On Certain Divisibility Property of Polynomials over Integral Domains

Luis F. Cáceres-Duque

Department of Mathematical Sciences, University of Puerto Rico at Mayagüez

P.O. Box 9000 Mayagez, Puerto Rico, 00681,USA

Tel: 1-787-832-4040 ext. /2647/3203 E-mail: luis.caceres1@upr.edu

José A. Vélez-Marulanda (Corresponding author)

Department of Mathematics & Computer Science, Valdosta State University

2072 Nevins Hall, 1500 N. Patterson St, Valdosta, GA, 31698-0040, USA

Tel: 1-229-333-7449 E-mail: javelezmarulanda@valdosta.edu

Received: February 14, 2011 Accepted: February 28, 2011 doi:10.5539/jmr.v3n3p28

Abstract

An integral domain R is a *degree-domain* if for given two polynomials $f(x)$ and $g(x)$ in $R[x]$ such that for all $k \in R$ $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, then $f(x) = 0$ or $\deg f \geq \deg g$. We prove that the ring of integers O_L is a degree-domain, where $\mathbb{Q} \subseteq L$ is a finite Galois extension. Then we study degree-domains that are also unique factorization domains to determine divisibility of polynomials using polynomial evaluations.

Keywords: Degree-domains, Ring of integers, Unique factorization domains, Divisibility properties of polynomials

1. Introduction

All the rings are assumed to be commutative with identity.

Definition 1. An integral domain R is a *degree-domain* if given two polynomials $g(x), f(x) \in R[x]$ such that for all $k \in R$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$ then $f(x) = 0$ or $\deg f \geq \deg g$.

Note that fields cannot be degree-domains.

In Section 2, we prove that $\mathbb{Z}$ is a degree-domain. We also present an example of an integral domain that is neither a field nor a degree-domain. In Section 3, we show that the ring of integers O_L is also a degree-domain, where $\mathbb{Q} \subseteq L$ is a finite Galois extension of fields. In Section 4, we study divisibility of polynomials over degree-domains that are also unique factorization domains. The obtained results allow us to determine non-trivial conditions on polynomials $f(x)$ and $g(x)$ with integer coefficients such that the following statement holds:

$$\text{If } g(n)|f(n) \text{ for all } n \in \mathbb{Z} \text{ with } g(n) \neq 0 \text{ then } g(x)|f(x) \text{ in } \mathbb{Z}[x]. \tag{$*$}$$

Note that the statement $(*)$ does not always hold: let p be a prime number and consider the polynomials $g(x) = p$ and $f(x) = x^p - x$, it follows (from Fermat's Little Theorem) that $g(n)|f(n)$ for all integers n but clearly $g(x) \nmid f(x)$ in $\mathbb{Z}[x]$.

For all $n \geq 0$ consider $p_n(x)$ and $q_n(x)$ defined as follows.

$$\begin{array}{lll} p_0(x) = 1, & p_1(x) = x, & p_{n+1}(x) = 2xp_n(x) - p_{n-1}(x), \\ q_0(x) = 0, & q_1(x) = 1, & q_{n+1}(x) = 2xq_n(x) - q_{n-1}(x). \end{array} \tag{$**$}$$

In (Jones J.P. & Matiyasevich Y.V., 1991, Equation (2.14)) it is proved that if $a \geq 2$ then $p_n(a)|q_{2n}(a)$. Can we say that $p_n(x)|q_{2n}(x)$ as polynomials? Consider the particular case $n = 4$:

$$\begin{aligned} q_8(x) &= -8x + 80x^3 - 192x^5 + 128x^7 \\ &= 8x\left(-1 + 2x^2\right)\left(1 - 8x^2 + 8x^4\right) \\ &= 8x\left(-1 + 2x^2\right)p_4(x) \end{aligned}$$

The above calculations show that $p_4(x)|q_8(x)$. Using the results obtained in Section 4, we prove that indeed $p_n(x)|q_{2n}(x)$ in $\mathbb{Z}[x]$, and hence the polynomials in $(**)$ provide non-trivial examples where the statement $(*)$ holds.

This paper is based on results from the second author M.Sc. thesis (Vélez-Marulanda, J.A., 2005), which was based on results from the first author Ph.D. thesis (Cáceres, L.F., 1998). The latter advised the former in the writing of his thesis.

2. Rings that are degree-domains

Lemma 2. The integral domain $\mathbb{Z}$ is a degree-domain.

Proof. Let $g(x)$ and $f(x)$ be polynomials with integer coefficients such that $f(x) \neq 0$ and $\deg g > \deg f$. If follows that $\lim_{k\to\infty} \frac{f(k)}{g(k)} = 0$. Then there exists $k_0 \in \mathbb{Z}^+$ such that $0 < |f(k_0)| < |g(k_0)|$, which implies that $g(k_0) \nmid f(k_0)$. This argument proves Lemma 2 by contradiction.

Example 3. Let Q be the set consisting of prime numbers p such that $p = 2$ or $p \equiv 1 \mod 4$. Consider the domain $\mathbb{Z}[W]$ where $W = \{1/p : p \in Q\}$. Note that the non-integer elements in $\mathbb{Z}[W]$ are of the form c/d where c and d are relatively prime and p is a prime factor of d if and only if $p \in Q$. Moreover, an element c/d is a unit in $\mathbb{Z}[W]$ if and only if any prime factor of c is an element of Q. To see this, assume that $(c/d)(u/t) = 1$ for some u/t in $\mathbb{Z}[W]$ and let p be a prime factor of c. Since $cu = dt$ and c and d are assumed to be relatively prime then p is a prime factor of t. Since u/t is an element of $\mathbb{Z}[W]$ with u and t relatively prime, then $p \in Q$. Conversely, if c is a product of primes in Q, it is clear that c/d is a unit in $\mathbb{Z}[W]$. Now consider an arbitrary element $a/b \in \mathbb{Z}[W]$ with a and b relatively prime. Look at $g(x) = x^2 + 1$ as a polynomial with coefficients in $\mathbb{Z}[W]$ (note in particular that $g(r) \neq 0$ for all $r \in \mathbb{Z}[W]$). Consider $g(a/b) = (a^2 + b^2)/b^2$, we want to show that $g(a/b)$ is a unit in $\mathbb{Z}[W]$. Observe that if $a^2 + b^2 = 2^k$ for some $k \geq 1$ then $g(a/b)$ is a unit in $\mathbb{Z}[W]$. So assume that $a^2 + b^2 \equiv 0 \mod p$ for some odd prime p. The condition that a and b are relatively prime implies that a or b , say a, is relatively prime to p. Let a' satisfying $aa' \equiv 1 \mod p$. It follows that $1 + (ba')^2 \equiv (aa')^2 + (ba')^2 \equiv 0 \mod p$, which implies that $(ba')^2 \equiv -1 \mod p$ making -1 a quadratic residue of p. Therefore $p \equiv 1 \mod 4$ (see (Burton, D.M., 2002, Theorem 9.2)), and hence $p \in Q$. This argument together with the observation above shows that $g(a/b)$ is a unit in $\mathbb{Z}[W]$. If we consider $f(x) = 1$ as a polynomial with coefficients in $\mathbb{Z}[W]$ then $g(r)|f(r)$ for all $r \in \mathbb{Z}[W]$, but clearly $\deg g > \deg f$. Hence the integral domain $\mathbb{Z}[W]$ is not a degree-domain. It is clear that $\mathbb{Z}[W]$ is not a field.

Proposition 4. Let R be an integral domain. Given polynomials $g(x, y), f(x, y) \in R[x][y]$ such that if $g(x, x^t) \neq 0$ then $g(x, x^t)|f(x, x^t)$ in $R[x]$ for any $t \in \mathbb{Z}^+$ arbitrarily large. Then $f(x, y) = 0$ or $\deg_y f \geq \deg_y g$.

Proof. Let $g(x, y), f(x, y) \in R[x][y]$ and suppose $g(x, x^t)|f(x, x^t)$ for t arbitrarily large. Assume that $f(x, y) \neq 0$ and $n = \deg_y f < \deg_y g = m$ with $f(x, y) = a_n(x)y^n + \cdots + a_1(x)y + a_0(x)$ and $g(x, y) = b_m(x)y^m + \cdots + b_1(x)y + b_0(x)$. Note that in particular we have $a_n(x) \neq 0$. Let $t \in \mathbb{Z}^+$ such that $t > \frac{|\deg a_n - \deg b_m|}{m-n}$ and $g(x, x^t) \neq 0$, and consider $h(x) = f(x, x^t)$ and $l(x) = g(x, x^t)$. Note that $\deg h = \deg a_n + tn$ and $\deg l = \deg b_m + tm$. By hypothesis $g(x, x^t)|f(x, x^t)$, which implies $l(x)|h(x)$. Then either $h(x) = 0$ or $\deg h \geq \deg l$. If $h(x) = 0$ then $a_n(x) = 0$, which contradicts that $a_n(x) \neq 0$. If $\deg h \geq \deg l$ then $t \leq \frac{\deg a_n - \deg b_m}{m-n} \leq \frac{|\deg a_n - \deg b_m|}{m-n}$, which contradicts our choice of t. Therefore $f(x, y) = 0$ or $\deg_y f \geq \deg_y g$.

We have the following direct consequence of Proposition 4.

Corollary 5. Let R be an integral domain. Then the ring of polynomials $R[x]$ is a degree-domain.

Proof. Assume that $R[x]$ is not a degree-domain. Then there exist two polynomials $f(x, y)$ and $g(x, y)$ in $R[x, y]$ such that for all $p(x) \in R[x]$ $(g(x, p(x)) \neq 0 \Rightarrow g(x, p(x))|f(x, p(x)))$ but $f(x, y) \neq 0$ and $\deg_y g > \deg_y f$. Note that the latter implies that $g(x, y) \neq 0$. Let $t \in \mathbb{Z}^+$ sufficiently large such that $g(x, x^t) \neq 0$. Using the assumptions on the polynomials $f(x, y)$ and $g(x, y)$, we obtain that $g(x, x^t)|f(x, x^t)$. It follows from Proposition 4 that $f(x, y) = 0$ or $\deg_y g \leq \deg_y f$, which is a contradiction.

3. Ring of Integers

We review the definition of integral elements.

Let R be a subring of a ring L. An element $\alpha \in L$ is *integral* over R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(\alpha) = 0$. In particular, when $R = \mathbb{Z}$, the element α is said to be an *algebraic integer* in L. It is well-known that the set C consisting of all the elements that are integral over R is a ring which is called the *integral closure* of R in L. In particular, if $R = \mathbb{Z}$ and L is a field containing $\mathbb{Z}$, the integral closure of $\mathbb{Z}$ in L is called the *ring of integers* of L, and we denote this ring by O_L. For example, let d be a square-free integer and consider $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$, the ring of integers in $\mathbb{Q}(\sqrt{d})$ is $O_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ where

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \mod 4 \end{cases}$$

We say that an integral domain R is *integrally closed* if R is equal to its integral closure in its field of fractions. In particular, $\mathbb{Z}$ is integrally closed.

Proposition 6. Let R be an integral domain and K be its field of fractions. Assume that $K \subseteq L$ is a finite Galois extension of fields and let C be the integral closure of R in L. Then $\sigma(C) = C$ for all $\sigma \in \mathrm{Gal}(L/K)$, where $\mathrm{Gal}(L/K)$ denotes the Galois group of the extension $K \subseteq L$. Moreover, if R is integrally closed, then $R = \{b \in C : \sigma(b) = b, \text{ for all } \sigma \in \mathrm{Gal}(L/K)\}$.

For a proof of Proposition 6, see (Lorenzini, D., 1996, Chapter 1, Proposition 2.19 (iv)).

Let R, K, L and C as in the hypotheses of Proposition 6. For all $p(x) = \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0 \in L[x]$ and $\sigma \in \mathrm{Gal}(L/K)$ let $p_\sigma(x) = \sigma(\alpha_n)x^n + \cdots + \sigma(\alpha_1)x + \sigma(\alpha_0)$. Note that $\deg p = \deg p_\sigma$. Moreover, if $p(x) = r(x)s(x)$ with $r(x), s(x) \in L[x]$ then $p_\sigma(x) = r_\sigma(x)s_\sigma(x)$.

Lemma 7. Let R, K, L and C be as in the hypotheses of Proposition 6 with R integrally closed and let $p(x) \in C[x]$.

(i) If $a \in R$ then $p_\sigma(a) = \sigma(p(a))$ for all $\sigma \in \mathrm{Gal}(L/K)$;

(ii) $p(x) = p_\sigma(x)$ for all $\sigma \in \mathrm{Gal}(L/K)$ if and only if $p(x) \in R[x]$.

Proof. Statement (i) follows directly from the fact that $R \subseteq K$. Assume that $p(x) = p_\sigma(x)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Then the coefficients of $p(x)$ are fixed by any element of $\mathrm{Gal}(L/K)$. Since R is integrally closed, the second conclusion in Proposition 6 implies that $p(x) \in R[x]$. Conversely, if $p(x) \in R[x]$ then $p(x) = p_\sigma(x)$ for all $\sigma \in \mathrm{Gal}(L/K)$ since $R \subseteq K$.

Let R, K, L and C be as in the hypotheses of Proposition 6. For all $p(x) \in L[x]$, let $N_{L/K}(p)(x)$ to be the polynomial $\prod_{\sigma\in\mathrm{Gal}(L/K)} p_\sigma(x)$. Note that $\deg N_{L/K}(p) = |\mathrm{Gal}(L/K)| \deg p$ and $N_{L/K}(p)(x) = 0$ if and only if $p(x) = 0$.

Lemma 8. Let R, K, L and C as in the hypotheses of Proposition 6 with R integrally closed and let $p(x) \in C[x]$. Then

(i) $N_{L/K}(p)(x) \in R[x]$;

(ii) $N_{L/K}(p)(a) \in R$ for all $a \in R$;

(iii) $N_{L/K}(p)(a) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(p(a))$ for all $a \in R$.

Proof. Let $q(x) = N_{L/K}(p)(x)$ (note that $q(x) \in C[x]$) and let τ be a fixed element in $\mathrm{Gal}(L/K)$. Then $\tau \circ \sigma \in \mathrm{Gal}(L/K)$ and $(p_\tau)_\sigma(x) = p_{\tau\circ\sigma}(x)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Note that τ induces a permutation of the finite group $\mathrm{Gal}(L/K)$. Then $q_\tau(x) = \prod_{\tau\circ\sigma\in\mathrm{Gal}(L/K)} p_{\tau\circ\sigma}(x) = q(x)$, which implies by Lemma 7(ii) that $q(x) \in R[x]$ proving (i). Note that (ii) is a direct consequence of (i) and the statement (iii) follows from Lemma 7(i).

Proposition 9. Let R, K, L and C as in the hypotheses of Proposition 6 with R integrally closed. If R is a degree-domain then the ring C is also a degree-domain.

Proof. Let $f(x)$ and $g(x)$ be two polynomials in $C[x]$ such that for all $k \in C$ $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. Consider $F(x) = N_{L/K}(f)(x)$ and $G(x) = N_{L/K}(g)(x)$. By Lemma 8(i), $F(x), G(x) \in R[x]$. Let b be an arbitrary element of R such that $G(b) \neq 0$. It follows that $g(b) \neq 0$, and hence $g(b)|f(b)$. Therefore $\sigma(g(b))|\sigma(f(b))$ for all $\sigma \in \mathrm{Gal}(L/K)$. Using properties of divisibility together with Lemma 8(ii) and Lemma 8(iii) we obtain that $G(b) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(g(b))$ divides $F(b) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(f(b))$ in R. Since R is a degree-domain then $F(x) = 0$ or $\deg G \leq \deg F$, which implies that $f(x) = 0$ or $\deg g \leq \deg f$. Therefore the ring C is also a degree-domain.

Since $\mathbb{Z}$ is integrally closed, the following result follows directly from Proposition 9.

Corollary 10. Let $\mathbb{Q} \subseteq L$ be a finite Galois extension. Then the ring of integers O_L is a degree-domain.

4. Degree-domains that are unique factorization domains

Let R be a unique factorization domain. For all $p(x) \in R[x]$ we denote by $C(p)$ the *content* of $p(x)$, i.e., the greatest common divisor of the coefficients of $p(x)$. Remember that $p(x) \in R[x]$ is said to be *primitive* if $C(p)$ is a unit. Gauss Lemma states that the product of two primitive polynomials over a unique factorization domain is also primitive. This implies that if $f(x), g(x)$ and $h(x)$ are polynomials in $R[x]$ with $g(x)$ primitive and $mf(x) = h(x)g(x)$ for some $m \in R$, there exists a polynomial $q(x) \in R[x]$ such that $h(x) = mq(x)$.

Proposition 10. Let R be a unique factorization domain and let K be its field of fractions. The following properties are equivalent.

(i) R is a degree-domain.

(ii) If $f(x), g(x) \in R[x]$ are such that $g(k)|f(k)$ for almost all $k \in R$, then $\frac{f(x)}{g(x)} \in K[x]$.

(iii) If $f(x), g(x) \in R[x]$ with $g(x)$ non-constant and primitive are such that for all $k \in R$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, then $g(x)|f(x)$ in $R[x]$.

Proof. (i) $\Rightarrow$ (ii). Let $g(x), f(x) \in R[x]$ such that for almost all $k \in R$, $g(k)|f(k)$. Let $A = \{k_1, \ldots, k_n\}$ be a finite subset of R such that $g(k)|f(k)$ for all $k \in R - A$. Let $k_1, \ldots, k_s \in A$ such that $g(k_i) \neq 0$ for $i = 1, \ldots, s$ and let $\beta = g(k_1)\cdots g(k_s)$. If $s = 0$, let $\beta = 1$. Consequently, for all $k \in R$ $(g(k) \neq 0 \Rightarrow g(k)|\beta f(k))$. Since R is a degree domain, $\beta f(x) = 0$ or $\deg g \leq \deg \beta f$. If $\beta f(x) = 0$ it follows that $f(x) = 0$, which trivially implies $\frac{f(x)}{g(x)} \in K[x]$. Suppose $\deg g \leq \deg \beta f$ and $g(x) = a_n x^n + \cdots + a_0$. Then there exist $q(x), r(x) \in K[x]$ and $s \in \mathbb{Z}^+$ such that $a_n^s \beta f(x) = g(x)q(x) + r(x)$, with $r(x) = 0$

or $\deg r < \deg g$. Note that if $r(x) = 0$ then $\frac{f(x)}{g(x)} \in K[x]$. Hence, assume that $\deg r < \deg g$ and denote $\alpha = a_n^s\beta$. Thus for all $k \in R$ with $g(k) \neq 0$ we have both $g(k)|\alpha f(k)$ and $g(k)|g(k)q(k)$, which implies $g(k)|r(k)$. Using the hypothesis for the polynomials $g(x)$ and $r(x)$ we obtain $r(x) = 0$ or $\deg r \geq \deg g$. Therefore $r(x) = 0$ and hence $\alpha f(x) = g(x)q(x)$. It follows that $\frac{f(x)}{g(x)} = \alpha^{-1}q(x) \in K[x]$.

(ii) $\Rightarrow$ (iii) Let $f(x), g(x) \in R[x]$ with $g(x)$ non-constant and primitive such that for all $k \in R$ $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. Since $g(x) \neq 0$, it follows that $g(k)|f(k)$ for almost all $k \in R$. By hypothesis we have $\frac{f(x)}{g(x)} = p(x) \in K[x]$. Assume that $p(x) = \frac{r_n}{s_n}x^n + \frac{r_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{r_1}{s_1}x + \frac{r_0}{s_0}$, where $r_i, s_i \in R$, with $s_i \neq 0$ for all $i = 0, \ldots, n$. Let $m = s_0s_1 \cdots s_n$ and consider $h(x) = mp(x) \in R[x]$. We have $mf(x) = mp(x)q(x) = h(x)g(x)$. As $g(x)$ is primitive and $mf(x) \in R[x]$, then there exists $q(x) \in R[x]$ such that $h(x) = mq(x)$. Consequently, $mq(x) = mp(x)$ and $p(x) = q(x) \in R[x]$, which implies $g(x)|f(x)$ in $R[x]$.

(iii) $\Rightarrow$ (i) Let $f(x)$ and $g(x)$ be polynomials in $R[x]$ such that for all $k \in R$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. If $g(x)$ is a constant polynomial and $\deg f < \deg g = 0$ then $f(x) = 0$. Suppose that $\deg g \geq 1$ and let $h(x)$ be a primitive polynomial in $R[x]$ such that $g(x) = C(g)h(x)$. By hypothesis, for all $k \in R$ we have $(h(k) \neq 0 \Rightarrow h(k)|f(k))$, which implies $h(x)|f(x)$ in $R[x]$. It follows that $f(x) = 0$ or $\deg f \geq \deg h = \deg g$. In both cases for $g(x)$ we obtain that $f(x) = 0$ or $\deg g \leq \deg f$. Therefore R is a degree-domain.

The following result, which is a consequence of Proposition 10 together with Lemma 2 provides non-trivial conditions on polynomials $f(x)$ and $g(x)$ such that statement $(*)$ holds.

Corollary 11. Let $f(x), g(x) \in \mathbb{Z}[x]$ with $g(x)$ a non-constant and primitive such that for all $k \in \mathbb{Z}$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. Then $g(x)|f(x)$ in $\mathbb{Z}[x]$.

Example. Let $n \geq 1$ and consider the polynomials $p_n(x), q_n(x)$ in $(**)$. For all $a \geq 2$ we know that $p_n(a)|q_{2n}(a)$; looking at the proof of this in (Jones J.P. & Matiyasevich Y.V., 1991, Equation (2.14)), we see that it can be extended to any $a \in \mathbb{Z}$ with $|a| \geq 2$. Observe also that the polynomials $p_n(x)$ are primitive. Applying Corollary 11 to the polynomials $g(x) = p_n(x)$ and $f(x) = q_{2n}(x)$, we obtain that $p_n(x)|q_{2n}(x)$ in $\mathbb{Z}[x]$.

Acknowledgment

The second author was sponsored by the Reassign Time for Research Scholarship of the Office of Academic Affairs at the Valdosta State University

References

Burton, D.M. (2002). *Elementary Number Theory, Fifth Edition*, McGraw-Hill.

Cáceres, L. F. (1998). *Ultraproducts of Sets and Ideal Theories of Commutative Rings*, Ph.D. Thesis, University of Iowa, Iowa City.

Lorenzini, D. (1996). *An Invitation to Arithmetic Geometry*, Graduate Studies in Mathematics, Volume 9, American Mathematical Society.

Jones J.P. & Matiyasevich, Y.V. (1991). Proof of Recursive Unsolvability of Hilbert's Tenth Problem, *American Math. Monthly*, 8, 689-709.

Vélez-Marulanda, J.A. (2005). *Some divisibility properties in ring of polynomials over unique factorization domains*, M.Sc. Thesis, University of Puerto Rico at Mayagüez.