An Introduction to Finite Group Theory

A Thorough Guide to the Fundamental Tools of Mathematical Symmetry

Edmonton, Alberta, Canada

Jacob Denson

2015

Table Of Contents

CHAPTER 1

What is a group?

Group theory is the theory of symmetries. In it simplified form, mathematics is naturally tailored towards symmetry. Symmetry simplifies problems, unveiling their underlying beauty. Below are two problems which attack a problem using symmetry. The methodology behind these problems will be established later in the book.

In 1761, Leonard Euler investigated the following number theoretic mapping. Take the totient function $\varphi : \mathbf{N} \to \mathbf{N}$, which maps a positive integer n to the number of relatively prime positive integers that are less than or equal to n. (a number is relatively prime to another number if they share no common factors). A few examples are below, with the set of relatively prime integers included.

$$\begin{aligned} \varphi(1) &= 1 & \{1\} \\ \varphi(10) &= 4 & \{1,3,7,9\} \end{aligned}$$

The totient function has many interesting properties. For instance, if p and q are two numbers that are relatively prime to one another, then $\varphi(pq) = \varphi(p)\varphi(q)$. Euler most interestingly showed that, for any two relatively prime integers a and b,

$$a^{\varphi(b)} \equiv 1 \pmod{b}$$

The idea of Euler's proof shows that the arithmetics of the integer multiples of a are symmetric to the arithmetic of the numbers relatively prime to b, which shows the two sets can be seen as identical. We uncover a symmetry between the two sets of objects which gives us the theorem for free.

Another problem which we have know since high school is finding roots of polynomial equations: values of x such that, for some specific specific sequence of other real numbers $(a_n, a_{n-1}, \ldots, a_1)$, we have the equality

$$a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0 = 0$$

The fundamental theorem of algebra shows every polynomial has at least one root in the complex plane. Practically, however, there is no general method to

finding these numbers; the fundamental theorem only affirms the existence of these roots.

One may remember learning that for a 'quadratic' polynomial, which we can write as

$$a_2x^2 + a_1x + a_0$$

there is a simple strategy of finding all roots of the polynomial. Simply plug the values of a_2, a_1, and a_0 into the formula

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2a_0}}{2a_2}$$

and the values of x generated are exactly the roots for the polynomial. When working with quadratics, this equations saves us a lot of effort. Thus, a natural question is whether there is a general 'quartic' formula to solve polynomials of the form

$$a_3x^3 + a_2x^2 + a_1x + a_0$$

and to extend the task even further, formulas for polynomials of higher degree.

In the 1500s, the mathematicians del Ferro, Cardano, and Tartaglia found one formula that would solve all degree 3 equations. Subsequently, Cardano's student Ferrari found a formula for all degree four equations. Unlike the quadratic equation the formulae are far too complicated to be memorized. For the next 300 years attempts were made to find further equations for larger polynomials. Unfortunately, a formula for polynomials of higher degree has never, and cannot ever, be found. Everiste Galois in the 1800s explored polynomial equations to determine the impossibility of a general formula for polynomials of degree five or higher. How was Galois able to prove this remarkable theorem? His idea was in finding a deep connection between permutations of roots of polynomials and the formation of an elementary formula to find these roots. Though this report will not get into solving this problem, the framework we will establish can be extended to solve this problem. One may go on to study 'Galois Theory' once one has a firm understanding of the theory of groups.

How do these problems connect? Both found interconnections between sets of objects that behave in a structured way. We call these mappings 'Symmetries' because of the similarity to the harmonious symmetries of geometry. The generalized consideration symmetries is what we study in the theory of groups. In this report we introduce the theory, focusing mainly on the finite case. Reader's should have experience with linear algebra from an abstract mindset, as well as knowledge of general mathematical structures that are commonplace in all mathematics. Aside from these easily testable skills, possessing the ineffable concept of 'mathematical maturity' will be integral in the sequel.

CHAPTER 2

Operations and Groups

Groups are a way to generalize the notion of a set with a well behaved operation. This operation gives us a relational structure between objects in the set. Examples include numbers, whose relational operations are inherent, and compositions of geometric symmetries of a shape. Since groups were defined in 1882 by Walter Dyck, the algebraic theory has arisen to become one of the largest fields in modern mathematics: abstract algebra. The power obtained from the simple definition of a group is that any proof in the system translates to a large number of specific objects. The first course of action to introducing our theory is of course to find the prerequisites with which we can rigorously describe the property of the 'well behavedness' of our structure.

Groups are intimately connected to the operations that define them. Thus, before we define a group, we must rigorously define what an operation is. Operations like addition and subtraction are mathematical structures that we use in everyday life. Thus, abstracting the general properties of operations is quite difficult for us to think of, as we are blinded by the everyday experience of using the operations. The formal definition is simple after a use of the set-theoretic concept of a function.

Definition 1. A **law of composition** or **assignment** on a set S is a function from $S \times S$ to S.

Think of an operation as a way of combining two elements of S into a new element in S. In our definition we have inherently incorporated the property of **closure**; the composition of any objects from the set S lies inside the set S.

If a and b are arguments to an assignment, we avoid using conventional symbols such as f or g for the assignment; formulas such as $f(a,b)$ and $g(a,b)$ are too clunky compared to the more elegant and suggestive notation (ab), $(a \circ b)$, or $(a+b)$. We put the symbol in the middle rather than at the front to maintain our intuititive view of operations. Good notation can make working with complex ideas much simpler.

When dealing with operations on numbers, formulae involving multiple numbers such as $1+5-7$ and $4\cdot 2\cdot 3$ are commonplace. The product of more than two elements is implicit, unlike in our definition of operation. Let us define this in our abstract opertion. Consider a given finite sequence of elements $(x_1, x_2, \ldots, x_n)$. Then the 'Pi' notation for a product of these elements is recursively defined as

$$\prod_{j=i}^{n} x_j = \left(\prod_{j=1}^{n-1} x_j\right) x_i$$

$$\prod_{j=i}^{i} x_j = x_j$$

The similarity to Σ notation used in arithmetical sums is intensional.

There are many rules for products, and it would be too pedantic to list them all. One example is that

$$\prod_{k=1}^{mn} x_k = \prod_{i=0}^{m-1} \prod_{j=1}^{n} x_{nm+j}$$

Properties such as the one above will be used inherently in our proofs. Consider it an exercise to extract all implicit uses of these rules, and proof them.

Unfortunately, the generality of our definition of an operation is too general for our future studies. Mathematically, the more general the theory one studies, the less facts one can obtain that apply to all objects. The set of all operations is thus too general to be studied in totality. Even when we narrow down functions to assignments, our study is too general. Thus we must specify subclasses of assignments which may prove more interesting. We take properties of common operations as inspiration.

The first problem with our definition of assignment is that it only considers combinations of pairs. Thus given a set of three elements abc, it is ambiguous whether to combine b and c first, then a, or to first form a and b together. For an arbitrary operation, this choice is integral to the outcome of the formula, as the resultant elements may differ based on the choice. We refine the operations of study so this problem never will be a worry.

Definition 2. An assignment on a set S is **associative** if, for any three elements a, b, and c in the set S,

$$a(bc) = (ab)c$$

so that we may operate them in any order we choose.

With this definition, we introduce our first algebraic structure – a set with a specialized set of operations. The main use of this definition will be more of a supplement to the concept of a group to make further theorems more elegant to state. The definition is still too general to obtain much intersting material, but it is still important to the development.

Definition 3. A **semigroup** is a set possessing an associative operation.

Ultimately, the property of associativity means brackets in an equation are irrelevant. We prove this rigorously, and then avoid using brackets for the rest of the report except for emphasizing segments of equations.

Theorem 2.1. Let there be given a semigroup S, and a finite sequence $(x_1, x_2, \ldots, x_n)$ of elements in S. Then, for any positive integers l and m such that $l + m = n$, it can be shown that

$$\Big(\prod_{k=1}^{l} x_k\Big)\Big(\prod_{k=1}^{m} x_{l+k}\Big) = \prod_{k=1}^{n} x_k$$

Proof. We prove by induction on n, the number of elements in the sequence $(x_1, \ldots, x_n)$. When $n = 1$, the statement is vacously true; there are no positive integers l and m such that $l + m = 1$. When $n = 2$, we have two elements x_1 and x_2. It of course follows that the only positive values of l and m that sum to two are $l = 1$, $m = 1$, and through a calculation,

$$\Big(\prod_{k=1}^{1} x_k\Big)\Big(\prod_{k=1}^{1} x_{k+1}\Big) = x_1 x_2 = \prod_{k=1}^{2} x_k$$

hence the theorem holds for $n = 2$. Now suppose for our inductive argument that for any sequence of $n-1$ elements, the statement to be proved holds, where $n - 1 \geqslant 2$. Consider a sequence of n elements $(x_1, x_2, \ldots, x_n)$ and two positive numbers l and m such that $l + m = n$. The following calculation below proves the statement needed, where $m \geqslant 2$ (and when is this used?). The case where $m = 1$ follows the same strategy, but is left for the reader to fill in.

$$(1) \qquad \Big(\prod_{k=1}^{l} x_k\Big)\Big(\prod_{k=1}^{m} x_{l+k}\Big) = \Big(\prod_{k=1}^{l} x_k\Big)\Big(\Big(\prod_{k=1}^{m-1} x_{l+k}\Big)\, x_m\Big)$$

$$(2) \qquad = \Big(\prod_{k=1}^{l} x_k \prod_{k=1}^{m-1} x_{l+k}\Big)\, x_m$$

$$(3) \qquad = \Big(\prod_{k=1}^{n-1} x_k\Big)\, x_m$$

$$(4) \qquad = \prod_{k=1}^{n} x_k$$

Here (1) follows by definition of Pi notation, (2) follows from the associativity law, (3) results from the inductive hypothesis, and (4) again from the definition of the notation. By induction, this statement holds for all values of n. □

An operation of multiple of the same object can be described in a way that should be familiar. Given a positive integer n, we can describe the exponential of the assignment on an element a as

$$a^n = \prod_{i=1}^{n} a$$

The following lemmas are obvious results of the exponential's definition in relation to Pi notation. However, they will be used inherently in future calculations, and thus must be explicity stated. Proofs are left as an exercise.

Lemma 2.2. For any two integers n and m, and any element a in a semigroup,

$$a^{n+m} = a^n a^m$$

Lemma 2.3. For any two positive integers n and m, and for any element a,

$$(a^n)^m = a^{nm}$$

Another property of assignments is a powerful characteristic of the integers, generalized to arbitrary operations.

Definition 4. An assignment on a set is **commutative** if, for any elements a and b in the set,

$$ab = ba$$

thus allowing pairs of elements to permute between one another.

The power of commutativity is that, given an associative and commmutative operation, we can permute any elements in an equation. Let us rigorously prove this.

THEOREM 2.4. For any finite sequence of elements $(x_1, x_2, \ldots, x_n)$ from a set upon which an associative and commutative assignment is defined, and for any permutation π on the numbers 1 to n,

$$\prod_{k=1}^{n} x_k = \prod_{k=1}^{n} x_{\pi(k)}$$

PROOF. We again prove by induction on the number of elements in the sequence. When the number of elements is one, the statement is obvious; the only permutation of one element is the identity permutation that leaves nothing changed. Now suppose by induction that the statement is true for an arbitrary permutation of $n-1$ elements. Let $(x_1, \ldots, x_n)$ be a sequence of elements, and π a permutation of the numbers in the range 1 to n. Let m be the number such that $\pi(n) = m$. The following calculation shows we can move x_m to the end of the product.

$$\prod_{k=1}^{n} x_k = \Big(\prod_{k=1}^{m-1} x_k\Big)\Big(x_m \prod_{k=m+1}^{n} x_k\Big) \tag{5}$$

$$= \Big(\Big(\prod_{k=1}^{m-1} x_k\Big)\Big(\prod_{k=m+1}^{n} x_k\Big)\Big)\, x_m \tag{6}$$

We transition from (5) to (6) by use of both the associativity and commutativity property of the assignment. Now, define a new permutation φ on the numbers between 1 and n by the piecewise formula

$$\varphi(x) = \begin{cases} x & x < m \\ x-1 & x > m \\ n & x = m \end{cases}$$

What follows is that, via a change of notation,

$$\Big(\prod_{k=1}^{m-1} x_k \prod_{k=m+1}^{n} x_k\Big)\, x_m = \Big(\prod_{k=1}^{n-1} x_{\varphi(k)}\Big)\, x_{\pi(n)}$$

As φ and π are permutations, so is $\pi \circ \varphi^{-1}$. If we restrict $\pi \circ \varphi^{-1}$ to only the numbers between 1 and $n-1$, we still have a permutation, because n is fixed in the permutation:

$$(\pi \circ \varphi^{-1})(n) = \pi(\varphi^{-1}(n)) = \pi(m) = n$$

Hence we can consider $\pi \circ \varphi^{-1}$ as a permutation of the numbers between 1 and $n-1$. By induction, and the fact that $(\pi \circ \varphi^{-1})(n) = m$, it follows that

$$\begin{aligned}\Big(\prod_{k=1}^{n-1} x_{\varphi(k)}\Big)\, x_{\pi(n)} &= \Big(\prod_{k=1}^{n-1} x_{(\pi\circ\varphi^{-1}\circ\varphi)(k)}\Big)\, x_{\pi(n)} \\ &= \Big(\prod_{k=1}^{n-1} x_{\pi(k)}\Big)\, x_{\pi(n)} \\ &= \prod_{k=1}^{n} x_{\pi(k)}\end{aligned}$$

Considering this process ad infinitum, we find that it is possible to reorder finite sequences of elements arbitrarily. □

Commutativity is in some sense too strong of a property to be studied. Though some operations we will study possess this, it will never implicitly hold unless we use $+$ as the symbol for our assignment. In addition, when addition is used as the operation Σ notation is used instead of Π notation, and the exponential a^n will be expressed as na. Algebraic objects that possess the quality of commutivity have the prefix **Abelian** or **Commutative** attatched to their name, after one of the great algebraists of the past, Niels Henrik Abel.

Via commutivity, an elementary theorem about the exponential arises. The same inductive strategy of previous proofs suffices to showing its correctness.

Lemma 2.5. If a and b are elements such that $ab = ba$, then

$$(ab)^n = a^n b^n$$

We have specified all of the 'global' properties of operations we will study in this report. There are more subtle 'local' properties that have not yet been mentioned. In particular, one property of addition and multiplication has not yet been mentioned. With addition, there is a number 0 such that, for any number x,

$$x + 0 = 0 + x = 0$$

Multiplication has a similar number with these properties, the 1 element. Both numbers are **idempotent**; that is, when we combine this number with any other number, the composition of the numbers stays the same. We generalize this concept to arbitrary operations in the following way.

Definition 5. An **identity** of a set S is an element e in S such that, for all other elements a in the set,

$$ae = ea = a$$

The symbol e is canonically used as the symbol for an element in an arbitrary group, and we say that it operates idempotently with the elements of the set.

Via the addition of the property of identity, we can refine the algebraic object of the semigroup.

Definition 6. A **monoid** is a semigroup that contains an identity.

Some easy examples are the positive integers under addition, the negative integers under addition, and so on. Extensive examples are not provided as the importance of the monoid structure is only to aid in the statement of theorems which relate monoids to groups. Here is the first such theorem.

Lemma 2.6. A monoid has a unique identity

Proof. Suppose a monoid has two identites, denoted e and e'. Because e is an identity, it holds that

$$ee' = e$$

Because e' is an identity, we obtain that

$$ee' = e'$$

By transitivity, we get the desired equality. □

If $\cdot$ is used as an operation's symbol, we write e as 1. If $+$ is used, we write the identity as 0. Though not used as numbers, The symbols 1 and 0 then become metaphors to help us think about the identity with more abstract operations.

For any monoid, we expand Pi notation with

$$\prod_{k=1}^{0} x_k = e$$

The exponential a^0 arises accordingly. The properties previously proved for exponentiation still hold. This follows as 0 is idempotent in addition,

$$a^0 a^n = ea^n = a^n = a^{n+0}$$

and zeroes out multiplication,

$$(a^0)^n = e^n = e = a^0 = a^{0n} \qquad (a^n)^0 = e = a^0 = a^{0n}$$

and thus properties of exponentiation hold quite naturally.

A further quality of addition and multiplication involves the interconnection between elements of the set. Given a number a, there is a number b such that $a + b = 0$. We typically use the symbol $-a$ for b, and write the operation more concisely as $a - a$. With multiplication, every non-zero element a has an number b such that $a \cdot b = 1$. We denote b as a^{-1} or $1/a$, and write the operation as a/a.

Definition 7. Given a monoid, we say an element a is **invertible** if there is another element b such that

$$ab = ba = e$$

the element b is normally denoted a^{-1} and called the **inverse** of a.

Intuitively, invertibility means that the action of operating with any element of the group is reversible. If $+$ is used for the operation, $-a$ is used for the inverse of the element a, and if $\cdot$ is used, $1/a$ might be used. This continues the metaphor established for identity elements. For an arbitrary assignment, the multiplicative notation a^{-1} is preferred.

Here are some properties common to all inverses in a monoid. Because of the monoid structure, we assume associativity, but not commutivity in the invertible operation. Proofs are abbreviated; we assume the reader can now handle the abstraction presented and hence can fill in the blanks between sentences of the argument.

Lemma 2.7. Let l and r and a be arbitrary elements of a monoid. If $la = e$ and $ar = e$, then $l = r$, and thus a is invertible.

Proof. For then it follows that $l = le = lar = er = r$. □

Lemma 2.8. For any element a in a monoid, a^{-1} is unique.

Proof. Lemma (2.6) shows any two inverses are the same, for if x and y are two inverses, substitute x for l and y for r in the statement above. □

Whenever we state that $a^{-1} = b$, we implicitly use the lemma above. If the lemma did not hold, we could have two inverses of a that were not equal, and hence the equation $a^{-1} = b$ would be misleading. The fact of the theorem above, though easy to prove, is important to any study of inverses.

We are now ready to state the fundamental description which will concern us for the rest of this report.

Definition 8. A **group** is a monoid where every element has an inverse.

The simplicity of the sentence that defines a group is deceiving. We are still discovering new things about groups over one hundred years after the theory's conception.

If $n < 0$, define $a^n = (a^{-1})^n$. Again, the previous exponential properties proved hold, but we leave it to the reader to show this.

Our first group theoretic properties result fairly easily from the definition. They all follow from the fact that the inverse of every element is unique. Let a and b be arbitrary elements of a group:

LEMMA 2.9. The inverse of an inverse of an element a is a. That is,

$$(a^{-1})^{-1} = a$$

PROOF. The proof follows because of the calculation

$$aa^{-1} = a^{-1}a = e$$

hence a is an inverse of a^{-1}, and is unique by Lemma (2.7). □

LEMMA 2.10. $(ab)^{-1} = b^{-1}a^{-1}$.

PROOF. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a = aea^{-1} = aa^{-1} = e$. □

LEMMA 2.11. Every equation $ax = b$ has a unique solution x.

PROOF. $x = ba^{-1}$ is a trivial solution, and is the only solution, as if x' is any other solution such that $ax = ax'$, then $a^{-1}ax = a^{-1}ax'$, which when evaluated gives us $x = x'$. □

An astute reader may have noticed we have skipped a possible algebraic structure of the road to the definition of a group. We could define left inverses of an element a: an element b such that $ba = e$, but where it is not necessarily true that $ab = e$, and define a 'psuedo-group' as a monoid possessing only left inverses. We show that the theory of the psuedo-group is no different to that of a group.

THEOREM 2.12. Any monoid where every element has a left inverse contains arbitrary inverses for an element, so that the monoid is a group.

PROOF. Let G be a monoid with the properties above, and suppose a is an arbitrary element of G. Then there is $b \in G$ such that $ba = e$. b also has a left inverse c such that $cb = e$. But then b has both a left and right inverse, so $a = c$ from Lemma (2.6). But that also means a has a right inverse when substituted for c, so b is the inverse of a. Since a was arbitrary, all elements are invertible, so G is shown to be a group. □

There are also many examples of groups. We list some interesting ones below. Begin by glancing through the bullets below; there are far too many examples to fully understand each and every one straight away. Instead, use this page as a reference for the groups we mention in later chapters. Right now just have a look at a choice few to get a feeling for what groups are:

- The set of integers, rational, real, and complex numbers under addition form the groups $\mathbf{Z}^+$, $\mathbf{Q}^+$, $\mathbf{R}^+$, and $\mathbf{C}^+$.

- The same sets with zero removed under the operation of multiplication form the groups $\mathbf{Z}^\times$, $\mathbf{Q}^\times$, $\mathbf{R}^\times$, and $\mathbf{C}^\times$.
- The set of bijective functions on a set X under composition form the symmetric group $S_{|X|}$. $S_{|X|}$ has a cardinality of $|X|!$, as this is precisely the number of bijective functions on the set.
- For a vector space V, the set of automorphisms under compositions form the general linear group $GL(V)$. An equivalent definition, if the vector space is dimension n in a field $\mathbf{F}$, is the set of invertible n by n matrices with entries in $\mathbf{F}$, which we denote $GL_n(\mathbf{F})$.
- Let S be a set, and G a group with operation $\cdot$. Then the set of functions from S to G form a group with operation $\circ$ defined by $(f \circ g)(x) = f(x) \cdot g(x)$. If f is in the group, f^{-1} is the set defined by $f^{-1}(x) = f(x)^{-1}$
- Consider an n-sided regular polyhedron (where regular means each side is equal). A symmetry on an n sided regular polyhedron is a distance preserving mapping between the edges of the shape. From this fact, each and every symmetry on the polyhedron can be considered a rotational symmmetry or a reflection symmetry. We have n of each kind of these symmetries, so the group formed by taking compositions of symmetries to form more symmetries forms the Dihedral group D_n of order $2n$. The transformational approach to geometry attempts to understand geometric properties of space in a group theoretic manner such as this.
- The quaternion group Q is equal to the set $\{\pm 1, \pm i, \pm j, \pm k\}$. One can work out all operations between elements from the following sequence of equations.

$$\begin{aligned} ij &= k & ji &= -k \\ jk &= i & kj &= -i \\ ki &= j & ik &= -k \end{aligned}$$

$$ii = jj = kk = -1$$

  Through these equations we have concisely presented the entire group to you. The presented group here is commonly used to represent three dimensional space in computer graphics.
- The Klein-4 Group or Viergruppe is a group with elements $\{a, b, c, e\}$, where for every element k in the group, $k^2 = e$, and such that $xy = z$ for any permutation (x, y, z) of (a, b, c).
- For any field $\mathbf{F}$, the set $\mathbf{F}^n$ with operation of addition forms an abelian group. In fact, a vector space is just an additive abelian group with scalar multiplication in addition!

The last few pages have introduced the basics of group theory, through which we can establish the complete theory discussed in the rest of the report. Additional tools developed in the last two centuries will be brought up when needed

to dissect the problems which arise when needed, but the main definitions have been brought to the attention of the reader.

Exercise 2.1. If G is a group such that, $x^2 = e$ for every element x, then G is abelian.

Exercise 2.2. In a group, one may specify the notion of identity elements and inverses by the property that any equation of the form $ax = b$ for two elements a and b has one and only one solution x. Prove that, in the case of a finite group, one can weaken the claim to the statement that $ax = b$ has a unique solution only if a solution exists.

Exercise 2.3. Let G be a finite abelian group written additively, with elements

$$\{x_1, x_2, \ldots, x_n\}$$

such that, for all elements $x \neq e$, $2x \neq e$. What is the value of

$$\left(\sum_{k=1}^{n} x_k \right)$$

Exercise 2.4 (Wilson's Theorem). If p is a prime number, prove that

$$(p-1)! \equiv -1 \mod p$$

One can prove the converse of Wilson's theorem, but we leave this for an aspiring number theorist rather than adding it as an additional exercise.

Exercise 2.5. A Latin Square is an $n \times n$ array such that any row and column is a permutation of a fixed set of n elements

$$\{x_1, x_2, \ldots, x_n\}$$

Given a finite group G of cardinality n, order elements of G by $(g_1, g_2, \ldots, g_n)$ and define an $n \times n$ array M by $M_{ij} = g_i g_j$. Prove that this is a latin square, and conversely, show that any latin square defines a finite group by a reverse of this construction.

CHAPTER 3

Subgroups, Generators, and Cosets

A mechanic understands a machine by deconstructing it into the various components from which the machine was built from. Likewise, we can understand a group by the various components that it contains. Most of this book will be attempting to define a group's components – they are not so evident as the gears of a car or the wheel that makes it turn. The first such component of a group we may find is a subgroup.

Definition 9. A **subgroup** H of a group G is a subset of G whose elements form a group sharing the same operation of G restricted to elements of H.

This is not the most conventional or useful definition of a subgroup. We state and prove the equivalency of the alternate definition below.

Theorem 3.1. A subset H of a group G is a subgroup if and only if for any two elements a and b in H, ab, a^{-1}, and b^{-1} are all in H.

Proof. Suppose H is a subgroup of G. Then of course if two elements a and b are in H, ab is in H, otherwise the operation of G restricted to H would not make sense. Furthermore, a^{-1} and b^{-1} are contained in H as otherwise H would not form a group. Thus any subgroup H satisfies these properties. Conversely, suppose H is a set with the alternate properties above. Since ab is in H whenever a and b are, it makes sense to restrict the operation of G to H. Because a is in H, a^{-1} is also in H, so we can let $b = a^{-1}$ in the property that H possesses to conclude $aa^{-1} = e$ is in H, so that H possesses an identity. The operation on H thus satisfies all of the properties that define a group, inheriting associativity from the operation on G, hence H is a subgroup of G. We conclude the two definitions are equivalent. □

There is a slight subtlety we miss in the proof above. We leave it to the exercises at the end of the chapter for the reader to fix this subtlety. Let us first consider some examples of subgroups.

- Given the general linear group $GL_n(\mathbf{F})$, define the special linear group $SL_n(\mathbf{F})$ to be the set of matrices in the general linear group with determinant one. The subgroup property follows as the determinant operation has the multiplicative property, so that if
$$\det(X) = \det(Y) = 1$$
it follows that
$$\det(XY) = \det(X)\det(Y) = 1$$
as well as
$$\det(X^{-1}) = \det(X)^{-1} = 1$$
- Let M be a set, and N a subset. Then the set of bijective functions on M that leave elements in N fixed is a subgroup of $S_{|M|}$. In some sense, this set of functions is equivalent to $S_{|M|-|N|}$ as the elements that are in N can be ignored in the definition of the function.
- Any group is a subgroup of itself, as is the set containing the identity. We call these trivial subgroups for self evident reasons.

Unexpectedly, we can verify subgroups based on a single statement, specified in the following lemma. We leave it to the reader to verify – the proof is just an unravelling of the definitions presented above.

Lemma 3.2. A non-empty subset H of a group G is a subgroup if and only if, for any elements a and b in H, ab^{-1} is in H.

Now we can get to the more specialized discoveries on subgroups. Here is a theorem that provides us with an extra tool to construct subgroups of groups.

Lemma 3.3. Let G be a group, and $(H_j)_{j\in\mathcal{J}}$ a family of subgroups. Then it follows that
$$\bigcap_{j\in\mathcal{J}} H_j$$
is also a subgroup of G.

Proof. If a and b are in $\bigcap_{j\in\mathcal{J}} H_j$, then they are in every group H_j, which means that (ab^{-1}) is in H_j for every H_j, hence (ab^{-1}) must be in the intersection of these groups. We conclude the intersection is a subgroup. □

Now let G be a group, and S a subset of that group. Take the set $\mathcal{M}$ to be the set of all subgroups of G which contain S. Of course, $\mathcal{M}$ is non-empty, as G is a subgroup which contains S. Suppose we can index $\mathcal{M}$ completely by an index set $\mathcal{J}$. We make the following definition.

Definition 10. Given a subset S of a group G, we define the subgroup generated by S to be the smallest subgroup that contains S, alternatively the intersection

of all subgroups that contain S. We denote the subgroup $\langle S \rangle$. We call S the **generator** of the group $\langle S \rangle$. If S is a finite group $\{s_1, s_2, \ldots, s_n\}$, we also write $\langle S \rangle$ as $\langle s_1, s_2, \ldots, s_n \rangle$.

Equivalently, the generated subgroup is the set of all elements of the form $x_1 x_2 \ldots x_n$ where either x_i or x_i^{-1} is in S. This is because this set forms a subgroup of G, and also every subgroup that contains S conversely must contain these elements. In this way, generators work for groups analogously to how bases work in vector spaces.

A simple example is taken from linear algebra. One standard theorem proven is that every invertible matrix is the product of elementary matrices. This means that $GL_n(\mathbf{F})$ is generated by the set of all elementary n by n matrices in the field $\mathbf{F}$.

Definition 11. If a group is generated by a single element, then the group is called **cyclic** . This means every element is a power of that element.

One example is $\mathbf{Z}^+$, which is generated by both 1 and -1.

Let g be an element of a group G, and suppose that the cardinality of $\langle g \rangle$ is a non-negative integer c. Then the following properties hold for g:

Lemma 3.4. $\{g, g^2, \ldots, g^c\}$ are all distinct elements of g.

Proof. Suppose $g^i = g^j$, for $i \neq j$, and such that $0 \leqslant j < i < c$. Then $g^{i-j} = e$, for $i - j \neq 0$. Take any element g^m in $\langle g \rangle$. Then, by the euclidean division algorithm,

$$m = (i - j)q + r$$

for some integers q and r, where $0 < r < i - j$. Then

$$g^m = (g^{i-j})^q g^r = g^r$$

hence the size of $\langle g \rangle$, which we have denoted c, is less than or equal to $i - j$, for every element in the set is g^r for some r between 0 and $n-1$. But $i - j < c$, which leads us to our contradiction. Hence $g^i \neq g^j$ for numbers i and j in the range $0 < i < j < c$. □

Corollary 3.5. For $0 < k < c$, $g^k \neq e$.

Corollary 3.6. If $\langle g \rangle$ is infinite, then $g^i \neq g^j$ if $i \neq j$.

Proof. If $g^i = g^j$ for some $i > j$, then $g^{i-j} = e$, showing the cyclic group is at most order $i - j$. □

Corollary 3.7. $g^c = e$.

PROOF. g^c cannot be equal to any element between g and g^{c-1}, so it must be the element of the group that is different from the other elements before it. Thus $g^c = e$, as no other element before g^c is e, and this is the only such element. □

LEMMA 3.8. $g^k = e$ if and only if $c \mid k$

PROOF. We leave this our argument to the reader. It is a simple application of euclidean division. □

Given an element g in an arbitrary group G, we define the order of g to be the cardinality of the group $\langle g \rangle$. Of course, if $\langle g \rangle$ is finite, this is exactly the least positive integer a such that $g^a = e$. We also call this number the period of a. If this is infinite, we say a has infinite period.

LEMMA 3.9. The order of an element (ab) is the same as the order of an element (ba).

PROOF. Consider the group $\langle ab \rangle$. We know that $(ba)^{-1} = a^{-1}b^{-1}$. Suppose the order of (ab) is finite, of order k. Then

$$(ab)^k = e$$

which means

$$b(ab)^k = b$$

and as $b(ab)^k = (ba)^k b$,

$$(ba)^k b = b$$

We conclude $(ba)^k = e$. Thus the order of (ba) is less than or equal to the order of (ab). This process can be done backwards to determine that the order of (ab) is less than or equal to the order of (ba), so the two must be equal. □

Now for any cyclic group $\langle g \rangle$, and for any integer a, one can verify $\langle g^a \rangle$ is a subgroup of $\langle g \rangle$. What is surprising is that any subgroup is of this form.

THEOREM 3.10. G is a subgroup of a cyclic group $\langle g \rangle$ if and only if G is of the form $\langle g^a \rangle$ for some integer a. In short, the only subgroups of a cyclic group are cyclic.

PROOF. Let G be a subgroup of $\langle g \rangle$. If $G = \{e\}$, then $G = \langle g^0 \rangle$. In any other case, G has some non-zero element g^a. Thus G contains an element with positive exponent, as if a is negative, $-a$ is positive, and g^{-a} must be an element of the group by the closure property of a subgroup. By the well-ordering principle, G contains an element with smallest positive exponent g^b. Using euclidean division, every element $g^c \in G$ is of the form g^{mb+n}, where $0 < n < b$. Now $g^n \in G$, as $g^n = g^c g^{-mb}$, so we must conclude $n = 0$, as it cannot be a smaller positive exponent than b. Thus every exponent in G is divisible by b, and every number divisible by b is in G, so we conclude $G = \langle g^b \rangle$. □

Theorem (3.10) has some interesting repercussions in number theory. First, some notation is needed. For a group with two subsets S and M, define

$$SM = \{sm : s \in S, m \in M\}$$

For a single element a, define $aM = \{a\}M$, and Ma equivalently.

- For any numbers $a, b \in \mathbf{Z}^+$, $a\mathbf{Z}^+ + b\mathbf{Z}^+$ is a group. so it is equal to some cyclic group $c\mathbf{Z}^+$ for an integer c. It turns out c is the greatest common denominator of a and b, denoted $\gcd(a, b)$.
- Given $a, b \in \mathbf{Z}^+$, $a\mathbf{Z}^+ \cap b\mathbf{Z}^+$ is a subgroup of $\mathbf{Z}^+$, so it too is $c\mathbf{Z}^+$, and c is the lowest common multiple of the two elements, denoted $\operatorname{lcm}(a, b)$.

Theorem 3.11. Consider a group G, with two elements g and h such that g is of order n and h is of order m. Then, if g and h commute (if $gh = hg$), and m and n are relatively prime, then the order of (gh) is mn.

Proof. Consider elements described above, and let the order of (gh) be p. $(gh)^{mn} = g^m h^n = e$, hence $p \mid mn$. We know that

$$(gh)^p = g^p h^p = e$$

hence, by multiplying both sides by n,

$$g^{mp} h^{mp} = g^{mp} = e$$

so that $n|mp$. As $\gcd(m, n) = 1$, $n|p$. □

We have another interesting number theoretic theorem before we finish our talk of cyclic groups. The proof is not trivial.

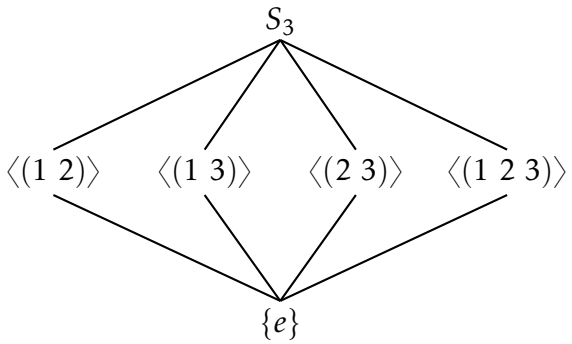
Theorem 3.12. For any prime p, $(\mathbf{Z}/p\mathbf{Z})^\times$ (consisting of all numbers that are invertible modulo p) is a cyclic group.

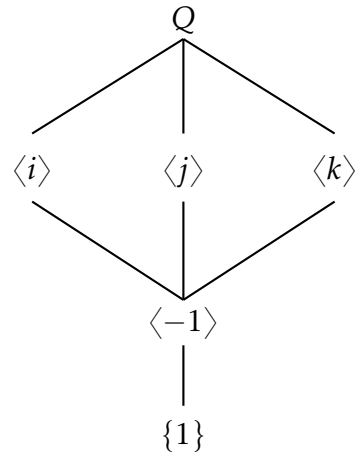
Proof. We will use the fact that for any $r \geqslant 1$, the equation $x^r \equiv 1 \mod p$ has no more than r solutions for x in $(\mathbf{Z}/p\mathbf{Z})^\times$ where p is prime. This follows that fact that the group is also a field, and thus roots of a polynomial decompose the polynomial into linear factors. Let n be the maximal order of elements in $(\mathbf{Z}/p\mathbf{Z})^\times$. We would like n to be order $p - 1$, from which we can conclude the group is cyclic. Of course, we know $n \leqslant p - 1$, as n is the order of a subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$. We know by our initial claim that the equation $x^n = 1$ has at most n solutions. But for every $g \in (\mathbf{Z}/p\mathbf{Z})^\times$, $g^n = 1$, hence we have $p - 1$ solutions. Thus $p - 1 \leqslant n$, and by combining the two inequalities, $p - 1 = n$. Thus there is an element g such that $\langle g \rangle$ has the same order as $(\mathbf{Z}/p\mathbf{Z})^\times$, so the two must be equal. □

The problem with the above proof is that it gives us no method to find a generating element for the multiplicative group. This is an open problem that is

incredibly important to cryptography, where multiplicative groups of the form above are used to construct encodings.

An interesting view of subgroups results from the tools considered above. Given a group, take the set of all its subgroups ordered by the subset relation. Then the set of subgroups form a lattice : every two subgroups has a smallest subgroup that contains the two subgroups (the generated set of the union of the two groups), as well as a biggest subgroup that both contain, the intersection of the two. This becomes very important in the context of Galois theory. We draw the lattices for the symmetric group S_3 and quaternion group Q below.





Now we have specified the concept of a subgroup, we can attempt to gain a deeper understanding of the group via the subgroups it contains. We do this through the tool of cosets. We were previously introduced to subgroups as an attempt to understand the group as a sum of its parts. Cosets expand upon this method to understand the group properties.

Definition 12. Let H be a subgroup of a group G. Define an equivalence relation $\sim$ on G by $x \sim y$ if $x \in yH$. The equivalence classes formed by the relation

are denoted G/H and pronounced as 'G modulo (mod) H'. Each equivalence class is called a **left coset**.

Think of cosets are subgroups that are translated around by an element in a group, like subspaces in a vector space shifted by a vector.

LEMMA 3.13. Every left coset is of the form gH for some element g that is in the equivalence class.

PROOF. Let C be an arbitrary equivalence class in G/H. Then C is non-empty; there is some element g in the class. We know $gH \subseteq C$, as for any element $h \in H$, $g \sim gh$. But also $C \subseteq gH$, as if $g \sim c$ for some $c \in C$, $c \in gH$ by definition of the equivalence relation. We conclude $C = gH$. □

Right cosets are defined equivalently to left cosets, by the equivalence relation $g \sim k$ if $g \in Hk$. Like left cosets, all right cosets can be written Hg for some g. We denote the set of right cosets by $H\backslash G$. Left cosets and right cosets form a dual, hence whether we use left cosets or right cosets does not matter, theorems can be proved in equal power for each. The theorem below shows a close connection.

LEMMA 3.14. There is a one to one correspondence between left cosets and right cosets of any group.

PROOF. Let G be a group, and H a subgroup that generates G/H. Consider the mapping from left cosets to right cosets defined by $gH \mapsto Hg^{-1}$. We claim this mapping is a function. Suppose for two elements g and g' in G, $gH = g'H$. Then $gh = g'h'$ for some elements h and h' in H. But then, it follows that $(gh)^{-1} = (g'h')^{-1}$, which when evaluated gives us the equation $h^{-1}g^{-1} = h'^{-1}g'^{-1}$. We rearrange to get that $g^{-1} = hh'^{-1}g'^{-1}$. By the property of closure in a group, $hh'^{-1} \in H$, so that $g^{-1} = h''g'^{-1}$ for $h'' = hh'$. This means precisely that $g^{-1} \in Hg'^{-1}$, but also $g^{-1} \in Hg^{-1}$ (simply take $e \in H$). As cosets partition the group, we must conclude that $Hg^{-1} = Hg'^{-1}$. The two are equal, as was desired. In addition to this, the map is a bijection, with an inverse function defined by $Hg \mapsto g^{-1}H$. Thus we have a one-to-one correspondence, as was required. □

The proof above makes the next definition independant of left or right cosets.

DEFINITION 13. The number of cosets in G/H or $H\backslash G$ is denoted $(G : H)$, and is called the **index** of H in G.

We now come to one of the most important theorems in basic group theory, named after one of the pioneers of group theory, the french mathematician Joseph-Louis-Lagrange. It gives a useful characteristic of all subgroups of a finite group. Though the statement is formidable, the mechanics we have built

up make the proof relatively simple – our definitions were the hard part to understand.

THEOREM 3.15 (Lagrange's Theorem). The order of a subgroup of a finite group divides the order of the entire group.

PROOF. Let G be a finite group, and H a subgroup. Let g and g' be arbitrary elements of G. Define a function from elements of gH to elements of $g'H$ defined by the mapping $gh \mapsto g'g^{-1}gh$. This mapping is bijective, as it has an inverse function defined by the mapping $g'h \mapsto gg'^{-1}g'h$. Thus the order of one coset is equal to the other coset. We know that the cardinality of G is the sum of its partitions. That is, if G is partitioned into $\{g_1H, g_2H, \ldots, g_nH\}$, then

$$|G| = \sum_{k=1}^{n} |g_kH|$$

But we have proved that the order of any two of these cosets are equal, hence, for any coset gH

$$|G| = \sum_{k=1}^{n} |gH| = n|gH|$$

and as n is the index of the subgroup H, we obtain the following correspondence: for any coset gH, $|G| = |gH|(G : H)$. By noting that H is a coset (simply take the coset of e), we obtain Lagrange's magnificant theorem as a corollary,

$$|G| = |H|(G : H)$$

hence $|H| \mid |G|$. □

Lagrange did not completely prove the theorem, showing it only for subgroups of the symmetric groups. The first complete theorem was published by Gauss in 1801. The following shows the power of Lagrange's theorem.

COROLLARY 3.16. Any group of prime order is cyclic.

PROOF. Let G be a group of prime order. Take a non-zero element $g \in G$ (which is possible since $|G| > 1$), and consider $\langle g \rangle$. This is a subgroup, and thus the order of the group must divide G. But the only numbers that divide G are 1 and the order of G, as the number is prime, and $\langle g \rangle$ definitely contains more than one element. Thus the order of $\langle g \rangle$ is the same as the order of G, so $G = \langle g \rangle$. □

COROLLARY 3.17 (The Multiplicative Property). Let G be a group, H a subgroup of G, and M a subgroup of H. Then $(G : M) = (G : H)(H : M)$.

PROOF. If M is a subgroup of H, Lagrange's theorem tells us that

$$|H| = |M|(H : M)$$

By further application of Theorem (3.15), it then follows that

$$|G| = |H|(G : H) = |M|(G : H)(H : M)$$

Noticing that M is also a subgroup of G,

$$|G| = |M|(G : M)$$

Thus we conclude

$$|M|(G : M) = |M|(G : H)(H : M)$$

By dividing by $|M|$ (which is non-zero as M is non-empty), we obtain the fact that $(G : M) = (G : H)(H : M)$. □

We now have the power to prove one of the theorems that introduced group theory at the beginning of the book. Euler used the methods of Lagrange to prove his totient function theorem. To show the power of group theory, we know prove his theorem. Let us be reminded of the theorem's statement.

Corollary 3.18 (Euler's Theorem). For any two relatively prime integers a and b,

$$a^{\varphi(b)} \equiv 1 \pmod{b}$$

where $\varphi(b)$ counts the number of integers less than b which are relatively prime.

Proof. Consider the group $\mathbf{N}^\times/b\mathbf{N}$, which consists of all invertible elements of $\mathbf{N}$ modulo b. We claim the size of this group is $\varphi(b)$, by showing that a necessary and sufficient property for inclusion in the group is being a relatively prime number of b congruent modulo b to a relatively prime integer less than or equal to b. Let x be an element of $\mathbf{N}^\times/b\mathbf{N}^\times$. Then there is some number y such that

$$xy \equiv 1 \pmod{b}$$

which means exactly that $xy + mb = 1$, for some integer m. Then it obviously follows that $\gcd(x, b) = 1$ by Bezout's lemma, hence x and b are relatively prime. Now suppose for some integer x, $\gcd(x, b) = 1$. Then there are two integers m and n such that

$$xm + bn = 1$$

so that $xm \equiv 1 \pmod{b}$. Taking $x \bmod b$ and $m \pmod{b}$, we obtain the same result, hence $x \bmod b$ is an element of $\mathbf{N}^\times/b\mathbf{N}$ and thus x is congruent to a number in the group. Now let x be an arbitrary positive integer relatively prime to b. Then $\langle x \bmod b\rangle$ forms a subgroup of $\mathbf{N}^\times/\mathbf{N}$. Since this group is order $\varphi(b)$ by the equivalency of the definition of the two, we have by Lagrange's theorem that the order of $x \bmod b$ divides $\varphi(b)$. But then

$$(x \bmod b)^{\varphi(b)} \equiv 1 \pmod{b}$$

By extracting the inner modulo b, we obtain the final conclusion that

$$x^{\varphi(b)} \equiv 1 \pmod{b}$$

Euler's theorem follows simply from the theory of groups. □

A simpler theorem results as a corollary to Euler's theorem. We leave it as an exercise to prove this without the powerful notions above.

Corollary 3.19 (Fermat's Little Theorem). If p is a prime, and a is a number that does not divide p, Then

$$a^{p-1} \equiv 1 \mod p$$

After this aside, we introduce some more tools for understanding subgroups. We focus on special subgroups that have interesting properties.

Theorem 3.20. Let H be a subgroup of a group G. The following statements are equivalent, and if any hold, we say H is normal in G and write $H \triangleleft G$:

(1) $gHg^{-1} \subseteq H$ for all g
(2) $gHg^{-1} = H$ for all g
(3) $gH = Hg$ for all g
(4) For all g, there is g' such that $gH = Hg'$

Proof. First we show (1) is equivalent to (2). Suppose $ghg^{-1} \subseteq H$ for all g. Then $gH \subseteq Hg$ (multiply both sides of the relation on the right by g. But also $g^{-1}Hg \subseteq H$, such that $Hg \subseteq gH$, so that $Hg = gH$. The reverse statement from (2) to (1) is obvious. We obtain (3) from (2) by multiplying both sides of the equation on the right by g, and the reverse by multiplying on the right by g^{-1}. The implication from (3) to (4) is obvious. From (4), note if $gH = Hg'$, $ge = g \in Hg'$, so that $Hg' = Hg$ as cosets are equal or disjoint. Thus all statements are shown to be equivalent by a web of implications. □

Some examples of normal subgroups are the following. Verification of normality is left as an exercise:

- Any subgroup of an abelian group is normal.
- $SL_n(\mathbf{F}) \triangleleft GL_n(\mathbf{F})$
- If H is a subgroup of G of index two, $H \triangleleft G$
- If a group G is normal, and H is a cyclic subgroup, for any subgroup I in H, $I \triangleleft G$.
- Given a group G and a subset S, consider the subgroup
$$N_G(S) = \{x \in G : xSx^{-1} = S\}$$
This is the normalizer of S , and if S is a group, $S \triangleleft N_G(S)$
- Given the last normal group, consider a group G and subset S, and a resultant subgroup
$$C_G(S) = \{x \in G : (\forall s \in S)(xsx^{-1} = s)\}$$

called the centralizer subgroup of S , which is obviously normal in G.

The normalizer of a subgroup is the largest group that it is normal in. The reader can fill in the blanks of the proof in the lemma below.

LEMMA 3.21. Let G be a group, and H and K two subgroups. If H is normal in K, then K is a subset of $N_G(H)$.

COROLLARY 3.22. A subgroup H of a group G is normal if and only if $N_G(H) = G$.

The following propositions are an easy test of knowledge about normality.

THEOREM 3.23. If K is a subgroup of $N_G(H)$, then KH is a group, and $H \lhd KH$.

PROOF. First we prove KH is a subgroup. If k_1h_1 and k_2h_2 are in KH, then $k_1h_1(k_2h_2)^{-1}$ is in KH by the following calculation, which shows that KH is a subgroup by Lemma (3.1):

$$\begin{aligned} k_1h_1(k_2h_2)^{-1} &= k_1h_1h_2^{-1}k_2^{-1} \\ &= k_1(k_2^{-1}k_2)h_1h_2^{-1}k_2^{-1} \\ &= (k_1k_2^{-1})\big[k_2(h_1h_2^{-1})k_2^{-1}\big] \end{aligned}$$

As $k_2 \in K$, $k_2 \in N_G(H)$, hence the value enclosed in square brackets above is an element of H. $k_1k_2^{-1}$ is in K as K is a subgroup, hence the entire equation is in KH. Thus we obtain that KH is a group. Now Consider an arbitrary element $h \in H$, and the equation $h^{-1}kh'h$ for some other arbitrary elements $k \in K$ and $h' \in H$. Using the same tricks as above,

$$h^{-1}kh'h = k\big[k^{-1}h^{-1}kh'h\big]$$

and the square brackets are contained in H. Thus $H \lhd KH$ □

The trivial group is always normal in any group is lies in, because given any element g,

$$g^{-1}eg = g^{-1}g = e \in \{e\}$$

Furthermore, for any group G, $G \lhd G$, resulting from the properties of closure in the group operation. It follows that no group possesses no normal subgroups. We must take this into account in defining the property of sparcity of normal subgroups.

DEFINITION 14. A group is **simple** if it contains no non-trivial normal subgroups, that is, if the only normal subgroups are $\{0\}$ and the group itself.

Think of simple groups as the equivalent of prime numbers for groups (they cannot be broken up into simple groups). If we can characterize all simple groups, then intuition tells us that there must be some way to put them together

to characterize all groups. This is why the Hölder program of mathematics attempts to classify all finite simple groups, and characterize all finite groups in the process. In 2008, over one hundred years since the program started, we succeeded in characterizing all finite simple groups. Each one belongs to one of 18 infinite families of groups, and 26 'sporadic' groups which we cannot organize into families. The proof of this has taken over tens of thousands of journal articles, and for obvious reasons we will not replicate it.

Exercise 3.1. In our definition of a subgroup H of a group G we also assume that the identity is in a subgroup. However, it could be true that there is a different element e' such that e' acts idempotently on all elements in H, but not necessarily on all of G, and thus becomes a second identity! Show that this is not possible.

Exercise 3.2. Let G be a finite cyclic group of order n, generated by an element g. Then g^a is a generator for G if and only if a is relatively prime to n.

Exercise 3.3. If G is a cyclic group with two generators x and y, then there exists a unique automorphism mapping x onto y

Exercise 3.4. Show that for every finite cyclic group G of period n, and for any integer d which divides n, there exists a unique subgroup of order d.

CHAPTER 4

Homomorphisms and Isomorphisms

Another way to understand objects is to create metaphors to objects we already understand. In group theory, metaphors are formalized as 'homomorphisms'.

Definition 15. Let G be a group with operation $\circ$ and H a group. A **homomorphism** between G and H is a function f such that for any elements x and y. $f(x \circ y) = f(x)f(y)$. We say that G and H are homomorphic. If a homomorphism is injective, we say that G can be embedded in H. If $G = H$, we call a homomorphism an endomorphism.

What a homomorphism means intuitively is that information about the group G can be implanted into a subgroup of H. Some elements may become one element, but the information is still there. The following definition outlines the specific elements that are merged into one by a homomorphic transformation.

Definition 16. The **kernel** of a homomorphism φ, denoted $\ker(\varphi)$ is the set of elements in the domain that are mapped to the identity element in the range.

The following properties hold for any homomorphism φ, which should be obvious as the properties are central to the structure of groups:

Lemma 4.1. $\varphi(e) = e$

Proof. $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, hence $\varphi(e)$ is idempotent. □

Lemma 4.2. $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof. $\varphi(a^{-1})\varphi(a) = \varphi(aa^{-1}) = \varphi(e) = e$. □

We use normal subgroups along with homomorphisms to connect groups. To tease this fact, we show the following theorem.

Lemma 4.3. The kernel of a homomorphism is a normal subgroup of the domain of the homomorphism.

Proof. Let G and H be groups, and φ a homomorphism between G and H. If $\varphi(j) = e$, $\varphi(gjg^{-1}) = \varphi(g)\varphi(j)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e$. Thus gjg^{-1} is in the kernel for any element g in G, and we have shown normality. □

Corollary 4.4. Let G be a group, and H and K subgroups of G such that $K \subset N_G(H)$. Then $H \cap K \lhd H$.

Proof. If $K \subset N_G(H)$, then KH is a group. Consider the cannonical mapping from H to H/K by the mapping $h \mapsto hK$. $hK = K$ when $h \in K$, hence the kernel of the mapping is $H \cap K$, and thus $H \cap K \lhd H$. □

Lemma 4.5. The image of a homomorphism is a subgroup

Proof. If a is a group element such that $\varphi(x) = a$ for some elements a and x, then $\varphi(x^{-1}) = a^{-1}$, and if b is an element such that $\varphi(y) = b$ for some element y, then $\varphi(x^{-1}y) = a^{-1}b$.by Lemma (3.1). □

Lemma 4.6. A homomorphism is injective if and only if $\varphi(a) = e$ implies $a = e$.

Proof. We prove both implications. Suppose a homomorphism is injective, and if $\varphi(a) = e$. Then $a = e$ as $\varphi(e) = e$. Instead, to prove the converse, if $\varphi(a) = e$ implies $a = e$, then if $\varphi(a) = \varphi(b)$, then $\varphi(ab^{-1}) = e$, so that $ab^{-1} = e$ and thus $a = b$. □

Some examples of homomorphisms are the following:

- The determinant function from $GL_n(\mathbf{F})$ to $\mathbf{F}^\times$.
- For any element a in a group G, the map from $\mathbf{Z}^+$ defined by $x \mapsto a^x$.
- The exponentiation map $x \mapsto e^x$.
- The absolute value map from $\mathbf{C}^\times$ to $\mathbf{R}^\times$.

Definition 17. An **isomorphism** is a bijective homomorphism. In this case the inverse of the homomorphism is also a homomorphism. A bijective endomorphism is also called an automorphism . If G is isomorphic to H, we write $G \cong H$.

An isomorphism states that all algebraic information about G holds in H; effectively, they are the same group, just with different names for the operations and elements that characterize the group. An automorphism basically states that various objects in the same group behave in the same way when permuted according to the function.

Let us consider an automorphism on $\mathbf{C}^\times$. Take the map

$$a + bi \mapsto a - bi$$

that swaps every complex number with it's complex conjugate, reflecting the complex number system about the real axis. What this automorphism means

is we could have introduced $-i$ as the basic element and the complex number system would have the same algebraic properties.

For a group, the set of automorphisms on the group, taken with the operation of composition of functions, form a group. Given an element g in G, the set of automorphisms $h \mapsto ghg^{-1}$ defines the set of inner automorphisms, a subgroup of the set of automorphisms. The map that sends g to its inner automorphism is a homomorphism. The kernel of this homomorphism is the center group

$$Z(G) = \{g \in G : \forall h : gh = hg\}$$

It is obviously normal.

The following theorem is useful, but clear. We leave it for the reader to prove.

THEOREM 4.7. Let G be a group, and S a subset such that $G = \langle S \rangle$. Suppose $f : S \to H$ is a map to another group H. If there is a homomorphism from G to H whose restriction to S is f, then this is the only homomorphism with this property.

The theorem is no different from the fact that two linear transformations which are equal when restricted to the basis elements of a vector space are equal in full.

We can finally use coset constructions to prove something meaningful. Let G be a group and H a normal subgroup. For two cosets M and N in G/H, define an operation $\circ$ on the cosets by $M \circ N = MN$. As $M = gH$ and $N = g'H$ for some $g, g' \in H$,

$$MN = gHg'H = gg'HH = gg'H$$

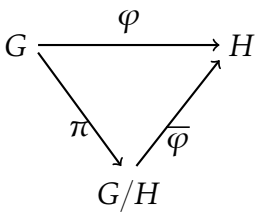
This follows by the normality of H. Thus the operation we have constructed is closed in G/H. The operation has an identity H, and the inverse of gH is $g^{-1}H$. With these properties, G/H forms another group: the factor or quotient group . H is the identity in this group. The map $g \mapsto gH$ is the canonical map or projection π from G to G/H, and is a surjective homomorphism. The kernel is H, hence we have shown that every normal subgroup is the kernel of some homomorphism.

THEOREM 4.8 (The First Isomorphism Theorem). Let φ be a homomorphism between two groups G and H. Then $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

PROOF. Let K be the kernel of φ. If $gK = hK$ for $g, h \in G$, $\varphi(g) = \varphi(h)$. Hence the mapping $\overline{\varphi}$ defined by $gK \mapsto \varphi(g)$ is well defined. It is a homomorphism as $gKhK = ghK$, so ghH is mapped to $\varphi(gh) = \varphi(g)\varphi(h)$. We then obtain that $\overline{\varphi} \circ \pi = \varphi$ by construction. Because π is surjective, the map is unique. We also obtain that $\overline{\varphi}$ is injective, because $\varphi(a) = \varphi(b)$ implies $\varphi(ab^{-1}) = e$; hence $ab^{-1} \in K$, and $ab^{-1}K = K$. As K is normal, it is also true that $ab^{-1}K = aKb^{-1}$, so that

$aKb^{-1} = K$, and thus $aK = Kb = bK$. The map is of course surjective onto its image, hence $\overline{\varphi}$ is an isomorphism, and we have proven what was needed. □

It is convenient here to introduce the concept of a commutative diagram. A commutative diagram is a directed graph where vertices are sets and edges are functions between the sets it connects, with the following property. If there are two paths



$$S \xrightarrow{f_1} A_1 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_n \xrightarrow{f_n} E$$
$$S \xrightarrow{g_1} B_1 \xrightarrow{g_2} \dots \xrightarrow{g_{m-1}} B_m \xrightarrow{g_m} E$$

from S to E, then $f_n \circ \cdots \circ f_1 = g_m \circ \cdots \circ f_1$. An example diagram represents the functions in the first isomorphism theorem.

Another notation that is more lateral is to consider sequences of groups

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \dots \xrightarrow{f_n} G_{n+1}$$

with arrows representing homomorphisms. This sequence is **exact** whenever $\mathrm{im}(f_i) = \ker(f_{i+1})$ for any i from 1 to $n-1$. To test your knowledge of this, note that the sequence

$$\{e\} \to G \xrightarrow{f} H$$

being exact states exactly that f is an injective homomorphism, as there is only one homomorphism from $\{e\}$ to any group. Likewise,

$$G \xrightarrow{f} H \to \{e\}$$

states that f is surjective.

A simple application of the first isomorphism theorem is a way classify the cyclic groups. Specifically, a classification is a set of equivalence classes defined by the relation on groups $x \sim y$ if $x \cong y$. In algebra, we refer to these as the isomorphism classes, and finding a classification of some segment of groups is a primary goal of group theory. One can only really say they 'know' a group if, given another group, one can intuitively say whether the two groups are isomorphic or not.

Theorem 4.9 (The Classification of Cyclic Groups). Every cyclic group is isomorphic to either $\mathbf{Z}^+$ or $\mathbf{Z}^+/n\mathbf{Z}$ for some integer n.

Proof. Let $\langle g \rangle$ be a cyclic group. Define a surjective homomorphism from $\mathbf{Z}^+$ to $\langle g \rangle$ by the mapping $r \mapsto g^r$. If $\langle g \rangle$ is order n, $n\mathbf{Z}^+$ is the kernel of the map. Then $\langle g \rangle \cong \mathbf{Z}^+/n\mathbf{Z}^+$ by the first isomorphism theorem. If $\langle g \rangle$ is infinite, the kernel of the map is $\{0\}$, and $\mathbf{Z}^+/0\mathbf{Z}^+ \cong \mathbf{Z}^+$, so $\langle g \rangle \cong \mathbf{Z}^+$. □

This theorem allows us to prove things about general cyclic groups in the context of only $\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z}$.

THEOREM 4.10. An infinite cyclic group has exactly two generators

PROOF. Any infinite cyclic group is isomorphic to $\mathbf{Z}$. Distinct generators of these cyclic groups are mapped to distinct generators in $\mathbf{Z}$, hence if we prove that $\mathbf{Z}$ has only two generators, then every infinite cyclic group has this property. Let x be a generator for $\mathbf{Z}$. Without loss of generality, assume x is positive (if x is negative than $-x$ is a positive generator, and x is definitely never 0 for an infinite group). Then $mx = 1$ for some positive integer m. If $x > 1$, and $m \geqslant 1$, we obtain that $mx > 1$, yet $mx = 1$, a contradiction. Hence $x = 1$, and thus the only other generator is $x = -1$. □

The first isomorphism is the catalyst to many important isomorphism theorems.

THEOREM 4.11 (The Second Isomorphism Theorem). Let G be a group, and K and H subgroups such that $K \subset N_G(H)$. Then we have that

$$H/(K \cap H) \cong HK/K$$

PROOF. We have already justified in our discussion of cosets that $K \cap H$ will be normal in H, and K normal in HK. Define an assignment map from H to HK/K by

$$h \mapsto hK$$

This is a surjective homomorphism, as any coset hkK can be written as a coset hK. If, for some element $h \in H$, $hK = K$, then it is sufficient and necessary for $h \in K$ as well. Thus the kernel of the mapping defined above is $H \cap K$, and by the first isomorphism theorem, we obtain that

$$H/(H \cap K) \cong HK/K$$

□

The second isomorphism theorem is known as the diamond isomorphism theorem because of the lattice of subgroups it forms.

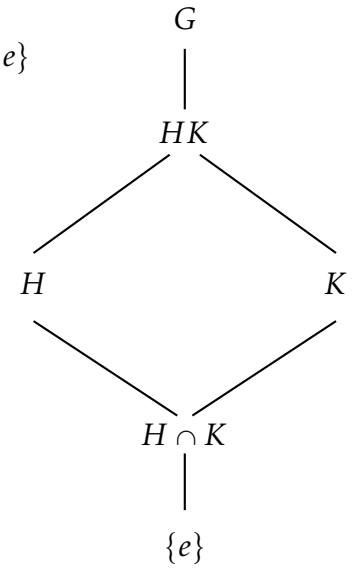
THEOREM 4.12 (The Third Isomorphism Theorem). Suppose M and N are normal subgroups of a group G, where N is also a normal subgroup of M. Then M/N is a normal subgroup of G/N, and we know that $(G/N)/(M/N) \cong G/M$.

PROOF. Define an assignment from G/N to G/M by $gN \mapsto gM$. It is a surjective homomorphism, well defined as N is a subgroup of M, so that $gN \subseteq gM$ for any g. The kernel of this map are all sets of elements gN such that $gM = M$, which is precisely the elements g that are elements of M. Then the kernel is M/N (a normal subgroup), so by the first isomorphism theorem, we obtain that $(G/N)/(M/N) \cong G/M$. □

All we have done is proven that the sequence

$$\{e\} \to M/N \to G/N \to G/M \to \{e\}$$

is exact, and the theorem follows naturally.



THEOREM 4.13 (The Lattice/Fourth Isomorphism Theorem). Let G be a group, and N a normal subgroup. Then for every subgroup H of G, the set

$$\{hN : h \in H\}$$

which we denote $(G/N)_H$, is a subgroup of G/N and also, for every subgroup $(G/N)_H$ of G/H the underlying set H is a subgroup of G. In addition, we have the following properties:

- $H \subset K$ if and only if $(G/N)_H \subset (G/N)_K$.
- If $K \subset H$, $(H : K) = ((G/N)_H : (G/N)_K)$.
- $(A \cap B)N = (G/N)_A \cap (G/N)_B$
- $H \lhd K$ if and only if $(G/N)_H \lhd (G/N)_K$
- $\langle (G/H)_S, (G/H)_T \rangle = G/H_{\langle S,T \rangle}$

PROOF. Given a subgroup H of G which contains N, define a mapping from H to G/N by $h \mapsto hN$. This is a homomorphism, and thus its range, which we have already defined as $(G/N)_H$, forms a subgroup of G/N. We have thus proved this in general that $(G/N)_H$ is a subgroup of G/H for every subgroup H of G. Now suppose $(G/N)_S$ is a subgroup of G/N for some set S. Suppose two elements a and b are in S, so that aN and bN are in $(G/N)_S$. Then $ab^{-1}N$ is in $(G/N)_S$ as it is a subgroup, hence ab^{-1} is in S, so S is a subgroup of G. We leave it to the reader to show the rest of the properties of this correspondence. □

The list of properties above is not exhaustive. Almost all properties of subgroups are preserved by the mapping, so stop a while and think whether you can think of more.

Exercise 4.1. Let a be an element of a group of finite order, and f a homomorphism. Show that the order of $f(a)$ divides the order of a.

Exercise 4.2. This exercise has two parts.

(1) If S and T are subgroups of a group G, then a $(S-T)$ double coset is a subset of G of the form SgT, where $g \in G$. Prove that the set of all $(S-T)$ double cosets partitions the group.
(2) Let S and T be subgroups of a finite group G, and suppose for some sequence $(g_1, g_2, \ldots, g_n)$ such that the double cosets Sg_kT are disjoint, we have that
$$G = \bigcup Sg_kT$$
Prove that
$$G = \sum_{k=0}^{n} (S : S \cap g_k T g_k^{-1})$$
Note this is a generalization of Lagrange's theorem, which results when $T = \{e\}$

Exercise 4.3. Consider a surjective homomorphism φ from a group G to a group H. Let H' be a normal subgroup of H, and define $G' = \varphi^{-1}(H')$. Show that G' is normal, and conclude that via the mapping $g \mapsto \varphi(g)H'$,
$$G/G' \cong H/H'$$

This exercise has important properties in the theory of solvable groups, a theory which we will study later on in the course.

CHAPTER 5

Group Actions and Symmetries

The symmetric group was previously defined as the set of permutations on a set. In the context of an example, this group seems trivial. This chapter will show why this is not so. One reason why the group is generally interesting is Cayley's theorem, which relates the set of groups to all other groups.

THEOREM 5.1 (Cayley's Theorem). Every group is isomorphic to a subgroup of a symmetric group:

PROOF. Let G be a group. For each $g \in G$, define a permutation π_g on the group defined by the map $h \mapsto gh$. The function is a permutation as it is bijective – there is an inverse function $h \mapsto g^{-1}h$. The map from the group to its permutation is a homomorphism as for any two elements g and g' $\pi_g \circ \pi_{g'} = \pi_{gg'}$. Furthermore, the homomorphism is injective, as if $\pi_g = \mathrm{id}$, then $gh = h$ for all elements h, and for any specific one, we obtain that $g = e$. Thus G is isomorphic to the image of the permutation map, which is a subgroup of $S_{|G|}$. □

Intuitively, what Cayley's theorem states is that every every element of a group can be considered a symmetry of some set of objects. For instance, in the group $\mathbf{Z}^+$, the number n can really be considered the symmetry of adding n to every number in $\mathbf{Z}$, shifting all numbers to the right such that the resultant object is symmetric to the original. This is exactly the symmetry to which n corresponds with in Cayley's proof.

Through Cayley's theorem, all groups can be considered subgroups of the symmetric group, hence all groups can be considered a symmetric action on some set. These actions provide another way to understand the structure of a group. Let us describe this in detail.

DEFINITION 18. A **group action** on a group G and set X is a homomorphism π from G to the symmetry group on $|X|$ characters, inducing a symmetry on X for each group element in G. To be concise, we write gs for the permutation $[\pi(g)](s)$ associated with g acting on s. We call X a **G-set** .

It is simple to show that, for any group action G on a G-set X, we have two properties:

(1) For all elements g and h in G and x in X, $g(hx) = (gh)x$
(2) For the identity e in G, and elements x in X, $ex = x$

These properties are just restatements of the definition of a homomorphism; another way of saying the first is that, if φ is the homomorphism defining the action,

$$\varphi(g) \circ \varphi(h) = \varphi(gh)$$

The second statement says

$$\varphi(e) = \mathbf{1}$$

where $\mathbf{1}$ is the identity transformation. This is just the definition of a homomorphism, hence these properties are just an equivalent way of defining a group action.

A basic example of a group action is to consider G acting on itself by conjugation. That is, our group action is defined by

$$gx \mapsto g^{-1}xg$$

It is trivial to verify the group action properties. More interesting than this verification, we find that the permutation associated with any g in G is an automorphism of G. This does not always hold when the set G operates on is a group. Any automorphism which can be considered a conjugation of elements is an **inner** automorphism.

Definition 19. Given a group G, and a G-set S, for $s \in S$, let the **orbit** of s be Gs, the set of all gs for $g \in G$. Let the set of all orbits be denoted X/G.

The relation on a G-set defined by $x \sim y$ if $Gx = Gy$ is an equivalence relation and partitions the set into orbits of S. We call the above object an orbit because intuitively, the group acts independently on each of a G-set's orbits, just like various planets orbit independently around the sun.

Definition 20. A G-set X is **transitive** if it has just one orbit. This just means that for any two elements x and y in X, there is some g in G such that $gx = y$.

Definition 21. An action is **faithful** if the homomorphism defining it is injective, which means that no group element other than the identity acts idempotently to the G-set associated with the group action.

Cayley's theorem asserts that for every group there exists an action that is faithful.

Definition 22. A map α from a G-set X to a G-set Y is a G-morphism if $\alpha(gx) = g\alpha(x)$ for all $g \in G$ and $x \in X$. α is a G-isomorphism if it is bijective.

Like homomorphisms between groups, G-morphisms and isomorphisms embed the algebraic structure of one set into another. The only algebraic structured assumed on a G-sets is its relation to G, so we must use the group action to define the isomorphism.

Definition 23. An element x in a G-set X is a **fixed point** if $gx = x$ for every $g \in G$. The set of all fixed points is denoted X^G.

Definition 24. Given any $x \in X$, the set G_x defined as

$$\{g \in G : gx = x\}$$

is a subgroup called the **isotropy subgroup** or **stabilizer** of x in G, and is normal in G.

As an example, let G act on itself by conjugation. The isotopy subgroups are called centralizers $C_G(h) = \{g \in G : gh = hg\}$. A fixed point is called a center, and the set of all centers is denoted $Z(G)$, which we have previously shown as the center group.

As another example, consider conjugation from G on its subgroups defined by the mapping

$$gH \mapsto gHg^{-1}$$

Then the isotropy group of a subgroup H is the normalizer $N_G(H)$. The fixed points of this transformation are precisely the normal subgroups.

As a more complicated example, consider the group $SL_n(\mathbf{R})$ acting on the upper half of the complex plane, the set

$$\{z \in \mathbf{C} : \mathrm{im}(z) > 0\}$$

by the mobius transform

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}$$

This defines a transitive action. The isotropy subgroup of the imaginary unit i is the special orthogonal group $SO(2)$, the set of matrices with orthonormal columns. A meromorphic function on H invariant under $SO(2)$ is called a modular function, and is essential to the study of number theory, string theory, and the study of monstrous moonshine.

We now give a theorem which establishes an intricate connection between G and its G-sets.

THEOREM 5.2 (Orbit Stabilizer Lemma). Let X be a G-set. Then, for every x in X, there exists a G-isomorphism from G/G_x to Gx. It follows that

$$|Gx| = (G : G_x)$$

PROOF. Define a mapping by

$$gG_x \mapsto gx$$

We leave the reader to verify this is a well defined function. The reasoning is similar to the verification of the function created in the first isomorphism theorem. This mapping is surjective by construction, and furthermore, the map is injective. If $gx = hx$, then $(h^{-1}g)x = x$, hence $(h^{-1}g) \in G_x$, so $gG_x = hG_x$. The mapping is also a G-isomorphism, hence we have constructed the required isomorphism. □

COROLLARY 5.3 (The Orbit Decomposition Formula). Given a G-set X, with a finite number of orbits $(X_1, X_2, \ldots, X_n)$. From each orbit, pick a representative x_i. Then we have

$$|X| = \sum_{k=1}^{n} (G : G_{x_i})$$

which we call the orbit decomposition formula. In particular, for every orbit which is a singleton $\{x\}$, $G_x = G$, hence $(G : G_x) = 1$; thus, if we collect all these orbits, and remove them from the list we have, we obtain that

$$|X| = |X^G| + \sum_{k=1}^{n} (G : G_{x_i})$$

where $\{x_1, \ldots, x_n\}$ is the new set of orbit representatives where the orbit is not one.

PROOF. X is the disjoint union of its orbits. Hence

$$|X| = \sum_{k=1}^{n} |Gx_i|$$

But we have contructed an isomorphism from Gx_i to G/G_{x_i} above, hence

$$|Gx_i| = |G/G_{x_i}|$$

and we obtain the final formula by Lagrange's theorem. □

The following corollary is just a specialization of the previous theorem, though is just as useful.

Corollary 5.4 (The Class Equation). Consider the group action of conjugation from a group G onto itself. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n-1} (G : C_G(x_i))$$

This theorem will be very useful for our next topic of study, Sylow theory. Before we get into this theory, let us consider an example to show the power of the class equation. Consider a group of order 55 acting on a set of order 39. We claim there is at least one fixed point in the group action. The orbit decomposition formula entails that we have

$$|X| = 39 = |X^G| + \sum_{k=1}^{n} (G : G_{x_i})$$

Each G_{x_i} forms a subgroup of G, hence by Lagrange's theorem, $|G_{x_i}| \mid 55$, so $|G_{x_i}|$ is either 1, 5, 11, or 55. If $|G_{x_i}| = k$, then $(G : G_{x_i}) = 55/k$, so if we let m_j denote the number of orbits whose isotropy subgroups are order j. Then

$$39 = 55m_1 + 11m_5 + 5m_{11} + m_{55}$$

Showing that there is at least one fixed point is the same as showing there is an isotropy group of order 55, for this means that some element in X is fixed by every point in G, and hence a fixed point. By considering all possible solutions to the equations above, we obtain that $m_{55} \geqslant 1$ and hence the theorem.

Lemma 5.5 (Burnside's Lemma). If X is a finite G-set, then

$$|X/G||G| = \sum_{g \in G} |X^g|$$

Proof. By a simple calculation,

$$\sum_{g \in G} |X^g| = |\{(g, x) : gx = x\}| = \sum_{x \in X} |G_x|$$

Combining this calculation with the orbit stabilizer lemma, we obtain that

$$\sum_{x \in X} |G_x| = \sum_{x \in X} |G|(G : G_x)^{-1} = |G| \sum_{x \in X} (G : G_x)^{-1}$$

Now $(G : G_x) = |Gx|$, hence

$$|G| \sum_{x \in X} (G : G_x)^{-1} = |G| \sum_{x \in X} |Gx|^{-1}$$

Now partion X into its orbit X/G. For each x and y in a particular orbit, it is obvious that $|Gx| = |Gy|$. Hence, if we have a partition $(X_1, X_2, \ldots, X_{|X/G|})$, and

we pick representatives from each x_i from each X_i, we have that

$$|G| \sum_{x \in X} |Gx|^{-1} = |G| \sum_{k=1}^{|X/G|} |X_k||Gx_k|^{-1}$$

Now for each $|X_k|$, we have that $|Gx_i| = |X_k|$ by definition, so finally, we obtain that

$$|G| \sum_{k=1}^{|X/G|} |X_k||Gx_k|^{-1} = |G| \sum_{k=1}^{|X/G|} |Gx_i|/|Gx_i| = |G| \sum_{k=1}^{|X/G|} 1 = |G||X/G|$$

and by transitivity, our proof is complete. □

Before we get into Sylow theory, let us establish some interesting facts about the symmetric group. First, of course, we must define some facts.

Definition 25. Given a set M and a permutation π on M, the **support** of π, denoted $\sup(\pi)$, is defined as the set

$$\{m \in M : \pi(m) \neq m\}$$

A **cycle** of length k is a permutation π such that $|\sup(\pi)| = k$, and we can order $\sup(\pi)$ to be $(x_0, x_1, \ldots, x_{k-1})$ in a way that $\pi(x_n) = x_{n+1 \bmod k}$. A cycle of length two is called a transposition .

We denote a cycle like π as $(x_1, x_2, \ldots, x_k)$.

If σ and τ are two permutations, such that $\sup(\sigma) \cap \sup(\tau) = \varnothing$, $\sigma \circ \tau = \tau \circ \sigma$. This is because the two act independently on the set they permute.

Theorem 5.6. Every permutation on a finite non-empty set which is not the identity can be written as the product of cycles with disjoint support. This is unique up to reordering:

Proof. Let σ be an arbitrary element of the symmetric group S_n, and consider the cyclic group generated by σ. Consider the set $\{1, 2, \ldots, n\}$, with $\langle \sigma \rangle$ acting on the set by the mapping

$$\pi k = \pi(k)$$

in the obvious manner. We obtain disjoint partitions of orbits from this action. We claim that π when restricted to this orbit is a cycle, and thus π consists of products of cycles from each orbit. Consider an orbit $(\langle \pi \rangle k)$ for some number k between one and n. Every integer in k's orbit can be written $\pi^m(k)$ for some integer m. For each integer l in the range, associate it with the smallest positive integer m such that $\pi^m(k) = l$. We obtain an ordering

$$(\pi^0(k), \pi^1(k), \pi^2(k), \ldots, \pi^n(k))$$

such that $\pi^{n+1}(k) = k$. This generates a cycle, and we have shown what was needed. □

If a permutation π is equal to the disjoint composition of cycles $\sigma_1, \sigma_2, \ldots, \sigma_n$, then we write $\pi = \sigma_1 \sigma_2 \ldots \sigma_n$. Every permutation on a finite set can be written in this way.

We would like to specify a specific set of permutations having the property of 'evenness', like the integers. Specifically, we would like the following properties:

(1) The composition of two even permutations is even.
(2) The composition of two odd (not even) permutations is even.
(3) The composition of an odd and even permutation is odd.

With the properties above, we can consider the property of 'evenness' to be a homomorphism from S_n to the multiplicative group consisting of ± 1. If $f(\pi) = 1$, then π is even. Thus our task is to characterize a homomorphism with this property. From elementary properties of homomorphisms, we know that **1** must be even (it is in the kernel). In addition,

(1) The inverse of an even permutation is even.
(2) The inverse of an odd permutation is odd.

Let us add the additional characteristic that any transposition must be odd. Then it follows that there is only one homomorphism with the properties above. The next few lemmas will establish this claim.

Lemma 5.7. S_n is generated by transpositions.

Proof. We have proved that S_n is generated by cycles, hence we need only prove that each cycle can be decomposed into transpositions. The calculation below shows that this is true.

$$(x_1, x_2, \ldots, x_n) = (x_1\ x_n)(x_1\ x_{n-1}) \ldots (x_1\ x_2)$$

□

Now of course, by Theorem (4.6) we may conclude that if there exists a homomorphism with the properties above, then it must be unique. Thus we need only establish that there exists a homomorphism with the properties above. We state the theorem in full.

Theorem 5.8. There is a unique homomorphism from S_n to $\{\pm 1\}$ such that the mapping from any transposition is -1.

PROOF. Consider a polynomial P defined for any tuple of natural numbers by

$$P(x_1, x_2, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$$

Define the map sgn from S_n to $\{\pm 1\}$ by

$$sgn(\pi) = \frac{P(\pi(1), \pi(2), \ldots, \pi(n))}{P(1, 2, \ldots, n)}$$

For any factor $(x_i - x_j)$ in $P(1, 2, \ldots, n)$, we either have the factor $(x_j - x_i)$ or the factor $(x_i - x_j)$ in $P(\pi(1), \pi(2), \ldots, n)$ (π just permutes the orders of the elements, hence the numerator and denominator only differ by sign, and the value of sgn is always positive or negative one. We have that

$$\frac{\pi(i) - \pi(j)}{i - j} = \frac{\pi(j) - \pi(i)}{j - i}$$

Therefore it does not matter whether $i < j$ as much as we do not add the same fraction twice. We conclude, for two permutations π and σ, that

$$\begin{aligned}
sgn(\pi \circ \sigma) &= \prod_{1 \leqslant i < j \leqslant n} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{i - j} \\
&= \prod_{1 \leqslant i < j \leqslant n} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{\sigma(i) - \sigma(j)} \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \\
&= \prod_{1 \leqslant \sigma(i) < \sigma(j) \leqslant n} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{\sigma(i) - \sigma(j)} sgn(\sigma) \\
&= \prod_{1 \leqslant i < j \leqslant n} \frac{\pi(i) - \pi(j)}{i - j} sgn(\sigma) \\
&= sgn(\pi) sgn(\sigma)
\end{aligned}$$

Here the third and fourth equality works because σ is a permutation of the numbers from 1 to n. From this calculation, we conclude sgn is a homomorphism; all that is left to prove is that for any transposition (x_1, x_2), $sgm((x_1, x_2)) = -1$.

$$\begin{aligned}
sgn((x_1, x_2)) &= \left(\prod_{\substack{1 \leqslant i < j \leqslant n \\ (i,j) \neq (x_1, x_2)}} \frac{i - j}{i - j} \right) \frac{x_2 - x_1}{x_1 - x_2} \\
&= -\frac{x_2 - x_1}{x_2 - x_1} \\
&= -1
\end{aligned}$$

Thus we have constructed the homomorphism that we wanted. □

The *sgn* map was constructed only to satisfy the proof. Here is a simpler way to think of the map. We know that any permutation π in S_n can be decomposed into the product of a finite number of transpositions. If we let k denote the number of transpositions, then we have that

$$sgn(\pi) = (-1)^k$$

which follows exactly from the homomorphic properties of the sign function. In fact, one way of creating the sign homomorphism is to define it precisely in this way. The only problem with this intuitive definition is proving that if a permutation is the product of two different sets of cycles, then the value of the function is the same. Of course, our homomorphism above proves this, but only by constructing the homomorphism with the properties that we need to get the sign homomorphism.

The kernel of the homomorphism we have created is called the alternating group A_n, a normal subgroup of S_n. It of course consists of all permutations that are products of an even number of transpositions. Let us flesh out the theory of A_n.

We state the first lemma without proof due to its triviality, though it is useful in characterizing the order of the alternating group.

Lemma 5.9. If τ is any transposition, S_n is the disjoint union of A_n and τA_n. Thus $A_n = n!/2$.

And now we will begin a chain of lemmas, leading up to the statement that A_n is simple for $n \neq 4$.

Lemma 5.10. A_n is generated by the set of three cycles.

Proof. A_n is of course generated by the set of all compositions of two transpositions, hence we need only prove that each pair of transpositions can be represented as a three cycle, and vice versa. Let $(i,j)(m,n)$ be an arbitrary pair of two cycles ($i \neq j$, $m \neq n$)). Then one of three cases apply:

(1) $i = m$, $j = n$: In this case $(i,j)(m,n) = \mathbf{1} = (123)^3$.
(2) $i = m$, $j \neq n$: Then $(i,j)(m,n) = (mnj)$
(3) $i \neq m$, $j \neq n$: Then $(i,j)(m,n) = (i,m,j)(i,m,n)$

We have covered all cases, hence any set of two pairs is generated by a three cycle, and thus any element in the alternating group. □

Lemma 5.11. Let $\pi \in S_X$ and $\sigma = (x_1\ x_2\ \ldots\ x_n)$. Then it follows that

$$\pi\sigma\pi^{-1} = (\pi(x_1)\ \pi(x_2)\ \ldots\ \pi(x_n))$$

Proof. This follows as

$$\pi\sigma\pi^{-1}(\pi(x_i)) = \pi\sigma(x_i) = \pi(x_{i+1})$$

If $x \notin \sup(\sigma)$, then

$$\pi\sigma\pi^{-1}(\pi(x)) = (\pi\sigma)(x) = \pi(x)$$

so that $\pi(x) \notin \sup(\pi\sigma\pi^{-1})$. Thus we have shown the value of $\pi\sigma\pi^{-1}$. □

Corollary 5.12. All n cycles are conjugate.

Proof. Let $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ be two three cycles. Consider a permutation φ such that $\phi(x_k) = y_k$. Then the lemma follows right from Lemma (5.11). □

Now we are ready to prove the most strenuous proof of the chapter, the simplicity of the alternating group.

Lemma 5.13. A_n is simple when $n > 4$

Proof. We show that if that if there is a normal subgroup of A_n that is not $\{e\}$, then it is precisely A_n. To do this, we need only show it contains all three cycles by Lemma (5.10). The normality of A_n in tandem with Corollary (5.12) means we need only show one three cycle is in A_n. Let G be a normal subgroup of A_n. Let $\varphi \neq \mathbf{1}$ be the permutation in G that contains the maximum number of fixed points. Partition φ into disjoint cycles. We must have at least one cycle with more than one element (else $\varphi = \mathbf{1}$). We want at least one cycle to be of length more than three so we can extract a three cycle. Suppose every cycle is of size two. Then, since φ is even, we must have at least two cycles. Denote two of these cycles (i, j) and (r, s). Pick some element k in the n characters acted on by A_n that is not i, j, r, or s (possible if the n in A_n is 5 or more), and let $\tau = (r, s, k)$. We know that, since G is normal, $\tau\varphi\tau^{-1}\varphi^{-1}$ is in G. This permutation leaves i and j fixed, as well as all other elements that φ fixes. In addition, it is not the identity; for example, s is not a fixed point. Thus we obtain an element with more fixed points that φ, a contadiction.

We conclude there is at least one cycle in φ with three or more characters, We pick three of these characters, and denote them i, j, and k. Suppose φ is not a three cycle. Then φ acts on at least five characters that are not fixed; it must then include at least one more than three characters else it is a three cycle, and if it only moves four, it is an odd permutation. Let two other elements in $\sup(\varphi)$ be denoted r and s. Let $\tau = (k, r, s)$, and, as before, consider $\tau\varphi\tau^{-1}\varphi^{-1}$. Then this new permutation leaves i fixed, and is not the identity, a contradiction. Our assumption was that φ was not a three cycle, thus it must be. □

The fact that A_4 is not simple results in far reaching ramifications in Galois theory, where it implies that there is no formula for finding the roots of quintic polynomial roots.

Exercise 5.1. If X is a G set that is not a singleton, then there is an element x in X with no fixed points.

Exercise 5.2. Suppose we have n prisoner's in jail, sentenced to death. The executioner's offer the prisoners a way to escape their judgement. They place n boxes in a room, each with a number from 1 to n in it, and a separate number from 1 to n inscribed on it (not related to the number inside the box in any way). They give each prisoner a unique number in the same manner of the boxes, and give each an opportunity. Each prisoner can open $n/2$ boxes, and if he finds inside a box a number sharing his or her own, then he succeeds his task. If every prisoner accomplishes this task, no-one will be executed. The naive method of solving this problem accomplishes this with a probability of less than 1%. Show, using the methods of permutations and cycles, that the prisoner's can design a strategy that leads to a 30% chance of success.

CHAPTER 6

Sylow Theory

In 1872, Norwegian mathematician Ludwig Sylow proved a collection of theorems, called the Sylow theorems, which give detailed information about subgroups of a certain size within a group. Unlike the majority of chapters in this book, we begin with a theorem, rather than a definition. A strange methodology used in this proof will be used throughout the chapter: we induct on the size of the group.

THEOREM 6.1. For every finite abelian group, and every prime number which divides the order of the group, there is an element whose order is that prime number.

PROOF. Let G be an abelian group, and p a prime number such that $p \mid |G|$. We prove this statement by induction on $|G|$. When $|G| = 1$, the statement holds vacously. Now suppose this theorem holds for all group sizes less than the order of another group G. Take an element g in G that is not the identity. If the order of g is pm, then g^m is order p. Instead, assume that g's order is not divisible by p. Since G is abelian, $\langle g \rangle$ is normal, hence we can form the group $G/\langle g \rangle$. We know that $|G| = |G/\langle g \rangle||\langle g \rangle|$. We know that $|\langle g \rangle|$ does not divide p, hence p must divide $|G/\langle g \rangle|$. As g is not the identity, we know the factor group is smaller than G, hence by induction, there is some element h in G such that $h\langle g \rangle$ is order p. Let n be the order of h. Then of course, since $h^n = e$, $p|n$. Using the same technique as before, we can obtain an element of order p from powers of h. □

A theorem of Cauchy generalizes this idea to arbitrary groups.

THEOREM 6.2 (Cauchy's theorem). Given any group whose order divides a prime, there is an element whose order is that prime.

PROOF. We prove this theorem by induction again. We need no base case, as a group of any size less than 6 is abelian and thus we can apply Theorem (6.1). Now suppose the theorem holds for all groups of order less than a group G. Let p be a prime, and suppose $p \mid |G|$. If G contains a proper subgroup whose order

is divisible by p, then we can apply induction rather easily to show that this theorem holds for G. The hard part is when G contains no proper subgroup whose order is divisible by p. Consider G acting on itself by conjugation. For every element g, the centralizer $C_G(g)$ is a subgroup of G. By Lagrange's theorem,

$$|G| = |C_G(g)|(G : C_G(g))$$

The class equation also gives us that

$$|G| = |Z(g)| + \sum_{k=1}^{n-1} (G : C_G(x_i))$$

If g is not in $Z(g)$, $C_G(g)$ is a proper subgroup of G, so by our assumption $p \nmid |C_G(g)|$, and by the equation created by Lagrange's theorem, we obtain that $p \mid (G : C_G(g))$. But then by rearranging the class equation, we obtain that $p \mid |Z(g)|$, hence $Z(g)$ cannot be a proper subgroup, and so $G = Z(g)$. Thus G is abelian, and we can apply (12.1) again. By case to cases analysis we obtain the truth of the statement. □

Definition 26. Let p be a prime number. A group G is called a **p-group** if the groups order is a power of p.

By Cauchy's theorem, we obtain an interesting corollary: a group is a p-group if and only if every element has order a power of a prime.

Lemma 6.3. Let G be a p-group. If G acts on a finite set X, then the fixed points X^G satisfies

$$|X^G| \equiv |X| \pmod{p}$$

Proof. It was previously proven that $|X| = |X^G| + \sum_{k=1}^{n-1} (G : G_{x_i})$, the class equation. For each G_{x_i}, we have that $p \mid (G : G_{x_i})$ by an easy application of Lagrange's theorem. This shows exactly the equation we were attempting to prove. □

Lemma 6.4. Let $G \neq \{e\}$ be a p-group. Then the center $Z(G) \neq \{e\}$.

Proof. Let G act on itself by conjugation. Then by Lemma (12.3), we have the $|Z(G)| \equiv |G| \pmod{p}$, so $|Z(G)| \equiv 0 \pmod{p}$ since $p \mid G$. We obtain that there are at least p elements that are fixed points, since there is at least one element that is in the group, the identity. □

Corollary 6.5. Let p be a prime. Every group of order p^2 is abelian.

Proof. Let G be a group of order p^2. According to Lemma (12.4), the center $Z(G)$ of G is non-trivial. Since $Z(G)$ is a subgroup, it thus must be order p or p^2 by Lagrange's theorem. Suppose that $Z(G)$ is order p, and let h be an element such that $h \notin Z(G)$. Also consider conjugation acting from G to itself. Then G_h is a group larger than $Z(G)$, since h itself is in G_h and h is in $Z(G)$, so we

conclude that G_h must be order p^2 since it too is a subgroup of G. This means of course that every element commutes with h, so h is in $Z(G)$, a contradiction. Hence $Z(G)$ is order p^2, and it follows that G is abelian. □

Now, to the real meat of the chapter – the proper Sylow Theorems!

Definition 27. Let G be a group of order $p^m q$, where p is a prime and q and p are relatively prime. Then a subgroup is called a **p-Sylow Subgroup** if the order of the subgroup is a power of p^m – the maximum order of a p subgroup in G.

In the next few proofs, let G be a group of cardinality $p^m q$.

Lemma 6.6. For every k such that $1 \leqslant k \leqslant m$, there is a subgroup of G of order p^k.

Proof. We prove by induction on the size of m. Observe if $m = 0$, the theorem holds trivially; simply consider the trivial subgroup. Now suppose by induction that for all groups of smaller cardinality than G the theorem holds. Consider the group action of conjugation of G acting on itself. We know by the class equation that

$$|G| = |Z(G)| + \sum_{i=1}^{n-1} (G : C_G(x_i))$$

We consider two cases to our proof. One where p divides the center group, and one where it does not. Suppose that $p \nmid |Z(G)|$. This implies that there is at least one x_i such that $p \nmid (G : C_G(x_i))$, as otherwise we could move the indexes to the left hand side of the equation and conclude that $p \mid |Z(G)|$. By Lagrange's theorem, $|G| = (G : C_G(x_i))|C_G(x_i)|$, and hence $p \mid |C_G(x_i)|$. We know that $|C_G(x_i)| = p^m q'$, as the index takes no powers of p away, and $q' < q$, as otherwise $C_G(x_i) = G$, and hence $Z(G)$ is empty. Hence we can use induction to show there is a subgroup of order p^k for each in $C_G(x_i)$ and hence in G for each k that we want. On the other size, suppose $p \mid |Z(G)|$. By Cauchy's theorem, we conclude there is some element g of order p. Since $Z(G)$ commutes with elements of G, every subgroup of $Z(G)$ is normal in G. Thus $\langle g \rangle \triangleleft G$. $G/\langle g \rangle$ is thus a group of order $p^{m-1}q$, so by induction there is a subgroup H of $G/\langle g \rangle$ such that $|H| = p^{k-1}$. H can be written as $V/\langle g \rangle$ for some subgroup V of G, and by Lagrange's theorem, $|V| = |H||\langle g \rangle| = p^{k-1}p = p^k$. □

Lemma 6.7. Let H be a p-subgroup of G, and P a p-Sylow subgroup. If $H \subset N_G(P)$, then $H \subset P$.

Proof. We know that HP is also contained in the normalizer, and $P \triangleleft N_G(P)$. But by the second isomorphism theorem, we know that

$$(HP : P) = (H : H \cap P)$$

Hence by Lagrange's theorem, $HP = |H|/(|H \cap P||P|)$, and since each number on the right hand side is a power of p, so must $|HP|$. Since $HP \geqslant P$, we must have $HP = P$, else HP is a p-group greater than the biggest exponentional of p in G, the p-Sylow group P. From the fact that $HP = P$ we conclude $H \subset P$. □

This theorem can be easily strengthened.

THEOREM 6.8. If H is any p-subgroup of G, and P a p-Sylow subgroup. Then H is contained in some p-Sylow subgroup of G that is conjugate to P.

PROOF. Consider the set X of cosets gP for g in G, and let H act on X by the mapping

$$h(gS) \mapsto hgS$$

The cardinality of X is $|G|/|P| = q$. We know that the number of fixed points of the action is congruent to q modulo p, and since q is relatively prime to q, we know that this number cannot be zero. Thus there exists gP such that $hgP = gP$ for all h in H, and thus $h = gsg^{-1}$ for each and every element h. Thus $H \subset gPg^{-1}$. Since gPg^{-1} is conjugate to P, it too is a p-Sylow subgroup, and hence we obtain the statement above. □

COROLLARY 6.9. All p-Sylow subgroups are conjugate.

PROOF. In the previous proof, let H be p-Sylow. Then H is contained in some conjugate p-Sylow subgroup to P. But H is the same size as this conjugate group, and hence H is equal to this conjugate p-Sylow subgroup. □

COROLLARY 6.10. If there is only one p-Sylow subgroup, the group is normal.

PROOF. If P is the unique p-Sylow subgroup in a group G, then, for every g in G, $g^{-1}Pg$ is a p-Sylow subgroup. But then this means $g^{-1}Pg = P$. □

THEOREM 6.11. Let s be the number of p-Sylow Subgroups of G. Then $s|q$.

PROOF. Let S be a p-Sylow subgroup of G of order p^k, and let X be the set of all p-sylow subgroups of G. Since all p-Sylow subgroups are conjugate to each other, the action of conjugation from G on X is transitive. Consider the normalizer $N_G(S)$. We obtain the class equation

$$|X| = (G : N_G(S))$$

hence $(G : N_G(S)) = s$. By the multiplicative property of indices,

$$(G : S) = (G : N_G(S))(N_G(S) : S)$$

By Lagrange's Theorem, we get that $(G : S) = |G|/|S| = p^m q/p^m = q$, hence the statement that $s \mid q$. □

THEOREM 6.12. If s is the number of p-Sylow subgroups, then $s \equiv 1 \pmod{p}$

PROOF. Let S be a p-Sylow subgroup. S acts on the set of all p-Sylow subgroup X via conjugation. We claim that S is the only fixed point in this action. We know that if S' is a fixed point, then $S \subset N_G(S')$. But then by Lemma (6.7) that $S \subset S'$. Both are the same size, hence $S = S'$. Thus S is the uniqued fixed point of the action. We then have proved our theorem, as $|X| \equiv |X^S| \pmod{p}$, by lemma (12.3), and $|X^S| = |\{S\}| = 1$. □

The theorems above are really powerful to treating groups of finite order. Here is a powerful theorem.

THEOREM 6.13. Let p and q be prime numbers such that $q < p$, and $p \nmid (q-1)$. Then every group of order pq is cyclic.

PROOF. Let S be a p-Sylow subgroup of G, and U a q-Sylow subgroup of G. Then the order of S is p and the order of U is q, and the groups are cylic. As the two are not equal, $S \cap U = \{e\}$, as this is a subgroup and thus must divide both primes. Let s be the number of p-Sylow subgroups, and r the number of q-Sylow subgroups. Then we know from theorem (12.9) that

$$r \equiv 1 \pmod{q} \qquad s \equiv 1 \pmod{p} \qquad s \mid q$$

As $s \mid q$, we know that $s = 1$ or $s = q$. If $s = q$, then $q \equiv 1 \pmod{p}$, hence $q-1 \equiv 0 \pmod{p}$, and thus $p \mid q-1$, a contradiction. Hence $s = 1$, and thus S is normal. It follows that SU is a subgroup of G. if $su = s'u'$, then $s'^{-1}s = u'u^{-1}$, and since the two groups are disjoint, $s'^{-1}s = u'u^{-1} = e$. Thus each su is distinct, and we must have $|S||U|$ elements in SU. Then SU contains qp elements so $SU = G$. We obtain that $G \equiv S \times U$. □

THEOREM 6.14. Let G be a group with cardinality p^2q, where p and q are prime, $p < q$, and $p \nmid (q-1)$. Then G is abelian.

PROOF. If s is the number of p-Sylow subgroups, and r the number of q-Sylow subgroups, then we have the following equations, as in the last proof.

$$r \equiv 1 \pmod{q} \qquad s \equiv 1 \pmod{p} \qquad s \mid q^2$$

□

THEOREM 6.15. Let G be a finite group, and p the smallest prime of G. A subgroup of index p is normal in G.

PROOF. Let H be a subgroup of G of index p. Consider G/H. G acts on G/H by operation on the left. This is a homomorphism from G to S_p. Suppose g is in the kernel of hormomorphism. Then $gg'H = g'H$ for every coset $g'H$. In particular, $gH = H$, hence g is in H. Let the kernel of the homomorphism be K. Then G/K is isomorphic to a subgroup of S_p, and hence its cardinality must divide $p!$. But

this means that

$$(G : K) = (G : H)(H : K) = p(H : K) \mid p!$$

hence $(H : K) \mid (p-1)!$. Now p is the smallest factor in $|G|$, and $(H : K) \mid |G|$, hence the only possible conclusion is that $(H : K) = 1$, else $|G|$ has a smaller factor. This means exactly that $H = K$, and hence H is normal in G as it is the kernel of a homomorphism. □

CHAPTER 7

Solvability

Solvability is the key to Galois' proof of the insolvability of the quintic. Furthermore, solvability is used in many more advanced settings throughout algebra. Thus it makes sense to introduce it in a group theory course before Galois theory to smoothen the transition between the theories.

Definition 28. Let G be a group. A **series** or **tower** is a finite sequence of groups beginning with G, and such that every sequential group is a subgroup of the previous.

To aid in remembering the definition, we write a sequence $(G_0, G_1, \ldots, G_m)$ which forms a tower as

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m$$

This chapter focuses on a very specific type of tower.

Definition 29. A tower is called a **normal series** if every group in the tower is normal in its predecessor, so for each G_i that is not at the end, we may form the factor group G_i/G_{i+1} with the next element in the sequence. A normal series is **abelian** if each such factor group is abelian, and **cyclic** if every factor group is cyclic.

As with the notation for an ordinary tower, we write a normal series $(H_0, H_1, \ldots, H_m)$ as

$$H = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m$$

so you needn't remember the definition if you're reading someone elses work; the notation tells you all you need to know!

Theorem 7.1. Consider a normal tower

$$H = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m$$

and a homomorphism φ from G to H. Define a tower on G by letting G_i be $\varphi^{-1}(H_i)$. The tower then formed is a normal series. This tower is abelian/cyclic if and only if the other tower is abelian/cyclic.

PROOF. As φ is any mapping from G to H, we have that

$$G_0 = \varphi^{-1}(H_0) = \varphi^{-1}(H) = G$$

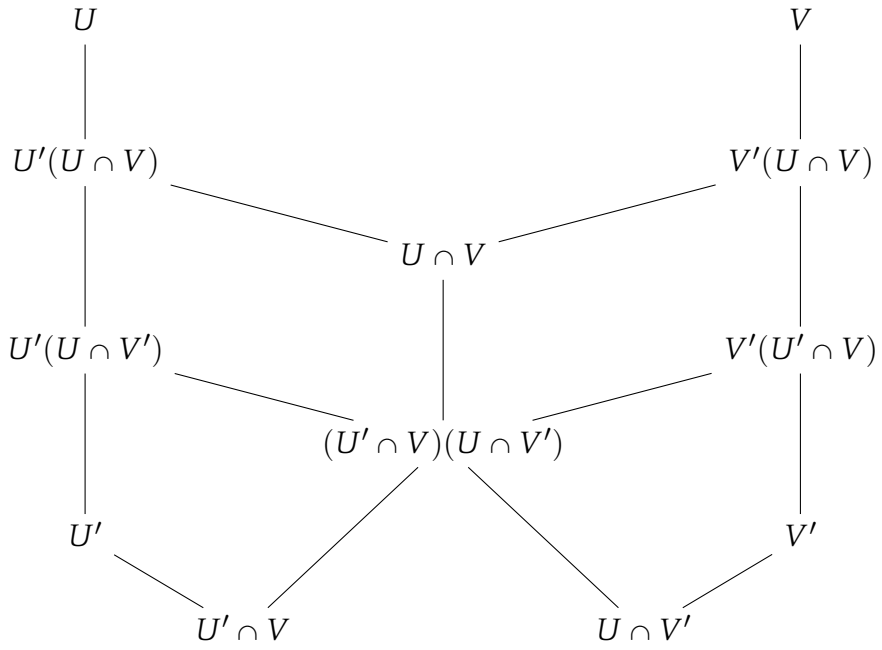
Now we know H_{i+1} is normal in H_i for any index i for which H_i is defined. Restrict φ to only elements of G_i. Then φ is of course surjective onto H_i; we are then in the same position as Exercise (12), and we may conclude that G_{i+1} is normal in G_i, and $G_i/G_{i+1} \cong H_i/H_{i+1}$, hence all algebraic properties needed transfer from the factor group of H to the factor group of G. □

The property of having a normal tower is not special. For any group G, simply take the tower $G \supset \{e\}$, and that tower is trivially normal, but its factor groups do not really tell us anything about the group. The longer the tower, the more we separate the properties of the entire group as factor groups. It thus makes sense to take a tower that is maximalized in some way, to strain out as many properties as possible from the group.

DEFINITION 30. A **refinement** of a tower is a new tower obtained by inserting finitely more subgroups into the original tower.

DEFINITION 31. We say two normal series S and T are **equivalent** if they have the same length and such that there is a permutation φ such that, for any group S_i in S but the terminating subgroup, $S_i/S_{i+1} \cong T_{\varphi(i)}/T_{\varphi(i)+1}$, so the factor groups obtained can really just be considered reorderings of one another.

The following lemma leads to an easy proof on the refinement of normal series. It's proof is perhaps the most technical in this report, but it at least has a nice picture corresponding with the lattice of subgroups to go along with it.



THEOREM 7.2 (The Butterfly Lemma (Zassenhaus' Lemma)). Let U and V be subgroups of a group G, and let U', V' be such that $U' \lhd U$, $V' \lhd V$. Then

$$U'(U \cap V') \lhd U'(U \cap V)$$

$$V'(U \cap V) \lhd V'(U \cap V)$$

and the factor groups are isomorphic:

$$\frac{U'(U \cap V)}{U'(U \cap V')} \cong \frac{(U \cap V)}{(U' \cap V)(U \cap V')} \cong \frac{V'(V \cap U)}{V'(V \cap U')}$$

PROOF. Our main strategy is to identify an isomorphism from the first formula to the second in the equation via the first isomorphism theorem. We will define a mapping from $U'(U \cap V)$ to $(U \cap V')/(U' \cap V)(U \cap V')$. Let the following mapping $u'x \mapsto x(U' \cap V)(U \cap V')$ be constructed. This mapping is well defined: If it is true that $ux = u'x'$, then $u'u^{-1} = xx'^{-1} \in U' \cap (U \cap V) = U' \cap V \subset (U' \cap V)(U \cap V')$, hence $x(U' \cap V)(U \cap V') = x'(U' \cap V)(U \cap V')$. Let us hope that the kernel of this mapping is $U'(U \cap V')$. We know that the kernel is precisely those elements representable as $u'x$, where $x \in (U' \cap V)(U \cap V')$, or that $u'x$ is an element of $U'(U' \cap V)(U \cap V') = U'(U \cap V')$, hence the kernel is $U'(U \cap V')$, and we have shown the isomorphism from first formula to second by the first isomorphism theorem, as the map is surjective. As the problem is symmetric, we obtain the isomorphism from third to second, and thus the entire chain of isomorphisms is created by transitivity of isomorphism. □

Do not worry if the statement above is unintuitive. It is only really a mechanic to be used in the next Theorem, and the author knows of no other use of it outside of this context.

THEOREM 7.3 (Shreier). Two normal series in a group G ending with the trivial group have refinements that are equivalent.

PROOF. Consider two normal towers

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$
$$G = G_0' \rhd G_1' \rhd \cdots \rhd G_m' = \{e\}$$

Define $G_{i,j} = G_{i+1}(G_j' \cap G_i)$ for i between 0 and $n-1$ and j between 0 and m. Then we have the tower

$$\begin{aligned} G = G_1(G) &= G_1(H_0 \cap G_0) \\ &= G_{0,0} \supset G_{0,1} \supset \cdots \supset G_{0,m} \supset G_{1,0} \supset \ldots \supset G_{n-1,m} \\ &\qquad = G_n(H_m \cap G_{n-1}) = \{e\} \end{aligned}$$

Similarily, if we define $G_{i,j}' = G_{i+1}'(G_j \cap G_i')$, with a tower of G_j' generated in a similar fashion. By the butterfly lemma, with $U = G_{i+1}$, $U' = G_i$, $V = G_{j+1}'$, and $V' = G_j'$, we obtain that

$$G_{i,j}/G_{i,j+1} \cong H_{i,j}/H_{i,j+1}$$

We must also show the equivalency for $G_{i,m}$, $G_{i+1,0}$, $G_{i,m}'$, and $G_{i+1,0}'$. What are these groups?

$$G_{i,m} = G_{i+1}(G_m' \cap G_i) = G_{i+1}\{e\} = G_{i+1}$$
$$G_{i+1,0} = G_{i+2}(G_0' \cap G_{i+1}) = G_{i+2}G_{i+1} = G_{i+1}$$
$$G_{i,m}' = G_{i+1}'$$
$$G_{i+1,0}' = G_{i+1}'$$

and hence

$$G_{i,m}/G_{i+1,0} \cong \{e\} \cong G_{i,m}'/G_{i+1}$$

We have verified the tower is normal and equivalent. They also refine the original towers as

$$G_{k,0} = G_k(G_0' \cap G_{k-1}) = G_k(G \cap G_{k-1}) = G_k G_{k-1} = G_k$$

and similarily for $G_{k,1}'$, so we may embed the original tower in the new one. □

The main corollary requires a new concept, which follows so simply we state it without proof.

DEFINITION 32. A **composition series** is a normal series which cannot be refined.

COROLLARY 7.4 (Jordan Hölder). All composition series of a set G are equivalent.

All finite groups possess a composition series, as there are only finitely many subgroups of the group. We note this is not true of all groups. Consider the additive group $\mathbf{Z}$. Then every subgroup is of the form $a\mathbf{Z}$ for some a, and every subgroup is normal. Suppose we have a normal series

$$\mathbf{Z} \rhd a_1\mathbf{Z} \rhd a_2\mathbf{Z} \rhd \cdots \rhd a_n\mathbf{Z}$$

Then we can always refine it to

$$\mathbf{Z} \rhd ma_1\mathbf{Z} \rhd a_1\mathbf{Z} \rhd a_2\mathbf{Z} \rhd \cdots \rhd a_n\mathbf{Z}$$

for any integer m greater than one. This shows that there are no composition series because, given any series, we can always refine it.

Composition series can be considered the maximality of a normal series. Simple groups are minimalizations of normality. It is intuitive to connect these concepts. This theorem characterizes this.

THEOREM 7.5. A normal series is a composition series if and only if all factor groups in the series are simple.

PROOF. Consider an arbitrary normal series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

Suppose G_k/G_{k+1} is not simple, so the factor group posesses a normal subgroup $(G_k/G_{k+1})_S$. By the lattice isomorphism theorem, there is a subgroup S such that $G_k \subset S \subset G_{k+1}$, and S is normal in G_{k+1}. Since G_{k+1} is normal in G_k, G_{k+1} is also normal in S, hence we have a refined normal series. This proof by contraposition shows that all factor groups are simple in a composition series. Of course, if a normal series is such that every factor group is simple, it must follow that the series cannot be refined, because the existence of a refinement shows exactly that there is a normal subgroup between the two, hence the tower is a composition series. □

We now proceed to specialize to a particular type of normal series. First, a lemma.

THEOREM 7.6. From any abelian tower of an abelian group we can construct a cyclic tower.

PROOF. Let us prove this for all abelian groups, by by induction on the order of the group. For a base case, we note any abelian tower on the trivial group $\{e\}$ is cyclic. Now, consider an abelian group G of order n where an abelian tower of any smaller group can be constructed into a cyclic tower. Suppose we have an abelian tower

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m$$

Consider a non-zero group element g in G, and the quotient group $G/\langle g\rangle$. We still have an abelian tower

$$G = G_0/\langle g\rangle \rhd G_1/\langle g\rangle \rhd \cdots \rhd G_m/\langle g\rangle$$

Because by the third isomorphism theorem, the quotient groups are isomorphic to the original abelian tower's quotient groups. By induction, we can construct refine this tower into a cyclic tower. We have the canonical homomorphism from G to $G/\langle g\rangle$, hence the inverse image is a cyclic tower in G. Thus the statement holds for all finite abelian groups. □

Corollary 7.7. An abelian tower on any group admits a cyclic refinement.

Proof. Suppose for a group G we have an abelian tower

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m$$

The lattice isomorphism theorem establishes a bijection between subgroups of G/X and subgroups of G that contain X. Consider a pair G_i and G_{i+1} in the tower. We have an abelian tower $G_i/G_{i+1} \rhd \{e\}$, and G_i/G_{i+1}, so we have a cyclic refinement of this tower. By Theorem (7.1), we can bring this refinement back to G, and this will also be cyclic, beginning with G_i, and ending with G_{i+1}. Thus we can refine our original abelian tower with the cyclic tower constructed from each pair G_i and G_{i+1} to form a new abelian tower. □

Definition 33. A group is **solvable** if it has an abelian tower whose last element is the trivial subgroup $\{e\}$.

Here we provide an explicit example before moving to the abstract. Consider the group $GL_n(\mathbf{F})$. Let $N_n(\mathbf{F})$ be the set of elements that are zero both on and below the diagonal. For any r between 1 and n, the set $U_r = I_n + (N_n(\mathbf{F}))^r$ is a subgroup of $GL_n(\mathbf{F})$ (the determinant of all the matrices is 1). For U_k, define a mapping from U_k to the additive group $\mathbf{F}^{n-k}$ by taking the k'th upper diagonal. That is, if a matrix $M_n = [m_{i,j}]$. Then $M_n \mapsto (a_{1,k}, a_{2,k+1}, \ldots, a_{n-k,n})$. This is an homomorphism because U_k is a matrix of the form

$$\begin{pmatrix}
1 & 0 & \ldots & 0 & a_{1,k} & \ldots & \ldots & a_{1,n} \\
0 & 1 & \ldots & 0 & 0 & a_{2,k+1} & \ldots & a_{2,n} \\
0 & 0 & \ddots & 0 & 0 & 0 & \ddots & \vdots \\
0 & 0 & \ldots & 1 & 0 & 0 & \ldots & a_{n-r,n} \\
0 & 0 & \ldots & \ldots & \ddots & \ldots & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

and hence for any two matrices $M = [a_{i,j}]$ and $N = [b_{i,j}]$ in U_k, $MN = [c_{i,j}]$ fits the equations $c_{n,k+n-1} = a_{n,k+n-1} + b_{n,k+n-1}$ (the identity matches up with the r'th column). The kernel of the homomorphism is U_{k+1}, hence U_{k+1} is normal in U_k, and $U_k/U_{k+1} \cong F^{k-r}$ and the factor group is abelian. Thus the sequence (U_k) is an abelian tower, and U is solvable.

Here is a simpler example. Let G be an abelian group. Then the series $G \triangleright \{e\}$ is an abelian tower, because $G/\{e\} \cong G$, and is hence abelian. Thus G is solvable.

THEOREM 7.8. A subgroup of a solvable group is solvable.

PROOF. Consider a solvable group G, and a subgroup H. Consider the tower that makes G solvable.

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

From this tower, construct a new sequence (H_k), where $H_k = G_k \cap H$. We know that, since G_k is normal in G_{k+1}, so too are H_k and H_{k+1} The second isomorphism theorem tells us that

$$(H \cap G_{i+1})/(H \cap G_i) = (H \cap G_{i+1})/(H \cap G_i \cap G) \cong (H \cap G_{i+1})G_i/G_i \subset G_{i+1}/G_i$$

and thus H_i/H_{i+1} is abelian. □

THEOREM 7.9. Let G be an arbitrary group, and H an arbitrary normal subgroup. G is solvable if and only if both H and G/H are.

PROOF. Let G be a solvable group, with an abelian tower

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

Given this abelian tower, consider the canonical mapping π from G to G/H, and define a new sequence (H_k) such that $H_k = \pi(G_k)$. We know H_k is normal in H_{k+1} by Exercise 13. Furthermore, we know that $H_k = G_k/H$, hence, by the third isomorphism theorem,

$$H_k/H_{k+1} = (G_k/H)/(G_{k+1}/H) \cong G_k/G_{k+1}$$

Conversely, suppose that H and G/H is solvable. Then by Theorem (7.1) we can construct an abelian tower on G, which ends with $H = \pi^{-1}(e)$. Combine this with the abelian series on H, and we obtain that G is solvable. □

DEFINITION 34. Let G be a group. A **commutator** is an element of G that can be written $ghg^{-1}h^{-1}$, for two elements g and h in G, which we also write as $[g,h]$. Define the **commutator** or **derived subgroup** $D(G)$ of the group G to be the group generated by the set of commutators in G.

LEMMA 7.10. For any G, $D(G)$ is normal in G.

Proof. Let g be an element of G, and $hkh^{-1}k^{-1}$ an element of $D(G)$,

$$ghkh^{-1}k^{-1}g^{-1} = (ghg^{-1})(gkg^{-1})(gh^{-1}g^{-1})^{-1}(gkg^{-1})^{-1}$$

Hence it is an element of the commutator. We leave it to the reader to prove that, if gkg^{-1} holds for every k in a set K which is a subset of a group G, from which g reside, then $\langle K \rangle$ is normal in G. □

Lemma 7.11. For any group G, $G/D(G)$ is commutative.

Proof. For any gh, $g^{-1}h^{-1}gh$ is in $D(G)$, hence

$$gD(G)hD(G) = ghD(G) = ghg^{-1}h^{-1}hgD(G) = hD(G)gD(G)$$

and we have calculated that the group is commutative. □

Lemma 7.12. For any homomorphism from G to H such that H is commutative, $D(G)$ is a subset of the kernel of H.

Proof. Let φ be the homomorphism above, and let g and h be arbitrary elements of G. By doing the following calculation,

$$\varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1})\varphi(h^{-1}) = \varphi(g)\varphi(g^{-1})\varphi(h)\varphi(h^{-1}) = e$$

Since these elements generate $D(G)$, every element in $D(G)$ is composed of elements like this, which all cancel out in φ, hence $D(G)$ is in the kernel of φ. □

Corollary 7.13. If G is a group with normal group N, and G/N is abelian, then $D(G) \subset N$.

Commutator groups give us the key to unravelling the notion of solvability. We know $D(G)$ is normal in G, and we also know $D(D(G))$ is normal in $D(G)$, and so on and so forth, and each factor group created is abelian. Define $D^n(G)$ recursively by $D^n(G) = D(D^{n-1}(G))$. Via this, for each n we get a normal series

$$G \rhd D(G) \rhd D^2(G) \rhd \cdots \rhd D^{n-1}(G) \rhd D^n(G)$$

If it eventually holds that $D^n(G) = \{e\}$ for some n, then we obtain an abelian series, and G is solvable. What is amazing is this statement holds in reverse.

Theorem 7.14. If a group G is solvable, $D^n(G) = \{e\}$ for some n.

Proof. Suppose G is solvable, and hence has an abelian normal series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

For each r, $D(G_r) \subset G_{r+1}$, as G_r/G_{r+1} is abelian. We claim $D^r(G) \subset G_r$. How do we prove this? Well $D(G) \subset G_1$, hence $D^2(G) \subset D(G_1) \subset G_2$. Thus the claim follows by induction. It follows that $D^n(G) \subset \{e\}$, and the two groups are hence equal as the only subgroup of the trivial group is itself. □

The main use of this theorem is not to show other groups are solvable, but to show that some groups are not solvable. Solvability began solely to answer questions in Galois field theory, which considers permutations of polynomial equations. This is just a representation of the symmetric group. You should see the connection between the following theorem and the insolvability of the quintic equation, at least in the numbers used.

THEOREM 7.15. S_n is not solvable when $n \geqslant 5$.

PROOF. Let i,j,k,r,s be 5 distinct characters that are being permuted in S_n. Let $\sigma = (i\ j\ k)$, and let τ be $(k\ r\ s)$. Then

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = (r\ k\ i)$$

As each r, k, and i were arbitrary, we know all three cycles are in $D(S_n)$. As only three cycles were used in the commutators above, all three cycles are also in $D^2(S_n)$, and so on inductively, hence we will never have $D^m(S_n) = \{\mathbf{1}\}$. Thus S_n is not solvable. □

THEOREM 7.16. If G is a p-group, G is solvable.

PROOF. Let G be of cardinality p^m. We proved in Lemma (6.6) that for any k between 1 and $m-1$ there is a subgroup of order p^k. In particular, there is a subgroup of order p^{m-1}. Denote this group G_1. G_1 is normal in G, and G/G_1 is of order p, so the group must be cyclic as p is prime. By induction, we must do this for G_1, G_2, etc. to construct a normal series where each factor group is cyclic. □

CHAPTER 8

Direct Products and Abelian Groups

This chapter presents methods for constructing new groups from smaller ones. By doing this, we will be able to break down a group into smaller, component groups via the reverse of this technique. We call a construction of this form the direct product.

Definition 35. Consider an indexed family of groups $\{G_i\}_{i\in I}$. The direct product of these groups, denoted $\times_{i\in I} G_i$ is the group formed by taking the cartesian product of elements in each G_i. The operation defined on the group is

$$\left[\bigtimes_{i\in I} g_i\right] \circ \left[\bigtimes_{i\in I} h_i\right] = \left[\bigtimes_{i\in I} g_i h_i\right]$$

where the operation is just taken coordinatewise.

Each individual group G_i in the direct product of a group can be studied in order to understand the entire direct product. If we can identify a group as isomorphic to the direct product of a set of groups, then we can understand the group by understanding each individual group from which it is structured. The following method shows how we can deconstruct a group into its direct products.

Theorem 8.1. If a group contains two subgroups who are disjoint but for the identity, commute with each other, and whose product contains the whole group, then the whole group is isomorphic to the direct product of the two subgroups.

Proof. Let G be a group, with two subgroups H and K such that $H \cap K = \{e\}$, H and K commute, and $HK = G$. Define a mapping φ from $H \times K$ to G by the calculation $(h,k) \mapsto hk$. Since H and K commute,

$$\varphi((hh',kk')) = hh'kk' = hkh'k' = \varphi(h,k)\varphi(h',k')$$

It follows that φ is a homomorphism. If $hk = e$, then $k = h^{-1}$, so k is in both H and K, which means $k = e$ as H and K are disjoint but for the identity. We have shown exactly that the kernel of the function φ is trivial. Furthermore,

φ is surjective, as $HK = G$. It has been shown that φ is an isomorphism, and therefore G is isomorphic to $H \times K$. □

An example of a direct product that we are very familiar is is the additive vector group $\mathbf{F}^n$, which is isomorphic to the direct product $(\times_{k=1}^{n} \mathbf{F})$. In general, for any ring R, the module R^n is isomorphic to $(\times_{k=1}^{n} R)$.

Another example is the group $E_{p^n} = (\times_{k=1}^{n} \mathbf{Z}/p\mathbf{Z})$, where p is a prime. The group is of order p^n; in general, a group $(\times_{k=1}^{n} G_i)$ has cardinality $\prod_{k=1}^{n} |G_i|$. Each non-trivial element is of order p. Consider the group E_{p^2} for some prime p. We know that if G and H are two subgroups of order p, then $G \cap H = \{e\}$ unless the two groups are equal. Thus if m is the number of p subgroups, then E_{p^2} possesses at least $(p-1)m+1$ distinct elements. Thus $(p-1)m+1 \leqslant p^2$, from which we conclude that m is bounded above by $p+1$. We leave it to the reader to identify the $p+1$ distinct subgroups which bound m below, from which we can conclude that m is exactly equal to $p+1$.

For each group G_k in a direct product $\times_{i \in I} G_i$, we have a homomorphism π_k from $\times_{i \in I} G_i$ to G_k defined by the surjective mapping $(\times_{i \in I} g_i) \mapsto g_k$. The kernel of this mapping is the set of all elements $(\times_{i \in I} g_i)$ such that $g_k = e$, and hence we can quotient this kernel out to get a direct isomorphism to G_k. Think of G_k as the coordinate axis in the direct product group.

Direct products are the key to classifying a certain class of abelian groups. The ideas of this classification you have probably learned before you even read this article; there is a distinct connection to the ideas of linear algebra. Here is the special class of abelian groups we will classify.

Definition 36. A group is finitely generated if it is generated from a finite set.

It will help to introduce some notation to deal with splitting up components of abelian groups. We note the formal definition in the infinite case is not used for now, but we include it for thoroughness.

Definition 37. Given a collection of abelian groups $(G_i)_{i \in I}$, we define the **direct sum** $\bigoplus_{i \in I} G_i$ to be the subgroup of the direct product of those groups consisting of all elements where there are only finitely many elements that are non-identity elements. In the case of a finite product of elements, the direct sum is equivalent to the direct product.

You can probably see how abelian groups connect to vector spaces. In some sense, vector spaces are the canonical abelian if you consider their addition as the fundamental operation that defines them. The definitions below should be familiar to you from a study of vector spaces.

Definition 38. If an abelian group is generated by a set S, then that set is a **basis** if every element in the group is uniquely represented by a sum of elements in S. If a group has a basis, we say the group is **free**.

For every set S, there is an abelian group whose basis is S. Let us construct this group. Consider the set of mappings from S to $\mathbf{Z}$. In particular, consider the mappings that assign 1 to some element s in S, and 0 to every other element. Then this set forms a basis to all of the function group, and we can consider S to be the basis of this set. The group we have constructed is called the free abelian group generated by S, which is commonly denoted $F_{ab}(S)$. Every free group is isomorphic to the free abelian group generated by its basis.

Theorem 8.2. Every abelian group is isomorphic to a factor group of a free abelian group.

Proof. Consider an abelian group G. Take a generating set S of G (in the worst case, we may take G as the generating set). Form the abelian group $F_{ab}(S)$. Define a homomorphism φ from $F_{ab}(S)$ to G by $\varphi(\sum_{k=1}^{n} n_k g_k) = \sum_{k=1}^{n} n_k g_k$. This homomorphism is surjective, hence G is isomorphic to the factor group by the kernel of the homomorphism with $F_{ab}(S)$. □

In particular, if an abelian group is finitely generated, this group is isomorphic to a factor group of $\mathbf{Z}^n$ for some n. This means if we want to classify all finitely generated abelian groups, we first must must classify subgroups on $\mathbf{Z}^m$ for every m. We will now build up the mechanics of how we can classify this.

Lemma 8.3. If a homomorphism φ maps from an abelian group G onto a free abelian group H, then G is isomorphic to the direct sum of the kernel of φ and H.

Proof. Let $h_{i\,i\in I}$ be a basis for H. For each h_i, consider some g_i in G such that $f(g_i) = h_i$. Take the group C generated by the set of elements g_i. We claim C is isomorphic to H. We know that φ restricted to C is still surjective, and if $\varphi(\sum_{i\in I} n_i g_i) = 0$, then $\sum_{i\in I} n_i h_i = 0$, hence all n_i are zero, which means $\sum_{i\in I} n_i g_i = 0$. Hence φ is injective when restricted to C, and we obtain an isomorphism. Let K be the kernel of φ. We have shown $C \cap K = 0$. Now we must show $C + K = G$. Let x be an arbitary element of G, and let $f(x) = \sum_{i\in I} n_i g_i$. Then $x - \sum_{i\in I} n_i h_i$. Thus $x - \sum_{i\in I}$ is in K, and $x \in K + C$. It follows that G is isomorphic to the direct sum of C and K. □

The next theorem allows us to characterize all subgroups of free groups, which connects to our objective of classifying subgroups of $\mathbf{Z}^n$.

Theorem 8.4. Every subgroup of a free abelian group with a finite basis is free, with a basis of size less than or equal to the size of the entire group.

PROOF. We prove by induction on the size of the group. If $n = 1$, the group is cyclic, and thus every subgroup is cyclic, generated by a single element which forms the basis provided the group is infinite. Now suppose that for $m \leqslant n$ this theorem holds. Let G be a free abelian group with basis $\{g_1, g_2, \ldots, g_n\}$, and consider a subgroup H. We have a homomorphism π_1 from G to $\langle g_1 \rangle$ defined by the mapping

$$\pi_1(\sum_{k=1}^{n} l_k g_k) = l_1 g_1$$

Consider the restriction of this homomorphism from H, and the resultant kernel H'. Then the range of this restricted homomorphism, and hence is of the form $\langle a g_1 \rangle$ for some integer a. The kernel H' is a subgroup contained in the group $\langle g_2, \ldots, g_n \rangle$, and hence has a basis $h_1, h_2, \ldots, h_q$, where $q \leqslant n-1$. If $a \neq 0$. By Lemma (8.3), there is a subgroup C of H isomorphic to $\langle a g_1 \rangle$, and $H = H' \cdot C$. Now C is either zero or infinite cyclic, which proves that H is free. □

COROLLARY 8.5. Every pair of bases of a finitely generated free abelian group is of the same cardinality.

PROOF. Let G a finitely generated free abelian group with two bases of size T and Q respectively. Using the basis corresponding to T, we conclude the group G/pG is a sum of T cyclic groups of order p, and is thus of cardinality p^T. Conversely, using the basis of Q, we conclude the basis is of order p^Q. But then $p^T = p^Q$, hence $T = Q$. □

The number of elements in the basis of a free abelian group is called the **rank** of the group. The problem with the proof above is it is not so easy to construct such a basis. For the next theorem, we will use the fact that any subgroup of a free group is finitely generated, but only to provide an algorithm to conclude our objective of classifying all subgroups of $\mathbf{Z}$.

THEOREM 8.6. Let G be a finitely generated abelian group, generated by a set of n elements. Then

$$G \cong \mathbf{Z}/a_1\mathbf{Z} \oplus \mathbf{Z}/a_2\mathbf{Z} \oplus \ldots \mathbf{Z}/a_r\mathbf{Z} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$$

where $r \leqslant n$ and such that $a_i \mid a_{i+1}$ for each a_i, and the number of $\mathbf{Z}$ groups in the direct product is $n - r$. This formulation is unique for any such subgroup.

PROOF. Consider the group G defined above. We know that $G \cong \mathbf{Z}^n/K$ for some subgroup K of $\mathbf{Z}^n$. Suppose we have an automorphism φ on $\mathbf{Z}^n$. Then this induces a mapping from K to another subgroup K', and $\mathbf{Z}^n/K \cong \mathbf{Z}^n/K'$. Our strategy is thus to simplify $\mathbf{Z}/K$ via these automorphisms to determine that each such group $\mathbf{Z}/K$ is isomorphic to one of the sets above. What's good about this algorithm is that it gives us a method to find this isomorphism.

Let K be a subgroup of $\mathbf{Z}^n$. Then we know that K is finitely generated by a set of elements $\{k_1, k_2, \ldots, k_l\}$. Each k_i is an array of n integers $(k_{i,1}, k_{i,2}, \ldots, k_{i,n})$, as it is an element of $\mathbf{Z}^n$. This motivates that we construct the matrix

$$\begin{pmatrix} k_{1,1} & k_{1,2} & \ldots & k_{1,n} \\ k_{2,1} & k_{2,2} & \ldots & k_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{l,1} & k_{l,2} & \ldots & k_{l,n} \end{pmatrix}$$

Can we create row and column operations which correspond to isomorphisms of $\mathbf{Z}^n$. We wouldn't be constructing this matrix if not! these are the operations we require:

- We may interchange two rows i and j. This corresponds to swapping the order of two generators in the set, which does not change the subgroup K we are operating on.
- Multiplying a row i by negative one corresponds to swapping a generator k_i with its inverse, $-k_i$. We note that this also does not change the subgroup K we are operating on.
- Adding row i to row j, where $i \neq j$, corresponds to replacing a generator k_i with $k_i + k_j$. These generators are equivalent, so K is the same.
- Interchanging Columns i and j corresponds to an automorphism of $\mathbf{Z}^n$ where we interchange two coordinates.
- Multiplying a column i by negative one corresponds to an automorphism of $\mathbf{Z}^n$ where a specific coordinate is inverted in every element.
- Adding a column i to a column j corresponds to an automorphism of $\mathbf{Z}^n$. This is perhaps the only non-trivial automorphism to see. We map a vector $(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n)$ to $(x_1, \ldots, x_i, \ldots, x_i + x_j, \ldots, x_n)$. Then $(x_1 + y_1, \ldots, x_i + y_i, \ldots, x_j + y_j, \ldots, x_n + y_n)$ is mapped to $(x_1 + y_1, \ldots, x_i + y_i, \ldots, x_i + x_j + y_i + y_j, \ldots, x_n + y_n)$, which is precisely the addition of the individual mappings, hence the mapping is a homomorphism. Verification that this mapping is an automprhism is left to the reader.

These actions are sufficient to reduce any matrix to the 'Smith Normal Form', a matrix of the form

$$\begin{pmatrix} \alpha_1 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & \alpha_n & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

where the only non-zero entries are on the diagonal, and each α_i divides α_{i+1}. How is this useful to us? It means precisely that every subgroup K can be by automorphisms transformed into $\alpha_1\mathbf{Z}\oplus\alpha_2\mathbf{Z}\oplus\cdots\oplus\alpha_n\mathbf{Z}\oplus\{0\}\oplus\cdots\oplus\{0\}$, and thus our original finitely generated abelian group is isomorphic to $\mathbf{Z}/\alpha_1\mathbf{Z}\oplus\mathbf{Z}/\alpha_2\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}/\alpha_n\mathbf{Z}\oplus\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}$. All that is left is show our method of reduction of an arbitrary integer matrix to Smith normal form. For now, we suppose it true, and we will establish the technique after this proof is complete. □

The technique to reducing an integer matrix to smith normal form turns out to be quite simple. Clearly, we need only provide a technique to reduce a matrix to the form

$$\begin{pmatrix}\alpha & 0\\ 0 & M\end{pmatrix}$$

Where M is a submatrix of one less column, and such that α divides every entry in M. By induction, the rest of the method is taken care of.

The first step of our algorithm is to check if the matrix you are reducing is the zero matrix; if this is true, we are done before we have even started. Otherwise, move the element in the matrix of smallest absolute value to the top left hand corner of the matrix, which we call the pivot. Secondly, repeatedly add or subtract the pivot row from each subsequent row such that the absolutel value of each pivot row and column entry is reduced. Do this for the pivot column from all other columns also.

Eventually, either all entries in the pivot row and column will be zero, or one will have absolute value smaller than the pivot entry. In this case, move this entry to the top left corner, and continue the process. We can only reduce the absolute value of an entry finitely many times before we are done, so eventually, the pivot row and column will be reduced to zero beside from the pivot entry.

Finally, check if the pivot entry divides every other entry in the matrix. If so, we can recurse to the submatrix. Otherwise, take the row that is not divisible by the pivot. Add this row to the first row, and return to adding and subtracting the rows and columns. This will reduce the size of the pivot, meaning we must eventually terminate.

It is best to learn an algorithm by computing out an example by hand. Here is an example. Consider a homomorphism from $\mathbf{Z}^3$ to a group G with kernel $\langle(6,3,3),(4,5,7),(3,2,2)\rangle$. What group is G isomorphic to. First, we form the matrix

$$\begin{pmatrix}6 & 3 & 3\\ 4 & 5 & 7\\ 3 & 2 & 2\end{pmatrix}$$

We bring the smallest entry, the one with the value of two, up to the pivot entry,

$$\begin{pmatrix} 2 & 3 & 2 \\ 5 & 4 & 7 \\ 3 & 6 & 3 \end{pmatrix}$$

then we reduce the row sizes

$$\begin{pmatrix} 2 & 3 & 2 \\ 1 & -2 & 3 \\ 1 & 0 & -1 \end{pmatrix}$$

and the column sizes

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & -3 & 2 \\ 1 & -1 & -2 \end{pmatrix}$$

We move the 1 on the first row to the pivot, and then reduce to get the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & -3 & -4 \end{pmatrix}$$

Continuing by induction, you should end up with a matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Which means K is isomorphic to $\mathbf{Z} \oplus \mathbf{Z} \oplus 6\mathbf{Z}$, and $\mathbf{Z}^3/K$ is isomorphic to $\mathbf{Z}/\mathbf{Z} \oplus \mathbf{Z}/\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/6\mathbf{Z}$.

EXERCISE 8.1. What is the order of $(\times_{i\in I} g_i)$ in relation to the order of each g_i in the direct product.

Index