the greatest common divisor of the coefficients of $p(x)$, so that $p(x) = dp'(x)$, where the g.c.d. of the coefficients of $p'(x)$ is 1. Such a factorization of $p(x)$ is unique up to a change in d (so up to a unit in R), and since d can be factored uniquely into irreducibles in R (and these are also irreducibles in the larger ring $R[x]$), it suffices to prove that $p'(x)$ can be factored uniquely into irreducibles in $R[x]$. Thus we may assume that the greatest common divisor of the coefficients of $p(x)$ is 1. We may further assume $p(x)$ is not a unit in $R[x]$, i.e., degree $p(x) > 0$.

Since $F[x]$ is a Unique Factorization Domain, $p(x)$ can be factored uniquely into irreducibles in $F[x]$. By Gauss' Lemma, such a factorization implies there is a factorization of $p(x)$ in $R[x]$ whose factors are F-multiples of the factors in $F[x]$. Since the greatest common divisor of the coefficients of $p(x)$ is 1, the g.c.d. of the coefficients in each of these factors in $R[x]$ must be 1. By Corollary 6, each of these factors is an irreducible in $R[x]$. This shows that $p(x)$ can be written as a finite product of irreducibles in $R[x]$.

The uniqueness of the factorization of $p(x)$ follows from the uniqueness in $F[x]$. Suppose

$$p(x) = q_1(x) \cdots q_r(x) = q_1'(x) \cdots q_s'(x)$$

are two factorizations of $p(x)$ into irreducibles in $R[x]$. Since the g.c.d. of the coefficients of $p(x)$ is 1, the same is true for each of the irreducible factors above — in particular, each has positive degree. By Corollary 6, each $q_i(x)$ and $q_j'(x)$ is an irreducible in $F[x]$. By unique factorization in $F[x]$, $r = s$ and, possibly after rearrangement, $q_i(x)$ and $q_i'(x)$ are associates in $F[x]$ for all $i \in \{1, \ldots, r\}$. It remains to show they are associates in $R[x]$. Since the units of $F[x]$ are precisely the elements of $F^\times$ we need to consider when $q(x) = \frac{a}{b}q'(x)$ for some $q(x), q'(x) \in R[x]$ and nonzero elements a, b of R, where the greatest common divisor of the coefficients of each of $q(x)$ and $q'(x)$ is 1. In this case $bq(x) = aq'(x)$; the g.c.d. of the coefficients on the left hand side is b and on the right hand side is a. Since in a Unique Factorization Domain the g.c.d. of the coefficients of a nonzero polynomial is unique up to units, $a = ub$ for some unit u in R. Thus $q(x) = uq'(x)$ and so $q(x)$ and $q'(x)$ are associates in R as well. This completes the proof.

Corollary 8. If R is a Unique Factorization Domain, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a Unique Factorization Domain.

Proof: For finitely many variables, this follows by induction from Theorem 7, since a polynomial ring in n variables can be considered as a polynomial ring in one variable with coefficients in a polynomial ring in $n-1$ variables. The general case follows from the definition of a polynomial ring in an arbitrary number of variables as the union of polynomial rings in finitely many variables.

Examples

(1) $\mathbb{Z}[x]$, $\mathbb{Z}[x, y]$, etc. are Unique Factorization Domains. The ring $\mathbb{Z}[x]$ gives an example of a Unique Factorization Domain that is not a Principal Ideal Domain.

(2) Similarly, $\mathbb{Q}[x]$, $\mathbb{Q}[x, y]$, etc. are Unique Factorization Domains.

We saw earlier that if R is a Unique Factorization Domain with field of fractions F and $p(x) \in R[x]$, then we can factor out the greatest common divisor d of the coefficients of $p(x)$ to obtain $p(x) = dp'(x)$, where $p'(x)$ is irreducible in both $R[x]$ and $F[x]$. Suppose now that R is an *arbitrary* integral domain with field of fractions F. In R the notion of greatest common divisor may not make sense, however one might still ask if, say, a *monic* polynomial which is irreducible in $R[x]$ is still irreducible in $F[x]$ (i.e., whether the last statement in Corollary 6 is true).

Note first that if a monic polynomial $p(x)$ is reducible, it must have a factorization $p(x) = a(x)b(x)$ in $R[x]$ with both $a(x)$ and $b(x)$ *monic, nonconstant* polynomials (recall that the leading term of $p(x)$ is the product of the leading terms of the factors, so the leading coefficients of both $a(x)$ and $b(x)$ are units — we can thus arrange these to be 1). In other words, a nonconstant *monic* polynomial $p(x)$ is irreducible if and only if it cannot be factored as a product of two *monic* polynomials of smaller degree.

We now see that it is not true that if R is an arbitrary integral domain and $p(x)$ is a monic irreducible polynomial in $R[x]$, then $p(x)$ is irreducible in $F[x]$. For example, let $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$ (a subring of the complex numbers) and let $p(x) = x^2+1$. Then the fraction field of R is $F = \{a+bi \mid a, b \in \mathbb{Q}\}$. The polynomial $p(x)$ factors uniquely into a product of two linear factors in $F[x]$: $x^2+1 = (x-i)(x+i)$ so in particular, $p(x)$ *is reducible in* $F[x]$. Neither of these factors lies in $R[x]$ (because $i \notin R$) so $p(x)$ *is irreducible in* $R[x]$. In particular, by Corollary 6, $\mathbb{Z}[2i]$ *is not a Unique Factorization Domain.*

EXERCISES

1. Let R be an integral domain with quotient field F and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$. Prove that if $a(x) \notin R[x]$ then R is not a Unique Factorization Domain. Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a U.F.D.
2. Prove that if $f(x)$ and $g(x)$ are polynomials with rational coefficients whose product $f(x)g(x)$ has integer coefficients, then the product of any coefficient of $g(x)$ with any coefficient of $f(x)$ is an integer.
3. Let F be a field. Prove that the set R of polynomials in $F[x]$ whose coefficient of x is equal to 0 is a subring of $F[x]$ and that R is not a U.F.D. [Show that $x^6 = (x^2)^3 = (x^3)^2$ gives two distinct factorizations of x^6 into irreducibles.]
4. Let $R = \mathbb{Z}+x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.
   (a) Prove that R is an integral domain and its units are ± 1.
   (b) Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. Prove that these irreducibles are prime in R.
   (c) Show that x cannot be written as the product of irreducibles in R (in particular, x is not irreducible) and conclude that R is not a U.F.D.
   (d) Show that x is not a prime in R and describe the quotient ring $R/(x)$.
5. Let $R = \mathbb{Z}+x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the ring considered in the previous exercise.
   (a) Suppose that $f(x), g(x) \in \mathbb{Q}[x]$ are two nonzero polynomials with rational coefficients and that x^r is the largest power of x dividing both $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$, (i.e., r is the degree of the lowest order term appearing in either $f(x)$ or $g(x)$). Let f_r and

g_r be the coefficients of x^r in $f(x)$ and $g(x)$, respectively (one of which is nonzero by definition of r). Then $\mathbb{Z}f_r + \mathbb{Z}g_r = \mathbb{Z}d_r$ for some nonzero $d_r \in \mathbb{Q}$ (cf. Exercise 14 in Section 2.4). Prove that there is a polynomial $d(x) \in \mathbb{Q}[x]$ that is a g.c.d. of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$ and whose term of minimal degree is $d_r x^r$.

(b) Prove that $f(x) = d(x)q_1(x)$ and $g(x) = d(x)q_2(x)$ where $q_1(x)$ and $q_2(x)$ are elements of the subring R of $\mathbb{Q}[x]$.

(c) Prove that $d(x) = a(x)f(x) + b(x)g(x)$ for polynomials $a(x), b(x)$ in R. [The existence of $a(x), b(x)$ in the Euclidean Domain $\mathbb{Q}[x]$ is immediate. Use Exercise 11 in Section 2 to show that $a(x)$ and $b(x)$ can be chosen to lie in R.]

(d) Conclude from (a) and (b) that $Rf(x) + Rg(x) = Rd(x)$ in $\mathbb{Q}[x]$ and use this to prove that R is a Bezout Domain (cf. Exercise 7 in Section 8.2).

(e) Show that (d), the results of the previous exercise, and Exercise 11 of Section 8.3 imply that R must contain ideals that are not principal (hence not finitely generated). Prove that in fact $I = x\mathbb{Q}[x]$ is an ideal of R that is not finitely generated.

9.4 IRREDUCIBILITY CRITERIA

If R is a Unique Factorization Domain, then by Corollary 8 a polynomial ring in any number of variables with coefficients in R is also a Unique Factorization Domain. It is of interest then to determine the irreducible elements in such a polynomial ring, particularly in the ring $R[x]$. In the one-variable case, a nonconstant monic polynomial is irreducible in $R[x]$ if it cannot be factored as the product of two other polynomials of smaller degrees. Determining whether a polynomial has factors is frequently difficult to check, particularly for polynomials of large degree in several variables. The purpose of irreducibility criteria is to give an easier mechanism for determining when some types of polynomials are irreducible.

For the most part we restrict attention to polynomials in one variable where the coefficient ring is a Unique Factorization Domain. By Gauss' Lemma it suffices to consider factorizations in $F[x]$ where F is the field of fractions of R (although we shall occasionally consider questions of irreducibility when the coefficient ring is just an integral domain). The next proposition considers when there is a factor of degree one (a *linear* factor).

Proposition 9. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, i.e., there is an $\alpha \in F$ with $p(\alpha) = 0$.

Proof: If $p(x)$ has a factor of degree one, then since F is a field, we may assume the factor is monic, i.e., is of the form $(x - \alpha)$ for some $\alpha \in F$. But then $p(\alpha) = 0$. Conversely, suppose $p(\alpha) = 0$. By the Division Algorithm in $F[x]$ we may write

$$p(x) = q(x)(x - \alpha) + r$$

where r is a constant. Since $p(\alpha) = 0$, r must be 0, hence $p(x)$ has $(x - \alpha)$ as a factor.

Proposition 9 gives a criterion for irreducibility for polynomials of small degree: