Revista Colombiana de Matemáticas
Volumen 47(2013)2, páginas 167-179

On the Infinitude of Prime Elements

Acerca de la infinitud de elementos primos

Luis F. Cáceres-Duque[1], José A. Vélez-Marulanda[2,a,✉]

[1]University of Puerto Rico at Mayagüez, Mayagüez, PR, USA

[2]Valdosta State University, Valdosta, GA, USA

The second author dedicates this article to his brother David Armando Vélez and his father José Leví Vélez

Abstract. Let R be an infinite unique factorization domain with at most finitely many units. We discuss the infinitude of prime elements in R when R is arbitrary and when R satisfies the following property: if f and g are polynomials with coefficients in R such that $f(r)$ divides $g(r)$ for all $r \in R$ with $f(r) \neq 0$, then either $g = 0$ or $\deg(f) \leq \deg(g)$.

Key words and phrases. Unique factorization domains, Prime elements.

2010 Mathematics Subject Classification. 11A41, 13G99.

Resumen. Sea R un dominio de factorización única que tiene a lo sumo un número finito de unidades. Nosotros discutimos la infinitud de elementos primos en R cuando R es arbitrario y cuando R satisface la siguiente propiedad: si f y g son polinomios con coeficientes en R tales que $f(r)$ divide $g(r)$ para todo $r \in R$ con $f(r) \neq 0$, entonces $g = 0$ ó grado$(f) \leq$ grado(g).

Palabras y frases clave. Dominios de factorización única, elementos primos.

1. Introduction

Throughout this article, we let R be a fixed integral domain with identity. We denote by $R^\times$ the set of all units of R and by $R[x]$ the ring of all polynomials in the variable x with coefficients in R. Let a and b be arbitrary elements of R. We say that a *divides* b in R and write $a \mid b$, provided that there exits an element c in R such that $b = ac$. We say that a and b are *associate*, provided

[a]Supported by the Release Time for Research Scholarship of the Office of Academic Affairs at the Valdosta State University.

that there exists u in $R^\times$ such that $a = ub$. Let p be an element that is neither zero nor a unit in R. Recall that p is said to be *prime* if for all elements r and s in R such that $p \mid rs$, then either $p \mid r$ or $p \mid s$. We denote by K the field of fractions of R. Recall also that a proper ideal $\mathfrak{p}$ of R is said to be *prime* if for all elements r and s in R such that $rs \in \mathfrak{p}$, then either $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$.

It is a well-known result that if R is infinite with finitely many units, then R has infinitely many prime ideals (see Lemma 2.1). In this article, we provide a proof of the following statement, which gives a modern generalization of Euclid's Theorem on the infinitude of prime integers: if R is an infinite unique factorization domain with finitely many units, then R has infinitely many non-associate prime elements (see Proposition 2.2). Thus, it is reasonable to discuss questions involving the infinitude a prime elements in certain unique factorization domains. In particular, we are interested on discussing infinitude of prime elements in R, provided that R is an infinite unique factorization domain with finitely many units and which is also a D-ring. We say that R is a *D-ring* provided that for two polynomials f and g in $R[x]$ with $f \neq 0$ and with the property that $f(r) \mid g(r)$ for almost all $r \in R$, then the ratio g/f is a polynomial with coefficients in K. These D-rings were introduced by H. Gunji and D.L. McQuillan in [7]. Observe that no field is a D-ring. There are examples of integral domains that are neither fields nor D-rings (see Example 3.3). In particular, there are two proposed (still open) problems concerning D-rings in [12, Problems XII, XIII, pg. 110].

If f is a polynomial with coefficients in R, we denote by $\mathcal{S}(f)$ the set of all prime ideals $\mathfrak{p}$ of R for which there exists $r \in R$ such that $f(r) \in \mathfrak{p}$. We denote by $\mathcal{P}(f)$ the set of all prime elements p of R such that there exists $r_p \in R$ with $f(r_p) \neq 0$ and $p \mid f(r_p)$. Observe that $\mathcal{P}(f) \neq \mathcal{S}(f)$ for all non-constant polynomials f in $R[x]$. If f is a polynomial in $R[x]$ with a root in R, then $\mathcal{S}(f) = \mathrm{Spec}(R)$, where $\mathrm{Spec}(R)$ denotes the set of all prime ideals of R. However, in the same situation, we have that $\mathcal{P}(f)$ is not necessarily the whole set of all prime elements in R. For example, $\mathcal{S}(0) = \mathrm{Spec}(R)$ and $\mathcal{P}(0) = \varnothing$. Observe also that if c is a constant in R, then $S(c)$ is the set of all prime ideals $\mathfrak{p}$ in R for which $c \in \mathfrak{p}$, whereas $\mathcal{P}(c)$ is the set of all prime factors of c in R. In particular, $\mathcal{S}(1) = \varnothing = \mathcal{P}(1)$.

The following result was established by H. Gunji and D. L. McQuillan in [7, Proposition 1] (see also [12, Theorem 8.1]).

Theorem 1.1. *The following statements about R are equivalent.*

(i) R is a D-ring.

(ii) Every polynomial f in $R[x]$ such that $f(r) \in R^\times$ for almost all $r \in R$, must be constant.

(iii) For all non–constant polynomials f in $R[x]$, the set $\mathcal{S}(f)$ is non–empty.

(iv) *For all non–constant polynomials f in $R[x]$ and non–zero constants $c \in R$, the set $\mathcal{S}(f) \smallsetminus \mathcal{S}(c)$ is infinite.*

(v) *For all non–constant polynomials f in $R[x]$, the set $\mathcal{S}(f)$ is infinite.*

In particular, if R is a D-ring then R has infinitely many prime ideals.

In Theorem 3.2(i), we prove that R is a D-ring if and only if R satisfies the following property $(*)$.

$$\text{If } f \text{ and } g \text{ are polynomials in } R[x] \text{ with the property that } f(r) \mid g(r) \text{ for all } r \in R \text{ with } f(r) \neq 0, \text{ then } g = 0 \text{ or } \deg(f) \leq \deg(g). \tag{$*$}$$

We use the property $(*)$ to prove the following result (see Theorem 3.2(ii)): if R is a unique factorization domain then R is a D-ring if and only if for two polynomials f and g in $R[x]$ with f non–constant and primitive, and with the property that $f(r) \mid g(r)$ for all $r \in R$ with $f(r) \neq 0$, then $f \mid g$ in $R[x]$.

For example, the characterization of D-rings by using the property $(*)$ is useful for proving, by contradiction, that the ring of integers $\mathbb{Z}$ is a D-ring as explained in the following argument (cf. [7, Corollary 1, pg. 293]). Assume that f and g are polynomials in $\mathbb{Z}[x]$ with $g \neq 0$ and $\deg(f) > \deg(g)$. Since $\lim_{r\to\infty} \frac{g(r)}{f(r)} = 0$, then there exists $r_0 \in \mathbb{Z}^+$ such that $0 < |g(r_0)| < |f(r_0)|$ and thus $f(r_0) \nmid g(r_0)$. Hence, $\mathbb{Z}$ is a D-ring in the sense of the property $(*)$.

In [4, Proposition 4], the property $(*)$ is used to give an alternative proof of that the ring of integers $\mathcal{O}_L$ of a finite Galois field extension $\mathbb{Q} \subseteq L$ is a D-ring (see Example 3.4 and Example 4, cf. [7, Corollary 1, pg. 293]).

We also prove the following adaptation of Theorem 1.1 that concerns prime elements instead of prime ideals in R.

Theorem 1.2. *Assume that R is an infinite unique factorization domain with finitely many units. The following statements are equivalent.*

(i) *R is a D-ring in the sense of the property $(*)$.*

(ii) *Every polynomial f in $R[x]$, satisfying that $f(r) \in R^\times$ for all $r \in R$ with $f(r) \neq 0$, must be constant.*

(iii) *For all non–constant polynomials f in $R[x]$, the set $\mathcal{P}(f)$ is non–empty.*

(iv) *For all non–constant polynomials f in $R[x]$ and non–zero constants $c \in R$, the set $\mathcal{P}(f) \smallsetminus \mathcal{P}(c)$ is infinite.*

(v) *For all non–constant polynomials f in $R[x]$, the set $\mathcal{P}(f)$ is infinite.*

Observe that by Theorem 1.2(v), there are infinitely many primes p such that the congruence $x^2 + 1 \equiv 0 \pmod{p}$ is solvable, which implies the well-known result that the set of prime numbers p such that $p = 2$ or $p \equiv 1 \pmod{4}$ is infinite (see Example 3.7, cf. [3, Theorem 9.3, Theorem 12.2] and [5, Lemma 8.17]). Therefore, Theorem 1.2 can be used for proving the infinitude of different classes of prime integers (see Example 3.7).

2. The Infinitude of Prime Elements

We denote the *Jacobson radical* of R by $\mathfrak{J}_R$, i.e., $\mathfrak{J}_R$ is the intersection of all maximal ideals of R. Recall that $r \in \mathfrak{J}_R$ if and only if $1 - sr \in R^\times$ for all $s \in R$ (see e.g., [2, Proposition 1.9]). In particular, $1 - r \in R^\times$ for all $r \in \mathfrak{J}_R$. On the other hand, if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals of R and $\mathfrak{a}$ is an ideal of R such that $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$, then there exists $i_0 \in \{1, \ldots, n\}$ such that $\mathfrak{a} \subseteq \mathfrak{p}_{i_0}$ (see e.g., [2, Proposition 1.11(i)]). Recall also that if $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are maximal ideals of R, then $\mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$.

The following well-known result is an exercise in [10, Exercise §1-1.8].

Lemma 2.1. *Assume that R is infinite with finitely many units. Then R has infinitely many maximal ideals. In particular, R has infinitely many prime ideals.*

Proof. Since R is infinite with finitely many units, then R is in particular not a field and therefore, every maximal ideal $\mathfrak{m}$ of R is non-zero. Thus, assume that $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ is a complete list of all maximal ideals of R, let $u_1, \ldots, u_m$ be a complete list of units of R and let x be a non-zero element of R belonging to $\mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{J}_R$. Since $1 - x$ is then a unit in R, it follows that there exists $i \in \{1, \ldots, m\}$ such that $x = 1 - u_i$. We then have in particular that $\mathfrak{J}_R \subseteq \{0, 1 - u_1, \ldots, 1 - u_m\}$, which implies that $\mathfrak{J}_R$ is a finite set. Thus, there exists an integer $k \geq 1$ such that $x^k = 1$. Let $j \in \{1, \ldots, n\}$ be fixed. Since x is an element of $\mathfrak{J}_R$, then x is also an element of $\mathfrak{m}_j$ and therefore $1 = x^k$ is an element of $\mathfrak{m}_j$. This contradicts the assumption that $\mathfrak{m}_j$ is a maximal ideal of R. Hence, R has infinitely many maximal ideals. ☑

Proposition 2.2. *Assume that R is a unique factorization domain with finitely many units and which is not a field.*

(i) If R has at most finitely many non–associate prime elements, then every maximal ideal of R is principal. In particular, if R is also Noetherian, then R is a principal ideal domain.

(ii) If R is infinite, then R has infinitely many non–associate prime elements.

Observe that Proposition 2.2(ii) above follows immediately from Lemma 2.1 provided that R is instead, an infinite principal ideal domain with finitely many units. This case applies to the set of integers $\mathbb{Z}$ but not to $\mathbb{Z}[x]$, for the latter,

being a unique factorization domain, it is not a principal ideal domain (see e.g., [5, §7.4, Example 3]).

Proof of Proposition 2.2.

(i) Assume that R has at most finitely many non–associate prime elements, say $p_1, \ldots, p_n$. Let $\mathfrak{m}$ be a maximal ideal of R and let x be a non-zero element of $\mathfrak{m}$. Since R is a unique factorization domain, then there exists an element $u \in R^\times$ and for all $1 \leq i \leq n$, there exists $s_i \geq 0$ such that

$$x = up_1^{s_1} \cdots p_n^{s_n}.$$

Since $\mathfrak{m}$ is maximal, then x cannot be a unit. Therefore, there exits $i \in \{1, \ldots, n\}$ such that $s_i > 0$, which implies that x is an element of $\langle p_i \rangle$. Hence,

$$\mathfrak{m} \subseteq \langle p_1 \rangle \cup \cdots \cup \langle p_n \rangle.$$

Since for all $1 \leq i \leq n$, the ideal $\langle p_i \rangle$ is prime in R, then there exists $i_0 \in \{1, \ldots, n\}$ such that $\mathfrak{m} \subseteq \langle p_{i_0} \rangle$. The maximality of $\mathfrak{m}$ implies that $\mathfrak{m} = \langle p_{i_0} \rangle$. This proves that every maximal ideal of R is principal. On the other hand, if R is also Noetherian, then it follows from [9, Theorem 12.3] that R is a principal ideal domain.

(ii) Assume now that R is infinite. By Lemma 2.1, R contains infinitely many maximal ideals. Assume that $p_1, \ldots, p_n$ is a complete list of all non–associate prime elements of R. By looking at the proof of (i), we see that the set of all maximal ideals of R is contained in the set $\{\langle p_1 \rangle, \ldots, \langle p_n \rangle\}$, which is finite. Since every subset of a finite set has to be finite, the latter argument contradicts the fact that R has infinitely many maximal ideals. Hence, R contains infinitely many non-associate prime elements. ☑

In particular, it follows from Proposition 2.2(ii) that there are infinitely many non–associate prime elements in $\mathbb{Z}[x]$.

3. D-rings

Recall that R denotes a fixed integral domain with identity and K denotes its field of fractions. Let f be a polynomial in $R[x]$. If R is a unique factorization domain, then we denote the *content* of f by $C(f)$, i.e., $C(f)$ is a greatest common divisor of the coefficients of f, which is unique up to multiplication by a unit in R. Recall that f is said to be *primitive* if $C(f)$ is a unit in R. Recall also that Gauss' Lemma states that the product of two primitive polynomials over a unique factorization domain is also primitive (see e.g., [8, Lemma III.6.11]). If R is a unique factorization domain, then Gauss' Lemma implies that if g and h are also polynomials in $R[x]$ with g primitive such that $mh = fg$ for some $m \in R$, then there exists a polynomial q in $R[x]$ such that $f = mq$.

Definition 3.1. R is said to be a *D-ring* if for two polynomials f and g in $R[x]$ with $f \neq 0$ and with the property that $f(r) \mid g(r)$ for almost all $r \in R$ (i.e., for all r with at most finitely many exceptions), then $\frac{g}{f}$ is a polynomial with coefficients in K.

The following theorem provides alternative characterizations for D-rings.

Theorem 3.2.

(i) The following conditions are equivalent.

- *(a) R is a D-ring.*
- *(b) R satisfies the property $(*)$.*

(ii) If R is also a unique factorization domain, then the following conditions are equivalent.

- *(a) R is a D-ring.*
- *(b) If f and g are polynomials in $R[x]$ with f non–constant and primitive, and with the property that $f(r) \mid g(r)$ for all $r \in R$ with $f(r) \neq 0$, then $f \mid g$ in $R[x]$.*

Proof. (i)(a) $\Rightarrow$ (i)(b) Let f and g be polynomials in $R[x]$ such that for all $r \in R$ with $f(r) \neq 0$ we have $f(r) \mid g(r)$. By hypothesis, $\frac{g}{f}$ is a polynomial with coefficients in K. It follows that there exists a polynomial h in $K[x]$ such that $g = fh$. Assume that $g \neq 0$. Then $h \neq 0$, which in turn implies $\deg(g) = \deg(f) + \deg(h) \geq \deg(f)$. (i)(b) $\Rightarrow$ (i)(a). Let f and g be polynomials in $R[x]$ such that for almost all $r \in R$, $f(r) \mid g(r)$. Let $A = \{r_1, \ldots, r_n\}$ be a finite subset of R such that $f(r) \mid g(r)$ for all $r \in R \setminus A$. Let $s_1, \ldots, s_m \in A$ such that $f(s_i) \neq 0$ for all $i = 1, \ldots, m$ and let $\beta = f(s_1) \cdots f(s_m)$. If $m = 0$, let $\beta = 1$. Therefore, for all $r \in R$ with $f(r) \neq 0$, we have $f(r) \mid \beta g(r)$. By hypothesis, $\beta g = 0$ or $\deg(f) \leq \deg(\beta g)$. If $\beta g = 0$ then $g = 0$, which trivially implies $\frac{g}{f}$ is a polynomial in $K[x]$. Suppose that $\deg(f) \leq \deg(\beta g)$. Since the leading coefficient of f is a unit in K, then by the Division Algorithm (see e.g., [8, Theorem III.6.2]), there exist suitable polynomials q and t in $R[x]$ and a non-zero constant γ in R such that $\gamma\beta g = fq + t$ with $t = 0$ or $\deg(t) < \deg(f)$. Note in particular that if $t = 0$ then $\frac{g}{f} \in K[x]$. Thus, assume that $\deg(t) < \deg(f)$ and let $\alpha = \gamma\beta$. Then for all $r \in R$ with $f(r) \neq 0$ we have $f(r) \mid \alpha g(r)$, which implies that $f(r) \mid t(r)$. By hypothesis, $t = 0$ or $\deg(f) \leq \deg(t)$, which implies that $t = 0$ and therefore $\alpha g = fq$. It follows that $\frac{g}{f} = \alpha^{-1} q \in K[x]$. Hence, R is a D-ring. (ii)(a) $\Rightarrow$ (ii)(b) Let f and g be polynomials in $R[x]$ with f non–constant and primitive and with the property that for all $r \in R$ such that $f(r) \neq 0$, we have $f(r) \mid g(r)$. Since in particular $f \neq 0$, it follows that $f(r) \mid g(r)$ for almost all $r \in R$. By hypothesis, $\frac{g}{f} = p$ is a polynomial in $K[x]$.

Assume then that $p(x) = \frac{s_n}{t_n}x^n + \frac{s_{n-1}}{t_{n-1}}x^{n-1} + \cdots + \frac{s_1}{t_1}x + \frac{s_0}{t_0}$, where $s_i, t_i \in R$, with $t_i \neq 0$ for all $1 \leq i \leq n$. Let $m = t_0 t_1 \cdots t_n$ and consider $h = mp \in R[x]$. We have $mg = mpf = hf$. Since f is primitive and $mg \in R[x]$, it follows from Gauss' Lemma that there exists $q \in R[x]$ such that $h = mq$. Consequently, $mq = mp$ and thus $p = q$, which implies that $f \mid g$ in $R[x]$. (ii)(b) $\Rightarrow$ (ii)(a) Let f and g be polynomials in $R[x]$ such that for all $r \in R$ with $f(r) \neq 0$ we have $f(r) \mid g(r)$. Assume that $g \neq 0$. If f is a constant polynomial, then we trivially get that $\deg(f) \leq \deg(g)$. Assume then that f is a non-constant polynomial and let h be a primitive polynomial in $R[x]$ such that $f = C(f)h$. Therefore, for all $r \in R$ with $h(r) \neq 0$ we have that $h(r) \mid g(r)$ in R. Thus by hypothesis, $h \mid g$ in $R[x]$, which implies that there exists a polynomial p in $R[x]$ such that $g = ph$ and therefore $\deg(f) = \deg(h) \leq \deg(g)$. Hence, using the equivalence (i)(a) $\Leftrightarrow$ (i)(b), we have that R is a D-ring. ☑

We already saw in Section 1 that the ring of integers $\mathbb{Z}$ is a D-ring in the sense of the property $(*)$. In the following example, which is an easy adaptation of [7, Example 1], we present an integral domain that is neither a field nor a D-ring (in the sense of the property $(*)$).

Example 3.3. Let Q be the set consisting of prime numbers p such that $p = 2$ or $p \equiv 1 \pmod 4$. 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 such that p is a prime factor of d if and only if $p \in Q$. Moreover, 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 $a/b \in \mathbb{Z}[W]$, where a and b are relatively prime. Consider $f(x) = x^2 + 1$ as a polynomial with coefficients in $\mathbb{Z}[W]$ and consider $f(a/b) = (a^2 + b^2)/b^2$. Note in particular that $f(r) \neq 0$ for all $r \in \mathbb{Z}[W]$. We want to show that $f(a/b)$ is a unit in $\mathbb{Z}[W]$. Observe that if $a^2 + b^2 = 2^k$ for some $k \geq 1$ then $f(a/b)$ is a unit in $\mathbb{Z}[W]$. So assume that $a^2 + b^2 \equiv 0 \pmod p$ for some odd prime p. Since a and b are relatively prime then a or b, say a, is relatively prime to p. Let a' satisfying $aa' \equiv 1 \pmod p$. It follows that $1 + (ba')^2 \equiv (aa')^2 + (ba')^2 \equiv 0 \pmod p$, which implies that $(ba')^2 \equiv -1 \pmod p$ making -1 a quadratic residue of p. Therefore $p \equiv 1 \pmod 4$ (see [3, Theorem 9.2]), and hence $p \in Q$. Thus, $f(a/b)$ is a unit in $\mathbb{Z}[W]$. If we consider $g(x) = 1$ as a polynomial with coefficients in $\mathbb{Z}[W]$, then $f(r) \mid g(r)$ for all $r \in \mathbb{Z}[W]$, but clearly $\deg(f) > \deg(g)$. Hence, the integral domain $\mathbb{Z}[W]$ is not a D-ring (in the sense of the property $(*)$).

Example 3.4. ([4, Proposition 9], cf. [7, Corollary 1, pg. 293]) Assume that R is a subring of a ring L. Recall that an element $\alpha \in L$ is *integral* over R if there exists a monic polynomial $f \in R[x]$ 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 a well-known result that the set B consisting of all the elements that are integral over R is a ring, which is called the *integral closure* of R in L (see e.g., [2, Corollary 5.3]). 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 $\mathcal{O}_L$. For example, let d be a square-free integer and consider $\mathbb{Q}\big(\sqrt{d}\big) = \big\{a + b\sqrt{d} : a, b \in \mathbb{Q}\big\}$. The ring of integers in $\mathbb{Q}\big(\sqrt{d}\big)$ is

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega] = \big\{a + b\omega : a, b \in \mathbb{Z}\big\}, \tag{1}$$

where

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

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

For more details concerning integral closures, see e.g., [2, Chapter 5] and [8, §VIII.5].

Let $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$ and consider the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. By [1, Theorem 13.2.5], $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is an infinite unique factorization domain with finitely many units. Therefore, from Proposition 2.2(ii), it follows that there are infinitely many non-associative prime elements in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

We have the following result that relates D-rings (in the sense of the property $(*)$) with the ring of integers $\mathcal{O}_L$.

Proposition 3.5. *Assume that $K \subseteq L$ is a finite Galois extension of fields and let C be the integral closure of R in L. If R is integrally closed and satisfies the property $(*)$, then the ring C also satisfies the property $(*)$.*

In particular, since for all $d \in \mathbb{Z}$ the field extension $\mathbb{Q} \subseteq \mathbb{Q}\big(\sqrt{d}\big)$ is Galois, then the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a D-ring $\big($in the sense of the property $(*)\big)$.

A proof of Proposition 3.5 is presented in Section 4.

Recall that for all polynomials f in $R[x]$, we denote by $\mathcal{P}(f)$ the set of all prime elements p in R such that there exists $r_p \in R$ with $f(r_p) \neq 0$ and $p \mid f(r_p)$. Observe in particular that $\mathcal{P}(0) = \mathcal{P}(1) = \varnothing$ and if c is a non–zero non–unit constant in R, then $\mathcal{P}(c)$ is the set of all prime elements p in R such that $p \mid c$.

We now present the proof of Theorem 1.2, which is also an adaptation of (yet not identical to) the proof of [7, Proposition 1].

Proof of Theorem 1.2. (i) $\Rightarrow$ (ii). Let f be a polynomial in $R[x]$ such that $f(r) \in R^\times$ for all $r \in R$ with $f(r) \neq 0$. Then for all $r \in R$ with $f(r) \neq 0$, we have $f(r) \mid 1$. By hypothesis, $\deg(f) \leq \deg(1) = 0$. Thus, f must be constant.

(ii) $\Rightarrow$ (iii). Assume that $\mathcal{P}(f) = \varnothing$ for some non–constant polynomial f in $R[x]$. Since R is a unique factorization domain then $f(r) \in R^{\times}$ for all $r \in R$ with $f(r) \neq 0$, contradicting (ii).

(iii)$\Rightarrow$(iv). Let f be a non–constant polynomial in $R[x]$ and let c be a non-zero constant in R. Assume that $\mathcal{P}(f) \setminus \mathcal{P}(c)$ is finite, say $\mathcal{P}(f) \setminus \mathcal{P}(c) = \{p_1, \ldots, p_n\}$. Let $m = p_1 \cdots p_n$ and assume that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_n \neq 0$. We first consider the case $f(0) = 0$. Let $\mathcal{Z}(f)$ be the set of all prime elements q in R such that $f(q) = 0$. Therefore, for all prime elements q of $R \setminus \mathcal{Z}(f)$, $f(q) \neq 0$ and $q \mid f(q)$. Thus, $\mathcal{P}(f)$ is the set of all prime elements of R belonging to $R \setminus \mathcal{Z}(f)$ and the set $\mathcal{P}(c)$ contains all prime elements of $R \setminus \mathcal{Z}(f)$, except $p_1, \ldots, p_n$. Assume that $\mathcal{Z}(f) = \{q_1, \ldots, q_s\}$ and let $\zeta = q_1 q_2 \cdots q_s$. Therefore, every prime element q in R divides ζcm. Let consider $g(x) = 1 + \zeta cmx$. Since by hypothesis $\mathcal{P}(g) \neq \varnothing$, then there exists a prime element q of R and an element $r_q \in R$ such that $g(r_q) \neq 0$ and $q \mid g(r_q) = 1 + \zeta cmr_q$. Since $q \mid \zeta cmr_q$ then $q \mid 1$, which is a contradiction. We then assume that $f(0) = a_0 \neq 0$ and let consider $h(x) = f(ca_0 x)$. Then $h(x) = a_0 g(x)$ with $g(x) = c^n a_0^{n-1} x^n + c^{n-1} a_0^{n-2} a_{n-1} x^{n-1} + \cdots + ca_1 x + 1$. It follows that for every $r \in R$ and for every prime element q in $\mathcal{P}(c)$, we get $q \mid g(r) - 1$. Thus, $\mathcal{P}(g) \cap \mathcal{P}(c) = \varnothing$. Observe that since $\mathcal{P}(g) \subseteq \mathcal{P}(f)$, then $\mathcal{P}(g) \subseteq \mathcal{P}(f) \setminus \mathcal{P}(c)$. Therefore, if the set $\mathcal{P}(g)$ is infinite then the set $\mathcal{P}(f) \setminus \mathcal{P}(c)$ is also infinite. Assume then that $\mathcal{P}(g)$ is a finite set, say $\mathcal{P}(g) = \{q_1, \ldots, q_s\}$. Let $b = q_1 q_2 \cdots q_s$. Therefore, the polynomial $u(x) = g(bx)$ has free term equal to 1 and all its remainder coefficients are divisible by b. Observe also that $\mathcal{P}(u) \subseteq \mathcal{P}(g)$. Moreover, it follows from (iii) that $\mathcal{P}(u)$ is non–empty. Thus, there exits $i_0 \in \{1, \ldots, s\}$ such that $q_{i_0} \in \mathcal{P}(u)$ and $q_{i_0} \mid u(r) - 1$ for all $r \in R$. This implies that $q_{i_0} \mid 1$, which contradicts the fact that q_{i_0} is a prime element in R.

(iv)$\Rightarrow$(v). Let f be a non-constant polynomial in $R[x]$. By (iv), the set $\mathcal{P}(f) = \mathcal{P}(f) \setminus \mathcal{P}(1)$ is infinite.

(v)$\Rightarrow$(i). Assume that R is not a D-ring in the sense of the property $(*)$, i.e., assume that there exist two polynomials f and g in $R[x]$ such that for all $r \in R$ with $f(r) \neq 0$ we have $f(r) \mid g(r)$, but with $g \neq 0$ and $\deg(f) > \deg(g)$. Therefore, f is non–constant and f does not divide g in $K[x]$. Thus, without losing the generality, we can assume that f and g are relatively prime in $K[x]$. Then there exist suitable polynomials α and β in $R[x]$ and a non-zero constant c in R such that

$$\alpha(x)f(x) + \beta(x)g(x) = c.$$

Since f is a non-constant polynomial, then it follows from (v) that the set $\mathcal{P}(f)$ is infinite, which in particular implies that $\mathcal{P}(f)$ is non-empty. Let p be a prime element in R that belongs to $\mathcal{P}(f)$. Then there exist $r_p \in R$ such that $f(r_p) \neq 0$ and $p \mid f(r_p)$. By hypothesis, $f(r_p) \mid g(r_p)$, which implies that $f(r_p) \mid c$. Since $p \mid f(r_p)$ then $p \mid c$. This proves that $\mathcal{P}(f) \subseteq \mathcal{P}(c)$, where $\mathcal{P}(f)$

is an infinite set and $\mathcal{P}(c)$ is a finite set. This is a contradiction. Hence, R is a D-ring in the sense of the property $(*)$. ☑

Corollary 3.6. (cf. [7, Corollary 5, pg. 292])

(i) The ring of polynomials $R[x_1, \ldots, x_n]$ is a D-ring.

(ii) Assume that R is not a field. If $\mathfrak{J}_R \neq 0$, then R is not a D-ring. In particular, if R is a local ring, then R is not a D-ring.

Proof. (i). It suffices to consider the case of one variable $R[x]$. Let f be a polynomial in $R[x][y] = R[x, y]$ with the property that for all $r \in R[x]$, $f(r)$ is a unit in $R[x]$. Since the units of $R[x]$ are the units of R, then for all $r \in R[x]$, $0 = \deg_x \big(f(r)\big) = \deg_y(f) \deg_x(r)$. It follows that $\deg_y(f) = 0$, which implies that f is a constant polynomial. Thus, Corollary 3.6(i) follows from Theorem 1.2 (i)⇔(ii).

(ii). Assume that R is not a field and that there exists a non-zero element m in $\mathfrak{J}_R$. Consider $f(x) = 1 - mx$ in $R[x]$. Therefore, $f(r)$ is a unit in R for all $r \in R$. Since f is a non-constant polynomial, it follows from Theorem 1.2 (i)⇔(ii) that R is not a D-ring. ☑

Observe that Corollary 3.6 implies in particular that the Jacobson radical of a ring of polynomials over an integral domain is always equal to zero.

In the following example, we apply Theorem 1.2 to give an alternative proof of the infinitude of prime integers p such that $p \equiv 1 \pmod 4$, $p \equiv 1 \pmod 8$ or $p \equiv 1 \pmod 3$.

Example 3.7. Consider the D-ring $\mathbb{Z}$ and let m be a positive integer. Consider the polynomial $f(x) = x^m + 1$. It follows from Theorem 1.2(v) that $\mathcal{P}(f)$ is an infinite set. If $m = 2$ then $\mathcal{P}(f)$ is the set of all prime integers p with $p \equiv 1 \pmod 4$ (see [5, Lemma 8.17]). Thus, there are infinitely many primes p such that $p = 4n + 1$ for some $n \geq 1$. Let $m = 4$ and let p be a prime in $\mathcal{P}(f)$. It follows that there exists an integer r_p such that $r_p^4 \equiv -1 \pmod p$, which implies that $r_p^8 \equiv 1 \pmod p$. By looking r_q as an element of the multiplicative group $(\mathbb{Z}/p)^\times$, it follows that the order of r_q divides 8. Since $r_q^4 \equiv -1 \pmod p$ then the order of r_q is 8. By Lagrange's Theorem, we get that the order of r_q divides the order of $(\mathbb{Z}/p)^\times$, which is $p-1$. Thus, $p \equiv 1 \pmod 8$, and therefore there are infinitely many primes p such that $p = 8n + 1$ for some $n \geq 1$ (cf. [6, Lemma 3.1.5.2]). Consider next the polynomial $g(x) = x^2+3$. As before, the set $\mathcal{P}(g)$ is infinite. Let p be an odd prime integer in $\mathcal{P}(g)$. Since -3 is a quadratic residue mod p if and only if $p \equiv 1 \pmod 3$, it follows that there are infinitely many primes p such that $p = 3n + 1$ for some $n \geq 1$ (cf. [6, Lemma 3.1.5.4]).

4. Proof of Proposition 3.5

Proposition 4.1. ([11, Chapter 1, Proposition 2.19 (iv)]) *Let R be an integral domain with identity 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 $R = \big\{b \in C : \sigma(b) = b,$ for all $\sigma \in \mathrm{Gal}(L/K)\big\}$.*

Let R, K, L and C be as in the hypotheses of Proposition 4.1 with R integrally closed. For all polynomial p in $L[x]$ with $p(x) = \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0$ and $\alpha_n \neq 0$, and for all $\sigma \in \mathrm{Gal}(L/K)$, let p_σ be the polynomial $p_\sigma(x) = \sigma(\alpha_n)x^n + \cdots + \sigma(\alpha_1)x + \sigma(\alpha_0)$. Note that for all $\sigma \in \mathrm{Gal}(L/K)$, $\deg(p) = \deg(p_\sigma)$ and that if $p = rs$ with $r, s \in L[x]$ then $p_\sigma = r_\sigma s_\sigma$.

Lemma 4.2. *Let p be a polynomial with coefficients in C.*

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

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

Proof. Statement (i) follows directly from the fact that $R \subseteq K$. Assume that $p = p_\sigma$ for all $\sigma \in \mathrm{Gal}(L/K)$. Then the coefficients of p are fixed by any element of $\mathrm{Gal}(L/K)$. Since R is integrally closed, the second implication of Proposition 4.1 implies that $p \in R[x]$. Conversely, if $p \in R[x]$ then $p = p_\sigma$ for all $\sigma \in \mathrm{Gal}(L/K)$ since $R \subseteq K$. ☑

For all polynomials p in $L[x]$, let $N_{L/K}(p)$ be the polynomial $\prod_{\sigma \in \mathrm{Gal}(L/K)} p_\sigma$. Note that if p is a polynomial in $L[x]$ then $\deg\big(N_{L/K}(p)\big) = \big|\,\mathrm{Gal}(L/K)\big|\deg(p)$ and $N_{L/K}(p) = 0$ if and only if $p = 0$.

Lemma 4.3. *Let p be a polynomial with coefficients in C. Then p satisfies the following properties.*

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

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

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

Proof. Let $q = N_{L/K}(p)$. Note that $q \in C[x]$. Let τ be a fixed element in $\mathrm{Gal}(L/K)$. Then $\tau \circ \sigma \in \mathrm{Gal}(L/K)$ and $(p_\tau)_\sigma = p_{\tau\circ\sigma}$ for all $\sigma \in \mathrm{Gal}(L/K)$. Note also that τ induces a permutation of the finite group $\mathrm{Gal}(L/K)$. Therefore, $q_\tau = \prod_{\tau\circ\sigma \in \mathrm{Gal}(L/K)} p_{\tau\circ\sigma} = q$, which implies by Lemma 4.2(ii) that $q \in R[x]$. This proves (i). Note that (ii) is a direct consequence of (i) and (iii) follows from Lemma 4.2(i). ☑

Proof of Proposition 3.5. Assume that $n = \big|\operatorname{Gal}(L/K)\big|$. Let f and g be two polynomials in $C[x]$ with the property that $f(r) \mid g(r)$ for all $r \in C$ with $f(r) \neq 0$. Assume that $g \neq 0$. Consider $F = N_{L/K}(f)$ and $G = N_{L/K}(g)$, which by Lemma 4.3(i) are polynomials in $R[x]$ with $G \neq 0$. Let r be an element in R such that $F(r) \neq 0$. In particular, we have that $f(r) \neq 0$. Since $R \subseteq C$, it follows by assumption that $f(r) \mid g(r)$, which in turn implies that $F(r) = \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma\big(f(r)\big)$ divides $G(r) = \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma\big(g(r)\big)$ in R. Since R satisfies property $(*)$, then either $G = 0$ or $n \deg(f) = \deg(F) \leq \deg(G) = n \deg(g)$ and therefore $\deg(f) \leq \deg(g)$. Hence, the ring C also satisfies the property $(*)$. ☑

References

[1] M. Artin, *Algebra*, second ed., Prentice Hall, 2011.

[2] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] D. M. Burton, *Elementary Number Theory*, fifth ed., McGraw Hill, 2002.

[4] L. F. Cáceres and J. A. Vélez-Marulanda, *On Certain Divisibility Property of Polynomials over Integral Domains*, J. Math. Research. **3** (2011), no. 3, 28–31.

[5] D. S. Dummit and R. M. Foote, *Abstract Algebra*, third ed., John Wiley & Sons Inc., 2004.

[6] B. Fine and G. Rosenberger, *Number Theory: An Introduction via the Distribution of Primes*, Birkhäuser, 2007.

[7] H. Gunji and D. L. McQuillan, *On Rings with Certain Divisibility Property*, Michigan. Math. J. **22** (1976), no. 4, 289–299.

[8] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics 73, Springer, 1974.

[9] I. Kaplansky, *Elementary Divisors and Modules*, Trans. Amer. Math. Soc. **66** (1949), 464–491.

[10] ———, *Commutative Rings*, Polygonal Publishing House, 1994.

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

[12] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Mathematics 1600, Springer, 1995.

(Recibido en mayo de 2013. Aceptado en julio de 2013)

Department of Mathematical Sciences
University of Puerto Rico at Mayagüez
P.O. Box 9000
Mayagüez, PR, 00681
United States of America
e-mail: luis.caceres1@upr.edu

Department of Mathematics & Computer Science
Valdosta State University
2072 Nevins Hall
1500 N. Patterson St.
Valdosta, GA, 31698-0040
United States of America
e-mail: javelezmarulanda@valdosta.edu

Esta página aparece intencionalmente en blanco