Section V.27. Prime and Maximal Ideals

Note. In this section, we explore ideals of a ring in more detail. In particular, we explore ideals of a ring of polynomials over a field, $F[x]$, and make significant progress toward our "basic goal." First, we give several examples of rings R and factor rings R/N where R and R/N have different structural problems.

Examples 27.1 and 27.4. Consider the ring $\mathbb{Z}$, which is an integral domain (it has unity and no divisors of 0). Then $p\mathbb{Z}$ is an ideal of $\mathbb{Z}$ (see Example 26.10) and $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\mathbb{Z}_p$ (see the bottom of page 137). We know that for prime p, $\mathbb{Z}_p$ is a field (Corollary 19.12). So a factor ring of an integral domain may be a field. Of course, $n\mathbb{Z}$ is also an ideal of $\mathbb{Z}$ for any $n \in \mathbb{N}$ but $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is not a field (not even an integral domain since it has divisors of 0) when n is not prime.

Example 27.2. Ring $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain since it has divisors of zero: $(0, m)(n, 0) = (0, 0)$ where m and n are nonzero. Let $N = \{(0, n) \mid n \in \mathbb{Z}\}$. Then N is an ideal of $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}/N$ is isomorphic to $\mathbb{Z}$ (map coset $m + N = m + \mathbb{Z}$ to $m \in \mathbb{Z}$). Of course, $\mathbb{Z}$ is an integral domain. So a factor ring of a ring may be an integral domain when the original ring is not an integral domain.

Example 27.3. Ring $\mathbb{Z}_6$ is not an integral domain ("$2 \times 3 = 0$") and $N = \{0, 3\}$ is an ideal of $\mathbb{Z}_6$. Now $\mathbb{Z}_6/N$ has elements $0+N$, $1+N$, $2+N$ and so is isomorphic to $\mathbb{Z}_3$ which is a field. So the factor ring of a non-integral domain can be a field (and hence an integral domain).

Definition. For ring R, R itself is an ideal called the *improper ideal.* Also, $\{0\}$ is an ideal of R called the *trivial ideal.* A *proper nontrivial ideal* of R is an ideal N such that $N \neq R$ and $N \neq \{0\}$.

Theorem 27.5. If R is a ring with unity and N is an ideal of R containing a unit, then $N = R$.

Corollary 27.6. A field contains no proper nontrivial ideals.

Proof. In a field, every nonzero element is a unit. So by Theorem 27.5, the only ideals are $\{0\}$ and the whole field. ∎

Note. The previous two results tell us that we are not interested in factor rings based on an ideal with a unit (and hence, not interested in "factor fields").

Definition 27.7. A *maximal ideal* of ring R is an ideal $M \neq R$ such that there is no proper ideal N of R properly containing M.

Example. For $R = \mathbb{Z}_6$, two maximal ideals are $M_1 = \{0, 2, 4\}$ and $M_2 = \{0, 3\}$. For $R = \mathbb{Z}_{12}$, two maximal ideals are $M_1 = \{0, 2, 4, 6, 8, 10\}$ and $M_2 = \{0, 3, 6, 9\}$. Two other ideals which are not maximal are $\{0, 4, 8\}$ and $\{0, 6\}$.

Theorem 27.9. (Analogue of Theorem 15.18)
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.

Example 27.10. Since $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ (see the bottom of page 137) and $\mathbb{Z}_p$ is a field if and only if p is prime (Theorem 19.11 and Corollary 19.12), so by Theorem 27.9, the maximal ideals of $\mathbb{Z}$ are precisely the ideals $p\mathbb{Z}$ where p is prime.

Corollary 27.11. A commutative ring with unity is a field if an only if it has no proper nontrivial ideals.

Note. Suppose R is a commutative ring with unity and $N \neq R$ is an ideal of R. Then R/N is an integral domain (i.e., has no divisors of zero) if and only if

$$(a + N)(b + N) = N \Rightarrow a + N = N \text{ or } b + N = N \qquad (*)$$

(since N is the additive identity in R/N). Since coset multiplication is defined using representatives and $(a+N)(b+N) = ab+N$, then condition $(*)$ is equivalent to

$$ab \in N \Rightarrow a \in N \text{ or } b \in N.$$

Definition 27.13. 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 all $a, b \in N$.

Note. The previous note combines with the definition of "prime ideal" to give the following.

Theorem 27.15. 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 27.16. Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof. If M is a maximal ideal in R, then R/M is a field by Theorem 27.9 and so is an integral domain. By Theorem 27.15, M is a prime ideal in R. ∎

Example 27.12. For $R = \mathbb{Z}$, we have the ideals $n\mathbb{Z}$ where $n \in \{0\} \cup \mathbb{N}$ are the ideals in R. The only time these ideals are prime ideals are when $n = p$ is prime and $N = p\mathbb{Z}$ (hence the term "prime ideal"). By Example 27.10, these are exactly the maximal ideals in $R = \mathbb{Z}$. This illustrates Corollary 27.16 in that the maximal ideals $p\mathbb{Z}$ are all prime ideals.

Note. The text emphasizes our knowledge of maximal and prime ideals at this stage as:

1. An ideal M of R is maximal if and only if R/M is a field.

2. An ideal N of R is prime if and only if R/N is an integral domain.

3. Every maximal ideal is a prime ideal.

Theorem 27.17. If R is a ring with unity 1 then the map $\phi : \mathbb{Z} \to R$ given by $\phi(n) = n \cdot 1$ where $n \cdot 1 = 1 + 1 + \cdots + 1$ (n times) for $n \in \mathbb{N}$ and $n \cdot 1 = (-1) + (-1) + \cdots + (-1)$ ($|n|$ times) for $-n \in \mathbb{N}$, is a homomorphism of $\mathbb{Z}$ into R.

Note. The following result shows that the rings $\mathbb{Z}$ and $\mathbb{Z}_n$ "form the foundations upon which all rings with unity rest" (page 249).

Corollary 27.18. 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 has a subring isomorphic to $\mathbb{Z}$.

Note. The following result shows that the fields $\mathbb{Q}$ and $\mathbb{Z}_p$ "form the foundations upon which all" fields rest (page 249).

Theorem 27.19. A field F is either of prime characteristic p and contains a subfield isomorphic to $\mathbb{Z}_p$, or it is of characteristic 0 and contains a subfield isomorphic to $\mathbb{Q}$.

Definition 27.20. The fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are *prime fields*.

Definition 27.21. If R is a commutative ring with unity and $a \in R$, the ideal $\{ra \mid r \in R\}$ of all multiples of a is the *principal ideal generated* by a, denoted $\langle a \rangle$. An ideal N of R is a *principal ideal* if $N = \langle a \rangle$ for some $a \in R$.

Example 27.22. Every ideal of the ring $\mathbb{Z}$ is of the form $n\mathbb{Z}$ by Example 26.11 and $n\mathbb{Z}$ is generated by n, so every ideal of $\mathbb{Z}$ is a principal ideal.

Example 27.23. The ideal $\langle x \rangle$ in $F[x]$ is the set of all products of the form $xp(x)$ for $p(x) \in F[x]$. So this principal ideal consists of all polynomials with zero constant term. What is $\langle x^2 \rangle$?

Theorem 27.24. If F is a field then every ideal in $F[x]$ is principal.

Note. The following result is instrumental in proving our "basic goal": Any non-constant polynomial $f(x) \in F[x]$ has a zero in some field E containing F (E is called an "extension field" of F). This result is called Kronecker's Theorem and will be proven in Section 29.

Theorem 27.25. An ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is irreducible over F.

Note. We now have the equipment to prove Theorem 23.18 concerning factorization and irreducible polynomials.

Theorem 23.18/27.27. 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 $s(x)$.

Revised: 2/16/2014