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 27.25 and 27.9.)
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 29. 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 29.20 and 29.21 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 27

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. Mark each of the following 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 $\mathbb{Z} \times \mathbb{Z}$.

16. Find a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not maximal.

17. Find a nontrivial proper ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not prime.

18. Is $\mathbb{Q}[x]/\langle x^2 - 5x + 6\rangle$ a field? Why?

19. Is $\mathbb{Q}[x]/\langle x^2 - 6x + 6\rangle$ a field? Why?

Proof Synopsis

20. Give a one- or two-sentence synopsis of "only if" part of Theorem 27.9.

21. Give a one- or two-sentence synopsis of "if" part of Theorem 27.9.

22. Give a one- or two-sentence synopsis of Theorem 27.24.

23. Give a one- or two-sentence synopsis of the "only if" part of Theorem 27.25.

Theory

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

25. Corollary 27.18 tells us that every ring with unity contains a subring isomorphic to either $\mathbb{Z}$ or some $\mathbb{Z}_n$. Is it possible that a ring with unity may simultaneously contain two subrings isomorphic to $\mathbb{Z}_n$ and $\mathbb{Z}_m$ for $n \neq m$? If it is possible, give an example. If it is impossible, prove it.

26. Continuing Exercise 25, is it possible that a ring with unity may simultaneously contain two subrings isomorphic to the fields $\mathbb{Z}_p$ and $\mathbb{Z}_q$ for two different primes p and q? Give an example or prove it is impossible.

27. Following the idea of Exercise 26, is it possible for an integral domain to contain two subrings isomorphic to $\mathbb{Z}_p$ and $\mathbb{Z}_q$ for $p \neq q$ and p and q both prime? Give reasons or an illustration.

28. Prove directly from the definitions of maximal and prime ideals that every maximal ideal of a commutative ring R with unity is a prime ideal. [*Hint*: Suppose M is maximal in R, $ab \in M$, and $a \notin M$. Argue that the smallest ideal $\{ra + m \mid r \in R, m \in M\}$ containing a and M must contain 1. Express 1 as $ra + m$ and multiply by b.]

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.)

30. Prove that if F is a field, every proper nontrivial prime ideal of $F[x]$ is maximal.

31. Let F be a field and $f(x), g(x) \in F[x]$. Show that $f(x)$ divides $g(x)$ if and only if $g(x) \in \langle f(x) \rangle$.

32. Let F be a field and let $f(x), g(x) \in F[x]$. Show that

$$N = \{r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in F[x]\}$$

is an ideal of $F[x]$. Show that if $f(x)$ and $g(x)$ have different degrees and $N \neq F[x]$, then $f(x)$ and $g(x)$ cannot both be irreducible over F.

33. Use Theorem 27.24 to prove the *equivalence* of these two theorems:

Fundamental Theorem of Algebra: Every nonconstant polynomial in $\mathbb{C}[x]$ has a zero in $\mathbb{C}$.

Nullstellensatz for $\mathbb{C}[x]$: Let $f_1(x), \cdots, f_r(x) \in \mathbb{C}[x]$ 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 $f_1(x), \cdots, f_r(x)$.

There is a sort of arithmetic of ideals in a ring. The next three exercises define sum, product, and quotient of ideals.

34. If A and B are ideals of a ring R, the **sum $A + B$ of A and B** is defined by

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

a. Show that $A + B$ is an ideal.

b. Show that $A \subseteq A + B$ and $B \subseteq A + B$.

35. Let A and B be ideals of a ring R. The **product AB of A and B** is defined by

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}.$$

a. Show that AB is an ideal in R.

b. Show that $AB \subseteq (A \cap B)$.

36. Let A and B be ideals of a *commutative* ring R. The **quotient $A : B$ of A by B** is defined by

$$A : B = \{r \in R \mid rb \in A \text{ for all } b \in B\}.$$

Show that $A : B$ is an ideal of R.

37. Show that for a field F, the set S of all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

for $a, b \in F$ is a **right ideal** but not a **left ideal** of $M_2(F)$. That is, show that S is a subring closed under multiplication on the *right* by any element of $M_2(F)$, but is not closed under *left* multiplication.

38. Show that the matrix ring $M_2(\mathbb{Z}_2)$ is a simple ring; that is, $M_2(\mathbb{Z}_2)$ has no proper nontrivial ideals.

SECTION 28 †GRÖBNER BASES FOR IDEALS

This section gives a brief introduction to algebraic geometry. In particular, we are concerned with the problem of finding as simple a description as we can of the set of common zeros of a finite number of polynomials. In order to accomplish our goal in a single section of this text, we will be stating a few theorems without proof. We recommend the book by Adams and Loustaunau [23] for the proofs and further study.

† This section is not used in the remainder of the text.