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

Proof If M is maximal in R, then R/M is a field, hence an integral domain, and therefore M is a prime ideal by Theorem 31.15. ◆

The material that has just been presented regarding maximal and prime ideals is very important and we shall be using it quite a lot. We should keep the main ideas well in mind. We must know and understand the definitions of maximal and prime ideals and must remember the following facts that we have demonstrated.

For a commutative ring R with unity:

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 of R is a prime ideal.

Prime Fields

We now proceed 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. Let R be any ring with unity 1. Recall that by $n \cdot 1$ we mean $1 + 1 + \cdots + 1$ for n summands for $n > 0$, and $(-1) + (-1) + \cdots + (-1)$ for $|n|$ summands for $n < 0$, while $n \cdot 1 = 0$ for $n = 0$.

31.17 Theorem If R is a ring with unity 1, then the map $\phi : \mathbb{Z} \to R$ given by

$$\phi(n) = n \cdot 1$$

for $n \in \mathbb{Z}$ is a homomorphism of $\mathbb{Z}$ into R.

Proof Observe that

$$\phi(n + m) = (n + m) \cdot 1 = (n \cdot 1) + (m \cdot 1) = \phi(n) + \phi(m).$$

The distributive laws in R show that

$$\underbrace{(1 + 1 + \cdots + 1)}_{n \text{ summands}}\underbrace{(1 + 1 + \cdots + 1)}_{m \text{ summands}} = \underbrace{(1 + 1 + \cdots + 1)}_{nm \text{ summands}}.$$

Thus $(n \cdot 1)(m \cdot 1) = (nm) \cdot 1$ for $n, m > 0$. Similar arguments with the distributive laws show that for all $n, m \in \mathbb{Z}$, we have

$$(n \cdot 1)(m \cdot 1) = (nm) \cdot 1.$$

Thus

$$\phi(nm) = (nm) \cdot 1 = (n \cdot 1)(m \cdot 1) = \phi(n)\phi(m).$$ ◆

31.18 Corollary Let R be a ring with unity. If R has 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 $\mathbb{Z}$.

Proof The map $\phi : \mathbb{Z} \to R$ given by $\phi(m) = m \cdot 1$ for $m \in \mathbb{Z}$ is a homomorphism by Theorem 31.17. The kernel must be an ideal in $\mathbb{Z}$. All ideals in $\mathbb{Z}$ are of the form $s\mathbb{Z}$ for some $s \in \mathbb{Z}$. By Theorem 23.14 we see that if R has characteristic $n > 0$, then the kernel of ϕ is $n\mathbb{Z}$. Then the image $\phi[\mathbb{Z}] \leq R$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. If the characteristic of R is 0, then $m \cdot 1 \neq 0$ for all $m \neq 0$, so the kernel of ϕ is $\{0\}$. Thus, the image $\phi[\mathbb{Z}] \leq R$ is isomorphic to $\mathbb{Z}$. ◆

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

Proof If the characteristic of F is not 0, the above corollary shows that F contains a subring isomorphic to $\mathbb{Z}_n$. Then n must be a prime p, or F would have 0 divisors. If F is of characteristic 0, then F must contain a subring isomorphic to $\mathbb{Z}$. In this case Corollaries 26.9 and 26.10 show that F must contain a field of quotients of this subring and that this field of quotients must be isomorphic to $\mathbb{Q}$. ◆

Thus every field contains either a subfield isomorphic to $\mathbb{Z}_p$ for some prime p or a subfield isomorphic to $\mathbb{Q}$. These fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are the fundamental building blocks on which all fields rest.

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

Ideal Structure in $F[x]$

Throughout the rest of this section, we assume that F is a field. We give the next definition for a general commutative ring R with unity, although we are only interested in the case $R = F[x]$. Note that for a commutative ring R with unity and $a \in R$, the set $\{ra \mid r \in R\}$ is an ideal in R that contains the element a.

31.21 Definition 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 and is denoted by $\langle a \rangle$. An ideal N of R is a **principal ideal** if $N = \langle a \rangle$ for some $a \in R$. ■

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

31.23 Example The principal ideal $\langle x \rangle$ in $F[x]$ consists of all polynomials in $F[x]$ having zero constant term. ▲

The next theorem is another simple but very important application of the division algorithm for $F[x]$. (See Theorem 28.2.) The proof of this theorem is to the division algorithm in $F[x]$ as the proof that a subgroup of a cyclic group is cyclic is to the division algorithm in $\mathbb{Z}$.

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

Proof Let N be an ideal of $F[x]$. If $N = \{0\}$, then $N = \langle 0 \rangle$. Suppose that $N \neq \{0\}$, and let $g(x)$ be a nonzero element of N of minimal degree. If the degree of $g(x)$ is 0, then $g(x) \in F$ and is a unit, so $N = F[x] = \langle 1 \rangle$ by Theorem 31.5, so N is principal. If the degree of $g(x)$ is ≥ 1, let $f(x)$ be any element of N. Then by Theorem 28.2, $f(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or (degree $r(x)$) $<$ (degree $g(x)$). Now $f(x) \in N$ and $g(x) \in N$ imply that $f(x) - g(x)q(x) = r(x)$ is in N by definition of an ideal. Since $g(x)$ is a nonzero element of minimal degree in N, we must have $r(x) = 0$. Thus $f(x) = g(x)q(x)$ and $N = \langle g(x) \rangle$. ◆

We can now characterize the maximal ideals of $F[x]$. This is a crucial step in achieving our **basic goal:** to show that any nonconstant polynomial $f(x)$ in $F[x]$ has a zero in some field E containing F.

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

Proof Suppose that $\langle p(x)\rangle \neq \{0\}$ is a maximal ideal of $F[x]$. Then $\langle p(x)\rangle \neq F[x]$, so $p(x) \notin F$. Let $p(x) = f(x)g(x)$ be a factorization of $p(x)$ in $F[x]$. Since $\langle p(x)\rangle$ is a maximal ideal and hence also a prime ideal, $(f(x)g(x)) \in \langle p(x)\rangle$ implies that $f(x) \in \langle p(x)\rangle$ or $g(x) \in \langle p(x)\rangle$; that is, either $f(x)$ or $g(x)$ has $p(x)$ as a factor. But then we can't have the degrees of both $f(x)$ and $g(x)$ less than the degree of $p(x)$. This shows that $p(x)$ is irreducible over F.

Conversely, if $p(x)$ is irreducible over F, suppose that N is an ideal such that $\langle p(x)\rangle \subseteq N \subseteq F[x]$. Now N is a principal ideal by Theorem 31.24, so $N = \langle g(x)\rangle$ for some $g(x) \in N$. Then $p(x) \in N$ implies that $p(x) = g(x)q(x)$ for some $q(x) \in F[x]$. But $p(x)$ is irreducible, which implies that either $g(x)$ or $q(x)$ is of degree 0. If $g(x)$ is of degree 0, that is, a nonzero constant in F, then $g(x)$ is a unit in $F[x]$, so $\langle g(x)\rangle = N = F[x]$. If $q(x)$ is of degree 0, then $q(x) = c$, where $c \in F$, and $g(x) = (1/c)p(x)$ is in $\langle p(x)\rangle$, so $N = \langle p(x)\rangle$. Thus $\langle p(x)\rangle \subset N \subset F[x]$ is impossible, so $\langle p(x)\rangle$ is maximal. ◆

31.26 Example Example 28.10 shows that $x^3 + 3x + 2$ is irreducible in $\mathbb{Z}_5[x]$, so $\mathbb{Z}_5[x]/\langle x^3 + 3x + 2\rangle$ is a field. Similarly, Theorem 27.11 shows that $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, so $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is a field. We shall examine such fields in more detail later. ▲

Application to Unique Factorization in $F[x]$

In Section 28, we stated without proof Theorem 31.27, which follows. (See Theorem 28.19.) Assuming this theorem, we proved in Section 28 that factorization of polynomials in $F[x]$ into irreducible polynomials is unique, except for order of factors and units in F. We delayed the proof of Theorem 31.27 until now since the machinery we have developed enables us to give such a simple proof. This proof fills the gap in our proof of unique factorization in $F[x]$.

31.27 Theorem 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 Suppose $p(x)$ divides $r(x)s(x)$. Then $r(x)s(x) \in \langle p(x)\rangle$, which is maximal by Theorem 31.25. Therefore, $\langle p(x)\rangle$ is a prime ideal by Corollary 31.16. Hence $r(x)s(x) \in \langle p(x)\rangle$ implies that either $r(x) \in \langle p(x)\rangle$, giving $p(x)$ divides $r(x)$, or that $s(x) \in \langle p(x)\rangle$, giving $p(x)$ divides $s(x)$. ◆

A Preview of Our Basic Goal

We close this section with an outline of the demonstration in Section 39 of our basic goal. We have all the ideas for the proof at hand now; perhaps you can fill in the details from this outline.

Basic goal: Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Show that there exists a field E containing F and containing a zero α of $f(x)$.

Outline of the Proof

1. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$.
2. Let E be the *field* $F[x]/\langle p(x)\rangle$. (See Theorems 31.25 and 31.9.)
3. Show that no two different elements of F are in the same coset of $F[x]/\langle p(x)\rangle$, and deduce that we may consider F to be (isomorphic to) a subfield of E.
4. Let α be the coset $x + \langle p(x)\rangle$ in E. Show that for the evaluation homomorphism $\phi_\alpha : F[x] \to E$, we have $\phi_\alpha(f(x)) = 0$. That is, α is a zero of $f(x)$ in E.

An example of a field constructed according to this outline is given in Section 39. There, we give addition and multiplication tables for the field $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$. We show there that this field has just four elements, the cosets

$$0+\langle x^2+x+1\rangle, \qquad 1+\langle x^2+x+1\rangle, \qquad x+\langle x^2+x+1\rangle,$$

and

$$(x+1)+\langle x^2+x+1\rangle.$$

We rename these four cosets 0, 1, α, and $\alpha+1$ respectively, and obtain Tables 39.21 and 39.22 for addition and multiplication in this 4-element field. To see how these tables are constructed, remember that we are in a field of characteristic 2, so that $\alpha+\alpha = \alpha(1+1) = \alpha 0 = 0$. Remember also that α is a zero of x^2+x+1, so that $\alpha^2+\alpha+1 = 0$ and consequently $\alpha^2 = -\alpha - 1 = \alpha + 1$.

EXERCISES 31

Computations

1. Find all prime ideals and all maximal ideals of $\mathbb{Z}_6$.

2. Find all prime ideals and all maximal ideals of $\mathbb{Z}_{12}$.

3. Find all prime ideals and all maximal ideals of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Find all prime ideals and all maximal ideals of $\mathbb{Z}_2 \times \mathbb{Z}_4$.

5. Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/\langle x^2+c\rangle$ is a field.

6. Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/\langle x^3+x^2+c\rangle$ is a field.

7. Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/\langle x^3+cx^2+1\rangle$ is a field.

8. Find all $c \in \mathbb{Z}_5$ such that $\mathbb{Z}_5[x]/\langle x^2+x+c\rangle$ is a field.

9. Find all $c \in \mathbb{Z}_5$ such that $\mathbb{Z}_5[x]/\langle x^2+cx+1\rangle$ is a field.

Concepts

In Exercises 10 through 13, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

10. A *maximal ideal* of a ring R is an ideal that is not contained in any other ideal of R.

11. A *prime ideal* of a commutative ring R is an ideal of the form $pR = \{pr \mid r \in R\}$ for some prime p.

12. A *prime field* is a field that has no proper subfields.

13. A *principal ideal* of a commutative ring with unity is an ideal N with the property that there exists $a \in N$ such that N is the smallest ideal that contains a.

14. Determine whether each of the following is true or false.

a. Every prime ideal of every commutative ring with unity is a maximal ideal.

b. Every maximal ideal of every commutative ring with unity is a prime ideal.

c. $\mathbb{Q}$ is its own prime subfield.

d. The prime subfield of $\mathbb{C}$ is $\mathbb{R}$.

e. Every field contains a subfield isomorphic to a prime field.

f. A ring with zero divisors may contain one of the prime fields as a subring.

g. Every field of characteristic zero contains a subfield isomorphic to $\mathbb{Q}$.

h. Let F be a field. Since $F[x]$ has no divisors of 0, every ideal of $F[x]$ is a prime ideal.

i. Let F be a field. Every ideal of $F[x]$ is a principal ideal.

j. Let F be a field. Every principal ideal of $F[x]$ is a maximal ideal.

15. Find a maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.