Abstract Algebra 110BH Sorta Quick (Ok, maybe not)

Andrew Nguyen

April 7, 2005

Of course, we need to give credit where it's due. Professor Elman taught our 110BH class, and so these proofs are styled after him. Any mistakes, of course, are mine alone. But I hope you enjoy reading all this!

Note: Things I proved I proved rigerously. A few things I didn't prove because they were long or the proofs were hard to typeset or whatever. However, I didn't write "formally". I (try to) crack jokes here and there. Hopefully it isn't boring! And I hope you enjoy my music rants. =)

For this class, we don't need to know anything from Chapter 6. But please scan through it. Those commutative diagrams took a lot of work! =P

And most importantly: did I really screw something up? E-mail me! annguyen@ucla.edu

Contents

Chapter 1

Ring Basics

Hint: It's not about getting married.

1.1 Quick Stuff

1.1.1 What's a Ring?

Definition 1.1.1. *A ring R is a set of mathematical objects in which we have certain binary operations (binary meaning that we get to stay within the set), usually denoted by $\cdot$ and $+$. Actually, we can even be more general, as these operations are actually maps that take two ojects in the ring back to the ring. Let's write it like this:*

$$+ : (R, R) \to R \stackrel{def}{=} r + r = r'$$

$$\cdot : (R, R) \to R \stackrel{def}{=} r \cdot r = r'$$

Of course, our operations need certain properties. For addition ($+$), we have essentially an additive (abelian) group:

1. $(a + b) + c = a + (b + c)$
2. $\exists 0$ *s.t.* $a + 0 = a = 0 + a$
3. $\forall a, \exists (-a)$ *s.t.* $a + (-a) = 0 = (-a) + a$
4. $a + b = b + a$

For multiplication ($\cdot$), we have similar stuff, except we're not guaranteed an inverse, or even commutivity:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $\exists 1$ *s.t.* $a \cdot 1 = a = 1 \cdot a$

1.1.2 Types of Rings

Yay! Now we know what rings are. Of course, we can do better if our rings were actually a bit more behaved.

Division Rings are rings in which each element (except zero) has an inverse. Remember, multiplication may not be commutative, so our inverses may be only one-way.

Commutative Rings are the ones in which multiplication commutes.

Domains are commutative rings in which $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

Lemma 1.1.1. *In a domain, if $a \neq 0$ then $a \cdot x = a \cdot y \Leftrightarrow x = y$.*

Proof. $a \cdot x = a \cdot y \Leftrightarrow a \cdot x - a \cdot y = 0 \Leftrightarrow a \cdot (x - y) = 0 \Leftrightarrow x - y = 0$ (as $a \neq 0$) $\Leftrightarrow x = y$ □

Fields are commutative division rings! So every element has an inverse (except zero) and commutes. Also, notice that fields are automatically domains! ¿Por qué? you might ask.

Lemma 1.1.2. *Fields are Domains*

Proof. Suppose we have $ab = 0$. If $a \neq 0$ we have: $a \in R$ a field, $a \neq 0 \Rightarrow \exists a^{-1}$ s.t. $a \cdot a^{-1} \cdot a = a \cdot a^{-1} = 1$. Observe: $a^{-1} \cdot a \cdot b = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0$ □

1.1.3 Units

Something cewl: if you take any ring R and just look at the stuff with a multiplicative inverse, it's a multiplicative ring. We denote this stuff with $R^\times$.

1.1.4 Homomorphisms, Isomorphisms, and Friends

Now, because I'm new to LaTeX (I'm doing this to practice on it) and I'm really annoyed with typing `\cdot` each time I want the multiplication sign ($\cdot$), I'm going to assume implicit multiplication ($a \cdot b \equiv ab$)

Homomorphisms are defined just as you would expect for a group, but they need to hold for both multiplication and division.

Definition 1.1.2. *$\varphi : R \to S$ is a ring homomorphism if:*

1. $\varphi(r + s) = \varphi(r) + \varphi(s)$
2. $\varphi(rs) = \varphi(r)\varphi(s)$

Of course, we have an epimorphism if the map is onto; it's a injection if it is 1-1, and it's an isomorphism if it's 1-1 and onto. Nothing really new.

1.2 Any Good Ideals?

1.2.1 The Whole Ideal

Now that we have rings and stuff, what's a convient sub-part of a ring? Well, one convient sub-part we can define is an ideal. In our class, we used these weird german characaters for these guys, for example, $\mathfrak{A}, \mathfrak{B}, \mathfrak{C} \ldots$. You get the point. So now, what's an ideal?

Definition 1.2.1 (Ideals)**.** *A subset $\mathfrak{A}$ of a ring R is an ideal if:*

1. $\forall a, b \in \mathfrak{A}, a + b \in \mathfrak{A}$
2. $\forall a \in \mathfrak{A}, \forall r \in R, ra \in \mathfrak{A}$

Actually, this is a left ideal; a right ideal means $ar \in \mathfrak{A}$. Of course if your ring is commutative, then $ar = ra$, so any left or right ideal is an ideal in its own right.

So why would we be interested in an ideal in the first place? Remember cosets from groups? They're sets in the form $x+N$. We can multiply two cosets together (in a multiplicative group) by $(x+N)(y+N) = xy+xN+yN+NN = (xy + N)$ (Ok, it's a little abuse of notation, but you get what I mean.) We could do this with normal subgroups, since we know $xN = N$ and $yN = N$, so $xN + yN + NN = N + N + N = N$.

If we have ideals, we can do the same thing with rings. $(x + \mathfrak{A})(y + \mathfrak{A}) = xy + x\mathfrak{A} + y\mathfrak{A} + \mathfrak{A}\mathfrak{A} = xy + \mathfrak{A}$

Lemma 1.2.1. *For ideals $\mathfrak{A}, \mathfrak{B}$ of R, $\mathfrak{A}\mathfrak{B}, \mathfrak{A} \cap \mathfrak{B}$, and $\mathfrak{A} + \mathfrak{B}$ are ideals. Also, $\mathfrak{A}\mathfrak{B} \subseteq \mathfrak{A} \cap \mathfrak{B} \subseteq \mathfrak{A} + \mathfrak{B}$.*

Proof. It's not hard, but it's annoying to typset. But I think it's pretty immediate. =P □

1.2.2 Generating Sets

In group theory, we had groups that could be generated by certain elements. We certainly have that with ideals! For an ideal to be generated by a single element a means:

$$\mathfrak{A} = \sum_{\text{finite}} r_i a s_i \text{ for some } r_i, s_i \in R$$

Of course, if we have a commutative ring this all simplifies to $\mathfrak{A} = Ra = \{s | s = ra, r \in R\}$. In any case, we write $\mathfrak{A} = (a)$.

For those ideals generated by a set $\{a_1, \ldots, a_n, \ldots\}$, we have:

$$\mathfrak{A} = \sum_{n}^{N} \sum_{i}^{K} r_i a_n s_i \text{ for some } r_i, s_i \in R$$

Once again, if we have a commutative ring, this all reduces to $\sum_{n=1}^{N} Ra_n$. And we write $\mathfrak{A} = (a_1, a_2, \ldots)$.

1.2.3 Ideals with Unit Generators

If an ideal contains a unit (elements with an inverse), our ideal becomes the whole ring! $u \in \mathfrak{A} \Rightarrow \{s|s = \sum r_i u\} \subseteq \mathfrak{A} \Rightarrow \{s|s = \sum (r_i u^{-1})u\} \subseteq \mathfrak{A}$. (Just relabel each r_i to be $r_i u^{-1}$.) Then ta-da! We can make any element in the whole ring that we want.

Definition 1.2.2 (Simple Rings)**.** *A simple ring is a ring in which the only ideals are the 0 ideal and the entire ring. Examples of simple rings include division rings and fields.*

Lemma 1.2.2. *A ring R is simple and commutative $\Leftrightarrow$ R is a field.*

Proof. Let $0 \neq a \in R$, a simple ring. $(a) \subseteq \mathfrak{A}$ But as $\mathfrak{A}$ is simple, $(a) = R$ So $\exists r \in R$ s.t. $ra = 1$. R is commutative $\Rightarrow ra = ar = 1$. So every non-zero element has a inverse (so it's a division ring). It's also commutative, so by definition, it's a field. For the converse direction, note that fields are simple (every non-zero element is a unit). Also, by definition, fields are commutative. □

1.2.4 More Ideal Stuff

Definition 1.2.3 (Principle Ideal Domains)**.** *If all the ideals of a (ring) domain R can be generated by a single element, we say R is a Principle Ideal Domain, apprviated PID.*

Studybreak! Random Fact: I am now listening to *There is no Arizona* by Jamie O'Neal. (Shiver © 2000 Mercury Records). =)

OK, now we know what a PID is. We also want to introduce a notion of how elements can divide each other in a ring.

Definition 1.2.4. *An element a divides an element b in a ring R if $\exists c \in R$ s.t. $ac = b$. We say $a|b$.*

From the above definition we even get an equivalence class.

Lemma 1.2.3. *Let $a \sim b$ and if $a|b$ and $b|a$. And $\sim$ is an equivalence relation.*

Proof. It can't be that hard, can it? □

Lemma 1.2.4. *$a|b$ and $b|a \Leftrightarrow a = bu, u \in R^\times$*

Proof. $(a|b$ and $b|a) \Rightarrow (ax = b$ and $by = a) \Rightarrow (byx = b) \Rightarrow (yx = 1)$ so in particular, x is a unit. For the other direction, $(a = bu) \Rightarrow (au^{-1} = b)$. ($u^{-1}$ exists as $u \in R^\times$) □

Lemma 1.2.5. *$a|x \Leftrightarrow x \in (a) \Leftrightarrow (x) \subseteq (a)$ Also, $a|x$ and $a|y \Leftrightarrow (x, y) \subseteq (a)$*

Proof. Immediate □

Definition 1.2.5 (Prime Ideals)**.** *P is a prime ideal of R if $ab \in P \Rightarrow a \in P$ or $b \in P$*

A quick note! Note how this fits our notion of a prime number. A number p is prime if $p|ab \Rightarrow p|a$ or $p|b$ which then means that if $(a,b) \in (p) \Rightarrow (a) \subseteq (p)$ or $(b) \subseteq (p)$. (Just think about it for a while.)

Definition 1.2.6 (Maximal Ideals)**.** *An ideal $\mathfrak{M}$ is maximal if $\nexists$ ideal $\mathfrak{A}$ s.t. $\mathfrak{M} \subsetneq \mathfrak{A} \subsetneq R$*

Lemma 1.2.6. *Maximal ideals are prime ideals.*

Proof. Given $\mathfrak{M}$ maximal. Suppose $ab \in \mathfrak{M}$. We need $a \in \mathfrak{M}$ or $b \in \mathfrak{M}$. Suppose $a \notin \mathfrak{M}$. Note the ideal $(a) + \mathfrak{M} = R$. So $ax + my = 1$, some $x, y \in R$. Then $abx + mby = b$. $abx \in \mathfrak{M}, mby \in \mathfrak{M}$, so $b \in \mathfrak{M}$. □

Lemma 1.2.7. *Prime Ideals of a PID are Maximal*

Proof. Let P be a prime ideal of a PID R. Suppose we have $P \subsetneq \mathfrak{A} \subseteq R$. As we are in a PID, we have $(p) \subsetneq (a) \subseteq R$. $p \in (a)$, so $p = ax$, and $ax \in P$. P prime, so $a \in P$ or $x \in P$. As $a \notin P$ (else $\mathfrak{A} = P$), then $x \in P$. So $x = py$. So substuting, we have $p = apy$. As we are in a domain, $1 = ay$. So $a \in R^\times$, and $\mathfrak{A} = (a) = R$. □

1.2.5 Quotient Rings!

Just as we used (normal) subgroups to define quotient groups in group theory, we'll be pulling off the same old trick here. Lets start with some "mod" notation.

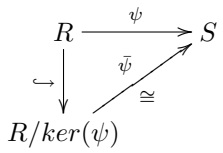
Definition 1.2.7. *$a \equiv b \bmod \mathfrak{A}$ if $a - b \in \mathfrak{A}$. We define $\bar{a}$ to be the set of all b s.t. the previous relation holds. These are kinda like "cosets." That is, $\bar{a} \stackrel{def}{=} a + \mathfrak{A}$. Of course, it's not hard to show that this is an equivalence relation.*

And we also have well-defined addition and multiplication of the representitives.

Definition 1.2.8. *$\bar{a} + \bar{b} \stackrel{def}{=} \overline{a+b}$, and $\bar{a} \cdot \bar{b} \stackrel{def}{=} \overline{a \cdot b}$*

And now we get our world famous isomorphism theorems! Yay!

Theorem 1.2.1 (First Isomorphism Theorem for Rings)**.** *Let $\psi : R \to S$ be a ring epimorphism from R to S (aka a onto ring homomorphism). Then we have the following commutative diagram:*



Where $\bar{\psi}(\bar{x}) \stackrel{def}{=} \psi(x)$
Yay! My first commutative diagram! But if you don't like commutative diagrams, then you can live with this: $R/ker(\psi) \cong S$

Proof. We need to show that $\bar{\psi} : R/ker(\psi) \to S$ is well defined, 1-1, and onto. Well defined: Given $\bar{a} = \bar{b}$, we have $a = b + k, k \in ker(\psi)$. Then $\bar{\psi}(\bar{a}) \stackrel{def}{=} \psi(a) = \psi(b + k) = \psi(b) + \psi(k) = \psi(b) \stackrel{def}{=} \bar{\psi}(\bar{b})$. We have 1-1 by $\bar{\psi}(\bar{x}) = 0 \Rightarrow \psi(x) = 0 \Rightarrow x \in \ker(\psi) \Rightarrow \bar{x} \stackrel{def}{=} x + \ker\psi = 0 + \ker\psi \stackrel{def}{=} \bar{0}$. We have onto by the fact that ψ is onto. □

Theorem 1.2.2 (Second Isomorphism Theorem for Rings)**.** *Given ideals $\mathfrak{A}$ and $\mathfrak{B}$ of ring R, we have $(\mathfrak{A} + \mathfrak{B})/\mathfrak{A} \cong \mathfrak{A}/(\mathfrak{A} \cap \mathfrak{B})$*

Proof. I'll put it in one day. No one ever really uses this theorem! □

Theorem 1.2.3 (Third Isomorphism Theorem for Rings)**.** *Given ideals $\mathfrak{A}, \mathfrak{B}$ with $\mathfrak{A} \subseteq \mathfrak{B} \subseteq R$, we have $(R/\mathfrak{A})/(B/\mathfrak{A}) \cong R/\mathfrak{B}$*

Proof. This is just the first isomorphsim theorem, of course, applied to the map $f : R/\mathfrak{A} \to R/\mathfrak{B}$. □

Theorem 1.2.4 (Correspondence Theorem)**.** *Given an ideal $\mathfrak{A}$ of R and the set of ideals $\{\mathfrak{K} : \mathfrak{A} \subseteq \mathfrak{K}, K$ an ideal of $R\}$, and a homomorphism $f : R \to S$, we have that there is an injection from $\{\mathfrak{K} : \mathfrak{A} \subseteq \mathfrak{K}, \mathfrak{K}$ an ideal of $R\} \to R/f(\mathfrak{A})$. This injection is given by $\bar{f} : \mathfrak{X} \to \mathfrak{X}/\mathfrak{A}$.*

Proof. Omitted for now! □

Corollary 1.2.1. *Let R be a commutative ring. $R/\mathfrak{A}$ is a field $\Leftrightarrow$ $\mathfrak{A}$ is a maximal ideal.*

Proof. We will use the Correspondence Theorem and Lemma **??**. Notice $R/\mathfrak{A}$ is commutative. The Correspondence Theorem tells us that the only ideals of $R/\mathfrak{A}$ are $\bar{0} = \mathfrak{A}/\mathfrak{A}$ and the entire ring $R/\mathfrak{A}$. Thus $R/\mathfrak{A}$ is simple. Thus as it is simple and commutative, it is a field (Lemma **??**). For the reverse direction, if $R/\mathfrak{A}$ is a field, it is simple and commutative, and again by the Correspondence Theorem, the only ideals are $\bar{0} = \mathfrak{A}/\mathfrak{A}$ and $R/\mathfrak{A}$. There are no proper ideals larger than $\mathfrak{A}$, so $\mathfrak{A}$ is maximal. □

Corollary 1.2.2. *$R/\mathfrak{A}$ is a domain ideal $\Leftrightarrow$ $\mathfrak{A}$ is a prime ideal.*

Proof. $R/\mathfrak{A}$ is a domain. Suppose $ab \in \mathfrak{A}$ (that is, $\bar{a}\bar{b} = \bar{0}$). Then ($\bar{a}\bar{b} = \bar{0} \Rightarrow$ $a = \bar{0}$ or $b = \bar{0}$) $\Leftrightarrow$ ($a \in \mathfrak{A}$ or $b \in \mathfrak{A}$) $\Leftrightarrow$ $\mathfrak{A}$ is prime. □

Hey! We haven't done anything stupid for a while. Here's a (hopefully) funny joke.
Q: What would a logician choose, a half egg or eternal bliss in the afterlife?
A: A half egg of course! Nothing is better than eternal bliss in the afterlife, and a half egg is better than nothing! =P

Chapter 2

Advanced Ring Structure

2.1 Characteristic

Ah, yes. We're looking for a few good rings, rings with character. =) Well, actually, as we'll see, every ring has a characteristic value.

Definition 2.1.1 (Characteristic)**.** *For $n \in \mathbb{Z}$, and $1_R \in R$ be the "one" element (the multiplicative identity.) We define $n \cdot 1_R \stackrel{def}{=} \underbrace{1_R + \cdots + 1 + R}_{n \text{ times}}$ The characteristic of a function is the smallest n s.t. $n \cdot 1_R = 0_R$. If there is no (finite) n s.t. this is true, we say that the ring has characteristic 0.*

This is actually something really cool. I mean, our ring elements might not even be numbers, right? But right away, we know what some ring elements look like! Actually, lets look at this some more.

Lemma 2.1.1. *If a ring R has characteristic n, then $(n) = 0$, and $\mathbb{Z}/n\mathbb{Z} \hookrightarrow R$.*

Proof. This is immediate. Note also if the ring has characteristic zero, then $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z} \hookrightarrow R$. □

Lemma 2.1.2. *If a ring R is a domain, then either it has characteristic 0 or charistic p, for some prime $p \in \mathbb{N}$.*

Proof. Suppose domain R has non-zero characteristic. Then $\mathbb{Z}/n\mathbb{Z} \hookrightarrow R$. If n is not prime, then we have $ab = n$, so $\bar{a}\bar{b} = \bar{n} = 0$. This also isomorphically occurs in domain R, a contradition. So n is prime. □

So now that we added some integers to our rings, what's the chance that we could have "rational" ring elements somewhere (as in rational numbers)? Actually, we can do even better! We don't even need characteristic, as we're going to make our "fractional" elements from ring elements themselves! Of course, we will get a "bigger" ring. (You'll see what I mean.) First, we need a new structure. (Very easy.)

Definition 2.1.2 (Multiplicative Set)**.** *$S \subseteq R$ is a multiplicative set if $\forall a, b \in S, ab \in S$. That is, it's closed under multiplication. That's it!*

Now let's make an equivalence class.

Definition 2.1.3. *Let R be a ring, $0 \notin S \subseteq R$ a multiplicative set. Define $(r, s) \in R \times S$. So we have a "cartesian product" of sorts. Define $(r_1, s_1) \sim (r_2, s_2)$ if $r_1 s_2 - s_1 r_2 = 0$. It's not hard to show that this is an equivalence relation. So let's call the representatives of our equivalence classes something familiar. For the equivalence class represented by (r_1, s_1), we'll call it $\frac{r_1}{s_1}$.*

This should start looking like fractions! Note that we defined $\frac{r_1}{s_1} = \frac{r_2}{s_2} \Leftrightarrow r_1 s_2 - s_1 r_2 = 0$, just as we would expect for fractions!

Then how does addition and multiplication work? The same as in fractions!

Definition 2.1.4. *Define $(r_1, s_1) + (r_2, s_2) \stackrel{def}{=} (r_1 s_2 + r_2 s_1, s_1 s_2)$ and $(r_1, s_1) \cdot (r_2, s_2) \stackrel{def}{=} (r_1 r_2, s_1 s_2)$.*

Or, with the fraction notation with coset representatives, $\frac{r_1}{s_1} + \frac{r_2}{s_2} \stackrel{def}{=} \frac{r_1 s_2 + s_1 r_2}{s_1 s_2}$ and $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} \stackrel{def}{=} \frac{r_1 r_2}{s_1 s_2}$

Lemma 2.1.3 (Localization)**.** *Under the above definitions and operations, the "fractions" of ring elements is itself a ring, a construction we call localization. (We denote this as $S^{-1}R$.)*

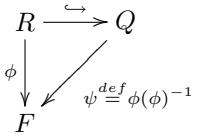
Proof. We just need to show that addition and multiplication are well defined and satisfy the ring axioms. This isn't hard to check. (Translation: it is 12:03 AM and I want to go to sleep.) □

Just a quick note: If $S = R \backslash 0$, Then $S^{-1}R$ is called the quotient field of R. And of course, $R \hookrightarrow Q$, via $r \to \frac{r}{1}$.

So lets sum up what we have! We've now have a way for turning a ring into a field! It's by forming "fractions" from the ring elements. This new bigger ring is called the quotient field.

Now we'll take a twist on this and see what we can do with quotient fields.

Theorem 2.1.1 (Universal Property of Factor Modules)**.** *If there exists an injection $\phi : R \to F$, R a ring and F a field, then there exists an injection ψ from the quotient field Q of R to F In particular, $\psi\left(\frac{a}{b}\right) = \phi(a)(\phi(b))^{-1}$. In terms of commutative diagrams, we have*



Proof. Well, we know ψ certainly exists as ϕ and $(\phi)^{-1}$) exist. (Recall F is a field, so every little guy has an inverse, except zero.) ψ is well defined as ϕ is well defined. And it's an injection: $\psi\left(\frac{a}{b}\right) = \phi(a)(\phi(b))^{-1} = 0 \Rightarrow \phi(a) = 0$ or $(\phi(b))^{-1} = 0$ (F is a field is a domain.) As $(\psi(b))^{-1} \neq 0$ (Recall ψ is an injection and $b \neq 0$), we have $\psi(a) = 0$. Again, ψ is an injection, so $a = 0$. Then $\frac{a}{b} = 0$. □

That's all fine and dandy, but what does it really mean? It's back to the characteristic stuff!

Corollary 2.1.1. *Let F be a field with characteristic 0. Then We have $\mathbb{Z} \hookrightarrow F$. Then we have the quotient field of $\mathbb{Z}$, aka $\mathbb{Q}$, isomorphically conatained in F.*

Proof. This really is an immediate corollary. □

Hey, we know a lot more now! If our field has characteristic 0, it contains the rationals in some sense!

Theorem 2.1.2 (Chinese Remainder Theorem)**.** *This is annoying to typset. Please look it up somewhere! I'll have this up one day.*

It's time for the song-I'm-listening-to-right-now. It's *Breakaway* by Kelly Clarkson. (Breakaway © 2004 Walt Disney Records) (On a light rock station.)

And why not a joke?
Q: Why do mathematicians, after a dinner at a Chinese restaurant, always insist on taking the leftovers home?
A: Because they know the Chinese remainder theorem!

2.2 Edgar Allan Posets

Aka Partially Ordered Sets. OK, OK, Posets not that scary. (If you get the joke, you might be too artsy!)

2.2.1 What are Partially Ordered Sets?

Definition 2.2.1 (Partially Ordered Sets)**.** *A set of objects S with a relation r is called a poset if $\forall A, B, C \in S$, the following axioms hold:*

1. *ArA*
2. *ArB and $BrA \Rightarrow A = B$*
3. *ArB and $BrC \Rightarrow ArC$*

This might look suspiciously like an equivalence relation, and it's very similar, except that axiom 2 is a little twisted. If you're not sure what's happening, replace "r" by "$\subseteq$". Sets under "$\subseteq$" form a poset. Another example is $\mathbb{Z}$ under "$\geq$". All of these objects are "partially ordered," and hence posets. For the second example, it's even better than partially ordered–it's well ordered!

Definition 2.2.2 (Comparable)**.** *Two elements A, B in a poset are comparable if ArB or BrA.*

Observe that if A and B are say, sets, and our relation $r \stackrel{def}{=} \subseteq$, it might not be true that $A \subseteq B$ or $B \subseteq A$.

Definition 2.2.3 (Chain)**.** *A chain is what it says it is–a chain of relations! Say, $ArBrCrD$.*

Definition 2.2.4 (Upper Bound)**.** *An element M is an upper bound for a poset S if $ArM \forall A \in S$*

Definition 2.2.5 (Inductive Posets)**.** *A poset is an inductive poset if every chain has an upper bound.*

Definition 2.2.6 (Maximal Element)**.** *An element N of a poset S is a maximal element if $NrA \Rightarrow N = A$.*

Maximal elements might make more sense if you think in terms of "$\subseteq$". A maximal N element is the "smallest upper bound," in some sense. So if the elements are comparable, then we automatically have $A \subseteq N$. So if $N \subseteq A$, we must have $N = A$ by axiom 2 of our poset axioms.

Axiom 2.2.1 (Zorn's Lemma)**.** *The chains of inductive posets contain a maximal element.*

It's a axiom. Don't ask me why it's called Zorn's *Lemma!* Now here's why we want Zorn's Lemma. We're hoping that maximal ideals exist! (Opps) I guess we didn't show that before. =P We showed some stuff with maximal ideals-they're prime, etc. It would be nice to know if they actually existed.

Lemma 2.2.1. *Maximal ideals exist.*

Proof. We need to show that ideals (or technically, the *set of ideals*) are inductive posets–that they're posets and that chains have a upper bound. The set of ideals are posets under "$\subseteq$." So let's show they're inductive. Let $\mathfrak{A}_1 \subseteq \mathfrak{A}_2 \subseteq \mathfrak{A}_3 \subseteq \ldots \subsetneq R$ be a chain. We need an upper-bound that is an ideal; consider $\bigcup_{i \in I} \mathfrak{A}_i$. This is certainly an ideal, as for any element $a, b \in \bigcup_{i \in I} \mathfrak{A}_i, a \in \mathfrak{A}_n, b \in \mathfrak{A}_m$, some n, m. Then $a + b \in \mathfrak{A}_{\max(n,m)} \subseteq \bigcup_{i \in I} \mathfrak{A}_i$. Similarly, for some $a \in \bigcup_{i \in I} \mathfrak{A}_i, a \in \mathfrak{A}_n \Rightarrow ra \in \mathfrak{A}_n \subseteq \bigcup_{i \in I} \mathfrak{A}_i$. $\bigcup_{i \in I} \mathfrak{A}_i \neq R$, else $1 \in \mathfrak{A}_n$, some n. Then $\mathfrak{A} = R$, but this is a contradiction as we said $\mathfrak{A}_i \subsetneq R$. And it's an upper bound by construction. So we're done! There exists a maximal element in the chain (and it's not the whole ring. I mean, the whole ring is an ideal. We knew that!) All the items in the chain are ideals, so this maximal element is a maximal ideal. □

Lemma 2.2.2. *If P is a prime ideal, then $\mathfrak{AB} \in P \Rightarrow \mathfrak{A} \in P$ or $\mathfrak{B} \in P$. In addition, if an ideal $\mathfrak{C}$ is not prime, $\exists \mathfrak{A} \supseteq P, \exists \mathfrak{B} \supseteq P$ s.t. $\mathfrak{AB} = P$.*

Proof. For the first part, let $\mathfrak{AB} \in P$. If $A \not\subseteq P$, then $\exists a_0 \in A$ s.t. $a_0 \notin P$. Note $a_0 b \in P \ \forall b \in \mathfrak{B}$. As P is a prime ideal, $b \in P$. For the second part, if $\mathfrak{C}$ is not prime, then $\exists a, b$ s.t. $ab \in \mathfrak{C}$ but $a, b \notin \mathfrak{C}$. Consider the ideals $(a) + \mathfrak{C}, (b) + \mathfrak{C}$. Observe: $[(a) + \mathfrak{C}] \cdot [(b) + \mathfrak{C}] = (a)(b) + (a)\mathfrak{C} + (b)\mathfrak{C} + \mathfrak{C}\mathfrak{C} = \mathfrak{C}$. □

Lemma 2.2.3 (Krull's Theorem)**.** *Let R be a ring, S a multiplicative set. Then $\exists M$, a maximal ideal relative to the condition that $M \cap S = 0$. M is also prime.*

Proof. This maximal M ideal relative to S certainly exists, using a proof very similar to our proof that maximal ideals in general exist. (Our chain would be restricted to $R \backslash S$). We just need to show it is prime. Suppose M is not prime. By our previous lemma, $\exists \mathfrak{A} \supset M, \exists \mathfrak{B} \supset M$ s.t. $\mathfrak{AB} = M$. M is maximal relative to avoiding S, so $\exists s_1 \in \mathfrak{A}, \exists s_2 \in \mathfrak{B}, s_1, s_2 \in S$. Note as $\mathfrak{AB} = M, s_1 s_2 \in M$ (and not in S). This is a contradiction, as S is a multiplicative set. □

And now finally, why we're doing all this! Lets characterize "nilpotent elements."

Definition 2.2.7. *An element r of ring R is nilpotent if $r^n = 0$ for some $n \in \mathbb{N}$. The set of nilpotent elements is denoted nil(R).*

Theorem 2.2.1. *$nil(R) = \bigcap_{P_i prime} P_i$ (ie, the intersection of all prime ideals.)*

Proof. $nil(R) \subseteq \bigcap_{P_i \text{prime}} P_i$, as $r^n = 0$, and $0 \in P_i \forall i$. (Note 0 is in every ideal!) Then as P_i are prime, $r \in P_i$. This holds $\forall i$, so done. For $\bigcap_{P_i \text{prime}} P_i \subseteq nil(R)$, suppose $\exists x \in \bigcap_{P_i \text{prime}} P_i \subseteq nil(R), x^n \neq 0 \ \forall n \in \mathbb{N}$. Note $\{x^k : k \in \mathbb{N}\}$ is a multiplicative set. We can choose a maximal ideal M (that is prime) and avoids the multiplicative set. Then $x \notin M$, a contradiction. □

Chapter 3

Irriducibles, Primes and Related Concepts

In the interest of time, I need to skip this. When I have time, I'll post it. If anybody wants to contribute, I'll be happy to stick it in. (With acknowledgements, of course!)

Chapter 4

Some Number Theory Results

In the interest of time, I need to skip this also. Sorry!

Chapter 5

Polynomial Rings

Now listening to: *Only Time* by Enya. (A Day Without Rain, 2000) (Actually, it's the remixed version; I don't know what album that's supposed to be. But I like the original better...)

5.1 What are Polynomial Rings?

Hey, what are polynomial rings? It's time for a definition!

Definition 5.1.1 (Polynomial Rings)**.** *A polynomial ring is exactly that! It's a ring with indeterminate powers of t with coefficients in R. It's denoted $R[t]$. Elements of $R[t]$ look like $a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ (Note the ring operations are the usual polynomial addition and multiplication.)*

and why not a second definition?

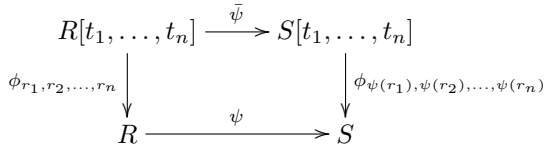
Definition 5.1.2 (Polynomial Rings with Multiple Variables)**.** *We define this inductively. $R[t_1, \ldots, t_{n+1}] = (R[t_1, \ldots, t_n])[t_{n+1}]$*

It might not be clear what's going on, and I didn't see it at first. But here's an example. An element of $R[t_1, t_2, t_3]$ looks like: $a(t_1)^2(t_3)^5 + b(t_1)^3(t_2)^4(t_3)^2$ See? We just have three indeterminates.

Lemma 5.1.1 (Evaluation Homomorphism)**.** *Let $r \in R$, R a ring. The map $\phi_r : R[t] \to R$ by $g(t) \to g(r)$ is a homomorphism. In fact, it's even onto, so its an epimorphism.*

Proof. This is actually pretty immediate! It's almost an observation. □

Theorem 5.1.1 (Evaluation Homomorphism)**.** *Given an evaluation homomorphism $\phi_{r_1, r_2, \ldots, r_n}$, and the ring homomorphism $\psi : R \to S$, we have the following commutative diagram:*



Where $\bar{\psi}$ acts on the coefficients of polynomials in $R[t]$.

Proof. This might look really intimidating, but don't worry! It LOOKS intimidating. Take out a piece of scratch paper and write out the case for only one indeterminate (aka one variable). As you see, it's a quick observation. □

Theorem 5.1.2. *Let F be a field. Then F[t] is an Euclidian Domain*

Proof. Sorry I'm writing so little. But hey! I have class also! The euclidian function is the degree of the polynomial, and it turns out you do your elementary polynomial division. I would write more, but it is a pain to type-set. (And I have some apps I need to work on.) □

There's more stuff that I can add, but this is enough for now. Hopefull I can attack it piece-meal over the next week or so.

Chapter 6

Module Basics

6.1 Quick Stuff

6.1.1 So What's a Module?

Time to define a module!

Definition 6.1.1. *A module is an additive (abelian) group M equipped with multiplication between the group elements and elements from a ring R, so that for $r \in R$ and $m \in M, r \cdot m \in M$. This is called a "R action," and satisfies the following axioms:*

1. $\forall r, s \in R$ *and* $m \in M, (r \cdot s) \cdot m = r \cdot (s \cdot m)$
2. $\forall r, s \in R$ *and* $m \in M, (r + s) \cdot m = r \cdot m + s \cdot m$
3. $\forall r, s \in R$ *and* $m \in M, m \cdot (r + s) = m \cdot r + m \cdot s$
4. $1_R \cdot m = m = m \cdot 1_R$

For short hand, we call M a R-Module, to denote what ring M is a module under.

Note a given abelian group can have different modules over different rings. Also, it might seem a little mysterious how this R Action this might work, but if it helps, we're headed towards vector spaces! For the common vector space of $\mathbb{R}^n$ over $\mathbb{R}$, we have multiplication from $\mathbb{R}$ into $\mathbb{R}^n$. FYI, a vector space is a type of module. The only additional requirement is that the ring R is a field. That's it!

Important Examples: Direct Products and Sums Let's talk about some examples of modules that we'll see quite a bit. They are the external direct product, the internal direct product, and the internal direct sum.

1. The external direct product is a cartesian product of (a possibly infinite number of) R-Modules, denoted $\prod_{i\in I} M_i = M_1 \prod \cdots \prod M_n \prod \cdots$ An element of $\prod_{i\in I} M_i$ is written as the tuple $(m_1, \cdots, m_n, \cdots)$, and is a module under component-wise operations.

2. The internal direct sum is similar to the external direct sum, but the restriction is there are only a finite number of non-zero terms. It is denoted $\coprod_{i\in I} M_i$, and is a subset of the internal direct product. It is, obviously, a module under componentwise operations.

3. Let M_i for some indexing set I be R-submodules of M s.t. $\left(\sum_{i\neq j} M_i\right) \cap M_j = 0$ Then $\sum_{i\in I} M_i$ is called a indirect sum, and is denoted $\bigoplus_{i\in I} M_i$. This is a module as M is a module. Note when we say sum, we mean finite sum.

Lemma 6.1.1. $\bigoplus_{i\in I} M_i \cong \coprod_{i\in I} M_i$

Proof. This actually isn't hard! Try it! □

Modules can also have generators, as we'll see:

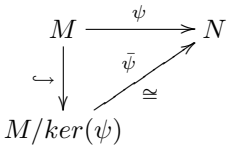
Definition 6.1.2 (Generators)**.** *A set $\{m_1, m_2, \cdots, m_n\}$ generates a R-module M if $M = R \cdot m_1 + R \cdot m_2 + \cdots + R \cdot m_n$. We say a module is cyclic if it has one generator.*

And we have homomorphisms just as we did in group theory and ring theory.

Definition 6.1.3 (Module Homomorphisms, Isomorphisms, Epimorphisms, and Injections)**.** *A map from R-modules M and N given by $\psi : M \to N$ is a ring homomorphism if $\psi(rm_1+m_2) = r\cdot\psi(m_1)+\psi(m_2)$. If ψ is 1-1, it is an injection; if ψ is onto, it is an epimorphism; if ψ is both an injection and epimorphism, we say it's an isomorphism.*

And of course, we have all the isomorphism theorems. The proofs are the same as in group theory. Note that all our submodules are subgroups, and since we're in an additive group, they're all normal.

Theorem 6.1.1 (First Isomorphism Theorem for Modules)**.** *Let $\psi : M \to N$ be a R-Module epimorphism from M to N (aka a onto module homomorphism). Then we have the following commutative diagram:*



Where $\bar{\psi}(\bar{x}) \stackrel{def}{=} \psi(x)$

Proof. It's the same as before. =) □

Theorem 6.1.2 (Second Isomorphism Theorem for Modules)**.** *Given submodules A and B of R-module M, we have $(A+B)/A \cong A/(A \cap B)$*

Proof. It's the same as before also! =) And again, no one really uses this. I think I've used all the variants of the Second Isomorphism Theorem twice in my entire life. □

Theorem 6.1.3 (Third Isomorphism Theorem for Modules)**.** *Given submodules A, B with $A \subseteq B \subseteq M$, we have $(M/A)/(B/A) \cong R/B$*

Proof. Don't worry, it's the same. =) □

Theorem 6.1.4 (Correspondence Theorem for Modules)**.** *Given a submodule A of M and the set of submodules $\{K : A \subseteq K, K$ a submodule of $M\}$, and a homomorphism $f : M \to N$, we have that there is an injection from $\{K : A \subseteq K, K$ a submodule of $R\} \to M/f(A)$. This injection is given by $\bar{f} : X \to X/A$.*

Proof. Guess what I'm going to say. □

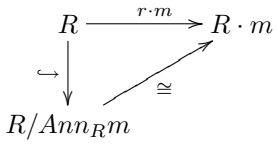
6.1.2 More Advanced Module Concepts

Definition 6.1.4 (Annihilators)**.** *The annhiliator of $m \in M$ is the set $\{r \in R : r \cdot m = 0\}$, and is denoted $Ann_R m$.*

A quick observation reveals that $Ann_R m$ is an ideal.

Lemma 6.1.2. *A R-module M is cyclic $\Leftrightarrow M \cong R/Ann_R m$, some $m \in M$.*

Proof. This really is the First Isomorphism Theorem.



Note the kernel of the map $\phi : r \to r \cdot m$ is, by definition, $Ann_R m$, so we have the above diagram. If we M is cyclic, then $M = R \cdot m$, some m, and we have $M = R \cdot m \cong R/Ann_R m$, as the above diagram shows. If $M \cong R/Ann_R m$, then as $R/Ann_R m = R \cdot m$, we have $M \cong R/Ann_R m. = R \cdot m$, so M is cyclic. □

We're going to introduce a concept that will help us down the road, called "zero sequences."

Definition 6.1.5 (Zero Sequences, Exact Sequences)**.** *A zero sequence is a diagram of module maps as shown below, such that the image of a preceeding map is contained in the kernel of the next map. If the image of the first map is precisely the kernel of the second map, it is termed a zero sequence.*

$$0 \overset{\hookrightarrow}{\to} A \overset{f}{\to} B \overset{g}{\to} C \overset{0 \cdot c}{\to} 0$$

A natural example of a exact (zero) sequence is:

$$0 \to Ker(f) \overset{\hookrightarrow}{\to} A \overset{f}{\to} Img(f) \to 0$$

Let's also introduce the concept of a free module.

Definition 6.1.6 (Free Modules)**.** *A free module is a module with a basis. We say the module is R-free, depending on the ring we're talking about.*

This might sound all nice and dandy, but free modules actually present some interesting issues, because many "nice" modules turn out to be not free! Here's a bunch of quick facts:

1. A cyclic module with generator m is R-free $\Leftrightarrow Ann_R m = 0$. (This is like linear independence with one vector.)
2. A finitely generated R-module is R-free $\Leftrightarrow$ it has a (finite) number of linearly-independent spanning vectors.
3. A R-module M is R-free $\Rightarrow |R| \leq |M|$. To see this, consider m a linearly independent vector in M. Note the kernel of the map $R \to R \cdot m$ is 0, so $R \hookrightarrow R \cdot m$ (So it's as if R was isomorphically contained in M).
4. $\mathbb{Q}$ is *not* $\mathbb{Z}$-free. Huh? It's a awful nice field! Why can't it be free? Turns out there are no two linearly independent vectors in $\mathbb{Q}$ (Note no one vector generates all of $\mathbb{Q}$. In fact, it's not finitely generated.), as given $\frac{a}{b}$ and $\frac{c}{d}$, $bc\frac{a}{b} - ad\frac{c}{d} = 0$
5. $\mathbb{Z}/6\mathbb{Z}$ is $\mathbb{Z}/6\mathbb{Z}$-Free (A linearly independent generator is $1_{\mathbb{Z}/6\mathbb{Z}}$, though $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are *not* $\mathbb{Z}/6\mathbb{Z}$-free (By the previous item, note that $|\mathbb{Z}/2\mathbb{Z}| \leq |\mathbb{Z}/6\mathbb{Z}|$ and $|\mathbb{Z}/3\mathbb{Z}| \leq |\mathbb{Z}/6\mathbb{Z}|$, so our module is smaller than the ring.) This is somewhat vexing, as $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
6. $\mathbb{Z}$ is $\mathbb{Z}$-free, with a generator of 1. (2) is also $\mathbb{Z}$-free, and the generator is 2. So a generator for a submodule doesen't have to be from the same set of generators of the module!

Rats! I guess this free business is not that much of a free lunch. But that's ok. Being free has a redeeming value, so so lets talk about it before we get too depressed. =P

Theorem 6.1.5 (Universal Property of Free Modules)**.** *Let N be a R-module. Let $\{m_1, \ldots, m_n\}$ be a basis for the free R-module M. Let there be an element map $\phi : M \to N$ by $m_i \to n_i$, some $n_i \in N$. Then ϕ extends to a homomorphism from $M \to N$.*

Proof. The proof is fairly immediate. I'll outline it because I'm going to see the musical *Evita* soon. =) But it's from this: $\phi(r_1 m_1 + \cdots + r_n m_n) \overset{def}{=} r_1\phi(m_1) + \cdots + r_n\phi(m_n)$. This is well defined as we have a basis for M (so we have unique representation). The fact that it is a homomorphism from all of M to N is immediate. □

Note we never claimed that the number of basis vectors was unique. It's certainly possible that a given R-Module might basis sets of different size! But we can be wishful that this isn't true. When basis vectors are well defined...

Definition 6.1.7 (Invariant Dimension Property and Rank)**.** *If M is a module that has a well defined basis set cardinality under ring R, we say that ring R satisfies the Invariant Dimension Property. The number of basis vectors is called the rank of R-Module M.*

Lemma 6.1.3. *A commutative ring satisfies the invariant dimension property.*

Proof. I'll prove this one day. =) □

6.2 Fundamental Theorem of Abelian Groups, Version 1

Now that we've had our intro to modules, and I'm back from the production of *Evita* (It was pretty cewl, actually), we're going to had towards some pretty heavy stuff. The Fundamental Theorem of Abelian Groups (abbreviated FTAG for us) is some pretty incredible machineary. We say "abelian groups" because we're dealing with modules, which are abelian groups (along with a ring). There really is a FTAG for truly "abelian groups," but it is a pretty trivial result from this more general theorem. (Let $\mathbb{Z}$ be your ring). But now it's Lemma Time! Sorry, not Miller Time. I'm a teatotaler anyway =)

6.2.1 Concepts Needed for FTAG 1

Theorem 6.2.1 (Smith Normal Form)**.** *Let A be a $n \times m$ matrix (ie, $\in M_{n\times m}$). Then $\exists B \in M_{n\times m}$ s.t. $B = PAQ$, some $P \in GL(M_{n\times n}), Q \in GL(M_{m\times m})$, and B is in Smith Normal Form. That is,*

$$B = \begin{pmatrix} d_1 & & & & \dots \\ & d_2 & & & \dots \\ & & d_3 & & \dots \\ \vdots & \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

With $d_1|d_2|\cdots|d_r, d_r \neq 0$ (Note all other entries are zero)
In short, B is a "diagonal matrix" (though it might not be a square matrix), with sucessive non-zero diagonal elements dividing each other. Moreover, B is unique relative to A!

Proof. There are a lot statements attached to that proof! I actually don't understand how it checks yet. The proof is quite long with a bunch of lemmas. So lets just believe it for now! =) □

Lemma 6.2.1. *Let R be a PID (It is commutative so it satisfies IDP). Let M be a free R-module of finite rank. Let N be a submodule of M. Then Rank(N) $\leq$ Rank(M).*

Proof. This proof is just a little long! Hold one! As M is free of finite rank (say n), we let $M = R^n = (R, R, \ldots, R)$. Construct the homomorphism $\phi : R^n \to R$, taking the first coordinate only. The kernel is the module $(0, R, \ldots, R)$, and is free of rank $n-1$. Then inductively, $Rank[Ker(\phi)] \leq n-1$. (that is, the rank of the kernel of the homomorphism restricted to N is inductively less-than or equal to n-1).

Consider the image of $\phi|_N$. The image is an ideal, and since we are in a PID, $Img(\phi|_N) = (a)$, some $a \in R$.

Lets notice some stuff about $R \cdot a = (a)$. Suppose $a \neq 0$. Note that $r \cdot a = 0 \Rightarrow r = 0$. ¿Por qué? We're in a domain! Yay! End of that!

Note also: as ϕ is onto R, we have $\phi : m \to a$, some $m \in M$. Lets show $R \cdot m$ is free of rank 1. Well, by definition, m generates $R \cdot m$. Is it linearly independent? $r \cdot m = 0 \Rightarrow \phi(r \cdot m) = \phi(0) = 0 \Rightarrow r \cdot a = 0 \Rightarrow r = 0$.

We're almost there! Case 1: a = 0. Then $N = Ker(\phi)$, so it's rank is n-1 or less.

Case 2, $a \neq 0$: Lets show $N = Ker(\phi) \bigoplus Rm$ We need that it spans N and that the intersection of the two sets is zero. Intersection is 0: Let $x \in Ker(\phi)$. Then $\phi(x) = 0$ As $x \in Rm, x = rm$ some $r \in R$. Then $\phi(rm) = r\phi(m) = r \cdot a = 0$. As $a \neq 0$ we have r=0. Then $x = r \cdot m = 0$.

For the spanning part, let $n \in N$ $\phi(n) \in (a), n = s \cdot a$, some $s \in R$ Then by the fact that ϕ is onto R, we have some $m \in M$ s.t. $\phi(m) = a$. Then $\phi(n - sm) = 0$. Then $n - sm \in Ker(\phi)$. Then $n = sm + k, k \in Ker(\phi)$. That's it! We have $N = R \cdot m \bigoplus Ker(\phi)$. This means that the rank is less than or equal to $[1 + (n-1)] = n$. □

Corollary 6.2.1. *Let M be finitely generated module over a PID. Then ∃ the exact sequence*

$$0 \to R^n \to R^m \to M \to 0.$$

With some n, m ∈ ℕ, and $n \leq m$, and R^n and R^m R-free.

Proof. This actually isn't bad! Let $\{m_1, \ldots, m_m\}$ be a spanning set for M. Then let $\{e_1, \cdots, e_m\}$ be the standard basis for R^m. Then let g be a set-map taking $e_i \to m_i$. Consider $Ker(g)$. By the previous proof, $Ker(g) = R^n$, some $n \leq m$. Now we have the exact sequence:

$$0 \to Ker(g) \overset{\hookrightarrow}{\to} R^m \overset{g}{\to} M \to 0.$$

Which is the same as:

$$0 \to R^n \overset{\hookrightarrow}{\to} R^m \overset{g}{\to} M \to 0.$$

□

6.2.2 FTAG Version 1

"It is time!" -Rafiki
(The baboon from Walt Disney's *The Lion King* (1994))

Theorem 6.2.2 (Fundamental Theorem of Abelian Groups, Version 1)**.** *Let M be a finitely generated R-module over a PID (ie, R is a PID). Then we have:*

$$M \cong R/d_1 \coprod R/d_2 \coprod \cdots \coprod R/d_n \coprod R^s$$

where $d_1|d_2|\cdots|d_n$. Note: We have broken our R module into cyclic components (The R/d_i's) and into a free part (the R^s). Also, the d_i's are called invariant factors.

Proof. We'll be using the lemmas above to prod us along. Let M be our R-module with a generating set of order n. We have the following exact sequence, with $m \leq n$:

$$0 \to R^m \xrightarrow{g} R^n \xrightarrow{h} M \to 0.$$

Let $S_m = \{e_1, \ldots, e_m\}$ and $S_n = \{f_1, \ldots, f_n\}$ be standard bases for R^m and R^n. Let $A = [g]_{S_m S_n} \in R^{n \times m}$. (It's the matrix that transfors R^m to R^n). Note by the Smith Normal Form theorem, $\exists\ B = PAQ, P \in GL_m$ and $Q \in GL_n$, B in Smith Normal Form. (ie, A is similar to a (unique) matrix in SNF.) Let:

$$B = \begin{pmatrix} d_1 & & & & \cdots \\ & d_2 & & & \cdots \\ & & d_3 & & \cdots \\ \vdots & \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

With $d_1|d_2|\cdots|d_r, d_r \neq 0$ (Note all other entries are zero.)

Then we have the following commutative diagram (with subscripts representing the change of basis) (and remember B=PAQ):

$$\begin{array}{ccc} [R^n]_{S_m} & \xrightarrow{A_{S_n S_m}} & [R^n]_{S_n} \\ \downarrow{\scriptstyle P^{-1}} & & \downarrow{\scriptstyle Q} \\ [R^n]_\beta & \xrightarrow{B_{\beta\gamma}} & [R^n]_\gamma \end{array}$$

Note β is the ordered basis given by $\{P^{-1}e_1, \ldots, P^{-1}e_n\}$, and γ is the ordered basis given by $\{Qf_1, \ldots, Qf_m\}$. In other words, P^{-1} is a change of basis matrix between $[R^n]_{S_m}$ and $[R^n]_\beta$; Q is a change of basis matrix between $[R^n]_{S_n}$ and $[R^n]_\gamma$.

Let's give a name to those vectors in the basis sets β and γ. $\beta = \{v_1, \cdots, v_m\}$, $\gamma = \{w_1, \cdots, w_n\}$, with (by definition of matrix multiplication) $v_j = \sum_{j=1}^m P_{ij}^{-1} e_j$, $w_j = \sum_{j=1}^m Q_{ij} e_j$.

Just some notation: Note that in our smith normal form (the matrix B), all the elements are zero except for the first handful of elements on the diagonal. (the d_i's). So to make life easier, we'll let $d_i = 0$ for $i > r$. Also, for these values, lets let g_i be the zero function and v_i be the zero vector.That way, we can say ($\forall$ i):

$$g(v_i) = d_i w_i, \text{ with } g : Rv_i \to Rw_i$$

Now we can say

$$\begin{array}{ccc} R^m & \xrightarrow{g} & R^n \\ \downarrow{=} & & \downarrow{=} \\ \bigoplus_{i=1}^m Rv_i & \xrightarrow{\bigoplus g_i} & \bigoplus_{i=1}^n Rw_i \end{array}$$

We've talked about the map g a lot. It's time to put $h : R^n \to M$ into the spotlight. Let $m_i = h(w_i)$ (Note this spans M as we got the W_i's from $Q(f_i)$, Q a isomorphism–it's in $GL_{n\times n}$–and the f_i's mapped to a spanning set of M.) We have $Rw_i \to Rm_i$, and we can write:

$$\begin{array}{ccc} R^n & \xrightarrow{h} & M \\ \downarrow{=} & & \downarrow{=} \\ \bigoplus_{i=1}^n Rw_i & \xrightarrow{\bigoplus h_i} & M \end{array}$$

We now have this exact sequence $\forall i$:

$$0 \to Rv_i \xrightarrow{g_i} Rw_i \xrightarrow{h_i} Rm_i \to 0$$

Recall that there might be more w_i's than v_i's, but we're extending the v_i's by making some more "zeroes." That way we can make the statement $\forall i$.

We now have this massive (at least for me) commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^m & \xrightarrow{g} & R^n & \xrightarrow{h} & M & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow{=} & & & & \\ 0 & \longrightarrow & \bigoplus Rv_i & \longrightarrow & \bigoplus Rw_i & & \downarrow{\cong (*)} & & \\ & & \downarrow{\cong} & & \downarrow{\cong} & & & & \\ 0 & \longrightarrow & \coprod Rv_i & \xrightarrow[\coprod g_i]{} & \coprod Rv_i & \xrightarrow[\coprod h_i]{} & \coprod M_i & \longrightarrow & 0 \end{array}$$

Where the isomorphism (*) is given by the 5-Lemma (Which I forgot to show earlier. It was in the homework anyway. Just believe me!) Now let's take a pause! What do we know now? So far, we know this:

$$M \cong \coprod_{i\in I} Rm_i$$

That's all nice and dandy, but what we really need to do is get those d_i's back in the picture. If you go back to the statement of the theorem, that's what we're after! Some observations: $rd_iw_i = 0$ in $R^n \Rightarrow rd_i = 0$ (as γ is a basis). As we are in a domain, either $r = 0$ or $d_i = 0$. So:

$$Rd_iw_i \cong \left\{ \begin{array}{ll} R & d_i \neq 0 \\ 0 & d_i = 0 \end{array} \right\} \cong (d_i)$$

What does this tell us? Another massive commutative diagram of exact sequences will help us. Just note: It is NOT the previous commutative diagram in a different form! It looks the same, but if you examine it closely, we're dealing with individual Rw_i's and Rm_i's, not all of M.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Img(g) & \longrightarrow & Rw_i & \longrightarrow & Rm_i & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} & & \\
0 & \longrightarrow & Rd_iw_i & \longrightarrow & Rw_i & \longrightarrow & Rm_i & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong (**)} & & \\
0 & \longrightarrow & (d_i) & \longrightarrow & R & \xrightarrow{(*)} & R/(d_i) & \longrightarrow & 0
\end{array}$$

Where (*) is given by the First Isomorphism Theorem and (**) is a consequence of the 5-Lemma.

We're almost there! We now know:

$$M \cong \coprod_{i \in I} Rm_i \cong \coprod_{i \in I} R/(d_i)$$

But hey, remember some of those d_i's are 0? And we know $R/0 = R$, so collecting all the $R/0$'s together, we get $\coprod R/0 \cong \coprod R = R^s$, some $s \in \{\mathbb{N} \cup 0\}$. And FINALLY!:

$$M \cong R/d_1 \coprod R/d_2 \coprod \cdots \coprod R/d_n \coprod R^s$$

where $d_1|d_2|\cdots|d_n$ (Because remember, these d_i's came from the Smith Normal Matrix. □

Wowie. That took all afternoon to typeset.

Theorem 6.2.3 (Uniqueness of FTAG Version 1)**.** *By FTAG 1, Let*

$$M \cong R/d_1 \coprod R/d_2 \coprod \cdots \coprod R/d_n \coprod R^s$$

where $d_1|d_2|\cdots|d_n$*, and also*

$$M \cong R/b_1 \coprod R/b_2 \coprod \cdots \coprod R/b_m \coprod R^t$$

where $b_1|b_2|\cdots|b_m$

Then $s = t, m = n$*, and* $d_i \sim b_i$ *(They're unique up to units.)*

Proof. Ha! You think I'm going to prove that! It's actually not as bad as the existence proof (I think), but I really don't get it yet. Just pretend it's true. Besides, I need to work on med-school apps. =) □

It's study break time! And a little music rant. I am now listening to *All You Wanted* by Michelle Branch (The Spirit Room © 2002 Maverick Recording Co.) Call me some artsy north campus liberal (I'm actually a very south campusy moderate republican!) but I think there is some pretty interesting symbolism in the music video for *All You Wanted*. If you want to talk about it sometime, I'm game. =P In other news, does anybody else think J. Lo's music sucks? (Ditto Britney Spears and Christina Aguilera.) Christina and her song *Dirty*! Please! Whatever happened to the George Gershwins? His *Rhapsody in Blue* (1923) is the unmistakeable United Airlines theme. =) The real version is indescribably gorgeous. A particulary awesome arrangement is found in the IMAX production *Fantasia 2000*, performed by the Philharmonic Orchestra under conductor James Levine. (Fantasia 2000: An Original Walt Disney Records Soundtrack © 1999 Walt Disney Records).

You know, on the side, I guess there still good George Gershwinish musicians...Coldplay, Cheryl Crow, Michelle Branch, Garth Brooks. Ah, all is good and well again. =P

6.2.3 Torsion Stuff

Definition 6.2.1 (Torsion and Torsion-Free)**.** *A torsion element of a R-module M is an element $m \in M$ s.t. $r \cdot m = 0, r \neq 0$. If every element in M is torsion, M is said to be a torsion module. If the only element in M that is torsion is 0, then M is torsion-free.*

Note that free and torsion-free should not be confused, but they are related concepts, as we'll see next.

Lemma 6.2.2. *Let R be a domain. A free R-module is torsion free.*

Proof. This should jump out and up and down like that paperclip in Microsoft Word. If it's free, it has a basis, say $\{b_1, \ldots, b_n\}$. Then consider m, $0 \neq m = \sum r_i b_i$. Then consider $a \neq 0$. $am = 0 \Rightarrow \sum a r_i b_i = 0 \Rightarrow a r_i = 0 \ \forall i \Rightarrow a = 0$. (we're in a domain.) □

Lemma 6.2.3. *Let R be a domain. Then m is not torsion $\Leftrightarrow$ $R \cdot m$ is torsion-free $\Leftrightarrow$ $R \cdot m$ is free.*

Proof. This isn't bad. If m is not torsion, then $r \cdot m = 0 \Rightarrow r = 0$. So if $s(rm) = 0, then s r = 0$. Then $s = 0$ or $r = 0$ (we're in a domain). If $r = 0$, then $rm = 0$, the zero element in the module, the trivial case. If $r \neq 0$, then $s = 0$. So we have $R \cdot m$ is torsion-free. Then it's pretty immediate that $R \cdot m$ is free with the single basis element m. ($R \cdot m$ spans, and $rm = 0 \rightarrow r = 0$.) And if its free with basis m, then m is not torsion. □

A note on this torsion stuff. A module being torsion-free is related to a ring being a domain. If a ring R is a domain, $rs = 0 \Rightarrow r = 0$ or $s = 0$. That is, we're multiplying by zero somewhere. If a module is torsion-free, then $r \cdot m = 0_M \Rightarrow r = 0_R$ or $m = 0_M$, so again, we're multiplying by zero somewhere.

Note that we don't necessarily have multiplication of two elements in the abelian group of the module (we only have ring-ring multiplication and ring-module multiplication), so we can't talk about $m_1 \cdot m_2 = 0_M$, as mulitplication is not defined.

Now here's another intersting thing. By the last lemma, we have that the R-module $R \cdot misfree \Leftrightarrow R \cdot mistorsion - free$. This equivilance is not true for modules in general. But when is it true? Turns out:

Lemma 6.2.4. *Let M be a finitely generated R-module over a PID. We have:*

$$M \cong R/d_1 \coprod R/d_2 \coprod \cdots \coprod R/d_n \coprod R^s$$

With $d_1|d_2|\cdots|d_n$.
Let $R/d_1 \coprod R/d_2 \coprod \cdots \coprod R/d_n = N_0$.
Let N_T *be the set of torsion elements in M. Then* $N_T = N_0$.

Proof. $N_0 \subseteq N_T$ is immedieately apparent, as d_n (the last of the invariant factors) will zero all elements in N_0. (Recall $d_1|d_2|\cdots|d_n$.)

For $N_T \subseteq N_0$, Let $x \in M, x = (a, b), a \in N_0, b \in R^s$. Then $kx = 0 \Rightarrow (ka, kb) = 0$. In particular, $kb = 0$ As R^s is free, $b = 0$. So $x \in N_0$. □

Lemma 6.2.5. *If M is a finitely generated R-Module over a PID, then M is free ⇔ M is torsion-free.*

Proof. Well, we already have that if R is a domain (not necess. a PID), then free ⇒ torsion-free.

As M is a finitely generated R-Module, and R is a PID, we have FTAG 1.

$$M \cong R/d_1 \coprod R/d_2 \coprod \cdots \coprod R/d_n \coprod R^s = N_0 \coprod R_s$$

Observe the following by the First Isomorphism Theorem:

$$R^s \cong (N_0 \coprod R^s)/(N_0) = M/N_0 = M/N_T$$

So if M is torsion-free, $N_T = 0$. By the previous lemma, $N_0 = N_T$. So $R^s = M/N_0 = M/N_T = M/0 = M$. Thus, We have $M = R^s$, so M is free. □

6.3 Fundamental Theorem of Abelian Groups, Version 2

It won't be that bad! We know quite a bit from our previous adventure! =)

6.3.1 Concepts Needed for FTAG 2

Lemma 6.3.1. *R a UFD (A Unique Factorization Domain.) Then* $R/(d) \cong R/(p_1^{e_1}) + \cdots + R/(p_n^{e_n})$, *where* p_i *is prime,* $e_i \geq 1$, *and* $d = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$

Proof. By the Chinese Remainder Theorem, $g : R \to R/(p_1^{e_1}) + \cdots + R/(p_n^{e_n})$ is onto. (Note the ideals $(p_i^{e_i})$ and $(p_j^{e_j})$ are comaximal for $i \neq j$, as their generating terms are relatively prime. If you're still not sure what is happening, think px + qy = 1 for p,q relatively prime.) The chinese remainder theorem also tell us that the kernel is the product of the ideals. And of course, $\prod p_i^{e_i} = d$. Then by the first isomorphism theorm, $R/(d) \cong R/(p_1^{e_1}) + \cdots + R/(p_n^{e_n})$. □

Lemma 6.3.2. *Let R be a PID, M a finitely generated torsion R module. Then* $M = \bigoplus_{i \in I} Rm_i$, *with* $Ann_R m_i = (d_i)$, *with* $d_1 | d_2 | \ldots | d_n$.

Proof. Hey! This is FTAG1! It's just we're a torsion module, so there's no free part. I guess we're done with that! □

We didn't need to make a big deal about that last lemma. But I think we made a stop there because it's the finite version of the Primary Decomposition Theorem.

6.3.2 FTAG Version 2

Theorem 6.3.1 (Fundamental Theorem of Abellian Groups, Version 2)**.** *Let M be a finitely generated R-Module, R a PID. Then:*

$$M \cong P \coprod \left(\coprod_{i \in I} \coprod_{j \in J_i} R/(p_i^{e_{ij}}) \right)$$

Note: The p_i*'s are called elementary divisors.*

Proof. This really does fall out quite rapidly from FTAG 1 and those lemmas we did. By FTAG 1,

$$M \cong R/d_1 \coprod R/d_2 \coprod \cdots \coprod R/d_n \coprod P$$

where $d_1 | d_2 | \cdots | d_n$, and P is free.

Then by Lemma **??**, all the d_i's break down into there respective prime factors. Collecting all the prime factors together, we get:

$$M \cong P \coprod \left(\coprod_{i \in I} \coprod_{j \in J_i} R/(p_i^{e_{ij}}) \right)$$

□

Theorem 6.3.2 (Uniqueness of FTAG 2)**.** *The representation in FTAG2 is unique. That is, if*

$$M \cong P \coprod \left(\coprod_{i \in I} \coprod_{j \in J_i} R/(p_i^{e_{ij}}) \right)$$

and ...

$$M \cong V \coprod \left(\coprod_{k \in K} \coprod_{l \in L_k} R/(q_k^{f_{kl}}) \right)$$

Then $I = K$, and assuming things are "ordered" correctly (we don't have a natural ordering), $J_i = L_k$ (for $i = k$), $p_i \sim q_k$ (for $i = k$), and $e_{ij} = f_{kl}$ (for $i = k$ and $j = l$), and $P \cong V$.

Proof. This falls away immediately from the fact that the invariant factors of FTAG 1 are unique up to units and that we are in a UFD. (so those invariant factors, in particular, factor into the elementary divisors uniquely). □

Yay! We survived those FTAG theorems! Or we glossed over them. No worries. It'll come one day. It's time for a rant again. I would tell you what I was listening to, but it might be getting old. Instead, I'll tell you I'm at San Jose's newest library (The Tully Community Library) It's awesome. And it's encouraging to see so many people using the library, from adults to little kids and all in between. We need more of these libraries! Maybe it'll bring world peace. =P OK, maybe not. But my joke is that if you gave everybody curly fries, there would be world peace, as everybody would be munching up on their curly fries. =)

6.4 Cool Stuff to do with FTAG 1

Under Construction Like Always

6.5 Cool Stuff to do with FTAG 2

Under Construction Like Always