CLASS 2, FEBRUARY 6TH: PRIME & MAXIMAL IDEALS

Much like the prime numbers play an important role in describing the structure of the integers, prime ideals play an invaluable role in describing the structure of rings. Recall the following definitions:

Definition 2.1. An ideal $\mathfrak{p} \subsetneq R$ is said to be **prime** if for every $r, r' \in R$ such that $r \cdot r' \in \mathfrak{p}$, either $r \in \mathfrak{p}$ or $r' \in \mathfrak{p}$.

An ideal $\mathfrak{m} \subsetneq R$ is said to be **maximal** if there exists no ideal $I \subsetneq R$ containing $\mathfrak{m}$. That is $\mathfrak{m}$ is maximal with respect to inclusion among ideals.

In Reid, he describes prime ideals as complements of **multiplicative sets**. To realize this comparison, see Homework 1 #3.

Next, I state another way to realize primality and maximality of ideals.

Proposition 2.2. *Let R be a commutative ring.*

- $\mathfrak{p}$ *is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.*
- $\mathfrak{m}$ *is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.*

Proof.

- Suppose $\mathfrak{p}$ is not prime. Then there exist $a, b \notin \mathfrak{p}$ such that such that $a \cdot b \in \mathfrak{p}$. But this implies
$$(a + \mathfrak{p}) \cdot (b + \mathfrak{p}) = a \cdot b + \mathfrak{p} = 0 + \mathfrak{p}$$
Implying $R/\mathfrak{p}$ is not an integral domain, since $a + \mathfrak{p} \neq 0 + \mathfrak{p} \neq b + \mathfrak{p}$ in $R/\mathfrak{p}$. The reverse implication is acquired by running through this argument in reverse.

- First note that R is a field if and only if the only ideal of R is the 0 ideal. Indeed, if R is not a field if and only if there exists a non-zero non-unit element $r \in R$, and thus $\langle r \rangle$ is a non-zero ideal.

  Suppose $R/\mathfrak{m}$ is not a field. Therefore, there exists a non-zero ideal $I \subseteq R/\mathfrak{m}$. Considering the natural map
$$\varphi : R \to R/\mathfrak{m}$$
We have that $J = \varphi^{-1}(I) \subsetneq R$ is an ideal, and furthermore $\mathfrak{m} \subsetneq J$. Thus $\mathfrak{m}$ is not maximal.

  If $\mathfrak{m}$ is not maximal, suppose $\mathfrak{m} \subsetneq J \subsetneq R$, where J is an ideal. One can check that $\varphi(J) \subseteq R/\mathfrak{m}$ is a non-zero ideal; this follows directly from the definition of the operations on $R/\mathfrak{m}$. Therefore $R/\mathfrak{m}$ is not a field.

$\square$

Corollary 2.3. *Every maximal ideal is necessarily prime.*

Definition 2.4. Given a ring R, call $\operatorname{Spec}(R)$ the set of all prime ideals of R and $\operatorname{m-Spec}(R)$ the collection of all maximal ideals.

$\operatorname{Spec}(R)$ has more structure than merely a set. At minimum it is a poset ordered by inclusion. It is in fact a topological space! We will return to this later.

Let's get into some examples:

Example 2.5. 1) If K is a field, then $\mathrm{Spec}(K) = \{0\}$ is a 1-point set.

2) It should be noted that this doesn't define fields: $R = K[x]/\langle x^n\rangle$ has the property that $\mathrm{Spec}(R) = \{\langle x\rangle\}$ is a single point. Of course, R is not even a domain!

3) If K is a field, then $\mathbb{A}^1_K = \mathrm{Spec}(K[x])$ is called the affine line (over K). Let's examine this in a few cases:

- If $K = \mathbb{C}$, or more genereally K is an algebraically closed field, then given the result of Homework 1 #4, we have that $I = \langle f\rangle$. But algebraic closedness implies
$$f = (x-\alpha_1)^{n_1}\cdots(x-\alpha_m)^{n_m}$$
As a result, the only possibility for f to be prime is the case where $m = n_1 = 1$, or f is a linear polynomial. Therefore, we can see that
$$\mathbb{A}^1_K = \{\langle x-\alpha\rangle \mid \alpha \in K\} \cup \{0\}$$
Therefore it is in bijection with K with one additional special point 0. This gives rationale to the name the affine *line*.
- If $K = \mathbb{R}$, then the situation is a bit more complicated. Still $\langle x-\alpha\rangle$ are prime for each $\alpha \in \mathbb{R}$, but now we have new irreducible polynomials, such as x^2+1. In fact, every quadratic polynomial $f = x^2+bx+c$ with $b^2-4c < 0$ is irreducible (since it has complex roots). In fact, these are all of the remaining irreducibles:
$$\mathrm{Spec}(\mathbb{R}[x]) = \{\langle x-\alpha\rangle \mid \alpha \in K\} \cup \left\{\langle x^2+bx+c\rangle \mid b^2-4c<0\right\} \cup \{0\}$$
- The situation gets more complicated for other non-algebraically closed fields, such as $\mathbb{Q}$ and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In these cases there are in fact irreducible polynomials in every degree! In the case of $\mathbb{Q}$, this can be seen by considering $f = x^n - p$, where p is a prime (or simply square-free) integer. This is irreducible by Eisenstein's Criterion. However, we can be more explicit. Over $\mathbb{C}$,
$$f = (x-\sqrt[n]{p})\cdot(x-\zeta\cdot\sqrt[n]{p})\cdots(x-\zeta^{n-1}\cdot\sqrt[n]{p})$$
where $\zeta = e^{\frac{2\pi i}{n}}$ is an n^{th} root of unity. Of course, if we multiply any less that all of the terms together, then the constant coefficient will have the form
$$\zeta^{m'}p^{\frac{m}{n}}$$
where $m < n$, and therefore cannot possibly be rational.
The case of $\mathbb{F}_p$ can be realized by a counting argument. There are only p many irreducibles of degree 1. Therefore, since x^2+bx+c can have p^2 many values, the ones for which
$$x^2+bx+c = (x-\alpha)(x-\beta)$$
are $\binom{p+1}{2} = \binom{p}{2}+p$-many. But $p^2 - \binom{p+1}{2} = \frac{p^2-p}{2} > 0$ for every prime p. The argument continues in this way. There is a pattern to be found, c.f. the Necklace Polynomial: `https://en.wikipedia.org/wiki/Necklace_polynomial`.

Next time, we will study $\mathrm{Spec}(K[x,y])$ and $\mathrm{Spec}(\mathbb{Z}[x])$.