If R Is a Unique Factorization Domain $R[X]$ Is also.

11/30/06 Radford

Throughout R is an integral domain.

1 Irreducible Constant Polynomials

Let $a \in R[X]$ be a non-zero constant polynomial. If $a = p(X)q(X)$, where $p(X), q(X) \in R[X]$, then $p(X), q(X) \neq 0$ and the calculation $0 = \operatorname{Deg} a = \operatorname{Deg} p(X) + \operatorname{Deg} q(X)$ means that $p(X), q(X)$ are constant polynomials as well. Since $R[X]^\times = R^\times$:

Lemma 1 *Let $a \in R$. Then the following are equivalent:*

(1) *a is an irreducible element of R.*

(2) *a is an irreducible element of $R[X]$.*

□

2 Primitive Polynomials

Let $p(X) = a_0 + \cdots + a_n X^n \in R[X]$. Note that the units of R divide the coefficients $a_0, \ldots, a_n$ of $p(X)$. We say $p(X)$ is *primitive* if the only divisors of $a_0, \ldots, a_n$ are the units of R. Thus the constant primitive polynomials of $R[X]$ are the units of R. If a_i is a unit for some $0 \leq i \leq n$ then $p(X)$ is primitive. Consequently the monic polynomials of $R[X]$ are primitive.

Suppose that $d \in R$ divides all of the coefficients $a_0, \ldots, a_n$ of $p(X)$. Then there are $a'_0, \ldots, a'_n \in R$ such that $a_i = da'_i$ for all $0 \leq i \leq n$. Set

$p'(X) = a'_0 + \cdots + a'_n X^n$. Then $p(X) = dp'(X)$. Note that any $d \in R$ divides all of the coefficients of $dp(X)$.

The primitive polynomials include irreducible polynomials of positive degree.

Lemma 2 *Let $p(X) \in R[X]$ be irreducible and have positive degree. Then $p(X)$ is primitive.*

PROOF: Suppose that $p(X)$ is irreducible, has positive degree, and $d \in R$ divides all of the coefficients of $p(X)$. Then $p(X) = dp'(X)$ for some $p'(X) \in R[X]$. Since $p(X)$ is irreducible the either d or $p'(X)$ is a unit. But $\operatorname{Deg} p'(X) = \operatorname{Deg} p(X) > 0$ means that $p'(X)$ is not a unit. Therefore d is a unit. $\square$

As a partial converse, primitive polynomials of degree one are irreducible.

Lemma 3 *Let $p(X), q(X), r(X) \in R[X]$, where $p(X)$ is primitive. Then:*

(1) *If $p(X) = q(X)r(X)$ then $q(X), r(X)$ are primitive.*

(2) *If $\operatorname{Deg} p(X) = 1$ then $p(X)$ is irreducible.*

(3) *Suppose that $q(X), r(X)$ are primitive. Then no prime of R divides all of the coefficients of $p(X)$.*

PROOF: Suppose $p(X) = q(X)r(X)$. Since $q(X)r(X) = r(X)q(X)$, to establish part (1) it suffices to show that the first factor $q(X)$ of $p(X)$ is primitive.

Let $d \in R$ divide all of the coefficients of $q(X)$. Then $q(X) = dq'(X)$ for some $q'(X) \in R[X]$ which means $p(X) = dq'(X)r(X)$. Therefore d divides all of the coefficients of $p(X)$; hence d is a unit since $p(X)$ is primitive.

To show part (2), suppose $\operatorname{Deg} p(X) = 1$ and $p(X) = q(X)r(X)$, where $q(X), r(X) \in R[X]$. Since $\operatorname{Deg} p(X) = 1$, one of $q(X)$, $r(X)$ is a constant polynomial, and primitive by part (1). Thus one of $q(X)$, $r(X)$ is a unit. Therefore $p(X)$ is irreducible.

To show part (3), let $p \in R$ be prime. Then $(p) = Rp$ is a prime ideal of R. Thus R/Rp, and hence $(R/Rp)[X]$, is an integral domain. The projection $R \longrightarrow R/Rp$ given by $r \mapsto r + Rp$ is a ring homomorphism and thus induces a ring homomorphism $R[X] \longrightarrow (R/Rp)[X]$ given by

$$f(X) = a_0 + \cdots + a_n X^n \mapsto (a_0 + Rp) + \cdots + (a_n + Rp)X^n = \overline{f(X)}.$$

Suppose that $f(X)$ is primitive. Since p is not a unit p does not divide a_i, or equivalently $a_i + Rp \neq 0$, for some $0 \leq i \leq n$. Thus $\overline{f(X)} \neq 0$.

Assume $q(X), r(X)$ are primitive. Then $\overline{q(X)r(X)} \neq 0$ since $\overline{q(X)r(X)} = \overline{q(X)}\ \overline{r(X)}$ is the product of two non-zero elements in an integral domain. Therefore p does not divide one of the coefficients of $q(X)r(X)$. $\Box$

Let $p(X)$ be primitive and have positive degree. Suppose that $p(X)$ is not irreducible. Then $p(X) = q(X)r(X)$ where neither one of $q(X), r(X) \in R[X]$ is a unit. By part (1) of Lemma 3 both $q(X)$ and $r(X)$ are primitive. This means neither $q(X)$ nor $r(X)$ is a constant polynomial since constant primitive polynomials are units. Thus $q(X)$ and $r(X)$ are primitive and have positive degree. Since $\operatorname{Deg} p(X) = \operatorname{Deg} q(X) + \operatorname{Deg} r(X)$ we conclude that $\operatorname{Deg} q(X), \operatorname{Deg} r(X) < \operatorname{Deg} p(X)$. By induction on $\operatorname{Deg} p(X)$ we have:

Proposition 1 *Every primitive polynomial of positive degree in $R[X]$ is the product of (primitive) irreducible polynomials of positive degree in $R[X]$.* $\Box$

Let F be the field of quotients of R. Then we may regard R as a subring with unity of F. Therefore we may regard $R[X]$ as a subring of $F[X]$, which is a Euclidean domain and hence a Unique Factorization Domain. Recall that irreducible polynomials of positive degree in $R[X]$ are primitive.

Lemma 4 *Let $p(X) \in R[X]$ be primitive of positive degree. If $p(X)$ is an irreducible polynomial of $F[X]$ then $p(X)$ is an irreducible polynomial of $R[X]$.*

PROOF: Suppose $p(X)$ is an irreducible polynomial of $F[X]$ and $p(X) = q(X)r(X)$, where $q(X), r(X) \in R[X]$. Since $p(X)$ is an irreducible polynomial of $F[X]$ necessarily one of $q(X), r(X)$ is a unit of F, that is $\operatorname{Deg} q(X) = 0$ or $\operatorname{Deg} r(X) = 0$. Thus $q(X)$ or $r(X)$ is a constant polynomial of $R[X]$ and hence is a unit of R since $p(X)$ is primitive. $\Box$

Exercise 1 Here is a more straight forward way of proving part (3) of Lemma 3. Suppose that $q(X) = a_0 + \cdots + a_m X^m$ and $r(X) = b_0 + \cdots + b_n X^n$ are *any* polynomials in $R[X]$ and $p \in R$ is a prime which does not divide all of the coefficients of $q(X), r(X)$.

(1) Show that there is an $0 \leq m' \leq m$ such that p divides a_ℓ for $0 \leq \ell < m'$ and p does not divide $a_{m'}$.

(2) Show that there is an $0 \leq n' \leq n$ such that p divides a_ℓ for $0 \leq \ell < n'$ and p does not divide $a_{n'}$.

(3) Write $q(X)r(X) = c_0 + \cdots c_{m+n}X^{m+n}$. Show that d does not divide $c_{m'+n'}$. [Hint: If p does not divide $a_u b_v$ then $u \geq m'$ and $v \geq n'$.]

3 The Special Case when R Is a Unique Factorization Domain

Throughout this section R is a Unique Factorization Domain unless otherwise specified. In any case F denotes the field of quotients of R.

Suppose that $f(X) = a_0 + \cdots + a_n X^n \in R[X]$ is a non-zero non-unit. Let d be a greatest common divisor of $a_0, \ldots, a_n$. Let $a'_0, \ldots, a'_n \in R$ satisfy $da'_i = a_i$ for all $0 \leq i \leq n$. Set $p(X) = a'_0 + \cdots + a'_n X^n$. Then $f(X) = dp(X)$. Now $p(X)$ is primitive since 1 is a greatest common divisor of $a'_0, \ldots, a'_n$. The reader is referred to Exercise 2 for details about greatest common divisors in R.

When d is not a unit of R then d is a product of irreducibles in $R[X]$; see Lemma 1. By Proposition 1 it follows that $p(X)$ is a product of irreducibles of $R[X]$ when $p(X)$ has positive degree. Therefore $f(X)$ is a product of irreducibles. Uniqueness of factorization is the issue. Part (4) of the following is in essence the Gauss Lemma.

Proposition 2 *Let $p(X), q(X) \in R[X]$ be primitive. Then:*

(1) *$p(X)q(X)$ is primitive.*

(2) *Suppose that $a, b \in R$ are not zero and $ap(X) = bq(X)$. Then a, b are associates; hence $p(X), q(X)$ are associates.*

(3) *Every non-zero $f(X) \in R[X]$ has a factorization $f(X) = ag(X)$ unique up to associates, where $a \in R$ and $g(X) \in R[X]$ is primitive.*

(4) *If $p(X)$ is an irreducible polynomial of $R[X]$ then $p(X)$ is an irreducible polynomial of $F[X]$.*

(5) *If $p(X), q(X)$ are associates in $F[X]$ then $p(X), q(X)$ are associates in $R[X]$.*

PROOF: No prime in R divides all of the coefficients of $p(X)q(X)$ by part (3) of Lemma 3. Since the irreducibles of R are the primes of R, no element of R which is a non-zero non-unit divides all of the coefficients of $p(X)q(X)$. Therefore this product is primitive. We have shown part (1).

Assume the hypothesis of part (2). Since $p(X)$ is primitive, 1 is a greatest common divisor of all of its coefficients. There $a1$ is the greatest common divisor of the coefficients of $ap(X)$ as is $b1$ since $q(X)$ is primitive and $ap(X) = bq(X)$. Therefore a, b are associates.

Write $b = ua$, where $u \in R^{\times}$. Then $ap(X) = auq(X)$ from which $p(X) = uq(X)$ follows by cancellation. Thus $p(X), q(X)$ are associates and the proof of part (2) is complete. Part (3) follows by the comments preceding the statement of the proposition and part (2).

Suppose that $p(X)$ is irreducible as a polynomial of $R[X]$ and let $p(X) = q(X)r(X)$, where $q(X)r(X) \in F[X]$. Clearing denominators and using part (3), we see there are non-zero $a, a', b, b' \in R$ such that $ap(X), bq(X) \in R[X]$ and $ap(X) = a'p'(X), bq(X) = b'q'(X)$, where $p'(X), q'(X) \in R[X]$ are primitive. Therefore

$$abp(X) = a'b'p'(X)q'(X).$$

Since $p'(X)q'(X)$ is primitive by part (1) it follows that $p(X), p'(X)q'(X)$ are associates by part (2). Thus $p(X) = up'(X)q'(X)$ for some $u \in R^{\times}$. Since $p(X)$ is an irreducible polynomial of $R[X]$, either $\operatorname{Deg} q(X) = \operatorname{Deg} q'(X) = 0$ or $\operatorname{Deg} r(X) = \operatorname{Deg} r'(X) = 0$. Therefore $p(X)$ is an irreducible polynomial of $F[X]$. We have established part (4).

Suppose that $p(X), q(X)$ are associates in $F[X]$. Then $q(X) = (a/b)p(X)$ for some quotient non-zero $a/b \in F$. Thus $a, b \neq 0$ and $bq(X) = ap(X)$. Part (5) now follows by part (2). $\square$

Theorem 1 *Let R be an integral domain. Then R is a unique factorization domain if and only if $R[X]$ is also.*

PROOF: Suppose that $R[X]$ is a Unique Factorization Domain. Since $R[X]^{\times} = R^{\times}$ by Lemma 1 it follows that R is a Unique Factorization Domain.

Conversely, suppose that R is a Unique Factorization Domain. Since F is a field $\mathcal{R} = F[X]$ is a Unique Factorization Domain as well. Let $f(X) \in R[X]$ be a non-zero non-unit. We have noted that $f(X)$ has a factorization into irreducibles. We need to show uniqueness.

Consider a factorization of $f(X)$ into irreducibles. By rearranging the factors if necessary we may write the factorization

$$f(X) = m_1 \cdots m_r p_1(X) \cdots p_s(X)$$

where $m_i \in R$ for all $1 \le i \le r$ and $p_j(X) \in R[X]$ has positive degree for all $1 \le j \le s$. By part (4) of Proposition 2 the $p_j(X)$'s are irreducible elements of $\mathcal{R}$. Let $a = m_1 \cdots m_r$ and $p(X) = p_1(X) \cdots p_s(X)$. If there are no factors in R, that is if $r = 0$, we set $a = 1$. If there are no factors of positive degree, that is if $s = 0$, we set $p(X) = 1$. In any event $f(X) = ap(X)$ and $p(X)$ is primitive by Lemma 2 and part (1) of Proposition 2. Any other factorization of $f(X)$ into irreducibles

$$f(X) = m'_1 \cdots m'_{r'} p'_1(X) \cdots p'_{s}(X)$$

gives a similar decomposition $f(X) = a'p'(X)$. By part (2) of Proposition 2 it follows that that a, a' are associates in R and $p(X), p'(X)$ are associates in $R[X]$; thus $p(X), p'(X)$ are associates in $\mathcal{R}$. This means $(a) = (a')$ and $\big(p(X)\big) = \big(p'(X)\big)$. Our notation is $(b) = Rb$ for all $b \in R$ and $\big(q(X)\big) = \mathcal{R}q(X)$ for all $q(X) \in \mathcal{R}$.

Since R and $\mathcal{R}$ are Unique Factorization Domains it follows that $r = r'$ and $s = s'$, and after possible rearrangement, $(m_i) = (m'_i)$ for all $1 \le i \le r$ and $\big(p_j(X)\big) = \big(p'_j(X)\big)$ for all $1 \le j \le s$. Therefore m_i, m'_i are associates in R, hence in $R[X]$, for all $1 \le i \le r$. Likewise $p_j(X), p'_j(X)$ are associates in $\mathcal{R} = F[X]$, hence in $R[X]$ by part (5) of Proposition 2, for all $1 \le j \le s$. $\square$

Exercise 2 Let R be a Unique Factorization Domain and $a, b \in R$.

(1) Suppose that $a = b = 0$. Show that 0 is *the* greatest common divisor of a and b.

(2) Suppose that a or b is a unit. Show that 1 is *a* greatest common divisor of a and b.

(3) Suppose that at least one of a, b is a non-zero non-unit. Let $(m_1), \ldots, (m_r)$ list the distinct R-maximal ideals which appear as a factor in either (a) or (b). Write

$$(a) = (m_1)^{\alpha_1} \cdots (m_r)^{\alpha_r} \qquad \text{and} \qquad (b) = (m_1)^{\beta_1} \cdots (m_r)^{\beta_r},$$

where $\alpha_i, \beta_i \geq 0$. Show that

$$d = m_1^{\min(\alpha_1, \beta_1)} \cdots m_r^{\min(\alpha_r, \beta_r)}$$

is greatest common divisor of a and b.

(4) Suppose that d is a greatest common divisor of q and b. Show that cd is a greatest common divisor of ca and cb for all $c \in R$.

(5) Let $a_1, \ldots, a_n \in R$ and suppose that d is a greatest common divisor of $a_1, \ldots, a_n$. Show that cd is a greatest common divisor of $ca_1, \ldots, ca_n$ for all $c \in R$. [Hint: When $n > 2$ show that d is a greatest common divisor of d' and a_n, where d' is a greatest common divisor of $a_1, \ldots, a_{n-1}$.]