Revista Integración, temas de matemáticas
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 35, No. 2, 2017, pág. 143–148

DOI:http://dx.doi.org/10.18273/revint.v35n2-2017001

When is $R[x]$ a principal ideal ring?

Henry Chimal-Dzul[a]*, C. A. López-Andrade[b]

[a] Ohio University, Department of Mathematics, Athens, USA.

[b] Benemérita Universidad Autónoma de Puebla, Facultad de Ciencias Físico Matemáticas, Puebla, México.

Abstract. Because of its interesting applications in coding theory, cryptography, and algebraic combinatorics, in recent decades a lot of attention has been paid to the algebraic structure of the ring of polynomials $R[x]$, where R is a finite commutative ring with identity. Motivated by this popularity, in this paper we determine when $R[x]$ is a principal ideal ring. In fact, we prove that $R[x]$ is a principal ideal ring if and only if R is a finite direct product of finite fields.

Keywords: Principal ideal ring, polynomial ring, finite rings.
MSC2010: 13F10, 13F20, 16P10, 13C05.

¿Cuándo $R[x]$ es un anillo de ideales principales?

Resumen. Debido a sus interesantes aplicaciones en teoría de códigos, criptografía y combinatoria algebraica, en décadas recientes se ha incrementado la atención en la estructura algebraica del anillo de polinomios $R[x]$, donde R es un anillo conmutativo finito con identidad. Motivados por esta popularidad, en este artículo determinamos cuándo $R[x]$ es un anillo de ideales principales. De hecho, demostramos que $R[x]$ es un anillo de ideales principales, si y sólo si, R es un producto directo finito de campos finitos.

Palabras clave: Anillo de ideales principales, anillo de polinomios, anillos finitos.

1. Introduction and preliminaries

Polynomials with coefficients in a finite commutative ring R with identity arise naturally, for instance, in practical applications dealing with coding theory, cryptography and algebraic combinatorics, e. g. [1], [2], [3], [4], [6]. For some of these applications, it is important to know the algebraic structure of either the ring of polynomials $R[x]$ or the

*E-mail: hc118813@ohio.edu
Received: 05 May 2017, Accepted: 04 September 2017.
To cite this article: H. Chimal-Dzul, C.A. López-Andrade, When $R[x]$ is a principal ideal ring?, *Rev. Integr. temas mat.* 35 (2017), No. 2, 143–148.

quotient ring $R[x]/A$, where A is an ideal of $R[x]$. In particular, often one wants to know when such rings are principal ideal rings (PIR's). Motivated by this question, in this paper we examine when $R[x]$ is a PIR. We prove that $R[x]$ is a principal ideal ring if and only if R is a finite direct product of finite fields. To this end, let us start remembering some facts about commutative finite rings with identity.

The most familiar example of a finite commutative ring with identity is the ring $\mathbb{Z}_m$ of integers modulo $m \geq 2$. When m is a composite number, the Chinese Remainder Theorem assures that

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}},$$

where $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of m, and $\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$ is the direct product of the rings $\mathbb{Z}_{p_i^{\alpha_i}}$, $1 \leq i \leq n$. Remember that for each i $(1 \leq i \leq k)$, $\mathbb{Z}_{p_i^{\alpha_i}}$ is a finite local ring with maximal ideal $\langle p_i \rangle$ (see [5]). In particular, note that if $\alpha = 1$, then $\mathbb{Z}_p$ is a finite field (see [4]). Consequently, the Chinese Remainder Theorem establishes that $\mathbb{Z}_m$ is isomorphic to a direct product of finite local rings. This is the simplest case of the following result.

Theorem 1.1 (Structure of Finite Commutative Rings, [5], Theorem VI.2). *Every finite commutative ring with identity is isomorphic to a direct product of finite commutative local rings with identity. This decomposition is unique up to the order of the factors.*

In view of the previous theorem, if R is a finite commutative ring with identity and $R_1 \times \cdots \times R_n$ is the unique decomposition of R as a direct product of local rings, then there exists a ring isomorphism $\varphi : R \to R_1 \times \cdots \times R_n$ which maps each element $r \in R$ into a unique n-tuple $\varphi(r) = (r_1, \ldots, r_n) \in R_1 \times \cdots \times R_n$. This map extends to a ring isomorphism

$$\Phi : R[x] \to R_1[x] \times \cdots \times R_n[x],$$

defined by

$$p(x) \mapsto \left(p_1^{(0)} + p_1^{(1)}x + \cdots + p_1^{(k)}x^k, \ldots, p_n^{(0)} + p_n^{(1)}x + \cdots + p_n^{(k)}x^k\right), \tag{1}$$

where $p(x) = p_0 + p_1 x + \cdots + p_k x^k$ and $\varphi(p_i) = \left(p_1^{(i)}, \ldots, p_n^{(i)}\right)$, $0 \leq i \leq k$.

Proposition 1.2. *Let $R_1, \ldots, R_n$ be commutative rings with identity. Then their direct product $R = R_1 \times \cdots \times R_n$ is a PIR if and only if R_i is a PIR for each i, $1 \leq i \leq n$.*

Proof. Let A be an ideal of R and for each i, $1 \leq i \leq n$, define $A_i = \{a_i \in R_i : (a_1, \ldots, a_i, \ldots, a_n) \in A\}$. Then A_i is an ideal of R_i and we claim that $A = A_1 \times \cdots \times A_n$. The inclusion $A \subseteq A_1 \times \cdots \times A_n$ is clear. To prove the reverse inclusion, let $a = (a_1, \ldots, a_n)$ be an element in $A_1 \times \cdots \times A_n$. It follows from the definition of A_i that there exist $\alpha_1, \ldots, \alpha_n \in A$ such that $a = \alpha_1 e_1 + \cdots + \alpha_n e_n$, where e_i denotes the element of R with a 1 in the ith coordinate and 0's elsewhere. Hence, using that A is an ideal of $R_1 \times \cdots \times R_n$, we have that $a \in A$. Therefore $A = A_1 \times \cdots \times A_n$, and so $A = \langle (a_1, \cdots, a_n) \rangle$ if and only if $A_i = \langle a_i \rangle$ for every i, $1 \leq i \leq n$. ☑

In light of Proposition 1.2 and the isomorphism Φ given in (1), $R[x]$ is a PIR if and only if $R_i[x]$ is a PIR for each i, $1 \leq i \leq n$. Hence, in order to determine whenever $R[x]$ is

a PIR, it is natural to ask when $R_i[x]$ is a PIR. This is the purpose of the next section. To illustrate the results of Section 2, we present in Section 3 three families of finite rings with identity that are relevant in the theory of finite commutative rings.

2. Ideals of $R[x]$

First of all, by a ring R we will always mean a commutative ring with identity $1 \neq 0$, and remember that a ring R is called local if it has a unique maximal ideal, or equivalently, R is a local ring with maximal ideal M if and only if $M = R \setminus U(R)$, where $U(R)$ denotes the group of units of R. We usually write (R, M) or (R, M, F) to denote a local ring R, its maximal ideal M and its residue field $F = R/M$ (using that M is a maximal ideal of R, the quotient ring R/M is indeed a field).

The simplest case of a finite local ring R is when R is a finite field. In this case the ring $R[x]$ of polynomials with coefficients in R is a PIR. In fact, $R[x]$ is a principal ideal domain (PID). Therefore, in what follows we focus our attention on a finite local ring R which is not a field.

Let (R, M, F) be a finite local ring which is not a field. Note that the natural surjective homomorphism $^- : R \to F$ induces a surjective polynomial ring homomorphism $\mu : R[x] \to F[x]$ given by

$$f_0 + f_1 x + \cdots + f_n x^n \mapsto \overline{f_0} + \overline{f_1}\, x + \cdots + \overline{f_n}\, x^n.$$

This ring homomorphism lets us deduce some facts about polynomials $f(x) = \sum_{i=0}^{n} f_i x^i \in R[x]$ by using the structure of $F[x]$. In particular, note that $\mu(f(x)) = \overline{0}$ if and only if $f_i \in M$ for all i, $0 \leq i \leq n$ and so, it follows that $\ker \mu$ is a proper ideal of $R[x]$ $\big($indeed, $\ker \mu$ is a prime ideal of $R[x]$ because $R[x]/\ker \mu \cong F[x]$ is an integral domain$\big)$.

On the other hand, remember that an element r of a ring R is called irreducible if it is neither 0 nor a unit in R and the condition $r = ab$, for some $a, b \in R$, implies that $a \in U(R)$ or $b \in U(R)$.

Having remembered the above, if $f(x) \in R[x]$ is such that $\mu(f(x))$ is irreducible in $F[x]$, then $f(x)$ is also irreducible in $R[x]$. Since for every finite field K and every positive integer n there exists an irreducible polynomial in $K[x]$ of degree n (see [4]), we conclude that irreducible polynomials in $R[x]$ of degree n exist for every positive integer n. It is worth to mention that the converse of this fact does not hold in general. That is, if $f(x)$ is an irreducible polynomial in $R[x]$ then $\mu(f(x))$ is not necessarily irreducible in $F[x]$. For instance, if $p \geq 2$ is a prime number, then $p \in \mathbb{Z}_{p^2}[x]$ is irreducible in $\mathbb{Z}_{p^2}[x]$ but $\mu(p) = \overline{0} \in \big(\mathbb{Z}_{p^2}/\langle p \rangle\big)[x]$ is not irreducible by definition. Furthermore, if $f(x) = x^2 + 2x + 3 \in \mathbb{Z}_4[x]$ then $f(x)$ is irreducible in $\mathbb{Z}_4[x]$; whereas $\mu(f(x)) = x^2 + \overline{1} = (x + \overline{1})^2 \in (\mathbb{Z}_4/\langle 2 \rangle)[x]$ is not irreducible.

Lemma 2.1. *Let (R, M) be a local ring which is not a field, $p(x)$ an irreducible polynomial in $R[x]$ and $\theta \in M \setminus \{0\}$. Then $\langle p(x), \theta \rangle$ is a proper ideal of $R[x]$.*

Proof. If $\mu(p(x)) = \overline{0}$, then $p(x) \in \ker \mu$, so that $\langle p(x), \theta \rangle \subseteq \ker \mu \subsetneq R[x]$. If $\mu(p(x)) \neq \overline{0}$, then we proceed by contradiction. Assume then the existence of some polynomials

$f(x), g(x) \in R[x]$ such that $1 = f(x)\theta + g(x)p(x)$. This implies that $\overline{1} = \mu(g(x))\mu(p(x))$, which contradicts the irreducibility of $p(x)$. Hence, for every irreducible polynomial $p(x)$ in $R[x]$ and $\theta \in M \setminus \{0\}$, $\langle p(x), \theta \rangle$ is a proper ideal of $R[x]$. ☑

If $p(x) = p_0 + p_1 x + \cdots + p_n x^n \in R[x]$ is an irreducible polynomial in $R[x]$ such that $\mu(p(x)) \neq \overline{0}$, then $\deg(\mu(p(x))) = k \geq 1$, since $\mu(p(x))$ can not be a unit in $F[x]$. This implies that $p_k \in U(R)$ and $p_{k+1}, \ldots, p_n \in M$ and so, for each nonzero polynomial $a(x) \in R[x]$ we have that $\deg(p(x)a(x)) \geq k \geq 1$. Consequently, every nonzero polynomial in $\langle p(x) \rangle \subset R[x]$ is not a constant polynomial, and so $M \nsubseteq \langle p(x) \rangle$.

Theorem 2.2. *Let (R, M) be a local ring which is not a field. Then $R[x]$ is not a PIR.*

Proof. Let $p(x) \in R[x]$ be an irreducible polynomial in $R[x]$ such that $\mu(p(x)) \neq \overline{0}$, and let $\theta \in M \setminus \{0\}$. Then we claim that $\langle p(x), \theta \rangle$ is not a principal ideal of $R[x]$. Assume the contrary; that is, suppose that there is a polynomial $h(x) \in R[x]$ such that $\langle p(x), \theta \rangle = \langle h(x) \rangle$. Then there exists $f(x) \in R[x]$ such that $p(x) = f(x)h(x)$. Using that $p(x)$ is irreducible, we have that $f(x) \in U(R[x])$ or $h(x) \in U(R[x])$. It follows immediately from Lemma 2.1 that $h(x) \notin U(R[x])$, and so $f(x) \in U(R[x])$. This implies that $\langle p(x), \theta \rangle = \langle h(x) \rangle = \langle p(x) \cdot f(x)^{-1} \rangle = \langle p(x) \rangle$, which is a contradiction since $\theta \notin \langle p(x) \rangle$. In consequence, $\langle p(x), \theta \rangle$ is not a principal ideal in $R[x]$. ☑

Note that we have proved implicitly in Theorem 2.2 that for every local ring (R, M, F) which is not a field, the family of ideals $\langle p(x), \theta \rangle$, where $p(x)$ is an irreducible element in $R[x]$ such that $\mu(p(x)) \neq \overline{0}$, and θ is a nonzero element in M, consists entirely of non-principal ideals of $R[x]$. This family contains an infinite number of elements since irreducible polynomials of degree n in $R[x]$ exist for every integer $n \geq 1$.

Theorem 2.3. *Let R be a finite ring. The following statements are equivalent:*

1. *$R[x]$ is a PIR.*
2. *R is isomorphic to a direct product of finite fields.*

Proof. It follows immediately from Proposition 1.2 and Theorems 1.1, 2.2. ☑

An equivalent way to state Theorem 2.3 is as follows: $R[x]$ is a not a PIR if and only if R is isomorphic to a direct product $R_1 \times \cdots \times R_i \times \cdots \times R_n$ of finite local rings such that at least one of them is not a finite field, say (R_i, M_i, F_i). In this case, for all $\theta \in M_i \setminus \{0\}$ and for all irreducible polynomials $p(x) \in R_i[x]$ with $\mu_i(p(x)) \neq \overline{0}$ in $F_i[x]$ we have that $\langle p(x), \theta_i \rangle \subset R_i[x]$ is not a principal ideal in $R_i[x]$. In consequence, by using the ring isomorphism Φ defined in (1), one can easily show that $\langle \Phi^{-1}(p_i(x) \cdot e_i), \Phi^{-1}(\theta_i \cdot e_i) \rangle \subset R[x]$ is not a principal ideal in $R[x]$.

Another equivalent way to state Theorem 2.3 is derived from the structure theorem for commutative PIR's due to Zariski-Samuel (see [7, Theorem 33]). This result states that every commutative PIR is (isomorphic to) a direct sum of PID's and of special PIR's. Therefore, Theorem 2.3 shows that Zariski-Samuel theorem can be expressed for the

ring of polynomials over a finite ring R as follows: *$R[x]$ is a PIR if and only if $R[x]$ is isomorphic to a direct product of PID's.* Moreover, the isomorphism Φ given in (1) presents one decomposition of $R[x]$ as a direct product of PID's. In addition, Theorem 2.2 also implies that for a local ring (R, M) which is not a field, the ring of polynomials $R[x]$ cannot be a special PIR.

3. Examples

As a first example we present the one that we used to motivate Theorem 1.1. Let $m \geq 2$ be an integer. Then

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}},$$

where $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of m. Since $\mathbb{Z}_{p_i^{\alpha_i}}$ is a finite field if and only if $\alpha_i = 1$, it follows from Theorem 2.3 that $\mathbb{Z}_m[x]$ is a PIR if and only if $\alpha_1 = \cdots = \alpha_k = 1$.

In order to generalize the previous example, let us to consider the ring $\mathbb{Z}_{p^\alpha}$, where p is a prime number and α is a positive integer. Let $f(u)$ be a monic polynomial of degree $r \geq 1$ in $\mathbb{Z}_{p^\alpha}[u]$ such that $\mu(f(u))$ is irreducible in $(\mathbb{Z}_{p^\alpha}/\langle p\rangle)[u]$. Then the Galois ring of characteristic p^α and cardinality $p^{\alpha r}$ is definied as the quotient ring

$$\begin{aligned} GR(p^\alpha, r) &= \mathbb{Z}_{p^\alpha}[u]/\langle f(u)\rangle \\ &= \{a_0 + a_1 u + \cdots + a_{r-1}u^{r-1} + \langle f(u)\rangle \ : \ a_i \in \mathbb{Z}_{p^\alpha}\}. \end{aligned}$$

This ring is a finite local ring with maximal ideal $\langle p + \langle f(u)\rangle\rangle$, and residue field isomorphic to $\mathbb{Z}_p[u]/\langle \mu(f(u))\rangle$ (see [5] for more details). Note that if $r = 1$ then

$$GR(p^\alpha, 1) = \mathbb{Z}_{p^\alpha}[u]/\langle a + u\rangle = \{a_0 + \langle a + u\rangle \ : \ a_0 \in \mathbb{Z}_{p^\alpha}\} \cong \mathbb{Z}_{p^\alpha}.$$

Consequently, $GR(p, 1) \cong \mathbb{Z}_p$ is a finite field, and for any integer $\alpha \geq 2$, $GR(p^\alpha, 1)$ is a finite local ring which is not a field. Furtheremore, if $r \geq 2$ and $\alpha = 1$, then $GR(p, r) = \mathbb{Z}_p[u]/\langle f(u)\rangle$ is a finite field with p^r elements (see [4]). Hereof it follows from Theorem 2.2 that

$$GR(p^\alpha, r)[x] \ \text{ is } \ \begin{cases} \text{a PIR} & \text{if } \alpha = 1, \\ \text{not a PIR} & \text{if } \alpha \geq 2. \end{cases} \tag{2}$$

Let $p_1, p_2, \ldots, p_k$ be prime numbers, α_i, r_i positive integers for $1 \leq i \leq k$, and consider the following ring which is a natural generalization of $\mathbb{Z}_m$:

$$R = GR(p_k^{\alpha_1}, r_1) \times \cdots \times GR(p_k^{\alpha_k}, r_k).$$

In analogy with $\mathbb{Z}_m$, we deduce from (2) and Theorem 2.3 that $R[x]$ is a PIR if and only if $\alpha_1 = \cdots = \alpha_k = 1$. On the other hand, $R[x]$ is not a PIR if and only if $\alpha_i \geq 2$ for some i, $1 \leq i \leq k$.

In the examples given above we have presented infinite families of finite rings for which the ring of polynomials with coefficients in these rings are not PIR. The common ground in both families of rings is that they are finite products of local rings whose ideals are principal and they are linearly ordered by inclusion. Any local ring satisfying these

conditions is called a *finite chain ring* (see [1]). In general, if R is a finite chain ring that is not a field, then $R[x]$ is not a PIR by Theorem 2.2, and so for every finite ring R such that it is isomorphic to a direct product of finite chain rings (of which at least one is not a field), the ring $R[x]$ is not a PIR by Theorem 2.3.

In the following lines, we are going to present a family of finite local rings which was introduced in [2].

Let p be a prime number, α a positive integer and denote by $\mathbb{F}_q$ the unique finite field with $q = p^\alpha$ elements (see [5]). Then for every integer $k \geq 1$, the quotient ring $R_k = \mathbb{F}_q[u_1, u_2, \ldots, u_k]/\langle u_1^2, u_2^2, \ldots, u_k^2 \rangle$ is a commutative ring with identity. Furthermore, it is proved in [2] that R_k is a finite local ring with maximal ideal $M = \langle [u_1], [u_2], \ldots, [u_k] \rangle$ and residue field $R_k/M \cong \mathbb{F}_2$. In consequence, Theorem 2.3 shows that $R_k[x]$ is not a PIR for any integer $k \geq 1$.

Since $k \geq 2$, the ring R_k described above is neither a PIR nor a chain ring in view of M is not a principal ideal and $\langle [u_i] \rangle$ and $\langle [u_j] \rangle$ are not linearly ordered by inclusion for $i \neq j$. However, it was pointed out in [2] that R_k is a *finite Frobenius ring*.

Acknowledgement

We would like to thank the anonymous referee for his/her useful comments and suggestions that significantly contributed to improve the quality of our manuscript.

References

[1] Dinh H.Q. and López-Permouth S.R., "Cyclic and negacyclic codes over finite chain rings", *IEEE Trans. Inform. Theory* 50 (2004), No. 8, 1728–1744.

[2] Dougherty S.T., Yildiz B. and Karadeniz S., "Codes over R_k, Gray maps and their binary images", *Finite Fields Appl.* 17 (2011), No. 3, 205–219.

[3] Gómez-Calderón J. and Mullen G. L., "Galois rings and algebraic cryptography", *Acta Arith.* 59 (1991), No. 4, 317–328.

[4] Lidl R. and Niederreiter H., *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[5] McDonald B., *Finite rings with identity*, Marcel Dekker, New York, 1974.

[6] Xiang-dong H.A. and Nechaev A.A., "A construction of finite Frobenius Rings and its application to partial difference sets", *J. Algebra* 309 (2007), No. 1, 1–9.

[7] Zariski O. and Samuel P., *Commutative Algebra I*, Springer-Verlag, New York, 1975.