Discrete Mathematics*, 339(11):2593–2604, 2016.

[13] Otávio JNTN dos Santos and Irene N Nakaoka. Cyclic covering of a module over an artinian ring. *International Journal of Algebra and Computation*, 26(04):763–773, 2016.

[14] Nicholas J Werner. Covering numbers of finite rings. *The American Mathematical Monthly*, 122(6):552–566, 2015.

[15] Yakov Berkovich. Coverings of finite groups by few proper subgroups. *Glasnik matematički*, 45(2):415–429, 2010.