Section III.6. Factorization in Polynomial Rings

Note. We push several of the results in Section III.3 (such as divisibility, irreducibility, and unique factorization) from rings to rings of polynomials. This is a vital step towards our ultimate goal of finding zeros of a polynomial.

Definition. Let R be a ring and $R[x_1, x_2, \ldots, x_n]$ be a ring of polynomials in n indeterminates. The *degree of a nonzero monomial* $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} \in R[x_1, x_2, \ldots, x_n]$ is the nonnegative integer $k_1 + k_2 + \cdots + k_n$. If f is a nonzero polynomial in $R[x_1, x_2, \ldots, x_n]$ then by Theorem III.5.4(v)

$$f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}} \in R[x_1, x_2, \ldots, x_n]$$

and the *(total) degree of polynomial* f is the maximum of the degrees of the monomials $a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}}$ such that $a_i \neq 0$, denoted $\deg(f)$. A polynomial which is a sum of monomials each of degree k is *homogeneous of degree* k. The *degree of* f *in* x_k is the degree of f considered as a polynomial in one indeterminate x_k over $R[x_1, x_2, \ldots, x_{k-1}, x_{k+1}, \ldots, x_k]$.

Note. The degree of f in x_k is simply the highest power of x_k in f. For example, $3x_1^2x_2^2x_3^2 + 3x_1x_3^4 - 6x_2^3x_3 \in \mathbb{Z}[x]$ has degree 2 in x_1, degree 3 in x_2, and degree 4 in x_3. The total degree is 6.

Note III.6.A. By convention we define the degree of the zero polynomial to be $-\infty$. This convention is useful, as we'll see in the proof of the Division Algorithm (Theorem III.6.2).

Theorem III.6.1. Let R be a ring and $f, g \in R[x_1, x_2, \ldots, x_n]$.

(i) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.

(ii) $\deg(fg) \leq \deg(f) + \deg(g)$.

(iii) If R has no zero divisors then $\deg(fg) = \deg(f) + \deg(g)$.

(iv) If $n = 1$ and the leading coefficient of f or g is not a zero divisor in R (in particular, if it is a unit) then $\deg(fg) = \deg(f) + \deg(g)$.

Note. The proof of Theorem III.6.1 is based on consideration of the highest power of x in fg when f and g are represented in the standard way. In fact, the result holds where "$\deg(f)$" is replaced with "degree of f in x_k." Several of the following results are also covered in Precalculus 1, Algebra (MATH 1710). See my online notes on Section 4.5. The Real Zeros of a Polynomial Function where The Division Algorithm (Theorem 4.5.A in those notes) is stated but not proved, The Remainder Theorem (Theorem 4.5.B) is proved, The Factor Theorem (Theorem 4.5.C) is proved, The Number of Real Zeros (Theorem 4.5.D, which corresponds to Theorem III.6.7 here) is proved, The Rational Zeros Theorem (Theorem 4.5.F, which corresponds to Proposition III.6.8 here with $D = F = \mathbb{Q}$) is stated but not proved. Of course the setting in Precalculus 1, other than The Rational Zeros Theorem, is $\mathbb{R}[x]$.

Theorem III.6.2. The Division Algorithm.

Let R be a ring with identity and $f, g \in R[x]$ nonzero polynomials such that the leading coefficient of g is a unit in R. Then there exist unique polynomials $q, r \in R[x]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.

Corollary III.6.3. Remainder Theorem.

Let R be a ring with identity and $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$.

Corollary III.6.4. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials.

Note. We now turn our attention to roots of polynomials and "linear factors."

Definition III.6.5. Let R be a subring of a commutative ring S, $c_1, c_2, \ldots, c_n \in S$ and

$$f = \sum_{i=0}^{m} a_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}} \in R[x_1, x_2, \ldots, x_n]$$

a polynomial such that $f(c_1, c_2, \ldots, c_n) = 0$. Then $(c_1, c_2, \ldots, c_n)$ is a *root* or *zero* of f (or a *solution* of the polynomial equation $f(x_1, x_2, \ldots, x_n) = 0$).

Note. The following result relates zeros of a polynomial to linear factors of the polynomial. This result is usually called the Factor Theorem (see Corollary 23.3 in Fraleigh).

Theorem III.6.6. Factor Theorem.
Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f.

Note. The following result is an important step on the road to proving the Fundamental Theorem of Algebra (see the appendix to Section V.5).

Theorem III.6.7. If D is an integral domain contained in an integral domain E and $f \in D[x]$ has degree n, then f has at most n distinct roots in E.

Note. Commutativity is necessary in Theorem III.6.7 (it was required when Theorem III.6.6 was used in the proof). This can also be shown explicitly by considering the polynomial $x^2 + 1$ over the (noncommutative) division ring of the real quaternions; see the supplement on Quaternions—An Algebraic View. Polynomial $x^2 + 1$ has an infinite number of roots here, including $\pm i$, $\pm j$, and $\pm k$. In fact, the roots are $\{x_1 i + x_2 j + x_3 k \mid x_1^2 + x_2^2 + x_3^2 = 1\}$.

Note. When looking for roots of a polynomial, the following result gives some candidates to consider for "root-hood."

Proposition III.6.8. Let D be a unique factorization domain with quotient field F (that is, F is the field of quotients produced from D) and let $f = \sum_{i=0}^{n} a_i x^i \in D[x]$. If $u = c/d \in F$ with c and d relatively prime (so u is in "reduced form"), and u is a root of f, then c divides a_0 and d divides a_n.

Example. We use Hungerford's example to illustrate the use of Proposition III.6.8 to search for rational roots of a polynomial in $\mathbb{Q}[x]$. See page 215 of Fraleigh (7th Edition) for a similar application (Corollary 23.12 and Example 23.14). Consider $f = x^4 - 2x^3 - 7x^2 - (11/3)x - 4/3 \in \mathbb{Q}[x]$. Then f has exactly the same roots as $3f = 3x^4 - 6x^3 - 21x^2 - 11x - 4 \in \mathbb{Z}[x]$. By Proposition III.6.8, a rational root of $3f$ must have a numerator dividing 4 and a denominator dividing 3. So the candidate rational roots are ± 1, ± 2, ± 4, $\pm 1/3$, $\pm 2/3$, and $\pm 4/3$. We find that only 4 is actually a root. Notice that we can then factor $3f$ into $q(x)(x-4)$ by the Factor Theorem (Theorem III.6.6) and we know that the third degree polynomial $q(x)$ has no zeros in $\mathbb{Q}$ and hence is irreducible in $\mathbb{Q}[x]$.

Note. Let D be an integral domain and $f \in D[x]$. If $c \in D$ and c is a root of f then repeated application of the Factor Theorem (Theorem III.6.6) and Theorem III.6.7 (even though we are not considering distinct roots here) we see that there is a greatest nonnegative integer m (where $0 \leq m \leq \deg(f)$) such that $f(x) = (x-c)^m g(x)$ for some $g(x) \in D[x]$ where $(x-c) \nmid g(x)$ (or equivalently by the Factor Theorem, $g(c) \neq 0$).

Definition. For integral domain D and $f \in D[x]$, the nonnegative integer m described in the previous note is the *multiplicity* of the root c of f. If $m = 1$ then c is a *simple root*. If $m > 1$ then c is a multiple root.

Note. In order to explore multiple roots we introduce the "formal derivative" of a polynomial. You might recall that for analytic function $f(x) = \sum_{i=0}^{\infty} a_n x^i$ (say $f : \mathbb{C} \to \mathbb{C}$) then $x = c$ is a zero of multiplicity m if $f(c) = f'(c) = f''(c) = \cdots = f^{(m)}(c) = 0$ and $f^{(m+1)}(c) \neq 0$. See Corollary IV.3.9 of my Complex Analysis 1 (MATH 5510) notes on Section IV.3. Zeros of an Analytic Function.

Definition. Let D be an integral domain and $f = \sum_{i=0}^{n} a_i x^i \in D[x]$. Then define the *formal derivative* of f as $\sum_{i=1}^{n} i a_i x^{i-1}$ and denote it as f'.

Note. Since this is an algebra course, we have no concept of distance (or "metric" or even "topology") so we will not deal with limits. None-the-less, we can symbolically define f'. The following result is familiar, but it must be established algebraically here!

Lemma III.6.9. Let D be an integral domain $f, g \in D[x]$. Then the formal derivatives f' and g' satisfy:

(i) $(cf)' = cf'$ for all $c \in D$;

(ii) $(f + g)' = f' + g'$;

(iii) $(fg)' = f'g + fg'$;

(iv) $(g^n)' = ng^{n-1}g'$ for all $n \in \mathbb{N}$.

Note. Definition III.3.3 defined an irreducible element of a commutative ring with identity. When applied to a nonzero polynomial $f \in R[x]$, where R is commutative with identity, this gives that "f is irreducible" means that f is not a unit and for $f = gh$ we have that either g or h is a unit in $R[x]$ (and so either g or h is a constant polynomial where the constant is a unit in R).

Theorem III.6.10. Let D be an integral domain which is a subring of an integral domain E. Let $f \in D[x]$ and $c \in E$.

(i) c is a multiple root of f if and only if $f(c) = 0$ and $f'(c) = 0$.

(ii) If D is a field and f is relatively prime to f', then f has no multiple roots in E.

(iii) If D is a field, f is irreducible in $D[x]$ and E contains a root of f, then f has no multiple roots in E if and only if $f' \neq 0$ (here, "$f' \neq 0$" means that f' is not the zero polynomial in $D[x]$).

Note. We close this section by considering the irreducible elements of $D[x]$ where D is an integral domain. The rest of the lemmas and theorems of this section concern the case where D is a UFD. Some easily established results are:

(i) The units in $D[x]$ are precisely the constant polynomials that are units in D (as shown in Corollary III.6.4 for D a field).

(ii) If $c \in D$ and c is irreducible in D then the constant polynomial c is irreducible in $D[x]$ (this follows from Theorem III.6.1 and part (i)).

(iii) Every first degree polynomial whose leading coefficient is a unit in D is irreducible in $D[x]$. In particular, every first degree polynomial over a field is irreducible.

(iv) Suppose D is a subring of an integral domain E and $f \in D[x] \subset E[x]$. Then f may be irreducible in $E[x]$ but not in $D[x]$ and vice versa (see the following example).

Example. $2x + 2 = 2(x + 1)$ is irreducible in $\mathbb{Q}[x] = E[x]$ by (iii) above. However $2x + 2 = 2(x + 1)$ is reducible in $\mathbb{Z}[x] = D[x]$ since neither 2 nor $x + 1$ is a unit in $\mathbb{Z}$ (from (i) above). So $f = 2x + 2$ is irreducible in $E[x]$ but not in $D[x]$ where $D[x] \subset E[x]$, illustrating (iv) above. Next, $x^2 + 1$ is irreducible in $\mathbb{R}[x] = D[x]$ (by the Factor Theorem) but is reducible in $\mathbb{C}[x] = E[x]$ as $(x + i)(x - i)$ (notice by (i) above that neither $x + i$ nor $x - i$ is a unit in $\mathbb{C}[x]$). So $x^2 + 1$ is irreducible in $D[x]$ but not in $E[x]$, illustrating (iv) above (the "vice versa" part).

Definition. Let D be a UFD and $f = \sum_{i=0}^{m} a_i x^i$ a nonzero polynomial in $D[x]$. A greatest common divisor of $a_0, a_1, \ldots, a_n$ (which exists by Theorem III.3.11(iii)) is a *content* of f.

Note. Since greatest common divisors are not unique, a given nonzero $f \in D[x]$ can have multiple contents. But any two contents of f are necessarily associates and any associates of a content of f is also a content of f (see the comment on page 140 after Definition III.3.10, and page 6 of these class notes for Section III.3). We write $b \approx c$ if b and c are associates. Then $\approx$ is an equivalence relation on D and since D is an integral domain then $b \approx c$ if and only if $b = cu$ for some unit $u \in D$ (by Theorem III.3.2(vi)).

Definition. Denote the equivalence class of the contents of $f \in D[x]$ where D is a UFD as $C(f)$. If $C(f)$ is a unit in D (i.e., $C(f)$ consists of units in D) then f is *primitive*.

Note. Any polynomial $g \in D[x]$ can be written as $g = C(g)g_1$ where g_1 is primitive.

Lemma III.6.11. (Gauss) If D is a unique factorization domain and $f, g \in D[x]$, then $C(fg) = C(f)C(g)$. In particular, the product of primitive polynomials is primitive.

Lemma III.6.12. Let D be a unique factorization domain with quotient field F and let f and g be primitive polynomials in $D[x]$. Then f and g are associates in $D[x]$ if and only if they are associates in $F[x]$.

Lemma III.6.13. Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.

Note. The following result shows that unique factorization extends from D to the ring of polynomials $D[x]$.

Theorem III.6.14. If D is a unique factorization domain, then so is the polynomial ring $D[x_1, x_2, \ldots, x_n]$.

Theorem III.6.15. **(Eisenstein's Criterion)** Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \;\; p | a_i \text{ for } i = 0, 1, \ldots, n-1; \;\; p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Example. If $f = 2x^5 - 6x^4 + 9x^3 - 15 \in \mathbb{Z}[x]$, then with $p = 3$ we have $a_5 = 2 \not\equiv 0 \pmod 3$, $a_4 \equiv a_3 \equiv a_2 \equiv a_1 \equiv a_0 \equiv 0 \pmod 3$, and $a_0 = -15 \not\equiv 0 \pmod 9$. So by the Eisenstein Criterion, f is irreducible in $\mathbb{Q}[x]$.