

The following notes are a summary of the material learned in Math 741 at the University of Wisconsin Madison from the fall of 2008. The course was taught by professor I. M. Isaacs and uses his text Algebra: A Graduate Course as a reference.

1 Introduction

Definition 1.1. Given a set $S \neq \emptyset$, we write $\text{Sym}(S)$ to be the set of all bijections mapping S to itself. We call $\text{Sym}(S)$ the *symmetric group* on S . Elements of $\text{Sym}(S)$ are called sometimes called *permutations*. If $S = \{1, 2, \dots, n\}$ we write $\text{Sym}(S) = S_n$.

Definition(Cayley) 1.2. Let G be a set with a binary operation multiplication. Assume:

1. $x(yz) = (xy)z$
2. $\exists e \in G$ such that $xe = ex = x$ for all $x \in G$
3. $\forall x \in G$, there exists $y \in G$ such that $xy = yx = e$

Then G is a *group* where e is the *identity* of G and y is the *inverse* of x .

Note that within any group G , the identity e is unique and inverses of particular elements are unique.

Definition 1.3. A map $\theta : G \rightarrow H$ where θ is a bijection is called an *isomorphism* if $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in G$. In this case, we say that G and H are *isomorphic* and we write that $G \cong H$.

A group isomorphism is a way of saying that, in essence, two groups behave the same as one another. An example is that we have a planet G where all people are blue. On another planet H , all people are green. If the people on both planets behave exactly the same, we wish to say that if one is colorblind, then the planets are essentially the same. The “Marty Isaacs the test” is a good test for determining which properties of a group are preserved by isomorphisms. If you have a group theoretic property which can be described with the word *the*, then this property is most likely preserved by group isomorphisms. A good example of this is *the center* of a group, described below.

Definition 1.4. Given G , the *center* of G , denoted $\mathbf{Z}(G)$, is defined as $\{z \in G \mid zg = gz \forall g \in G\}$.

Using our Marty Isaacs *the* test, we see that if $\theta : G \rightarrow H$ is an isomorphism, then we have that $\theta(\mathbf{Z}(G)) = \mathbf{Z}(H)$.

Theorem(Cayley) 1.1. Every group G is isomorphic to a permutation group.

Proof. See homework assignment 1, problem 3. □

Definition 1.5. An *automorphism* of a group G is an isomorphism from G to G .

Lets start with the proof of an easy but helpful lemma.

Lemma 1.1. The map $x \mapsto x^{-1}$ is an automorphism of G if and only if G is abelian.

Proof. If G is an abelian group, then $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$, and this taking inverses is an automorphism. To see the converse, assume that taking inverses is an automorphism. Then $(xy)^{-1} = x^{-1}y^{-1}$. Taking inverses of both sides yields that $xy = (x^{-1}y^{-1})^{-1} = yx$. Therefore $xy = yx$ and G is abelian. \square

We next define the very important concept of an inner automorphism of a group.

Definition 1.6. Fix $g \in G$ and let $\tau_g : G \rightarrow G$ be defined by $x \mapsto g^{-1}xg$. The map τ_g is called *conjugation by g* and is an automorphism of the group G .

One ought to check that conjugation indeed defines an automorphism. We leave this as an exercise (to be completed here):

We also note that this τ_g notation is not really standard, and it is much more standard to write conjugation by $g \in G$ on an element x using exponential notation, x^g . This is not to be confused with the notation of x^n , which is to be interpreted as the element x multiplied by itself n times.

Notationally, we refer to the set of all inner automorphisms of G as $\text{Inn}(G)$ and the full set of all automorphisms of G as $\text{Aut}(G)$.

Definition 1.7. If g^n is the identity, $n > 0$ and n is the smallest integer with this property, we say that n is the *order* of g and write $n = o(g)$. If no such natural number exists, we say that $o(g) = \infty$.

We prove another easy lemma as a warm up, and because the technique is useful.

Lemma 1.2. If G is a group and $|G| < \infty$, then each element $g \in G$ has finite order.

Proof. Suppose not. Then there exist integers n and m such that $g^n = g^m$ as G is finite. Without loss, assume that $n > m$. Multiplying both sides of this equation by g^{-m} , we obtain $g^{-m}g^n = g^{-m}g^m$, or $g^{n-m} = g^0 = 1$. Yet $n > m$, so $g^{n-m} = 1$, which is a contradiction. \square

Definition 1.8. A subset $H \subseteq G$ where G is a group is a *subgroup* if H is a group with respect to the same multiplication in G .

We now present a few important examples of subgroups.

Examples 1.1. A few (of many):

- For any $g \in G$, the group generated by g is a subgroup, written $\langle g \rangle$. Additionally, if $X \subseteq G$ is a subset of G $\langle X \rangle$ is a subgroup.
- If $X \subseteq G$ is a subset, we define the *centralizer of X* to be $\mathbf{C}_G(X) = \{g \in G \mid gx = xg \forall x \in X\}$.
- Maximal subgroups: $M \subset G$ is a *maximal* subgroup of G if $M < G$ and there does not exist a subgroup $H \subseteq G$ such that $M < H < G$.
- The intersections of subgroups is always a subgroup. One important example of this is the *Frattini subgroup*, which is the intersection of all maximal subgroups of a group G . We denote the Frattini subgroup by $\Phi(G)$.
- The *derived subgroup* or *commutator subgroup* of G , denoted G' , is equal to $\langle \{xyx^{-1}y^{-1} \mid x \in G, y \in G\} \rangle$.

It is often helpful to think of “the group generated by X ” as the intersection of all subgroups which contain the set X . This is a particularly helpful way of thinking when we get to ring/field theory.

The Frattini subgroup is a very important subgroup of a given group G , and it will definitely come up later on. We introduce an equivalent way of thinking about the Frattini subgroup:

Theorem 1.1. Let us (for the time being) call an element $u \in G$ *useless* if whenever $X \subseteq G$ is a subset and $\langle X \cup \{u\} \rangle = G$, then in fact $\langle X \rangle = G$. In other words, u is useless in G if adjoining it to a subset that doesn’t generate G still doesn’t generate G . Show that if G is finite, then $\Phi(G)$ is exactly the set of useless elements of G .

Proof. See assignment 2, number 3. □

2 Normal Subgroups and Cosets

In the rest of our notes, we will often get a bit sloppy with our notation, writing $H \subseteq G$ to imply that H is actually a subgroup of G , unless otherwise specified.

2.1 Normal Subgroups

Definition 2.1.1. Let H be a subgroup of G . We say that H is *characteristic* in G if $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$.

Definition 2.1.2. If $H \subseteq G$, we say that H is a *normal* subgroup of G if $\sigma(H) = H$ for all $\sigma \in \text{Inn}(G)$. We use the notation $H \triangleleft G$ to denote that H is a normal subgroup of G .

Additionally, we often extend our exponential notation when talking about conjugation from elements to subgroups. Therefore if we wish to consider the image of a subgroup H under conjugation by an element $g \in G$, we write H^g to represent this set.

NOTE: It is a common mistake to assume that if $K \triangleleft H$ and $H \triangleleft G$, we then have that $K \triangleleft G$. This is NOT true. What is true is the following lemma:

Lemma 2.1.1. Let K be characteristic in H and let $H \triangleleft G$. Then $K \triangleleft G$.

Proof. We wish to show that $K^\sigma = K$ for all $\sigma \in \text{Inn}(G)$. So fix $\sigma \in \text{Inn}(G)$ and let τ represent σ restricted to H . Note that $\tau \in \text{Aut}(H)$. As $H \triangleleft G$, we have $H^\sigma = H$. Then since $K \subseteq H$, we find that $K^\sigma \subseteq H^\sigma$, or as we are now only dealing with quantities in H , this is equivalent to stating that $K^\tau \subseteq H^\tau = H$. Yet $\tau \in \text{Aut}(H)$ and K is characteristic in H , so $K^\tau = K^\sigma = K$. Hence $K \triangleleft G$. \square

The next lemma is also very important: it states that if we wish to show that H is a normal subgroup of G , it suffices to show that for all $g \in G$, we have $H^g \subseteq H$. That is, it is enough to show containment for an arbitrary group element.

Lemma 2.1.2. Let $H \subseteq G$ and suppose that $H^g \subseteq H$ for all $g \in G$. Then $H \triangleleft G$.

Proof. Given any $g \in G$, we have that $H^g \subseteq H$. We must show that $H \subseteq H^g$. We know that $H^g \subseteq H$, so if we conjugate both sides by g^{-1} we have that $H \subseteq H^{g^{-1}}$ for all $g \in G$. Applying this result with g^{-1} in place of g , we find that $H \subseteq H^g$. Thus $H^g = H$ for all $g \in G$ and therefore $H \triangleleft G$. \square

This is one of those tricky proofs where we have that something is true for ALL $g \in G$, and therefore we may switch out any element with its inverse (or think of it as every element is the inverse of something) to obtain our result.

We now concern ourselves with many tests for normal subgroups. To do this, we make one more elementary definition.

Definition 2.1.3. If X and Y are subsets of a group G , we define their *product* $XY = \{xy | x \in X, y \in Y\}$.

We are primarily concerned with when we take our subsets X and Y to be subgroups H and K of a group G . It is important to note that HK need NOT be a subgroup of G . However, there are a few specific examples of when HK does form a subgroup. The proofs of these facts is currently omitted.

Examples 2.1.1. If H, K are subgroups of a group G , then HK is also a subgroup of G when:

- $HK = KH$. Note that this does NOT mean that H and K commute.
- One of H or K is normal in G .

2.2 Cosets

Definition 2.2.1. Let $H \subseteq G$. Then if we fix $g \in G$, $Hg = \{hg|h \in H\}$ is a *right coset* of H in G . Similarly, we may define $gH = \{gh|h \in H\}$ to be a *left coset* of H in G .

A good mnemonic for this is to recall that the left or right refers to where the fixed element is. Throughout the rest of the proofs, we will be concerning ourselves with right cosets of a subgroup H in G . I believe it is more standard to deal with left cosets, but there really is no loss in dealing with right cosets.

The next lemma gives us two very important facts about cosets. As Marty Isaacs likes to say:

Cosets are slippery beasts, and they are known by many names. So you must be very very careful when dealing with them.

Also, the following lemma will show us that we may partition a group by the distinct right cosets of a given subgroup.

Lemma 2.2.1. Let $H \subseteq G$.

1. If $h \in H$ then $Hh = H$.
2. If $x \in Hy$ then $Hx = Hy$.
3. If $Hu \cap Hv \neq \emptyset$ then $Hu = Hv$.

Proof. For 1, we know that $Hh \subseteq H$ as H is a subgroup and is therefore closed under multiplication. To see that $H \subseteq Hh$, let $k \in H$. We will show that $k \in Hh$. As $h \in H$ and H is a group, we have that $kh^{-1} \in H$. Hence $kh^{-1}h = k$ is in Hh .

For 2, we see that since $x \in Hy$ we may write $x = hy$ for some $h \in H$. So $Hx = Hhy = Hy$ by 1.

For 3, let $x \in Hu \cap Hv$ as $Hu \cap Hv \neq \emptyset$. By 2, $Hx = Hu$. Also by 2, $Hx = Hv$. Therefore transitivity yields that $Hu = Hv$. \square

Definition 2.2.2. Given $H \subseteq G$, we define the *index* of H in G as $|\{Hg|g \in G\}|$; i.e., the number of right cosets. We denote the index of H in G by $|G : H|$.

With this definition in hand, we are ready to prove LaGrange's Theorem, a very useful theorem in finite group theory.

Theorem(LaGrange) 2.2.1. If $|G| < \infty$, then $|G : H| = |G|/|H|$.

Proof. This follows as G is the disjoint union of the distinct right cosets of H in G . \square

We may now deduce many helpful Corollaries to LaGrange's Theorem.

Corollary 2.2.1. Suppose that $|G| < \infty$ and let $H \subseteq K \subseteq G$ be subgroups. Then $|G : H| = |G : K||K : H|$.

Proof. By LaGrange's Theorem, we know that $|G : H| = |G|/|H|$. Also by LaGrange, we find that $|G : K| = |G|/|K|$, and that $|K : H| = |K|/|H|$. Altogether then, we find that:

$$|G : K||K : H| = \frac{|G|}{|K|} \frac{|K|}{|H|} = \frac{|G|}{|H|} = |G : H|$$

□

As another corollary of LaGrange's Theorem, we can now show that in a finite group, the order of an element divides the order of the group.

Corollary 2.2.2. Assume $|G| < \infty$. Then for any $g \in G$, we have that $o(g)$ divides $|G|$.

Proof. Note that $|\langle g \rangle| = o(g)$, and that $\langle g \rangle$ forms a subgroup of G . So $|\langle g \rangle|$ divides $|G|$ by LaGrange. □

Finally, we prove a lemma which demonstrates the relationship between normal subgroups and left and right cosets. (Note: one can also show, using LaGrange's theorem, that there is a bijection between the left and right cosets of a subgroup H in G . This proof is omitted, but the fact may be useful, and at least lets us know that there is no loss in considering either only left or only right cosets).

Lemma 2.2.2. Let $N \subseteq G$ be a subgroup. TFAE:

1. $N \triangleleft G$.
2. $Ng = gN$ for all $g \in G$.
3. Every right coset of N in G is a left coset of N in G .
4. Every left coset of N in G is a right coset of N in G .
5. $(Nx)(Ny) = Nxy$ for all $x, y \in G$.
6. The set of right cosets of N in G is closed under multiplication.

Proof. To see that $1 \rightarrow 2$, we note that $Ng = gg^{-1}Ng = gN$ as $N \triangleleft G$. That 2 implies 3 (and likewise, that 2 implies 4) is trivial. (I hate the use of that word, but it is just by definition).

To see that $3 \rightarrow 2$, We pick a coset Ng of N in G . We know that Ng is also some left coset of N in G . Additionally, $g \in Ng$ as $1 \in N$. As we may represent the left coset by any one of its members by Lemma 2.2.1, we find that $Ng = gN$ for all $g \in G$.

That $5 \rightarrow 6$ is again trivial. To see that $2 \rightarrow 5$, we know that $Nx = xN$, so if we have $(Nx)(Ny)$, we may think of this as $N(xN)y = NNxy = Nxy$ as N is a subgroup of G and is therefore closed.

Finally, we show that $6 \rightarrow 1$. Let $g \in G$. We wish to show that $N^g = g^{-1}Ng = N$. So consider $Ng^{-1}Ng$, which can only be larger than N^g .

Note that $Ng^{-1}Ng$ is a coset by assumption, and as $g \in Ng$, one element of $g^{-1}Ng$ is $g^{-1}g = 1$. Hence $N^g \subseteq Ng^{-1}Ng \subseteq N1 = N$, and lemma 2.1.2 yields the result. \square

3 Factor Groups and Homomorphisms

Definition 3.1. If $N \triangleleft G$, we write $G/N = \{Ng | g \in G\}$, pronounced G mod N , to be a *factor group* or *quotient group*.

It is another good exercise to verify that this set of cosets actually does form a group when $N \triangleleft G$. We leave space for this straightforward verification:

Definition 3.2. Given groups G and H and a map $\theta : G \rightarrow H$, we say that θ is a *homomorphism* from G to H if $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in G$.

We here present a very important example.

Example 3.1. Let $N \triangleleft G$ and define $\pi : G \rightarrow G/N$ via $\pi(g) = Ng$. Then by lemma 2.2.2, we find that $\pi(xy) = Nxy = NxNy = \pi(x)\pi(y)$. Therefore π defines a homomorphism from G to G/N , which is called the *canonical homomorphism*.

We now list a few very important properties of homomorphisms. Another quick notational note: I will try to designate with a subscript to which group the identity belongs (i.e. 1_G or 1_H) when I think that this point may be confusing. However, it is often clear from context to which group the identity belongs, or which identity element I am referring to, so I may not always be rigorous with this notation. In what follows below, assume $\theta : G \rightarrow H$ is a homomorphism.

- $\theta(1_G) = 1_H$.
- $\theta(x^{-1}) = \theta(x)^{-1}$.
- If $X \subseteq G$ is a subgroup, then $\theta(X) \subseteq H$ is a subgroup.
- If $Y \subseteq H$ is a subgroup, let $X = \{g \in G | \theta(g) \in Y\}$. We call X the *preimage* of Y , and $X \subseteq G$ is a subgroup.

Definition 3.3. Given a homomorphism $\theta : G \rightarrow H$, the *kernel* of θ , denoted $\ker(\theta) = \{x \in G | \theta(x) = 1\}$.

We next prove a very important fact about kernels of homomorphisms.

Lemma 3.1. Let $\theta : G \rightarrow H$ be a homomorphism. Then $\ker(\theta) \triangleleft G$.

Proof. We first establish that $\ker(\theta)$ is a subgroup of G . As $\theta(1) = 1$, we see that $\ker(\theta)$ is nonempty and contains the identity. To see that $\ker(\theta)$ is closed, let $x, y \in \ker(\theta)$. Then $\theta(x) = 1$ and $\theta(y) = 1$. Thus $\theta(x)\theta(y) = \theta(xy) = 1$, so $xy \in \ker(\theta)$. Finally, we show that $\ker(\theta)$ is closed under inverses. So let $x \in \ker(\theta)$. Then $\theta(x) = 1$, and by the properties listed above, $1 = \theta(x)^{-1} = \theta(x^{-1})$, so $x^{-1} \in \ker(\theta)$. So $\ker(\theta)$ is a subgroup of G . To see that $\ker(\theta) \triangleleft G$, We wish to show that if $x \in \ker(\theta)$, then $g^{-1}xg \in \ker(\theta)$ for all $x \in G$. Now $\theta(g^{-1}xg) = \theta(g^{-1})\theta(x)\theta(g)$ since θ is a homomorphism. As $x \in \ker(\theta)$, this simplifies to $\theta(g^{-1})\theta(g) = \theta(g)^{-1}\theta(g) = 1$, which implies that $g^{-1}xg = x^g \in \ker(\theta)$. Hence $\ker(\theta)^g \subseteq \ker(\theta)$ for all $g \in G$, so lemma 2.1.2 implies that $\ker(\theta) \triangleleft G$. \square

We now begin stating and proving the many homomorphism theorems or group theory, which help lead us up to the all important correspondence theorem. This first homomorphism theorem tells us that ALL group homomorphisms are isomorphic to canonical homomorphisms. Essentially, this tells us that if one wishes to understand homomorphisms, it suffices to study canonical homomorphisms.

A word of warning for this proof: Marty Isaacs likes to do function composition from left to right, which can be very confusing. In the following proof, I follow that convention.

Theorem 3.1. Let $\theta : G \rightarrow H$ be a surjective homomorphism, and let $N = \ker(\theta)$. Then there exists a unique $\varphi : G/N \rightarrow H$ such that $\pi\varphi = \theta$, and where φ is an isomorphism.

Proof. Given $g \in G$, we must have $(g)\pi\varphi = g\theta$. That is to say, we must have $Ng\varphi = g\theta$. So if this result is to hold, we are forced to define φ on G/N by $Ng\varphi = g\theta$. (This statement essentially guarantees the uniqueness of φ). As “Cosets are slippery beasts”, we must check to see that this map is well defined. So suppose that $Nx = Ny$. We need to know that $Nx\varphi = Ny\varphi$. By the way we’ve defined φ , this holds if and only if $x\theta = y\theta$. Yet this follows since homomorphisms are well defined, so φ is a well defined map. To see that φ is an isomorphism, we note that via the properties of cosets, $(NxNy)\varphi = (Nxy)\varphi = (xy)\theta = x\theta y\theta = (Nx)\varphi(Ny)\varphi$. This establishes that φ is a homomorphism.

Finally, we must check that φ is both injective and surjective. To see that φ is injective, we check that $|\ker(\varphi)| = 1$. So suppose that $Ng \in \ker(\varphi)$. Then $(Ng)\varphi = 1$, which implies that $g\theta = 1$. So $g \in \ker(\theta)$, which implies that $g \in N$. So $Ng = N$ and $|\ker(\varphi)| = 1$, so φ is injective. To see that φ is surjective, let $h \in H$. We must show that there exists some element of G/N which maps to h . Now as $h \in H$ and $\theta : G \rightarrow H$ is surjective, there exists some $g \in G$ such that $g\theta = h$. Yet $g\theta = (Ng)\varphi$, so $(Ng)\varphi = h$, as desired. \square

We state without proof, another useful version of the homomorphism theorem. In words, it states that a group, modulo its kernel, is isomorphic to its image.

Theorem 3.2. If $\theta : G \rightarrow H$ is any homomorphism, $\theta(G) \subseteq H$ is a subgroup and θ is surjective onto $\theta(G)$. Hence $G/\ker(\theta) \cong \theta(G)$.

NOTE: When working with homomorphisms, it is easy to get carried away when modding out by groups. It doesn't make any sense to attempt to mod out by subgroups which aren't normal, so don't do it. Before considering a factor group, ALWAYS be certain that the group you wish to mod out by is normal.

The next lemma we prove is incredibly useful and we often refer to it simply as the diamond lemma. I will include a hand sketched picture of what the lemma proves, which is very useful. If I get around to it, I will alter this document to include a computerized drawing.

Lemma 3.2. Let $H \subseteq G$ and let $N \triangleleft G$. Then $H \cap N \triangleleft H$ and $NH/N \cong H/(H \cap N)$

Proof. Let $\pi : G \rightarrow G/N$ be our canonical homomorphism. Let σ represent the restriction of π to the subgroup H . Now $\sigma : H \rightarrow G/N$, but what is $\sigma(H)$? By definition, $\sigma(H) = \{Nh|h \in H\}$. Using coset notation, this may be thought of as $\{Nnh|h \in H \text{ and } n \in N\} = NH/N$. By our previous version of the homomorphism theorem, $H/\ker(\sigma) \cong NH/N$. To determine $\ker(\sigma)$, we search for elements such that $\sigma(x) = 1$ where $x \in H$. As σ is just restriction of π to the group H , we find that $\ker(\sigma) = H \cap \ker(\pi) = H \cap N$. By lemma 3.1, we see that $H \cap N \triangleleft H$ and that $NH/N \cong H/(H \cap N)$. \square

Here is a space to draw in the result of this proof:

As a corollary, we are able to conclude some results about indices in finite groups.

Corollary 3.1. Suppose that $H \subseteq G$, $N \triangleleft G$, and that $|G| < \infty$. Then $|NH : N| = |H : N \cap H|$ and $|NH : H| = |N : N \cap H|$.

Proof. We know that $|NH : N| = |NH|/|N| = |H|/|H \cap N| = |H : H \cap N|$, where the finiteness of G is essential in order for the second equality to hold. For the second part of this result, we know that $|NH : N \cap H| = |NH : N||N : N \cap H|$. However, we also know that $|NH : N \cap H| = |NH : H||H : N \cap H|$. We may set these two equations equal to one another, and by the first part of our result, find that we may cancel out $|NH : N|$ with $|H : N \cap H|$, implying that $|NH : H| = |N : N \cap H|$. \square

As these notes are simply meant to be a summary, the next two Corollaries are stated without proof. They were done in class to familiarize us with the concepts and mechanisms of the homomorphism theorems. They would make good

exercises to prove again. As a hint, notice just how similar the two Corollaries are; the second is just a generalization of the first.

Corollary 3.2. $\text{Inn}(G) \cong G/\mathbf{Z}(G)$.

Proof. Exercise. □

Corollary 3.3. Let $N \triangleleft G$. Then $\mathbf{C}_G(N) \triangleleft G$ and $G/\mathbf{C}_G(N)$ is isomorphic to some subgroup of $\text{Aut}(G)$.

Proof. Exercise. □

3.1 The Correspondence Theorem

The following is one of the most heavily used theorems from first semester group theory. Recall that unless otherwise specified, $H \subseteq G$ carries with it the notion that H is a subgroup of G . Additionally, we will again leave room for a picture to be inserted within these notes following the proof of the Correspondence Theorem.

Theorem(Correspondence) 3.1.1. Let $\theta : G \rightarrow H$ be a surjective homomorphism, and let $N = \ker(\theta)$. Let $\mathcal{X} = \{U | N \subseteq U \subseteq G\}$. Similarly, let $\mathcal{Y} = \{V | V \subseteq H\}$. The map that carries $X \mapsto \theta(X)$ is a bijection from \mathcal{X} to \mathcal{Y} . Now suppose $X \in \mathcal{X}$ and $Y = \theta(X) \in \mathcal{Y}$. Then:

1. $|G : X| = |H : Y|$
2. $X \triangleleft G$ if and only if $Y \triangleleft H$
3. If $X \triangleleft G$ and $Y \triangleleft H$ then $G/X \cong H/Y$.

Proof. We first show that the map defined by $X \mapsto \theta(X)$ is a bijection. To do this, we will show that the map θ is invertible. Define $\varphi : \mathcal{Y} \rightarrow \mathcal{X}$ by $\varphi(Y) = \theta^{-1}(Y)$. (NOTE: We are NOT assuming what we wish to prove, what is written is simply an unfortunate abuse of notation. By $\theta^{-1}(Y)$, we mean the inverse image of the subgroup Y , which is always defined.) We need to show that $\varphi(\theta(X)) = X$ for all $X \in \mathcal{X}$ and that $\theta(\varphi(Y)) = Y$ for all $Y \in \mathcal{Y}$.

We first show that $\theta(\varphi(Y)) = Y$. One direction of containment is clear: that $\theta(\varphi(Y)) \subseteq Y$. For the other direction, let $y \in Y$. As θ is surjective, there exists some $g \in G$ such that $\theta(g) = y$. SO by construction, $g \in \theta^{-1}(Y) = \varphi(Y)$, and $\theta(g) = y$, so $y \in \theta(\varphi(Y))$. Hence $\theta(\varphi(Y)) = Y$.

To see that $\varphi(\theta(X)) = X$, we again show double containment. Again, one direction is clear: namely, that $X \subseteq \varphi(\theta(X))$. To see the other direction, let $g \in \varphi(\theta(X))$, which exists as θ is surjective. By definition, this means that $\theta(g) \in \theta(X)$. This implies that $\theta(g) = \theta(x)$ for some $x \in X$. Thus $Ng = Nx$, which implies that $g \in Nx$ or that $g = nx$ for some $n \in N$. Yet $nx \in X$ as $N \subseteq X$ and $x \in X$, so $g \in X$.

Next, we show that $|G : X| = |H : Y|$. To do this, we show that $|\{Xg | g \in G\}| = |\{Yh | h \in H\}|$. To do this, we show that there is a bijection between these two sets of cosets. Given a coset Xg , consider $\theta(Xg) =$

$\theta(X)\theta(g) = Y\theta(g)$, which is a right coset of Y in H . We show that this map is a bijection. To see that it is injective, suppose that $\theta(Xg_1) = \theta(Xg_2)$. Then we have that $\theta(X)\theta(g_1) = \theta(X)\theta(g_2)$, or equivalently, that $Y\theta(g_1) = Y\theta(g_2)$. So $\theta(g_1) \in Y\theta(g_2)$, and we may write $\theta(g_1) = y\theta(g_2)$. So $y = \theta(g_1)\theta(g_2)^{-1}$, or that $\theta(g_1g_2^{-1}) \in Y$. This implies that $g_1g_2^{-1} \in X$, and multiplying both sides on the right by g_2 gives $g_1 \in Xg_2$. Hence $Xg_1 = Xg_2$, as desired. The surjectivity of this map follows from the surjectivity of θ .

We next show that $X \triangleleft G$ if and only if $H \triangleleft Y$. Suppose first that $X \triangleleft G$. So let $h \in H$, and we will show that $Y^h = Y$. Now $h \in H$ implies that $h = \theta(g)$ for some $g \in G$ as θ is surjective. So $Y^h = Y^{\theta(g)}$. As $Y = \theta(X)$, we have that $Y^h = \theta(g^{-1})\theta(X)\theta(g) = \theta(g^{-1}Xg) = \theta(X) = Y$. Now suppose that $Y \triangleleft H$. We need to show that $X^g \subseteq X$ for all $g \in G$. So let $g \in G$ be arbitrary. Now $\theta(X^g) = \theta(g^{-1}Xg) = \theta(g^{-1})\theta(X)\theta(g) = \theta(g)^{-1}Y\theta(g) = Y$. So we find that both X and X^g map to Y under θ , and by an earlier part of this proof, the injectivity of θ on the sets \mathcal{X} and \mathcal{Y} implies that $X = X^g$.

Finally, we show that if $X \triangleleft G$ and $Y \triangleleft H$ then $G/X \cong H/Y$. If π is the canonical homomorphism from $H \rightarrow H/Y$, then we have that $G \xrightarrow{\theta} H \xrightarrow{\pi} H/Y$. So $\theta\pi$ maps G to H/Y . As G mod its kernel is isomorphic to its image, we find that $\ker(\theta\pi) = X$ as $\ker(\pi) = Y$ and $\theta^{-1}(Y) = X$. Therefore the homomorphism theorem yields the result. \square

Here is a picture which demonstrates the result of this important theorem.

Although lengthy, the proof of the correspondence theorem is essentially what professor Isaacs would call a “follow your nose proof”. How do you show equality? With double containment of course. How do you show a bijection? By showing both that the map is both injective and surjective, etc. In retrospect, the part of this proof which demonstrates that θ is a bijection from \mathcal{X} to \mathcal{Y} is very reminiscent of the way things are proved using Galois connections.

We now draw a few corollaries of the correspondence theorem and introduce a few more important topics which use it.

Corollary 3.1.1. Let $N \subseteq X \triangleleft G$ where $N \triangleleft G$. Then:

$$\frac{G/N}{X/N} \cong G/X$$

Proof. Follows directly from the third part of the correspondence theorem. A picture also shows the result quite clearly: \square

Before we draw our next corollary, we introduce the very important notion of a simple group.

Definition 3.1.1. A group G is a simple group if $|G| > 1$ and its only normal subgroups are 1 and G .

Note that just as with prime numbers, where 1 is not considered to be prime, we do not allow the trivial group to be considered a simple group. We now proceed with the next corollary.

Corollary 3.1.2. Let M be a maximal normal subgroup of G . Then G/M is a simple group.

Proof. If we had $V \triangleleft G/M$ such that $1 < V < G/M$, then the correspondence theorem would imply that there exists a subgroup N such that $N \triangleleft G$ and $M < N < G$, which contradicts the fact that M is maximal normal in G . \square

Using the previous corollary, we may now introduce another important application of the correspondence theorem: composition series.

Let $G = G_0$ be a finite group, and take G_1 to be maximal normal in G . Let $S_1 = G/G_1$. If the order of G_1 is prime, stop. Otherwise, take G_2 to be maximal normal in G_1 , and let $S_2 = G_1/G_2$. Again, if $|G_2| = p$ for p a prime, stop. Otherwise, let G_3 be maximal normal in G_2 , etc. As G is a finite group, this process is guaranteed to halt, and the sequence $G_0 > G_1 > \dots > G_n > 1$ is called a *composition series* for G and the factor groups S_i are the corresponding *composition factors* of G . The ability to perform this process shows that all finite groups have a composition series. The question of which groups have composition series is an interesting question, which will be brought up again later in the semester.

4 Group Actions

Definition 4.1. Let G be a group and let Ω be a non-empty set. Assume that we have a rule which assigns to each element $\alpha \in \Omega$ and $g \in G$ a new $\alpha \cdot g \in \Omega$. Assume that $\alpha \cdot 1 = \alpha$ for all $\alpha \in \Omega$ and that $(\alpha \cdot g) \cdot h = \alpha \cdot gh$ for all $g, h \in G$. In this situation, \cdot is an *action* and we say that G *acts* on Ω via \cdot .

We now list many common examples of group actions.

Examples 4.1. Let G be a group and Ω a non-empty set.

- If $\Omega = G$, define $x \cdot g = xg$. This is called the *regular action*.
- If $\Omega = G$, we can define the *conjugation action* as $x \cdot g = x^g$.
- If Ω is equal to the set of all subsets of G , we may define $X \cdot g = X^g$.
- If Ω is equal to the set of all subsets of G , we may define $X \cdot g = Xg$.

According to Marty Isaacs, there are really only three things we ever care about when considering group actions. The three primary functions of group actions are to find subgroups, find normal subgroups, and to count things.

Definition 4.2. Let G act on Ω . Let $\alpha \in \Omega$. We write $G_\alpha = \{g \in G \mid \alpha \cdot g = \alpha\}$. G_α is called the *stabilizer* of α .

To get more familiar with dealing with group actions, we prove the following lemma.

Lemma 4.1. G_α is a subgroup of G .

Proof. First, we must know that G_α is nonempty; which it is as $\alpha \cdot 1 = \alpha$ implies that $1 \in G_\alpha$. To see that G_α is closed, note that if $g, h \in G_\alpha$, we have that $\alpha \cdot gh = (\alpha \cdot g) \cdot h = \alpha \cdot h = \alpha$, so $gh \in G_\alpha$. Finally, if $g \in G_\alpha$, we show that $g^{-1} \in G_\alpha$. But $\alpha = \alpha \cdot 1 = (\alpha \cdot g) \cdot g^{-1} = \alpha \cdot g^{-1}$, so $\alpha \cdot g^{-1} = \alpha$ and $g^{-1} \in G_\alpha$. \square

The next two examples help us to realize specifically what subgroup of G we find when we know the action.

Example 4.2. Let G act on itself via conjugation, and let $x \in G$. Then $G_x = \{g \in G \mid x^g = x\} = \mathbf{C}_G(x)$.

Example 4.3. Let G act on its set of subsets via conjugation, and let $X \subseteq G$. Then $G_X = \{g \in G \mid X^g = X\} = \mathbf{N}_G(X)$, the *normalizer* of X in G .

Another way to view the normalizer of a subgroup is as the largest subgroup in which a given subgroup is normal. A subgroup X may not be normal in the whole group, but there is some subgroup in which it is normal (at least itself), and this is the normalizer of X in G .

We prove another lemma. By itself, it isn't very useful, but the proof technique is valuable. The technique is that if we wish to show that a group is normal, we can show that its normalizer is equal to the whole group.

Lemma 4.2. Let $N \triangleleft G$, and assume that N is abelian. Let $H \subseteq G$, and assume $NH = G$. Then $(N \cap H) \triangleleft G$.

Proof. We wish to show that $\mathbf{N}_G(N \cap H) = G$. We know that $N \subseteq \mathbf{N}_G(N \cap H)$ as N is abelian. But $N \cap H \triangleleft H$ by the diamond lemma, so $H \subseteq \mathbf{N}_G(N \cap H)$. Therefore NH , the smallest subgroup containing both N and H must be contained in $\mathbf{N}_G(N \cap H)$. Yet $NH = G$, so $G \subseteq \mathbf{N}_G(N \cap H)$. Hence $G = \mathbf{N}_G(N \cap H)$ and thus $(N \cap H) \triangleleft G$. \square

We now include another important fact. Let $H \subseteq G$ and let $\Omega = \{Hx \mid x \in G\}$, that is, Ω is the set of right cosets of H in G , where G acts on Ω by right multiplication. We wish to determine G_{Hx} . Now $G_{Hx} = \{g \in G \mid Hxg = Hx\}$. So if $g \in G_{Hx}$, we then have that $xg \in Hx$, which when we multiply on the left by x^{-1} , we must have $g \in x^{-1}Hx = H^x$. So $G_{Hx} = H^x$, and in particular, $G_H = H$.

Finally, we obtain an important theorem. Recall that we read function composition from left to right.

Theorem 4.1. Let G act on Ω and define the map $f_g : \Omega \rightarrow \Omega$ by $f_g(\alpha) = \alpha \cdot g$. Then $f_g \in \text{Sym}(\Omega)$ and the map $\theta : G \rightarrow \text{Sym}(\Omega)$ defined by $g \mapsto f_g$ is a homomorphism.

Proof. To see that θ is a homomorphism, let $g, h \in G$. We will show that $\theta(gh) = \theta(g)\theta(h)$. If $\alpha \in \Omega$ is arbitrary, we have $(\alpha)f_{gh} = \alpha \cdot gh = (\alpha \cdot g) \cdot h = (f_g(\alpha))f_g \cdot h = (f_g(\alpha))f_g f_h$. As $(\alpha)f_{gh} = (\alpha)f_g f_h$, we have that $f_{gh} = f_g f_h$. As $\theta(gh) = f_{gh} = f_g f_h = \theta(g)\theta(h)$, we see that θ is a homomorphism. To see that $f_g \in \text{Sym}(\Omega)$, we need to know that f_g is a bijection for all $g \in G$. Yet $f_g f_{g^{-1}} = f_{gg^{-1}} = f_1 = i$, the identity on Ω , so $f_{g^{-1}}$ is the inverse map of f_g . This implies that f_g is a bijective on Ω , so $f_g \in \text{Sym}(\Omega)$. \square

Whenever a group homomorphism is considered, it is almost always important to determine the kernel of that homomorphism. For θ as defined in theorem 4.1, we see that $g \in \ker(\theta)$ if and only if $\alpha \cdot g = \alpha$ for all $\alpha \in \Omega$; equivalently, $g \in \ker(\theta)$ if and only if $g \in \bigcap_{\alpha \in \Omega} G_\alpha$. Note that the if $N = \ker(\theta)$, N is commonly referred to as the *kernel of the action*. If $N = 1$, we say that the action is *faithful*.

We now move on to another important example.

Example 4.4. Let $H \subseteq G$, and let $\Omega = \{Hx | x \in G\}$, the set of right cosets of H in G . Let G act on Ω by right multiplication. If $\alpha = Hx$, then $G_\alpha = H^x$. Then N , the kernel of the action, is equal to $\bigcap_{\alpha \in \Omega} G_\alpha = \bigcap_{x \in G} H^x$. In this example, N is called the $\text{core}_G H$.

To wrap our head around the core of H in G , suppose that M is any other normal subgroup of G which is contained in H . Then if $x \in G$ is arbitrary, we have that $M^x = M \subseteq H^x$, so $M \subseteq \bigcap_{x \in G} H^x = \text{core}_G(H)$. Intuitively, this demonstrates that the core of H in G is the largest normal subgroup of G which is contained in H .

NOTE: Recall that the normalizer of H in G is the largest subgroup of G which contains H . The core of H in G acts as sort of a dual; it is the largest normal subgroup of G contained inside H .

The next theorem we prove, although not terribly useful on its own, has as a corollary a very important theorem, commonly referred to as the $n!$ theorem.

Theorem 4.2. Let $H \subseteq G$, and suppose that $|G : H| = n < \infty$. Then $|G : \text{core}_G(H)|$ divides $n!$.

Proof. Let $\Omega = \{Hx | x \in G\}$. Note that $|\Omega| = n$ as this is the definition of the index of H in G . Let $\theta : G \rightarrow \text{Sym}(\Omega)$ via $g \mapsto f_g$ as defined in theorem 4.1. This theorem tells us that θ is a homomorphism, with $N = \ker(\theta) = \text{core}_G(H)$. Then by the homomorphism theorem, we have that $G/N \cong \theta(G) \subseteq \text{Sym}(\Omega)$. As $|\Omega| = n$, we see that $|\text{Sym}(\Omega)| = n!$, so $|G : \text{core}_G(H)| = |G/N| = |\theta(G)|$, which is a subgroup of a group of size $n!$. Therefore by LaGrange's theorem, we have that $|\theta(G)|$ divides $n!$, and therefore so does $|G : \text{core}_G(H)|$. \square

Corollary 4.1. If G is a simple group and $H < G$ and $|G : H| = n < \infty$, then $|G|$ divides $n!$.

Proof. Let $\Omega = \{Hx | x \in G\}$, and let $N = \text{core}_G(H)$. We know that $N \triangleleft G$ and as G is simple, we must have that $N = 1$ or $N = G$. As $H < G$ and $N \subseteq H$, we must have that $N = 1$ and the action is faithful. By the previous theorem, we know that $|G : N|$ divides $n!$, yet as $N = 1$, we have that $|G : N| = |G|$. Hence $|G|$ divides $n!$. \square

The following will be a useful corollary when we wish to prove that a finite group is not simple.

Corollary 4.2. Let $H \subseteq G$ where $|G : H| = p$ for p a prime. Assume $|G| < \infty$ and that p is the smallest prime divisor of $|G|$. Then $H \triangleleft G$.

Proof. We consider $|G : \text{core}_G(H)|$, which we may write as $|G : H| |H : \text{core}_G(H)|$, and which divides $p!$. As $|G : H| = p$, we see that $|H : \text{core}_G(H)|$ divides $(p-1)!$. Therefore all prime factors of $|H : \text{core}_G(H)|$ are strictly smaller than p . Yet this index must divide the order of G , so there cannot be any prime divisors as p is the smallest prime dividing $|G|$. Therefore $H = \text{core}_G(H)$, and as $\text{core}_G(H)$ is always normal inside G , we have that $H \triangleleft G$. \square

We now continue with a few more definitions.

Definition 4.3. A group G is said to be a p -group if $|G| = p^e$ where p is a prime and $e \geq 0$ is an integer.

It is a known fact that if G is a p -group and $H \subseteq G$ is a subgroup with index p , then $H \triangleleft G$. This will follow later as we will find that p -groups are solvable.

Definition 4.4. Suppose that G acts on Ω and let $\alpha \in \Omega$. define $\mathcal{O}_\alpha = \{\alpha \cdot g | g \in G\}$. We call \mathcal{O}_α the *orbit* of α under G .

When we introduced the notion of the stabilizer, this was all of the elements of G which kept an element $\alpha \in \Omega$ fixed. The orbit again acts sort of as a dual to the notion of a stabilizer; it is all the different “places” so to speak that a particular element may travel to within Ω . As we will later see, the orbits of an action are in many ways similar to cosets within a group.

The first similarity that we notice is that orbits may be named by any one of their elements. Recall that we had a similar result when speaking about cosets.

Lemma 4.3. Let $\beta \in \mathcal{O}_\alpha$. Then $\mathcal{O}_\beta = \mathcal{O}_\alpha$.

Proof. Let $\gamma \in \mathcal{O}_\beta$. Then there exists some $g \in G$ such that $\beta \cdot g = \gamma$. Yet $\beta \in \mathcal{O}_\alpha$, so there exists $h \in G$ such that $\beta = \alpha \cdot h$. So $\gamma = (\alpha \cdot h) \cdot g = \alpha \cdot gh$, and $\gamma \in \mathcal{O}_\alpha$. To see that $\mathcal{O}_\alpha \subseteq \mathcal{O}_\beta$, let $g \in G$ be such that $\beta = \alpha \cdot g$. If we act on both sides of this by g^{-1} , we find that $\beta \cdot g^{-1} = \alpha \cdot g \cdot g^{-1} = \alpha \cdot 1 = \alpha$. So $\mathcal{O}_\alpha \subseteq \mathcal{O}_\beta$, as desired. \square

The biggest thing about this result is the same conclusion that we drew about cosets: the orbits of Ω under G partition Ω .

The next two topics that we cover when considering group actions are conjugacy classes and transitive group actions.

Definition 4.5. If G is a group and $\Omega = G$ where the action is conjugation. Then if $x \in G$, $\mathcal{O}_x = \{x^g | g \in G\}$ is called the *conjugacy class* of x in G , denoted $\text{cl}_G(x)$.

Definition 4.6. An action is said to be *transitive* if Ω is a single orbit.

Theorem 4.3. Assume that G acts on Ω , where $\alpha \in \Omega$ and $H = G_\alpha$. Then there exists a bijection from $\{Hx | x \in G\}$ onto \mathcal{O}_α .

Proof. Define θ by $Hx = \alpha \cdot x$. As “cosets are slippery beasts”, one may assume that “orbits are slippery beasts, and they go by many names”. Therefore we first check that θ is well defined. So if $Hx = Hy$, we need that $\theta(Hx) = \theta(Hy)$. So $\theta(Hx) = \alpha \cdot x$ and $\theta(Hy) = \alpha \cdot y$. We wish to show that $\alpha \cdot x = \alpha \cdot y$. As $Hx = Hy$, we know that $y = hx$ for some $h \in H$. So $\alpha \cdot y = \alpha \cdot hx = (\alpha \cdot h) \cdot x$. Yet $H = G_\alpha$ by our construction, so $\alpha \cdot h = \alpha$, and thus $\alpha \cdot y = \alpha \cdot x$. Hence θ is well defined. That θ is injective, we must see that $\theta(Hx) = \theta(Hy)$ implies that $Hx = Hy$. So $\theta(Hx) = \theta(Hy)$ implies that $\alpha \cdot x = \alpha \cdot y$. If we act on both sides of this equality by y^{-1} , we see that $\alpha \cdot xy^{-1} = \alpha$. This implies that $xy^{-1} \in H$, and if we multiply on the right by y , we find that $x \in Hy$, so $Hx = Hy$. Finally, to see that θ is surjective, let $\gamma \in \mathcal{O}_\alpha$. Then $\gamma = \alpha \cdot g$ for some $g \in G$, and we may therefore find a preimage for γ by the coset Hg . \square

We now conquer the third reason for studying group actions, which is counting. We gain the following as an immediate corollary to the previous theorem. This corollary is often referred to as the Fundamental Counting Principle, or FCP.

Corollary(FCP) 4.3. $|\mathcal{O}_\alpha| = |G : G_\alpha|$.

Corollary 4.4. if $|G| < \infty$ and $\Omega = G$ where the action is conjugation, then $|\text{cl}_G(x)| = |G : \mathbb{C}_G(x)|$. Similarly, if $H \subseteq G$, then the number of conjugates of H in G is equal to $|G : \mathbb{N}_G(H)|$.

Proof. When G acts on itself via conjugation, the stabilizer of an element $x \in G$ is $\mathbb{C}_G(x)$ and the orbit of x is $\text{cl}_G(x)$. In the case where we consider subgroups instead of elements, the stabilizer is $\mathbb{N}_G(H)$ for a subgroup H of G . \square

Here, the second corollary is a direct application of the first.

For the next few proofs, we are only concerned with groups G and sets Ω of finite size. So until further notice, we assume that $|G| < \infty$ and $|\Omega| < \infty$.

We will soon be moving into Sylow theory, where an important topic of study is that of p -groups. The following yields our second result in that area: that p -groups have nontrivial centers.

Theorem 4.4. Suppose that $|G| = p^a$ where p is prime. Let $N \triangleleft G$, $N \neq 1$. Then $N \cap \mathbb{Z}(G) > 1$. In particular, $\mathbb{Z}(G) > 1$.

Proof. I have a proof written down here, but I have a common sense notion of why this is true. I will write that here and check it for a flaw. Let G act on N by conjugation. As N is also a p -group, N is partitioned by the orbits of this action. We wish to show that the number of elements $n \in N$ such that $|\mathcal{O}_n| = 1$ is greater than 1, as the elements with orbit size 1 are exactly the elements of $N \cap \mathbb{Z}(G)$. So suppose that it is not. Note that if $|\mathcal{O}_n| > 1$, then it must be divisible by p . Hence $|N|$, a p -power, is equal to the sum of the sizes of the G -orbits, all of which are divisible by p except for 1. This is a contradiction to the number theoretic fact that if p divides a and p divides b the p divides $a - b$. \square

We now return our attention to a finite group G acting upon itself via conjugation. Say G has k classes, and say the sizes of those classes are c_1, \dots, c_k . We know that all of the c_i divide the order of G by the FCP. Assume that $c_1 = 1$, as we know that $|\mathcal{O}_1| = 1$. We also know that the orbits of an action partition Ω , which here is G , so we know that $c_1 + c_2 + \dots + c_k = |G|$. This equation is called the *class equation* if G . From the class equation, we may derive many facts, including two relatively easy results. Namely, $k = 1$ if and only if G is the trivial group, and $k = |G|$ if and only if G is abelian.

As the final theorem for this section, we prove what Marty Isaacs likes to call the “Not Burnside Theorem”. The theorem we are about to prove was, for many years, wrongfully associated with the mathematician Burnside. It was later squabbled over as to who actually proved the theorem. I don’t know (and neither does Marty Isaacs) who actually proved the theorem in the end. All we know is that it wasn’t Burnside!

Theorem 4.5. Let G act on Ω and let N be the number of orbits. Given $g \in G$, write $\chi(g) = |\{\alpha \in \Omega | \alpha \cdot g = \alpha\}|$. Then $N = \frac{1}{|G|} \sum_{g \in G} \chi(g)$.

Proof. Consider $\sum_{g \in G} \chi(g) = \{(\alpha, g) | \alpha \in \Omega, g \in G, \alpha \cdot g = \alpha\}$. This sum is equivalent to $\sum_{\alpha \in \Omega} |G_\alpha|$. By the FCP, we know that $|\mathcal{O}_\alpha| = |G|/|G_\alpha|$. So we have that:

$$\sum_{\alpha \in \Omega} |G_\alpha| = \sum_{\alpha \in \Omega} \frac{|G|}{|\mathcal{O}_\alpha|} = |G| \sum_{\alpha \in \Omega} \frac{1}{|\mathcal{O}_\alpha|}$$

If we then break up single sum into a double sum, we find that this is equal to $|G| \sum_{\text{orbits } \mathcal{O}} \sum_{\alpha \in \mathcal{O}} \frac{1}{|\mathcal{O}|}$. Yet the inner summation is 1, so we find that this equals $|G| \sum_{\text{orbits } \mathcal{O}} 1$, or $|G|N$. As we began by considering the sum $\sum_{g \in G} \chi(g)$, we find that $\sum_{g \in G} \chi(g) = |G|N$, and the result follows. \square

As a corollary to the FCP, we gain an important counting result.

Corollary 4.5. Let $H, K \subseteq G$ be subgroups of G . Then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof. Let $\Omega = \{Hx | x \in G\}$ and let K act on Ω by right multiplication. Now $HK = \bigcup_{k \in K} Hk$. As $Hk = H \cdot k$, we see that HK is in fact the union of the cosets within Ω which contain H in their orbit. By the FCP, we know that $|\mathcal{O}_H| = |K : K_H|$, where $K_H = \{k \in K | H \cdot k = H\}$; that is, $K_H = H \cap K$. As cosets are disjoint and each coset contains exactly $|H|$ many elements, we find that $|HK| = |H||\mathcal{O}_H| = |H||K : H \cap K| = (|H||K|)/(|H \cap K|)$. \square

NOTE: I don't seem to have a great copy of this proof lying around. This is a little messy and needs to be cleaned up.

5 Sylow Theory

Definition 5.1. Let p be a prime and G be a finite group. Write $|G| = p^a m$ where $a \geq 0$, $m \geq 1$ and such that p does not divide m . A subgroup $S \subseteq G$ is a *Sylow p -subgroup* if $|S| = p^a$. We denote the set of Sylow p -subgroups of G by $\text{Syl}_p(G)$.

I believe it is a common practice for the theorems that follow to number them. We do not follow this convention; we instead assign letters to the three important Sylow theorems which imply more about what the theorems actually say than a number does.

Theorem(Sylow-E) 5.1. $\text{Syl}_p(G) \neq \emptyset$. In words: Sylow subgroups exist for all finite groups G and primes p .

Although simply stated, the proof is slightly difficult to prove. To prove this fact, we first prove a number theoretic lemma which will help in the proof of this theorem and will also be quite helpful later on in Galois theory when dealing with fields of characteristic p for p a prime.

Proof.

Lemma 5.1. Let p be a prime number. Then $\binom{p^a m}{p^a} \equiv m \pmod{p}$.

Proof. $(1+x)^p = 1+x^p \pmod{p}$ as each coefficient in the binomial expansion contains a factor of p in the coefficient. Using this, we find that $(1+x)^{p^2} \equiv 1+x^{p^2} \pmod{p}$, or inductively, that $(1+x)^{p^a} \equiv 1+x^{p^a} \pmod{p}$. This implies that $(1+x)^{p^a m} \equiv (1+x^{p^a})^m \pmod{p}$. We now examine the coefficient of x^{p^a} . By the binomial theorem, we have on the left hand side of this equivalence that $\binom{p^a m}{p^a}$ is the coefficient. On the right hand side, we have that the coefficient of x^{p^a} is $\binom{m}{1} = m$. So modulo p , we have that these two things are equivalent. \square

We now proceed with the proof of the Sylow-E theorem.

Let Ω be the set of all *subsets* of G with cardinality p^a ; that is, $\Omega = \{X \subseteq G \mid |X| = p^a\}$. So $|\Omega| = \binom{p^a m}{p^a} \equiv m \pmod{p}$ by our previous lemma. Note that as p does not divide m by hypothesis, the size of Ω cannot be congruent to 0 modulo p . Let G act on Ω by right multiplication. There must be an orbit of size not divisible by m as m is not congruent to 0 modulo p . Call this orbit \mathcal{O} . By the FCP, we know that $|\mathcal{O}| = |G|/|H|$ where $H = G_X$ for some $X \in \mathcal{O}$. Replacing $|G|$ with $p^a m$, we have that $|\mathcal{O}| = \frac{p^a m}{|H|}$. Since p does not divide $|\mathcal{O}|$, we must have that p^a divides $|H|$; this shows that $|H| \geq p^a$. We now wish to show that $|H| \leq p^a$. So let $x \in X$, where X is such that $H = G_X$. Recall that $Xh = X$ for $h \in H$. Then $xh \in X$ for all $h \in H$. Thus $xH \subseteq X$. Yet the sizes of cosets are equal, so we must have that $|xH| = |H| \leq |X| = p^a$. So H is a subgroup of G with size p^a , and therefore $\text{Syl}_p(G)$ is nonempty. \square

Simply knowing the existence of Sylow subgroups allows us to exclude particular numbers as the orders of simple groups. Consider the following corollary:

Corollary 5.1. Suppose $|G| = pq$, where p and q are prime, $p < q$. Then G cannot be simple.

Proof. Let $H \subseteq G$ be a Sylow q -subgroup of G which exists by the Sylow-E theorem. Then $|G : H| = pq/q = p$, which is the smallest prime divisor of $|G|$; hence $1 < H \triangleleft G$, and G is not simple. \square

It is a bit harder, but it is a good exercise to show that if $|G| = pqr$ where p, q , and r are distinct primes that G cannot be a simple group. It is a great exercise to determine all numbers up to 1000 which cannot be the orders of simple groups. Most are straightforward: there are only two which are tricky, and are listed in Guillermo's notes.

We next prove a theorem which has as two of its corollaries the Sylow-C and Sylow-D theorems; the C stands for conjugation and the D stands for development.

Theorem 5.2. Let $S \in \text{Syl}_p(G)$, and let $P \subseteq G$ be a p -subgroup. Then there exists $g \in G$ such that $P \subseteq S^g$.

Proof. Let $\Omega = \{Sx \mid x \in G\}$ and let P (notice P NOT G) act on Ω by right multiplication. Then $|\Omega| = |G : S|$ is not divisible by p as $S \in \text{Syl}_p(G)$. So there must exist a P -orbit \mathcal{O} of size not divisible by p , as the sum of multiples of p is always a multiple of p . However, $|\mathcal{O}|$ must divide $|P|$ by the FCP. So $|\mathcal{O}|$ is a power of p as P is a p -group. Hence $|\mathcal{O}| = 1$. So what is \mathcal{O} ? It is some coset of S in G , say Sg , such that for all $x \in P$, we have $Sgx = Sg$. So $P \subseteq G_{Sg} = S^g$. \square

NOTE: It might be a good idea to look at this proof again. It contains a LOT of important concepts.

As an immediate corollary, we obtain the Sylow-C theorem, which states that all members of $\text{Syl}_p(G)$ are conjugate to one another.

Corollary(Sylow-C) 5.2. If $S, P \in \text{Syl}_p(G)$ then $P = S^g$ for some $g \in G$.

Proof. By the previous theorem, we know that there exists $g \in G$ such that $P \subseteq S^g$. Yet this implies equality as the size of the groups is finite and conjugation is a bijection. \square

Corollary(Sylow-D) 5.3. Let $P \subseteq G$ be a p -subgroup. Then P is contained in some Sylow p -subgroup of G .

Proof. Let $S \in \text{Syl}_p(G)$, which exists by the Sylow-E theorem. Then by the Sylow-C theorem, there exists $g \in G$ such that $P \subseteq S^g$. Yet $S^g \in \text{Syl}_p(G)$ as conjugation preserves orders. \square

We will often be concerned with the number of Sylow p -subgroups a group G has. We refer to this number as $n_p(G) = |\text{Syl}_p(G)|$. Note that $n_p(G) = 1$ if and only if $S \in \text{Syl}_p(G)$ is normal in G . In fact, if $n_p(G) = 1$ and S is that Sylow p -subgroup, it is *the* Sylow p -subgroup of G and is therefore characteristic in G .

We consider an important example involving $n_p(G)$. Let $S \in \text{Syl}_p(G)$ and let G act on its set of subsets via conjugation. Then $n_p(G) = |\mathcal{O}_S| = |G : G_S|$. Recall that with this action, $G_S = \mathbf{N}_G(S)$, so it may also be written that $n_p(G) = |G : \mathbf{N}_G(S)|$.

Then next theorem, although not a lettered Sylow theorem, is very heavily used when proving that groups of a given order cannot be simple, and is often called the Sylow Counting Theorem.

Theorem (Sylow Counting) 5.3. $n_p(G) \equiv 1 \pmod{p}$.

Proof. As we did in the proof of the Sylow-E theorem, we first prove a lemma which will help to prove the Sylow counting theorem.

Lemma 5.2. Let $S \in \text{Syl}_p(G)$. Let P be a p -subgroup of $\mathbf{N}_G(S)$. Then $P \subseteq S$.

Proof. Let $N = \mathbf{N}_G(S)$. Note that $S \in \text{Syl}_p(G)$ and $S \subseteq N$ implies that $S \in \text{Syl}_p(N)$. Then by the Sylow-C theorem, there exists $n \in N$ such that $P \subseteq S^n$. Yet $S \triangleleft N$, so $S^n = S$, and therefore $P \subseteq S$. \square

With this lemma, we now continue with the proof of the Sylow counting theorem.

Let $S \in \text{Syl}_p(G)$. Let S act on $\text{Syl}_p(G)$ by conjugation (the Sylow-C theorem shows that this is indeed a group action). One orbit of this action is $\{S\}$. It suffices to show that all other orbits have sizes which are divisible by p . Yet all of the orbit sizes must divide the order of the group acting on it, which is S . So all orbit sizes are p -powers, and we must simply show that they are not all zero powers of p . To do this, we show that if $\{T\}$ is an orbit, then $\mathcal{O} = \{S\}$. So suppose $\{T\}$ is an orbit. Then $T^s = T$ for all $s \in S$. Then $T \subseteq \mathbf{N}_G(S)$, and as $T \in \text{Syl}_p(G)$, we see that T is a p -group. So by our lemma, $T \subseteq S$. Yet $|T| = |S|$, and in finite groups, this implies that $T = S$. Thus the only Sylow p -subgroup with an orbit of size p^0 is one, and all other orbits have size divisible by p , and the result holds. \square

Most of this equipment is being set up in order to show that groups of particular sizes cannot be simple. We do one example here, and leave a slightly more complicated example as an exercise.

Lemma 5.3. Suppose that $|G| = pq^2$, where p, q are prime and $p \neq q$. Then G is not simple.

Proof. To show that G is not simple, we will show that either $n_p(G) = 1$ or $n_q(G) = 1$. If $p < q$, then if $S \in \text{Syl}_q(G)$, we have that $|S| = q^2$ and therefore $|G : S| = p$, which is the smallest prime divisor of $|G|$. Hence $S \triangleleft G$ and G is not simple. So $q < p$. Now if $S \in \text{Syl}_p(G)$, we know that $n_p(G) = |G : \mathbf{N}_G(S)|$ and therefore $n_p(G)$ divides q^2 . So $n_p(G) \in \{1, q, q^2\}$. Yet $n_p(G)$ must also be congruent to 1 mod p , so either $q \equiv 1 \pmod{p}$ or $q^2 \equiv 1 \pmod{p}$. As $q < p$ by the case we are in, we cannot have that $n_p(G) = q$ as $q \equiv q \pmod{p}$. So there are q^2 subgroups of order p . This accounts for $q^2(p-1)$ elements of G , each with order p . So the elements with order not equal to p is at most q^2 . Yet this implies that if $Q \in \text{Syl}_q(G)$, then $|Q| = q^2$, and there is no room left for any other subgroups. Therefore Q is the Sylow q -subgroup of G and is thus normal. In either case, we find that G has a normal subgroup, and therefore G cannot be simple. \square

We now leave as an exercise a slightly more difficult version of this proof.

Exercise 5.1. Suppose that $|G| = pq^3$ where $p \neq q$ and both p and q are prime. Then G has a normal Sylow p or Sylow q -subgroup or $|G| = 24$.

Proof. Exercise. \square

As these types of problems are extremely popular on the qualifying exam, I leave one more as an example. It would definitely be worth looking up many more examples.

Exercise 5.2. Any group G with order $616 = 2^3 \cdot 7 \cdot 11$ is not a simple group.

Proof. Exercise. \square

The next notion we introduce is what is known as the Frattini argument.

Theorem 5.4. Let $N \triangleleft G$, where N is finite, and let $P \in \text{Syl}_p(N)$. Then $G = \mathbf{N}_G(P)N$.

Proof. Let $g \in G$. Then $P^g \subseteq N^g = N$ as $N \triangleleft G$. So $P^g \subseteq N$ and as $|P^g| = |P|$, we see that $P^g \in \text{Syl}_p(N)$. By the Sylow-C theorem, we know that there exists some $n \in N$ such that $(P^g)^n \subseteq P$. This implies that $P^{gn} = P$. So $gn \in \mathbf{N}_G(P)$. This implies that $g \in \mathbf{N}_G(P)n^{-1}$, and as $n^{-1} \in N$ as $n \in N$, we have that for all $g \in G$, we may write it in this form. \square

We now prove a very general theorem. The more useful application of the theorem will be a particular case, which will follow immediately as a corollary.

Theorem 5.5. Let G be a finite group, and let $\Phi(G) \subseteq N$, where $N \triangleleft G$. Assume that $N/\Phi(G)$ has a normal Sylow p -subgroup. Then N has a normal Sylow p -subgroup.

Proof. By assumption, the factor group $N/\Phi(G)$ has a normal Sylow p -subgroup, say $U/\Phi(G) \in \text{Syl}_p(N/\Phi(G))$. In fact, as $U/\Phi(G)$ is *the* Sylow p -subgroup of $N/\Phi(G)$, it is actually characteristic in $N/\Phi(G)$. As $N \triangleleft G$, we know that $N/\Phi(G) \triangleleft G/\Phi(G)$, and as $U/\Phi(G)$ is characteristic in a normal subgroup of $G/\Phi(G)$, we see that $U/\Phi(G) \triangleleft G/\Phi(G)$. Then by the Correspondence Theorem, $U \triangleleft G$.

Let $P \in \text{Syl}_p(U)$. We claim that $P\Phi(G) = U$. Let $|U| = p^a m$, where m is not divisible by p . As $P \in \text{Syl}_p(U)$, we see that $|U : P| = m$, and as $U/\Phi(G) \in \text{Syl}_p(N/\Phi(G))$, we know that $|U/\Phi(G)|$ is a p -power. As indices are preserved by homomorphisms, we have that $|U : \Phi(G)|$ is a p -power. Therefore the order of their product is the product of their orders, which is $|U|$, and the claim is proved.

Now, we see that the Frattini argument applies, and we have that $\mathbf{N}_G(P)U = G$. As $U = P\Phi(G)$, we see that $G = \mathbf{N}_G(P)P\Phi(G) = \mathbf{N}_G(P)\Phi(G)$. Yet $\Phi(G)$ is in some sense, the set of useless group elements (see 1.1). So $G = \mathbf{N}_G(P)$, and thus $P \triangleleft G$. If $P \triangleleft G$, we certainly have that $P \triangleleft N$, as desired. \square

The special case that we are interested in is when $N = \Phi(G)$. In this case, there are really no hypotheses except that G be a finite group.

Corollary 5.4. If G is a finite group, then all Sylow p -subgroups of $\Phi(G)$ are normal.

6 Nilpotent Groups

At this point and time in the course, start studying things like nilpotent, solvable, and supersolvable groups. All of these different ideas came about as weakenings of the property of a group being abelian. It turns out, in group theory, that being abelian is quite boring: we can classify everything. So in a sense, it is often too strong to require that a group be abelian. However, we can weaken our assumptions a little, and have our groups be “not quite abelian”, we can get some interesting behavior.

Definition 6.1. Let G be a group, and suppose we have a collection of subgroups $N_i \triangleleft G$ where $1 = N_0 \subseteq N_1 \subseteq N_2 \subseteq \dots \subseteq N_r = G$. Then we say that the N_i form a *normal series* for the group G . We say that this series is a *central series* in G if $\frac{N_i}{N_{i-1}} \subseteq \mathbf{Z}\left(\frac{G}{N_{i-1}}\right)$ for $1 \leq i \leq r$.

Definition 6.2. A group G is said to be *nilpotent* if it has a central series.

It may be worth noting that we mean for there to be no repeated subgroups in a normal or central series. It is often therefore assumed within the definition that for all N_i, N_j where $i \neq j$, we have that $N_i \neq N_j$.

As in the discussion above, a group being nilpotent is a weaker assumption than a group being abelian. Therefore all abelian groups are automatically nilpotent. For an example of groups which are nilpotent but not necessarily abelian, we turn to p -groups.

Theorem 6.1. Every finite p -group is nilpotent.

Proof. If G is a p -group, let $Z_0 = 1$, and let $Z_1 = \mathbf{Z}(G)$. We then construct Z_2 such that $Z_2/Z_1 = \mathbf{Z}(G/Z_1)$, and as p -groups have non-trivial centers, we see that $Z_2 > Z_1$. We then continue in this manner, allowing $Z_{i+1}/Z_i = \mathbf{Z}(G/Z_i)$. Note that this process will halt finitely as G is a finite group. This series is known as the *upper central series* of G . \square

We next prove one of our most useful theorems when dealing with nilpotent series. This theorem is often quoted with the tagline: “normalizers grow”, and according with our previous example, it is not uncommon to hear: “In p -groups, normalizers grow”.

Theorem 6.2. Let G be a finite group. TFAE:

1. G is nilpotent.
2. If $H < G$, then $\mathbf{N}_G(H) > H$.
3. Maximal subgroups of G are normal.
4. All Sylow subgroups of G are normal.
5. If $N \triangleleft G$ and $N < G$, then $\mathbf{Z}(G/N) > 1$

Proof. As we did in the previous section, we prove two lemmas prior to proving the theorem in order to ease the proof of the theorem.

Lemma 6.1. If $N \triangleleft G$ and $P \in \text{Syl}_p(G)$ with $P \triangleleft G$, then NP/N is a normal Sylow p -subgroup of G/N .

Proof. As $P \subseteq NP$, we know that $|G : NP|$ is p' (we use this notation to mean not divisible by p). By the correspondence theorem, we then find that $|G/N : NP/N|$ is p' . Also by the correspondence theorem, as $NP \triangleleft G$ since both N and P are normal in G , we know that $NP/N \triangleleft G/N$. To see that $|NP/N|$ is a power of p , we compute:

$$|NP/N| = |NP : N| = |NP|/|N| = \frac{|N||P|}{|N \cap P|} = \frac{|P|}{|N \cap P|}$$

which this last quantity is a p -power as $P \in \text{Syl}_p(G)$ and $N \cap P \subseteq P$. Hence $NP/N \triangleleft G/N$ and $NP/N \in \text{Syl}_p(G/N)$ as NP/N has p -power order and index relatively prime to p . \square

The proof of the previous lemma is one which follows almost immediately from the correct picture. I leave a gap in order to draw that picture in:

The next lemma we will use is very similar to the result that p -groups have nontrivial centers: as p -groups are nilpotent groups, the next lemma actually states that nilpotent groups have nontrivial centers.

Lemma 6.2. Let G have all Sylow subgroups for all primes normal. Assume that G is nontrivial. Then $\mathbf{Z}(G) > 1$.

Proof. Choose a prime p such that p divides $|G|$. Also choose $P \in \text{Syl}_p(G)$. As p divides $|G|$, we see that P is not the trivial group. Write $Z = \mathbf{Z}(P)$. Note that Z is also not the trivial group as p -groups have nontrivial centers. We will show that $Z \subseteq \mathbf{Z}(G)$. To do this, we will show that $\mathbf{C}_G(Z) = G$. So assume for the sake of contradiction that $\mathbf{C}_G(Z) < G$, and let q be a prime dividing $|G : \mathbf{C}_G(Z)|$. Since $Z = \mathbf{Z}(P)$, we know that $P \subseteq \mathbf{C}_G(Z)$, so $q \neq p$. Let $Q \in \text{Syl}_q(G)$. $Q \triangleleft G$ by hypothesis, and $Z \triangleleft G$ as Z is characteristic inside P which is normal in G . Also, $Q \cap Z = 1$ as the elements in Z all have p -power order and the elements in Q all have q -power order. Then by a homework assignment (and it is not difficult to prove) Q and Z commute (result known as disjoint normal subgroups commute) and thus $Q \subseteq \mathbf{C}_G(Z)$. Yet this implies that q does not divide $|G : \mathbf{C}_G(Z)|$ as $Q \in \text{Syl}_q(G)$, which is a contradiction. Therefore there does not exist a prime q dividing the index, and $|G : \mathbf{C}_G(Z)| = 1$, and $Z \subseteq \mathbf{Z}(G)$. \square

We finally return to the proof of our main theorem on nilpotent groups. We begin with $1 \rightarrow 2$. So assume that G is nilpotent, and let $H < G$. As G is nilpotent, we have that there exists a central series for G , that is, normal subgroups N_i with the property that $1 = N_0 \subseteq N_1 \subseteq \dots \subseteq N_r = G$, and such that $N_{i+1}/N_i \subseteq \mathbf{Z}(G/N_i)$ for all $1 \leq i \leq r$. As $H < G$, we see that N_r is not contained in H , but $N_0 = 1$ certainly is contained in H . Fix i such that $N_i \subseteq H$ but $N_{i+1} \not\subseteq H$. We know that $N_{i+1}/N_i \subseteq \mathbf{Z}(G/N_i)$. As anything in the center of a group is in the normalizer of any subgroup, we have that $N_{i+1}/N_i \subseteq \mathbf{N}_{G/N_i}(H/N_i)$. Also, the normalizer of a subgroup is always greater than or equal to itself so $H/N_i \subseteq \mathbf{N}_{G/N_i}(H/N_i)$. Therefore as $H/N_i, N_{i+1}/N_i \subseteq \mathbf{N}_{G/N_i}(H/N_i)$, we have that $HN_{i+1}/N_i \subseteq \mathbf{N}_{G/N_i}(H/N_i)$, and thus by the correspondence theorem, $HN_{i+1} \subseteq \mathbf{N}_G(H)$. Yet $N_{i+1} \not\subseteq H$, so $HN_{i+1} > H$, and $HN_{i+1} \subseteq \mathbf{N}_G(H)$.

That $2 \rightarrow 3$ is obvious. To see that $3 \rightarrow 4$, let $P \in \text{Syl}_p(G)$. We will show that $P \triangleleft G$. So assume to the contrary that $\mathbf{N}_G(P) < G$ and let $M < G$ be maximal such that $\mathbf{N}_G(P) \subseteq M$. Now $M \triangleleft G$ by 3, and as $P \subseteq \mathbf{N}_G(P) \subseteq M$ we have that $M \in \text{Syl}_p(M)$. Thus the Frattini argument applies, and we see

that $G = \mathbf{N}_G(P)M$. Yet $\mathbf{N}_G(P) \subseteq M$, so we see that $G = M$, which is a contradiction to M being maximal in G . Hence $\mathbf{N}_G(P) = G$ and $P \triangleleft G$.

To see that $4 \rightarrow 5$, we assume that all Sylow p -subgroups are normal and show that if $N \triangleleft G$ and $N < G$ then $\mathbf{Z}(G/N) > 1$. To do this, we use our lemmas. $N \triangleleft G$ by assumption, and if P is any Sylow p -subgroup of G for any prime p , we know that NP/N is a normal Sylow p -subgroup of G/N by lemma 1. Then lemma 2 tells us that as G/N is a group with all Sylow p -subgroups for all primes p normal, and G is nontrivial as $N < G$, we see that $\mathbf{Z}(G/N) > 1$ by lemma 2.

To complete our proof, we show that $5 \rightarrow 1$. We assume by the case we are in that $G > 1$. So G has a nontrivial center by 5, and we construct the upper central series for G by letting $Z_0 = 1$ and $Z_1 = \mathbf{Z}(G)$. If $\mathbf{Z}(G) \neq G$, we continue, using 5 to conclude that our centers are “growing” (this is essentially the same proof that p -groups have nontrivial centers and are therefore nilpotent.) □

We do not prove, but rather note the useful fact that subgroups and factor groups of nilpotent groups are nilpotent (Isaacs’ book has a proof, or else it may be done as an exercise).

We end the section on nilpotent groups with a slight digression towards elementary abelian groups.

Definition 6.3. A p -group G is said to be *elementary abelian* if it is abelian and $x^p = 1$ for all $x \in G$.

An example of an elementary abelian p -group is U_8 , the group of integers relatively prime to 8. We did not use elementary abelian groups much throughout the semester, but I think it is a good exercise to be able to come up with examples of things.

We do one proof regarding elementary abelian groups. It uses a very common and helpful proof technique: if you wish to show that a factor group is abelian, you show that the commutator is contained in the kernel.

Corollary 6.1. If G is a p -group, then $G/\Phi(G)$ is elementary abelian.

Proof. We must show that $G/\Phi(G)$ is a p -group (which follows as G is a p -group), that $G/\Phi(G)$ is abelian, and that $x^p = 1$ for all $x \in G/\Phi(G)$. To see that $G/\Phi(G)$ is abelian, we show that $G' \subseteq \Phi(G)$. It suffices to show that $G' \subseteq M$ for all M maximal in G . As G is a p -group, it is nilpotent, and therefore if M is maximal in G , M is also normal in G . By the maximality of M , we then find that G/M has no subgroups, and must be of order p . As all prime ordered groups are cyclic and therefore abelian, we find that $G' \subseteq M$. Yet M was an arbitrary maximal subgroup of G , so $G' \subseteq \Phi(G)$. Finally, we show that any element of $G/\Phi(G)$ raised to the p power is the identity. As all elements of $G/\Phi(G)$ are cosets of $\Phi(G)$ in G , they have the form $\Phi(G)x$ for some $x \in G$. We want to show that $(\Phi(G)x)^p = \Phi(G)$, or that $x^p \in \Phi(G)$ for all $x \in G$. It therefore suffices to show that $x^p \in M$ for all M maximal in G . Let y be the

image of x mod M . We know that $|G : M| = p$, so if $y \in G/M$, then $y^p = 1$, which implies that $x^p \in M$. \square

7 Solvable Groups

Our next main topic is a different class of nonabelian groups which, in many ways, have “nice” abelian-like properties.

Definition 7.1. A group G is *solvable* if there exist subgroups $N_i \triangleleft G$ such that $1 = N_0 \subseteq N_1 \subseteq \dots \subseteq N_r = G$ where N_{i+1}/N_i is abelian for all $1 \leq i \leq r$.

Note that being solvable is a weaker condition than being nilpotent; that is, nilpotent groups are automatically solvable groups, as are abelian groups. We therefore search for examples of groups which are solvable but not nilpotent.

Recall for a given group G its derived subgroup $G' = \langle \{[x, y] = xyx^{-1}y^{-1} \mid \forall x, y \in G\} \rangle$. As an exercise on homework assignment 4 problem 4, we showed that given $H \subseteq G$, we had $G' \subseteq H$ if and only if $H \triangleleft G$ and G/H is abelian. We denote by $G^{(n)}$ the n th commutator subgroup; the commutator of the commutator of the commutator, etc. We call the collection of $G^{(i)}$ the *derived series* for a group G . The derived series of a group is closely tied in with the property of a group being solvable.

Lemma 7.1. Given a group G , G is solvable if and only if $G^{(n)} = 1$ for some $n \in \mathbb{N}$.

Proof. First, fix n smallest such that $G^{(n)} = 1$. Then $1 = G^{(n)} \subseteq G^{(n-1)} \subseteq \dots \subseteq G^0 = G$ forms a normal series for G as each $G^{(i)}$ is in fact characteristic in G (it is the i th commutator subgroup of G). Additionally, we know that any group modulo its commutator subgroup is abelian, and therefore each of the factor groups $G^{(i-1)}/G^{(i)}$ is abelian.

For the other direction, suppose that G is solvable, and let $1 = N_0 \subseteq N_1 \subseteq \dots \subseteq N_r = G$ is a normal series for G such that N_i/N_{i-1} is abelian. Then for each N_i , we see that $(N_i)' \subseteq N_{i-1}$. So $G' \subseteq N_{r-1}$, and in general, $G^{(k)} \subseteq N_{r-k}$. In particular, this implies that $G^{(r)} \subseteq N_0 = 1$, as desired. \square

Definition 7.2. If G is solvable, then the *derived length* of G is the minimum $n \in \mathbb{N}$ such that $G^{(n)} = 1$. We denote this by $dl(G)$.

We note two things: first, G is abelian if and only if $dl(G) = 1$, and if G is a simple group, then G is solvable if and only if G is abelian.

NOTE: $G' \neq \{xyx^{-1}y^{-1} \mid x, y \in G\}$. It is equal to the *group generated by these elements*; that is, $\langle [x, y] \mid x, y \in G \rangle$. It CAN include elements which are not of the form $xyx^{-1}y^{-1}$, although I do not have an example of this. As homework, I should really come up with one.

We again note that subgroups and factor groups of solvable groups are solvable. We actually have a stronger result also when dealing with solvable groups, which we prove as a lemma. Note that the stronger part of the following lemma is NOT true for nilpotent groups.

Lemma 7.2. Let G be a group.

1. If G is solvable and $H \subseteq G$, then H is solvable.
2. If $\theta : G \rightarrow H$ is a surjective homomorphism and G is solvable, then H is solvable.
3. Let $N \triangleleft G$. Assume that N is solvable and G/N is solvable. Then G is solvable.

Proof. For 1, we note that if $H \subseteq G$, then $H^{(m)} \subseteq G^{(m)}$ for all $m \in \mathbb{N}$. Yet G is solvable, so $G^{(n)} = 1$ for some n . Hence $H^{(n)} = 1$, and H is solvable.

As $G^{(n)}$ is actually characteristic for G , note that $\theta(G^{(n)}) = H^{(n)}$ as homomorphisms preserve group theoretic properties. Therefore if $G^{(n)} = 1$, we have that $\theta(1) = \theta(G^{(n)}) = H^{(n)}$, and therefore H is solvable.

For 3, let π be the canonical homomorphism from $G \rightarrow G/N$. We know that G/N is solvable, so say r is such that $(G/N)^{(r)} = 1$. Then $(\pi(G))^{(r)} = 1$, and hence $\pi(G^{(r)}) = 1$. So $G^{(r)} \subseteq N$. Yet N is solvable by assumption, so there exists s such that $N^{(s)} = 1$. Hence $(G^{(r)})^{(s)} = 1$. Yet $(G^{(r)})^{(s)} = G^{(r+s)}$, so G is solvable. \square

We note (although it is in my notes officially as a corollary) that when dealing with solvable groups, say G has $1 = N_0 \triangleleft N_1 \triangleleft \dots \triangleleft N_r = G$ with factor groups abelian. Then it is enough for each N_i to simply be normal within N_{i+1} . It is not actually necessary for each $N_i \triangleleft G$. The result follows by induction and by part 3 of the previous theorem.

Theorem 7.1. Let G be a finite solvable group.

1. Let N be minimal normal in G . Then N is an elementary abelian p -group for some prime p .
2. Let M be maximal in G . Then $|G : M|$ is a prime power order.

Proof. Since $N \subseteq G$ and G is solvable, we know that $G^{(k)} = 1$ for some integer k . As subgroups of solvable groups are solvable, we know that $N^{(m)} = 1$ for some m . Hence $N' < N$. But N' is characteristic in N and $N \triangleleft G$, so $N' = 1$, and N is therefore abelian. Choose $x \in N$ with order p for some prime p . Let $S = \{t \in N \mid t^p = 1\}$. As $x \in S$, we see that $|S| > 1$. As N is abelian, we claim that S is a subgroup of N . First of all, it contains inverses as the inverse of any element has the same order, and it is closed as if $s, t \in S$, then $(st)^p = s^p t^p = 1$, where the distribution of the p -power uses our abelian assumption. However, from our definition we see that S is characteristic in N (it is *the* set of elements $x \in N$ such that $x^p = 1$), and therefore $S \triangleleft G$. Yet N is minimal normal, so we must have $S = N$, and thus N is elementary abelian. To see that N is a p -group, note that by Cauchy's theorem, if q is a prime dividing $|N|$, then there must exist an element of order q . Yet all elements in N have order p , so such an element cannot exist. Hence N is a p -group.

For part (b), let $K = \text{core}_G(M)$, recalling that the core of M in G is the largest normal subgroup of G contained in M . Now $K < G$ as $K \subseteq M < G$ and as factor groups of solvable groups are solvable, G/K is a nontrivial solvable group. So G/K has a nontrivial minimal normal subgroup, say X/K . Now $K \subseteq X \subseteq G$ and $X \triangleleft G$ by the correspondence theorem. So $X \not\subseteq M$ as $X > K$ and $K = \text{core}_G(H)$ by construction. Yet XM is a subgroup of G as $X \triangleleft G$, and $XM > M$ as $X \not\subseteq M$. So by the maximality of M , we must have $XM = G$. Applying part (a), we see that X/K is a p -group. Yet by the diamond lemma, $|G|/|M| = |G : M| = |X : X \cap M|$. Yet $|X : X \cap M|$ is a p -power as X is a p -group, and the result holds. \square

Perhaps the most important things about solvable groups are that subgroups and factor groups of solvable groups are solvable, and that the derived series works as a normal series for any solvable group.

8 Finite Symetric Groups

For this section, we will be working with Ω and $\text{Sym}(\Omega)$, where we usually take $\Omega = \{1, 2, \dots, n\}$ and in this case, write $\text{Sym}(\Omega) = S_n$. Recall then that $|S_n| = n!$.

Definition 8.1. An element $g \in S_n$ is a r -cycle for $1 \leq r \leq n$ if there exist r distinct elements $\alpha_1, \alpha_2, \dots, \alpha_r \in \Omega$ such that $\alpha_1 \xrightarrow{g} \alpha_2 \xrightarrow{g} \dots \xrightarrow{g} \alpha_r \xrightarrow{g} \alpha_1$ and g fixes all other points in Ω . For short, we write $g = (\alpha_1, \alpha_2, \dots, \alpha_r)$.

If g is an r -cycle, we may also write $g = (\alpha_2, \alpha_3, \dots, \alpha_r, \alpha_1)$, so every r -cycle actually has r names.

Definition 8.2. If $x, y \in S_n$, we say that x and y are *disjoint* if the sets of moved points are disjoint.

As a quick example, take $(3, 5, 7)(1, 2, 4, 9)$ inside S_n where $n \geq 9$.

We reference two theorems which we do not prove but are very heavily used. First, that disjoint cycles commute. Second, that every nonidentity element of S_n can be written as the product of disjoint cycles, which is therefore unique except up to the ordering of the factors.

It is standard, when writing down a cycle, to omit the fixed points, rather than writing them as single cycles.

It is very hard to explain precisely how multiplying cycles works, but I will include an example, from which the experienced reader can figure out how to multiply cycles.

Example 8.1. $(2, 1, 3, 5)(4, 6, 9) \cdot (1, 7, 3)(6, 4, 10) = (2, 7, 3, 5)(6, 9, 10)$

We also introduce a bit of notation in the definition of a cycle structure. As in example, in S_6 , the element $(2, 4)(3, 1, 5)$ has *cycle structure* $1^1 2^1 3^1$; we write the cycle size taken to the power of the number of those cycles in the decomposition.

We now do a very important example in S_5 , where we count all of the group elements according to their cycle structure and order. Here, the order of the element is the LCM of the cycle sizes.

Structure	How Many	Order
1^5	1	1
$1^3 2^1$	$\binom{5}{2} = 10$	2
$1^1 2^2$	$\binom{5}{2} \binom{3}{2} / 2 = 15$	2
$1^2 3^1$	$\binom{5}{3} = 10$	3
$2^1 3^1$	$\binom{5}{2} 2 = 20$	6
$1^1 4^1$	$\binom{5}{4} 3! = 30$	4
5^1	$4! = 24$	5

Example 8.2.

One can check that the number of elements adds up to 120, the size of S_5 . As an example, we explain the counting argument for the cycle $1^1 4^1$. There are $\binom{5}{4}$ elements that we can put into the four cycle; however, we still have options for the order of the 4-cycle. As there is no “first” element of a cycle, fix a starting place. There are $3!$ ways to order the remaining three elements, and then the cycle is determined. Another way to view this is as $4!$ ways to order the cycle, and then we must divide out by the number of names each cycle has, so $3! = 4!/4$.

If any of these counting arguments seem difficult or took a bit of thought, it is a great exercise to make this sort of a table for S_6 . I did for a homework assignment, and it was a good experience in getting my hands dirty. Not to mention that it gets slightly more complicated to count in S_6 due to the particular permutation with cycle structure 2^3 . I leave this as an exercise.

We next consider what it looks like to conjugate cycles; that is, what is $(\alpha_1, \alpha_2, \dots, \alpha_r)^g$? We define it to be $(\alpha_1 \cdot g, \alpha_2 \cdot g, \dots, \alpha_r \cdot g)$. We exhibit an example of conjugation below.

Example 8.3. $(1, 2)(3, 4, 5)^{(1, 2, 3)} = (2, 3)(1, 4, 5)$

Notice that in the example our original cycle structure is preserved under the conjugation action. What is most important about conjugation is that it always preserves cycle structures. Conversely, any two elements with the same cycle structure are conjugate.

We now move on to a new topic which is important within symmetric groups.

Definition 8.3. A *transposition* in S_n is a two-cycle.

Note that any r -cycle can be written as a product of $(r - 1)$ transpositions, so any cycle can be represented via transpositions.

Definition 8.4. An element g of S_n is *even* if it can be written as a product of an even number of transpositions. We say that g is *odd* if it is the product of an odd number of transpositions.

It is a theorem, and a very important one, that no element of S_n is both even and odd. We will prove this fact, but we may gloss over some details.

Theorem 8.1. No element of S_n is both even and odd.

Proof. Assume to the contrary that this is false, and write an element g as $t_1 t_2 \dots t_k = s_1 s_2 \dots s_l$ where the t_i and s_j are transpositions, such that k is odd and l is even. We then get that $t_1 t_2 \dots t_m = 1$, where $m = k+l$, and the t_i are all transpositions. Note that this follows as transpositions are their own inverses. We do this with the smallest possible m . We note a clever trick; that if t and s are transpositions, we have that $st = ts^t$. This follows as $ts^t = tt^{-1}st = st$. As conjugation preserves cycle structures, this allows us to rearrange the order of multiplication within a product of transpositions without altering the result OR the number of transpositions.

We claim that all of the t_i are different. This follows as if, say, $t_1 = t_j$ for some j , we may essentially move t_j next to t_1 by replacing $t_{j-1}t_j$ by $t_j t_{j-1}^{t_j}$ from our observation above. Yet this lowers the number of transpositions by two, and we assumed that m was minimal and odd, which is a contradiction. This may be a little unclear, so I leave space for a drawing to clarify:

It is without loss to assume that $t_1 = (1, 2)$. Say that $t_i = (1, a_i)$ for $1 \leq i \leq k$ and t_{k+1} is not of this form. Assume that we select k as large as possible with this property. That is, of all possible ways to write $t_1 t_2 \dots t_m$, select one which has a 1 in the first component for as long as possible. Note that this means that after t_k , the number 1 no longer appears in any of the transpositions; this follows as if there were a 1 in any transposition after t_k , we could move this transposition to the left of t_k using the previous conjugation trick, and this would contradict our maximal selection of k . Also note that as $t_1 = (1, 2)$, we know that t_2 through t_k do not include the number 2 as m is minimal. So within $t_1 t_2 \dots t_k$, 1 is mapped to 2 in t_1 , and then t_2 through t_k leave one there. From t_{k+1} through t_m , 2 may be mapped somewhere, but as k is maximal such that t_1 through t_k mention 1, and t_{k+1} through t_m do not mention one, 2 never makes it back to one.

I'm afraid that this reads a terrible mess, so I leave room for another small picture. My notes and memory of the lecture are far clearer than this explanation.

□

We move on to another important property of S_n ; the subgroup A_n , the set of even permutations; we obtain that A_n is a group by thinking of the identity as an even permutation. Note further that $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.

We include now what initially seems like a strange definition. However, it is quite useful when showing that particular groups are not simple.

Definition 8.5. We say that $g \in G$ acts *oddly* if $\pi_g \in \text{Sym}(\Omega)$ is an odd permutation.

Another way to think of an element acting oddly is that the map taking g to the permutation which is “dotting” by the element is an odd permutation. So if G acts on Ω and the element of $\text{Sym}(\Omega)$ which is defined by $g \mapsto \alpha \cdot g$ for all $\alpha \in \Omega$ is odd, then g acts oddly on Ω .

Lemma 8.1. Let G act on Ω where both G and Ω are finite, and assume that there exists $g \in G$ which acts oddly on Ω . Then $\exists N \triangleleft G$ such that $|G : N| = 2$.

Proof. Let θ be our odd action. We have homomorphisms $G \xrightarrow{\theta} \text{Sym}(\Omega) \xrightarrow{\text{sgn}} \{1, -1\}$, which maps a function in $\text{Sym}(\Omega)$ to 1 if the function is even and -1 if the function is odd. Then the composition of the maps θ and sgn is a map from $G \rightarrow \{1, -1\}$, which is surjective; namely, g maps to -1 , and 1 maps to 1. Therefore if N is the kernel of this map, then $|G : N| = 2$. \square

Corollary 8.1. Let $|G| = 2m$ where m is odd. Then there exists a normal subgroup N such that $|N| = m$.

Proof. Let $x \in G$ be an element of order 2, and let G act on itself by right multiplication. We claim that x acts oddly on G . To prove this, we show that the cycle structure of the permutation induced by x is all two cycles. To see that the elements of the permutation are at most two cycles, note that as $o(x) = 2$, we know that the second power of the permutation induced by x is the identity, so we have only transpositions and fixed points as possibilities in the cycle structure of the permutation induced by x . Yet $g \neq 1$, so $gx \neq g$ for any $g \in G$, so we cannot have any fixed points. Therefore the permutation induced by x is exactly m transpositions. As m is odd, this implies that the permutation induced by x is odd, and the previous lemma implies that there exists $N \triangleleft G$ such that $|G : N| = 2$, so $|N| = m$. \square

The biggest consequence of this Corollary is that if the order of any group G is $2m$ for m an odd number (greater than one), then G cannot be the order of a simple group.

The next large theorem finally renders our first good example of nonabelian simple groups; the alternating groups for A_5 and larger. The proof is a bit involved, and essentially follows by induction once we show that A_5 is a simple group. Therefore the first very important part of the proof deals with showing that A_5 is a simple group.

Theorem 8.2. Let $n \geq 5$. Then A_n is a simple group.

Proof. We begin by counting the cycle structures within A_5 in order to get a better understanding of this very important group.

Structure	How Many	Order
1	1	1
$1^1 2^2$	15	2
$1^2 3$	20	3
5^1	24	5

Although I did not here include the binomials which lead to computing the number of permutations with a given cycle structure, the counting arguments can be found in table 8.2. So suppose that $1 < N \triangleleft G$, where $G = A_5$. We wish to show that $N = A_5$. So suppose that 3 divides $|N|$. Then N contains a Sylow 3-subgroup of G . Since $N \triangleleft G$, N contains all Sylow 3-subgroups of G as all Sylow 3-subgroups are conjugate by the Sylow-C theorem. So $|N| \geq 21$, and by LaGrange's theorem, we see that $|N| \in \{30, 60\}$.

Now suppose instead that 5 divides $|N|$. Then by an analogous argument, N contains all elements of order 5 and hence $|N| \geq 25$. Therefore we again find by LaGrange that $|N| \in \{30, 60\}$. Yet if $|N| = 30$, it is divisible by both 3 and 5, therefore containing all elements of order three AND all elements of order 5. Hence $|N| \geq 20 + 24 + 1 = 45$, which is a contradiction. So if either 3 or 5 divides $|N|$, we must have that $|N| = 60$ and $N = G = A_5$.

We may therefore assume that either $|N| = 4$ or $|N| = 2$. If $|N| = 4$, then we have that N is a Sylow 2-subgroup of G . But $N \triangleleft G$, so N contains all elements of order 2, which implies that $|N| \geq 15$, which is clearly a contradiction. We therefore assume that $|N| = 2$. It is no loss to assume that $N = \{1, (1, 2)(3, 4)\}$. We show that N is not normal in G . To do this, note that $(1, 2, 5) \in G$, yet $(1, 2)(3, 4)^{(1, 2, 5)} = (2, 5)(3, 4)$, which is not the identity nor is it $(1, 2)(3, 4)$. This contradicts that $N \triangleleft G$, so $|N| \neq 2$. Therefore $N = G$, and we have that A_5 is a simple 5.

We proceed by induction, so assume that $n > 5$. Let H be a point stabilizer in A_n . Then $H \cong A_{n-1}$. By our inductive hypothesis, this means that H is simple. Then if $1 < N \triangleleft A_n$, then $N \cap H \triangleleft H$ by the diamond lemma, so we either have that $N \cap H = 1$ or $N \cap H = H$. We first suppose that $N \cap H = H$. Then $H \subseteq N$ so $|N| \geq |H|$, so we have either $N = H$ or $N = A_n$ by LaGrange. If $N = A_n$ we are done, so suppose that $N = H$. We note that all point stabilizers are conjugate; this follows as $G_\alpha^g = G_{\alpha \cdot g}$. So as $H \subseteq N$ and $N \triangleleft A_n$, we have that $H^g \subseteq N^g = N$ for all $g \in G$ (again, we are sometimes referring to G as A_n). So N not only contains H , but in fact all point stabilizers in A_n . So every permutation that fixes one point lies in N . Since every product of 2 transpositions fixes a point ($n \geq 5$), every such product is in N . Yet every permutation can be written as a product of products of 2 transpositions (they are all even), so $N = A_n$.

This leaves us in the case where $N \cap H$ is trivial. Thus, the intersection of N with every point stabilizer is trivial via a similar conjugacy argument to that in the previous paragraph. In other words, no nonidentity element of N

fixes a point. So choose $x \in N$ such that $x \neq 1$, and we may assume without loss that $x : 1 \rightarrow 2$ and $x : 3 \rightarrow 4$. (If 3 maps to 1, rename 4 = 3). So $x = (1, 2, \dots, 3, 4, \dots)$, and consider $x^{(4,5,6)} = (1, 2, \dots, 3, 5, \dots)$, which lies in N as N is normal. Now let $y = x^{-1}x^{(4,5,6)}$. Of course, $y \in N$ since $x^{-1} \in N$ and $x^{(4,5,6)} \in N$, and $y : 2 \rightarrow 2$ implies that $y = 1$. Yet x is clearly not equal to $x^{(4,5,6)}$ as $x : 3 \rightarrow 4$ and $x^{(4,5,6)} : 3 \rightarrow 5$. This is a contradiction, so $N \cap H \neq 1$. \square

As examples of how to apply the previous theorem, we do two examples.

Corollary 8.1. If $|G| = 120$ then G is not simple.

Proof. As $|G| = 120 = 2^3 \cdot 3 \cdot 5$, we know that $n_5 \in \{1, 2, 4, 8, 3, 6, 12, 24\}$. Yet $n_5 \equiv 1 \pmod{5}$, so $n_5 \in \{1, 6\}$. If we wish for G to be simple, we assume that $n_5 = 6$. So let $H = \mathbf{N}_G(P)$, where $P \in \text{Syl}_5(G)$. So $|G : H| = 6$ by our previous conclusion. Let G act via right multiplication on $\Omega = \{Hx \mid x \in G\}$. Now $\theta : G \rightarrow \text{Sym}(\Omega)$ via the “dotting” map and θ is a homomorphism. As $|\Omega| = 6$, we see that $\text{Sym}(\Omega) \cong S_6$, so θ may be thought of as a map from G to S_6 . As no element of g acts oddly, we in fact have $\theta : G \rightarrow A_6$. Yet $\ker(\theta) = \text{core}_G(H) \subseteq H < G$. As G is assumed to be simple, we must have that $\ker(\theta) = 1$. So $\theta(G)$, the image of G under θ , is actually isomorphic to G , and $\theta(G) \subseteq A_6$. Yet $|G| = |\theta(G)| = 120$, and $|A_6| = 6!/3 = 360$. Hence $|A_6 : \theta(G)| = 3$. However, the $n!$ theorem implies then that $|A_6|$ divides $3!$, which is clearly a contradiction. \square

Corollary 8.2. Let $n \geq 5$. Then the only normal subgroups of S_n are 1, A_n , and S_n .

Proof. Let $N \triangleleft S_n$. Assume that $N \neq 1$ and $N \neq S_n$. We show that $N = A_n$. By the diamond lemma, $N \cap A_n \triangleleft A_n$, so either $N \cap A_n = A_n$ or $N \cap A_n = 1$ as A_n is simple. If $N \cap A_n = A_n$, then $A_n \subseteq N$. As $|S_n : A_n| = 2$, we must have either $A_n = N$ or $N = S_n$. As $N \neq S_n$ by assumption, we have $A_n = N$. So assume that $N \cap A_n = 1$. Then as $|A_n| = \frac{1}{2}n!$, we can only have that $|N| = 2$. So $N = \{1, x\}$ for some $x \in S_n$. WLOG, assume that x maps 1 to 2. Then $x^g \subseteq N$ for all $g \in S_n$. Yet $x^{(2,3)}$ maps 1 to 3, which happens neither in x nor for 1. So $x^{(2,3)} \notin N$, which contradicts that $N \triangleleft S_n$. \square

9 Direct Products

The next main topic we discuss is that of direct products. We first distinguish between external and internal direct products, and end with the fundamental theorem of finite abelian groups. Note that we are now allowing groups to be infinite unless otherwise specified.

NOTE: Professor Isaacs uses a direct product notation in class which is a product symbol with a dot inside the product symbol to denote “internal direct product”. I cannot for the life of me figure out how to make that symbol in LaTeX. I therefore just write out the phrase “internal direct product” or insert

clauses like, “where this product is direct”. The notation is really clumsy and for that I apologize.

Definition 9.1. Suppose that G_1, G_2, \dots, G_r are groups, and let $P = \{(x_1, x_2, \dots, x_r) | x_i \in G_i\}$. We can make P into a group by defining $(x_1, x_2, \dots, x_r) \cdot (y_1, y_2, \dots, y_r) = (x_1y_1, x_2y_2, \dots, x_ry_r)$. When we do this, we say that P is the *external direct product* of the groups G_i , and we write $P = G_1 \times G_2 \times \dots \times G_r$.

Notationally, we may wish to refer to the subgroups of this direct product which are isomorphic to the original groups G_i . We write $\widetilde{G}_i \subseteq P = \{(1, 1, \dots, \underbrace{x}_{\text{pos. } i}, 1, \dots, 1) | x \in G_i\}$.

Note that every element of \widetilde{G}_i commutes with every element of \widetilde{G}_j if $i \neq j$. Additionally, each $\widetilde{G}_i \triangleleft P$ since every group is normal within itself, so $\widetilde{G}_i \subseteq \mathbf{N}_P(\widetilde{G}_i)$ and all other \widetilde{G}_j commute with \widetilde{G}_i so they certainly normalize \widetilde{G}_i ; hence $\widetilde{G}_j \subseteq \mathbf{N}_P(\widetilde{G}_i)$ for all $i \neq j$. So $P = G_1 \times G_2 \times \dots \times G_r$ is contained in the normalizer of \widetilde{G}_i .

Definition 9.2. Given a group G , assume $N_i \triangleleft G$ for $1 \leq i \leq r$. Suppose that $G = \prod_{i=1}^r N_i$. Also, assume that every element $g \in G$ is uniquely of the form $g = t_1 \dots t_r$ with $t_i \in N_i$. Then G is the *internal direct product* of the subgroups N_i .

We sometimes wish to write explicitly that we are considering an internal direct product. We signify this by placing a dot over the times symbol, like so: $\dot{\times}$. We state without proof one lemma relating external and internal direct products.

Lemma 9.1. If P is the external direct product $P = G_1 \times G_2 \times \dots \times G_r$ then P is the internal direct product of the subgroups \widetilde{G}_i .

A theorem we will state with proof is the following:

Theorem 9.1. If G is the internal direct product of subgroups N_i for $1 \leq i \leq r$, then G is isomorphic to the external direct product of the N_i .

Proof. As we have done with other proofs, we first prove a useful lemma.

Lemma 9.2. Assume that G is the internal direct product of the N_i for $1 \leq i \leq r$. Then $N_i \cap \prod_{i \neq j} N_j = 1$.

Proof. Let $g \in N_i \cap \prod_{i \neq j} N_j$. Then we may write $g = t_1 t_2 \dots t_r$ where $t_i = g$ and $t_j = 1$ for all $j \neq i$, as $g \in N_i$. Also, as $g \in \prod_{j \neq i} N_j$, we may write $g = s_1 s_2 \dots s_r$ where $s_k \in N_k$ for all k and $s_i = 1$. By the “directness” of the product, we have that $s_k = t_k$ for all k , so $g = t_i = s_i = 1$. \square

We draw as a corollary the following important fact.

Corollary 9.1. If G is the internal direct product of N_i for $1 \leq i \leq r$ then $N_i \cap N_j = 1$ for $i \neq j$ and so the elements of N_i commute with the elements of N_j .

We now proceed with the proof of the theorem.

We wish to exhibit an isomorphism θ from the external direct product of the N_i to G . Let $\theta(n_1, n_2, \dots, n_r) = n_1 n_2 \dots n_r$, which is in G . Note that θ is surjective as G is the internal direct product of the N_i . Also, θ is injective by the uniqueness assumption of the internal direct product. So we must show that θ is in fact a homomorphism. So:

$$\theta((x_1, x_2, \dots, x_r) \cdot (y_1, y_2, \dots, y_r)) = \theta(x_1 y_1, x_2 y_2, \dots, x_r y_r) = x_1 y_1 x_2 y_2 \dots x_r y_r$$

Yet $x_1 y_1 x_2 y_2 \dots x_r y_r = x_1 x_2 \dots x_r y_1 y_2 \dots y_r$ as each y_i commutes with all x_j such that $i \neq j$. This is $\theta(x_1, x_2, \dots, x_r) \theta(y_1, y_2, \dots, y_r)$, so we see that θ is a homomorphism. □

Before getting to the fundamental theorem of finite abelian groups, we prove a few more useful results involving direct product.

Theorem 9.2. Suppose that $G = \prod_{i=1}^r N_i$ where each N_i is normal in G . Then G is actually the internal direct product of the N_i if $N_1 N_2 \dots N_k \cap N_{k+1}$ is always trivial for all $1 \leq k < r$. Note that it is NOT enough for the N_i to intersect trivially pairwise.

Proof. We must show that if $x_1 x_2 \dots x_r = y_1 y_2 \dots y_r$, then $x_i = y_i$ for all i . So assume that it is false, and choose k minimal such that $x_k \neq y_k$. Then $x_1 x_2 \dots x_k = y_1 y_2 \dots y_k$, so moving things around yields:

$$x_k y_k^{-1} = x_{k-1}^{-1} x_{k-2}^{-1} \dots x_1^{-1} y_1 y_2 \dots y_{k-1}$$

where the result, $x_k y_k^{-1}$ lies in N_k as $x_k, y_k \in N_k$. However, due to the right hand side of the equation above, the result is also in $N_1 N_2 \dots N_{k-1}$. By our hypothesis, we see that we must then have that $x_k y_k^{-1} = 1$, and hence $x_k = y_k$. Yet this is a contradiction to the fact that k is our minimal criminal, so we must have $x_k = y_k$ for all $1 \leq i \leq r$. □

Corollary 9.2. Let G be finite and nilpotent and let p_1, p_2, \dots, p_r be the distinct prime divisors of $|G|$. Let P_i be the unique element of the set of Sylow p_i -subgroups. Then G is the internal direct product of the P_i .

Proof. As G is nilpotent, we have that each $P_i \triangleleft G$. Let $H = \prod_{i=1}^r P_i$. H is a subgroup of G as each $P_i \triangleleft G$. Since $P_i \subseteq H$ for all i , it follows that p_i does

not divide $|G : H|$ for any i . So $|G : H| = 1$ and thus $H = G$. We must next look at $\left(\prod_{i=1}^{k-1} P_i\right) \cap P_k$. Now the order of $\prod_{i=1}^{k-1} P_i$ involves only the primes p_i for $1 \leq i \leq k-1$, and $|P_k|$ involves only the prime p_k , which is by assumption distinct from each p_i where $1 \leq i \leq k-1$. Hence the orders of these subgroups are coprime, and the only element of their intersection is thus the identity. \square

We have as our next lemma, a sort of converse to the previous corollary. As a result of the next lemma, we can conclude that nilpotent groups are exactly the groups constructed as the external direct product of p -groups.

Lemma 9.3. Let G be an external direct product $Q_1 \times Q_2 \times \dots \times Q_r$ where each Q_i is a p -group for some prime p . Then G is nilpotent.

Proof. As G is the external direct product of the Q_i , we know that G is actually equal to the internal direct product of the \widetilde{Q}_i , and that each of the $\widetilde{Q}_i \triangleleft G$ by lemma 9.1. Also, we know that $\widetilde{Q}_i \cong Q_i$, so each \widetilde{Q}_i is nilpotent. From our homework, we know that $\mathbf{F}(G)$, the Fitting subgroup, is the (unique) largest nilpotent subgroup of any group G . Thus $G = \prod_{i=1}^r \widetilde{Q}_i \subseteq \mathbf{F}(G)$, so $G = \mathbf{F}(G)$. Yet $\mathbf{F}(G)$ is nilpotent, so G must also be nilpotent. \square

We now get to the apex of this section: the Fundamental Theorem of Finite Abelian Groups.

Theorem 9.3. Let G be finite and abelian. Then there exist cyclic p -subgroups C_i such that G is equal to the internal direct product of the C_i .

Proof. The proof of this theorem is rather involved, so as we have done before, we first prove a few lemmas before finishing the proof of the theorem.

Lemma 9.4. Suppose that $G = \prod_{i=1}^r N_i$, where this product is direct, and that $N_i = \prod_{j=1}^{m_i} M_{ij}$, where this product is direct. Then $G = \prod M_{ij}$, where this product is direct.

Note that if we assume the result of the lemma, we are well on our way to having the proof of our theorem. That is, G being abelian implies that G is nilpotent, so we may write $G = \prod_{i=1}^n P_i$ where the P_i are Sylow. So it suffices to show that an abelian p -group is a direct product of cyclic subgroups. To obtain this result, we need another lemma.

Lemma 9.5. Let P be a finite abelian p -group. Let $C \subseteq P$ be cyclic of maximum possible order. Then $P = C \times B$ for some subgroup $B \subseteq P$, where this product is direct.

Proof. Since we may take $B = 1$ and $C = P$, we may assume that $C < P$ and we choose $x \in P \setminus C$ of smallest possible order. Since $x \neq 1$, we see that $o(x^p) < o(x)$ and therefore $x^p \in C$. If x^p generates C , then $|\langle x \rangle| = p|C|$, which contradicts our choice of C . Thus x^p is a nongenerator of the cyclic group p -group C . It follows that x^p is a p th power in C , so we may write $x^p = y^p$ for some $y \in C$. Now $xy^{-1} \notin C$ and $(xy^{-1})^p = x^p(y^p)^{-1} = 1$. By the choice of x , we have that $o(x) \leq o(xy^{-1}) = p$, so $o(x) = p$.

Now let $X = \langle x \rangle$, and we use overbars to denote the canonical homomorphism from $G \rightarrow G/X$; that is, $\overline{G/X} = \overline{G}$. Since $|X| = p$, we have that $C \cap X = 1$, and our bar maps C to \overline{C} in a 1-1 fashion. Thus \overline{C} is cyclic with order equal to $|C|$. If \overline{G} has a cyclic subgroup $\langle \overline{g} \rangle$ with order larger than \overline{C} , then:

$$|\langle g \rangle| = o(g) \geq o(\overline{g}) = |\langle \overline{g} \rangle| > |\overline{C}| = |C|$$

and this contradicts our choice of C . It therefore follows that \overline{C} is a cyclic subgroup of \overline{G} with maximal possible order. Since $|\overline{G}| < |G|$, we may work via induction on $|G|$ and conclude that \overline{C} is a direct factor of \overline{G} . Since every subgroup of \overline{G} has the form \overline{B} for some $X \subseteq B \subseteq G$, we have find a B such that $X \subseteq B$ and where $\overline{G} = \overline{C} \dot{\times} \overline{B}$. Thus $\overline{G} = \overline{CB} = \overline{BC}$ (as the bar map is a homomorphism) and hence $CB = G$. Also, $\overline{C} \cap \overline{B} = 1$ by the directness of the product so $C \cap B \subseteq X$. Yet $C \cap B \subseteq C \cap X = 1$, and this proves that the product $G = C \times B$ is actually a direct product. \square

Although slightly wishy washy, this proof, shows that abelian p -groups may always be expressed as a direct product. Combined with the first lemma we stated in this proof, we know that we are allowed to piece together direct products of direct products, and this finishes the proof. \square

10 X groups

The section we are beginning is Marty Isaacs' way of introducing modules to one who is not familiar with modules. This section is not particularly important to the rest of group theory, but is an interesting introduction to ring and module theory. Throughout this section, although I will try to be precise, if I ever type just simple or just subgroup, I most likely mean X -simple or X -subgroup. It is sloppy notation not to include it, yet sometimes Isaacs gets lazy and I've forgotten to correct it.

Suppose that X is any set (yes, X can be the empty set) and that G is a group. Suppose that for all $x \in X$, we have a map $G \rightarrow G$ via $g \mapsto g^x$. We want this to be a group homomorphism. If this is the case, then we say that G is an X -group. If $H \subseteq G$ is a subgroup, then it is an X -subgroup if for every $h \in H$, $h^x \in H$ for all $x \in X$.

It is, in fact, an important case when $X = \emptyset$. In this case, we may think of the action as being vacuous, and in this case, any conclusion we draw is simple a result in group theory. That is, any old group is an X -group when X is

the empty set. Another important example is when X is the group itself and the action is conjugation. Then all X -subgroups are normal subgroups of the original group.

Definition 10.1. An X -group G is X -simple if it is not the identity and the only X -normal subgroups are 1 and G .

Note that this definition seems a little tricky at first. First of all, a group could have a proper normal subgroup which does not form an X -subgroup and still be X -simple. Likewise, it could have many X -subgroups so long as they are not normal. Don't worry too much about it. This section isn't very important. However, we will be doing the Jordan-Holder theorem in terms of X -groups, so it cannot be entirely ignored.

Definition 10.2. An X -isomorphism, say θ , from $G \rightarrow H$ satisfies $\theta(g^x) = \theta(g)^x$ where θ is a bijection. Similarly, $\theta : G \rightarrow H$ is an X -homomorphism if $\theta(g^x) = \theta(g)^x$.

Note that all correspondence theorems still hold when dealing with X -groups. We simply repeat each proof checking all along that θ is an X -homomorphism, etc. One can therefore conclude, for example, that if θ is an X -homomorphism, then $\ker(\theta)$ is an X -normal subgroup.

In this section, and when we move on to rings, we no longer assume that all of the groups that we are dealing with are finite. We will, however, be searching for some sorts of conditions which make the rings "not too badly infinite". With that in mind, we introduce another familiar notion for X -groups.

Definition 10.3. Given an X -group G , let $1 = N_0 \triangleleft N_1 \triangleleft N_2 \triangleleft \dots \triangleleft N_r = G$ where N_i are X -subgroups and N_{i+1}/N_i is X -simple for $0 \leq i < r$. Then the N_i form an X -composition series for G .

We note that if G is an infinite group, having an X -composition is one such finiteness condition which states that the group is not too badly infinite.

We now prove our first main theorem about X -groups, in order to become familiar with them. This is also quite an important result which is useful for Jordan-Holder like problems.

Theorem 10.1. Let G be an X -group and suppose that G has an X -composition series. Let $M \triangleleft G$ be an X -subgroup. Then there exists an X -composition series for G that runs through M .

Proof. Let $1 = N_0 \triangleleft N_1 \triangleleft \dots \triangleleft N_r = G$ be a composition series for G , and consider \mathcal{S} be the series $1 = M \cap N_0 \subseteq M \cap N_1 \subseteq \dots \subseteq M \cap N_r = M = MN_0 \subseteq MN_1 \subseteq \dots \subseteq MN_r = G$. Look at two consecutive terms of \mathcal{S} ; say $M \cap N_i \subseteq M \cap N_{i+1}$. Let $U = N_i(M \cap N_{i+1})$. This is a very diamond lemma type argument, so I will again leave a blank space for a picture.

Since $M \triangleleft G$, we have that $M \cap N_{i+1} \triangleleft N_{i+1}$. Thus we have by the diamond lemma that $U \triangleleft N_{i+1}$. Likewise, $M \cap N_i \triangleleft N_{i+1}$ as it is the intersection of two normal subgroups of G . By the way the N_j are nested, we then find that $M \cap N_i \triangleleft M \cap N_{i+1}$. Since N_{i+1}/N_i is X -simple, there are only two possibilities for U ; either $U = N_{i+1}$ or $U = N_i$.

If $U = N_i$, then $M \cap N_i = M \cap N_{i+1}$. (In this case, we delete one of the two groups within \mathcal{S}). If $U = N_{i+1}$, we then have:

$$\frac{M \cap N_{i+1}}{M \cap N_i} \cong \frac{U}{M \cap N_i} = \frac{N_{i+1}}{N_i}$$

which is X -simple by hypothesis.

In either case, we find that when we consider two consecutive terms of \mathcal{S} of the form $M \cap N_i$ and $M \cap N_{i+1}$ our composition series remains in tact. So now suppose that we examine two consecutive terms of \mathcal{S} of the form MN_i and MN_{i+1} . We again leave a space for a picture, which is useful:

First, we see that $MN_i \triangleleft MN_{i+1}$ since both $M, N_{i+1} \subseteq \mathbf{N}_G(MN_i)$. So let $V = MN_i \cap N_{i+1}$. Now $V \triangleleft N_{i+1}$ as it is the intersection of X -normal subgroups. Again by the X -simplicity of the factor groups, we have that either $V = N_i$ or $V = N_{i+1}$. Via an identical argument to the intersection case, we find that $\frac{MN_{i+1}}{MN_i} \cong \frac{V}{N_i}$, and either we have that the factor group is trivial or simple. By deleting all trivial factor groups, we obtain an X -composition series which contains $M = M \cap N_r$ as one of its terms. \square

We now state and prove the all important Jordan-Hölder theorem.

Theorem(Jordan-Hölder) 10.2. Let $1 = N_- \triangleleft N_1 \triangleleft \dots \triangleleft N_r = G$ and $1 = M_0 \triangleleft M_1 \triangleleft \dots \triangleleft M_s = G$ be X -composition series for some X -group G . Then $r = s$ and the X -groups N_i/N_{i-1} and M_j/M_{j-1} are X -isomorphic in some order.

Proof. We choose to induct on r . If $r = 0$, then $G = 1$ (the only composition series of length one are trivial; they otherwise have at least two, G and 1.) and if $G = 1$ we must have $s = 1$. We may therefore assume that $r > 0$ and that $r \leq s$. If $N_{r-1} = M_{s-1}$, the inductive hypothesis applies in the groups $N_{r-1} = M_{s-1}$ and the following composition series (we shall call them R_0 and S_0 , respectively). Hence $r-1 = s-1$ and therefore $r = s$. Also by our inductive hypothesis then $R_0 \cong S_0$. But the factors of R , the composition series including the factors of the N_i are all those of R_0 along with G/N_{r-1} . While the factors of S , the composition series including factors of M_i are all those factors of S_0 along with G/M_{s-1} . Therefore by assumption we must have $(G/N_{r-1}) \cong (G/M_{s-1})$, and we are finished.

We therefore assume that $N_{r-1} \neq M_{s-1}$. Then we must have that $N_{r-1}M_{s-1} = G$ as both of the factor groups G/N_{r-1} and G/M_{s-1} are X -simple and $N_{r-1}M_{s-1} \triangleleft G$. Say $D = N_{r-1} \cap M_{s-1}$. Note that $D \triangleleft G$ by the diamond lemma. Let T be a composition series for D , and note that such a series exists as $D \triangleleft G$, G has a composition series, and by the previous theorem. We may gain a new composition series for N_{r-1} by appending the factor group N_{r-1}/D to the composition series T . In order to ensure that this actually is an X -composition series, we must know that N_{r-1}/D is X -simple, which is true again by the diamond lemma. Similarly, we may gain a new composition series for M_{s-1} in a similar fashion, by appending M_{s-1}/D to T . We shall call these new composition series T_r and T_s , respectively. Now our inductive hypothesis applied to R_0 and T_r tells us that $R_0 \equiv T_r$, so the length of $T_r = r - 1$. Likewise, the length of $T_s = 1 +$ the length of $T =$ length of $T_r = r - 1$. We again use the inductive hypothesis to conclude that $T_s \equiv S_0$; we may therefore conclude that $s - 1 = r - 1$ and therefore that $s = r$. Let cf denote the multi-set of composition factors. Then we have that:

$$\begin{aligned}
cf(R) &= cf(R_0) \cup \{G/N_{r-1}\} \\
&= cf(T_r) \cup \{G/N_{r-1}\} \\
&= cf(T) \cup \{N_{r-1}/D\} \cup \{G/N_{r-1}\} \\
&= cf(T) \cup \{G/M_{s-1}\} \cup \{G/N_{r-1}\} \\
&= cf(S_0) \cup \{G/M_{s-1}\} \\
&= cf(S)
\end{aligned}$$

Although this finishes the proof, it is a good exercise to write next to each equality why it holds. I will do that when I print a copy of these notes. Also, I have many pictures drawn in my notes that aid tremendously in the clarity of this proof, so I will again leave a space for these pictures to be inserted. \square

Having established that the length of a composition series is well defined, we introduce a bit of notation. For an X -group G having an X -composition series, we write $l(G)$ to denote the composition length.

NOTE: If we assume that $N \triangleleft G$, where G is an X -group and N is a normal X -subgroup, and we assume further that G has an X -composition series, we then find that $l(G) = l(N) + l(G/N)$. This is analogous to the fact that $|G| = |N| \cdot |G/N|$ for finite groups.

10.1 Partially Ordered Sets

As we transition into ring theory, we will be in search of a few more finiteness conditions to inflict upon our rings. Although there is plenty to keep one interested in finite groups, finite rings are fairly boring. This is essentially because a ring has such a forced structure to begin with, forcing the ring to be finite eliminates a lot of interesting behavior. Once we are in ring theory, we most often assume that our rings are infinite, but inflict some sort of “Not too badly infinite” condition upon them. This section will lead us to discover these finiteness conditions, only we introduce them in a far more general context.

In this context, we will be considering partially ordered sets, (sometimes cutely referred to as posets). Along with these posets, we have a binary relation \leq for which we may *sometimes* write $x \leq y$ for $x, y \in P$, where P is of course our poset.

We inflict upon the less than relation three necessary axioms:

1. $x \leq x$ for all $x \in P$ (reflexive)
2. If $x \leq y$ and $y \leq z$ then $x \leq z$ (transitive)
3. If $x \leq y$ and $y \leq x$ then $x = y$ (antisymmetric)

If we also have (4), that if whenever $x, y \in P$ we have either $x \leq y$ or $y \leq x$, then we call our poset P a *totally ordered set*.

We can think of many examples of posets which are totally ordered, like the integers, real numbers, or the alphabet ordered lexicographically. For an example of a poset which is NOT totally ordered, and one poset we will be very interested in, we turn to the set of all subsets of a group (or any arbitrary set for that matter).

Definition 10.1.1. An *ascending chain* in a poset P is a list of elements $x_i \in P$ subscripted by the natural numbers and such that $x_1 \leq x_2 \leq \dots$. Similarly, a *descending chain* in P is such that $x_1 \geq x_2 \geq \dots$.

Definition 10.1.2. The *ascending chain condition*, denoted ACC, on P states that if $x_1 \leq x_2 \leq \dots$ is an ascending chain, then there exists a natural number r such that $x_r = x_s$ for all $s \geq r$. Similarly, we may define the *descending chain condition*, or DCC.

We give a familiar example to explore these new definitions.

Example 10.1.1. If $P = \{1/n | n \in \mathbb{N}\}$, and we consider the natural order, then P does not satisfy the DCC but P does satisfy the ACC.

As Marty Isaacs likes to point out, these two conditions seem very similar considering that their definitions are like mirrors. However, it is quite interesting to discover that one cannot draw mirrored conclusions about rings which satisfy the ACC and the DCC. Rings which satisfy the ACC often turn out to have very different properties than rings which satisfy the DCC. I hope to include an example of this in future notes or at least point out when a similar or analogous result does not hold for the other condition.

Definition 10.1.3. A poset P satisfies the *maximal condition* if every non-empty subset X of P has a maximal element. Similarly, a poset P satisfies the *minimal condition* if every non-empty subset X of P has a minimal element.

Although we introduce these new definitions, the next theorem we proves deems them unnecessary as new definitions.

Theorem 10.1.1. Let P be a poset. Then P satisfies the ACC if and only if P satisfies the maximal condition. Similarly, P satisfies the DCC if and only if it satisfies the minimal condition.

Proof. Assume that P satisfies the ACC. Let X be a non-empty subset of P . Assume that X has no maximal element. Let $x_1 \in X$. Choose $x_2 \in X$ such that $x_1 < x_2$. Now choose $x_3 \in X$ such that $x_2 < x_3$, and so on. This is an ascending chain, which has no maximal element as X does not satisfy the maximal condition. This contradicts the ACC, so we must have that X satisfies the maximal condition. Now suppose that P satisfies the maximal condition. Let $x_1 \leq x_2 \leq \dots$ be an ascending chain. Let $X = \{x_i | i \geq 1\}$. X is certainly non-empty. Let $m \in X$ be a maximal element, say $m = x_r$ for some r . Let $s \geq r$. Then $m = x_r \leq x_s$ so $x_s = m$ since x_s is not bigger than m . So $x_s = m = x_r$. Essentially, what this says is that every ascending chain forms a non-empty subset of the poset, and therefore eventually stabilizes. The proof for the equivalence of the DCC to the minimal condition is equivalent. \square

Although these two definitions have now been shown to be the same, it is nice to know that when we know one thing, we automatically have the other. We find in proofs that it is often easier to prove that something has the ACC, but more powerful to assume the maximal condition. Examples of this will follow in our work with rings.

Finally, we work towards ring theory.

Definition 10.1.4. Let M be an abelian X -group. We say that M is *noetherian* if the poset of X -subgroups of M satisfies the ACC. Similarly, an abelian X -group M is *artinian* if the posets satisfy the DCC.

As the concepts of noetherian and artinian rings will be quite important in our study of ring theory, we discover some more facts about these rings in the more general context of X -groups. We begin this discovery with a little lemma.

Lemma 10.1.1. Let M be an abelian X -group and $N \subseteq M$ an X -subgroup. Then M is noetherian if and only if both N and M/N are noetherian.

Proof. First, assume that M is noetherian. Then N is noetherian as any ascending chain in N is an ascending chain in M . Likewise, M/N is noetherian by the correspondence theorem.

Now assume that both N and M/N are noetherian. Let $U_1 \subseteq U_2 \subseteq \dots$ be an ascending chain of X -subgroups in M . Then $U_1 \cap N \subseteq U_2 \cap N \subseteq \dots$ is an ascending chain in N , and therefore there exists r such that $U_r \cap N = U_s \cap N$ for all $s \geq r$. Similarly, $(U_1 N)/N \subseteq (U_2 N)/N \subseteq \dots$ is an ascending

chain in M/N . Therefore there exists t such that $(U_t N)/N = (U_s N)/N$ for all $s \geq t$. Let $m = \max\{r, t\}$. Then if $s \geq m$, we have that $U_m \cap N = U_s \cap M$ and $(U_m N)/N = (U_s N)/N$. Hence $U_s N = U_m N$. As $s \geq m$, we know that $U_m \subseteq U_s$. Yet $U_s \subseteq NU_s = NU_m$. Therefore Dedekind's lemma applies, and we have that $U_s = U_m(N \cap U_s) = U_m(N \cap U_m) = U_m$. \square

A few notes on the above proof: first, Dedekind's lemma is a useful lemma which we proved on a homework assignment. I will state it formally below, and leave its proof as an exercise. Also, it is worth mentioning that an analogous statement to that of the previous lemma is also true for abelian X -groups which are artinian. Here is the formal statement of Dedekind's lemma:

Lemma(Dedekind) 10.1.2. Let U, V , and W be subgroups of a group G , and assume that $U \subseteq W$. Then $W \cap UV = U(W \cap V)$.

Proof. Exercise. \square

Theorem 10.1.2. Let M be an abelian X -group. Then M has an X -composition series if and only if M is both noetherian and artinian.

Proof. First, assume that M has a composition series. We induct on $l(M)$, the composition length, to show both artinian and noetherian. If $l(M) = 0$, then M is the trivial group, so M is both noetherian and artinian trivially.

Now assume that $l(M) > 0$. Let N be penultimate (next to last) in the X -composition series for M . Then M/N is X -simple, so it is both artinian and noetherian (its poset of X -subgroups is finite: it is a set of size 2). But $l(N) = l(M) - 1$ so our induction hypothesis applies and we see that N is both noetherian and artinian. Now our previous lemma applies, and we see that as N and M/N are both noetherian and artinian, and therefore M is noetherian and artinian as well.

For the converse, assume that M is both noetherian and artinian. Let $\mathcal{X} = \{U \subseteq M \mid U \text{ has a composition series}\}$. Note that $\mathcal{X} \neq \emptyset$ as the trivial group has a composition series. By the maximal condition, there exists $N \in \mathcal{X}$ such that N is maximal with this property. We wish to show that $N = M$. To see this, we suppose that it is not true, and let $\mathcal{Y} = \{V \subseteq M \mid N < V\}$. Our hypothesis ensures that $M \in \mathcal{Y}$, so we know that \mathcal{Y} is not empty. By the minimal condition, we see that \mathcal{Y} has a minimal element, say K . By the minimality of K , K/N is X -simple. Yet then $K > N$ and K has an X -composition series, which contradicts the maximality of N . Therefore \mathcal{Y} must be empty, and we have that $N = M$. \square

The preceding proof is an excellent example of how one uses the maximal/minimal condition. It is quite canonical, in that sense. The next proof we do will demonstrate a claim that I made earlier; the claim that being noetherian and artinian are quite different notions. Although for lemma 10.1.1 we did find an analogous result for abelian X -groups which are artinian, no such analogous result holds for the next theorem.

Theorem 10.1.3. Let M be an abelian X -group. Then M is noetherian if and only if every subgroup of M is finitely generated.

Proof. Assume that all X -subgroups of M are finitely generated. We wish to show that M is noetherian. Let $N_1 \subseteq N_2 \subseteq \dots$ be an ascending chain in M . Let $N = \bigcup_{i=1}^{\infty} N_i$. Normally, N would not be a subgroup of M , but as the N_i are nested, it follows that $N \subseteq M$ is an X -subgroup. Therefore N is finitely generated. Let F represent the finite set of generators for N . Then $\langle F \rangle = N$. Given $t \in F$, there exists i_t such that N_{i_t} such that $t \in N_{i_t}$. Let $m = \max\{i_t | t \in F\}$. Then for all $t \in F$, we have that $t \in N_m$. Yet this implies that $N \subseteq N_m$. Thus $N = N_m$ and for all $s \geq m$, we find that $N_s = N_m$.

Now assume that M is noetherian, and let $\mathcal{X} = \{U \subseteq M | U \text{ is finitely generated}\}$. Note that $\mathcal{X} \neq \emptyset$ as the trivial subgroup is finitely generated. So let $V \in \mathcal{X}$ be maximal with this property. We want that $V = M$. So suppose not. Then there exists $m \in M \setminus V$. Yet if we now consider $W = \langle V, m \rangle$, we see that W is finitely generated, and yet $W > V$. This is a contradiction, so we must have that $V = M$, as desired. \square

11 Rings

We finally move from X -groups into ring theory.

Definition 11.1. Let R be an additive abelian group with multiplication such that:

1. $(rs)t = r(st)$ for all $r, s, t \in R$
2. $(r + s)t = rt + st$ for all $r, s, t \in R$
3. $t(r + s) = tr + ts$ for all $r, s, t \in R$
4. $1 \in R$; that is, R has a multiplicative identity. We say 1 is the *unity* of R .

Then R is a *ring*.

We note that some textbooks do not require (4), that a ring have unity, in which case many different behaviors occur. We now present many examples of rings:

Example 11.1. We take addition and multiplication to be standard, unless otherwise noted.

- \mathbb{Z} , the ring of integers.
- The integers modulo n form a ring, and we denote it $\mathbb{Z}/n\mathbb{Z}$.
- An object which will be of future interest in second semester, polynomial rings. If \mathbb{F} is a field, $\mathbb{F}[X]$, the collection of polynomials with coefficients in \mathbb{F} .

- The ring of $n \times n$ matrices.
- For a less standard example, the ring of all real-valued functions of a single variable under pointwise addition and multiplication.

Definition 11.2. A *right R -module* is an abelian additive group M together with an “action” of the ring R on M such that if $m \in M$ and $r \in R$, then $mr \in M$.

With modules, there are a few axioms that we may assume:

1. For $m \in M$ and $r, s \in R$, we have $((m)r)s = m(rs)$.
2. For $m \in M$ and $r, s \in R$, we have $m(r + s) = mr + ms$.
3. For $m, n \in M$ and $r \in R$, we have $(m + n)r = mr + nr$.
4. $m1 = m$ for all $m \in M$.

We note that although properties two and three look similar, (3) says that action by $r \in R$ is an *endomorphism* of M , so M is an R -group. Property two simply states that modules uphold the distributive property.

We also note that given a right R -module M , we may naively try to make it a left R -module by defining $rm = mr$. Yet this only actually works if our multiplication is commutative, so we should not be fooled.

Let M be a right R -module. Then $N \subseteq M$ is a *submodule* if N is an additive subgroup of M and for $n \in N$ and for all $r \in R$, we have that $nr \in N$.

We continue with our definitions.

Definition 11.3. Suppose that U, V are right R -modules and $\varphi : U \rightarrow V$ is an additive homomorphism. Then φ is an *R -module homomorphism* if $(ur)\varphi = (u\varphi)r$ for all $u \in U$ and $r \in R$. For left R -modules (undefined, but defined analogously) the condition is such that $\varphi(ur) = \varphi(u)r$.

We here introduce a bit of tricky notation. Let R be a ring. Denote by $R^\bullet = R$ as an additive group. That is R^\bullet is the ring in question, but here we are thinking of it only as a group instead of the ring. Another way to view this is that R^\bullet is the ring R written as a module. Similarly, although essentially unused, we write $\bullet R$ to denote the ring R thought of as a left R -module.

We will momentarily introduce the notion of an ideal of a ring R , but we note here that the submodules of R^\bullet are the right ideals of R , and the submodules of $\bullet R$ are the left ideals of R .

Definition 11.4. I is an *ideal* of R if it is both a right ideal and a left ideal.

One example of ideals of R are as follows. Let $a \in R$. Then aR is a right ideal of R and Ra is a left ideal of R .

It is a little tricky, when we discussed cosets, we had right and left referring to where the fixed element was. In ring theory, it is a whole new world, so we

have left and right referring to where the multiplication by the ring element is taking place.

Not to be confused with a R -module homomorphism, we now introduce the notion of a ring homomorphism.

Definition 11.5. If R, S are rings and $\theta : R \rightarrow S$ is such that $\theta(x + y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in R$, then θ is a *ring homomorphism*.

We also require with the above definition that $\theta(1) = 1$, which again, other textbooks do not always require.

Just as with group homomorphisms, we are interested in the kernel of ring homomorphisms, and what information they give us about the ring. Here, $\ker(\theta) = \{r \in R \mid \theta(r) = 0\}$. The information that we gain about the ring is that $\ker(\theta)$ is an ideal.

If $I \subseteq R$ is an ideal, then we define R/I to be the set $\{I + x \mid x \in R\}$. Then R/I is an additive group, and multiplication on R/I is defined by $(I + x)(I + y) = I + xy$. The additive identity of $R/I = I$, so I is the zero of the factor ring, and $I + 1$ is the 1 of the factor ring.

We comment on a few things before narrowing our focus. First of all, as with groups where you cannot mod out by arbitrary subgroups, a similar restriction holds with rings. One cannot mod out by a right ideal or a left ideal, only by an ideal (one which is both left and right). Furthermore, this notation is reminiscent of coset notation, and cosets were slippery beasts with many names. So you must check that this definition is well defined. This computation is straightforward, and is left as an exercise.

11.1 Simple Right Modules

We now shift our focus to studying rings from the point of view of their simple right modules.

Definition 11.1.1. Let R be a ring and M be a right R -module. If $m \in M$, the *annihilator of m* , written $\text{ann}(m)$, is equal to the set $\{r \in R \mid mr = 0\}$, and $\text{ann}(M) = \{r \in R \mid Mr = 0\}$.

We now prove our first lemma to do with rings.

Lemma 11.1.1. Let M be a right R -module, and let $m \in M$.

1. The map $\theta : r \rightarrow mr$ is a module homomorphism from R^\bullet into M .
2. $\ker(\theta) = \text{ann}(m)$ is a right ideal.
3. $R^\bullet / \text{ann}(m) \cong mR$.

Proof. To see that θ is a module homomorphism, we check that it distributes additively and that $(rs)\theta = (r\theta)s$. To see that $\theta(r + s) = \theta(r) + \theta(s)$, we see that $\theta(r + s) = m(r + s) = mr + ms = \theta(r) + \theta(s)$, where the third equality holds by axiom two for modules. To see that $(rs)\theta = (r\theta)s$, we see that $(rs)\theta = m(rs) = (mr)s$ by axiom (1) for modules, and this is $(r\theta)s$.

For (2), we compute $\ker(\theta)$, which is by definition $\{r \in R^\bullet \mid mr = 0\}$, which is $\text{ann}(m)$ by definition. As θ is a module homomorphism, we see that $\ker(\theta)$ is a submodule of R^\bullet and is therefore a right ideal of R .

We know by one of our homomorphism theorems that and ring mod its kernel is isomorphic to the image, so $R^\bullet / \ker(\theta) \cong \theta(R^\bullet)$. Yet $\theta(R^\bullet) = mR^\bullet = mR$. \square

We now introduce the concepts of artinian and noetherian to rings.

Definition 11.1.2. We say that a ring R is *right artinian* if the module R^\bullet is artinian, i.e., the set of right ideals of R satisfies the DCC.

We note that in order for an ideal of R to be proper, it cannot contain the identity; that is, if $I \subseteq R$ is an ideal and $1 \in I$, then $I = R$. Clearly, if $I = R$ then $1 \in R$. Likewise, if $1 \in I$ then we must have that $1r \in I$ for all $r \in R$, so $R \subseteq I$.

In group theory, we discovered that if G is a group and M is a maximal normal subgroup, then G/M was a simple group. With rings, we find that if I is a maximal ideal of R , then R^\bullet/I is a simple right R -module. This follows simply by the correspondence theorem for rings.

Lemma 11.1.2. Let S be a simple right R -module. Then, up to isomorphism, $S \cong R^\bullet/I$, where I is a maximal right ideal.

Proof. Recall from the previous lemma, that given a ring R and a right R -module M , the map $\theta : R^\bullet \rightarrow M$ via $r \mapsto mr$ is a module homomorphism, where the kernel of θ is $\text{ann}(m)$, and such that $R^\bullet/\text{ann}(m) \cong mR$. So we select $s \in S$ such that $s \neq 0$, and consider the map $\theta : R^\bullet \rightarrow S$ via $r \mapsto sr$. Then $R^\bullet/\text{ann}(s) \cong sR$, where $sR \subseteq S$ as S is a right R -module and is therefore closed under right multiplication by R . Now as sR is a right R -module contained in S and S is simple, we must either have $sR = 0$ or $sR = S$. Yet $sR \neq 0$ as $s1 = s \in sR$, and $s \neq 0$ by selection. Hence $sR = S$, and we find that $R^\bullet/\text{ann}(s) \cong S$. Thus $\text{ann}(s)$ is a maximal right ideal by the correspondence theorem. \square

We now introduce Zorn's lemma, which we use more heavily second semester, but which is often helpful in ring theory. For the purpose of this definition, we return to the more general context of posets.

Zorn's Lemma. Let \mathcal{P} be a partially ordered set. Assume that for every totally ordered subset $\mathcal{X} \subseteq \mathcal{P}$, there exists an element $b \in \mathcal{P}$ such that $x \leq b$ for all $x \in \mathcal{X}$. Then \mathcal{P} has a maximal element.

As drawing analogies to group theory helps me tremendously, I make one more before stating and proving the next lemma. Inside a group G , if we took any subgroup H of G , we knew that we could find a maximal subgroup M of G which contained H . In the context in which we used this fact, I believe our groups were always finite, in which case this fact was elementary. As with rings we are mostly concerned with infinite objects, we now prove essentially the same fact, only we need to apply Zorn's lemma to obtain the result.

Lemma 11.1.3. Let A be a proper right ideal of R . Then there exists a maximal right ideal M of R such that M contains A .

Proof. Let $\mathcal{P} = \{U \subseteq R \mid U \text{ is a proper right ideal and } A \subseteq U\}$. Note that $\mathcal{P} \neq \emptyset$ as $A \in \mathcal{P}$. Let $\mathcal{X} \subseteq \mathcal{P}$ be totally ordered and nonempty; we may make the hypothesis that \mathcal{X} be nonempty without loss as if \mathcal{X} is empty our statement is vacuously true. Let $B = \bigcup \mathcal{X}$. Normally, unions of right ideals need not be right ideals; however, B is a right ideal as the elements of \mathcal{X} are nested. Note that $X \subseteq B$ for all $X \in \mathcal{X}$ and $A \subseteq B$. As all elements of \mathcal{X} are proper right ideals, $1 \notin X$ for all $X \in \mathcal{X}$ and therefore $1 \notin \bigcup \mathcal{X} = B$. Hence B is a proper right ideal containing A , so $B \in \mathcal{P}$ and B is maximal for the elements of \mathcal{X} . We may therefore apply Zorn's lemma and deduce that \mathcal{P} has a maximal element, and the result holds. \square

The above proof is a very standard application of Zorn's lemma and is quite a good canonical example of how to apply it.

We previously introduced the notion of the annihilator of an element, $\text{ann}(m)$. We additionally introduced $\text{ann}(M) = \{r \in R \mid Mr = 0\}$. Another convenient way to view $\text{ann}(M)$ is as the intersection of all of the annihilators of the individual elements; that is, $\text{ann}(M) = \bigcap \{\text{ann}(m) \mid m \in M\}$. It is a convenient fact that $\text{ann}(M)$ is an ideal of R , not just a right ideal.

11.2 The Jacobson Radical

The final concept we present for the semester is that of the Jacobson Radical. It expands the theory of rings from the point of view of simple modules, and is in many ways analogous to the Frattini subgroup from group theory. I perhaps need to work a few examples with the Jacobson radical as this was the last section of the course and we were essentially never tested with this material.

Definition 11.2.1. We denote by $J(R)$ the *Jacobson radical*, where $J(R) = \bigcap \{\text{ann}(S) \mid S \text{ is a simple right } R\text{-module}\}$.

We note that $J(R)$ is an ideal, and that $J(R/J(R)) = 0$.

We now introduce a different way to think about the Jacobson radical.

Lemma 11.2.1. $J(R) = \bigcap \{M \subseteq R \mid M \text{ is a maximal right ideal of } R\}$.

Proof. Let $j \in J(R)$. We show that $j \in M$ for all maximal right ideals M of R . As M is a maximal right ideal of R , we know that R^\bullet/M is a simple right R -module. As $j \in J(R)$, we know that $(R^\bullet/M)j = 0$. In particular, we have that $(M+1)j = 0$, so $(M+1)j = M$, since M is the zero of the module R^\bullet/M . Yet $(M+1)j = M+j$, so $M+j = M$, so $j \in M$.

To show the other containment, let $t \in \bigcap \{M \subseteq R\}$ as M runs over all maximal right ideals of R . Let S be a simple right R -module. We wish to show that $St = 0$. Now let $s \in S$. We wish to show that $st = 0$. If $s = 0$ we are finished, so assume that $s \neq 0$. Then $\text{ann}(s)$ is a maximal right ideal by one of our previous lemmas (**SLOPPY**). Yet t is in the intersection of all maximal right ideals of R so $t \in \text{ann}(s)$, and we have $st = 0$ as desired. \square

We may gain as a corollary to this lemma the fact we stated earlier, that $J(R/J(R)) = 0$.

Corollary 11.2.1. $J(R/J(R)) = 0$

Proof. By the correspondence theorem, we know that all maximal ideals of $R/J(R)$ are of the form $M/J(R)$, where M is a maximal right ideal of R . Thus $J(R/J(R)) = \bigcap \{M/J(R) \mid M \text{ is a maximal right ideal of } R\} = 0$. \square

Although this was not done in class, I feel as if a picture is helpful for the preceding Corollary, so I leave room for one:

We now continue with a few more tricky definitions. Although not immediately clear as to what their applications are, we find that these definitions are computationally more convenient than others.

Definition 11.2.2. An element $r \in R$ is said to be *right regular* if there exists $s \in R$ such that $rs = 1$.

NOTE: Being right regular does NOT imply that an element has a multiplicative inverse. This is because we do NOT know that our multiplication is commutative, and it could be the case that $sr \neq 1$. I am attempting to find an example of this, without much luck.

Definition 11.2.3. An element $r \in R$ is *right quasiregular* if $(1 - r)$ is right regular; i.e. there exists $s \in R$ such that $(1 - r)s = 1$. We often abbreviate right quasiregular by rqr.

Here is the theorem which helps make this definitions applicable.

Theorem 11.2.1. Let $j \in J(R)$. Then j is rqr.

Proof. Consider $(1 - j)R$, which is a right ideal of R . If j is rqr, then $(1 - j)R = R$, so suppose that $(1 - j)R < R$ for contradiction. Then there exists a maximal right ideal M of R such that $(1 - j)R \subseteq M$. Also, $j \in J(R) \subseteq M$ and $1 - j \in M$. So $j + (1 - j) = 1 \in M$. Yet this contradicts the fact that M is maximal in R , so we must have $(1 - j)R = R$, and hence j is rqr. \square

Theorem 11.2.2. Let $I \subseteq R$ be a right ideal, and assume that all elements of I are rqr. Then $I \subseteq J(R)$.

Proof. It suffices to show that $I \subseteq M$ for all maximal right ideals M of R . So fix M a maximal right ideal, and assume that $I \not\subseteq M$. Then as $I + M$ is a right ideal of R , we must have that $I + M = R$ and hence we have elements $i \in I$ and $m \in M$ such that $i + m = 1$, or $(1 - i) = m$. Yet i is rqr, so there exists $r \in R$ such that $(1 - i)r = 1$. So $mr = 1$, but $mr \in M$ as M is a right ideal. Yet this implies that $1 \in M$, and M is not maximal, which is a contradiction. \square

Definition 11.2.4. An element $x \in R$ is said to be *nilpotent* if $x^n = 0$ for some $n \geq 0$.

We note quickly that if x is nilpotent in R then x is both right and left quasi-regular.

We wish to make clear now, with a technical theorem, that we have not been at a loss defining the Jacobson radical in terms of right ideals.

Theorem 11.2.3. $J(R) = J_l(R)$, where $J_l(R)$ is the left Jacobson radical.

Proof. We wish to show that $J_l(R) \subseteq J(R)$. $J_l(R)$ is an ideal and therefore $J_l(R)$ is a two sided ideal. It suffices to show that elements of $J_l(R)$ are rqr. Let $u \in J_l(R)$. We know that U is lqr, so there exists an element $x \in R$ such that $x(1 - u) = 1$. Let $y = 1 - x$. Then $x = 1 - y$, and we have that $x(1 - u) = (1 - y)(1 - u) = 1$. So $-u - y + uy = 0$, which means that $y = yu - u$. Now $u \in J_l(R)$ and $yu \in J_l(R)$ as $J_l(R)$ is a left ideal. So $yu \in J_l(R)$ and $y \in J_l(R)$ so y is lqr. So there exists $z \in R$ such that $z(1 - y) = 1$. As $x = 1 - y$, we have that $zx = 1$. Then $zx(1 - u) = 1 - u$, which implies that $z = 1 - u$ since $x(1 - u) = 1$. Since $z(1 - y) = 1$, we have that $(1 - u)x = 1$. Thus u is rqr. A symmetric argument shows that $J(R) \subseteq J_l(R)$, which completes the proof. \square

As corollaries, we discover, via identical proofs, that if $x \in J(R)$ then x is lqr and that if $I \subseteq R$ is a left ideal with all lqr elements, then $I \subseteq J(R)$.

Definition 11.2.5. Let $A \subseteq R$ be an additive subgroup. Then A is *nil* if every element of A is nilpotent.

As another immediate corollary, we may conclude that if $A \subseteq R$ is nil, then $A \subseteq J(R)$.

Definition 11.2.6. Let $A, B \subseteq R$ be additive subgroups. We then define AB to be the set of finite sums of products ab where $a \in A$ and $b \in B$.

Note that this definition is necessary as we are now inside rings, where we have two operations, and the subgroups we are dealing with are most likely infinite. Keeping this definition in mind, we introduce another definition.

Definition 11.2.7. Let $A \subseteq R$ be an additive subgroup. Then A is *nilpotent* if $A^n = 0$ for some $n \in \mathbb{N}$.

Theorem 11.2.4. Assume that R is right artinian. Then $J(R)$ is nilpotent.

Proof. Consider the sequence $J(R), J(R)^2, J(R)^3, \dots$. Note that this sequence forms a descending chain of left ideals, so as R is artinian there exists some $n \in \mathbb{N}$ such that $J(R)^n = J(R)^m$ for all $m \geq n$. Let $N = J(R)^n$, and we wish to show that $N = 0$. So assume for the sake of contradiction that it is not. Let $\mathcal{K} = \{K | KN \neq 0\}$, and note that \mathcal{K} is not empty as $N \in \mathcal{K}$. Let K be minimal in \mathcal{K} . Then $KN \neq 0$ and $KNN = KN \neq 0$. So $KN \in \mathcal{K}$. But $KN \subseteq K$ as K is a right ideal, so $KN = K$ by the minimality of K . Let $x \in K$ such that $xN \neq 0$. So $xNN = xN \neq 0$. Yet $xN \subseteq K$ and $xN = K$. But $x \in K$, so $xr = x$ for some $r \in N$. So $x - xr = 0$, which implies that $x(1 - r) = 0$, which implies that $(1 - r)y = 1$, so $0 = x(1 - r)y = x$, which is a contradiction. \square

We may draw as an immediate corollary to the previous theorem that in a right artinian ring, every nil one sided ideal is nilpotent.

Definition 11.2.8. An element $e \in R$ is *idempotent* if $e^2 = e$.

As we will see, idempotent elements are quite important in rings.

Lemma 11.2.2. Let I be a minimal right ideal in R , and assume that $I^2 \neq 0$. Then $I = eR$ for some idempotent $e \in R$.

Proof. Since $I^2 \neq 0$ we know that there exists $x \in I$ such that $xI \neq 0$. Note that xI is a right ideal, and $xI \subseteq I$. As I is minimal, we therefore have that $xI = I$. So $x = xe$ for some $e \in I$. So $xe = xe^2$, and we have that $xe - xe^2 = 0$, or $x(e - e^2) = 0$. But $e - e^2 \in I$, so $e - e^2 \in (I \cap \text{ann}(x))$. Yet $I \cap \text{ann}(x)$ is a right ideal contained in I , and it cannot be equal to I as $xI \neq 0$. Therefore $I \cap \text{ann}(x) = 0$ and $e - e^2$ is equal to zero. Hence $e^2 = e$, and e is idempotent. Now $e \in I$ and $eR \subseteq I$. We again use the minimality of I to conclude that eR is either 0 or I . If $eR = 0$, then $e = 0$, and $x = xe$ is zero, which is contrary to our selection of x, e . Thus $eR = I$, as desired. \square

We note that if $e \in R$ is idempotent, then so is $(1 - e)$. This is true as $(1 - e)(1 - e) = 1 - 2e + e^2$, which is $1 - 2e + e = 1 - e$. This fact will be useful when proving the next lemma.

Lemma(Peirce Decomposition) 11.2.3. Let $e \in R$ be idempotent and $eR \subseteq U$ where U is a right ideal. Then $U = eR + V$ where V is a right ideal.

Proof. Let $V = (1 - e)U$. Then $(1 - e)u = u - eu$ where $u \in U$ and $eu \in U$ as $e \in U$ and $u \in U$; hence $V \subseteq U$. We wish to show that $U = eR + V$; in fact, we only need to show that $U \subseteq eR + V$. So let $u \in U$. Write u as $(e + (1 - e))u = eu + (1 - e)u$. Now $eu \in eR$ and $(1 - e)u \in V$. To see that this product is direct, we must show that $eR \cap V = 0$. Let $x \in eR \cap V$. We want to show that $x = 0$. Since $x \in eR$, we have that $x = er$ for some $r \in R$. Yet $e^2 = e$ so $x = er = eer = ex$. Also, $x \in V$ so $x = (1 - e)u$ for some $u \in U$. So $x = ex = e(1 - e)u = (e - e)u = 0$. \square

We now move on to our last topic of the semester; Wedderburn-Artin theory.

11.3 Wedderburn-Artin Theory

Definition 11.3.1. We say that a ring R is a *Wedderburn ring* if R is artinian and $J(R) = 0$.

Theorem 11.3.1. Let R be a Wedderburn ring. Then every right ideal of R is a direct sum of finitely many minimal right ideals.

Proof. Assume to the contrary that the statement is false, and let U be a right ideal minimal such that it is not the direct sum of finitely many right ideals (we know that such an ideal exists as R is artinian). We know that U is not

zero as the zero ideal trivially satisfies our properties. As R is artinian, let I be a minimal right ideal contained in U (recall that minimal implies not the zero ideal). We know that $I^2 \neq 0$, or else $I \subseteq J(R) = 0$, yet $I \neq 0$. So then $I = eR$ where e is idempotent by one of our previous theorems. So we have that $eR \subseteq U$. By Peirce, we may write $U = eR + V$ where V is a right ideal. As $eR \neq 0$, we know that $V < U$, and the minimality of U implies that V may be written as a finite direct sum of minimal right ideals, say n of them. But then U is the direct sum of $n + 1$ minimal right ideals, which is a contradiction. \square

From this theorem we may now draw a few important corollaries.

Corollary 11.3.1. Let R be a Wedderburn ring. Then R is a direct sum of finitely many minimal right ideals.

Corollary 11.3.2. Let R be a Wedderburn ring. Then R is right noetherian.

Proof. Write R^\bullet as a direct sum, which we may do as all minimal right ideals of R are simple submodules; say $R^\bullet = \sum_{i=1}^r \bullet I_i$. As stated, each I_i is a simple submodule. Now $0 \subseteq I_1 \subseteq I_1 + I_2 \subseteq \dots \subseteq \sum_{i=1}^r \bullet I_i = R^\bullet$ is a composition series for R^\bullet . \square

Lemma 11.3.1. Let I be a minimal right ideal of R and let S be any simple right R -module. If $SI \neq 0$ then $S \cong I$ as right R modules.

Proof. Let $s \in S$ be such that $sI \neq 0$. We saw previously that we have a module homomorphism $\theta : I \rightarrow sI$ via $x \mapsto sx$, where the image of I is nonzero. Hence $\ker(\theta) < I$. Yet $\ker(\theta)$ is a right ideal of I , so $\ker(\theta) = 0$. So $I \cong sI \subseteq S$. Yet $sI \neq 0$ and S is a simple module, so we must have that $sI = S$. \square

Corollary 11.3.3. Let R be a Wedderburn ring. Then there exist only finitely many isomorphism types of simple right R -modules.

Proof. As R is a Wedderburn ring, we may write $R^\bullet = \sum_{i=1}^r \bullet I_i$ where I_i are minimal right ideals. Let S be a simple right R -module. We claim that $S \cong I_t$ for some $1 \leq t \leq r$. We know that $SR \neq 0$, so $SI_t \neq 0$ for some t . Then by the previous lemma, $S \cong I_t$. \square

We now prove just one of the Wedderburn-Artin Theorems.

Theorem 11.3.2. Let R be a Wedderburn ring and let S_i for $1 \leq i \leq m$ be a representative set for the simple right R -modules. Then $R = \sum_{i=1}^m \bullet U_i$ where the U_i are minimal ideals of R . Also, $S_j U_i = 0$ if $i \neq j$ and $S_i U_i \neq 0$.

Proof. Write $R^\bullet = \sum_{t=1}^k \bullet I_t$ exactly as before, where each I_t is a minimal right ideal. Now define $U_i = \sum \{I_t | I_t \cong S_i\}$. Clearly, U_i is a right ideal. Note that $S_i U_j = 0$ if $i \neq j$. To see why this holds, let I_t be one of the summands of U_j . Then by definition, $I_t \cong S_j \not\cong S_i$. Therefore by the contrapositive of our lemma, $S_i I_t = 0$. This $S_i U_i = 0$. We wish to show that U_i is an ideal, not just a right sided one. It is enough to show that $I_t U_i \subseteq U_i$ for all t . If so, then $R U_i \subseteq U_i$ and this implies that U_i is a left ideal, hence an ideal. If $I_t \not\cong S_i$, then $I_t \cong S_j$ where $j \neq i$, and we know that $S_j U_i = 0 \subseteq U_i$. So now assume that $I_t \cong S_i$. Then by the definition of U_i , we have $I_t \subseteq U_i$. Thus $I_t U_i \subseteq I_t \subseteq U_i$. Thus U_i is an ideal as wanted.

It remains to be show that the U_i are minimal. To begin, we know that $U_i \neq 0$. So let $V < U_i$ where V is an ideal. We want to show that $V = 0$. Let I_t be a summand of U_i with $I_t \not\subseteq V$. Note that $I_t \cap V$ is a right ideal, and $(I_t \cap V) < I_t$. Then by the minimality of I_t , we see that $I_t \cap V = 0$. Now $I_t V \subseteq I_t$ as I_t is a right ideal. Yet $I_t V \subseteq V$ as V is a left ideal. So $I_t V \subseteq I_t \cap V = 0$, so $I_t V = 0$. But $I_t \cong S_i$, and this $S_i V = 0$. Also, $S_j V \subseteq S_j U_i = 0$ if $i \neq j$. So V annihilates ALL simple right R -modules. Thus $V \subseteq J(R) = 0$ as R is a Wedderburn ring. Thus $V = 0$ and U_i is minimal.

Finally, we claim that $S_i U_i \neq 0$. Otherwise, we would have that $S_i U_i = 0$ and $S_j U_i = 0$ if $j \neq i$. But this would imply that $U_i \subseteq J(R) = 0$, which is a contradiction. \square

We now suppose that we are dealing with a Wedderburn ring R , and we write R as in the previous theorem, as $R = \sum_{i=1}^m \bullet U_i$. Write $1 = e_1 + e_2 + \dots + e_m$ where $e_i \in U_i$. We note that $U_i U_j = 0$ whenever $i \neq j$ just as in the previous theorem. Hence $e_i = e_i \cdot 1 = e_i \sum_{j=1}^m e_j = e_i e_i$ (all the $e_i e_j$ terms are 0 when $i \neq j$). So e_i is always idempotent. Similarly, $U_i = 1 U_i 1 = (e_1 + e_2 + \dots + e_m) U_i (e_1 + e_2 + \dots + e_m) = e_i U_i e_i$ as again, all of the other cross terms are zero. So e_i is a unity element in U_i , and R is therefore isomorphic to an external direct sum of rings.

Finally, we claim that the U_i are simple rings. To see this, let $V < U_i$ be an ideal of U_i . Then V is an ideal of R . But then V must be 0 by the minimality of the U_i .

It is a theorem, which we did not prove, that every artinian simple ring is actually something much stronger, it is isomorphic to a division ring.

This concludes the first semester of algebra notes.