1 A Review of Rings

We do a quick, informal review of things that we should know already.

Definition 1.1. A **Ring** R is (put simply) a set with two binary operations.

Definition 1.2. An **ideal** is a subset of a ring which is closed under addition and has the absorption property of multiplication, namely

$$RI \subseteq I$$

Definition 1.3. A **quotient ring by an ideal** I denoted R/I is the ring whose elements are the cosets $x + I$, often denoted by $\overline{x}$. It is a frequent exercise to check that this notation is non-ambiguous.

Proposition 1.4. *There is a 1-1 correspondence between ideals in R/I and ideals in R containing I.*

Proof. *(Exercise) Hint: think about the projection map.* □

A number particular types of ideals will be of use to us over the course of this class, namely:

1. Principle: Generated by a single element
2. Maximal: Nontrivial ideal which isn't in any others
3. Prime Ideal: An ideal P such that $x \notin P$ and $y \notin P$ then $xy \notin P$. Moreover if $xy \in P$, then $x \in P$ or $y \in P$. E.g. take any ideal in $\mathbb{Z}$ generated by a prime number.

Notice that the structure of quotient rings by ideals classifies nicely:

Theorem 1.5 (Quotient Ring Classification)**.**

1. *R/M is a field $\longleftrightarrow$ M is maximal*
2. *R/P is an Integral domain $\longleftrightarrow$ P is prime.*

Proof. Solution given by Saskia:

(1.)

($\Rightarrow$) R/M is a field, so it therefore has no nontrivial ideals. Then also, by the correspondence theorem R has no ideals I with $M \subset I \subset R$.

($\Leftarrow$) Works the same way as forward direction. $\triangle$

(2.)

$\Rightarrow$. We have that $[x], [y] \in R/M$, so then $x_1 \in [x], y_1 \in [y]$, but then $[x_1 y_1] = [xy] = 0$ iff $[x]$ or $[y] = 0$. Then, by definition of an ideal, $x_1 y_1 \in M \Leftrightarrow x_1$ or $y_1 \in M$.

($\Leftarrow$) Since M is a prime ideal, $xy \in M$ means that one of x or y is in M, then $[xy] = [x][y] = 0 \Leftrightarrow [x] = 0$ or $[y] = 0$

$\square$

Proof. Alternative proof of the field condition given by Ishaan.

($\Rightarrow$) Let I be an ideal such that $M \subseteq I$. Then let $a \in I$ be given such that $a \notin M$. Then $a + M \neq 0 + M$, and also $\exists b + M$ such that $(a + M)(b + M) = 1 + M$. Then $ab + M = 1 + M$, which indicates that $ab - 1 \in M \subsetneq I$. Thus $ab \in I, 1 \in I$, so $1 \in I = R$.

($\Leftarrow$) Suppose that M is maximal, then let $a + M \in R/M$ such such that $a + M \neq 0 + M$. Now notice that if we attempt to extend the ideal M via a, we will get the whole ring. So then since $1 \in R$, $\exists r \in R$, $\exists m \in M$ such that $1 = ra + m$, so $1 + M = ra + M$, and $(r + M)(a + M)$.

$\square$

Note. Every maximal ideal is prime.

Proposition 1.6. *Every ring has a maximal ideal.*

Proof. *(Exercise)* $\square$

Corollary 1.7. *Every ideal is contained in some maximal ideal*

Corollary 1.8. *Every non-unit is contained in a maximal ideal*

Definition 1.9. A **local ring** is a ring which has a single maximal ideal

Proposition 1.10. *Suppose $m \subseteq R$ such that every $\alpha \in m^c$ is a unit. Then R is local with maximal ideal m.*

Example 1.11. Let $C^0(\mathbb{R}) = \{\text{continuous functions} j : \mathbb{R} \to \mathbb{R}\}$, and take the ring identified by the collection of germs $[f]_0$ which are centered at 0.

Notice that the collection of functions vanishing at 0 is a maximal ideal.

Proof. Define the evaluation map at zero $\begin{matrix} \mathrm{ev}_0 : C^0(R)_0 \to \mathbb{R} \\ \mathrm{ev}_0(f) \mapsto f(0) \end{matrix}$.. Notice that for any continuous function $f \neq 0$ at 0., the $\frac{1}{f}$ is also continuous at 0, and $f * \frac{1}{f} = 1$. $\square$

1.1 Exercises

1. Prove (1.4)

2. Prove (1.5)

3. Let K be a field show that $(f(x)) = (g(x))$ iff f and g differ by a constant for $f(x), g(x) \in K[x]$,

   Proof. This proof was given by Grace.

   ($\Rightarrow$) Suppose that $(f(x)) = (g(x))$, $f(x), g(x) \in K[x]$, then there exists some $k(x), k'(x) \in K[x]$ such that $f(x) = k(x)g(x)$ and $g(x) = k'(x)f(x)$. Then $\deg(f(x)) = \deg(k) + \deg(g) = \deg k + \deg k' + \deg f$, and so the degree of the ks must be zero.

   ($\Leftarrow$) Suppose that $\exists c, c' \in \mathbb{R}$ such that $f(x) = cg(x)$ and $g(x) = c'f(x)$

   $\square$

4. Prove that if R is an integral domain, then $R[x]$ is too.

5. Define $\mathbb{C}[[x]] = \{\sum_{n=0}^{\infty} a_n x^n \mid a_n \in \mathbb{C}\}$. This is the ring of formal power series. Show that $\mathbb{C}[[x]]$ is a local ring.

   Proof. This proof was given by Me.

   Consider the ideal of non-units $M = \langle x \rangle$, i.e. the ideal of all formal power series with constant term $= 0$.

   It is trivially obvious that this is an ideal.

   Now notice that $\mathbb{C}[[x]]/M \cong \mathbb{C}$ since $\forall a \in \mathbb{C}[[x]]$,

$$a = \sum_{i=0}^{\infty} a_i x^i = \underbrace{\left(\sum_{i=1}^{\infty} a_i x^i \right)}_{\in \langle x \rangle} + a_0,$$

   so in $\mathbb{C}[[x]]/M$, $\overline{a}$ is in bijection with a_0 in $\mathbb{C}$. Then, since $\mathbb{C}$ is a field, M must indeed be maximal. Now suppose that there was some other maximal ideal $M' \neq M$. But if this is the case, then there must be some unit $u \in M'$, which means that $1 = uu^{-1} \in M'$, so $M' = \mathbb{C}[[x]]$. And thus M is indeed a unique maximal ideal[1]. $\square$

---

[1] There is an assumption here that M really is the ideal containing all the non units, but this is easy to show

2 Ideal Quotient and Radicals

Definition 2.1 (Ideal Quotient)**.** The **ideal quotient** is defined as

$$\begin{aligned}(i : j) &= \{x \in R \mid xJ \subseteq I\} \\ &= \{x \in R \mid xj \in I \ \forall j \in J\}\end{aligned}$$

Example 2.2. $(6 : 18) = \mathbb{R}$
$(18 : 6) = (3)$

Definition 2.3. $r(I)$, called the radical of an ideal I is defined as

$$\{x \in R \mid x^n \in I \text{ for some } n \in \mathbb{N}\}$$

Example 2.4. $r(8) = (2)$.

Proposition 2.5. *For $m = p_1^{r_1} \dots p_n^{r_n}$, $r(m) = (p_1 \cdot p_2 \cdot \dots p_n)$*

Proof. *Exercise.* □

2.1 Algebraic Geometry

Let K be an algebraically closed field, and let $R = k[x_1, \dots, x_n]$.

Definition 2.6. The **zero locus** of a polynomial $f \in R$ is defined as

$$Z(j) = \{p \in K^n \mid f(p) = 0\}$$

Example 2.7. $y - x^2 \in \mathbb{R}[x, y]$ will have a zero locus shaped like a parabola in the $x - y$ plane.

Definition 2.8. For $A \subseteq K^n$, define

$$I(A) = \{f \in R \mid f(p) = 0 \forall p \in A\}$$

Example 2.9. Taking $A = \{-2, 2\}$, and we get $(x - 2) \cap (x + 2) = (x^2 - 4)$.

Ideally[2] we would like for there to be a 1-1 correspondence between the zero loci of polynomials and ideals... Is this so?p

Example 2.10. $Z(x^2) = 0 = Z(0)$.

Well dang. There goes that idea. Here's a better one:

Theorem 2.11 (Hilbert's Nullstelensatz (I spelt this wrong))**.** *Let $I \subseteq R$ and suppose that f vanishes on all of $Z(I)$, then $f^r \in I$ for some r.*

[2]pun intended

2.2 Exercises

1. For $\mathbb{Z}$, show:
   (a) $(m) + (n) = (\gcd(m, n))$
   (b) $(m) \cap (n) = (\operatorname{lcm}(m, n))$
   (c) $(m)(n) = (mn)$
2. For $\mathbb{Z}$ $(m : n) = \left(\frac{m}{\gcd(m,n)}\right)$
3. Prove Proposition 2.5
4. Problem 15 in Atiyah.
5. Problem 17 in Atiyah.
6. Problem 19 in Atiyah.

3 Will Talks about Categories of Modules

The idea for this talk was spurned on by an offhand comment by Richard E. Borcherds, who mentioned that rings act on modules in a similar way to how groups act on sets. So we'll do some category theory to justify this

Definition 3.1. A *category* $\mathcal{C}$ is comprised of the following data:

1. A collection of objects, denoted ob$\mathcal{C}$,
2. A collection of morphisms

$$\mathcal{C}(a, b) = \{f : a \to b\} \quad \text{for } a, b \in \mathrm{ob}\mathcal{C}$$

3. A collection of *identity morphisms*

$$j_a : 1 \to \mathcal{C}(a, a)$$

We call a function an identity morphism pursuant to the following diagrams. First, see that for a composition law, we need that for

$$\cdot : \mathcal{C}(b, c) \times \mathcal{C}(a, b) \to \mathcal{C}(a, c)$$

We get that

$$\begin{tikzcd}
(\mathcal{C}(c,d) \times \mathcal{C}(b,c)) \times \mathcal{C}(a,b) \arrow[rr, "\text{ass}"] \arrow[d, "\circ\times\mathrm{id}"] & & \mathcal{C}(c,d) \times (\mathcal{C}(b,c) \times \mathcal{C}(a,b)) \arrow[d, "\mathrm{id}\times\circ"] \\
\mathcal{C}(b,d) \times \mathcal{C}(a,b) \arrow[dr, "\circ"] & & \mathcal{C}(c,d) \times \mathcal{C}(a,c) \arrow[dl, "\circ"] \\
& \mathcal{C}(a,d) &
\end{tikzcd}$$

We also need that the identities are actually identities, in other words:

$$\begin{tikzcd}
\mathcal{C}(b,b) \times \mathcal{C}(a,b) \arrow[r, "\circ"] & \mathcal{C}(a,b) & \mathcal{C}(a,b) \times \mathcal{C}(a,a) \arrow[l, "\circ"'] \\
1 \times \mathcal{C}(a,b) \arrow[u, "j_b\times\mathrm{id}"] \arrow[ur, "\cong"] & & \mathcal{C}(a,b) \times 1 \arrow[u, "\mathrm{id}\times j_a"'] \arrow[ul, "\cong"']
\end{tikzcd}$$

We have many examples of categories, we will not list them all here... but here are a few:

Example 3.2.
1. Groups with group homomorphisms
2. Representations with G-equiv. maps
3. Posets with order-preserving maps
4. Posets
5. Quivers
6. Top. with continuous functions
7. Manifolds with C^∞ maps.
8. and et. cetera.

Another quick definition,

Definition 3.3. A morphism f is an *epimorphism* if $hf = gf \Rightarrow h = g$. A *monomorphism* if $fh = fd \Rightarrow h = g$, and an *isomorphism* if it is a morphism with an inverse.

3.1 The Punchline

The kind of general idea here stated in **very** broad strokes is that group actions can be thought of as maps from a one-element category to Set, and likewise we can think of rings as an enriched one object category over Abelian Groups, and this structures functor to abelian groups is a module.