Abstract Algebra Notes

James Marshall Reber

December 8, 2016

Contents

Chapter 1

Preliminaries (Day 1-2)

Some things are covered about set theory, functions, and proof methods, but I know these extremely well at this point and don't want to waste time by writing more. So we're going to skip over this and straight into induction.

1.1 Induction (Day 2)

Induction is often used to prove things.

Example 1. *Prove, by induction,*

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Proof. We must first show the base case. For $n = 2$, we have $1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$, as required. Next, assume it holds for n. Then we need to show it holds for $n + 1$.
If it holds for n, we have $1 + \ldots + n = \frac{n(n+1)}{2}$. For $n + 1$, we add $n + 1$ to both sides to get $1 + \ldots + n + (n + 1) = \frac{n(n+1)}{2} + (n + 1) = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$, as required. Thus, induction has been shown, and the statement is true. □

Definition 1.1.1. (Well Ordering Principle) Any nonempty set A of $\mathbb{N}$ has a least element.

We use the well ordering principle to show induction.

Theorem 1. *(Weak Induction) Let $A \subset \mathbb{Z}_{>0} = \{x \mid x \in \mathbb{Z} \text{ and } x > 0\}$. Suppose that the following two conditions hold:*

1. $1 \in A$
2. *If $n \in A$, then $n + 1 \in A$*

Then $A = \mathbb{Z}_{>0}$.

Proof. Suppose $A^c \neq \emptyset$, since $\mathbb{Z}_{>0}$ is the sample space. Then A^c has aa least element, denoted by $b \in A^c$, by the well ordering principle. Then $b - 1 \in A$, since $b - 1 \neq -$ as $1 \in A$, and $b > 1$. If $b - 1 \in A$, then $(b - 1) + 1 \in A$ by property (2). This is a contradiction, though. □

Theorem 2. *(Strong Induction) Let $A \subset \mathbb{Z}_{>0}$. Now suppose that the following is true:*
If for all $k \in (0, n)$, $k \in A$, then $n \in A$.
Then $A = \mathbb{Z}_{>0}$.

Proof. Again, suppose $A^c \neq \emptyset$, and prove by contradiction. If $A^c \neq \emptyset$, then there is a least element $b \in A^c$. This implies $b - 1 \in A$, or $1, \ldots, b - 1 \in A$. But if $1, \ldots, b - 1 \in A$, then $b \in A$ by hypothesis, and thus we have a contradiction. □

Theorem 3. *(Division Algorithm) Let $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$. THen there exists a unique $q, r \in \mathbb{Z}$ such that $m = nq + r$, where $0 \leq r < n$.*

Proof. Assume $m > 0$ (the argument for $m < 0$ follows similarly). Consider the set $A = \{b \mid nb - m \geq 0\} \subset \mathbb{Z}_{>0}$. Note that this is not an empty set ($A \neq \emptyset$). By the well ordering principle, A has a least element, denoted q. Then $nq - m = r \geq 0$, by definition. But this $|r| < n$. Suppose that it's not, or $|r| \geq n$. This implies $nq + r = m$. If $|r| \geq n$, then we can rewrite the original statement as $nq + n + r' = m \rightarrow n(q+1) + r' = m$. This is a contradiction, snce we now have a smaller q. Now we need to consider uniqueness.
Assunme that q', r' are also factors. Then we have $m = q'n + r' = nq + r \rightarrow n(q' - q) = r - r'$. However, $r - r' < n$, which implies $r - r' = 0$, and $q - q' = 0 \rightarrow r = r'$ and $q = q'$. □

1.1.1 Exercises

Question 1: Prove that for all positive integers $n > 0$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

.

Chapter 2

Groups (Day 3- 19)

2.1 General Group Properties (Day 3-7)

Definition 2.1.1. (Binary Operation) A binary binary operation on a nonempty set A is the map $\circ : A \times A \to A$ such that

1. $\circ$ is defined for every pair of elements in A
2. $\circ$ uniquely associates each pair of elements in A to some element of A.

Definition 2.1.2. (Group) A group, denoted $(G, \cdot)$, is a set with a binary operation such that

1. There exists an identity element, denote e; i.e., $\forall a \in G, ae = ea = a$.
2. There exists inverses; i.e., $\forall a \in G$, there exists an $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.
3. The associative law is upheld; i.e. $\forall a, b, c \in G$, $a(bc) = (ab)c$.

Example 2. *Let K, M be two sets. Then $Fun(K, M) := \{f : K \to M\}$. Let $\circ : Fun(K, K) \times Fun(K, K) \to Fun(K, K)$ such that $(f \circ g)(x) = f(g(x))$. Then we will see that $G \subset Fun(K, K)$ of bijective functions is a group using the binary operation. In order to do so, we need to go through the axioms.*

1. *There is an identity: $\mathbb{1} : K \to K$ which maps $\mathbb{1}(x) = x$. Note that $(f \circ \mathbb{1})(x) = f(\mathbb{1}(x)) = f(x)$ and $(\mathbb{1} \circ f)(x) = \mathbb{1}(f(x)) = f(x)$.*
2. *Since the functions are bijective, there exists an $f^{-1} \in G$ such that $(f \circ f^{-1}) = f(f^{-1}(x)) = x$. Likewise, we have $(f^{-1} \circ f) = f^{-1}(f(x)) = x$. Note that this axiom requires the functions to be bijective.*
3. *The associative law is upheld. Note that $f \circ (g \circ h) = f \circ (g(h(x)) = f(g(h(x)))$ and $(f \circ g) \circ h = (f(g(x)) \circ h = f(g(h(x)))$. So, the associative law is upheld.*

Thus, G is a group.

Definition 2.1.3.
1. A function $f : K \to M$ is surjective if for all $m \in M$, $\exists k \in K$ such that $f(k) = m$.
2. A function $f : K \to M$ is injective if whenever $f(k) = f(k')$, we have $k = k'$, $\forall k, k' \in K$.
3. A function $f : K \to M$ is bijective if it is both injective and surjective.

Example 3. *The symmetric group S_n is the group of bijective functions from the set $K = \{1, \dots, n\}$ to itself. Notice that the group has order $|S_n| = n!$.*

Definition 2.1.4. (Order) The order of a finite group, denoted $|G|$, is the number of elements in G.

Definition 2.1.5. (Equivalence Relation) Given a set A, an equivalence relation on A is a subset $K \subset A \times A$ such that the following three properties are satisfied:

1. (Reflexive) If $a \in A$, then $(a, a) \in K$.
2. (Symmetric) If $(a, b) \in K$, then $(b, a) \in K$.
3. (Transitive) If (a, b) and (b, c) are both in K, then $(a, c) \in K$.

Definition 2.1.6. (Congruence) Two integers are congruent, mod an integer n (denoted $a \equiv b$) if $n|(a - b)$. Notice that congruence gives an equivalence relation on the integers.

Definition 2.1.7. (Abelian or commutative) A group is called commutative, or Abelian, if for all $a, b \in G$, $ab = ba$.

Remark. *The group $\mathbb{Z}_n$ is the group of integers modulo n.*

Example 4. $\mathbb{Z}_3 = \{0, 1, 2\}$.

Lemma 3.1. *$(\mathbb{Z}_n, +)$ is an Abelian group.*

Proof. We need to show that $(\mathbb{Z}_n, +)$ satisfies the group axioms.

1. We have that 0 is the identity element – $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}_n$.
2. If $0 < a \leq n$, then $n - a \in \mathbb{Z}_n$ is an inverse, since $(n - a) + a = n = 0$.
3. Associativity follows from the associativity of addition on the integers.
4. (Remark) Commutativity also follows from the properties of addition.

So, we can see that it's a group, and not only that but an Abelian group. □

Remark. *Note that all finite Abelian groups in some sense look like $(\mathbb{Z}_n, +)$.*

Lemma 3.2. *Every group has a unique identity.*

Proof. Assume that there are two identities – e and e'. Then we have that $ee' = e$. By definition, though, $ee' = e'$, and so we have $e' = e$. □

Lemma 3.3. *For every element in G there is a unique inverse.*

Proof. Suppose g' and g'' are two possible inverses. Then we have $g' = eg' \leftrightarrow g' = (g''g)g' \leftrightarrow g' = g''(gg') \leftrightarrow g' = g''e \leftrightarrow g' = g''$. □

Lemma 3.4. *(Cancellation Law) If we have $ab, c \in G$ and $ab = ac$ then $b = c$.*

Proof. We can multiply a^{-1} to the left hand side of both sides of the equation to get $a^{-1}(ab) = a^{-1}(ac)$. Using the associativity law, we then have $(a^{-1}a)b = (a^{-1}a)c \leftrightarrow b = c$. □

Definition 2.1.8. A subgroup H of a group G is a subset $H \subset G$ such that

1. It is closed under the identity; i.e., $e \in H$.
2. It is closed under multiplication; i.e., if $g, h \in H$ then $gh \in H$.
3. It is closed under inverses; i.e., if $h \in H$, then $h^{-1} \in H$.

Lemma 3.5. *If H is a subgroup, then H is a group with respect to the operation induced by G.*

Proof. The proof is trivial and is left to the reader as an exercise (**Question 2**). As a general outline, though, one would exhaust the group axioms using the definition of a subgroup. □

Proposition 3.1. *Every subgroup of $\mathbb{Z}$ is of the form $b\mathbb{Z}$ for some $b \in \mathbb{Z}_{>0}$.*

Remark. *We can defined the GCD using this. Note that heuristically, the GCD is the greatest number that divides both integers given; i.e. $gcd(a, b) = d$ where d is the greatest number such that $d|a$ and $d|b$.*

Properties 2.1.1. For $g \in G$, we have

1. $g^n g^m = g^{n+m}$.
2. $(g^n)^m = g^{n \cdot m}$.

2.1.1 Exercises

Question 3: Prove that $(g^{-1})^{-1} = g$.

2.2 Cyclic Groups (Day 8-9)

Definition 2.2.1. (Cyclic Group) G is a cylic group if $G =< g >$ for some $g \in G$. Note that $< g >= \{g^n \mid n \in \mathbb{Z}\}$.

Example 5. *Note that $(\mathbb{Z}, +, 0)$ is a cyclic group. It's generators are ± 1.*

Remark. *The smallest subgroup of G containing $g \in G$ is $< g >$.*

Definition 2.2.2. (Order of an Element) The order of $g \in G$ is the smallest integer n such that $g^n = e$. If there is no such integer, then we say that the element has infinite order.

Theorem 4. *Let $G =< g >$ be a group.*

1. *If the order of g is infinite, then $g^i = g^j \leftrightarrow i = j$.*
2. *If the order of g is n, then $g^i = g^j \leftrightarrow n|(i-j)$.*

Proof. 1. Suppose $|g|$ is infinite. Then it's trivial to note if $i = j$, then $g^i = g^k$. On the other hand, suppose $g^i = g^j$. We can assume arbitrarily that $i > j$. Then $g^i g^{-j} = e$. By properties of exponents, we then have $g^{i-j} = e$, which implies g has finite order. This is a contradiction, and so if $g^i = g^j$ then $i = j$.

2. Suppose $|g| = n$. Assume $n|(i-j)$. THen by definition, ther exists a $q \in \mathbb{Z}$ such that $i - j = nq$. It follows, then, that $g^{i-j} = (g^n)^q$. However, any multiple of the order still results in the identity, and so $g^{i-j} = e^q$. Multiplying g^j on the right of both sides gives us $g^i = g^j$.

   Now assume $g^i = g^j$. THen this implies $g^{i-j} = e$. Assume arbitrarily that $i > j$, since if $i = j$, its trivial. Now note $i - j = nq + r$ for $0 \leq r < n$ by the division algorithm. If this is true, then $g^{i-j} = g^{nq}g^r = (g^n)^q g^r = e^q g^r = g^r = e$. This is a contradiction of the definition of order if we assume $0 < r < n$. Thus, $r = 0$. Since $r = 0$, we get $n|(i-j)$.

□

Corollary 4.1. *Let $G =< g >$, and $|g| = n$.*

1. *$|g| = | < g > |$*
2. *If $g^k = e$ for some k, then n divides k.*

Proof. 1. If $|g|$ is infinite, then all elements in $< g >$ are distinct, which implies that $| < g > |$ is infinite.

2. Suppose $|g|$ is finite and equal to n. Then the group $< g >= \{e, \ldots, g^{n-1}\}$, in particular $| < g > | \leq n$. However, if $| < g > |$ is less than n, then this means $g^k = g^0$, which implies $n|k$ for $k < n$. This is impossible, and so $| < g > | = n$.

□

Theorem 5. *Suppose $g \in G$ has order n. THen $< g^k >=< g^{gcd(n,k)} >$ and $|g^k| = \frac{n}{gcd(n,k)}$.*

Proof. Let $d = \gcd(n, k)$. We must first show $< g^k > \subset < g^d >$. In other words, it's sufficient to show $g^k \in < g^d >$. Since d divided k, then $dm = k$ for some m, and thus $g^k = (g^d)^m \in < g^d >$. Next, it's sufficient to show $g^d \in < g^k >$. Assume $k = md + r$. Then the rest follows as a consequence of the divison algorithm (see piror proofs for examples of what to do from here).
Next we need to show that $|g| = \frac{n}{\gcd(n,k)}$. By prior, we have that $|g^k| = | < g^d > |$.

Claim 1. *If $d|n$ then $|g^d| = n/d$.*

Proof. We have $(g^d)^{n/d} = g^n = e \rightarrow |g^d| | \frac{n}{d}$. Suppose for contradiction $|g^d| < n/d$. Let $|g^d| = r$. THen this implies that $dr < n$, and this implies $g^{dr} = e$. This is a contradiction, and so there must be equality. □

With this claim, the theorem is proven. □

Corollary 5.1. *Suppose G and H are cyclic of order m and n respectively. THen $G \times H$ is cyclic if n, m are coprime.*

Remark. *The converse is also true.*

Proof. Let $G =< g >$, $H =< h >$. Then $(g, h) \in G \times H$. First, $(g, h)^{nm} = e = (g^{nm}, h^{nm})$. Then $|(g, h)||nm$. We will ow show $nm||(g, h)|$. Suppose $|(g, h)| = k$. Then $g^k = e \to m|k$. Similarly, $h^k = e \to n|k$. Then $nm|k \to nm = k$. □

Remark. *If $gcd(n, m) = 1 \to lcm(n, m) = nm$.*

Example 6. *What is an example of a cyclic group of order 40? $\mathbb{Z}_{40}$.*
What is an example of a noncyclic group of order 40? $\mathbb{Z}_4 \times \mathbb{Z}_{10}$.

Proposition 5.1. *Let G be a cyclic group of order n, $G =< g >$.*

1. *Every subgroup of G is cyclic.*

2. *For every divisor, k, of n, there is exactly one subgroup of order k, namely $< g^{n/k} >$.*

Proof.

1. Let $H \subset G$, then $e \in H$. If $H = \{e\}$, then $H =< e >$. therwise, there exists $g^m \in H$ such that $m > 0$. Let $H_+ = \{m \mid g^m \in H, m > 0\}$. Let b be the smallest element in H_+, which exists by the well ordering principle. This implies $< g^b >\subset H$. THen we want to show $H \subset< g^b >$. Proceed by contradiction. Suppose $h \in H$ such that $h \notin< g^b >$. Then $h = gk$ for some k. By the division algorithm, $k = qb + r$, $0 < r < b$. THen $g^k = g^{qb}g^r \leftrightarrow g^{k-qb} = g^r$. Since H is a subgroup, $g^{k-qb} \in H$, and so this implies $g^r \in H$. This is a contradiction. Thus, we have $r = 0$, and so we have $H \subset< g^b >$ and by set equality $< g^b >= H$.

2. By previous corollary, $| < g^{n/l} > | = \frac{n}{\gcd(n,n/k)} = \frac{n}{n/k} = k$. If $H \subset G$, then we know $H =< g^r >$ for some r. Then we need to show $< g^r >=< g^k >$ where $k|n$. By previous corollary, $< g^r >=< g^{\gcd(n,r)} >$.

□

Definition 2.2.3. Homomorphism

1. A homomorphism from G to G' is a function $f : G \to G'$ such that $f(e_G) = e_{G'}$ and $f(g \cdot h) = f(g)f(h)$.

2. A function f is an isomorphism if f is a homomorphism and it's bijective.

Remark. *Let $f : G \to H$ and $g : H \to K$ where g and f are isomorphisms. Then $g \circ f$ is an isomorphism.*

Theorem 6.

1. *If G is an infinite cyclic group, then $G \cong (\mathbb{Z}, +, 0)$.*

2. *If G is cyclic of order n, then $G \cong (\mathbb{Z}_n, +, 0)$.*

Proof.

1. Suppose $G =< g >$. Let $f : \mathbb{Z} \to G$ be the function defined by $f(n) = g^n$. THus, we need to show $f(e_{\mathbb{Z}}) = e_G$ and $f(n + m) = g^n g^m$. However, this is trivial – $f(0) = g^0 = e$, and $f(n + m) = g^{n+m} = g^n g^m$. Thus, this is a homomorphism. We now need to show that f is bijective. Suppose $f(n) = f(m), n = m$. This follows, however, from the theorem earlier. Therefore, f is injective. To show that it's surjective, note that if there's a $g^k \in G$, then we have $f(k)$.

2. Proven exactly the same way, except we use $f : \mathbb{Z}_n \to G$.

□

2.3 Symmetric Group and Permutations (Day 10)

Remark. *Recall that D_n is the dihedral group, and A_n is the alternating group. Note that $D_n \subset S_n$ is a subgroup and $A_n \subset S_n$ is a subgroup. Also recall that D_n is the symmetries of the n-gon. The alternating group is the symmetries of three dimensional objects.*

Example 7. *Following is an example of cycle notation:*

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

Here, we have $1 \to 2$, $2 \to 3$, $3 \to 5$, $4 \to 6$, $5 \to 1$, $6 \to 4$.

Definition 2.3.1. (Cycle Notation) Let $\alpha : \{1, \ldots, n\} \to \{1, \ldots, n\}$ be a cycle. Then we can denote it using cycle notation:

$$\begin{pmatrix} 1 & \ldots & n \\ \alpha(1) & \ldots & \alpha(n) \end{pmatrix}$$

Definition 2.3.2. (Cycle) A cycle of length m is a sequence $(\alpha_1, \ldots, \alpha_m)$ where α_i are distinct integers between 1 and n.

Lemma 6.1. *Disjoint cycles commute*

Proof. α is a cycle, and β is another disjoint cycle. We want to show that $\alpha \circ \beta = \beta \circ \alpha$. In other words, for all $i \in \{1, \ldots, n\}$, $\alpha(\beta(i)) = \beta(\alpha(i))$. Suppose i is an element of β, then $\alpha(\beta(i)) = \beta(i)$. Then $\alpha \circ \beta = \beta \circ \alpha$ if $i \in \beta$. The argument for $i \in \alpha$ is the same. If $i \notin \alpha, \beta$, then α and β fix it, and thus $\alpha \circ \beta = \beta \circ \alpha$. □

Theorem 7. *Every permutation can be written as a disjoint product of cycles.*

Proof. (Outline of constructive proof): Let $\alpha : \{1, \ldots, n\} \to \{1, \ldots, n\}$, and select arbitrary a. Then you have $(1, \alpha(a), \ldots)(a, \alpha(a), \ldots)$. There's no way a is in the first cycle, so it follows that $\alpha^n(a)$ is not in the cycle. Doing so repeatedly eventually construct all disjoint cycles. □

Corollary 7.1. *The order of a permutation is the least common multiple of the lengths of cycles appearing in it's decomposition into a disjoint product of cycles.*

Proof. Suppose α and β are cycle of length n, m and they are disjoint. Then we need to show $r := |\alpha\beta|$ divides $\text{lcm}(n, m)$ and $\text{lcm}(n, m)|r$. Suppose r is the order, then $(\alpha\beta)^{\text{lcm}(n,m)} = \alpha^{\text{lcm}(n,m)}\beta^{\text{lcm}(n,m)} = e$. This implies $r|\text{lcm}(n, m)$. Suppose r is the order again. Then we have $e = (\alpha\beta)^r = \alpha^r\beta^r \to \alpha^r = \beta^{-r}$. The only way this is true is if $\alpha^r = e$ and $\beta^{-r} = e$. THis means $n|r$ and $m|r$. So we have $r = \text{lcm}(n, m)$. □

2.4 More on Groups (Day 11-15)

Definition 2.4.1. (Automorphisms) An automorphism is an isomorphism from a group to itself.

Theorem 8. $Aut(\mathbb{Z}_n) \cong (\mathbb{Z}_n^\times, \cdot, 1)$.

Proof. An automorphism from a group to itself is entirely determined by where it sends the generator. Therefore, we have that the function can only send a generator to other generators, which are all the numbers coprime to it. Therefore, we have that $\text{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}_n^\times, \cdot, 1)$. □

Definition 2.4.2. We defined the equivalence class of an element to be $[a] := \{b \in S | a\ n\}$, where $a\ b$ denotes that two elements are equivalent under a relation.s

Lemma 8.1. *Given two elements a and b, we have*

$$[a] \cap [b] = \begin{cases} \emptyset \\ [a] = [b] \end{cases}$$

Lemma 8.2. *Both left equivalence and right equivalence are relations on G. The equivalence classes are of the form, for $_R$, H_a, and for the left equivalence are of the form aH where $a \in G$.*

Definition 2.4.3. $aH := \{ah \mid h \in H\}$ and $Ha := \{ha \mid h \in H\}$.

Proof. Note that the proof for $_L$ is the same as for $_R$. It is sufficient, then, to just show one of them. We want to show $_R$ is an equivalence relation. We then need to go through the axioms for this equivalence relation. First, not $K = \{(a, b) \mid ab^{-1} \in H\}$.

1. Reflexive: We need to show $a \ _R a$. However, by definition, this means we need to show $aa^{-1} \in H$. Since H is a subgroup, this is true.

2. Symmetric: Need to show that if we assume $a \ _R b$, then $b \ _R a$. This means, by definition, that if we assume $ab^{-1} \in H$, then we need to show $b^{-1}a \in H$. However, since H is a subgroup, it's closed under inverses, and so $(ab^{-1})^{-1} \in H \rightarrow ba^{-1} \in H$.

3. Transitive: Need to show if $a \ _R b$, $b \ _R c$, then $a \ _R c$. So, by definition, if $ab^{-1} \in H$, and $bc^{-1} \in H$, then we need to show $ac^{-1} \in H$. Since H is a subgroup, it's closed under multiplication, and so $(ab^{-1}(bc^{-1}) \in H \leftrightarrow ac^{-1} \in H$.

Thus, K is an equivalence relation. (The left equivalence relation follows similarly.) □

Corollary 8.1. *Let G be a group, and $H \subset G$ a subgroup.*

1. $aH = bH \leftrightarrow b^{-1}a \in H \leftrightarrow a^{-1}b \in H$

2. $Ha = Hb \leftrightarrow ab^{-1} \in H \leftrightarrow ba^{-1} \in H$

3. $$aH \cap bH = \begin{cases} \emptyset \\ aH = bH \end{cases}$$

Definition 2.4.4. (Index) $[G : H]$ is the number of left (respectively, right) cosets of H.

Theorem 9. *If G is finite, then $[G : H]|H| = |G|$. In other words, $[G : H] = |G|/|H|$.*

Proof. First, a lemma.

Lemma 9.1. *If G is a group, and $H \subset G$ a subgroup, then for any a there exists a bijection between H and aH.*

Proof. Let $\phi : H \rightarrow aH$ be the function defined by sending $\phi(h) = ah$ for $h \in H$. It's injective, because if $a, b \in H$, then if $\phi(a) = \phi(b)$, we have $ah = bh$, and by the cancellation theorem $a = b$. For surjectivtiy, if we have ah, then this implies there is an $h \in H$ such that $\phi(h) = ah$. So, ϕ is bijective. □

First, note that G is finite, and so $[G : H]$ is finite. Then let $a_1H, \ldots, a_nH$ denote the distinct cosets of H. Hence, $r = [G : H]$. However, since $_R$ is an equivalence relation, then $_R$ is a partition, and so $|G| = \sum_{i=1}^{r} |a_iH|$. However, we have a bijective function from all a_iH to H. So, $|a_iH| = |H|$. Therefore, we have $|G| = \sum_{i=1}^{r} |H| \leftrightarrow |H| = r|H|$. However, $r = [G : H]$, and so $|G| = [G : H]|H|$. □

Corollary 9.1. *If G is finite, then for any $g \in G$, $|g|||G|$.*

Proof. We have $|g| = | < g > |$, and by the theorem prior, $[G :< g >]|g| = |G|$,and so $|g|||G|$. □

Corollary 9.2. *1. $|H|||G|$.*

2. For any $g \in G$, $|g|||G|$.

3. For any $g \in G$, $g^{|G|} = e$.

Example 8. *Show that A_4 has no subgroup of order 6.*

Proof. Let $H \subset A_4$ be a subgroup of order 6. Then $[G : H] = 2$, because by Lagrange's theorem, $[G : H]|H| = |G|$. By definition, this means there are two cosets for H. In other words, $\exists a \in G$ such that H and aH are two cosets (remark: $a \notin H$).

Claim 2. $|A| \neq 3$

Proof. Since there are only two cosets, this means that $a^2H + H$oor aH. If $|a| = e$, then this means that $a^3H = aH$ which means that $H = aH$. This can't be true, since we took a to be an element where these cosets are distinct. □

This implies that all elements of order 3 are in H. This is a contradiction, since there are 8 elements of order 3 in A_4. □

Corollary 9.3. *(Fermat's Little Theorem) For any integer a and a prime p, $a^p \equiv a$ mod$p$.*

Proof. We can prove this using group theory. Recall $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$, and so if p is prime $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$ implies $|\mathbb{Z}_p^\times| = p - 1$. By the division algorithm, we have $a = kp + r$, where $0 \leq r < p$. Then $a^p \equiv r^p$ mod$p$. Assume $r \neq 0$. Then we have $r^p = r$ mod$p$. By the corollary, we have $r^{p-1} = 1$ mod$p$ and so $r^p = r$ mod$p$. □

Remark. *We can also use representations to show groups. For example, we have that $D_{2n} =< r, f \mid (rf)^2 = e, f^2 = e, r^n = e >$. We als o have $G =< g \mid g^n = e >$ is another way to write the cyclic group.*

Theorem 10. *If G is a group of order $2p$, then $G \cong \mathbb{Z}_{2p}$ or $G \cong D_{2p}$.*

Proof. The proof is too long for these notes, and is excluded. □

2.5 Normal Groups (Day 16)

Definition 2.5.1. (Normal Group) A subgroup $H \subset G$ of G is a normal subgroup if $aH = Ha$ for all $a \in G$.

Remark. *First, note that $aH = Ha$ does not mean that every element commutes, but rather it means that for all $a \in G, h \in H$ we have $ah = h'a$.*
Second, if it s true that every element commutes with $h \in H$, then $aH = Ha$ is trivially true. In other words, every $H \subset G$ of an abelian group G is normal.

Theorem 11. *$H \subset G$ is normal if and only if for all $x \in G$, $xHx^{-1} \subset H$. By definition, we have $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$.*

Proof. Suppose H is normal. THen given any $h \in H$ and $x \in G$, there exists $h' \in H$ such that $xh = h'x$. This implies, after multiplying x^{-1} on the right hand side, that $xhx^{-1} = h'$. This implies $xhx^{-1} \in H$ for all $h \in H, x \in G$. This therefore implies $xHx^{-1} \subset H$.
Next, we have that for all $x \in G, xHx^{-1} \subset H \to xH \subset Hx$. Since this is true for all x, apply with x^{-1} to get $Hx \subset xH$. Therefore, $xH = Hx$. □

Remark. *Note that the center is the largest Abelian group, and so when we apply $G/Z(G)$, we get a group which is not Abelian.*

Theorem 12. *If $H \subset G$ is a normal subgroup, then G/H is a group where we define $aH * bH = abH$.*

Proof. We must first check that $aaH * bH$ is well defined. We need to show that if $aH = a'H$, $bH = b'H$ then $abH = a'b'H$. Saying that these two cosets are the same is equivalent to saying $ah = h'a$ for some $h, h' \in H$, and similarly $bh'' = h'''b$ for some $h'', h''' \in H$. In particular, this means $h'^{-1}ah = a'$, and $h'''^{-1}bh'' = b'$. Thus, if one were to write $(b')^{-1}$, one would have $h''^{-1}b^{-1}h'''$, likewise $(a')^{-1} = h^{-1}a^{-1}h''$. This implies in particular that $(b')^{-1}(a')^{-1}ab = h''^{-1}b^{-1}h'''h^{-1}a^{-1}h'ab$. We need to then note that this is in H. Note $h'a = ah''''$. Thus, we have $h''^{-1}b^{-1}h'''h^{-1}a^{-1}ah''''b$. Do this similarly with b to get a bunch of h's, which means that $(b')^{-1}(a')^{-1}ab \in H$, as required. Thus, multiplication is well defined. Now, we need to exhaust the axioms of a group:

1. There exists an identity: $eH \to aH * eH = eH * aH = aH$.

2. $(aH)^{-1} = a^{-1}H$.

3. Note $(aH * bH) * cH = (ab)HcH = (ab)cH = a(bc)H = aH(bc)H = aH(bH * cH)$.

Thus, G/H is a group. $\square$

Theorem 13. *If H, K are normal subgroups such that $H \cap K = \{e\}$ and $G = HK$, then $\phi : H \times K \to G$ is an isomorphism.*

Theorem 14. *(Cauchy's 2nd Theorem) Let G be a finite Abelian group. Then there exists an element of order p for every prime dividing $n = |G|$.*

Proof. Suppose $n = p_1^{n_1} \cdots p_r^{n_r}$, where p_i are prime. Then there exists an $x \in G$ such that the order of x is p_i for some i. This is because G is a nontrivial group. It is implied there is some $g \in G$ where $|g| = m$ and $m|n$. This implies $m = qr$ for some prime diving n. Then note x^r has order q. Let $H =< x^r >$. Let $y = x^r$. tHen $H =< y >$. Since G is Abelian, $H \trianglelefteq G$. This implies G/H is a group. Note $|H| = q$, then $|G/H| = \frac{p_1^{n_1} \cdots p_r^{n_r}}{q} < n$. By induction, there exists $y' \in G/H$ such that $|y'| = p_{i'}$, $i' \neq i$. This means $y' < y >$ has order $p_{i'}$, where $y' \in G$. This means $y'^{p_{i'}} < y > = < y > \to y'^{p_i'} \in < y > \to y'^{p_i'} = e$. By induction, this means that there is an element in G of order p_i for all i. $\square$

Theorem 15. *Let $f : G \to H$ be a group homomoprhism. Then*

1. $\ker(f) \trianglelefteq G$
2. *$Im(f)$ is a subgroup of H.*
3. *If H' is a subgroup of G, $Im(H')$ is a subgroup of H.*
4. *If $g \in G$, then $|f(g)|$ divides $|g|$ and $|f(g)|$ divides $|H|$.*
5. *$f(g^n) = f(g^n)$ for all n.*

Proof.
1. To show that $\ker(f)$ is a normal subgroup, we need to show that $xyx^{-1} \in \ker(f)$ for all $y \in \ker(f)$, $x \in G$. However, to show that, we need to then show that $f(xyx^{-1}) = e$. Using the properties of homomorphisms, we have $f(x)f(y)f(x^{-1}) = f(x)f(y)f(x)^{-1}$. Note that $y \in \ker(f)$, and so $f(y) = e$. Therefore, we have $f(x)ef(x)^{-1} = f(x)f(x)^{-1} = e$. So, by definition, $xyx^{-1} \in \ker(f)$ for all $x \in G$, $y \in \ker(f)$, as required.

2. To show that it's a subgroup, we can use the one-step subgroup test $-$ that is, if for all $x, y \in Im(f)$, we have $xy^{-1} \in Im(f)$, then we have that $Im(f)$ is a subgroup. However, by definition, $Im(f) = \{h \in H \mid f(g) = h \text{ for some } g \in G\}$. So we have $f(g) = x$ and $f(g') = y$ for some $g, g' \in G$. Therefore, we want to show $f(g)f(g')^{-1} \in Im(f)$. However, by properties of homomorphisms, this is equivalent to asking $f(gg'^{-1}) \in Im(f)$, which is true since $gg'^{-1} \in G$. Therefore, the image of a homomorphism is a subgroup.

3. We have that H' is a subgroup of G, and thus for all $x, y \in H$, $xy^{-1} \in H'$. We then need to show that $Im(H')$ is a subgroup of H. We then want to use the subgroup test. Let $x, y \in Im(H')$, then we want to show that $xy^{-1} \in Im(H')$. However, if $x, y \in Im(H')$, this means that there are $x', y' \in H'$ such that $f(x') = x$ and $f(y') = y$. Therefore, we want to show that $f(x')f(y')^{-1} \in Im(H')$. However, by properties of homomorphisms, this is equivalent to asking to show that $f(x'y'^{-1}) \in Im(H')$. However, we know that $x'y'^{-1} \in H'$ by the subgroup test, and so by definition it's image is in the image of H', which means that $Im(H')$ is a subgroup.

4. From prior, we know that $f(g)$ is a subgroup of H and so by Lagrange it must be a divisor of the order of H. Next, let $|g| = n$. Then we have $f(g^n) = f(e) = e$, by properties of homomorphisms. However, this also means $f(g)^n = e$, which means that $|f(g)||n$.

5. We can prove this using induction. By properties of homomorphisms, we know that $f(g^2) = f(g \cdot g) = f(g) \cdot f(g) = f(g)^2$. Assume it holds for n. Then we have $f(g^{n+1}) = f(g^n \cdot g) = f(g^n) \cdot f(g) = f(g)^n \cdot f(g) = f(g)^{n+1}$, as required. For negative numbers, we can use the inverse.

$\square$

Example 9. *How many homomorphisms are there from* $\mathbb{Z}_3 \to \mathbb{Z}_5$*? We can find them using the fact that the imge of a cyclic group must also be a cyclic group, by the prior theorme. THerefore, a generator must map to a generator. There are no elements of order* 3 *in* $\mathbb{Z}_5$ *however, and so the only homomorphism is the trivial one.*
Generalizing further, to find the number of homomorphisms from $\mathbb{Z}_n \to \mathbb{Z}_m$*, where* $n < m$*, we look for the number of elements of oder* n *in* $\mathbb{Z}_m$*.*

2.6 Fundamental Theorem for Group Homomorphisms (Day 17-18)

Theorem 16. *(Fundamental Theorem for Group Homomorphisms)*

Remark. *This is sometimes referred to as the First Homomorphism Theorem instead of the Fundamental Theorem.*

Let ϕ *be a homomorphism of* G *onto* G' *with kernel* K*. Then* $G' \cong G/K$*, the isomorphism between these being effected by the map*

$$\psi : G/K \to G'$$

defined by $\psi(Ka) = \phi(a)$*.*

Proof. Define $\psi : G/K \to G'$ by $\psi(Ka) = \phi(a)$ for $a \in G$. Our first task is to show that ψ is well defined. In other words, we want to show if $Ka = Kb$ then $\psi(Ka) = \psi(Kb)$. But if $Ka = Kb$, then we know that $a = kb$ for some $k \in K$. Hence, $\phi(a) = \phi(kb) = \phi(k)\phi(b)$. Since $k \in K$, the kernel of π, then $\phi(k) = e$. So we have $\phi(a) = \phi(b)$. Therefore, the mapping of ψ is well defined.
Because ϕ is onto G', given $x \in G'$, then $x = \phi(a)$ for some $a \in G$, thus $x = \phi(a) = \psi(Ka)$. This shows that ψ maps G/K onto G'.
Next, we need to establish whether or not ψ is 1-1. Suppose that $\psi(Ka) = \psi(Kb)$, then $\phi(a) = \psi(Ka) = \psi(Kb) = \phi(b)$. Therefore, $e' = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1})$. Because ab^{-1} is thus in the kernel of ϕ, which is K, we have $ab^{-1} \in K$. This implies that $Ka = Kb$. Thus, we have ψ is 1-1.
Finally, we need to show that ψ is a homomorphism to establish that it is an isomorphism. We check $\psi((Ka)(Kb)) = \psi(Kab) = \phi(ab) = \phi(a)\phi(b) = \psi(Ka)\psi(kb)$. Consequently, ψ is a homomorphism of G/K onto G'. □

Example 10. *If* $\mathbb{Z} \to \mathbb{Z}_n$*,* $f(k) = k \ modn$*, then the* $\ker(f) = \{x \in \mathbb{Z} \mid n|x\}$*. By the theorem,* $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$*.*

Theorem 17. *Let* G *be a group, and* $H, K \subset G$ *be normal subgroups such that* $HK = G$ *and* $H \cap K = \{e\}$*. Then* $H \times K \cong G$*.*

Theorem 18. *Let* G *be a group such that* $|G| = p^2$ *where* p *is a prime. Then* $G \cong \mathbb{Z}_{p^2}$ *or* $\mathbb{Z}_p \times \mathbb{Z}_p$*.*

Proof. Note that by Lagrange, the possible order of elements for G are $1, p$, and p^2. Suppose it has an element of order p^2. Then we're done, since this element therefore generates the group. Suppose that otherwise, then Then we have that every non-trivial element has order p. Let $H =< g >$ where $|g| = p$. Then there exists a $g' \in G$ such that $g' \notin H$. Let $K =< g' >$. We then need to check that H, K are normal in G, $HK = G$, and $H \cap K\{e\}$. Note that $H \cap K = \{e\}$ is trivial since $g' \notin H$ and so none of it's powers are in H. $HK = G$ follows since $|HK| = p^2$. So we then need to check that H and K are normal.
To check that H is normal, we need to check that $xhx^{-1} \in H$ for all $x \in G$, $h \in H$. We have two possible options – either $x \in K$ or $x \in H$. If $x \in H$, then the results is trivial by properties of subgroups. Assume $x \in K$, then. Also assume that $xhx^{-1} \notin H$ – then it follows that $xhx{-}1 \in K$. Then this implies that $xhx^{-1} = g'^n$ for some n. But $h = g^s$ for some s. Note $x = g'^t$ for some t. So we have $g'^t g^s g'^{-t} = g'^n \to g^s = g'^{-t} g'^n g'^t$, which implies that $g^s \in K$, a contradiction. So therefore $xhx^{-1} \in H$, and so H is normal. The argument for the normality of K follows similarly, and so we have that $\mathbb{Z}_p \times \mathbb{Z}_p \cong G$. □

2.7 Structure Theorem For Finite Abelian Groups (Day 18-19)

Theorem 19. *(Structure Theorem for Finite Abelian Groups) Let G be a finite Abelian group. Then G is isomorphic to a direct product of cyclic groups of prime power order. Moreover, the number of factors in this product and the prime power orders are uniquely determined by G.*

Before proving this, we need to first establish a few lemmas and corollaries.

Lemma 19.1. *Any finite Abelian group G of order $p^k m$ (where $gcd(p, m) = 1$) can be written as $G \cong H \times K$, where $H = \{x \in G \mid x^{p^k} = e\}$, $k = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^k$.*

Proof. First, we need to know that H and K are subgroups, and we need to (trivially) know that they are normal.
Showing that they are subgroups: For H, $e \in H$ and if $x \in H$, then $x^{p^k} = e$ which implies $x^{-p^k} = e$, which implies $x^{-1} \in H$. If $x, y \in H$, then $x^{p^k} y^{p^k} = (xy)^{p^k}$ since H is Abelian, and so $xy \in H$. For K, e have $e \in K$. If $x \in K$, then we have $x^m = e$, and so $x^{-m} = e$. This implies that $x^{-1} \in K$. If $x, y \in K$, then $x^m y^m = (xy)^m$, which implies $xy \in K$. So, H and K are subgroups. We need to now check that $H \cap K = \{e\}$. Suppose there is a $x \in H \cap K$. Then $x^{p^k} = e$ and $x^m = e$, which means that $|x||\gcd(p^k, m)$ which implies $|x| = 1$, or in other words, $x = \{e\}$.
Finally, we need to show that $HK = G$. We trivially know that $HK \subset G$ $k \in K$. Since $\gcd(p, m) = 1$, then we know there exist $s, t \in \mathbb{Z}$ such that $1 = sp^k + tm$. Note then that $x = x^{sp^k} x^{tm}$. However, $x^{sp^k} \in K$, and $x^{pm} \in H$, since some power of x^{sp^k} has order dividing m, and similarly x^{tm} has some order dividing p^k. Finally, we need to show $|H| = p^k$. Suppose it isn't – suppose $|H| = p^{k'}, k' < k$. Then we have $|G| = |K||H| \leftrightarrow p^k m = p^{k'}|K|$. This implies $p||K|$, and thus there exists some $x \in K$, $x \neq e$, $|x| = p$. This cannot happen, though, since we assumed the $\gcd(p, m) = 1$. So, $|H| = p^k$. ☐

Corollary 19.1. *Any finite Abelian group is a product of groups of prime power order.*

Remark. *This is not saying the same thing as the theorem – the groups here are not necessarily cyclic.*

Proof. Suppose $|G| = n$. If $n = 1$, there's nothing to really show. If $n = p^r b$ for some b where $\gcd(p, b) = 1$, then the lemma implies $G \cong H \times K$, where $|H| = p^r$. By induction, $K \cong H_2 \times \ldots \times H_s$, where H_i are groups of prime power order. This implies $G \cong H_1 \times \ldots \times H_s$. ☐

Lemma 19.2. *If G is a group of prime power order , say p^k and $a \in G$ is an element of maximal order, then $G \cong < a > \times K$ for some $K \subset G$.*

Proof. Let $a \in G$ be an element of maximal order, say $p^{k'}$, where $k' < k$. If $a \in G$, $|a| = p^k$ then $G \cong < a > \times \{e\}$. Let $b \in G / < a >$, whose order is minimal. Let $\phi : G \to G / < k > =: \bar{G}$. Let $\bar{x} := \phi(x)$, i.e., $\bar{x} = x < b >$.

Claim 3. $< a > \cap < b > = \{e\}$

Proof. If $| < b > | = p$, then $< b > \cong \mathbb{Z}_p$. If $x \in < a > \cap < b >$, $< b > \subset < a >$,. THis is a contradiction, since $b \notin < a >$. ☐

Claim 4. $\bar{G} \cong < \bar{a} > \times \bar{k}$ *for some* $\bar{k}$

Proof. First, note that $\bar{a}$ has maximal order. Suppose not, i.e. $(\bar{a})^{p^{k'}-1} = e \to (a < b >)^{p^{k'}-1} = < b >$. Then this implies that $a^{p^{k'}-1} = e$, since $a^{p^{k'}-1} \in < b >$. However, this is a contradiction, since this implies $a^{p^{k'}-1} \neq a^{p^{k'}}$. This implies $\bar{a} = a^{p^{k'}}$, i.e., maximal order. We know that $|\bar{G}| < |G| >$. By induction, $\bar{G} = < \bar{a} > \times K$, for some $\bar{K}$. Let $K = \phi^{-1}(\bar{K})$. Then we need to show $G \cong < a > \times K$.

Claim 5. $G \cong < a > \times K$.

Proof. $< a > \cap K = \{e\}$ since if $x \in < a > \cap K \to \bar{x} \in < \bar{a} > \cap \bar{K} = e \to \bar{x} \in < b > \to x \in < b > \to x \in < a > \cap < b > \to x = e$. ☐

☐

Claim 6. $< a > K = G$.

Proof. This follows from an order argument, since $| < b > | = p$. ☐

Claim 7. $| < b > | = p$

Proof. Recall $b \in G/ < a >$ with minimal order. So, if we show there is some leement of order p which is in $G/ < a >$, then $|b| = p$, since all elements must have order greater than or equal to pp. Look at $|b^p| = |b|/p \to b^p \in< a >\to b^p = a^i$ for some i. Note that $p|i \to i = pq$ for some $q \in \mathbb{Z}$. Let $c \in G/ < a >= a^{-q}b$. Then we have $c^p = e$, since $a^{-qp}b^p = e$. Also note that $c \neq e$, and that $c \notin< a >$, since if $c = a^l$, then $a^{l+q} = b$. Then the order of b has to be p. ☐

With all of this, the lemma follows.

☐

Proof. (Proof of Theorem) By Corollary, $G \cong H_1 \times \ldots \times H_t$, where i has order of prime power.

Claim 8. *Every finite Abelian group G of order p^k is a product of cyclic groups of prime power order.*

Proof. If $|G| = p$ then this implies $G \cong \mathbb{Z}_p$. Otheriwse, if $|G| = p^K$, then by Lemma 2 $G \cong< a > \times K$, where $|K| = p^{k'}$, $K' < K$. By induction, $K \cong K_1 \times \ldots \times K_r$, where K_i are cyclic of prime power order. Therefore, we have $G \cong< a > \times K_1 \times \ldots \times K_r$.
If $G \cong H_1 \times \ldots \times H_r$ of prime power order, then each $H_i = H_i^{(1)} \times \ldots \times H_i^{(s_i)}$, where $H_i^{(j_i)}$ is a cyclic group of prime order. Then we have $G \cong H_1^{(1)} \times \ldots \times H_1^{(S_i)} \times \ldots \times H_r^{(1)} \times \ldots \times H_r^{(S_i)}$. ☐

☐

Example 11. *If we have a finite Abelian group of order 8, then the possible options are* $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Chapter 3

Rings (Day 20-27)

Rings will be done more heuristically. As such, there are not many sections to seperate this by.

Definition 3.0.1. (Ring) A set $(R, +, \times)$ is a ring if the following properties hold:

1. $+$ and $\times$ are laws of composition which are associative.
2. $(R, +, 0)$ is an Abelian group.
3. $\times$ has an identity denoted by $1 \in R$ when you restrict $R/\{0\}$.
4. The distributive property holds – i.e., $a, b, c \in R \to a \times (b+c) = ab + ac$ and $(b+c) \times a = ba + ca$.

Remark. *We will only be studying commutative rings – or rings in which multiplication is commutative.*

Example 12. *1. $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are all rings.*

2. $M_n(\mathbb{R}) = \{n \times n$ -values over $\mathbb{R}\}$ is a ring, but not a commutative ring.

3. $\mathbb{C}[x] = \{a_n x^n + \cdots + a_0$, where $a_i \in \mathbb{C}, n \geq 0\}$ (this is not just restricted to the complex numbers, but rather $\mathbb{Z}[x], \mathbb{R}[x]$, and $\mathbb{Q}[x]$ are all rings as well).

Lemma 19.3. *Let $(R, +, \times, 0, 1)$ be a ring.*

1. $0 \times a = 0$.
2. $(-1) \times a = -a$.
3. $-(-a) = a$.

Remark. *Note that the cancellation law holds for addition, but not necessarily for multiplication (we need to be over a field for this to be true).*

Proof. 1. We know that $(0+0)a = 0a$. Distributing gives us $0a + 0a = 0a$. By the cancellation law of addition, we then have $0a = 0$.

2. We know that $-a = (-a) + 0$. Note that this is equivalent to $-a = (-a) + (1 + (-1))a$. Distributing, we have $-a = -a + 1(a) + (-1)a$. By the multiplicative identity, we know that $1(a) = a$, and so we have $-a = -a + a(-1)a$. This results in $-a = (-1)a$.

3. $a = a + 0$, which is equivalent to $a = a + (-a + -(-a))$, and by the associative law we have $a = (a + (-a)) + (-(-a))$. Note that $(a + (-a) = 0$, and so we have $a = (-(-a))$

□

Definition 3.0.2. (Integral Domain) A ring R is an integral domain if for all $a \in R/\{0\}$, $b, c \in R$, if $ab = ac \to b = c$. Equivalently, we have that if $ab = 0$, then either $a = 0$ or $b = 0$.

Example 13. *We have that $\mathbb{Z}$ is an integral domain.*

Remark. *A field is a ring, but with multiplicative inverses.*

Definition 3.0.3. (Subring) If R is a ring, then a subset $R' \subset R$ is a subring if

1. It's closed under addition and multiplication.
2. $0, 1 \in R'$
3. If $r \in R'$, then $-r \in R'$, where $-r$ denotes the additive inverse.

Lemma 19.4. *A subring R' is a ring with the induced $+, 0, \times, 1$, etc.*

Lemma 19.5. $(R_1 \times \cdots \times R_n, +, \times, (1_1, \ldots, 1_n), (0_1, \ldots, 0_n))$ *is a ring.*

Definition 3.0.4. (Polynomial Ring) Given a ring R we define the polynomial ring of R to be $R[x]$, where

$$R[x] = \{p_m x^m + \ldots + p_1 x^1 + p_0 \mid p \in R$$

Definition 3.0.5. (Ideal) An ideal $I \subset R$ is an additive subgroup such that if $a \in I$ then $ra \in I$ for all $r \in R$.

Lemma 19.6. *If $1 \in I$, then $I = R$*

Proof. If $1 \in I$, then since it's an ideal we have $a(1) \in I$ for all $a \in R$. However, this means that $R \subset I$, and it's given that $I \subset R$, so we have $I = R$. □

Lemma 19.7. $(\alpha_1, \ldots, \alpha_k)$ *is an ideal in R.*

Proof. $0^k \in (\alpha_1, \ldots, \alpha_k)$ trivially, and the additive inverse is also clear.
Note that $r_1\alpha_1 + \cdots + r_k\alpha_k + s_1\alpha_1 + \cdots + s_k\alpha_k = (r_1 + s_1)\alpha_1 + \cdots + (r_k + s_k)\alpha_k \in (\alpha_1, \ldots, \alpha_k)$.
Thus, the ideal property is clear by construction. □

Definition 3.0.6. (Ring Homomorphism) A function $f : R \to R'$ is a ring homomorphism if

1. f is a group homomorphism; i.e. $f(R, +) \to (R', +)$ such that $f(a + b) = f(a) + f(b)$, $f(0) = 0$.
2. $f(1) = 1$ and $f(ab) = f(a)f(b)$.

Definition 3.0.7. (Ring Isomorphism) A ring isomorphism is a bijective ring homomorphism

Lemma 19.8. *If $f : R \to R'$ is a ring homomorphism, then $\ker(f)$ is an ideal.*

Theorem 20. *If R is a ring, and $I \subset R$ is an ideal, then $(R/I, +, \times)$ is a ring.*

Proof. It's left as an exercise, though all that really needs to be done is to check that multiplication is well defined. □

Theorem 21. *Let $\phi : R_1 \to R_2$ be a surjective ring homomorphism. Then the induced map $\bar{\phi} : R_1/I \to R_2$ is an isomorphism. (Note: $I = \ker(\phi)$.*

Remark. *This derives from the Fundamental Group Homomorphism Theorem.*

Lemma 21.1. *(Polynomial Rings) Let R be a ring such that R is an integral domain. Then $R[x]$ is an integral domain.*

Proof. IF $f, g \in R[x]$, $f \neq 0, g \neq 0$, then $fg \neq 0$. If $f, g \neq 0$, then note $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + x b_0$, where $a_n, b_m \neq 0$. Then this implies that $f(x)g(x) = a_n b_m x^{n+m} + \cdots$. Since $a_n \neq 0$ and $b_m \neq 0$, then $a_n b_m \neq 0$ since we're in an integral domain. □

Definition 3.0.8. (Unit) An element of R is a unit if it has a multiplicative inverse.

Definition 3.0.9. (Factors of a Polynomial) Given $f, g \in R[x]$, we say that $g|f$ if there exists $h \in R[x]$ such that $f = gh$.

Corollary 21.1. *Let $f \in F[x]$.*

1. *$f(a)$ is the remainder of $f(x)|(x - a)$ for any $a \in F$.*

2. *If $f(a) = 0$, then $x - a$ divides $f(x)$*

3. *If deg$(f) - n$ and $f \neq 0$, then $f(x)$ has at most n-zeroes.*

Proof. 1. Consider $f(x) - f(a) \in F[x]$. By the division algorithm, we know $f(x) - f(a0 = g(x)(x - a) + r(x)$. If one set $x = a$, we have $0 = r(a)$. THerefore, $r(x) = 0$, so therefore we have $f(x) - f(a) = g(x)(x - a)$. Adding $f(a)$ to both sides then gives $f(x) = g(x)(x - a) + f(a)$. Therefore, the remainder is $f(a)$.

2. By (1), if $f(a0 = 0$ then $f(x) = g(x)(x - a)$ which implies $(x - a)|f(x)$.

3. IF $a_1, \ldots, a_{n+1}$ are unique zeroes, then $(x - a_1) \cdots (x - a_{n+1})|f(x)$, a contradiction.

□

Lemma 21.2. *Any unit $u(x) \in F[x]$ is a non-zero constant polynomial.*

Proof. Suppose $u(x) \in F[x]$ is a unit. Then $u(x)u^{-1}(x) = 1 \to \deg(u(x)) + \deg(u^{-1}(x)) = 0$. However, the degree is greater than or equal to zero, and so this implies that $\deg(u(x)) = \deg(u^{-1}(x)) = 0$. □

Definition 3.0.10. (Associates) We say that $f, g \in F[x]$ are associates if there exists a unit such that $f = ug$.

Definition 3.0.11. (Monic Polynomial) A monic polynomial is a polynomial whose leading coefficient is 1.

Remark. *For every polynomial there is an associated polynomial which is monic. We can note that this associated monic polynomial is unique.*

Definition 3.0.12. (GCD of Polynomials) If $f, g \in F[x]$, and $f, g \neq 0$, then $\gcd(f, g)$ is a polynomial $d \in F[x]$ such that

1. $d|f$, dg

2. If $k|f$ and $k|g$, then $k|d$

3. d is monic.

Remark. *If $a|b$ and $b|a$, then we cannot say $a = b$, since this is true if they are associated. If they were monic, though, then $a = b$.*

Definition 3.0.13. (Principal Ideal Domain) A principal ideal domain is an integral domain R such that every ideal in R is principal; i.e., $I \in R$ implies $I = (a)$ for some $a \in R$.

Theorem 22. *$F[x]$ is a principal ideal domain.*

Proof. Let $I \subset F[x]$. If $I = \{0\}$, there's nothing to show. Suppose $I \neq \{0\}$. Observe $S = \{n \in \mathbb{Z}_{>0} \mid \exists p(x) \text{ of } \deg p = n \text{ in } I\}$. Then there exists a polynomial, d, of minimal positive degree in I. Note that $d \in I$ implies $(d) \subset I$.

Claim 9. *$I \subset (d)$.*

Proof. Assume for contradiction that there is a $f \in I/(d)$. Applying the division algorithm, we have $f = qd + r$, which implies $r = f - qd$. However, f and $qd \in I$, which means that $r \in I$. So we found something of smaller degree in I, which is a contradiction. □

□

Theorem 23. *For $f, g \in F[x]$, the gcd exists and is unique*

Proof. Using the prior theorem, we have $(f) + (g) = (f, g) \to (f, g) = (d)$. Let the gcd be the unique monic polynomial generating (d). Then one may establish that this has all the properties of the gcd. □

Definition 3.0.14. (Irreducibility) Let D be an integral domain. A polynomial $f(x) \in D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(xx)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called reducible over D. In the case that an integral domain is a field F, it is equivalent and more convenient to define a nonconstant $f(x) \in F(x)$ to be irreducible if $f(x)$ cannot be expressed as a product of two polynomials of lower degree.

Lemma 23.1. *Let F be a field. If $f(x) \in F[x]$ and $deg(f(x)) = 2, 3$, then $f(x)$ is said to be reducible over F if and only if $f(x)$ has a zero (or root) in F.*

Lemma 23.2. *$p(\frac{s}{t}) = 0$ implies $s|a_0$ and $t|a_n$, where $p(x) = a_n x^n + \cdots + a_0$. In other words, all rational roots of a polynomial are of the form s/t, where $s|a_0$ and $t|a_n$.*

Remark. *The proof is not really worth knowing.*

Theorem 24. *Let $f(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$ for $h, g \in \mathbb{Q}[x]$. Then there exists $G(X), H(X) \in \mathbb{Z}[x]$ such that $f(x) = G(X)H(X)$.*

Remark. *Once again, I feel like the proof does not give any insight to the theorem.*

Theorem 25. *Let $f(x) \in \mathbb{Z}[x]$ which is monic. Suppose there exists p a prime such that $f(x) \in \mathbb{Z}_p[x]$ is irreducible. Then $f(x)$ is irreducible.*

Proof. If $f(x) = g(x)h(x) \in \mathbb{Z}[x]$ then we have $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$. □

Example 14. *SHow that $x^4 + 10x^2 + 7 = f(x)$ is irreducible.*
We can map this to $\mathbb{Z}_5[x]$ to get $x^4 + 7$. Then we can note that $x^4 + 7$ is irreducible in $\mathbb{Z}_5[x]$.

Lemma 25.1. *Suppose $f(x) \in \mathbb{Z}[x]$ and $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$. If $p|a_i$ for all i, then $p|b_i$ for all i or $p|c_i$ for all i (here, a_i denotes coefficients of f, b_i denotes coefficients of g, and c_i denotes coefficients of h).*

Proof. Suppose $p \nmid$ all b_i or c_i. THen there is some largest b_t or c_t suc hthat $b \nmid b_t$ or c_t. Let b_t and c_s denote these values, respectively. Then ovserve $a_{t+s} = b_0 c_{s+t} + \cdots + b_{s+t} c_0$. Note that all of these values are of the form $b_i c_j$. If $i < t$ then $p|b_i c_j$, if $j < s$ then $p|b_i c_j$ and thus p divides all the coefficients on the right hand side except $b \in c_s$. Let $h = b_t c_s$. THen this implies $p|h$ which implies $p|b_t$ or $p|c_s$, which is a contradiction. □

Theorem 26. *(Eisenstein's Criteria) Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and p a prime such that $p \nmid a_n$, $p|a_i$ for all $i \neq n$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible.*

Example 15. *Let $f(x) = x^{p-1} + \cdots + 1$. Then by the geometric sum (see: Probability Notes) we have $f(x) = \frac{x^p - 1}{x - 1}$. Substituting $x = y + 1$, we have $\frac{(y+1)^{p-1} - 1}{y}$. Using the binomial formula, we have $y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + \binom{p}{p-1}$, which satisfies Eisensteins criteria.*

Definition 3.0.15. (Primitive) A polynomial $f(x) = a_0 + a_1 x^1 + \cdots + x^n \in \mathbb{Z}[x]$ is called primitive if the gcd of all its coefficients is 1.

Lemma 26.1. *(Gauss's Lemma) If $f, g \in \mathbb{Z}[x]$ are primitive, then so is fg.*