Group Theory

Jacob Denson

June 19, 2020

Table Of Contents

Chapter 1

What is Abstract Algebra?

In mathematics, one often focuses on certain families of objects with a family of properties. In order to understand this property, it is natural to consider transformations between these objects which preserve the properties of the objects.

Example. *In Euclidean Geometry, rotations and translations preserve the angles between lines and distances between points. If we only care about such properties, we can translate and rotate any particular figure to a canonical form to simplify the situation; a triangle can always be rotated and translated to one side lies horizontally, and if we don't care about distances, we can dilate space so that one line of the triangle has length one.*

The technique of applying symmetries to simplify situations occurs over and over in mathematics, and so it is important to classify the general tools we can use when we meet new objects, and wish to understand their symmetries. The general study of symmetries in mathematics is known as *group theory*. Due to its utility, the theory provides a foundation to many rich mathematical theories.

Let us reconsider symmetries from a more abstract viewpoint. One of the basic objects of mathematics is the function, which transforms elements of some set A into elements of another set B. If the function is denoted f, which we often introduce using the abbreviated notation $f : A \to B$, then the b associated to an a is denoted $f(a)$. Given another map $g : B \to C$, we may consider the *composition map* $g \circ f : A \to C$, which maps a point $a \in A$ to $g(f(a))$ – that is, if a is mapped to b by f, and g maps

b to c then $g \circ f$ maps a to c. A pleasant algebraic fact about the composition is that it satisfies the *associative property*. Given a third map $h : C \to D$, we find that $h \circ (g \circ f) = (h \circ g) \circ f$, a relation taken for granted when we forget parenthesis and write $h \circ g \circ f$. The first idea leading to abstract algebra is that we can identify a *functional definition* of the identity map with an *algebraic definition* involving a series of algebraic relations with respect to composition. A key idea of group theory is that we can study the functional properties of symmetries by looking at the compositional properties of maps without losing essential information.

Example. *On each set B we have an* identity map $id_B : B \to B$, *such that $id(b) = b$ for each $b \in B$. For any $g : A \to B$ and $h : B \to C$, we find $id_B \circ g = g$, and $h \circ id_B = h$. If $f : B \to B$ is any map satisfying $f \circ g = g$ and $h \circ f$ for any g and h, then f is equal to the identity map, since $f = f \circ id_B = id_B$. Thus an 'identity map' is just an idempotent element with respect to composition.*

Example. *If a function $f : A \to B$ is bijective, then there is $f^{-1} : B \to A$, defined by mapping an element b to the unique element a with $f(a) = b$. We find that $f^{-1} \circ f = id_A$, and $f \circ f^{-1} = id_B$. If g is any function such that $g \circ f = id_A$ and $f \circ g = id_B$, then*

$$g = g \circ id_B = g \circ f \circ f^{-1} = id_A \circ f^{-1} = f^{-1}$$

Thus the inverse of a map is precisely one which composes with the map to give the identity map.

Again, we see that functions can be identified by algebraic relations with respect to the composition operator. Abstract algebra is the mathematical field whose goal is to study mathematical objects via an understanding of the algebraic relations of operations on that set, with the hope that less obvious properties of the object will be unvealed via the underlying algebraic properties. In the case of the theory of functions, the operator studied is composition. In the theory of classical algebra, the operators studied are addition, multiplication, subtraction, and division. The key realization of abstract algebra is that it is often more simple to discuss arbitrary, 'abstract operators' satisfying certain properties, for then we need not deal with the minutiae which occurs which studying the set theoretic aspects of functions. In these notes, we talk about a specific class of objects which generalizes the algebraic properties of a set of invertible functions from a set to itself. These objects are known as *groups*.

Let us consider what properties the class of functions under composition should satisfy. Let X be a set, and let $\circ : X \times X \to X$ be an abstract 'composition function' on X. This means exactly that, given two objects $x, y \in X$, we may consider their composition $x \circ y \in X$. Now assume that $\circ$ satisfies the associative law $x \circ (y \circ z) = (x \circ y) \circ z$ for any three $x, y, z \in X$; This fact is no longer always true because our composition operation isn't necessarily a normal function composition operation. Elements of X need not even be functions. An 'identity' in X can then be defined to be an element $e \in X$ such that $e \circ x = x \circ e = x$ for all $x \in X$. We may then define an 'inverse' of an element $x \in X$ to be an element $y \in Y$ such that $x \circ y = y \circ x = e$. The element y is rarely denoted by anything other than x^{-1}, to parallel the set theoretic notation. Thus if $\circ$ is associative and the underlying set has an identity, then the resulting pair $(X, \circ)$ imitates a subset of functions from a set to itself, which is closed under composition. We call the pair $(X, \circ)$ a *monoid*. If every element of X is invertible, then $(X, \circ)$ imitates a set of invertible functions from a set to itself, closed under inversion, and we call this pair a *group*. Since symmetries can often be described as families of invertible functions, group theory describes the tools to understand these families. If the operation is obvious, we often abuse notation and just say that X is a group. To be even more brief, the symbol for the operation is often ignored as well, so we write xy for the composition $x \circ y$ of two elements.

Example. *Consider a topological space X. Then the set of all continuous functions from X to itself forms a monoid, and the set of all homeomorphisms from X to itself forms a group. This follows directly because if f and g are continuous, then $g \circ f$ is continuous, and the identity function is certainly continuous. If the space has a fixed metric, then the space of all isometries of the space forms a group as well.*

Example. *The set of all linear maps from a vector space V to itself forms a monoid. The set* $\mathrm{GL}(V)$ *of all invertible linear maps froms a group, known as the* general linear group. *If V has finite-dimension n, then we may essentially identify linear endomorphisms on V with the set of all $n \times n$ matrices $M_n(k)$ with entries in the scalar field k upon which V is defined, which can be viewed*

as a set with the abstract composition operation

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix}$$
$$= \begin{pmatrix} a_{11}b_{11} + \cdots + a_{1n}b_{n1} & \dots & a_{11}b_{1n} + \cdots + a_{1n}b_{nn} \\ \vdots & \ddots & \vdots \\ a_{n1}b_{11} + \cdots + a_{nn}b_{n1} & \dots & a_{n1}b_{1n} + \cdots + a_{nn}b_{nn} \end{pmatrix}$$

Then the matrix I with ones on the diagonal operates as an identity, and $\mathrm{GL}(V)$ *can be identified with the subfamily of matrices*

$$\mathrm{GL}_n(k) = \{M \in M_n(k) : MN = NM = I \text{ for some } N \in M_n(k)\}.$$

This family is also called the general linear group.

Example. *Certain vector fields $X : U \to \mathbf{R}^n$ on open subsets of Euclidean space induce 'one parameter groups' $\phi : U \times \mathbf{R} \to U$ (where the image of (x,t) is denoted $\phi_t(x)$, which we can view as a 'parameterized' family of maps), which satisfy the differential equation*

$$\frac{d\phi_t(x)}{dt} = X_{\phi_t(x)}$$

and also satisfy $\phi_t \circ \phi_s = \phi_{t+s}$, and $\phi_0 = id_U$, so this set of functions really is a group. The study of differential equations is really just the study of the relationship between smooth vector fields and the one-parameter groups of diffeomorphisms they generate, especially in certain particular situations.

Example. *Combinatorics and algebra intertwine when we study finite groups. The classical finite group is the class of all bijective maps from a set containing n elements to itself. This is the* symmetric group *of order n, denoted S_n. The group contains $n!$ elements, because an arbitrary permutation $\pi : [n] \to [n]$ can be obtained by first choosing $\pi(1) \in [n]$ (for which we have n choices), then choosing $\pi(2) \in [n] - \pi(1)$, and so on and so forth. More generally, if X is a set, we can consider the group of bijections on X, denoted $Sym(X)$. Using cycle notation, we denote the permutation π satisfying $\pi(a_1) = a_2$, $\pi(a_2) = a_3, \dots, \pi(a_m) = a_1$, and fixing all other elements by $(a_1\ a_2\ \dots\ a_m)$. We shall find that all permutations on a finite set have a unique cycle decomposition, when we discuss the symmetric group in more detail later.*

Example. *The integers* $\mathbf{Z}$ *form a group under addition, with the inverse of an integer* n *being* $-n$*. We can also consider the additive group* $\mathbf{Z}_n$ *of integers modulo* n*, which form a group modulo* n*. But most interestingly, we can combine the study of addition and multiplication by studying the multiplicative group* $\mathbf{Z}_n^*$ *of integers modulo* n *which are* relatively prime *to* n*. Thus group theory has many applications to number theory.*

Example. *We can often form groups by abstractly defining relations between objects in a set. For instance, consider the set consisting of 8 symbols*

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}.$$

We can then try and find a composition operation $Q \times Q \to Q$ *which makes* Q *into a group. It is natural to expect that* $(-1)i = -i$*,* $(-1)(-i) = 1$*, and so on and so forth. Less trivially, we also want* $i^2 = j^2 = k^2 = ijk = -1$*. We obtain the multiplication table, with the element in the row labelled* x *and column labelled* y *giving the value of* xy*.*

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

One can check that the induced operation is associative. The group Q *is known as the* quaternion *group. It is a particular subset of the quaternions, which are expressions of the form* $a + bi + cj + dk$ *with* $a, b, c, d \in \mathbf{R}$*, which provide an algebraic model for the set of all rotations in three dimensional space. Thus, even though abstractly defined,* Q *can still be interpreted in a meaningful way as a symmetry on a group.*

Chapter 2

Basic Properties of Groups

Now we shall start the general theory of groups, starting with the theory of 'manipulating equations', of which every student of compulsory education should be very familiar. Consider a finite sequence of elements $x_1, \ldots, x_n$ in a monoid X. Then the 'pi' notation for multiplication is introduced, defined recursively by setting

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

It is a convention that if $k > i$, then $\prod_{j=k}^{i} x_j = e$. The similarity to Σ notation used in arithmetical sums is intentional, and the two definitions correspond in the monoid $(\mathbf{Z}, +)$. Ultimately, the property of associativity means brackets in an equation are irrelevant. For instance, for any a, b, c, d, e, we have

$$((ab)c)(de) = a((b(cd))(e)).$$

Thus the expression $abcde$ is unambiguous. We prove this rigorously, and then dodge the use of brackets in the rest of these notes, except in emphasizing components of equations.

Theorem 2.1. *Let there be given an associative operation on S, and a finite sequence $(x_1, \ldots, x_n)$ of elements in S. Then, for any integer $1 \leqslant l < n$,*

$$\left(\prod_{k=1}^{l} x_k \right) \left(\prod_{k=l+1}^{n} x_k \right) = \prod_{k=1}^{n} x_k$$

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 obvious by definition. We now proceed inductively. If we are now given n elements $(x_1,\ldots,x_n)$, and an integer $1 \leqslant l < n$, then

$$\left(\prod_{k=1}^{l} x_k\right)\left(\prod_{k=l+1}^{n} x_k\right) = \left(\prod_{k=1}^{l} x_k\right)\left(\left(\prod_{k=l+1}^{n-1} x_k\right)\ x_n\right)$$
$$= \left(\prod_{k=1}^{l} x_k \prod_{k=l+1}^{n-1} x_k\right)\ x_m = \left(\prod_{k=1}^{n-1} x_k\right)\ x_m = \prod_{k=1}^{n} x_k$$

By induction, this statement holds for all values of n. □

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 2.2. *For any finite sequence of elements $(x_1,\ldots,x_n)$ from a set upon which an associative and commutative assignment is defined, and for any permutation $\pi \in S_n$,*

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

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, which changes nothing. 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.

$$\prod_{k=1}^{n} x_k = \left(\prod_{k=1}^{m-1} x_k\right)\left(x_m \prod_{k=m+1}^{n} x_k\right) = \left(\left(\prod_{k=1}^{m-1} x_k\right)\left(\prod_{k=m+1}^{n} x_k\right)\right)\ x_m$$

The permutation which swaps the remaining $n-1$ elements really does only swap $n-1$ elements, hence by induction the equality is obtained, and we find that it is possible to reorder finite sequences of elements arbitrarily. □

So now we have seen proofs of facts intuitively obvious from a elementary school education. Of course, our main source of inspiration behind the concept of a group is a collection of invertible functions. A *group of functions* G on a set X is a collection of bijections of X which is closed under composition and inversion. Before we start our real work, we should establish that groups are not that much more general than sets of functions. Arthur Cayley is credited with noticing that the synthetic definition really is the same as the intutive one, so that our algebraic relations uniquely model the theory of bijective functions.

Theorem 2.3. *Any synthetic group is equivalent to a group of functions.*

Proof. Let G be a synthetic group. For each $g \in G$, consider the function $g_* : G \to G$, defined by $g_*(h) = gh$. Then g_* is a bijective function, for it has an inverse $(g^{-1})_*$. The transformation $g \mapsto g_*$ 'preserves' the operation of the group, for $(gh)_* = g_* \circ h_*$ so $G_* = \{g_* : g \in G\}$ really is a group of functions, which is essentially the same group as G, for the algebraic equations that occur in the one group are equivalent to the algebraic equations in the other group. We will later make these notions precise by saying G and G_* are *isomorphic* by this map. □

Thus we are back where we started. We have the abstract group theory at our tool belt, but when all is said and done, we really are just discussion groups of transformations. The formalism gives us abstract insight into these groups, but we aren't abstracting for an arbitrary reason, since every group can be considered as a concrete set of functions. The following properties are trivial for groups of functions, and thus also hold for general groups by Cayley's theorem.

- Any group has a unique identity element.
- The inverse of any group element is uniquely determined.
- If $gh = e$ or $hg = e$, then $h = g^{-1}$.

Thus we have an algebraic system which describes precisely the semantics of families of invertible functions.

2.1 Subgroups and Cosets

Often in math the 'symmetries' to choose from are not completely obvious, and as we range our symmetries to preserve an increasingly strict set of properties, the number of symmetries we have reduces to a smaller and smaller family. Thus from our group of symmetries we obtain a *subgroup*, a subset of a group whose elements also form a group. Even if we really do care about the entire group, the subgroups of the group enable us to understand what parts of the group are 'self contained', which enables us to understand the entire group by the components it contains.

Example. *Define the special linear group $SL_n(k)$ to be the subset of matrices in the general linear group $GL_n(k)$ with determinant one. The determinant operation det : $GL_n(k) \to k^*$ satisfies*

$$\det(MN) = \det(M)\det(N) \qquad \det(M^{-1}) = \det(M)^{-1}$$

which enables us to easily show $SL_n(k)$ is closed under composition and inversion. We will later see that this is a special case of forming a subgroup from the kernel of a homomorphism.

Example. *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.*

Example. *If G is a group, then G is trivially a subgroup of itself. Similarily, the subset $\langle e \rangle = \{e\}$ is also a subgroup. These subgroups are known as the* trivial subgroups *of G.*

Example. *Consider the group $\mathbf{Z}$ of integers under addition, and let G be a subgroup. If $G \neq \langle 0 \rangle$, then G must containg a smallest positive integer n. The Euclidean algorithm then verifies that any element of G must be a positive multiple of n, so that $G = \langle n \rangle$. To see this, we note that if m is a positive integer in G, we can write $m = kn + r$, with $0 \leqslant r < n - 1$. Since $r = m - kn \in G$ and is smaller than n, we conclude that r cannot be positive, so $r = 0$, so that m is a multiple of n.*

For a fixed group G, the family of subgroups of G form an interesting lattice structure. The next proposition shows that we can find a greatest lower bound to any set of subgroups of a group.

Proposition 2.4. *If $\{H_\alpha\}$ are subgroups of G, then $\bigcap H_\alpha$ is a subgroup of G.*

Proof. Suppose $a, b \in \bigcap H_\alpha$. Then $a, b \in H_\alpha$ for each index α, which means that ab and a^{-1} are in H_α since H_α is a subgroup. But this means that ab and a^{-1} are in $\bigcap H_\alpha$ since α was arbitrary. □

Conversely, let G be a group, and S a subset of elements, we can consider the set $\mathcal{M}$ of all subgroups of G which contain S. Of course, $\mathcal{M}$ is non-empty, as G is a subgroup which contains S. If we take $\bigcap \mathcal{M}$, then we obtain a group containing S, which is contained in every group which contains S. This 'smallest' group is called the group *generated by* S, denoted $\langle S \rangle$. Equivalently, the generated subgroup is the set of all elements of the form $x_1 x_2 \dots x_n$ 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, which are formed by arbitrary sums of the generators.

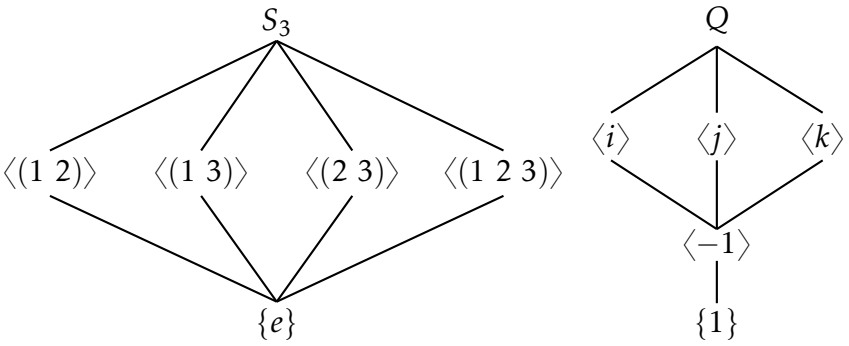
Example. *Gaussian elimination shows that every invertible matrix is the product of elementary matrices, so $GL_n(k)$ is generated by the elementary matrices.*

Example. *The integers form a group under addition, which is generated by* 1*, because every positive integer $n > 0$ can be written as*

$$n = 1 + 1 + \cdots + 1$$

and is thus in the group generated by 1*, and thus $-n$ is also in the group generated by* 1 *as well, hence all integers. A group generated by a single element is known as a* cyclic group.

The greatest lower bound of a set of subgroups of a group is the group generated by the union of the elements of a group. We have a maximal subgroup, which is the entire group, and a minimal subgroup, which is the trivial group $\{e\}$. Thus the family of subgroups forms a *bounded lattice* under the subgroup operation. We can ofte gain insight into the structure of finite groups by drawing a subgroup lattice; these lattices are essential in applications of group theory to Galois theory. Here are the lattices for S_3, and the group of quaternions.



We can gain a deeper understanding of the relations between elements of a group, because a subgroup neatly contains all possible algebraic structure between the elements trapped in the subgroup. A natural question is how much we can obtain about the relations obtained by composing elements outside of a subgroup with elements inside the subgroup. We cannot hope to understand this question by studying the subgroup as an isolated object, so we must see the subgroup as part of the overall group. One tool for understanding this containment is by studying cosets, which break apart the group by its relations with elements of a subgroup.

Let $H < G$. Define an equivalence relation $\sim$ on G by $x \sim y$ if $x \in yH$. The collection of equivalence classes formed by the relation are denoted G/H, pronounced as 'G mod H'. Each element of G/H is known as a *left coset*, and every coset can be expressed as $gH = \{gh : h \in H\}$, for some $g \in G$. 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.

Remark. Right cosets can be defined equivalently 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 $H\backslash G$. It doesn't really matter whether we talk about left or right cosets, because we have a natural map from one family to the other, mapping the coset gH to the coset Hg^{-1}. We choose to use left cosets as a simple convention.

The *index* of a subgroup H of a group G is the quantity

$$(G : H) = \#(G/H) = \#(H\backslash G).$$

Example. *For any non-zero integer N, the subgroup $N \cdot \mathbf{Z}$ of $\mathbf{Z}$ is a subgroup, and $[\mathbf{Z} : N \cdot \mathbf{Z}] = N$. The cosets of $\mathbf{Z}/N\,\mathbf{Z}$ are precisely*

$$\{0 + N\,\mathbf{Z}, \ldots, (N-1) + N\,\mathbf{Z}\}.$$

Example. *The additive group* $\mathbf{Q}$ *has the interesting property that it contains* no nontrivial finite index subgroups. *Indeed, suppose that* G *is a finite index subgroup, and set* $[\mathbf{Q} : G] = N$. *Then, for any rational number* $x \in \mathbf{Q}$, $Nx \in H$. *But clearly this implies that* $G = \mathbf{Q}$, *so* $N = 1$. *The third isomorphism theorem (proved later) therefore shows that* $\mathbf{Q}/\mathbf{Z}$ *has no finite index subgroups.*

We note that each $A \in G/H$ has the same cardinality as H; indeed, if $A = gH$, then the map $h \mapsto gh$ gives a bijection between H and A. Thus we conclude that if G is a finite group, then

$$\#(G) = \sum_{A \in G/H} \#(A) = \sum_{A \in G/H} \#(H) = (G : H) \cdot \#(H).$$

We remark that this theorem can be interpreted for infinite groups if we interpret $(G : H)$, $\#(H)$, and $\#(G)$ as a formula about cardinalities of groups. The fact that all cosets of a group have the same cardinality gives a very fruitful theorem, 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.

Theorem 2.5 (Lagrange's Theorem)**.** *If* G *is a finite group and* $H < G$, *then*

$$\#(H) \mid \#(G).$$

Lagrange did not give a complete proof, showing it only for subgroups of the symmetric group. The first complete theorem was published by Gauss in 1801.

Corollary 2.6. *Any group of prime order is cyclic.*

Proof. Let G be a group of prime order. Take a non-zero element $g \in G$, 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 2.7. *If* $L < H < G$, *then* $(G : L) = (G : H)(H : L)$.

Proof. We have three equations, $\#(G) = (G : H)\#(H) = (G : L)\#(L)$, and $\#(H) = (H : L)\#(L)$. Putting these three equations together, we conclude that

$$(G : H)(H : L)\#(L) = (G : L)\#(L).$$

Thus, dividing out be $\#(L)$, we conclude that $(G : H)(H : L) = (G : L)$. □

Remark. If we are a little more careful, we can prove this formula for infinite groups if we interpret the product as the product of infinite cardinalities.

We now have the power to prove another interesting number theoretic statement, known as Euler's theorem. Consider the totient function φ, which takes an integer n and gives us the number of integers relatively prime to n, which are less than n. The theorem is simple with the power of the methods we now possess.

Corollary 2.8. *For any relatively prime n, m, $n^{\varphi(m)} \equiv 1 \pmod{m}$.*

Proof. For any integer m, let $\mathbf{Z}_m^*$ denote the set of integers $n \in \mathbf{Z}_m$ for which there exists an integer $a \in \mathbf{Z}_m$ such that $an \equiv 1 \pmod{m}$. It will suffice for us to prove the cardinality of $\mathbf{Z}_m^*$ is equal to $\varphi(m)$, since we can then apply Lagrange's theorem. We note that for any integers n and m, the greatest common divisor of n and m is the smallest positive integer which can be written in the form $an + bm$, for $a, b \in \mathbf{Z}$. If n and m are relatively prime, then we can find a and b such that $an + bm = 1$, which implies $an \equiv 1 \pmod{m}$. Conversely, if $an \equiv 1 \pmod{m}$, then we can find an integer $b \in \mathbf{Z}$ such that $an + bm = 1$. But this means that the greatest common divisor of n and m is equal to 1, hence n and m are relatively prime. For any $n \in \mathbf{Z}_m^*$, $\langle n \rangle$ is a subgroup containing $\operatorname{ord}(n)$ elements. By Lagrange's theorem, $\operatorname{ord}(n)$ divides $\varphi(m)$. But this means that $n^{\varphi(m)} = 1$. □

One corollary is Fermat's Little Theorem.

Corollary 2.9. *If p is a prime, and $p \nmid n$, then $n^{p-1} \equiv 1 \mod p$.*

Lagrange's theorem is often very powerful, especially when analyzing finite subgroups. Here are some common applications of Lagrange's theorem, where we let G be a group with subgroups H_1 and H_2:

- If H_1 and H_2 are subgroups of G and have relatively prime orders, then $H_1 \cap H_2 = \{e\}$.
- If $[G : H_1]$ and $[G : H_2]$ are relatively prime, then

$$[G : H_1 \cap H_2] = [G : H_1][G : H_2].$$

To see this, we note $[G : H_1]$ and $[G : H_2]$ divide $[G : H_1 \cap H_2]$, and

$$\begin{aligned}[G : H_1 \cap H_2] &= [G : H_1][H_1 : H_1 \cap H_2] \\ &= [G : H_1][H_1 H_2 : H_2] \leqslant [G : H_1][G : H_2].\end{aligned}$$

- If $H_2 \triangleleft G$ and $\#(H_1)$ and $[G : H_2]$ are relatively prime, then $H_1 < H_2$. To see this, consider the homomorphism $\varphi : H_1 \to G/H_2$ given by setting $\varphi(x) = xH_2$. If K is the kernel, then $[H_1 : K]$ divides both $\#(H_1)$ and $\#(G/H_2) = [G : H_2]$, so $[H_1 : K] = 1$, implying $K = H_1$, so φ is trivial, so $H_1 \subset H_2$.

- We say a subgroup H of a finite group G is a *Hall subgroup* if $\#(H)$ and $[G : H]$ are relatively prime. If H is a Hall subgroup of G, and we consider a normal subgroup $N \triangleleft G$, then $N \cap H$ is a Hall subgroup of N. To see why, we note that $\#(H)$ and $[G : H]$ are relatively prime. Now HN is a subgroup of G, and we can write $[G : H] = [G : HN][HN : H]$, and $\#(H) = [H : H \cap N]\#(H \cap N)$. By the second isomorphism theorem,

  $$[N : H \cap N] = [HN : H] \mid [G : H].$$

  Since $\#(H \cap N)$ divides $\#(H)$, we conclude $[N : H \cap N]$ and $\#(H \cap N)$ are relatively prime, completing the proof.

  If $\#(G) = p^k m$, where p does not divide m, then we say a subgroup $H < G$ is a p *Sylow subgroup* if $\#(H) = p^k$. A subgroup of G with a prime power order is Sylow precisely when it is a Hall subgroup. Thus our proof above shows that if $N \triangleleft G$ and H is a Sylow subgroup of G, then $H \cap N$ is a Sylow subgroup of N.

Thus the cardinality of a group gives more structural information about the group than might be realized.

One might ask whether there is a converse to Lagrange's theorem. For an integer n dividing the cardinality of a group G, is there a subgroup of order G? The easiest kind of theorem of this type is Cauchy's theorem, of which we give an elementary proof here.

Theorem 2.10. *If p is a prime dividing $\#(G)$, then there is $x \in G$ of order p.*

Proof. Let

$$S = \{(x_1, \ldots, x_p) \in G^p : x_1 \ldots x_p = e\}.$$

Then $\#(S) = \#(G)^{p-1}$. Define an equivalence relation on S by declaring $(x_1, \ldots, x_p) \sim (x_i, \ldots, x_p, x_1, \ldots, x_{i-1})$ for any $i \in \{1, \ldots, p\}$, i.e. elements are

equivalent if one can obtain one sequence from the other by a cycle permutation. If $x_1 \dots x_p = e$, then

$$x_p x_1 \dots x_{p-1} = x_p (x_1 \dots x_{p-1} x_p) x_p^{-1} = x_p (e) x_p^{-1} = e.$$

Since p is prime, all cycle permutations of $(x_1, \dots, x_p)$ are distinct, except in the trivial case where $x_1 = \cdots = x_p$. Thus if we let k denote the number of size one equivalence classes, and n denote the number of size p equivalence classes, then we conclude

$$\#(G)^{p-1} = \#(S) = k + pn.$$

Since p divides $\#(G)$, k is divisible by p. But $k \geqslant 1$, since $(e, \dots, e) \in S$. Thus we conclude $k \geqslant p$, and so, in particular, there exists $x \in G$ with $x^p = e$. $\square$

Later on, we will prove a stronger statement, called Sylow's theorem, which shows that for each prime p dividing the order of a finite group G, the group G has a p Sylow subgroup.

2.2 Normal Subgroups

Let G be a group, and H a subgroup. We emphasized previously that we can think of G as a family of symmetries on some space. A natural operation associated with a symmetry is a 'coordinate transformation'. If $e_1, \dots, e_n$ are the standard basis in k^n, then for each matrix $M \in GL_n(k)$, we can associate a new basis $f_1, \dots, f_n$ with $f_i = Me_i$ for each $i \in \{1, \dots, n\}$. If $T : \mathbf{R}^k \to \mathbf{R}^k$ is a linear transformation, we can associate it with two matrices N_0 and N, where for each $x \in \mathbf{R}^n$,

$$T(x_1 e_1 + \cdots + x_n e_n) = (N_0 x)_1 e_1 + \cdots + (N_0 x)_n e_n,$$

and for each $y \in \mathbf{R}^n$,

$$T(y_1 f_1 + \cdots + y_n f_n) = (Ny)_1 f_1 + \cdots + (Ny)_n f_n.$$

Thus N_0 represents the transformation T in the standard coordinates of $\mathbf{R}^n$ relative to the basis $\{e_1, \dots, e_n\}$, and N represents the transformation T in the new coordinate system induced by the basis $\{f_1, \dots, f_n\}$. It is not difficult to see that $N = MN_0M^{-1}$, so the coordinate change is given by a conjugation operation.

Given this view of conjugation, we can see that some subgroups of a group are 'compatible' with coordinate changes in the larger group, and some groups are not. For instance, the orthogonal group $O_n(\mathbf{R})$ is *not* compatible with general coordinate changes in $GL_n(\mathbf{R})$; if we change a basis, a rotation need not be a basis anymore. More rigorously, there exists a matrix $M \in GL_n(\mathbf{R})$ and $N \in O_n(\mathbf{R})$ such that $MNM^{-1} \notin O_n(\mathbf{R})$. On the other hand, for any matrix $N \in SL_n(\mathbf{R})$ and $M \in GL_n(\mathbf{R})$, $MNM^{-1} \in SL_n(\mathbf{R})$, since

$$\det(MNM^{-1}) = \det(M)\det(N)\det(M)^{-1} = \det(M)\det(M)^{-1} = 1.$$

Thus an element of $SL_n(\mathbf{R})$ 'looks the same' under any coordinate change in $GL_n(\mathbf{R})$. The subgroups with this invariance property will be known as *normal groups*.

Theorem 2.11. *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* $g \in G$.
2. $gHg^{-1} = H$ *for all* $g \in G$.
3. $gH = Hg$ *for all* $g \in G$.
4. $G/H = H\backslash G$.

Proof. Clearly (2) and (3) are equivalent, (2) implies (1) trivially, and (3) implies (4) trivially. To show (1) implies (2), we suppose $ghg^{-1} \subseteq H$ for all $g \in G$. Then $gH \subseteq Hg$. But also $g^{-1}Hg \subseteq H$, so that $Hg \subseteq gH$, which implies $Hg = gH$. From (4), we note that if $g_1, g_2 \in G$ and $g_1H = Hg_2$, then $g_1e \in g_1H = Hg_2$, so that $g_1 \in Hg_2$. Because cosets are equal or disjoint, this means that $Hg_2 = Hg_1$, and so $g_1H = Hg_1$. □

If G is an abelian group, then every subgroup H is normal, because

$$gHg^{-1} = Hgg^{-1} = H.$$

Normality is only an interesting phenomenon in non-abelian groups.

Example. *We have already shown that $SL_n(k) \triangleleft GL_n(k)$.*

Example. *Given a group G and a set $S \subset G$, consider the* normalizer subgroup

$$N_G(S) = \{g \in G : gSg^{-1} = S\}.$$

If S is a subgroup of G, then $S \triangleleft N_G(S)$, and moreover, $N_G(S)$ is the largest subgroup of G in which S is a normal subgroup. We can also define the centralizer subgroup

$$C_G(S) = \{x \in G : xs = sx \text{ for all } s \in S\}.$$

Then $C_G(S) \triangleleft N_G(S)$. If $S = G$, then we call $C_G(S)$ the **center** *of G, also denoted as $Z(G)$.*

Theorem 2.12. *If $K < N_G(H)$, then KH is a group, and $H \triangleleft KH$.*

Proof. We begin by noticing that $KH = HK$. Thus

$$(KH)(KH) = (KH)(HK) = K((HH)K) = K(HK) = K(KH) = KH.$$

Thus KH is closed under composition. Similarily,

$$(KH)^{-1} = H^{-1}K^{-1} = HK = KH,$$

so KH is closed under inversion. Thus KH is a group. To see that H is normal in KH, we note that for $k \in K$ and $h \in H$,

$$khHh^{-1}k^{-1} = kHk^{-1} = H.$$

Thus $H \triangleleft KH$. □

Trivial subgroups of a group are always normal. Thus any group has normal subgroups. We say a group is *simple* if it contains no non-trivial normal subgroups. Thus simple groups are the equivalent of prime numbers, they cannot be 'broken up' into simpler groups. If G is not a simple group, it contains a nontrivial normal subgroup H, and then the groups G/H and H can be viewed as a partition of the structure of G. These structures do not describe the structure of G completely, but at least describe a large majority of the structure.

Example. *Let $G = 2\mathbf{Z}_4$ and $H = \mathbf{Z}_2 \times \{0\}$ be subgroups of $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_2$ respectively. Then $G \cong H$, and $\mathbf{Z}_4/G \cong (\mathbf{Z}_2 \times \mathbf{Z}_2)/H$. Nonetheless, $\mathbf{Z}_4$ is not isomorhpic to $\mathbf{Z}_2 \times \mathbf{Z}_2$.*

If we can characterize all simple groups, then intuitively we have made huge strides in characterizing the structure of all groups. The Hölder program of mathematics attempts to classify all finite simple groups. In 2008, over one hundred years after the program began, mathematicians succeeded in characterizing all groups. Each finite simple group can belong to one of 18 infinite families of groups, or is one of 26 'sporadic' groups, which do not seem to have a simple characterization. The proof of this result has taken over ten thousand journal articles, and modern work in this field has attempted to simplify parts of this proof so it is comprehensible to a single human.

2.3 Homomorphisms and Quotients

Another way to understand groups is to understand how they are interrelated to one another. In group theory, the interrelations between different groups are formalized as 'homomorphisms'. If G and H are groups, a *homomorphism* between G and H is a function $f : G \to H$ such that $f(g_1g_2) = f(g_1)f(g_2)$ for $g_1, g_2 \in G$. The homomorphism is an *embedding* if it is injective, and a homomorphism from a group to itself is known as an *endomorphism*. Intuitively, a homomorphism is map which preserves the group structure of G. For instance, if $\varphi : G \to H$ is a homomorphism, then one easily verifies that $\varphi(e) = e$, $\varphi(a^{-1}) = \varphi(a)^{-1}$, so the identity and inversion is preserved. Intuitively, a homomorphisms is a map which implants some of the information of G into a subgroup of H, in such a way that certain elements may be identified. The *kernel* of a homomorphism φ, denoted $\ker(\varphi)$, is the set of elements in the domain of the homomorphism which map to the identity. In some senses, it represents the information that is lost by the map φ.

Lemma 2.13. *If $\varphi : G \to H$, and K is the kernel of φ, then $K \lhd G$.*

Proof. Let G and H be groups, and φ a homomorphism between G and H. If $k \in K$, then $\varphi(k) = e$, and so for any $g \in G$,

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e.$$

Thus $gkg^{-1} \in K$. □

One verifies easily that a homomorphism is injective if and only if the kernel of the homomorphism is trivial. The image of a homomorphism is a subgroup of the range, but is not necessarily normal.

Example. *If M and N are matrices, the fact that* $\det(MN) = \det(M)\det(N)$ *implies that the map* $\det : GL_n(k) \to k^\times$ *is a homomorphism from the group of invertible matrices to the multiplicative group of non-zero elements in k.*

Example. *If $g \in G$, the map $n \mapsto g^n$ is a homomorphism from the additive group $mathbf Z$ to G. Similarily, we can consider the exponential map $e : \mathbf{C} \to \mathbf{C}^*$ from given by $e(x) = e^x$, which is a homomorphism from the additive group of complex numbers to the multiplicative group of nonzero complex numbers.*

Example. *The absolute value map $abs : \mathbf{C}^* \to \mathbf{R}^*$ given by setting $abs(z) = |z|$, is a homomorphism, since $|zw| = |z||w|$.*

An *isomorphism* is a bijective homomorphism. If there exists an isomorphism between two groups, G and H, we denote this by writing $G \cong H$. It is easy to see, like in linear algebra, that the inverse of a group isomorphism $f : G \to H$ is a group isomorphism $f^{-1} : H \to G$. The existence of an isomorphism means that all algebraic information about the domain is preserved in the image, and conversely, all the information in the range is contained in the domain. An *automorphism* is a bijective homomorphism from a group to itself. Thus an automorphism says that various objects in a group behave the same way. Note that the set of all automorphisms on a group G is a set of invertible functions on a space preserving some structure, and thus forms a group, denoted $\mathrm{Aut}(G)$.

Example. *The conjugation map $z \mapsto \overline{z}$ is an automorphism of both the multiplicative and additive group of complex numbers. Thus the number i, introduced to the real numbers to form the complex numbers, operates algebraically exactly the same as the number $-i$. Engineers sometimes work with $-i$, denoted j, to perform calculations; the only difference being that they work 'clockwise', instead of 'anticlockwise'.*

Example. *For each $g_0, g_1 \in G$, we let $g_0^{g_1} = g_1^{-1} g_0 g_1$. The map $\varphi_{g_1} : G \to G$ given by setting $\varphi_{g_1}(g_0) = g_0^{g_1}$ is an automorhpism of G, known as an* inner automorphism. *Moreover, the map $\varphi : G \to Aut(G)$ obtained by setting $\varphi(g) = \varphi_g$ is a homomorphism, since for $g_0, g_1, g_2 \in G$,*

$$g_0^{g_1 g_2} = (g_1 g_2)^{-1} g_0 (g_1 g_2) = g_2^{-1}(g_1^{-1} g_0 g_1) g_2 = (g_0^{g_1})^{g_2}.$$

The kernel of φ is equal to $Z(G)$.

The next theorem is essentially 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.

Theorem 2.14. *Let G be a group generated by a subset S. Given any other group H and any function $f_0 : S \to H$, there is at most one homomorphism $f : G \to H$ such that $f(s) = f_0(s)$ for each $s \in S$.*

Proof. Given two homomorphisms $f_1, f_2 : G \to H$, the set of elements of $g \in G$ with $f_0(g) = f_1(g)$ is a subgroup of G containing S, which is therefore equal to G. □

We can use the coset construction on a pair $H \triangleleft G$ to assign algebraically meaning information to G/H. Given two cosets g_1H and g_2H, we find

$$(g_1H)(g_2H) = g_1(Hg_2)H = g_1(g_2H)H = (g_1g_2)H.$$

Thus the operation on G/H given by multiplication of cosets is a well defined composition operation. It is easy to see that the coset H acts as an identity for this operation, and the inverse of a coset gH is the coset $g^{-1}H$. It follows that G/H has a natural group structure, known as the *quotient group* of G by H.

Example. *Consider the additive group of integers $\mathbf{Z}$. The set $n\mathbf{Z}$ of integer multiples of n is a subgroup of $\mathbf{Z}$, trivially normal because $\mathbf{Z}$ is abelian. Thus we can consider the quotient group $\mathbf{Z}/(n\mathbf{Z})$, which is precisely the additive group of integers modulo n.*

For $H \triangleleft G$, the map $\pi : G \to G/H$ given by setting $\pi(g) = gH$ is a canonical surjective homomorphism between the two sets, with kernel H. In particular, we note this construction shows that any normal group is a kernel of some homomorphism. Thus we can view a normal group as a subgroup which 'can be a kernel' for a homomorphism. The next theorem shows again that the kernel is the information 'lost' by a homomorphism.

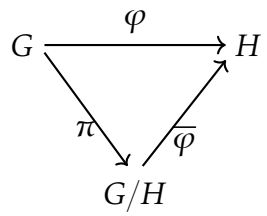
Theorem 2.15 (The First Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a surjective homomorphism with kernel K. Then $G/K \cong H$.*

Proof. Let K be the kernel of φ. If $A \in G/H$, and $g_0, g_1 \in A$, then $g_0 g_1^{-1} \in K$ so $\varphi(g_0) = \varphi(g_1)$. Thus we can define a map $\varphi_0 : G/K \to H$ such that for each coset $gH \in G/H$, $\varphi_0(gH) = \varphi(g)$. The map φ_0 is a homomorphism with respect to the quotient group operations on G/H, because

$$\varphi_0((g_1H)(g_2H)) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi_0(g_1H)\varphi_0(g_2H).$$

If $\varphi_0(gH) = e$, then $\varphi_0(g) = e$, so $g \in K$. Thus the kernel of φ_0 is trivial. Thus φ_0 is bijective, so φ_0 is an isomorphism. □

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, 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 $0 \to G \to H$ is exact precisely when the homomorphism between G and H is injective. Likewise, $G \to H \to 0$ is exact precisely when the map between G and H is surjective.

The first isomorphism is the catalyst for many other important isomorphism theorems, which enables us to construct canonical isomorphisms between objects.

Theorem 2.16 (The Second Isomorphism Theorem)**.** *Let G be a group, and consider subgroups $K, H < G$ such that $K \subset N_G(H)$. Then $(H \cap K) \triangleleft H$, and*

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

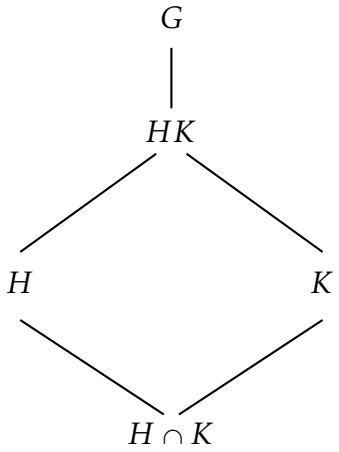


Figure 2.1: *The Diamond Isomorphism Theorem*

Proof. We have already seen that $K \triangleleft HK$, so that the quotient group HK/K makes sense. If we define $\varphi : H \to HK/K$ by setting $\varphi(h) = hK$, then φ is a homomorphism, because for $h_1, h_2 \in H$,

$$\varphi(h_1h_2) = (h_1h_2)K = (h_1K)(h_2K) = \varphi(h_1)\varphi(h_2).$$

The map φ is also surjective, because any coset of HK/K is of the form hK for some $h \in H$. The kernel of φ is equal to $H \cap K$, from which it follows that $H \cap K \triangleleft H$, and the first isomorphism theorem implies 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. Let us consider an example application.

Theorem 2.17 (The Third Isomorphism Theorem)**.** *Consider normal subgroups $H, N \triangleleft G$, with $N \triangleleft H$. Then $H/N \triangleleft G/N$, and*

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

Proof. Define $\varphi : G/N \to G/H$ by setting $\varphi(gN) = gH$. Then φ is surjective, with kernel H/N. Thus H/N is a normal subgroup of G/N, and the first isomorphism implies that

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

□

All we showed in this theorem is that $0 \to H/N \to G/N \to G/H \to 0$ is an exact sequence of groups; the theorem then follows directly from the first isomorphism theorem.

Theorem 2.18 (The Lattice/Fourth Isomorphism Theorem)**.** *Consider a normal subgroup $N \triangleleft G$. For each subgroup $H < G$, let $f_*(H) = HN/N$. Then $f_*(H)$ is a subgroup of G/H. Any subgroup of G/N can be written uniquely as H/N for some subgroup H of G with $N \subset H$, and we define $f^*(H/N) = H$. The functions f_* and f^* are order preserving, $f^*(f_*(H)) = HN$ for any group H, and $f_*(f^*(H/N)) = H/N$ for any subgroup of G/N. Thus we obtain an order preserving bijection between the family of subgroups of G containing N, and the family of subgroups of G/N. The correspondence (f_*, f^*) satisfies the following properties:*

1. *If $N < K < H < G$, $(H : K) = (f_*(H) : f_*(K))$.*
2. *If $N < K, H < G$, then $f_*(K \cap H) = f_*(K) \cap f_*(H)$.*
3. *If $N < K, H < G$, and $H \vee K$ denotes the smallest subgroup of G containing H and K, then $f_*(H \vee K) = f_*(H) \vee f_*(K)$.*
4. *If $N < K < H < G$, then $K \triangleleft H$ if and only if $f_*(K) \triangleleft f_*(H)$.*

Proof. Clearly f_* is surjective, and that $f_* \circ f^*$ is the identity map. Since the image of f^* contains all subgroups of G containing N, this verifies the bijection. To obtain (1), we note that if $N < K < H < G$, a method like that used in the third isomorphism theorem shows that

$$(f_*(H) : f_*(K)) = (H/N : K/N) = (H : K).$$

To prove (2), we calculate that

$$f_*(K \cap H) = (K \cap H)/N \subset K/N \cap H/N = f_*(K) \cap f_*(H)$$

But if $f_*(K \cap H)$ was a proper subset of $K/N \cap H/N$, then there would be a group L containing $K \cap H$ as a proper subgroup such that $L/N = K/N \cap H/N$. But if there is $k \in K$ and $h \in H$ such that $kN = hN$, then $h^{-1}k \in N \subset H$, so that $k \in H$, and similarily, $h^{-1}k \in N \subset K$, so $h \in K$. Thus $k, h \in H \cap K$, so that any element of $K/N \cap H/N$ is an element of $(K \cap H)/N$.

To prove (3), we note that $f_*(H \vee K) = (H \vee K)/N$ contains $f_*(H) \vee f_*(K) = H/N \vee K/N$ as a subgroup, so $(H \vee K)/N$ contains H/N and K/N. But if L is any subgroup of G containing N such that L/N contains H/N and K/N, then L contains H and K, so L contains $H \vee K$, which means that $H \vee K$ is a subgroup of L. Thus we conclude that $f_*(H) \vee f_*(K) = H/N \vee K/N$ contains $f_*(H \vee K) = (H \vee K)/N$.

Finally, to prove (4), we note that if $N < K < H < G$, and if K is normal in H, then the third isomorphism theorem shows that K/N is a normal subgroup of H/N. Conversely, if K/N is a normal subgroup of H/N, then for any $h \in H$,

$$(hN)(K/N)(h^{-1}N) = K/N.$$

But $h^{-1}N = Nh^{-1}$, so this theorem says that

$$h(N(K/N)N)h^{-1} = K/N.$$

In particular, for any $k_1 \in K$, there exists $k_2 \in K$ $h(kN)h^{-1} = k_2N \subset K$. But this clearly means that $hkh^{-1} \in K$, so that K is normal in H. □

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.

Theorem 2.19. *Suppose $\varphi : G \to H$ is surjective, and N_0 is a normal subgroup of H. If we define $N = \varphi^{-1}(N_0)$, then $N \lhd G$, and $G/N \cong H/N_0$.*

Proof. The homomorphism $G \to H \to H/N_0$ is surjective and has kernel N, so we can apply the first isomorphism theorem. □

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

Chapter 3

Examples

3.1 Cyclic Groups

Recall that a group is cyclic if it is generated by a single element. A simple application of the first isomorphism theorem enables us to essentially determine the complete structure of these groups.

Theorem 3.1. *Every cyclic group is isomorphic to* $\mathbf{Z}$ *or* $\mathbf{Z}_n$ *for some integer* n.

Proof. Let G be a cyclic group, generated by g. Define a surjective homomorphism $\varphi : \mathbf{Z} \to G$ by setting $\varphi(n) = g^n$. If G has finite order n, the kernel of φ is precisely integer multiples of n, and so the first isomorphism theorem says that $\mathbf{Z}_n$ is isomorphic to G. If G has infinite order, then φ itself is an isomorphism, so $\mathbf{Z}$ is isomorphic to G. □

The power of this theorem is that we need only look at $\mathbf{Z}$ and $\mathbf{Z}_n$ to prove general results about cyclic groups.

Theorem 3.2. *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. If n is a generator for $\mathbf{Z}$, then there is an integer m such that $mn = 1$. But this is clearly only possible if $n = \pm 1$. □

Theorem 3.3. *Let* G *be a finite cyclic group of order* n*, generated by an element* g*. Then* g^m *is a generator for* G *if and only* $(n, m) = 1$.

Theorem 3.4. *If G is a cyclic group with two generators x and y, then there exists a unique automorphism mapping x onto y.*

Theorem 3.5. *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.*

Lemma 3.6. *Let g be an element of a group G, and suppose that the cardinality of $\langle g \rangle$ is a non-negative integer n. Then $g, g^2, \ldots, g^n$ 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 3.7. *For $0 < k < c$, $g^k \neq e$.*

Corollary 3.8. *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 3.9. *$g^c = e$.*

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 3.10. *$g^k = e$ 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 3.11. *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 3.12. *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 3.13. *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.

Theorem 3.14. *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 a field, and thus roots of a polynomial decompose the polynomial into linear factors. Let n be the maximal order of the cyclic subgroups $\langle m \rangle$, for $m \in (\mathbf{Z}/p\mathbf{Z})^\times$, generated by an integer g. Consider the polynomial $X^n - 1$. For any $m \in (\mathbf{Z}/p\mathbf{Z})^\times$, the order of m

divides n, since the order of gm is the lowest common multiple of m and n, and must be less than n, and is hence equal. Thus $X^n - 1$ has $p - 1$ different solutions, but this implies $n \geqslant p - 1$. Of course, $n \leqslant p - 1$, so equality is obtained, and thus the group is cyclic. □

A generator of this group is known as a **primitive root**, and has many applications in number theory and cryptography. 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. Finding the primitive root for a really large prime is very difficult, which makes then very useful for cryptography.

3.2 Permutation Groups

Recall that S_n is the group of all permutations of the finite set $\{1,\dots,n\}$. In this section we study it's properties in more detail. To begin with, it's simple to see that S_n has at most $n!$ elements. More generally, given any set X, we can consider the set $S(X)$ of bijections from X to itself. For any set X and any bijection $\pi \in S(X)$, we let $\mathrm{supp}(\pi)$, the *support* of π, be the family of all $x \in X$ such that $\pi(x) \neq x$. If two permutations have disjoint support, then they commute with one another.

An *n cycle* $\pi \in S(X)$ is a permutation with finite support containing n elements $x_1,\dots,x_n \in X$ such that $\pi(x_i) = x_{i+1}$, where addition is interpret modulo n. We write such a permutation as $(x_1 \cdots x_n)$. A cycle of length two is called a *transposition*. It is intuitive that any element of S_n can be written as a product of cycles with disjoint support, unique up to reordering of the cycles.

A simple corollary of this is that S_n is generated by transpositions. Indeed, we can write

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

so any cycle is generated by transpositions, and any element of S_n can be written as a product of cycles. This equation is not necessarily unique; there might be two different ways of writing an element of S_n as a product of cycles. For instance,

$$(1\ 2)(3\ 4)(2\ 3) = (1\ 2\ 4\ 3) = (1\ 2)(2\ 4)(4\ 3)$$

However, what is surprisingly true is that the *parity* of the number of transpositions in this decomposition is independant of the decomposition.

Theorem 3.15. *There exists a unique homomorphism $\varepsilon : S_n \to \{\pm 1\}$ such that $\varepsilon(\tau) = -1$ for any transposition τ. Thus $\varepsilon(\pi) = 1$ if π is decomposable into an even number of transpositions, and $\varepsilon(\pi) = -1$ if π is decomposable into an odd number of transpositions.*

Proof. Consider the homomorphism $\phi : S_n \to GL_n(\mathbf{R})$, where we associate $\pi \in S_n$ with the *permutation matrix* $\phi(\pi) \in GL_n(\mathbf{R})$, which has the property that for each $x \in \mathbf{R}^n$,

$$\phi(\pi)(x)_i = x_{\pi(i)}.$$

We define $\varepsilon(\pi) = \det(\phi(\pi))$. Since the determinant of a matrix negates when we swap two rows, it follows that $\varepsilon(\tau) = -1$ for any transposition, since $\phi(\tau)$ is obtained from the identity by swapping two rows for any transposition τ. From this, it also follows that $\varepsilon(\pi) \in \{\pm 1\}$ for each permutation π. □

We say a permutation π is *even* if $\varepsilon(\pi) = 1$, and odd if $\varepsilon(\pi) = -1$. The theorem above shows that the set A_n of even permutations is an index two normal subgroup of S_n, since it is the kernel of the map ε, thus having $n!/2$ elements. A_n is called the *alternating group* of order n.

Before we move on to more sophisticated questions, it will be useful to find tractable families of generators for S_n and A_n.

Lemma 3.16. *S_n is generated by $\{(i\ i+1) : i \in \{1, \dots, n-1\}\}$.*

Proof. All transpositions are of the form $(i\ i+k)$ where $i+k \leqslant n$. We prove all transpositions are generated by the transpositions above by induction. Indeed, the case $k = 1$ holds by assumption. If the case k holds, then

$$^{(i+k\ i+k+1)}(i\ i+k) = (i\ i+k+1),$$

which gives the case $k+1$, completing the proof. □

Lemma 3.17. *S_n is generated by $(1\ 2)$ and $(1 \cdots n)$.*

Proof. For each $i \in \{1, \dots, n-1\}$,

$$^{(1\cdots n)^{i-1}}(1\ 2) = (i\ i+1).$$

But these elements generate S_n. □

Lemma 3.18. *If n is a prime number, then S_n is generated by an n-cycle and any transposition.*

Proof. Let π be an n-cycle and τ be a transposition. Write $\tau = (a_1 a_2)$. But then there exists some $i \in \{0, \dots, n-1\}$ such that $\pi^i(a_1) = a_2$. Since n is prime, π^i is still an n-cycle of the form $(a_1 a_2 \dots a_n)$. But then the previous case verifies that π^i and τ generate S_n. □

Lemma 3.19. *A_n is generated by three cycles.*

Proof. It clearly suffices to show that the product of two transpositions can be written as the product of three cycles. If $a, b, c, d \in \{1, \dots, n\}$ are distinct, then

$$(ab)(cd) = (abc)(bcd)$$

is the product of three cycles. This works for all products of transpositions but those of the form $(ab)(ac)$, for distinct $a, b, c \in \{1, \dots, n\}$. But

$$(ab)(ac) = (acb)$$

is also the product of three cycles. □

In the next proof, we note that for any set X and any two permutations $\pi, \sigma \in S(X)$, and any $x \in X$, recalling ${}^{\pi}\sigma = \pi \circ \sigma \circ \pi^{-1}$, then

$${}^{\pi}\sigma(\pi(x)) = \pi(\sigma(x)).$$

In particular, if $\sigma = (a_1 \cdots a_n)$, then ${}^{\pi}\sigma = (\pi(a_1) \cdots \pi(a_n))$.

Corollary 3.20. *If $n \geqslant 5$, then all 3 cycles are conjugate in A_n.*

Proof. Consider two three cycles $\pi_1 = (a_1 a_2 a_3)$ and $\pi_2 = (b_1 b_2 b_3)$. Then consider any permutation $\eta \in S_n$ with $\eta(a_i) = b_i$ for $i \in \{1, 2, 3\}$. If $\eta \in A_n$, we are done since ${}^{\eta}\pi_1 = \pi_2$. If η is odd, then there exists $a_4, a_5 \in \{1, \dots, n\} - \{a_1, a_2, a_3\}$, and if $\eta' = (a_4 a_5)\pi$, then η' is even and ${}^{\eta'}\pi_1 = \pi_2$. □

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

Lemma 3.21. *A_n is simple if $n \geqslant 5$*

Proof. Let G be a nontrivial normal subgroup of A_n. It suffices to show $G = A_n$, and to do this, it suffices to show a single three cycle. Let $\pi \in G$ be an element of G which has the largest number of fixed points, excluding the identity. Then clearly all cycles of π must have the same length, because if π contains an n and an m cycle, for $n < m$, then $\pi^n \neq e$ and fixes more points than π, which gives a contradiction. Suppose π consists of only 2-cycles. Then π contains at least two 2-cycles, which we may write as $(a_1 a_2)$ and $(a_3 a_4)$. If $a_5 \in \{1,\dots,n\} - \{a_1,\dots,a_4\}$, and we set $\eta = (a_3 a_4 a_5)$, then $\pi^\eta \pi \in G$ is an element of G which fixes all elements that π does, except perhaps for a_5, but fixes a_1 and a_2, which gives a contradiction since $\pi^\eta \pi(a_4) = a_5$, so $\pi^\eta \pi \neq e$. Thus π consists of only n-cycles, for some $n \geqslant 3$. If π is not a 3-cycle, then we may find distinct $a_1, a_2, a_3, a_4, a_5 \in \{1,\dots,n\}$ such that $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, and $\pi(a_4) = a_5$. Let $\eta = (a_3 a_4 a_5)$. Then $\pi^\eta \pi \in G$ fixes all points that π does, but in addition, $\pi(a_1) = a_1$. Since $(\pi^\eta \pi)(a_2) = a_5$, $\pi^\eta \pi \neq e$, which gives a contradiction showing that G contains some 3-cycle. □

The fact that A_n is simple for $n \geqslant 5$ has strong ramifications in Galois theory, where it implies there is no formula for finding the roots of quintic polynomials roots. In particular, it implies that S_n is not solvable.

Theorem 3.22. *For $n \geqslant 5$, S_n is not solvable.*

Proof. The group A_n is a normal subgroup of S_n, and $S_n/A_n \cong \mathbf{Z}_2$ is abelian. Thus S_n is solvable if and only if A_n is solvable. Since A_n is simple and non-abelian, it is not solvable. □

Let us end this section by describing the lattice structure of the subgroups of A_4, which has the useful property of being planar. A_4 has three subgroups of order 2, corresponding to the three elements of A_4 of order two, i.e. $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, and $(1\ 4)(2\ 3)$. There are four subgroups of A_4 of order 3, namely the groups generated by $(1\ 2\ 3)$, $(1\ 2\ 4)$, $(1\ 3\ 4)$ and $(2\ 3\ 4)$. Any group of order four must only contain elements of order two, and one can verify that the set G consisting of the identity and all order two elements is indeed such a group. It is precisely the set of elements of G that are either the identity, or fix no points. To prove these are all subgroups, it suffices to show that any subgroup H of A_4 containing a three cycle and a product of 2-cycles is all of A_4. We can then clearly find distinct indices a_1, a_2, and a_3 such that $\pi = (a_1\ a_2\ a_3)$ and $\tau = (a_1\ a_2)(a_3\ a_4)$

are elements of H. But then ${}^{\tau}\pi = (a_1\ a_4\ a_2) \in H$, $\pi\tau = (a_1\ a_3\ a_4) \in H$, and ${}^{\pi\tau}\pi = (a_1 a_4 a_3) \in H$, which generate all three cycles, and hence all of A_n.

TODO: Draw lattice for A_n.

Exercise 3.1. *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, uniformly randomly, 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, but if a single prisoner fails, everyone 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 greater than 30% chance of success.*

Proof. The state of the boxes can be written as a bijection $\pi : \{1,\dots,n\} \to \{1,\dots,n\}$, such that box i contains the number $\pi(i)$. We then consider the following strategy: the prisoner labelled i_1 picks the box labelled i_1. He then recieves a new number $i_2 = \pi(i_1)$. If $i_2 \neq i_1$, he then opens the box i_2, recieving a number $i_3 = \pi(i_2)$. He continues this way, only failing if he generates $n/2$ numbers $i_1,\dots,i_{n/2}$. In particular, we see that the prisoners only fail if the bijection π contains a cycle with length greater than $n/2$. Clearly there can be at most one such cycle in any particular bijection. For each length $l > n/2$, there are exactly

$$\binom{n}{l}(l-1)!(n-l)! = \frac{n!}{l}$$

different permutation with a cycle of length l. Thus the total number of permutations with a cycle of length exceeding $n/2$ is

$$\sum_{l=n/2+1}^{n} \frac{n!}{l} = n! \cdot [\log(n) - \log(n/2) + O(1/n)] = n![\log(2) + O(1/n)]$$

Since there are $n!$ possible bijections of S_n, we conclude that that probability of the prisoners failing is $1 - \log(2) + O(1/n) \approx 0.31 + O(1/n)$. □

3.3 Matrix Groups

3.4 Isometry Groups

3.5 Direct Products

This section presents methods for constructing new groups from smaller ones. Conversely, one can break groups into simpler groups by reversing this technique. Let us begin with the simplest construction, the direct product.

Let $\{G_\alpha : \alpha \in I\}$ be an indexed family of groups. The direct product of these groups, denoted by $\prod_{\alpha\in I} G_\alpha$, whose underlying set is the cartesian product of the groups, and with group operation

$$\left(\prod_{\alpha\in I} g_\alpha^1\right)\left(\prod_{\alpha\in I} g_\alpha^2\right) = \prod_{\alpha\in I}(g_\alpha^1 g_\alpha^2).$$

The direct product of a finite family of groups $\{G_1,\dots,G_N\}$ is often denoted by $G_1 \times \cdots \times G_N$. If a group G is isomorphic to a direct product of subgroups $\{G_\alpha\}$, then to understand G it suffices to understand the individual groups G_α. The following theorem gives criteria to ensure this occurs.

Theorem 3.23. *Suppose G contains two normal subgroups H and K. Then HK is a subgroup of G, and*

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

In particular, if $H \cap K = \{e\}$, then HK is isomorphic to $H \cap K$. such that $H \cap K = \{e\}$.

Proof. Assume first that $H \cap K = \{e\}$. Then the assumptions guarantee that $hk = kh$ for all $h \in H$ and $k \in K$. Thus the map $\varphi : H \times K \to HK$ given by setting $\varphi(h,k) = hk$ is an isomorphism, completing the proof. For the general case, we note that $H/(H \cap K)$ and $K/(H \cap K)$ are normal subgroups of $HK/(H \cap K)$ with trivial intersection, so we can apply the previous case. □

Example. *If n is odd, then D_{2n} is isomorphic to the direct product $D_n \times \{\pm 1\}$. To see this, we let $r \in D_{2n}$ be a primitive rotation. Then $r^n \in Z(D_{2n})$, and so $H = \langle r^n \rangle$ is a normal subgroup of D_{2n} isomorphic to $\{\pm 1\}$. To obtain a copy of D_n in D_{2n}, we note that we can inscribe two regular n-vertex polygons in a regular $2n$-vertex polygon. The set of elements of D_{2n} which preserve these two polygons is then a subgroup of G of D_{2n} isomorphic to D_n, which we can see to be normal since it has index two in D_{2n}. Since n is odd, $r^n \notin G$, so $G \cap H = \{e\}$. But $\#(G) = 2n$, and $\#(H) = 2$, so $\#(G \times H) = 4n = \#(D_{2n})$. Thus we conclude that $D_{2n} = GH \cong G \times H \cong D_n \times \{\pm 1\}$.*

For each group G_α is the direct product $G = \prod_{\alpha \in I} G_\alpha$, we have a surjective homomorphism $\pi_\alpha : G \to G_\alpha$. The kernel of this mapping is just the set of elements $g \in \prod_{\alpha \in I}$ with $g(\alpha) = e$. Thus we can quotient this kernel out to obtain a group isomorphic to G_α. Given any family of homomorphisms $f_\alpha : H \to G_\alpha$ from a group H, there is a unique map $f : H \to \prod G_\alpha$ such that $\pi_\alpha \circ f = f_\alpha$ for each α. This is a *universal property* establishing the direct product, in the sense of category theory; up to isomorphism, $G_0 = \prod G_\alpha$ is the unique group for which there exists projections $\pi_\alpha : G_0 \to G_\alpha$ such that for each function $f_\alpha : H \to G_\alpha$, there exists a unique map $f : H \to G_0$ such that $f_\alpha = \pi_\alpha \circ f$ for each α. This is because if some other group H exists with this property with projections $\nu_\alpha : H \to \alpha$, then there exists a unique map $t : H \to \prod_\alpha G_\alpha$ such that $\pi_\alpha \circ t = \nu_\alpha$, as well as a map $s : \prod_\alpha G_\alpha \to H$ such that $\nu_\alpha \circ s = \pi_\alpha$. It does not take much work to show that s is the inverse of t, because

$$\pi_\alpha \circ (t \circ s) = \nu_\alpha \circ s = \pi_\alpha;$$

But the identity map $1 : \prod_\alpha G_\alpha \to \prod_\alpha G_\alpha$ is the unique map such that $\pi_\alpha \circ i = \pi_\alpha$ for each α; a similar argument works to show $s \circ t$ is the identity.

3.6 Free Products

The free product is another construction associated with a family of groups, and can also be described by a universal property 'dual' to the previous property considered. Given a family of groups $\{G_\alpha\}$, we desire to construct a group $\coprod_\alpha G_\alpha$, together with homomorphisms $i_\alpha : G_\alpha \to \coprod_\alpha G_\alpha$, such that for each family of homomorphisms $f_\alpha : G_\alpha \to H$, there exists a unique homomorphism $f : \coprod_\alpha G_\alpha \to H$ such that $f_\alpha = f \circ i_\alpha$ for each index

α. This describes the *free product* of the groups $\{G_\alpha\}$, up to isomorphism. Thus it suffices to show such a group exists. To achieve this, we start by constructing the *free groups*.

Let S be a set of symbols. We construct a group $F(S)$, known as the *free group* generated by S. Let $\mathcal{S}$ denote the alphabet of S, consisting of all finite (possibly empty) words $w_1 \dots w_n$, where for each i, either $w_i = s$ or $w_i = s^{-1}$, for some $s \in S$. We consider the equivalence relationship generated by letting $w_1 s s^{-1} w_2 \sim w_1 w_2$ for each $s \in S$. We let $F(S)$ denote the set of equivalence classes of $\mathcal{S}$ under this relation. Clearly if $w_1 \sim w_2$ and $u_1 \sim u_2$, then $w_1 u_1 \sim w_2 u_2$, so composition is well defined on $F(S)$. This composition operation on $F(S)$ is associative, and has an identity (the empty string). Moreover, every element has an inverse; for instance, the inverse of $s_1 \dots s_n$ is $s_n^{-1} \dots s_1^{-1}$.

We note that if G is a group, and $f : S \to G$ is a map, then there exists a unique homomorphism $f_* : F(S) \to G$ such that $f_*(s) = f(s)$ for each $s \in S$. We can use this as a universal property which uniquely specifies the free group of G up to isomorphism. In the language of category theory, we might say that the free group construction is the *left adjoint* to the forgetful functor from the category of groups to the category of sets.

A combinatorially complicated way of constructing groups is by means of *generators and relations*. We consider a set S, and let R be some family of elements of $F(S)$. If we let N be the smallest normal subgroup of $F(S)$ generated by R, then we call the group $G = F(S)/N$ the *group generated by S with relations R*. If $S = \{x_1, \dots, x_n\}$ and $R = \{s_1, \dots, s_m\}$, we sometimes use the notation

$$G = \langle x_1, \dots, x_n | s_1 = \dots = s_m = e \rangle.$$

If G is any group generated by some set $S \subset G$, then the inclusion map $i : S \to G$ induces a surjective homomorphism $f : F(S) \to G$. Thus any group is generated by a set subject to certain relations.

Example. *Recall the Dihedral group D_n of isometries of an n sided regular polygon is generated by two elements r and s, where r is a primitive rotation, and s is any reflection. For these elements, $r^n = s^2 = (rs)^2 = e$. We claim that*

$$D_n \cong \langle r, s | r^n = s^2 = (rs)^2 = e \rangle.$$

If G denotes the generated group, then we certainly have a surjective homomorphism $f : G \to D_n$. If we can show that G has at most $2n$ elements, then f is

an isomorphism, which would complete the proof. But the relations in G imply that $rs = sr^{n-1}$*, so any element of G is of the form* $s^i r^j$ *for some* $i \in \{0,1\}$ *and* $j \in \{0,\dots,n-1\}$*, from which it clearly follows that* $\#(G) \leqslant 2n$*.*

Now suppose $\{G_\alpha\}$ is a family of groups; we assume the sets defining the groups G_α are disjoint from one another. Then we let F be the free group generated by $\bigcup G_\alpha$, with inclusion maps $i_\alpha : G_\alpha \to F$. If $f_\alpha : G_\alpha \to H$ is a family of maps, the universal property of the free group implies there is a unique homomorphism $f : F \to H$ such that $f \circ i_\alpha = f_\alpha$. However, this does not imply F is the coproduct, because the inclusion maps i_α are not homomorphisms. But we can fix this. Let K be the smallest normal subgroup of F containing all elements of the form $i_\alpha(g_1)i_\alpha(g_2)i_\alpha(g_1g_2)^{-1}$ for each α and $g_1, g_2 \in G_\alpha$. Then the induced maps $j_\alpha : G_\alpha \to F/K$ are homomorphisms. Moreover, if $f_\alpha : G_\alpha \to H$ are *homomorphisms*, then the induced homomorphism $f : F \to H$ factors through K, because the kernel of f contains $i_\alpha(g_1)i_\alpha(g_2)i_\alpha(g_1g_2)^{-1}$ for each α and each $g_1, g_2 \in G_\alpha$. Thus there is a unique homomorphism $g : F/K \to H$ such that $g \circ j_\alpha = f_\alpha$ for each α. The group F/K is therefore the coproduct we were looking for! Thus we have shown that the coproduct of an arbitrary family of groups exists.

3.7 Semidirect Products, and Fibre Products

Chapter 4

Group Actions and Symmetries

Recall Cayley's theorem, which we proved in the introductory chapter, which says that every group G is isomorphic to a subgroup of $S(A)$, for some set A. The goal of this chapter is to study what information about a group G we can understand from homomorphisms $\phi : G \to S(X)$ for some set X, or, from the dual perspective, to try and understand what properties a homomorphism ϕ can have given knowledge of the structure of the group G.

A *group action* of a group G acting on a set X is a map $F : G \times X \to X$, where we denote $F(g,x)$ by gx, such that $g_1(g_2x) = (g_1g_2)x$ for any $g_1, g_2 \in G$ and $x \in X$. If, for each $g \in G$, we let $\phi(g) \in S(X)$ denote the permutation such that $\phi(g)(x) = gx$, then we obtain a homomorphism $\phi : G \to S(X)$, which we call a *permutation representation* of the group G. Conversely, given any permutation representation $\phi : G \to S(X)$, we obtain a group action of G on X by letting $gx = \phi(g)(x)$. Thus group actions are ways of studying homomorphisms of G. A set X with an action from a set G is called a G *set*. Here is some useful terminology to describe group actions:

- A group action is *faithful* if the induced permutation representation is injective.
- Given a G set X and $x \in X$, we can consider the *stabilizer*

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

  which forms a subgroup of G.

- On any G set X, we can consider an equivalence relation on X by setting $x_1 \sim x_2$ if there is $g \in G$ such that $x_2 = gx_1$. The equivalence classes are known as *orbits* of X. Each orbit can be written as Gx, for some $x \in X$, and we write the set of all such orbits as X/G. To understand the action of G, it then clearly suffices to analyze each orbit of X individually.

- A group action is *transitive* if there exists only a single orbit.

- 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.

Example. *The permutation group S_n acts on $\{1,\ldots,n\}$ by permuting integers in the obvious manner. The action is faithful and transitive, and for any i, the stabilizer subgroup S_i is isomorphic to S_{n-1}.*

Example. *The group D_n acts faithfully and transitively on the set V_n of vertices of the regular n sided polygon. If n is even, then the stabilizer $(D_n)_p$ of any point $p \in V_n$ is trivial. If n is odd, the stabilizer $(D_n)_p$ of any point $p \in V_n$ consists of the identity and the unique reflection in D_n about the line passing through p and the centre of the polygon; thus the stabilizer is isomorphic to $\mathbf{Z}_2$.*

Example. *Any set G acts on itself by multiplication, i.e. for $g,x \in G$, gx is just group multiplication. This is the representation we used to prove Cauchy's theorem. A deeper application of the group action is given by* conjugation*, i.e. the group action given by the group representation $\phi(g)(x) = {}^g x = gxg^{-1}$. The kernel of the conjugation representation is precisely the centre $Z(G)$ of G. For each $g \in G$, the* stabilizer *of g is precisely the* centralizers *$C_G(h) = \{g \in G : gh = hg\}$. An interesting fact is that $\phi(g)$ is a* homomorphism *of G for each $g \in G$, any such homomorphism being known as an* inner homomorphism*. A homomorphism $\phi : G \to Aut(H)$ for two groups G and H is called a* group representation *of G.*

Example. *A very similar group action is obtained by letting X be the set of all subgroups of G. Then G acts on X by conjugation, i.e. letting $\phi : G \to S(X)$ by given by setting $\phi(g)(H) = {}^g H = gHg^{-1}$. The stabilizer of a subgroup H is the normalizer $N_G(H)$, and the fixed points of this action are precisely the normal subgroups of G.*

Example. *If M is a compact manifold, and X is a vector field on M, then there is a unique family of diffeomorphisms $\{\phi_t : t \in \mathbf{R}\}$ of M such that for each $x \in M$ and $s \in \mathbf{R}$,*

$$\left.\frac{\partial \phi_t(x,s)}{\partial t}\right|_{t=0} = X_s.$$

One verifies that $\phi_t \circ \phi_s = \phi_{t+s}$ for each $t, s \in \mathbf{R}$, so the map $t \mapsto \phi_t$ is a permutation representation of $\mathbf{R}$ on the set M.

Example. *Consider the group $SL_n(\mathbf{R})$ acting on the upper half of the complex plane, the set*

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

by the mobius transform

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

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.

For any group action G on a set X, it is easy to verify that $G_{gx} = {}^gG_x$. Thus stabilizers of elements belonging to a common orbit are isomorphic by an inner automorphism. In particular, if G acts faithfully on X, then for any $x_0 \in X$,

$$\bigcap_{g \in G} {}^gG_{x_0} = \bigcap_{x \in X} G_x = \{e\}.$$

Theorem 4.1. *Suppose G is an abelian group acting faithfully on a set X. Then if $g \neq e$, then $gx \neq x$ for all $x \in X$. If G acts transitively on X, then $\#(G) = \#(X)$.*

Proof. For each $x \in X$ and $g \in G$, the fact that G is Abelian implies ${}^gG_x = G_x$. But then the previous equation tells us that

$$G_x = \bigcap_{g \in G} {}^gG_x = \{e\}.$$

Thus we conclude that $gx \neq x$ for any $g \neq e$. If G acts transitively on X, and we fix $x_0 \in X$, then the map $g \mapsto gx_0$ is a bijection from G to X. □

Let G be a group acting transitively on a set X. a *block* of the action is a set $A \subset X$ such that for each $g \in G$, $g(A) = A$, or $A \cap G(A) = \varnothing$. The family of sets

$$Y = \{gA : g \in G\}$$

is then a partition of X. To understand the action of G on X, it then clearly suffices to analyze the action of G on A, and of the action of G on Y. A *primitive* group action is a transitive one for which no block exists.

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.

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

Theorem 4.2 (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 4.3 (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 4.4 (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 4.5 (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. □

Chapter 5

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 5.1. *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 5.2 (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. □

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 5.3. *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 5.4. *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 5.5. *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!

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 5.6. *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 5.7. *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 5.8. *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 5.9. *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 5.10. *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 5.11. *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 5.12. *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 5.13. *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 5.14. *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 5.15. *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 6

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.

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.

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 6.1. *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.

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

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 6.2 (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 6.3 (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

$$G_{k,0} = G_k(G'_0 \cap G_{k-1}) = G_k(G \cap G_{k-1}) = G_kG_{k-1} = G_k$$

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.

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

Corollary 6.4 (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 6.5. *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

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

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 6.6. *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

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

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

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

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 6.7. *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. □

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 $\mathrm{GL}_n(\mathbf{F})$. 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 $G \rhd \{e\}$ is an abelian tower, because $G/\{e\} \cong G$, and is hence abelian. Thus G is solvable.

Theorem 6.8. *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 6.9. *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. □

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 6.10. *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 6.11. *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 6.12. *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 6.13. *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 6.14. *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 6.15. *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 6.16. *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 7

Direct Products and Abelian Groups

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.

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.

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.

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 7.1. *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 7.2. *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 7.3. *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 $\langle ag_1 \rangle$ 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 $\langle ag_1 \rangle$, and $H = H' \cdot C$. Now C is either zero or infinite cyclic, which proves that H is free. □

Corollary 7.4. *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 7.5. *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 7.1. *What is the order of* $(\times_{i \in I} g_i)$ *in relation to the order of each* g_i *in the direct product.*