Section 27: Prime and Maximal Ideals

Factoids: This section explores the connection that factor rings have to integral domains and to fields. Here are some interesting factoids:

- A factor ring of an integral domain may be a field. Example: $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}$.
- A factor ring of a ring may be an integral domain even though the original ring is not. Example: $(\mathbb{Z} \times \mathbb{Z})/N \simeq \mathbb{Z}$ where $N = \{(0, n) | n \in \mathbb{Z}\}$.
- If R is not even an integral domain, it is still possible for R/N to be a field. Example: $\mathbb{Z}_6/\{0, 3\} \simeq \mathbb{Z}_3$.
- A factor ring may also have a worse structure than the original ring. Example: $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}_6$ is not.

Thm. If R is a ring with unity, and N is an ideal of R containing a unit, then $N = R$.

Corollary: A field contains no proper nontrivial ideals.

Note: This makes the factor rings of a field not very interesting. The factor ring will either be $\{0\}$ or the field itself.

Def: The *maximal ideal* of a ring R is an ideal M different from R such that there is no proper ideal N of R properly containing M.

Thm. Let R be a commutative ring with unity. Then M is a maximal ideal of R if and only if R/M is a field.

Proof Sketch: Suppose that M is a maximal ideal in R and that there is an element in R/M that does not have a multiplicative inverse. We can then construct an ideal of R that contains M, contradicting the original assumption. Therefore, every element in R/M needs to have a multiplicative inverse and is thus a field.

Example: $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. Therefore $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p$ is a field.

Corollary: A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

Def: An ideal $N \neq R$ in a commutative ring R is a *prime ideal* if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$.

Example: $\{0\}$ is a prime ideal in any integral domain.

Note: Prime ideals are based on considering the zero divisors of factor rings. The definition is derived from the fact that

$$(a+N)(b+N)+N \implies a+N=N \text{ or } b+N=N$$

if we want our factor ring to be an integral domain. This is stated in the following theorem.

Thm. Let R be a commutative ring with unity, and let $N \neq R$ be an ideal in R. Then R/N is an integral domain if and only if N is a prime ideal in R.

Corollary: Every maximal ideal in a commutative ring with unity is a prime ideal.

Summary: Maximal and prime ideals are a very important concept to understand going forward. Here is a summary of the major results so far:

1. An ideal M of R is maximal iff R/M is a field.
2. An ideal N of R is prime iff R/N is an integral domain.
3. Every maximal ideal of R is a prime ideal.

Notice that these 3 statements form a hierarchy of ideals. Just like how a field is an integral domain with more requirements, a maximal ideal is a prime ideal with more requirements.

Goal: To show that the rings $\mathbb{Z}$ and $\mathbb{Z}_n$ form foundations upon which all rings with unity rest, and that $\mathbb{Q}$ and $\mathbb{Z}_p$ perform a similar service for all fields.

Thm. If R is a ring with unity 1, then the par $\phi : \mathbb{Z} \to R$ given by $\phi(n) = n \cdot 1$ for $n \in \mathbb{Z}$ is a homomorphism of $\mathbb{Z}$ into R.

Corollary: If R is a ring with unity and characteristic $n > 1$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If R has characteristic 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Snarky Remark: It seems that the major results in this chapter are all in the corollaries. It seems that the author should label his theorems as lemmas and his corollaries as theorems!

Proof Sketch: Make use of the last theorem and "throw" the integers into a ring with characteristic n and then with characteristic 0.

Thm. A field F is either of prime characteristic p and contains a subfield isomorphic to $\mathbb{Z}_p$. If R has characteristic 0, then R contains a subring isomorphic to $\mathbb{Q}$.

Def: The fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are *prime fields*.

Def: If R is a commutative ring with unity and $a \in R$, the ideal $\{ra | r \in R\}$ of all multiples of a is the *principal ideal generated by* a and is denoted by $\langle a \rangle$. An ideal N of R is a *principal ideal* if $N = \langle a \rangle$ for some $a \in R$.

Example: Every every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is generated by n, so every ideal of $\mathbb{Z}$ is a principal ideal.

Thm. If F is a field, every ideal in $F[x]$ is principal.

Thm. An ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is irreducible over F.

Example: $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$. Therefore, $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ is a field.

Thm. Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.

Proof: Let $p(x)$ divide $r(x)s(x)$.
Then $r(x)s(x)$ must be a multiple of $p(x)$ and therefore $r(x)s(x) \in \langle p(x) \rangle$.
$\langle p(x) \rangle$ is a maximal ideal of $F[x]$ since $p(x)$ is irreducible over F.
Therefore, $\langle p(x) \rangle$ is also a prime ideal.
Hence, $r(x)s(x) \in \langle p(x) \rangle$ implies that either $r(x) \in \langle p(x) \rangle$ or $s(x) \in \langle p(x) \rangle$.
This implies that either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$. ■

Selected Exercises:

24. Let R be a finite commutative ring with unity. Show that every prime ideal in R is a maximal ideal.

29. Show that N is a maximal ideal in a ring R if and only if R/N is a *simple ring*, that is, it is nontrivial and has no proper nontrivial ideals. (compare with theorem 15.18)

33. Use the result that every ideal in $F[x]$ is principle to prove the equivalence of the following two theorems:

1. *Fundamental Theorem of Algebra:* Every non constant polynomial in $\mathbb{C}[x]$ has a zero in $\mathbb{C}$.
2. *Nullstellensatz for* $\mathbb{C}[x]$: Let $f_1(x) \dots f_r(x) \in \mathbb{C}[x]$ and suppose that every $\alpha \in \mathbb{C}$ that is a zero of all r of these polynomials is also a zero of a polynomial $g(x) \in \mathbb{C}[x]$. Then some power of $g(x)$ is in the smallest ideal of $\mathbb{C}[x]$ that contains the r polynomials $f_1(x) \dots f_r(x)$.