

The theorem that follows provides a tool for this task. You should notice that the theorem gives information about the division algorithm that we did not mention in Theorem 28.2. We use the same notation here as in Theorem 28.2, but with \mathbf{x} rather than x . If $f(\mathbf{x}) = g(\mathbf{x})h(\mathbf{x})$ in $F(\mathbf{x})$, then $g(\mathbf{x})$ and $h[\mathbf{x}]$ are called “**divisors**” or “**factors**” of $f(\mathbf{x})$.

37.7 Theorem (Property of the Division Algorithm) Let $f(\mathbf{x})$, $g(\mathbf{x})$, $q(\mathbf{x})$, and $r(\mathbf{x})$ be polynomials in $F[\mathbf{x}]$ such that $f(\mathbf{x}) = g(\mathbf{x})q(\mathbf{x}) + r(\mathbf{x})$. The common zeros in F^n of $f(\mathbf{x})$ and $g(\mathbf{x})$ are the same as the common zeros of $g(\mathbf{x})$ and $r(\mathbf{x})$. Also the common divisors in $F[\mathbf{x}]$ of $f(\mathbf{x})$ and $g(\mathbf{x})$ are the same as the common divisors of $g(\mathbf{x})$ and $r(\mathbf{x})$.

If $f(\mathbf{x})$ and $g(\mathbf{x})$ are two members of a basis for an ideal I of $F[\mathbf{x}]$, then replacement of $f(\mathbf{x})$ by $r(\mathbf{x})$ in the basis still yields a basis for I .

Proof If $\mathbf{a} \in F^n$ is a common zero of $g(\mathbf{x})$ and $r(\mathbf{x})$, then applying $\phi_{\mathbf{a}}$ to both sides of the equation $f(\mathbf{x}) = g(\mathbf{x})q(\mathbf{x}) + r(\mathbf{x})$, we obtain $f(\mathbf{a}) = g(\mathbf{a})q(\mathbf{a}) + r(\mathbf{a}) = 0q(\mathbf{a}) + 0 = 0$, so \mathbf{a} is a zero of both $f(\mathbf{x})$ and $g(\mathbf{x})$. If $\mathbf{b} \in F[\mathbf{x}]$ is a common zero of $f(\mathbf{x})$ and $g(\mathbf{x})$, then applying $\phi_{\mathbf{b}}$ yields $f(\mathbf{b}) = g(\mathbf{b})q(\mathbf{b}) + r(\mathbf{b})$ so $0 = 0q(\mathbf{b}) + r(\mathbf{b})$ and we see that $r(\mathbf{b}) = 0$ and $g(\mathbf{b}) = 0$.

The proof concerning common divisors is essentially the same, and is left as Exercise 15.

Finally, let B be a basis for an ideal I , let $f(\mathbf{x}), g(\mathbf{x}) \in B$, and let $f(\mathbf{x}) = g(\mathbf{x})q(\mathbf{x}) + r(\mathbf{x})$. Let B' be the set obtained by replacing $f(\mathbf{x})$ by $r(\mathbf{x})$ in B , and let I' be the ideal having B' as a basis. Let S be the set obtained from B by adjoining $r(\mathbf{x})$ to B . Note that S can also be obtained by adjoining $f(\mathbf{x})$ to B' . The equation $f(\mathbf{x}) = g(\mathbf{x})q(\mathbf{x}) + r(\mathbf{x})$ shows that $f(\mathbf{x}) \in I'$, so we have $B' \subseteq S \subseteq I'$. Thus S is a basis for I' . The equation $r(\mathbf{x}) = f(\mathbf{x}) - q(\mathbf{x})g(\mathbf{x})$ shows that $r(\mathbf{x}) \in I$, so we have $B \subseteq S \subseteq I$. Thus S is basis for I . Therefore $I = I'$ and B' is a basis for I . ♦

A Familiar Linear Illustration

A basic technique for problem solving in linear algebra is finding all common solutions of a finite number of linear equations. For the moment we abandon our practice of never writing “ $f(\mathbf{x}) = 0$ ” for a nonzero polynomial, and work a typical problem as we do in a linear algebra course.

37.8 Example (Solution as in a Linear Algebra Course) Find all solutions in \mathbb{R}^3 of the linear system

$$\begin{aligned}x + y - 3z &= 8 \\ 2x + y + z &= -5.\end{aligned}$$

Solution We multiply the first equation by -2 and add it to the second, obtaining the new system

$$\begin{aligned}x + y - 3z &= 8 \\ -y + 7z &= -21\end{aligned}$$

which has the same solution set in \mathbb{R}^3 as the preceding one. For any value z , we can find the corresponding y -value from the second equation and then determine x from the first equation. Keeping z as parameter, we obtain $\{(-4z - 13, 7z + 21, z) \mid z \in \mathbb{R}\}$ as solution set, which is a line in Euclidean 3-space through the point $(-13, 21, 0)$. ▲

In the notation of this section, the problem in the preceding example can be phrased as follows:

Describe $V(\langle x + y - 3z - 8, 2x + y + z + 5 \rangle)$ in \mathbb{R}^3 .

We solved it by finding a more useful basis, namely

$$\{x + y - 3z - 8, -y + 7z + 21\}.$$

Notice that the second member, $-y + 7z + 21$, of this new basis can be obtained from the original two basis polynomials as a remainder $r(x, y, z)$ in a division process, namely

$$\begin{array}{r} 2 \\ x + y - 3z - 8 \overline{) 2x + y + z + 5} \\ \underline{2x + 2y - 6z - 16} \\ -y + 7z + 21 \end{array}$$

Thus $2x + y + z + 5 = (x + y - 3z - 8)(2) + (-y + 7z + 21)$, an expression of the form $f(x, y, z) = g(x, y, z)q(x, y, z) + r(x, y, z)$. We replaced the polynomial f by the polynomial r , as in Theorem 37.7, which assures us that $V(\langle f, g \rangle) = V(\langle g, r \rangle)$ and that $\langle f, g \rangle = \langle g, r \rangle$. We chose a very simple, 1-step problem in Example 37.8. However, it is clear that the method introduced in a linear algebra course for solving a linear system can be phrased in terms of applying a division algorithm process repeatedly to change a given ideal basis into one that better illuminates the geometry of the associated algebraic variety.

A Single Indeterminate Illustration

Suppose now that we want to find the variety $V(I)$ in \mathbb{R} associated with an ideal I in $F[x]$, the ring of polynomials in the single indeterminate x . By Theorem 31.24, every ideal in $F[x]$ is principal, so there exists $f(x) \in F[x]$ such that $I = \langle f(x) \rangle$. Thus $V(I)$ consists of the zeros of a single polynomial, and $\{f(x)\}$ is probably as simple a basis for I as we could desire. We give an example illustrating computation of such a single generator $f(x)$ for I in a case where the given basis for I contains more than one polynomial. Because a polynomial in $\mathbb{R}[x]$ has only a finite number of zeros in \mathbb{R} , we expect two or more randomly selected polynomials in $\mathbb{R}[x]$ to have no common zeros, but we constructed the basis in our example carefully!

37.9 Example Let us describe the algebraic variety V in \mathbb{R} consisting of common zeros of

$$f(x) = x^4 + x^3 - 3x^2 - 5x - 2 \quad \text{and} \quad g(x) = x^3 + 3x^2 - 6x - 8.$$

We want to find a new basis for $\langle f, g \rangle$ having polynomials of as small degree as possible, so we use the division algorithm $f(x) = g(x)q(x) + r(x)$ in Theorem 28.2, where $r(x)$ will have degree at most 2. We then replace the basis $\{f, g\}$ by the basis $\{g, r\}$.

$$\begin{array}{r} x - 2 \\ x^3 + 3x^2 - 6x - 8 \overline{) x^4 + x^3 - 3x^2 - 5x - 2} \\ \underline{x^4 + 3x^3 - 6x^2 - 8x} \\ -2x^3 + 3x^2 + 3x - 2 \\ \underline{-2x^3 - 6x^2 + 12x + 16} \\ 9x^2 - 9x - 18 \end{array}$$

Because zeros of $9x^2 - 9x - 18$ are the same as zeros of $x^2 - x - 2$, we let $r(x) = x^2 - x - 2$, and take as new basis

$$\{g, r\} = (x^3 + 3x^2 - 6x - 8, x^2 - x - 2).$$

By dividing $g(x)$ by $r(x)$ to obtain a remainder $r_1(x)$, we will now be able to find a basis $\{r(x), r_1(x)\}$ consisting of polynomials of degree at most 2.

$$\begin{array}{r}
 x^2 - x - 2 \overline{) \begin{array}{l} x^3 + 3x^2 - 6x - 8 \\ x^3 - x^2 - 2x \\ \hline 4x^2 - 4x - 8 \\ 4x^2 - 4x - 8 \\ \hline 0 \end{array}}
 \end{array}$$

Our new basis $\{r(x), r_1(x)\}$ now becomes $\{x^2 - x - 2\}$. Thus $I = \langle f(x), g(x) \rangle = \langle x^2 - x - 2 \rangle = \langle (x - 2)(x + 1) \rangle$, and we see that $V = \{-1, 2\}$. ▲

Theorem 37.7 tells us that the common divisors of $f(x)$ and $g(x)$ in the preceding example are the same as the common divisors of $r(x)$ and $r_1(x)$. Because $0 = (0)r(x)$, we see that $r(x)$ itself divides 0, so the common divisors of $f(x)$ and $g(x)$ are just those of $r(x)$, which, of course, include $r(x)$ itself. Thus $r(x)$ is called a “*greatest common divisor*” (abbreviated gcd) of $f(x)$ and $g(x)$.

■ EXERCISES 37

In Exercises 1–4 find a basis for the given ideals in $\mathbb{R}[x, y]$.

1. The set of polynomials with constant 0.
2. The kernel of the evaluation homomorphism $\phi_{(2,3)} : \mathbb{R}[x, y] \rightarrow \mathbb{R}$.
3. The kernel of the evaluation homomorphism $\phi_{(-4,5)} : \mathbb{R}[x, y] \rightarrow \mathbb{R}$.
4. The set of all polynomials with zeros on the circle centered at the origin with radius 1.

In Exercises 5–8, use the techniques from Examples 37.8 and 37.9 to find a simpler basis for the ideal where the field is \mathbb{R} . Describe the algebraic variety associated with the ideal.

5. $I = \langle x + y + z, 2x + y + 3z - 4 \rangle$
6. $I = \langle 3x + 4y + 7z - 10, 2x + 3y - 2z + 1 \rangle$
7. $I = \langle x^4 + 5x^3 + 3x^2 - 7x - 2, x^3 + 6x^2 + 3x - 10 \rangle$
8. $I = \langle x^6 - x^5 - 6x^4 + 3x^3 - 8x^2 - 4x + 3, x^3 - 2x^2 - 9 \rangle$
9. Describe the algebraic variety for the ideal $\{0\}$ in $F[x, y]$.
10. Describe the algebraic variety for the ideal $\{1\}$ in $F[x, y]$.
11. Describe the algebraic variety in F for the ideal $\langle x^2 + 1 \rangle$ a) for $F = \mathbb{R}$ and b) for $F = \mathbb{C}$.
12. Compare the algebraic varieties for the ideals $I = \langle x^2 + 4xy + 4y^2 \rangle$ and $J = \langle x + 2y \rangle$.

Concepts

13. Determine whether each of the following is true or false.
 - a. Every ideal in $F[\mathbf{x}]$ has a finite basis.
 - b. Every subset of \mathbb{R}^2 is an algebraic variety.
 - c. The empty subset of \mathbb{R}^2 is an algebraic variety.
 - d. Every finite subset of \mathbb{R}^2 is an algebraic variety.
 - e. Every line in \mathbb{R}^2 is an algebraic variety.
 - f. Every finite collection of lines in \mathbb{R}^2 is an algebraic variety.
 - g. A greatest common divisor of a finite number of polynomials in $\mathbb{R}[x]$ (one indeterminate) can be computed using the division algorithm repeatedly.

- h. In the context of ideals in a commutative ring with unity, elements in a basis are independent.
- i. If R is a Noetherian ring, then so is $R[x]$.
- j. The ideals $\langle x, y \rangle$ and $\langle x^2, y^2 \rangle$ are equal because they both yield the same algebraic variety, namely $\{(0, 0)\}$, in \mathbb{R}^2 .

Theory

- 14. Show that if f_1, f_2, \dots, f_r are elements of a commutative ring R with unity, then $I = \{c_1 f_1 + c_2 f_2 + \dots + c_r f_r \mid c_i \in R \text{ for } i = 1, \dots, r\}$ is an ideal of R .
- 15. Show that if $f(\mathbf{x}) = g(\mathbf{x})q(\mathbf{x}) + r(\mathbf{x})$ in $F[\mathbf{x}]$, then the common divisors in $F[\mathbf{x}]$ of $f(\mathbf{x})$ and $g(\mathbf{x})$ are the same as the common divisors in $F[\mathbf{x}]$ of $g(\mathbf{x})$ and $r(\mathbf{x})$.
- 16. Let F be a field. Show that if S is a nonempty subset of F^n , then

$$I(S) = \{f(\mathbf{x}) \in F[\mathbf{x}] \mid f(\mathbf{s}) = 0 \text{ for all } \mathbf{s} \in S\}$$

is an ideal of $F[\mathbf{x}]$.

- 17. Referring to Exercise 16, show that $S \subseteq V(I(S))$.
- 18. Referring to Exercise 16, give an example of a subset S of \mathbb{R}^2 such that $V(I(S)) \neq S$.
- 19. Referring to Exercise 16, show that if N is an ideal of $F[\mathbf{x}]$, then $N \subseteq I(V(N))$.
- 20. Referring to Exercise 16, give an example of an ideal N in $\mathbb{R}[x, y]$ such that $I(V(N)) \neq N$.
- 21. Prove for R a commutative ring with unity, R is a Noetherian ring if and only if every ideal in R has a finite basis.

SECTION 38 [†]GRÖBNER BASES FOR IDEALS

We tackle the problem of finding a nice basis for an ideal I in $F[\mathbf{x}] = F[x_1, x_2, \dots, x_n]$. In view of our Section 37 illustrations for the linear and single indeterminant cases, it seems reasonable to try to replace polynomials in a basis by polynomials of lower degree, or containing fewer indeterminates. It is crucial to have a systematic way to accomplish this. As you probably learned in linear algebra, when row reducing matrices, it is important to follow the standard order for which matrix entries you make zero. If you make an entry in the second column zero before dealing with the first column, you may have wasted your time. As a first step in our goal, we tackle this problem of specifying an order for polynomials in a basis.

Ordering Power Products

Our polynomials in $F[\mathbf{x}]$ have terms of the form $ax_1^{m_1}x_2^{m_2}\dots x_n^{m_n}$ where $a \in F$. Let us consider a **power product** in $F[\mathbf{x}]$ to be an expression

$$P = x_1^{m_1}x_2^{m_2}\dots x_n^{m_n} \text{ where all the } m_i \geq 0 \text{ in } \mathbb{Z}.$$

Notice that all x_i are present, perhaps some with exponent 0. Thus in $F[x, y, z]$, we must write xz^2 as xy^0z^2 to be a power product. We want to describe a *total ordering* $<$ on the set of all power products so that we know just what it means to say that $P_i < P_j$ for two power products, providing us with a notion of relative size for power products. We can then try to change an ideal basis in a systematic way to create one with polynomials having terms $a_i P_i$ with as “small” power products P_i as possible. We denote by 1 the power product with all exponents 0, and require that an ordering of the power products has the properties listed below. Suppose that such an ordering has been described and that $P_i \neq P_j$ and P_i divides P_j so that $P_j = PP_i$ where $1 < P$. From Property 4, we then have $1P_i < PP_i = P_j$, so $P_i < P_j$. Thus P_i divides P_j implies that

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