23. $\langle x^2y - x - 2, xy + 2y - 9\rangle$

24. $\langle x^2y + x, xy^2 - y\rangle$

25. $\langle x^2y + x + 1, xy^2 + y - 1\rangle$

26. $\langle x^2y + xy^2, xy - x\rangle$

Concepts

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

a. Polynomials in a Gröbner basis are linearly independent.

b. The set $\{1\}$ is a Gröbner basis.

c. The set $\{0\}$ is a Gröbner basis.

d. The order one picks for the power products does not affect the resulting Gröbner basis.

e. For any total ordering of all the power products, $x_1^2 > x_1$.

f. A Gröbner basis can be used to determine if a graph can be colored with n colors starting with a basis consisting of polynomials each of degree at most n.

g. A Gröbner basis can be used to determine if a graph can be colored with n colors starting with a basis consisting of $r + s$ polynomials where r is the number of vertices in the graph and s is the number of edges in the graph.

h. I have computed Gröbner bases before I knew what they were.

i. Any ideal in $F[\mathbf{x}]$ has a unique Gröbner basis.

j. A basis for an ideal I in $F[x_1, x_2, \ldots, x_n]$ is a Gröbner basis if and only if each polynomial in the basis cannot be reduced further using the division algorithm.

28. Let $\mathbb{R}[x, y]$ be ordered by lex. Give an example to show that $P_i < P_j$ does not imply that P_i divides P_j.

29. What other orders of the indeterminate a, c, x, y, d_1, d_2 would you expect the equation of an ellipse to result from computing a Gröbner basis for the ideal in Example 38.7?

30. Use a Gröbner basis to derive the formula for a hyperbola in standard position. Recall that a hyperbola in standard position is the set of all points in the plane whose difference in distances from $(c, 0)$ and $(-c, 0)$ is $\pm 2a$. You may use a computer to compute the Gröbner basis.

31. Use a Gröbner basis to show that the graph with vertex set $\{x_1, x_2, x_3, x_4, x_5\}$ and edge set $\{\{x_1, x_2\}, \{x_2, x_3\}, \{x_3, x_4\}, \{x_1, x_3\}, \{x_1, x_5\}, \{x_5, x_4\}\}$ cannot be colored with three colors, but it can be colored with four colors. You may use a computer to compute the Gröbner basis.

Theory

32. Show that $\{xy, y^2 - y)$ is a Gröbner basis for $\langle xy, y^2 - y\rangle$, as asserted after Example 38.1.

33. Show that $\{-4yp + x^2, d - y - p\}$ is a Gröbner basis for the ideal $\langle -4yp + x^2, d - y - p\rangle$ as asserted in Example 38.6.

34. Prove Theorem 38.8. [Hint: Think about coloring a graph with the n^{th} roots of unity.]

PART VIII

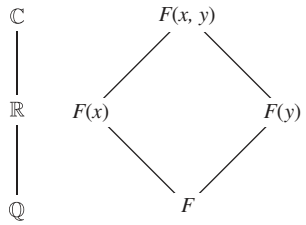
Extension Fields

SECTION 39 INTRODUCTION TO EXTENSION FIELDS

Our Basic Goal Achieved

We are now in a position to achieve our **basic goal,** which, loosely stated, is to show that every nonconstant polynomial has a zero. This will be stated more precisely and proved in Theorem 39.3. We first introduce some new terminology for some old ideas.

39.1 Definition A field E is an **extension field of a field** F if $F \leq E$. ■



39.2 Figure

Thus $\mathbb{R}$ is an extension field of $\mathbb{Q}$, and $\mathbb{C}$ is an extension field of both $\mathbb{R}$ and $\mathbb{Q}$. As in the study of groups, it will often be convenient to use subfield diagrams to picture extension fields, the larger field being on top. We illustrate this in Fig. 39.2. (Recall that $F(x)$ is the field of quotients constructed from $F[x]$.) A configuration where there is just one single column of fields, as at the left-hand side of Fig. 39.2, is often referred to, without any precise definition, as a **tower of fields.**

Now for our *basic goal!* This great and important result follows quickly and elegantly from the techniques we now have at our disposal.

† Section 41 is not required for the remainder of the text.

39.3 Theorem **(Kronecker's Theorem) (Basic Goal)** Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

Proof By Theorem 28.21, $f(x)$ has a factorization in $F[x]$ into polynomials that are irreducible over F. Let $p(x)$ be an irreducible polynomial in such a factorization. It is clearly sufficient to find an extension field E of F containing an element α such that $p(\alpha) = 0$.

By Theorem 31.25, $\langle p(x)\rangle$ is a maximal ideal in $F[x]$, so $F[x]/\langle p(x)\rangle$ is a field. We claim that F can be identified with a subfield of $F[x]/\langle p(x)\rangle$ in a natural way by use of the map $\psi : F \to F[x]/\langle p(x)\rangle$ given by

$$\psi(a) = a + \langle p(x)\rangle$$

for $a \in F$. This map is one-to-one, for if $\psi(a) = \psi(b)$, that is, if $a + \langle p(x)\rangle = b + \langle p(x)\rangle$ for some $a, b \in F$, then $(a - b) \in \langle p(x)\rangle$, so $a - b$ must be a multiple of the polynomial $p(x)$, which is of degree ≥ 1. Now $a, b \in F$ implies that $a - b$ is in F. Thus we must have $a - b = 0$, so $a = b$. We defined addition and multiplication in $F[x]/\langle p(x)\rangle$ by choosing any representatives, so we may choose $a \in (a + \langle p(x)\rangle)$. Thus ψ is a homomorphism that maps F one-to-one onto a subfield of $F[x]/\langle p(x)\rangle$. We identify F with $\{a + \langle p(x)\rangle \mid a \in F\}$ by means of this map ψ. Thus we shall view $E = F[x]/\langle p(x)\rangle$ as an extension field of F. We have now manufactured our desired extension field E of F. It remains for us to show that E contains a zero of $p(x)$.

■ HISTORICAL NOTE

Leopold Kronecker is known for his insistence on constructibility of mathematical objects. As he noted, "God made the integers; all else is the work of man." Thus, he wanted to be able to construct new "domains of rationality" (fields) by using only the existence of integers and indeterminates. He did not believe in starting with the real or complex numbers, because as far as he was concerned, those fields could not be determined in a constructive way. Hence in an 1881 paper, Kronecker created an extension field by simply adjoining to a given field a root α of an irreducible nth degree polynomial $p(x)$; that is, his new field consisted of expressions rational in the original field elements and his new root α with the condition that $p(\alpha) = 0$. The proof of the theorem presented in the text (Theorem 39.3) dates from the twentieth century.

Kronecker completed his dissertation in 1845 at the University of Berlin. For many years thereafter, he managed the family business, ultimately becoming financially independent. He then returned to Berlin, where he was elected to the Academy of Sciences and thus permitted to lecture at the university. On the retirement of Kummer, he became a professor at Berlin, and with Karl Weierstrass (1815–1897) directed the influential mathematics seminar.

Let us set

$$\alpha = x + \langle p(x)\rangle,$$

so $\alpha \in E$. Consider the evaluation homomorphism $\phi_\alpha : F[x] \to E$, given by Theorem 27.4. If $p(x) = a_0 + a_1x + \cdots + a_nx^n$, where $a_i \in F$, then we have

$$\phi_\alpha(p(x)) = a_0 + a_1(x + \langle p(x)\rangle) + \cdots + a_n(x + \langle p(x)\rangle)^n$$

in $E = F[x]/\langle p(x)\rangle$. *But we can compute in $F[x]/\langle p(x)\rangle$ by choosing representatives, and x is a representative of the coset $\alpha = x + \langle p(x)\rangle$.* Therefore,

$$\begin{aligned} p(\alpha) &= \left(a_0 + a_1x + \cdots + a_nx^n\right) + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0 \end{aligned}$$

in $F[x]/\langle p(x)\rangle$. We have found an element α in $E = F[x]/\langle p(x)\rangle$ such that $p(\alpha) = 0$, and therefore $f(\alpha) = 0$. ◆

We illustrate the construction involved in the proof of Theorem 39.3 by two examples.

39.4 Example Let $F = \mathbb{R}$, and let $f(x) = x^2 + 1$, which is well known to have no zeros in $\mathbb{R}$ and thus is irreducible over $\mathbb{R}$ by Theorem 28.11. Then $\langle x^2 + 1\rangle$ is a maximal ideal in $\mathbb{R}[x]$, so $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is a field. Identifying $r \in \mathbb{R}$ with $r + \langle x^2 + 1\rangle$ in $\mathbb{R}[x]/\langle x^2 + 1\rangle$, we can view $\mathbb{R}$ as a subfield of $E = \mathbb{R}[x]/\langle x^2 + 1\rangle$. Let

$$\alpha = x + \langle x^2 + 1\rangle.$$

Computing in $\mathbb{R}[x]/\langle x^2 + 1\rangle$, we find

$$\begin{aligned}\alpha^2 + 1 &= (x + \langle x^2 + 1\rangle)^2 + (1 + \langle x^2 + 1\rangle)\\ &= (x^2 + 1) + \langle x^2 + 1\rangle = 0.\end{aligned}$$

Thus α is a zero of $x^2 + 1$. We shall identify $\mathbb{R}[x]/\langle x^2 + 1\rangle$ with $\mathbb{C}$ near the close of this section. ▲

39.5 Example Let $F = \mathbb{Q}$, and consider $f(x) = x^4 - 5x^2 + 6$. This time $f(x)$ factors in $\mathbb{Q}[x]$ into $(x^2 - 2)(x^2 - 3)$, both factors being irreducible over $\mathbb{Q}$, as we have seen. We can start with $x^2 - 2$ and construct an extension field E of $\mathbb{Q}$ containing α such that $\alpha^2 - 2 = 0$, or we can construct an extension field K of $\mathbb{Q}$ containing an element β such that $\beta^2 - 3 = 0$. The construction in either case is just as in Example 39.4. ▲

Algebraic and Transcendental Elements

As we said before, most of the rest of this text is devoted to the study of zeros of polynomials. We commence this study by putting an element of an extension field E of a field F into one of two categories.

39.6 Definition An element α of an extension field E of a field F is **algebraic over** F if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$. If α is not algebraic over F, then α is **transcendental over** F. ■

39.7 Example $\mathbb{C}$ is an extension field of $\mathbb{Q}$. Since $\sqrt{2}$ is a zero of $x^2 - 2$, we see that $\sqrt{2}$ is an algebraic element over $\mathbb{Q}$. Also, i is an algebraic element over $\mathbb{Q}$, being a zero of $x^2 + 1$. ▲

39.8 Example It is well known (but not easy to prove) that the real numbers π and e are transcendental over $\mathbb{Q}$. Here e is the base for the natural logarithms. ▲

Just as we do not speak simply of an *irreducible polynomial,* but rather of an *irreducible polynomial over F*, similarly we don't speak simply of an *algebraic element,* but rather of an *element algebraic over F*. The following illustration shows the reason for this.

39.9 Example The real number π is transcendental over $\mathbb{Q}$, as we stated in Example 39.8. However, π is algebraic over $\mathbb{R}$, for it is a zero of $(x - \pi) \in \mathbb{R}[x]$. ▲

39.10 Example It is easy to see that the real number $\sqrt{1 + \sqrt{3}}$ is algebraic over $\mathbb{Q}$. For if $\alpha = \sqrt{1 + \sqrt{3}}$, then $\alpha^2 = 1 + \sqrt{3}$, so $\alpha^2 - 1 = \sqrt{3}$ and $(\alpha^2 - 1)^2 = 3$. Therefore $\alpha^4 - 2\alpha^2 - 2 = 0$, so α is a zero of $x^4 - 2x^2 - 2$, which is in $\mathbb{Q}[x]$. ▲

To connect these ideas with those of number theory, we give the following definition.