Math 702

Contents

CHAPTER 1

Rings and their properties

Definition 1. *A Ring is a set R with two binary operations, + and $\times$, such that the following are true:*

(1) $(R, +)$ *forms an abelian group*
(2) $(R - \{0\}, \times)$ *is associative*
(3) *The distributive law holds. I.e.,* $a \times (b + c) = a \times b + a \times c$ *and* $(b + c) \times a = b \times a + c \times a$

The following statements refer to terminology surrounding types of rings:

(i) R is a ring with identity if if there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$
(ii) A ring R with 1 is called a division ring if every nonzero element has a multiplicative inverse
(iii) If R is a division ring and $\times$ is commutative, R is called a field.

Example.

$$\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}(+, \times)$$

This is a ring, with identity (or, as we call it, "with 1"). However, it is not a division ring (and therefore not a field) -because not every element of $\mathbb{Z}$ will have a multiplicative inverse that is in the set of integers.

Other examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Example.

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, ...(n - 1)\}$$

this forms a ring under modular multiplication and addition with respect to n. It happens to be a commutative ring with identity, but is not a field in general- but is a field if n is a prime integer.

Example. Choosing some $K \in \mathbb{Z}$ we see that $K \cdot \mathbb{Z}$ is a ring without an identity (multiplicative identity, of course)

The following are assorted properties of a ring R, where $a \in R$:

(1) $0 \cdot a = a \cdot 0 = 0$
(2) (-a)(b)= (a)(-b)
(3) (-a)(-b)=(a)(b)
(4) If $\exists 1 \in R$, it is unique.

Definition 2. *A unit is an element of R with a multiplicative inverse*

Definition 3. *A zero divisor is a nonzero element $a \in R$ such that when $b \in R$, $a \cdot b = b \cdot a = 0$ for some $b \neq 0$*

These properties of elements of a ring are mutually exclusive.

Proof. Suppose a is a unit. Then,

$$x \cdot a = 1$$

for some $x \in r$. If $a \cdot b = 0$, then since $b = 1 \cdot b$,

$$x \cdot a \cdot b = x \cdot 0 = 0$$

by which we see a contradiction. □

Example. In $\mathbb{Z}$, the units are ± 1

Example. For $\mathbb{Z}/n\mathbb{Z}$, we claim that each element is either a unit or a zero divisor. The proof of this claim will be excluded.

The result of the would-be proof of the above example would lead us to the conclusion that if n was prime, every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ would be relatively prime to n, and thus would be a unit. If every element is a unit, it then has a multiplicative inverse, and thus $\mathbb{Z}/n\mathbb{Z}$ would be a field.

Example.

$$R[x] = \text{polynomials of x with coefficients in R}$$
$$= \{a_0 + a_1 x + a_2 x^2 + ... + a_n x^n | n \geq 0, a_i \in r\}$$

If ring R has an identity, then $R[x]$ must also have an Identity. Also notice that when $R = \mathbb{Z}$ the element x (which is in $\mathbb{Z}$) is not a unit (because no polynomial can act on x to yield 1) but it is also not a zero divisor. This demonstrates that while the properties of being a unit/zero divisor may be mutually exclusive, an element is not forced to be one or another.

Definition 4. *An integral domain is a ring with no zero divisors. For example, $\mathbb{Z}$ is an integral domain because if $x, y \in \mathbb{Z}$ and $xy = 0$, we know that either $x = 0$ or $y = 0$ (or both). This is equivalent to the claim that 'there are no zero divisors'.*

Notice that if R is an integral domain, and $a, b, c \in R$ and $ac = bc$ then $ac - bc = 0$, so $(a - b)c = 0$, so we know that $a - b = 0$ or 0 or $a = b$ or $c = 0$. This is also helpful in showing that a ring is not an integral domain.

Example. Take the modulus group $R = \mathbb{Z}/n\mathbb{Z}$, and let $a, b, c \in R$. Then we know that if R is an integral domain, we can apply the rules above. However, suppose n=6, c=3, a=2 and b=0. We can then see that $a \cdot c = b \cdot c$, but $c \neq 0$ and $a \neq b$, so we see that $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

We should notice that we picked a convenient value for n. We should notice the following relation:

$$\mathbb{Z}/n\mathbb{Z} \text{ is an integral domain} \iff \mathbb{Z}/n\mathbb{Z} \text{ is a field} \iff \text{n is prime}$$

THEOREM 1. *Any finite integral domain is always a field.* [1]

PROOF. We need to show that if $a \in R, a \neq 0$, then a has a multiplicative inverse. Consider the following maps:

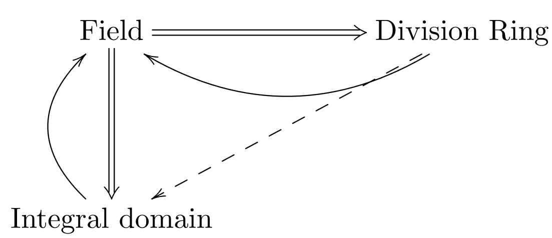
$$R \mapsto r$$

$$x \mapsto a \cdot x$$

This is a one to one function[2], and since R is finite, this map is a bijection. So, ax=1 for some x, so a must have an inverse $x \in R$. This demonstrates that all nonzero elements are unites, so R is a field. □

We can now understand that a Field is always a Division ring and an integral domain. The reverse relationship isn't always true; A division ring is a field only if every nonzero element is a unit and its operation $\times$ is commutative. Also, a division ring is an integral domain if it has commutativity. The diagram looks something like the following:

(1)



EXAMPLE.

$$\mathbb{Z}[D] \subseteq {}^{3}\, \mathbb{Q}[D] = \{a + b\sqrt{D} | a, b \in \mathbb{Q}\}$$

Taking the case where D=-1, we have:

$$\mathbb{Z}[D] = \{a + bi | a, b \in \mathbb{Z}\}$$

This set is called "The Gaussian Integers", and is a subring of $\mathbb{Z}[-1] \subseteq \mathbb{C}$

DEFINITION 5. *The degree of an element $p(x) \in R[x]$ is n if $p(x) = a_n x^n + ... + a_1 x + a_0$ where $n > 0$*

Let R be an integral domain, and let $p(x), q(x) \in R[x]$. The following are true:

(1) $deg(p(x) \cdot q(x)) = deg(p(x)) \cdot deg(q(x))$
(2) R[x] is an integral domain
(3) The units of R[x] are units of R

The proofs for these properties will be excluded. Also notice that if S is a subring of R, the following is true:

$$S[x] \subseteq R[x]$$

[1]an integral domain is always a commutative ring with 1
[2]a one to one function is a function f from A to B such that f(a)=f(c)=b, a=c
[3]We have started to use the symbol '⊆' to mean 'subring of'

DEFINITION 6. *Let R and S be rings. A ring homomorphism is a function* $\varphi : R \to S$ *such that* $\varphi(x+y) = \varphi(x) + \varphi(y)$ *and* $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

EXAMPLE. Given R, consider a map from R[x] to R:

$$eval : R[x] \to R$$

Where this map takes $p(x) \in R[x]$ and maps its constant term a_0 to R. Since $eval(p(x) \cdot q(x)) = eval(p(x)) \cdot eval(q(x))$ and $eval(p(x)q(x)) = eval(p(x)) \cdot eval(q(x))$ so the map $eval$ is a homomorphism.

DEFINITION 7. *Given* $\varphi : R \to S$*, a homomorphism, we define the Kernel and Image of* φ *to be the following:*

$$Ker(\varphi) = \{a \in R | \varphi(a) = 0\}$$

$$Im(\varphi) = \{b \in S | b = \varphi(a), a \in R\}$$

EXAMPLE. Take the homomorphism$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. We see that the $Ker(\varphi) = n\mathbb{Z}$ and that $Im(\varphi) = \mathbb{Z}/n\mathbb{Z}$

From this example we can now interpret different things about the Kernel and Identity, specifically:

$$Ker(\varphi) = 0 \iff \text{The homomorphism } \varphi \text{ is injective}$$

$$Im(\varphi) = S \iff \text{The homomorphism } \varphi \text{ is surjective}$$

Also, the homomorphism φ is bijective if it is both injective and surjective. Another Fact to notice is that:

$$Ker(\varphi) \subseteq R) \text{ and } Im(\varphi) \subseteq S$$

Recall from group theory that if G is a group and N is a normal subgroup, that G/N is a group. We defined $N \leq G$ to be normal if and only if:

$$gNg^{-1} \subseteq N \; \forall g \in G, \text{ or } gN = Ng \; \forall g \in G$$

The elements of G/N are equivalence classes under $g_1 \sim g_2$ if and only if $g_1 g_2^{-1} \in N$. G/N is a group with the well defined operation $(g_1N)(g_2N) = (g_1g_2)N$

CHAPTER 2

Quotient Rings

Definition 8. *Let R be a ring. A [Left] right ideal is a subset I such that:*

$$a \cdot I \subset I \text{ (or for a left ideal) } [I \cdot a \subset eqI] \; \forall a \in R$$

If I is a left AND right deal, then we just say that I is an ideal. Notice that if R is commutative, left and ideals are automatically the same.

Example. Let a ring $R = \mathbb{Z}, I = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, ...\}$ To check that I is a right ideal, we have to check that given $n \in \mathbb{Z}$, $n \cdot I \subseteq I$. This is true, because no matter what integer you multiply a factor of 3 by, you will always end up with another factor of 3.

More generally, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for all $n \in \mathbb{Z}$.

One remark to notice is that although $3\mathbb{Z}$ is a sub-ring of $\mathbb{Q}$, $3\mathbb{Z}$ is not an ideal of $\mathbb{Q}$, because it will not be closed under multiplication of elements in $\mathbb{Q}$.

Example. Let $R = \mathbb{Z}[x]$, $I =$ sub-ring of polynomials with even coefficients. Since this subset I is closed under multiplication, it is an ideal.

Theorem 2. *Let I be a sub-ring of R. Then,*

$$R/I = \{a + I | a \in R\} \text{ under the equivalence relation:}$$

$$a + I \sim b + I \iff a - b \in I$$

Is a ring under the operations:

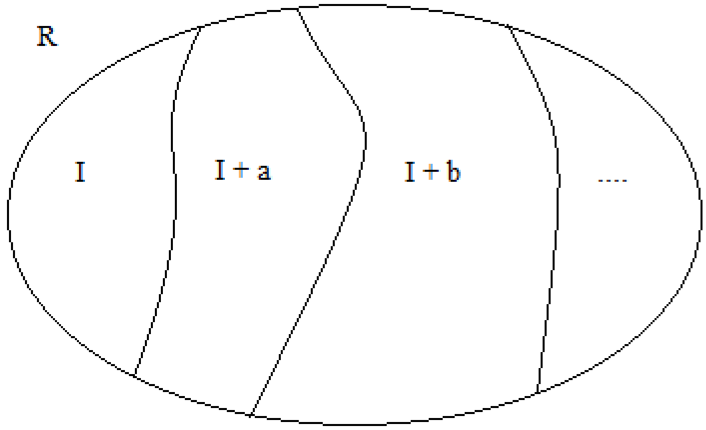
$$(a + I) + (b + I) = ((a + b) + I) \text{ and } (a + I)(b + I) = (ab + I)$$

If and only if I is an ideal.

The following is a diagram illustrating the concept of how a group R would be split up into a quotient group- the collection of the elements of R are split up into equivalence classes, which will be the elements of the quotient group. The most common and easy to understand example of a quotient group is the modulus group $\mathbb{Z}/n\mathbb{Z}$, where the elements are divided into equivalence classes under modular arithmetic with respect to n.

Notice that if $r \in I$, then $r + I \sim 0 + I$. Then,

$$(r + I)(s + I) = rs + I \text{ and } (0 + I)(s + I) = 0 + I$$



So we need $rs + I \sim 0 + I$ for it to be a well defined equivalence relation. So, $rs \in I$ if $r \in I, s \in R$, which is always true since we assumed I was an ideal of R.

On the other hand, if I is an ideal:

$$(r + I) \cdot (s + I) \stackrel{?}{=} (r + i_1 + I) \cdot (s + i_2 + I) = rs + ri_2 + i_1S + i_1i_2 + I$$

for some $i_i, i_2 \in I$? Consider the following:

$$(rs + I) - (rs + ri_2 + i_1S + i_1i_2 + I) = (ri_2 + i_1s + i_1i_2)$$

We know that $i_1i_2 \in I$ since I is a sub-ring, and closed under multiplication. We can say that ri_2 is in I if I is a left ideal, and similarly we can say that i_1s is in I if I is a right ideal. Therefore, to nail down the equivalence relation and to ensure that elements will be closed under actions, we have to assume that I is both a right and left ideal.

Fact. When given a homomorphism $\varphi : R \to S$, where R and S are both rings, the $Ker(\varphi)$ is an ideal

Operations on Ideals: Let I, J be ideals in R.

(1) $I + J = \{a + b | a \in I, b \in J$. Since I and J are ideals, $r(a + b) = ra + rb \in I + J$ for some $r \in R$.
(2) $IJ = \{\sum_{i=1}^{n} a_ib_i | a_i \in I, b_i \in J\}$

Let $A \subseteq R$ be any subset of R. The smallest ideal of R containing A will be:

$$= \bigcap_{I \leq A,\ \text{'I' an Ideal}} I, \text{ sometimes denoted '(A)'}$$

Called the 'ideal generated by A'.

Fact. If R is a commutative ring, then

$$(A) = \{ra | r \in R, a \in A\}$$

is an ideal. Any ideal containing A must contain this, so therefore it is the smallest ideal containing A, or '(A)'

DEFINITION 9. *Let R be a ring. A principal ideal is an ideal that can be generated by a single element,* $I = (a)$*, for some* $a \in R$*.*

EXAMPLE. Take the ideal $n\mathbb{Z} \in \mathbb{Z}$

$$n\mathbb{Z} = (n) = \{K \cdot n | K \in \mathbb{Z}\} = (-n) = \{K \cdot -n | K \in \mathbb{Z}\}$$

EXAMPLE. Take the ideals (3) and (6) in $\mathbb{Z}$. For any $m|n$ where $m, n \in \mathbb{Z}$, $(n) \subseteq (m)$. Therefore, $(6) \subseteq (3)$

THEOREM 3. *The* 1^{st} *isomorphism theorem:*

If $\varphi : R \to S$ *is a ring homomorphism, then* $R/Ker(\varphi) \cong Im(\varphi)$

PROOF. Suppose there is a map:

$$r + Ker\varphi \mapsto \varphi(r)$$

The following is then true:

$$(r + Ker(\varphi) \cdot (s + Ker(\varphi)) = rs + Ker(\varphi) \mapsto \varphi(rs) =$$
$$= \varphi(r) \cdot \varphi(s) = F(r + Ker\varphi) \cdot F(s + Ker(\varphi))$$

For some function F. Thus we see that there exists some relationship between $\varphi(rs)$ and some function F involving what looks like the members of the quotient group $R/Ker(\varphi)$. □

If I is an ideal of R, then:

$$R \overset{\pi}{\longmapsto} R/I, r \mapsto r + I$$

Which is a ring homomorphism. The Kernel of this map is exactly I, since:

$$\pi(r) = r + I = 0 + I \Rightarrow r \in I$$

THEOREM 4. *The* 4^{th} *isomorphism theorem: if R is a ring an I is an ideal, then there is a bijection between:*

$$\textit{Subrings of } R \textit{ containing } I \longleftrightarrow \textit{ Subrings of } R/I$$

This suggests a map:

$$A \longmapsto A/I$$

which implies that if A is an ideal of R, A/I *is an ideal of* R/I*. This correspondence preserves ideals.*

FACT. Let I be an ideal of R. If $I \subseteq S \subseteq R$, then $sI \subseteq I \forall s \in S$. So, I is thus an ideal of S.

Let R be a ring with 1. The following are then true:

(1) Let I be an ideal. Then, I=R $\iff$ I contains a unit.
(2) If R is a field, then the only ideals are R and $\{0\}$.

PROOF. If I contains a unit, some $a \in I$, then we know that $x \cdot a = 1$ for some $x \in R$. $x \cdot a \in I$, so we know that $1 \in$. Then, since $y = y \cdot 1$ for any $y \in R$, we can see that by taking the actions of all elements in R on the element 1 in I, that $I = R$. □

PROOF. If I is an ideal of a field R, and $I \neq 0$, then I contains some $a \in R, a \neq 0$, which is a unit- so therefore, using the same reasoning as above, $I = R$. □

DEFINITION 10. *An ideal M of R is maximal if there is no ideal N of R such that:*

$$M \subsetneq N \subsetneq R$$

THEOREM 5. *Let R be a commutative ring with identity, where M is an ideal of R. M is maximal if and only if R/M is a field..*

PROOF. By the fourth isomorphism theorem, we see that:

$$\text{Ideals A of R containing M} \overset{1-1}{\longleftrightarrow} \text{Ideals of } R/M$$

$$A \mapsto A/M$$

If R/M is a field, then the only ideals of R/M are 0 and R/M. This implies the only ideals A of R containing M are $A = M$ and $A = R$, so M must be maximal. In proving the other direction of this statement, assume M is maximal. Note that:

$$A \mapsto A/M$$

$$M \mapsto M/M = 0$$

$$R \mapsto R/M$$

Since M is maximal, then there does not exist some ideal A such that $M \subsetneq A \subsetneq R$,, so there is no ideal such that $0 \subsetneq A/M \subsetneq R/M$. Since, 0 must be maximal in R/M. In a result proved in the homework (mainly that if the maximal ideal of a ring is 0, that ring is a field) we see that R/M is a field. □

FACT. If R is a ring, and A is an ideal of R, then there exists some maximal ideal M of R, containing A.

EXAMPLE. Ideals of $\mathbb{Z}$ are $n\mathbb{Z}$, for some integer n. All these ideals are principle ideas, since $n\mathbb{Z} = (n) = (-n)$. $n\mathbb{Z}$ is maximal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field, which we already know happens when n is a prime number.

EXAMPLE. Look at the ideal $(2, x) \in \mathbb{Z}[x]$. This ideal looks like this:

$$(2, x) = \{2 \cdot p(x) + xq(x) | p(x), q(x) \in \mathbb{Z}[x]\}$$

This first term $(2 \cdot p(x))$ is any polynomial with all even constant terms. The second term $(xq(x))$ is any polynomial with a zero constant term. Thus, the elements in $\mathbb{Z}[x]$ this set contains are all polynomials with even constant terms. This turns out to not be a principal idea.

EXAMPLE. Now consider:

$$\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/2\mathbb{Z}$$

Where:

$$p(x) + (2,x) \mapsto p(0) \text{ mod } 2$$

$\mathbb{Z}_2$ is a field, so therefore $(2,x)$ must be maximal in $\mathbb{Z}[x]$.

EXAMPLE. Let R be the ring of functions from $X \to \mathbb{R}$. Pick some p in X, and let the ideal I be functions $f : X \to \mathbb{R}$ such that $f(p) = 0$. Consider the quotient: $R \to \mathbb{R}$. By definition, Ker(f(p))=I. By the 1^{st} isomorphism theorem,

$$R/I \cong Im(f) \cong \mathbb{R}$$

And since $\mathbb{R}$ is a field, I must be a maximal ideal.

FACT. An ideal P of R where $P \neq R$ is called prime, or 'a prime ideal of R', if it satisfies the following:

Whenever $ab \in P$, where $a, b \in R$, either $a \in P$ or $b \in P$.

EXAMPLE. When $R = \mathbb{Z}$, the ideals are $n\mathbb{Z}$, where $n \in \mathbb{Z}$. For which n is $n\mathbb{Z}$ a prime ideal? Well, if $ab \in n\mathbb{Z}$, then either $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$. As the name of the ideal implies, it turns out that this happens when n is a prime number. This is because if ab=nm, we know that either $n|a$ or $n|b$, so either $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$. On the other hand if $n\mathbb{Z}$ is a prime ideal than n is a prime number. If $n|ab \Rightarrow n|a$ or $n|b, \forall a, b$ then n is prime.

EXAMPLE. If n=4, $2 \cdot 2 \in 4\mathbb{Z}$, but $2 \notin 4\mathbb{Z}$. So $4\mathbb{Z}$ is not a prime ideal.

THEOREM 6. *Let R be a commutative ring with 1. Then P is a prime ideal in R if and only if R/P is an integral domain.*

PROOF. P is prime means that $ab \in P \Rightarrow a \in P$ or $b \in P$. (R/P is commutative with identity: $1 + P$ since R is commutative.) R/P not having any zero divisors implies and is implied by:

$$(a + P) \cdot (b + P) = (0 + P) \Rightarrow 0 + P$$

Which means that

$$a + P = o + P \text{ or } b + P = 0 + P$$

$$ab + P = 0 + P \Rightarrow a + P = 0 + P \text{ or } b + P = 0 + P$$

Where $(ab \in P)$. This would imply that P is a prime ideal. □

EXAMPLE. Let $R = \mathbb{Z}[x]$. Let $I = (x)$, all polynomials without constant terms. The following is then true:

$$\mathbb{Z}/(x) \cong \mathbb{Z}$$

Which is an integral domain, which tells us that I is prime. This isomorphism is brought about by the following map:

$$eval : \mathbb{Z}[x] \mapsto \mathbb{Z}$$

$$eval(p(x)) \mapsto p(0)$$

I.e., the map 'eval' is yeilds the constant term of the polynomial $p(x)$. This is also a ring homomorphism. Notice that:

$$Ker = (x)$$

Because (x) will yeild all polynomials without constant terms, we can see that $Ker((x)) = 0$. Thus, by the first isomorphism theorem,

$$\mathbb{Z}[x]/Ker = \mathbb{Z}/(x) \cong Im(eval) = \mathbb{Z}$$

However, (x) is not maximal in $\mathbb{Z}[x]$, because:

$$(x) \subsetneq (x, 2) \subsetneq \mathbb{Z}[x]$$

FACT. When R is a commutative ring with 1, every maximal ideal is prime.

PROOF. If an ideal I is maximal in R, this implies that R/I is a field, which implies that R/I is an integral domain, which implies that I is prime in R. □

1. Understanding Fractions:

Think of the field $\mathbb{Q}$, a set of what we commonly call 'fractions'. It is an understandable question to ask how this set was constructed. Consider 'elements', called fractions, $\frac{a}{b}$ where $a, b \in \mathbb{Z}$. However, there are immediate problems that arise from this idea, we need a stronger set of definitions to ensure that $\frac{1}{2} = \frac{2}{4} = \frac{3}{6}$. It turns out we will admit the following definition:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

The General idea is that given a ring R and some subset D of R, we think of as elements of R that we want to invert (multiplicatively). We have chosen the letter 'd' to represent this subset, because it will intuitively stand for 'denominator'. Consider pairs:

$$(a, b) \in R \times D$$

with the equivalence relation:

$$(a, b) \sim (c, d) \iff x(ad - bc) = 0$$

For some element $x \in D$. As you can see, this mimics the structure of what we would usually call a 'fraction'. Taking the equivalence classes, call this set:

$$D^{-1}R$$

And try to define a ring by the following operations:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Now, the following conditions must be upheld:

(1) We need D to be closed under multiplication in order for addition to be defined and nonempty
(2) If we want a map $i : R \to D^{-1}R, r \to \frac{r}{1}$ to be 1-1, we need D to have no zero divisors. This is because if we can show that $d \in D$ is a zero divisor, $\frac{d}{1} \sim \frac{0}{1}$. Suppose that $d \cdot x = 0$ then $\frac{d}{1} = \frac{dx}{x} = \frac{0}{x} = 0 = \frac{0}{1}$. Thus the map i is not 1-1, since there are elements in the $Ker(i)$ that are not equal to 0.

THEOREM 7. *Let R be a commutative ring with 1, and D is a nonempty subset of R closed under multiplication. there then exists a commutative ring with 1 denoted $D^{-1}R$ and a ring homomorphism:*

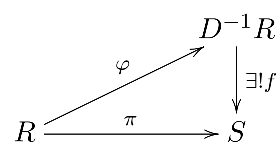
$$\varphi : R \mapsto D^{-1}R$$

such that:

(1) *If $d \in D$ is a zero divisor, $\varphi(d) = 0$*
(2) *If $d \in D$ is not a zero divisor, $\varphi(d)$ is a unit*
(3) *$D^{-1}R$ is the 'smallest such ring'.*

For any S with some map $\pi : R \to S$ that satisfies requirements (1) and (2), there exists a uniqe ring homomorphism $f : D^{-1}R \to R$ such that $f \circ \varphi = \pi$

(2)



Restating this theorem more directly, considering the ring homomorphism $I : R \to D^{-1}R$ we have th following 4 properties:

(1) If $x \in D \subseteq R$ is not a zero divisor, then $i(d) \in D^{-1}R$ has an inverse under multiplication.
(2) Given any ring S and a homomorphism $\pi : R \to S$ such that $\pi(d)$ is invertible whenever $d \in D$ is not a zero divisor, then there exists a unique ring homomorphism $f : D^{-1}R \to S$ such that $f \circ i = \pi$
(3) If D has no zero divisors, then $i : R \to D^{-1}R$ is 1-1 (so, we can think of R as sitting inside $D^{-1}R$, and all the elements of D are invertible).
(4) If D has no zero divisors and $D = R - 0$, then $D^{-1}R$ is a field.

PROOF. Construct $D^{-1}R$. Take:

$$R \times D = \{r, d | r \in R, d \in D\}$$

And consider the following equivalence relation:

$$(r_1, d_1) \sim (r_2, d_2) \text{ or } \frac{r_1}{d_1} \cong \frac{r_2}{d_2} \iff x(r_1 d_2 - r_1 d_1) = 0 \text{ for some } x \in D^{-1}R$$

This definition satisfies the reflexive, symmetric, and transitive properties for a valid equivalence relationship. We then define operations in $D^{-1}R$ as follows:

$$\frac{r_1}{d_1} + \frac{r_2}{d_2} = \frac{r_1 d_2 + r_2 d_1}{d_1 d_2} \text{ and } \frac{r_1}{d_1} \cdot \frac{r_2}{d_2} = \frac{r_1 r_2}{d_1 d_2}$$

We would then like to show that this makes $D^{-1}R$ a commutative ring with 1[1].

Therefore, $D^{-1}R$ must be well defined, commutative, an abelian group under addition, associative under multiplication, and the distributive law must hold. Define:

$$i : R \to D^{-1}R \text{ as } i(r) = \frac{rd}{d}, d \in D$$

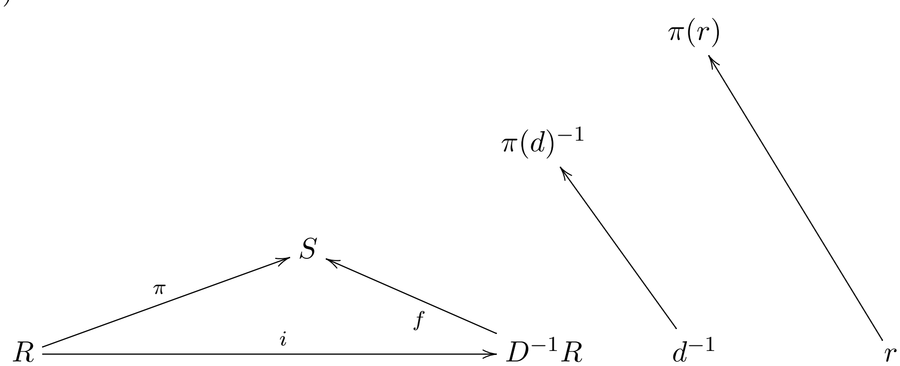
Notice that:

$$\frac{rd}{d} \sim \frac{re}{e}, \text{ and that } i(r_1 + r_2) = \frac{(r_1 + r_2)d}{d} = \frac{r_1 d}{d} + \frac{r_2 d}{d} = i(r_1) + i(r_2)$$

Now suppose that $d \in D$ and d isn't a zero divisor. Then, $i(d) = \frac{de}{e}$. Does this have an inverse? Under our definitions of multiplication, we can see that it will have an inverse as follows:

$$\frac{de}{e} \cdot \frac{e}{de} = \frac{de^2}{de^2} \sim 1 \in D^{-1}R$$

To prove out second requirement, that there exists a unique ring homomorphism $f : D^{-1}R \to S$, we offer the following diagram:
(3)



$$r \longrightarrow i(r) = \tfrac{rd}{d} = r)d_d^{-1}$$

Look at the Kernal of $I : R \to D^{-1}R$. $I(r) = \frac{rd}{d} \sim \frac{0}{d} \iff x(rd^2 - d \cdot 0) = 0, x \in D$. This implies that $rxd^2 = 0$, so, $x \in D, d \in D \Rightarrow xd^2 \in D$, since D is closed under multiplication. Since we assumed that D had no zero divisors, we know that r must then be zero.

[1]To really understand $D^{-1}R$, we need to have a good understanding of some concept of '1'. A good candidate will be $\frac{d}{d}$, for all $d \in D$.

To prove the 4th claim, let $D = R - \{0\}$, and let D have no zero divisors. Then, $i : R \to D^{-1}R$ is 1-1 and every nonzero element of $D^{-1}R$ is invertible, so $D^{-1}R$ is a field. □

This leads us to an interesting result:

FACT. Every integral domain sits inside some 'field', called 'the field of fractions' of an integral domain.

We now need to address why $0 \notin D$. Since we know the following:

$$(a, b) \sim (c, d) \iff x(ad \cdot -bc) = 0 \text{ for some } x \in D$$

We can always let $x = 0$, and we then see that any elements $(a, b), (b, c)$ are equivalent under this relation. Thus, every element reduces down to zero; the restriction is made on D to avoid the trivial case.

EXAMPLE. Let $R = \mathbb{Z}, D = \mathbb{Z} - \{0\}$. Then, $D^{-1}R \cong \mathbb{Q}$ since $0 \notin D$, so $x(ad - bc) = 0$ is really just the same as $ad - bc = 0$.

EXAMPLE. Let $R = \mathbb{Z}, D = 2\mathbb{Z} - \{0\}$. Then, $D^{-1}R = \{a/2b | a, b \in \mathbb{Z}, b \neq 0\}$. Since the following is true:

$$\frac{x}{y} = \frac{2x}{2y} = \frac{z}{2y}, \ z \in \mathbb{Z}, z = 2x$$

We realize that we can assign the following relationship between $\mathbb{Q}$ and $D^{-1}R$:

$$\mathbb{Q} \xrightarrow{f} D^{-1}R \qquad D^{-1}R \xrightarrow{g} \mathbb{Q}$$
$$\frac{x}{y} \to \frac{2x}{2y} \qquad \frac{a}{2b} \to \frac{a}{2b}$$

$f \circ g = Id$, since $\frac{a}{2b} \sim \frac{2a}{2(2b)}$ And, $g \circ f = Id$, since $\frac{2x}{2y} \sim \frac{x}{y}$. Thus:

$$D^{-1}R \cong \mathbb{Q}$$

DEFINITION 11. *A Ring of formal power series:*

$$\sum_{n \geq 0} a_n x^n, \ n \in \mathbb{Z} = a +_0 + a + 1x + a_2 x^2 + ...$$

CHAPTER 3

The Chinese Remainder Theorem

An arithmetic problem: suppose we are given $m_1, \dots, m_n \in \mathbb{Z}^+$ and $b_1, \dots, b_n \in \mathbb{Z}$, with $g.c.d.(m_i, m_j) = 1\ \forall i \neq j$. Can we find an $x \in \mathbb{Z}$ such that $x \equiv b_i \bmod m_i\ \forall 1 \leq i \leq n$? The answer is yes, and we find out that if x works, then so does $x + (m_1 m_2 \cdots m_n)$; there is a unique solution up to a multiple of $m = m_1 m_2 \cdots m_n$.

1. Construction

Consider $R = \mathbb{Z}$. For each i, let $I_i = (m_i)$ be an ideal of $\mathbb{Z}$ (recall: $m\mathbb{Z} + n\mathbb{Z} = g.c.d.(m,n)\mathbb{Z}$). Since $g.c.d.(m_i, m_j) = 1$ for $i \neq j$, we get that $I_i + I_j = \mathbb{Z}\ \forall i \neq j$ (In such a case that $I_i + I_j = R$, we call I_i and I_j $co - maximal$).
We want $x - b_i \in I_i = m_i\mathbb{Z} = (m_i)\ \forall 1 \leq i \leq n$, and we write this: $x_i \equiv b_i$ (mod I_i). Then the question becomes: Is there a function f such that:

$$f : \mathbb{Z} \to \mathbb{Z}/I_i \times \ldots \times \mathbb{Z}/I_n$$

Or equivalently,

$$f : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}$$

Under such a function, we would get

$$x \mapsto (b_1, \ldots, b_n)$$

All that would be left to show is surjection (which is clear), and we know that the kernel of such a function is exactly $m\mathbb{Z}$, where $m = m_1 \cdots m_n$.

Theorem 8 (Chinese Remainder Theorem). *Let R be a ring with identity and $A_1, \ldots, A_n$ be ideals. Suppose that for all $i \neq j$ we have $A_i + A_j = R$ (A_i, A_j are comaximal). Then,*

$$\pi : R \to R/A_1 \times R/A_2 \times \ldots \times R/A_n$$

Where $\pi(r) = (r \text{ mod } A_1, \ldots, r \text{ mod } A_n) = (r + A_1, \ldots, r + A_n)$ is surjective and the kernel is $\bigcap_{k=1}^n A_k$.

Corollary. $R/\bigcap_{k=1}^n A_k \cong R/A_1 \times \ldots \times R/A_n$.

Remark. In $\mathbb{Z}$, $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$ for $g.c.d.(m,n) = 1$. So, $\bigcap_i m_i\mathbb{Z} = (m_1 \cdots m_n)\mathbb{Z}$ for $g.c.d.(m_i, m_j) = 1$.
Proof: $r \in Ker(\pi)$ implies $\pi(r) = (0, \ldots, 0) = (0 + A_1, \ldots, 0 + A_n)$. But, $\pi(r) = (r + A_1, \ldots, r + A_n)$ so $r \in A_i\ \forall i$, so $r \in A_1 \cap \ldots \cap A_n =$

$A_1 \cdots A_n \Rightarrow Ker(\pi) \subset A_1 \cap \ldots \cap A_n$. Similarly, $A_1 \cap \ldots \cap A_n \subseteq Ker(\pi)$. Hence, $Ker(\pi) = A_1 \cap \ldots \cap A_n = A_1 A_2 \cdots A_n$.

PROOF. Consider n=2 (rest follows from induction). Since they are comaximal, $A_1 + A_2 = R$. That means, we can choose $x \in A_1$, $y \in A_2$ such that $x + y = 1$. This gives us a couple of congruences, namely $y \equiv 1 \bmod A_1$ and $x \equiv 1 \bmod A_2$. So given $(b_1 \bmod A_1, b_2 \bmod A_2) \in R/A_1 \times R/A_2$, we get the following:

$$\begin{aligned}(b_1 mod A_1, b_2 mod A_2) &= (b_1 mod A_1, 0) + (0, b_2 mod A_2)\\ &= (b_1 mod A_1, b_1 mod A_1)(1,0) + (b_2 mod A_2, b_2 mod A_2)(0,1)\\ &= \pi(b_1)\pi(y) + \pi(b_2)\pi(x)\\ &= \pi(b_1 y + b_2 x)\end{aligned}$$

So π is surjective.

All that's left to show is $A_1 \cap \ldots \cap A_n = A_1 A_2 \cdots A_n$.

FACT. $A_1 \cap A_2 \cap \ldots \cap A_n = A_1 \cdots A_n$ when R is commutative.

CLAIM. $A_1 \cap A_2 = A_1 \cdot A_2 = \{\sum_{i=1}^n a_i b_i | a_i \in A_1, \, b_i \in A_2\}$.

[Subclaim: $M \cdot N \subseteq M \cap N$ is always true for ideals in a ring. By definition of ideals, $\sum a_i \cdot b_i \in M \cap N$ since $m_i \cdot n_i \in M$ and $m_i \cdot n_i \in N \, \forall i$.]

Proof of claim: We need to check that $A_1 \cap A_2 \subseteq A_1 \cdot A_2$. Write $1 = x + y$ where $x \in A_1, y \in A_2$. Given $a \in A_1 \cap A_2$ implies:

$$a = 1a = (x+y)a = xa + ya \in A_1 \cdot A_2$$

In this case, $x, a \in A_1$ and $y, a \in A_2$, and this sum $xa + ya \in A_1 \cdot A_2$.

$\square$

EXAMPLE. Let $m, n \in \mathbb{Z}$, $g.c.d.(m,n) = 1$. Let $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. By the theorem, this is surjective with kernel $m\mathbb{Z} \cap n\mathbb{Z} = (mn)\mathbb{Z}$. So,

$$\mathbb{Z}/mn\mathbb{Z} \overset{as\, rings}{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ for } g.c.d.(m,n) = 1$$

COROLLARY. Let $n = p_1^{k_1} \cdots p_j^{k_j}$ for $n \in \mathbb{Z}$ where each p_i are distinct primes $\forall \, 1 \leq i \leq j$ $(k_1, \ldots k_n \geq 1 \in \mathbb{Z})$. Then,

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_j^{k_j}\mathbb{Z}$$

CHAPTER 4

Domains

One should note that generally speaking, when considering a ring R in this section, it will be an Integral Domain.

The following will be stated as true now, but will eventually be proven:

$$\text{Fields} \subseteq \text{Euclidean Domains} \subseteq \text{Principal Ideal Domains} \subseteq$$

$$\text{Unique Factorization Rings} \subseteq \text{Integral Domains}$$

DEFINITION 12. *A Norm on a ring R is a function*

$$N : R \to \mathbb{Z}^+ \cup \{0\}$$

Such that $N(0) = 0$. If $N(r) \neq 0$ for $r \neq 0$, we say that N is a positive norm.

EXAMPLE. Let $R = \mathbb{Z}$. The candidate for a norm would be as follows:

$$N(k) = |k|, k \in \mathbb{Z}$$

This happens to be an example of a positive norm.

EXAMPLE. Let R be a polynomial ring, say $S[x]$ where S is any ring. Let:

$$N(p(x)) = deg(p(x))$$

If $s \in S, s \neq 0$, then $N(s) = 0$.

DEFINITION 13. *An integral domain R is a Euclidean domain if there is a norm such that for any two elements $a, b \in R, b \neq 0$, there are $q, r \in R$ such that:*

$$a = qb + r \text{ Where r=0 or N(r)} < \text{N(b)}$$

EXAMPLE. Let $R = \mathbb{Z}$, with $N(K) = |K|$. Given $a, b \in \mathbb{Z}, b \neq 0$, we see that:

$$a = qb + r \text{ where } r = 0 \text{ or } |r| < |b|$$

This shows that $\mathbb{Z}$ is a Euclidean domain.

EXAMPLE. Extending the example of a norm on a polynomial ring $S[x]$, we see that if $S = R$ that the given definition of a norm would also qualify $S[x]$ as a Euclidean domain.

This form in a Euclidean Domain allows an algorithm called the division algorithm, which is as follows: In a domain R, given $a, b \in R, b \neq 0$, we can write:

$$\begin{aligned} a &= q_0 b + r_0 \text{ where } r_0 = 0 \text{ or } N(r_0) < N(b) \\ &\text{assuming } r_0 \neq 0 \text{ we see that:} \\ b &= q_1 r_0 + r_1 \text{ where } r_1 = 0 \text{ or } N(r_1) < N(r_0) \\ r_0 &= q_2 r_1 + r_2 \text{ where } r_2 = 0 \text{ or } N(r_2) < N(r_1) \\ r_1 &= q_3 r_2 + r_3 \text{ where } r_3 = 0 \text{ or } N(r_3) < N(r_2) \\ &\vdots \\ &\text{this process continues until } r_n = 0. \end{aligned}$$

Example. If F is a field, then F is a Euclidean domain with the norm:

$$N : F \to \mathbb{Z}^+ \bigcup \{0\} \text{ where } N(x) = 0$$

Given $a, b \in F, b \neq 0$ we see that:

$$a = ab^{-1} + 0 \text{ where } ab^{-1} \text{ will be the "q" term and 0 will be the r term}$$

Since F is a field, $ab^{-1} \in F$, so this norm holds.

Example. Let $R = \mathbb{Z}$, and $N(x) = 0$. Then:

$$a = qb + 0$$

But since not every element of $\mathbb{Z}$ has an inverse, we will not always find a good candidate for 'q'. Take for example:

$$2 = q3 + 0$$

Since $\frac{2}{3}$ is not a member of $\mathbb{Z}$, this will not be a valid Euclidean domain under this Norm.

Definition 14. *An integral domain R is called a principle ideal domain (PID) if every ideal in R is principle, i.e., it is generated by a single element.*

Example. Let $R = \mathbb{Z}$. The ideals of R are then $n\mathbb{Z}$, for $n \in \mathbb{Z}$ and since $n\mathbb{Z} = (n) = (-n)$, so $\mathbb{Z}$ is a principle ideal domain.

Example. Take $R = \mathbb{Z}[x]$. Then consider the ideal $(2, x)$. This ideal cannot be generated by a single element, so thus $\mathbb{Z}[x]$ is not a PID.

Theorem 9. *Every Euclidean domain is a Principle ideal domain.*

Proof. Let R be a Euclidean Domain under some norm N. Let I be an ideal of R. We have to show that I is principle. Chose $a \in I, a \neq 0$, and $N(a)$ to be smallest in that ideal. Since $a \in I$ we know that $(a) \in I$, which shows that $(a) \subseteq I$. We then have to show the reverse inclusion to prove that $(a) = I$. We know that for any $b \in I$, we can make the following representation: $b = a \cdot x, x \in I$. Let's assume that $b \neq 0, a \neq 0$. Since R is a Euclidean domain, we know that there exist $q, r \in R$ such that:

$$b = qc + r \text{ where r=0 or } N(r) < N(a)$$

Since we assumed that the norm of the element a was the smallest in the ideal I, we know that r must then be zero. So then, we conclude that $b = q \cdot a$, so $b\ in(a)$, and since b is any arbitrary element in I, we know that $I \subseteq (a)$. This shows that $I = (a)$, which tells us that R is a Principle ideal domain. □

DEFINITION 15. *A greatest common divisor of 2 elements $a, b \in R$ (denoted 'gcd') is an element $d \in R$ such that:*

(1) *$d|a$ and $d|b$ (i.e., $d = dx, b = dy, x, y \in R$)*
(2) *If $e|a$ and $e|b, thene|d$.*

REMARK. Taking this definition of a common divisor of elements are putting it in terms of ideals, we have:

$$d|a \iff a = dx, \text{ for some x } \iff a \in (x) \iff (a) \subseteq (d)$$

And

$$d|b \iff b = dy \text{ for some y } \iff b \in (d) \iff (b) \subseteq (d)$$

So then, we have the following two requirements in terms of ideals:

(1) $d|a$ and $d|b \iff (a, b) \subseteq (d)$ Where $(a, b) = \sum c \cdot a + f \cdot b = \sum c \cdot dx + f \cdot dy = d \sum (cx + fy)$
(2) If $(a, b) \subseteq (e)$, then $(d) \subseteq (e)$.

So, the gcd of a and b is d, if (d) is the smallest principle ideal containing (a, b).

EXAMPLE. In $\mathbb{Z}$, let $a, b \in \mathbb{Z}, a = 12, b = 16$. Since $(4) = (-4)$ are the smallest principle ideals containing $(12, 16)$, we know that the greatest common divisors of a and b are ± 4.

FACT. The following are true:

(1) If (a,b) is principle, then (a,b)=(x) and x is the greatest common divisor of a and b.
(2) If R is a PID, for any two elements $a, b \in R$, the greatest common divisor of a and b exists.

EXAMPLE. $\mathbb{Z}[x]$ is not a PID, because $(2, x)$ is not principle. But, we know that the greatest common divisor of 2 and x does exist. In finding the gcd, (let's call it 'p') we need to find an element such that the following is true:

$$p|2 \text{ and } p|x$$

Since the only candidate for p is ± 1, we know that the greatest common divisor of 2 and x is ± 1.

LEMMA. If $(d) = (d')$, where both ideals are non zero in a ring R, $d' = ud$ for some unit $u \in R$. So, any two greatest common divisors (d, d') differ by some unit u.

PROOF. If $(d) = (d')$, then $d \in (d')$, so $d = xd'$. Similarly, $d' \in (d)$ so $d' = yd$. Thus, $d = xyd$, which implies that $x(1 - xy) = 0$. So, $xy = 1$ since we know that these ideals are nonzero in R, displaying that x and y are units. Thus, d and d' differ only by a unit. □

REMARK. If $(a, b) \subseteq (d), (a, b) \subseteq (d')$ then d and d' are gcds of a and b if and only if $(d) = (d')$.

DEFINITION 16. *x and y are called 'associates' if $x = uy$ for some unit u.*

Recall that if R is a Euclidean Domain and $a, b \in R, a, b \neq 0$ that

$$a = q_0 b + r_0, N(r_0) < N(b) \text{ or } r_0 = 0$$

$$\vdots$$

And that we can continue this process until we get some r_n, where $r_{n+1} = 0$. Our Claim is now that this r_n is a[1] greatest common divisor of a, b.

PROOF. We need to show that $r_n | a$ and $r_n | b$. This is easy to do. We know that:

$$r_n | r_{n-1}$$

And by working up, that

$$r_n | r_{n-2}$$

$$\vdots$$

$$r_n | a, \ r_n | b$$

Then we need to show that $r_n = xa + yb$, for some x, y. Then, if $e | a$ and $e | b$, then we know that $e | r_n$, which will show that r_n is a greatest common divisor. Again, this comes from working upwards:

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-2} - q_{n-1} r_{n-2})$$

$$\vdots$$

$$r_n = \backsim\backsim a + \backsim\backsim b$$

□

[1]we say 'a' greatest common divisor because as we've seen, the gcd of two elements does not have to be unique.

FACT. $(a|b, b|a) \iff ((b) \subseteq (a)$ and $(a) \subseteq (b)) \iff$ a and b are associates. If a and b are associates, then $a = bu, u^{-1}a = b$. Conversely, if (a)=(b) then

$$(a) \subseteq (b) \Rightarrow a = bx$$

And

$$(b) \subseteq (a) \Rightarrow b = ay$$

Thus,

$$a = bx = axy \Rightarrow a(1 - xy) = 0$$

Thus, $xy = 1$ so x and y are units. Since $a = bx$, where x is a unit, we know that a and b are associates.

COROLLARY.

$$(a) = R \text{ if and only if a is a unit.}$$

PROOF. R=(1), so if (a)=(1), (a)=R. This happens if and only if a and 1 are associates, i.e. $ax = 1$ for some x. And we know that this happens when a is a unit. □

Recall, if an ideal M is maximal in R, then M is prime.

$$M \text{maximal in R} \iff R/M \text{ is a field } \Rightarrow R/M \text{ is an integral domain}$$
$$\iff M \text{ is a prime Ideal in R.}$$

EXAMPLE. Notice that :

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$$

Which is an integral domain, not a field. Thus, (x) is prime but not maximal in $\mathbb{Z}[x]$.

THEOREM 10. *If R is a PID, every nonzero prime ideal in R is maximal.*

PROOF. Let (p) be a prime ideal in R, a principle ideal domain. We want to show that if $(p) \subseteq$ some ideal (m) $\subseteq R$, that $(m) = (p)$ or $(m) = R$. If $(p) \subseteq (m)$, this means that $p \in (m)$, so $p = mr$ for some $r \in R$. Thus, $mr \in (p)$, which is a prime ideal, so either $m \in (p)$ or $r \in (p)$. If $m \in (p)$, then $(m) \subseteq (p) \Rightarrow (m) = (p)$. If $r \in (p)$, then $r = xp$, and since $p = mr$, $p = mxp$. Thus $mx = 1$, so m is a unit, and $(m) = R$. □

REMARK. If F is a field, F[x] is a Euclidean domain and thus a Principle ideal domain. The Converse is also true, if R[x] is a PID, R is then a field.

PROOF.

$$R[x]/(x) \cong (R) \text{ by the first isomorphism theorem}$$

So thus (x) is prime. But R[x] is a PID, so (x) is maximal, and since $R[x]/(x) \cong R$, R is a field. □

DEFINITION 17. *Let R be an integral domain.*

(1) *We say that* $r \in R$ *is irreducible if* r *is not a unit, and whenever* $r = a \cdot b$ a *is a unit or* b *is a unit. Otherwise, we say that* r *is reducible.*
(2) $p \in R$ *is called prime if* (p) *is a prime ideal in* R*.*

Lemma. In any integral domain, every prime element is irreducible.

Proof. Let p be prime, so (p) is a prime ideal. Suppose $p = ab$, we need to show that either a or b is a unit. Since $ab \in (p)$, this implies that $a \in (p)$ or $b \in (p)$. I.e., a=px or b=py.

$$\text{if } a = px = abx, \text{ so bx=1, showing that b is a unit}$$

$$\text{if } b = py = aby \text{ so ay=1, so a is a unit}$$

Thus, either a or b is a unit. □

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$.

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

We can see that 3 divides 3, and thus should divide the right hand side, but 3 does not divide $2 \pm \sqrt{-5})$

$$(3 \cdot (a + b\sqrt{-5}) \neq 2 \pm \sqrt{-5} \quad \forall a, b \in \mathbb{Z})$$

Thus, 3 is not prime, i.e. (3) is not prime.

$$q = (2 + \sqrt{-5})(2 - \sqrt{-5}) \in (3)$$

But $(2 \pm \sqrt{-5}) \notin (3)$. However, 3 is irreducible in this ring.

Lemma. Let R be an integral domain. $r \in R$ is irreducible $\iff$ (r) is 'maximal among all principle ideals', i.e.: If $(r) \subseteq (s) \subseteq R$ then $(r) = (s)$ or $(s) = R$ where (s) is principle.

Proof. Suppose whenever $(r) \subseteq (s) \subseteq R$ that either $(r) = (s)$ or $(s) = R$.We would r to be irreducible, so let $r = ab$. Then, $a|r$ so $(r) \subseteq (a) \subseteq R$. By our assumption, $(r) = (a)$ or $(a) = R$, which implies r and s are associates where b is a unit, or s itself is a unit. This shows that r is irreducible.

Now let r be irreducible, and $(r) \subseteq (s) \subseteq R$. So, r=st. If s is a unit then (s)=R. If t is a unit, then r and s are associates, so $(r) = (s)$. □

Corollary. In a PID, r is irreducible if and only if r is maximal. The proof of this comes directly from the Lemma, since maximal ideals are equivalent to maximal among all principal ideals.

Corollary. In a PID R, for $r \in R$, the following are equivalent:
(1) (r) is prime
(2) r is prime
(3) r is irreducible
(4) (r) is maximal

Definition 18. *A unique factorization domain or UFD is an integral domain R such that:*

(1) *For $r \in R$, where r is not a unit and $r \neq 0$, we can write:*

$$r = p_1 p_2 .... p_n$$

Where p_i is irreducible for all i.

(2) *(There is uniqueness up to associates) If*

$$r = p_1 p_2 ... p_n$$

And

$$r = q_1 q_2 ... q_m$$

Where q_i, p_i are irreducible for all i, then $m = n$ and every p_i is an associate of exactly one q_i, and cive versa.

$$\exists r \in \sum_n \text{ such that } p_i \text{ is an associate of } q_{\sigma(i)}$$

Example. If F is a field, F is a UFD. Every element is a unit, so every element has a multiplicative inverse. There is nothing to check here, because every non-zero element is a unit.

Example.

$$\mathbb{Z}[2i] = \{a + b2i | a, b \in \mathbb{Z}\}$$

Notice that 'i' isn't in this ring. We see that the following is true:

$$4 = 2 \cdot 2 = (2i) \cdot (-2i)$$

Are 2,2i, and -2i irreducible? Well:

$$2 = a \cdot b \Rightarrow \text{ a or b} = \pm 1$$

And

$$2i = c \cdot d \Rightarrow \text{ c or d} = \pm 1$$

Thus, $2, \pm 2i$ are irreducible since 1 is a unit. Are 2 and $2i$ associates? This would imply that

$$2 \cdot (x + i2y) = 21$$

Where (x+i2y) is a unit. Since the units in this ring are ± 1, we see that this is impossible. Thus we see that we have a nonunique factorization of 4 into a product of irreducibles.

Claim: In a UFD, x is prime if and only if x is irreducible.

Proof. In a UFD, which is an integral domain, prime elements are always irreducible. Suppose x is irreducible in a UFD. We would like to show that x is prime, which we can do by showing that (x) is prime. Suppose $ab \in (x)$. We would like to show that either $a \in (x)$ or $b \in (x)$; i.e., if $a|ab \Rightarrow x|a$ or $x|b$. Suppose that $x|(a, b)$. Then,

$$xc = ab = (a_1 a_2 ... a_n)(b_1 b_2 ... b_m)$$

Because we are working in a unique factorization domain. This shows that:

$$x \cdot (c_1 c_2 ... c_n) = (a_1 a_2 ... a_n)(b_1 b_2 ... b_m)$$

and by uniqueness, x is an associate of some a_i or b_i. If x is an associate of a_i, this implies that $x \cdot x = a_i$ for some unit d. This means that $x|a_i$, so $x|(a_1 a_2 ... a_n)$, which in turn means that $x|a$. Similarly, if x is an associate of b_k then $x|b$. Thus, x is prime. □

FACT. In a UFD, greatest common divisors always exist. Given:

$$a = p_i^{k_1} p_2 \cdot ... \cdot_m^{k_n}$$

and

$$b = p_i^{j_1} \cdot ... \cdot p_n^{j_n}$$

Where p_i are distinct primes (irreducibles), the following is true:

$$gcd(a, b) = p_1^{min(k_1, j_1)} \cdot ... \cdot p_n^{\min(k_n, j_n)}$$

Our claim is that:

(1) $d|a$ and $d|b$
(2) if $e|a$ and $e|b$ then $e|d$

Consider: the following representation of the element 'e':

$$e = c_1^{m_1} c_2^{m_2} \cdot ... \cdot c_r^{m_r}$$

Where c_i are distinct primes for all i. Since e divides both a and b,

$$e = p_1^{s_1} p_2^{s_2} \cdot ... \cdot p_n^{s_n} \cdot u$$

Where u is a unit. Thus, we see that since $e|a$ and $e|b$, $s_i \leq min(k_i, j_i)$. This then implies that $e|d$. Notice that:

$$a \cdot b = (gcd(a, b)(lcm(a, b))$$

THEOREM 11. *Every principle ideal domain is a unique factorization domain.*

PROOF. Let R be a PID, $r \in R$ be a non-unit. We would like to show that r is equal to a product of non-units. If r is not irreducible, then:

$$r = r_1 r_2$$

Where r_1, r_2 are not units. If r_1 is reducible, then:

$$r = (r_{11} r_{12}) r_2$$

If $r_1 1$ is reducible, then:

$$r = ((r_{111} r_{112}) r_{12}) r_2)$$

$$\vdots$$

We need to check that this process can't go on forever, that eventually r will be written as a product of irreducibles. If it were so, that means:

$$r_1 | r, \;\; r_{11} | r_1, \;\; r_{111} | r_{11} \ldots$$

And in terms of ideals, this means:

$$(r) \subseteq (r_1) \subseteq (r_{11}) \subseteq (r_{111}) \subseteq ... \subseteq R$$

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq R$$

The claim is that $I_n = I_{n+1} = I_{n+2} = ... = R$ for some n. The proof of that is the

$$I = \bigcup_j I_j$$

is an ideal, and in a principle ideal domain, every ideal is principal. Thus, I is principal. So, I=(a), so $a \in I_n$ for some n. This implies that:

$$(a) \subseteq I_n \subseteq I = (a)$$

so

$$(a) = I_n = I_{n+1} = I_{n+2} = ...I$$

In a PID, the ascending chain of ideals is a principle ideal. So, we can factor irreducibles into finitely many irreducibles. In showing uniqueness, we see that when

$$p_1 p_2 ... p_k = q_1 q_2 ... q_n$$

That we can pick off elements one by one (since given a p_i it must divide $q_1 q_2 ... q_n$) until we see that the factorization was unique. □

Corollary. Since $\mathbb{Z}$ is a Euclidean Domain, and therefor a PID, it is thus a UFD.

$$n = p_1 p_2 p_3 ... p_k$$

Where p_i are prime numbers for all i, and this factorization is unique up to a reordering of p_i's and multiplication by the units in $\mathbb{Z}$, which are ± 1.

Recall: $R[x]$ for any ring R denotes "polynomials in x with coefficients in R".

Definition 19. *Let R be a ring. The following is true:*

$$R[x_1, x_2, ...x_n]) = (R[x_1, x_2, ...x_{n-1})[x_n])$$

Also recall that $R[x]$ has a norm given by:

$$N(p(x)) = deg(p(x))$$

And the units of $R[x]$ are units of R. If R is an integral domain, then so is $R[x]$.

Proof. If

$$p(x) \cdot q(x) = 0 \Rightarrow N(p((x) \cdot q(x)) = N(p(x)) + N(q(x)) = 0 = N(constant)$$

So thus, either $N(p(x)) = 0$ or $N(q(x)) = 0$. This implies that both $p(x)$ and $q(x)$ constant, we'll call them a and b respectively. We then know that:

$$a \cdot b = 0$$

And since R is an integral domain, we know that either $a = 0$ or $b = 0$. Thus, $p(x) = 0$ or $q(x) = 0$. □

Let I be an ideal in R. Since I is a subring of R, we can say that $I[x] \subseteq_{subgring} R[x]$. Given an element $(r_0 + r_1x + ...r_nx^n)$, we see that when taking an element $(a_kx^k) \in I[x]$, then when you multiply these elements you get: $(a_kr_0x^K + a_kr_1x^{k+1} + ...a_kr_nx^{k+n})$. We see that the coefficients $(a_kr_0, a_kr_1, ...a_kr_n)$ will live in I, since I is an ideal. From this we can conclude that $I[x]$ is an ideal of $R[x]$ if I is an ideal of R (it turns out the converse is also true; if $I[x]$ is an ideal of $R[x]$, then I is an ideal of R).

REMARK.

$$R[x]/I[x] \cong (R/I)[x]$$

Where the isomorphism is in terms of rings.

PROOF. Define a homomorphism:

$$\varphi : R[x] \mapsto (R/I)[x]$$

where

$$\varphi(\sum_{k=1}^{n} r_kx^k) = \sum_{k=1}^{n}(r_k + I)x^k$$

(e.g., let $I = 3\mathbb{Z} \subseteq \mathbb{Z}$. The element $4x^5 + 3x^2 + 1 \overset{\varphi}{\longmapsto} x^5 + 1$, because the coefficients would be reduced by modulo 3). The map φ is surjective, because

$$Ker(\varphi) = \{p(x)| \text{ the coefficients of p(x) are in I } \} = I[x]$$

And by the first isomorphism theorem,

$$R[x]/I[x] \cong Im(\varphi) = (R/I)[x]$$

□

COROLLARY. If I is prime in R, $I[x]$ is prime in $R[x]$.

PROOF.

$$\text{I prime in R } \iff$$
$$(R/I) \text{ is an integral domain } \iff$$
$$R[x]/I[x] \text{ is an integral domain } \iff$$
$$I[x] \text{ is prime in } R[x]$$

□

EXAMPLE. $n\mathbb{Z} \subseteq \mathbb{Z}$ is a prime ideal if and only if n is prime. So, $(n\mathbb{Z})[x]$ is prime in $\mathbb{Z}[x]$ if and only if n is prime.

If F is a field then $F[x]$ is a Euclidean domain, where $N(p(x)) = deg(p(x))$. Given $a(x), b(x) \in F[x]$ where $b(x) \neq 0$ we see that $a(x) = b(x)q(x) + r(x)$ where $r(x) = 0$ or $N(r(x)) < N(b(x))$. So, $F[x]$ is a unique factorization domain. We'll show that $R[x]$ is a unique factorization if and only if R is a unique factorization domain.

PROOF. The one direction of this statement is trivial: if $R[x]$ is a unique factorization domain, then R must also be a UFD, since $R \subseteq R[x]$. We'll use the ring of fractions F of R to better understand the oppositve direction of this statement. □

EXAMPLE. $\mathbb{Q}[x]$ is a Euclidean domain, since $\mathbb{Q}$ is a field. Notice that $(2, x)$ is a prime ideal in $\mathbb{Q}[x]$, because $(2, x) = \mathbb{Q}[x]$. T

We would like to use the ring of fractions F of R to study factorization in $R[x]$. A brief paraphrase of Gauss's lemma goes as follows: "Given R (a UFD) and F (a field of factors of R), if you can factor in F[x] then you can factor in R[x]".

THEOREM 12. *Let $p(x) \in R[x]$ and suppose $p(x) = A(x) \cdot B(x)$ where $A(x), B(x) \in F[x]$, then there exists $r, s \in F$ such that:*

$$r \cdot A(x) = a(x) \in R[x]$$

$$s \cdot B(x) = b(x) \in R[x]$$

and

$$p(x) = a(x)b(x)$$

EXAMPLE.

$$x^2 \in \mathbb{Z} \subseteq \mathbb{Q}[x]$$

Factoring x^2 in $\mathbb{Q}[x]$, we get:

$$x^2 = 2x \cdot \frac{1}{2}x$$

Then, we can do the following:

$$\frac{1}{2}(2x) = x \text{ and } 2(\frac{1}{2}x) = x$$

where $2, \frac{1}{2} \in \mathbb{Q}$.

PROOF. Given $p(x) = A(x)B(x)$ where the coefficients of $A(x)$ and $B(x)$ are elements of F, i.e., are "fractions" as we think of them. Let $d =$ product of all denominators of the fractions . Then,

$$dp(x) = m(x)n(x)$$

Where $m(x), n(x) \in R[x]$. $d \in R$ since R is a unique factorization domain, and:

$$d = c_1 c_2 ... c_n$$

Where c_i is irreducible in r. We then conclude that:

$$c_1 c_2 ... c_n p(x) = m(x)n(x)$$

We would like to show that for each i, $c_i | m(x)$ or $c_i | n(x)$. We know that:

$$R/(c_i) \text{ is an integral domain } \Rightarrow R/(c_i)[x] \text{ is an ID}$$

and

$$(R/(c_i))[x] \cong R[x]/(c_i)[x]$$

So, when considering

$$c_1c_2...c_np(x) = m(x)n(x)$$

reduce modulus c_i term by term, i.e., send the coefficients in R to coefficients in $R/(c_i)$. Let $i = 1$. Then,

$$0 \equiv m(\bar{x}) \cdot n(\bar{x})$$

So, $m(\bar{x})$ and $n(\bar{x})$ are elements of $(R/(c_i))[x]$, which we know to be an integral domain. Thus, by the definition of an integral domain, either:

$$m(\bar{x}) = 0 \text{ or } n(\bar{x})] = 0$$

So, c_i must divide the coefficients of either m(x) or n(x). This implies that

$$\frac{m(x)}{c_i} \in R[x] \text{ or } \frac{n(x)}{c_i} \in R[x]$$

Taking this operation for all i, we end up getting $p(x) = a(x) \cdot b(x)$ where $a(x), b(x) \in R[x]$.

□

The Idea is that if you can factor with field coefficients, then you can factor with ring coefficients. However, we still would like to give a solid proof that R is a UFD if and only if $R[x]$ is a UFD. To help this along, we have the following corollary:

Corollary. Let R be a UFD, and suppose that $p(x) \in R[x]$. If The greatest common divisor of the coefficients of p(x) is 1, then p(x) is reducible in R[x] if and only if p(x) is reducible in F[x]/

Proof. If p(x) is reducible in F[x], then p(x) is reducible in R[x] by Gauss's lemma (recall that p(x) is reducible in F[x] if and only if p(x)=a(x)b(x) where a(x) and b(x) are not constants). So by Gauss's lemma, we factor p(x) into non-units in R[x].

If p(x) is reducible in R[x], then p(x)=a(x)b(x), where $a(x), b(x) \in R[x]$ and $a(x), b(x)$ are not units. If coefficients of p(x) have a greatest common divisor of 1 (bear in mind you can force this condition by factoring out by the greatest common divisor in R), then a(x) and b(x) must not be constant polynomials- otherwise, if $a(x) = a_0$ then $a_0|p(x) \Rightarrow a_0|$the greatest common divisor of p(x) and since the gcd(p(x))=1, we know that $a_0 = 1$, which is a unit. Thus, $p(x) = a(x)b(x)$ where $deg(a(x)) \geq 1$ and $deg(b(x)) \geq 1$.

Then, a(x) and b(x) are not units in F[x], so $p(x) = a(x)b(x)$ is a factorization of $p(x) \in F[x]$ into non-units, so we know that p(x) is reducible in F[x]. □

Example. The following polynomial is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$:

$$2x^3 + 3x^2 + 5x + 7$$

Take an even easier example- is 2x reducible in $\mathbb{Z}$? We know that this is true if and 2x is reducible in $\mathbb{Q}[x]$. And since:

$$2x = 2 \cdot x = \frac{2}{47} \cdot 47 \cdot x = ...$$

2x isn't uniquely factor able in $\mathbb{Q}$, we know that 2x is irreducible in $\mathbb{Q}[x]$. On the other hand though, it turns out that 2x is reducible in $\mathbb{Z}[x]$, and this doesn't violate our corollary because the greatest common divisor of 2x is not 1.

DEFINITION 20. *A polynomial:*

$$a_n x^n + a_{n-1} x^{n-2} + ... + a_1 x + a_0$$

Is called monic if $a_n = 1$. *Notice that a monic polynomial in R[x] is irreducible in R[x] if and only if it is irreducible in F[x], since the leading coefficient forces the greatest common divisor of the coefficients to be 1.*

THEOREM 13. *R is a UFD if and only if R[x] is a UFD.*

PROOF. If R[x] is a UFD, then R is a UFD since $R \subset R[x]$ under the map $a \mapsto a + 0x^1 + 0x^2 + ...$

No suppose that R is a UFD and $p(x) \in R[x]$. we can write p(x) as:

$$p(x) = \text{a gcd of the coefficients of p(x) } \cdot q(x)$$

We want to show that we can factor p(x) uniquely (up to associates) into irreducibles in R[x]. We know that the following is true from the fact that R is a UFD:

$$p(x) = gcd(p(x)) \cdot q(x) = (d_1 \cdot d_2 \dots d_n) q(x) \qquad q(x) \in R[x], d_i \in R$$

Focus of the q(x) term- we know that the greatest common divisor of its coefficients is 1, since we factored out by the greatest common divisor of p(x). Recall that if(q)x is irreducible in R[x], we're finished with this proof. Otherwise, if q(x) is reducible in F[x], then q(x) is reducible in R[x]. We can claim the following:

$$q(x) = \underbrace{m(x)n(x)}_{\in F[x]} = \underbrace{\underbrace{r}_{\in F} m(x) \cdot \underbrace{s}_{\in F} n(x)}_{\in R[x]}$$

This follows from Gauss's lemma. Since the gcd of q(x) was 1, we know that m(x) and n(x) were not constants, otherwise they would be units.

Think of q(x) as a polynomial with field coefficients, $q(x) \in F[x]$, and since F is a field, F[x] is a Euclidean Domain and thus $F[x]$ is a UFD. So, we can write:

$$q(x) = q_1(x) \cdot q_2(x) \dots q_n(x)$$

Where $q_i(x) \in F[x]$ are irreducible. By Gauss's lemma, we can write the following:

$$q(x) = r_1 p_1(x) \cdot r_2 p_2(x) \dots r_n p_n(x)$$

Where moreover, $r_ip_i(x) \in R[x]$ and $r_i \in F$. We know know the following two things:

(1) We know that the gcd in R of $a_ip_i(x)$ is 1, because we know that the greatest common divisor of q(x) is 1.
(2) Each $a_ip_i(x)$ is irreducible in F[x], since $a_i \in F$ is a unit and $q(x) \in F[x]$ is irreducible because $F[x]$ is a UFD.

Now, through these facts and our lemma, we know that $a_ip_i(x)$ is irreducible in $R[x]$ for each i. (recall that the lemma said that if $p(x) \in R[x] and gcd(p(x)) = 1$ that $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $F[x]$. However, we still need to prove that this factorization of q(x) is unique.

Suppose we have the following factorizations of q(x):

$$q(x) = q_1(x)q_2(x)\dots q_n(x) = s_1(x)s_2(x)\dots s_m(x)$$

Where $s_i(x), q_i(x)$ are irreducible in $R[x]$. We need to prove that each $q(x)$ is an associate of some $s(x)$.

First, recall that each representation of q(x) is a factorization in F[x] into irreducibles. Since $F[x]$ is a UFD, we know that $n = m$ and after a reordering, that:

$$q_i = \frac{a_i}{b_i}s(x)$$

So

$$b_iq(x) = a_is_i(x) \quad a_i, b_i \in R$$

We know that a_i and b_i are associates since the greatest common divisor of $q_i(x)$ and $s_i(x)$ is 1. This implies that:

$$a_i = ub_i \quad \text{and } \frac{a_i}{b_i} = u \text{ where u is a unit in R}$$

□

Example. $\mathbb{Z}[x, y] = (\mathbb{Z}[x])[y]$ Is $\mathbb{Z}[x]$ a UFD? The answer is yes, since $\mathbb{Z}$ is a UFD, so analogously we know that $(\mathbb{Z}[x])[y]$ is also a UFD! The following corrolary follows from this idea.

Corollary. $\mathbb{Z}[x_1, x_2, ...x_n]$ is a UFD

Definition 21. *A root of a polynomial* $p(x) \in R[x]$ *is an element* $r \in R$ *such that* $p(r) = 0$.

Lemma. $p(x) \in F[x]$ has a degree 1 factor if and only if $p(x)$ has a root in F. This is true because:

$$p(x) = q(x) \cdot (x - \alpha) + r(x) \text{ and } r(x) = 0 \text{ or } deg(r(x)) < deg(x - \alpha) = 1$$

$$0 = p(\alpha) = q(\alpha) \cdot 0 + r(\alpha)$$

So we can conclude that r(x)=0. Thus, $(x - \alpha)|p(x)$.

Corollary. If deg(p(x))=2 or deg(p(x)) = 3, $p(x) = F[x]$, p(x) is irreducible if and only if p(x) has no roots in F. (the reason for 2 or 3 is because it forces linear factors.)

Example.

$$p(x) = x^2 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x]$$

The only elements in $\mathbb{Z}/2\mathbb{Z}$ are 0 and 1, neither of which are roots for this polynomial. Thus, $p(x)$ is irreducible in $\mathbb{Z}/2\mathbb{Z}$.

However, if $p(x) \in \mathbb{Z}/3\mathbb{Z}$, p(x) is reducible since p(1) = 0. Also notice that when factoring in this ring, the following is true:

$$p(x) = (x-1)(x-1) \text{ under mod } 3$$

We do have other root tests for polynomials of higher degree, take for example:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in R[x]$$

If $p(\frac{r}{s}) \in F = 0$ and (r,s)=1 where R is a UFD and F is a field of fractions, the following is true

$$r|a_0 \text{ and } s|a_n$$

This can be shown through the following:

$$\begin{aligned} 0 = p(\frac{r}{s}) &= a_n(\frac{r}{s})^n + a_{n-1}(\frac{r}{s})^{n-1} + ...a_1\frac{r}{s} + a_0 \\ -s^n a_0 &= a_n r^n + a_{n-1}x^{n-1} + ... + a_i r s^{n-1} \\ &\Rightarrow r|s^n a_0 \end{aligned}$$

And since r and s are relatively prime, we know that $r|a_0$. Similarly we can show that $s|a_n$.

Example. Suppose that p(x) is a monic polynomial, $p(x) \neq 0 \forall r \in R$ such that $r|a_0$ and

$$p(x) = 1x^n + ... + a_o$$

We can conclude that p(x) has no roots in F, since the monic property of p(x) forces $s = 1$.

Example.

$$p(x) = x^3 - 3x - 1 \in \mathbb{Z}[x]$$

Since this polynomial is monic, and only $\pm 1|a_0$ we only have to try ± 1 for r. Since $p(1) \neq 0$ and $p(-1) \neq 0$, we can conclude that p(x) has no roots in $\mathbb{Z}$, and is irreducible.

Property. Let I be a principle ideal of a ring R. We have the following maps:

$$R[x] \to R/I[x]$$

$$p(x) \mapsto p(\bar{x})$$

Where $p(\bar{x})$ denotes p(x) reduced with respect to the ideal I.

Let p(x) be monic, and non constant. If there is no factorization of $p(\bar{x}$ into polynomials of lower degree, then p(x) cannot be factored into polynomials of strictly lower degree $\in R[x]$.

PROOF. Suppose that p(x) is reducible in $R[x]$. Thus,

$$p(x) = a(x)b(x), \quad a(x), b(x) \neq \text{ constants}$$

Then,

$$p(\bar{x}) = a(\bar{x}) \cdot b(\bar{x})$$

Is a factorization of $p(\bar{x})$ into polynomials of strictly lower degree, since $deg(p(\bar{x})) = deg(p(x)$ (which follows from p(x) being monic and I being a proper ideal, which ensures that there are no units in I). □

EXAMPLE.

$$x^2 + x + 1 \in \mathbb{Z}$$

Reduce this polynomial by the ideal $I = 2\mathbb{Z}$. Since this polynomial has no roots in $\mathbb{Z}/2\mathbb{Z}[x]$, it has no factorization in $\mathbb{Z}[x]$ and is thus irreducible.

EXAMPLE.

$$x^2 + 1 \in \mathbb{Z}[x]$$

And let $I = 3\mathbb{Z}$. $x^2 + 1$ has no roots in $\mathbb{Z}/3\mathbb{Z}$, so $x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ since it is irreducible in $\mathbb{Z}/3\mathbb{Z}[x]$. Notice that we should not allow $I = 2\mathbb{Z}$, because this polynomial does have roots in $\mathbb{Z}/2\mathbb{Z}[x]$. However the existence of roots in the quotient group is not enough to show that p(x) is reducible in $\mathbb{Z}[x]$.

CHAPTER 5

Eisenstein's Criterion

The following is a theorem refered to as Eisenstein's Criterion:

THEOREM 14. *Let R be a ring, P a prime ideal, and*

$$p(x) = x^n + c_{n-1}x^{n-1} + ... + c_0$$

Where $c_i \in P$ *and* $c_0 \notin P^2 = (P \cdot P)$*. Then, p(x) is irreducible in R[x].*

PROOF. Suppose that p(x) is reducible in $R[x]$, say

$$p(x) = a(x)b(x)$$

Where $a(x)$ and $b(x)$ are nonconstant polynomials. Reducing this equation modulo P and using the assumptions on the coefficients of p(x) we get the equation:

$$x^n = a(x)\bar{b}(x) \in (R/P)[x]$$

Where the bar denotes the polynomials with coefficients reduced with respect to the prime ideal P. Since P is prime, we know that R/P is an integral domain, and it follows that the constant terms of both a(x) and b(x) are elements of P, and thus $a(\bar{x})$ and $b(\bar{x})$ have 0 as their constant terms. But if this were true, it would follow that the constant term c_0 of p(x) would be the product of two elements of P, and thus be an element of P^2, a contraction.

□

This is commonly applied to $\mathbb{Z}[x]$, and the result is stated explicitly below:

COROLLARY. Let p be a prime in $\mathbb{Z}$ and let

$$p(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Z}[x], n \geq 1$$

Suppose that p divides a_i for all i, but that p^2 does not divide a_0. From this we can conclude that p(x) is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

EXAMPLE. Take the following polynomial:

$$x^6 + 1 - x^4 + 15x + 5$$

Notice that the prime number 5 divides 10,15, and 5, but 5^2 does not divide 5. Thus, this polynomial is irreducible. The same idea applies to a polynomial in the following form:

$$x^n - p$$

Where p is prime, because p^2 does not divide p.

REMARK. Recall that if $F[x]$ is a ED, it is then also a PID and therefore a UFD. Given $f(x) \in F[x]$, we know that $f(x)$ is irreducible if and only if the ideal generated by f(x) is maximal; $(f(x))$ is maximal. This is due to the fact that if (f(x)) is maximal it would cause $F[x]/(f(x))$ to be a field, and we know that $f(x)$ has a root α if and only if $x - \alpha | f(x)$, which would happen since $F[x]/(f(x))$ is a field. Through induction, we see that f(x) has roots $\alpha_1, \alpha_2, ...\alpha_n$ if and only if $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) | f(x)$.

One consequence of this is that:

$$\begin{aligned} n &= deg[(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)] \\ &= \text{ The number of roots in the set } \{\alpha_1, \alpha_2, ..., \alpha_n\} \\ &= \text{ The number of roots of f(x) } \leq \text{ than the degree of f.} \end{aligned}$$

CHAPTER 6

Modules and Algebras

Definition 22. *Let R be a ring. A left R-module is an abelian group $(M, +)$ with a function from:*

$$R \times M \to M, \quad (r, m) \mapsto r \cdot m$$

Such that the following properties hold:

(1) $(r \cdot s)\mathbf{m} = r(s \cdot \mathbf{m})$
(2) $(r + s)\mathbf{m} = r\mathbf{m} + s\mathbf{m}$
(3) $r \cdot (\mathbf{m} + \mathbf{n}) = r\mathbf{m} + r\mathbf{n}$

For all $r, s \in R$ and $\mathbf{m}, \mathbf{n} \in M$. Also, if $1 \in R$, we demand that $1 \cdot m = m$.

Definition 23. *Suppose that $R = (\mathbb{R}, +, \cdot)$ and that $M = \mathbb{R}^n = \{(v_1, v_2, ..., v_n) | v_i \in \mathbb{R}\}$. Thus, M is an abelian group under addition, and:*

$$\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$$

Under the mapping

$$(r, (v_1, v_2, ..., v_n)) \mapsto (rv_1, rv_2, ..., rv_n)$$

This defines a left $\mathbb{R}$ module.

More generally, left $\mathbb{R}$ modules are called $\mathbb{R}$-vector spaces. Even more generally, if F is a field, left F-modules are the same as right F-modules, or "vector spaces over F".

Example. If R is a ring, then R is an abelian group under addition, and $M = R$ is a left R-module under the mapping

$$R \times R \to R \quad (r, m) \mapsto (r \cdot m)$$

Which holds by associativity and the distributive law thanks to the ring structure of R.

Example. A submodule of a left R-module M is a subgroup $N \subseteq M$ such that:

$$R \times N \to R \times M \to M \to N$$

Where the last arrow really implies that the action of R on the subgroup N of M has an image back in N, and it's function defines a left R-module.

We claim that submodules of vector spaces are really what we've called subspaces.

EXAMPLE. What are the submodules of the R-module R? Well, we need a subgroup $S \subseteq R$ such that

$$R \times S \to R \times R \to R \to S$$

i.e., if $r \in R, s \in S, r \cdot s \in S$ so S is a subring of R and a left ideal of R.

EXAMPLE. If F is a field, define:

$$F^n = \{a_1, a_2, ..., a_n | a_i \in F\}$$

F^n is then a F-vector space under the following map:

$$F \times F^n \to F^n \quad (\alpha, (a_1, a_2, ..., a_n)) \mapsto (\alpha a_1, \alpha a_2, ..., \alpha a_n)$$

E.g., $(\mathbb{Z}/p\mathbb{Z})^n$ is a $\mathbb{Z}/p\mathbb{Z}$ vector space.

Similarly, we can define for any ring R and $n \in \mathbb{N}$ a left R-module:

$$R^n = \{a_1, a_2, ..., a_n | a_i \in R\}$$

Notice that if n=1, this is the same as the example above in which R is a left R-module over itself. This module is called a "free left R-module of rank n".

EXAMPLE. Let $R = \mathbb{Z}$. A natural question to ask is, what are $\mathbb{Z}$-modules? Our claim is that a $\mathbb{Z}$-module is exactly an abelian group.

PROOF. By definition, every $\mathbb{Z}$-module is an abelian group. Conversely, suppose that $(M, +)$ is an abelian group. We can make $(M, +)$ into a $\mathbb{Z}$-module in the following way:

$$\mathbb{Z} \times M \to M \quad (k, m) \mapsto \underbrace{m + m + m + ... + m}_{\text{k times}}$$

This map satisfies the following properties:

(1) $j(k \cdot m) = (jk)m$ (Follows from the properties of group addition)
(2) $(j + k)m = (jm + km)$ (Follows from associativity)
(3) $m(j + k) = mj + km$ (Follows from M being an abelian group)

□

EXAMPLE. Fix an F-vector space V. Consider S, an abelian group under composition:

$$S = \{T | T : V \to V \text{ is a linear isomorphism}\} \quad T(a+b) = T(a)+T(b) \text{ and } T(c\dot{a}) = c \cdot T(a)$$

Now consider the ring F[x]. We can define an F[x]-module structure on S in the following way:

$$F[x] \times S \to S$$

e.x.: $(x^2 + 3x + 2, T) \mapsto T \circ T + 3T + 2 \cdot Id$ (remember that the sum of linear transforms is still a linear transform). In other words, we're defining a map as follows:

$$(p(x), T) \mapsto p(T)$$

It needs to be checked that the conditions for a valid module structured are upheld here, it's unclear whether or not they are.

DEFINITION 24. *Let R be a ring with 1_R. An R-Algebra is a ring A with 1_A, together with a ring homomorphism*

$$f : R \to A$$

Such that:

(1) $f(1_R) = 1_A$
(2) $f(R) \subseteq$ *the center of* A

An alternative definition is as follows: An R-Algebra is a ring A with 1_A that is also an R-module, and for $a, b \in A, r \in R$ the following is true:

$$r \star (a \cdot b) = (r \star a) \cdot b$$

Where $\cdot$ denotes the action in the module A and $\star$ denotes the action in the ring R. The idea behind an algebra is that it supports a type of compatibility between the Algebra's operation and the Module's operation.

EXAMPLE. Let $R = \mathbb{R}$, and let $A = nxn$ matrices with coefficients in $\mathbb{R}$. A is a ring under addition and multiplication, and it has an identity, which we will denote 1_A. A is an R-module,

$$\mathbb{R} \times A \to A \quad (r, [a_{ij}]) \to [r \cdot a_{ij}]$$

Notice that:

$$r([a_{ij}] \cdot [b_{ij}]) = ([r \cdot a_{ij}]) \cdot [b_{ij}]$$

so, A is also an R-Algebra.

EXAMPLE. Let $R = \mathbb{R}$, and let A= functions from $\mathbb{R} \to \mathbb{R}$ under multiplication. The identity for A will be the constant function, f(x)=1. Thus we have a map:

$$\mathbb{R} \times A \to A \quad (r, f) \mapsto rf$$

This defines a module. Moreover, A is an $\mathbb{R}$-algebra because it satisfies the extra conditions in the definition of an Algebra.

Our claim is now that our first definition implies our second definition.

PROOF. Given:

$$f : R \to A$$

A ring homomorphism, we want to define an R-module on A such that:

$$R \times A \to A$$

$$(r, a) \mapsto \underbrace{f(r) \cdot a}_{\text{the '$\cdot$' represents multiplication in A}} =: \underbrace{r \star a}_{\text{where $\star$ is in the module structure}}$$

Why does this homomorphism happen to define an R-module? Consider the following for $r, s \in R$ and $a \in A$:

$$\begin{aligned} r \star (s \star a) &= f(r) \cdot (f(s) \cdot a)) \\ &= (f(r) \cdot f(s))a \\ &= f(rs) \cdot a = (rs) \star a \end{aligned}$$

Where we use the fact that (f) is a ring homomorphism in line 2. From this we can conclude the following:

(1) $1_R \cdot a = f(1_R) \cdot a = 1_A \cdot a = a$
(2) $f(r) \cdot a = a \cdot f(r) \quad \forall r \in R, a \in A$
(3) $r \star (a \cdot b) = f(r) \cdot (a \cdot b) = (f(r) \cdot a) \cdot b = (r \star a) \cdot b$

Using these properties, we can show that the definitions are compatible. Suppose that we are given a ring R with 1_R, an R-module A with 1_A, and let $r(ab) = (ra)b$. We then define the following map:

$$f : R \to A \quad \text{so that} f(1_R) = 1_A$$

$$f(r) = f(r \cdot 1_R) = f(r) \cdot f(1_R) = f(r) \cdot 1_A$$

Now using the map that we've defined, we can do the following:

$$R \times A \to A \quad (r, a) \mapsto r \star a$$

Where the operation $\star$ denotes how an element of R acts on an element of the R-module A. If we also define:

$$f(r) = r \star 1_A$$

We can show that f is a ring homomorphism in the following way:

$$\begin{aligned} f(r \cdot s) &= (r \cdot s) \star 1_A \overset{Def.2}{=} r \star (s \star 1_A) \\ &= r \star f(s) \\ &= r \star (1_A \cdot f(s)) \\ &= r \star 1_A \cdot f(s) \\ &= f(r) \cdot f(s) \end{aligned}$$

And since $f(r) = r \star 1_A$, we know that:

$$f(1_R) = 1_R \star 1_A = 1_A \quad \text{since } 1_R \cdot a = a \quad \forall a \in A$$

The last question we need to ask is if $f(r) \in$ the Center of A. In other words, is the following true:

$$f(r) = (r \star 1_A) \in C_A \Rightarrow (r \star 1_A) \cdot a \overset{?}{=} a \cdot (r \star 1_A)$$

This can be shown to be true. □

Definition 25. *Let M and N be R-modules. An $R-$ module homomorphism is a group homomorphism:*

$$f : M \to N \text{ such that } f(r \cdot m) = r \cdot f(m) \quad \forall r \in R, m \in M$$

Example. $\mathbb{Z}$-modules are abelian groups, and $\mathbb{Z}$-module homomorphisms are exactly group homomorphisms as we're used to them:

$$K \in \mathbb{Z}, \quad f(K \cdot g) = \underbrace{f(g + ... + g)}_{\text{K times}} = \underbrace{f(g) + ... + f(g)}_{\text{K times}} = Kf(g)$$

EXAMPLE. Let F be a field, and let $R = F[x]$. Given V, an F-vector space, if:

$$T : V \to V$$

is a linear transform and $p(x) \in F[x]$ where

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + ...a_1 x + a_0$$

Let

$$p(T) = a_n T^n + a_{n-1}T^{n-1} + ... + a_1 T + a_0 \cdot Id$$

Where a linear transform to a power n is equal to the following:

$$T^n = \underbrace{T \circ T \circ T.... \circ T}_{n}$$

Notice that if $p(x), q(x) \in F[x]$ the following is true:

$$(p \cdot q)(T) = p(T) \cdot q(T)$$

which makes the set of linear transforms into an $F[x]$-module. If you fix a given T once and for all, you see that p(T) is a linear transform,

$$p(T) : V \to V$$

which gives us a function

$$F[x] \times V \to V \quad (p(x), v) \mapsto [p(T)](v) =: p \cdot v$$

Which makes V into an $F[x]$-module. To prove this, we have to check the following:

(1) $(p \cdot q) \cdot v = (p \cdot q)(T)v = (p(T) \cdot q(T)) \cdot v = p(T) \cdot (q(T)v) = p \cdot (q \cdot v)$
(2) $(p + q) \cdot v = (p(T) + q(T)) \cdot v = p(T)v + q(T)v = p \cdot v + q \cdot v$

for $p, q \in F[x]$ and $v \in V$. It can similarly be shown that

$$p \cdot (v_1 + v_2) = p \cdot v_1 + p \cdot v_2$$

So the distributive law holds up under our scrutiny, and V is indeed a $F[x]$-module.

EXAMPLE. Let T=0, then $p(T) = a_0 \cdot Id$. Then,

$$F[x] \times V \to V \quad (p, v) \mapsto p(T)(v) = a_0 Idv = a_o \cdot v$$

EXAMPLE. Let T=Id. Then, $p(T)(v) = (a_n + a_{n-1} + ... + a_1 + a_0)v$. We can then derive the following fact:

$$\{\text{V, an F[x] Module}\} \stackrel{1-1}{\longleftrightarrow} \{\text{ V, an F-vector space and } T : V \to V\text{, a linear transform}\}$$

DEFINITION 26. *Let A and B be left R-modules. We define a new set $Hom_R(A, B)$ in the following way:*

$$\begin{aligned} Hom_R(A, B) &= \{f | f : A \to B \textit{ where f is a group homomorphism } f(r \cdot a) = r \cdot f(a)\} \\ &= \{f | \textit{ f is an R-module homomorphism from A to B}\} \end{aligned}$$

It is natural to wonder about the structure of this set $Hom_R(A, B)$. For starters, we can show that:

$$Hom_R(A, B) \text{ is an abelian group}$$

This property comes from the following:

$$(f[+_{\in Hom_R(A,B)}]g)(a) = f(a)[+_{\in B}]g(a)$$

And since we know that the addition of homomorphisms is abelian, putting that together with the fact that B must be an abelian group under addition, we see that $Hom_R(A, B)$ is abelian. Through this we can see that the inverse of a function $f \in Hom_R(A, B)$ is simple $-f$. Since it can also be shown that:

$$f + g \in Hom_R(A, B) \quad \text{and } - f \in Hom_A(A, B)$$

Looking at $Hom_R(A, B)$, we see that it's actually an abelian group. Another natural question is "is $Hom_R(A, B)$ a natural R-module?" We have the following candidate for a map:

$$R \times Hom_R(A, B) \to Hom_R(A, B) \quad (r, f) \mapsto r \cdot f$$

Where

$$(r \cdot f)(a) = r \cdot f(a)$$

To show that $Hom_R(A, B)$ qualifies as a valid R-module, we have to show the following:

$$r \cdot (s \cdot f) \stackrel{?}{=} (r \cdot s) \cdot f$$

Which can be shown through the following:

$$\begin{aligned}(r \cdot (s \cdot f))(a) = & \\ & = r \cdot)(s \cdot f)(a)) \\ & = r \cdot (s \cdot f(a)) \\ & = (r \cdot s) \cdot f(a) \\ & = ((r \cdot s) \cdot f)(a)\end{aligned}$$

And since the other qualifications are the distributive laws, where:

$$(r + s) \cdot f = r \cdot f + s \cdot f$$

And

$$r \cdot (f + g) = r \cdot f + r \cdot g$$

We omit their proofs but acknowledge that they hold. Now we check that:

$$r \cdot f \in Hom_R(A, B)\text{ff} \in Hom_R(A, B)$$

The group homomorphism properties hold, and we have to prove the following:

$$(r \cdot f)(s \cdot a) \stackrel{?}{=} s \cdot (r \cdot f)(a) \text{ for} r, s \in R, a \in A,$$

We know the following through the properties of a homomorphism on this structure:

$$(r \cdot f)(s \cdot a) = f \cdot f(s \cdot a) = r \cdot (s \cdot f(a)) \text{ since f is a R-module homomorphism}$$

$$= r \cdot (s \cdot f(a))$$

Which we would like to equal:

$$= s \cdot (r \cdot f(a))$$

Which we can see would happen when the ring R is commutative. So, we see that $Hom_R(A, B)$ is a natural R-module when R is a commutative ring. Otherwise, we can't assume that this works. In summary,

If R is commutative, then $Hom_R(A, B)$ is a left R-module

EXAMPLE. If F is a field, then $Hom_R(V, W)$ is an F-vector space for any F-vector spaces V and W. This follows naturally from F being a commutative ring.

Observe the following:

$$Hom_R(A, B) \times Hom_R(A, B) \to Hom_R(A, C) \quad (f, g) \mapsto g \circ f$$

And notice that

$$g \circ f(r \cdot a) = g(r \cdot f(a)) = r \cdot g(f(a)) = r \cdot (g \circ f)(a)$$

Take the special case:

$$Hom_R(A, A) \times Hom_R(A, A) \to Hom_R(A, A) \quad (f, g) \mapsto g \circ f$$

Which is a associative, non-commutative operation. The R-module homomorphism $f : A \to A$ given by $f(a) = a$, i.e. the identity homomorphism, will be the identity for composition under this operation. From this structure, we have the following result:

$Hom_R(A, A)$ is a ring under addition, and composition, or $(R, +, \circ)$

This is defined as the Endomorphism ring of A.

We know the following:

$Hom_R(A, B)$ is an R-module if R is commutative.

$Hom_R(A, B)$ is a ring under addition and function composition.

Notice that both of these are true for $Hom_R(A, A)$ as a special case of $Hom_R(A, B)$. Together, these two statements define an R-algebra:

$$r \cdot (f \circ g) = (r \cdot f) \circ g = f \circ (r \cdot g)$$

EXAMPLE. Take the case where F is a field, and let A=V, a F-vector space. Thus, $Hom_F(V, V)$ is an F-algebra. If V=$\mathbb{R}^n$, $Hom_F(V, V) = M_{n \times n}$ We have the following operations that allow $Hom_F(V, V)$ to be an F-algebra:

(1) Normal addition, +
(2) Multiplication of matrices
(3) Scalar multiplication of matrices

If A is an R-module and B is a submodule, we have the following:

$$R \times A/B \to A/B \quad (r, a+B) \mapsto r \cdot a + B$$

Which is a well defined map, and defines an R-module. A/B is then called 'the quotient module'.

Example. Consider the $M_{n\times n}$ modules $\mathbb{R}^n$. We then know the following about $A, B \in M$ and $v, w \in \mathbb{R}^n$:

(1) $A(Bv) = (AB)v$
(2) $A(v+w) = Av + AW$
(3) $(A+B)v = Av + Bv$

Allow a map $A : \mathbb{R}^n \to \mathbb{R}^n$ to be $\mathbb{R} - linear$. This means that:

$$A(v+w) = Av + Aw \text{ and } A(c \cdot v) = c \cdot (Av)$$

When is A considered and $M_{n\times n}$ module homomorphism? It turns out that this holds if and only if:

$$\forall x \in M_{n\times n} \quad A(Xav) = \underbrace{x}_{\text{in Ring}} (\underbrace{A}_{\text{a linear Map}} \underbrace{v}_{vector})$$

So, $Ax = xA \quad \forall x \in M_{n\times n}$ when x is in the center of $M_{n\times n}$.

As already mentioned, if $N \subseteq M$ and $N \lhd M$, then we know that M/N is a quotient module, which implies that we have a map:

$$R \times M/N \to M/N \quad (r, a+N) \mapsto ra + N$$

If $f : M \to N$ is an R-module homomorphism, where M and N are any R-modules, we define the following sets, similar to ring theory:

$$Ker(f) = \{m \in M | f(m) = 0\} \quad \text{(is a submodule of M)}$$

$$Im(f) = \{f(m) | m \in M\} \quad \text{(which is a submodule of N)}$$

As in the case of rings and groups, we see that the $Ker(f) \lhd M$, or it is an "ideal". We then have the following definition for the 1^{st} isomorphism theorem:

Definition 27. *The 1^{st} isomorphism Theorem: If*

$$f : M \to N \quad \textit{is an R-module isomorphism, then}$$

$$M/Ker(f) \xrightarrow{\varphi} Im(f) \quad m + M \mapsto f(m)$$

Is an isomorphism of R-modules.

Example. Given R, a ring, and $R^n = \{(r_1, r_2, ..., r_n) | r_i \in R\}$ is an R-module. We have the following map:

$$\pi_i : R^n \longrightarrow R \quad \pi_i(r_1, r_2, ..., r_n) \mapsto r_i$$

Where π_i is clearly a surjective R-module homomorphism. We see that:

$$Ker(\pi_i) = \{(r_1, r_2, .., 0 \cdot r_i, ...r_n) | r_i \in R\}$$

So using the 1^{st} isomorphism theorem, we see that:

$$R^n/Ker(\pi_i) \cong Im(\pi_i) = R$$

e.g., let the ring R=$\mathbb{R}$. Then we have a map:

$$i : \mathbb{R}^2 \longrightarrow \mathbb{R}^3 \quad (x, y) \mapsto (x, y, 0)$$

Then considering the map π_i on this structure, we have the following:

$$\pi_3 : \mathbb{R}^3 \longrightarrow \mathbb{R}$$

so from this, we can conclude that:

$$R^3/Ker(\pi_i) = R^3/Im(i) \cong R$$

Where this is an R-module isomorphism.

REMARK. If A is an R-algebra, then we have the following:

$$a \times b = a \cdot b - b \cdot a \quad \text{which is called a lie algebra.}$$

Interestingly, this will always satisfy the Jacobi identity,

$$(a \times b) \times c + (c \times a) \times b + (b \times c) \times a = 0$$

CHAPTER 7

Operations on R-Modules

Let $N_1, N_2, ...N_k$ be R-modules. Then, we have the following:

$$N_1 + N_2 + ... + N_k = \{r_1 a_1 + r_2 a_2 + ...r_k a_k | r_i \in R, a_i \in N$$

which can be thought of as "all linear combinations" of the elements from the R-modules. If A is any subset of M, we have the following:

$$RA = \{r_1 a_1 + ... + r_n a_n | n \in \mathbb{N}, r_i \in R, a_i \in A\}$$

Which we call the "submodule of M generated by A", a subset of the R-module M. If N is a submodule of M, we say that N is 'finitely generated' if N=RA, where A is a finite subset of M.

If $A = \{a\}$, we'll write Ra for RA. We say that N is 'cyclic' if N=Ra for some $a \in A$.

Example. Let the ring $R = \mathbb{Z}$. We know that $\mathbb{Z}$-modules are abelian groups. If M=G is an abelian group, we say that:

$$\begin{aligned} N &= \mathbb{Z} \cdot a \quad \text{for some a} \\ &= \{0, \pm a, \pm 2a, \pm 3a...\} \\ &= \text{ a cyclic subgroup generate by } a \in M \end{aligned}$$

Which implies that N is finitely generated for an R-module. We see that the term "finitely generated for an R-module" is equal to the term "finitely generated for a group".

Example. Let R be a ring, and let the R-module M be the R-module R. We now ask, what are the cyclic submodules of R? Recall that an R-submodule of R is exactly a left ideal I of R. Thus, I is cyclic if and only if $I = R \cdot a$ for some $a \in A$, or in other words, if I is a principal idea.

Example. Surprisingly, it turns out that a submodule of a finitely generated module need not be finitely generated. Suppose that a ring R has some element 1. Thus, R is a cyclic R-module, since $R = R \cdot 1$. Now let R be the ring:

$$\mathbb{Q}[x_1, x_2, x_3, ...]$$

This ring is a cyclic R-module since it's generated by the element 1. Now consider the following:

$$R \cdot x_1 \text{ is a submodule of R}$$
$$R \cdot x_2 \text{ is a submodule of R}$$
$$R \cdot x_3 \text{ is a submodule of R}$$
$$\vdots$$

Now consider the 'linear combinations' of the submodules of R, which looks like the following:

$$Rx_1 + Rx_2 + Rx_3 + ... = \text{ polynomials without a constant term}$$

This is a $R = \mathbb{Q}[x_1, x_2, ...]$-module! But, the claim is that this module is not finitely generated. This is because we claim there exists an infinite number of variables, whereas if you tried to use a finite number of generators, you would miss out on variables. And naturally, you can't use any constant terms, since this combination has no constant terms.

Definition 28. *Let M and N be left R-modules. We define the direct sum in the following way:*

$$M \oplus N = \{(m,n) | m \in M, n \in N\}$$

To be an abelian group under the following operation:

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$$

$M \oplus N$ is a left R-module by the following formula:

$$r \cdot (m,n) = (r \cdot m, r \cdot n)$$
$$r \cdot (s \cdot (m,n)) = (rs) \cdot (m,n)$$

Which allows for the two distributive laws.

Example. Consider $\mathbb{R}^n$ as an R-module, where $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$, and $\mathbb{R}^n = \underbrace{\mathbb{R} \oplus \mathbb{R} ... \oplus \mathbb{R}}_{n}$ There turns out to be a fairly obvious isomorphism of R-modules as follows:

$$(M \oplus N) \oplus P \longrightarrow M \oplus (N \oplus P) \quad ((m,n),p) \longmapsto (m,(n,p))$$

Also notice that $M \oplus N \cong N \oplus M$ under the simple isomorphism:

$$(m,n) \mapsto (n,m)$$

Also notice that $\{0\}$ is an R-module, and that:

$$M \oplus \{0\} \cong \{0\} \oplus M \cong M, \quad (m,0) \longleftrightarrow (0,m) \longleftrightarrow m$$

Remark. Notice that there aren't always inverses!

$$M \oplus ? \cong 0$$

It turns out nothing can really fit in to the '?' spot- this isomorphism holds only when $M \cong \{0\}$, which isn't really the most interesting example.

DEFINITION 29. *Given* $\{M_1, M_2, ...\}$ *, countably many*[1] *Manifolds, let:*

$$M_1 \oplus M_2 \oplus ... := \bigoplus_{k=1}^{\infty} M_k = \bigoplus_{k\geq 1} M_k$$

$$:= \{(m_1, m_2, ...)|m_i \in M \forall \text{ but finitely many } m_i \text{ are zero } \}$$

Where we impose the following restrictions on operations:

(1) *Addition will be defined entry-wise*
(2) *A left R-module multiplication on* $\bigoplus_{k\geq 1} M_k$ *is defined entry wise*

An example of this could be $\bigoplus_{k\geq 1} \mathbb{R}$.

DEFINITION 30. *Letting M and N be left R-modules, we define the direct product in the following way:*

$$M_1 \underset{\text{direct product}}{\times} M_2 \times ... =: \prod_{k\geq 1}^{\infty} M_k = \prod_{k\geq 1} M_k$$

$$=: \{(m_1, m_2, ...|m_i \in M_i\}$$

Where addition and left R-module structure operations are defined as they were for $\oplus$*; entry-wise.*

EXAMPLE. Consider:

$$(1, 0, 1, 0, 1, 0, ...) \in \prod_{k\geq 1} \mathbb{R}$$

But, notice that:

$$(1, 0, 1, 0, 1, 0, ...) \notin \bigoplus_{k\geq 1} \mathbb{R}$$

Because infinitely many $m_i = 0$.

REMARK. But, the following is true:

$$\bigoplus_{k\geq 1} M_k \subseteq \prod_{k\geq 1} M_k$$

EXAMPLE. As we know, $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. Considering the elements of $\bigoplus_{k\geq 1} M_k$ and $\prod_{k\geq 1} M_k$, suppose we try to write out all the elements of $\prod_{k\geq 1} \mathbb{Z}_2$:

$$\mathbf{a_1}, a_2.a_3.a_4, ...$$
$$b_1, \mathbf{b_2}, b_3, b_4, ...$$
$$c_1, c_2, \mathbf{c_3}, c_4, ...$$
$$d_1, d_2, d_3, \mathbf{d_4}, ...$$

[1] In mathematics, a countable set is a set with the same cardinality (number of elements) as some subset of the set of natural numbers. A set that is not countable is called uncountable

Now consider the following new element, $x \in \prod_{k\geq 1}\mathbb{Z}$:

$$x = (a_1 + 1), (b_2 + 1), (c_3 + 1), (d_4 + 1), ...$$

However, since we've assumed that $x \in \prod_{k\geq 1}\mathbb{Z}_2$, we claim that x wasn't in our original list! Thus, we see that $\prod_{k\geq 1}\mathbb{Z}_2$ isn't countable. Clearly, $x \notin \prod_{k\geq 1}\mathbb{Z}_2$, since it (x) may have infinitely many zeros.

Example. If R is a ring, the n-fold direct sums of R with itself: $R^n = \underbrace{R \oplus R \oplus ... \oplus R}_{n}$ are called free R-modules of rank n. The intuitive notion is that M is free of rank n if there exist n elements $e_1, e_2, ...e_n$ in M such that for any $x \in M$ there exist unique $r_1, r_2, ...r_n \in R$ such that $r_1e_1 + r_2e_2 + ...r_ne_n = x$. The idea is similar to having a basis on a vector space.

Notice that R^n is free of rank n, since we can let $e_i = (0_1, 0_2, ...1_i, ...)$ for all i. Then,

$$x = (x_1, x_2, x_3, ...x_n) = (x_1 \cdot 1, x_2 \cdot 1, x_3 \cdot 1, ...x_n \cdot 1)$$

Theorem 15. *Let the ring R be a field, called F. Then we have the following theorem, which we won't prove:*

$$\textit{n-dimensional F-vector spaces} \overset{1-1}{\longleftrightarrow} \textit{free F-modules of rank n}$$

Example. Notice that $\underset{k\geq 1}{\oplus} R$ or $\prod_{k\geq 1} R$ are not free of rank n for any $n \geq 1$.

Example. Given $\mathbb{Z}_6$ as a $\mathbb{Z}$-module, we see that it is not free of rank n. This is due to the fact that an element of $\mathbb{Z}_6$ can be represented through a non-unique way through multiplication or addition of other elements. I,e, for any $e_1 \in \mathbb{Z}_6$, the following is true:

$$x = r_1 \cdot e_1 = r_2 \cdot e_1 \quad \text{where } r_1 \neq r_2$$

No matter how we chose $e_1 \in \mathbb{Z}_6$:

$$r_1 \cdot d_1 = (r_1 + 6)e_1, \quad r_1 \neq r_1 + 6 \in \mathbb{Z} \text{ since it's a } \mathbb{Z}\text{-modules}$$

So, $\mathbb{Z}_n$ is not a free $\mathbb{Z}$ module. As seen in the homework, if we took an abelian group G that has torsion (which means that there exist elements of finite order, i.e. $n \cdot y = 0$) then G is not free. This argument holds even if n is prime.

Fact. M is free of rank n if and only if:

$$M \cong R^n$$

$$M \longrightarrow N, \quad x = r_1e_1 + r_2e_2 + ... + r_ne_n \mapsto (r_1, ...r_n)$$

Example. Consider $\mathbb{Q}$. Since $\mathbb{Q}$ is abelian and therefore a $\mathbb{Z}$-module, we know that $\mathbb{Q}$ is not free of any rank. What this implies is that for any finite collection of primes, the following cannot be done uniquely:

$$\frac{a}{b} = c_1\frac{1}{p_1} + c_2\frac{1}{p_2} + ... + c_k\frac{1}{p_k}$$

Which is true because the denominator 'b' may just be the next prime, p_{k+1}. And, if you take an infinite list of primes, you lose the property of uniqueness, showing that $\mathbb{Q}$ is not free.

The motivation for $\otimes$ is the following:

$$(-,-) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$$

DEFINITION 31. *Given x,y, their direct product is taken as follows:*

$$(x, y) = x_1 y_1 + x_2 y_2 + ... + x_n y_n$$

This definition admits the following properties:

1. $(\alpha x y) = (x, \alpha y) \forall \alpha \in \mathbb{R} = \alpha(x, y)$
2. $(x + z, y) = (x, y) + (z, y)$
3. $(x, y + z) = (x, y) + (x, z)$

Also, notice that $(x + z, y + w) \neq (x, y) + (z, w)$.

Consider the following idea: If M and N are R-modules (where R is a commutative ring with 1) the elements of $M \otimes_R N$ are sums:

$$m_1 \otimes r_1 + ... + m_k \otimes r_k$$

With the following properties:

1. $(r \cdot m_1) \otimes n_1 = m_1 \otimes (r \cdot n_1) =: r \cdot (m \otimes n)$
2. $m_1 \otimes n_1 + m_2 \otimes n_1 = (m_1 + m_2) \otimes n_1$
3. $m_1 \otimes n_1 + m_1 \otimes n_2 = m_1 \otimes (n_1 + n_2)$

EXAMPLE. The inner product on vector space is exactly an R-module homomorphism:

$$\mathbb{R} \otimes_{\mathbb{R}} \mathbb{R} \longrightarrow \mathbb{R}$$

Let M be a left R module, where

$$(r, m) \mapsto r \cdot m \in M$$

The question is, given some new operation $\star$, with the following definition:

$$m \star r \overset{definition}{=} r \cdot m$$

does this operation make M into a right R module? Well, we know the following to be true:

1. $(m_1 + m_2) \cdot r = r \cdot (m_1 + m_2) = m_1 \star r + m_2 \star r$
2. $m \star (r_1 + r - 2) = m \star_1 + m \star r_2$

But is the following true?

$$(m \star r_1) \star r_2 \overset{?}{=} m \star (r_1 \star r_2)$$

It turns out that generally, this property holds. Unless, R is communative- in which case, ever left R module is naturally a right R module by defining this new operation as such.

DEFINITION 32. *A (R,S)-bimodule is an abwelian group M such that:*

(1) *M is a left R-module*
(2) *M is a right S-module*
(3) $(r \cdot m) \cdot s = r \cdot (m \cdot s)$

Example. If R is communative, every left R-module is naturally a (R,R)-bimodule. Take for example:

$$M_{n\times n}(\mathbb{C})$$

Which is a left $\mathbb{C}$-module, and is a right $M_{n\times n}\mathbb{R}$-module. I.e., we ask the following question:

$$((a+bi)\cdot A)\cdot B \stackrel{?}{=} (a+bi)(A\cdot B)$$

Where A is a matrix with complex entries, and B is a matrix with real entries. It turns out that this equality holds, which implies that

$$M_{n\times n} \text{ is a } (\mathbb{C}, M_{n\times n}(\mathbb{R}))\text{-bimodule}$$

Example. If A is an R-algebra, we know the following about elements $r \in R, a_1, a_2 \in A$:

$$r\cdot(a_1\cdot a_2) = (r\cdot a_1)\cdot a_2$$

Which impleis to us that A is in fact a (A, A)-bimodule, where we have the following:

$$A\times A \quad (a_1, a_2)\mapsto a_1\cdot a_2$$

It is clear that thsis map satisfies all necessary properties to qualify as a bimodule. Also notice that A itself is an (R,A)-bimodule, since

$$r_1(a_1\cdot a_2) = (r\cdot a_1)\cdot a_2$$

Suppose we have the following two bimodules: M, an (R,S)-bimodule, and N a (S,T) -bimodule. We then claim that there exists a new (R,T)-bimodule, called:

$$M\otimes_S N$$

Which is defined by the following free abelian group:

$$(M\times N)/\{\text{subgroup generated by all:}$$

$$(m_1+m_2,n)-(m_1,n)-(m_2,n),(m,n_1+n_2)-(m,n_1)-(m,n_2),(ms,n)-(m,sn)\}$$

The reason for quotienting out by those subgroups is because we want this new operation $\otimes$ to satisfy a few nice properties, namely:

(1) $ms\otimes n - m\otimes s\cdot n = 0$
(2) $(m_1+m_2)\otimes n - m_1\otimes n - m_2\otimes n = 0$
(3) $m\otimes(n_1+n_2) - m\otimes n_1 - m\otimes n_2$

We will write the representatives for the equivelance classes as:

$$\sum m_i\otimes n_i$$

R acts on $M\otimes_S N$ on the left by the following:

$$(r, \sum m_i\otimes n_i)\mapsto (\sum r\cdot m_i\otimes n_i)$$

Similarly, T acts on $M \otimes_S N$ on the right by:

$$(\sum m_i \otimes n_i, t) \mapsto (\sum m_i \otimes n_i \cdot t)$$

REMARK. If $0 \in M$, and $n \in N$, then:

$$0 \otimes n \in M \otimes N$$

Is equivelant to 0. This follows from:

$$\begin{aligned} 0 \otimes n &= \\ &= (0+0) \otimes N = \\ &= 0 \otimes N + 0 \otimes N \\ &\Rightarrow 0 = 0 \otimes N \end{aligned}$$

EXAMPLE. Consider $\mathbb{Z}_2$ as a $(\mathbb{Z}, \mathbb{Z})$ bimodule. We then notice that:

$$\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 = \{\underbrace{0 \otimes 0, \ \ 0 \otimes 1, \ \ 1 \otimes 0,}_{\text{equal to } 0} \quad \underbrace{1 \otimes 1}_{\text{not equal to } 0} \quad \}$$

From this, we conclude that the cross product of $\mathbb{Z}$)2 with itself is a simple group of order 2, and is thus isomorphis to $\mathbb{Z}_2$ as a $(\mathbb{Z}, \mathbb{Z})$-bimodule.

It is also worth noticing that one can manipulate the properties of the tensor product to obtain similar conclusions with the tensors of other modules.

EXAMPLE.

$$\mathbb{Z}_2 \otimes \mathbb{Z}_3$$

Given $a \otimes b \in \mathbb{Z}_2 \otimes \mathbb{Z}_3$ we see that we have the following problem:

$$\begin{aligned} a \otimes b &= 3a \otimes b \\ &= a \otimes 3b \\ &= a \otimes 0 \\ &= 0 \end{aligned}$$

Thus, we can conclude that $\mathbb{Z}_2 \otimes \mathbb{Z}_3$=$\{0\}$

EXAMPLE. $\mathbb{Q}$ is a $(\mathbb{Z}, \mathbb{Z})$-bimudle, and let A be a finite abelian group.Thus, every $a \in A$ has finite order, and given:

$$\mathbb{Z} \otimes_{\mathbb{Z}} A$$

We notice that we can do the following with elements in this tensor product, given:

$$\frac{p}{a} \otimes a = \frac{pn}{qn} \otimes a = \frac{p}{qn} \cdot n \otimes a = \frac{p}{qn} \otimes na = \frac{p}{qn} \otimes 0 = 0$$

Where n in this case is the element that pushes the element a of finite order to 0.

EXAMPLE. Let V be a $\mathbb{R}$-vector space. Thus,

$$\underbrace{V}_{\text{a }(\mathbb{R},\mathbb{R})\text{-bimodule}} \otimes_{\mathbb{R}} \underbrace{\mathbb{C}}_{\text{a }(\mathbb{R},\mathbb{R})\text{-bimodule}}$$

This is called "the complexification of a real vector space", and has some applications to complex analysis. This leads to the following claim:

CLAIM.

$$V \otimes_{\mathbb{R}} \mathbb{C} \overset{\text{as real vector spaces}}{\cong} V \oplus i \cdot V$$

With the following map:

$$\sum v_j \otimes (a_j + ib_j) \mapsto \sum (a_j v_j, i(b_j b_j))$$

This is actually an $(\mathbb{R}, \mathbb{C})$-module, that has the following properties:

(1) $(M \otimes_s N) \otimes_T P \cong M \otimes_S (N \otimes_T P)$
(2) $M \otimes_S (N_1 \oplus N_2) \cong (M \otimes_S N_1) \oplus (M \otimes_S N_2)$
(3) $(N_1 \oplus N_2) \otimes_S M \cong (N_1 \otimes_S M) \oplus (N_2 \otimes_S M)$

Notice that we have the following interesting properties relating to multiplication as we're used to it:

$$Multiplication : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

And that

(1) $(a + b) \cdot c) = a \cdot c + b \cdot c$
(2) $a(b + c) = a \cdot b + a \cdot c$
(3) $(a \cdot b) \cdot c) = a \cdot (b \cdot c)$

These properties imply that multiplication of real numbers is actually given by a function:

$$\mathbb{R} \otimes_{\mathbb{R}} \mathbb{R} \to \mathbb{R}$$

Recall that $\mathbb{R} \otimes_{\mathbb{R}} \mathbb{R} = \{\sum a_i \otimes b_i | i \in \mathbb{N}, a_i, b_i \in \mathbb{R}\}$, which satisfy the following relations:

(1) $a \otimes c + b \otimes c = (a + b) \otimes c$
(2) $a \otimes b + a \otimes c = a \otimes (b + c)$
(3) $ab \otimes c = a \otimes bc$

For example, $3 \otimes 1 + 4 \otimes 1 = (3 + 4) \otimes 1$. Let's now show that multiplication gives a well defined function from $\mathbb{R} \otimes \mathbb{R} \xrightarrow{M} \mathbb{R}$. We have the following candidate:

$$a \otimes b \mapsto a \cdot b \in \mathbb{R}$$

More generally,

$$\sum_{i=1}^{n} a_i \otimes b_i \mapsto \sum_{i=1}^{n} a_i \cdot b_i$$

Is it then true that the map M satisfies the following?

$$M(a \otimes c + b \otimes c) \overset{?}{=} M((a + b) \otimes c)$$

From what we know about normal multiplication, we see that this is true. From this we can even go a little bit further, to say that multiplication in a ring R, where R is an R-bimodule (or an abelian group) is really just a function

$$M : R \otimes_{\mathbb{Z}} R \to R$$

Now consider $\mathbb{R} \otimes_{\mathbb{R}} \mathbb{R}$. Which $\mathbb{R}$-module is that? Our claim is that:

$$\mathbb{R} \otimes_{\mathbb{R}} \mathbb{R} \cong \mathbb{R}$$

And more generally, $M \otimes_R R \cong M$ for any right R-module M, and R with 1. Consider:

$$M \otimes_R R \to M \quad , m \otimes r \mapsto m \cdot r$$

And where

$$m \otimes r_1 + n \otimes r_2 \mapsto r \cdot r_1 + n \cdot r_2$$

And all the other analogous natural properties we would like this map to posess. Is this map onto? We see that the answer is, because

$$m \otimes 1_R \mapsto m \cdot 1 = m$$

And is 1-1, because:

$$m \otimes r \in M \otimes_R R, \Rightarrow m \otimes r = m \otimes (r \cdot 1) = (m \cdot r) \otimes 1$$

So if

$$m \otimes r \mapsto m \cdot r = 0 \text{ this implies that } m \otimes r = m \cdot r \otimes 1 = 0 \Rightarrow m \cdot r = 0$$