Mathematica Bohemica

Brahim Boudine

Characterization of irreducible polynomials over a special principal ideal ring

Mathematica Bohemica, Vol. 148 (2023), No. 4, 501–506

Persistent URL: http://dml.cz/dmlcz/151970

CHARACTERIZATION OF IRREDUCIBLE POLYNOMIALS OVER A SPECIAL PRINCIPAL IDEAL RING

Brahim Boudine, Fez

Received December 5, 2021. Published online September 8, 2022.
Communicated by Simion Breaz

Abstract. A commutative ring R with unity is called a special principal ideal ring (SPIR) if it is a non integral principal ideal ring containing only one nonzero prime ideal, its length e is the index of nilpotency of its maximal ideal. In this paper, we show a characterization of irreducible polynomials over a SPIR of length 2. Then, we give a sufficient condition for a polynomial to be irreducible over a SPIR of any length e.

Keywords: polynomial; irreducibility; commutative principal ideal ring

MSC 2020: 13F20, 13B25

1. Introduction

The irreducibility of polynomial functions is among the most important topics in the abstract algebra. They are widely used in number theory [7], cryptography [5], coding theory [2] and complexity theory [8].

It is well known that irreducible polynomials in $\mathbb{C}[X]$ are exactly the ones of degree 1 and in $\mathbb{R}[X]$, irreducible polynomials are of degree 1 and those of the form $aX^2 + bX + c$, where $b^2 - 4ac < 0$. But in the general case of fields or commutative rings, irreducible polynomials are not really known. Some good tools are used to find more information about them like Eisenstein's criterion and the Newton polygon. But this was not sufficient to find all of them.

In this paper, we are interested in irreducible polynomials over the commutative special principal ideal ring (SPIR). Recall that a SPIR is a non integral principal ideal ring which contains only one nonzero prime ideal (see [3], page 176, Definition 14.3). If k is its residual field, πR is its maximal ideal and e its index of nilpotency, we denote $(R, \pi R, k, e)$ and we say that R is a SPIR of length e.

DOI: 10.21136/MB.2022.0187-21

Our aim is to give a complete characterization of irreducible polynomials over a SPIR of length 2; this allows to identify completely irreducible polynomials over $\mathbb{C}[Y]/(Y^2)$ and $\mathbb{R}[Y]/(Y^2)$. Moreover, we give a sufficient condition for a polynomial f to be irreducible over a SPIR of any length e. So we get some irreducible polynomials over $\mathbb{C}[Y]/(Y^e)$ and $\mathbb{R}[Y]/(Y^e)$.

2. Preliminaries

For every $x \in R$ we denote by $\overline{x}$ the class of x in $k = R/\pi R$, and for every polynomial $f(X) = a_0 + a_1X + \ldots + a_nX^n$ we denote by $\overline{f}$ the polynomial in $k[X]$ defined by $\overline{f}(X) = \overline{a_0} + \overline{a_1}X + \ldots + \overline{a_n}X^n$.

Proposition 2.1 (Hensel's development)**.** *Let $(R, \pi R, k, e)$ be a SPIR. Then:*

$$\forall\, x \in R\ \exists!\, (\overline{x_0}, \ldots, \overline{x_{e-1}}) \in k^e\colon\ x = \sum_{k=0}^{e-1} \pi^k x_k,$$

$$\forall\, f \in R[X]\ \exists!\, (\overline{f_0}, \ldots, \overline{f_{e-1}}) \in k[X]^e\colon\ f = \sum_{k=0}^{e-1} \pi^k f_k,$$

and f is a unit in $R[X]$ if and only if f_0 is a unit in $k[X]$.

P r o o f. Since R contains only one nonzero prime ideal, the nilradical of R is its maximal ideal $\mathrm{Nil}(R) = \pi R$. It follows that π is nilpotent. Let e be its index of nilpotency. Now for any $x \in R$, there is a unique $\overline{x_0} \in k = R/\pi R$ such that $\overline{x} = \overline{x_0}$. Then $x - x_0 \in \pi R$, namely there exists $x_0' \in R$ such that $x = x_0 + \pi x_0'$. By the same method, there exists a unique $\overline{x_1} \in k$ such that $\overline{x_0'} = \overline{x_1}$. Then $x = x_0 + \pi x_1 + \pi^2 x_1'$, where $x_0' - x_1 = \pi x_1'$. By induction we conclude that there exists a unique $(\overline{x_0}, \overline{x_1}, \ldots, \overline{x_{e-1}}) \in k^e$ such that $x = x_0 + \pi x_1 + \ldots + \pi^{e-1}x_{e-1}$ since $\pi^e = 0$. Notice that R is local. Then x is a unit in R if and only if $\overline{x} \neq 0$ in k if and only if $x_0 \neq 0$. Now let $f(X) = a_0 + a_1X + \ldots + a_nX^n \in R[X]$ and $a_k = a_{0,k} + \pi a_{1,k} + \ldots + \pi^{e-1}a_{e-1,k}$ for each $k \in \{0, \ldots, n\}$. Then $f = f_0 + \pi f_1 + \ldots + \pi^{e-1}f_{e-1}$, where $f_i(X) = a_{i,0} + a_{i,1}X + \ldots + a_{i,n}X^n$ for each $i \in \{0, \ldots, e-1\}$. Notice that $f = f_0 + \pi F$ for some $F \in R[X]$. If f_0 is a unit and g_0 is its inverse, then $f \sum_{k=0}^{e-1} (-1)^k f_0^{e-k-1} (\pi F)^k = f_0^e + (-1)^{e-1}(\pi F)^e = f_0^e$, then $fg = 1$, where $g = g_0^e \sum_{k=0}^{e-1} (-1)^k f_0^{e-k-1} (\pi F)^k$. Conversely, if f is a unit, then there exists a polynomial g such that $fg = 1$. Let $f = f_0 + \pi F$ and $g = g_0 + \pi G$ for some F and G in $R[X]$. Then $f_0 g_0 = 1$. This completes the proof. □

E x a m p l e 2.2. The ring $\mathbb{Z}/3^5\mathbb{Z}$ is a SPIR, where $\pi = 3$, $3\mathbb{Z}/3^5\mathbb{Z}$ is its maximal ideal and $e = 5$ its index of nilpotency. We get for example:

$$\overline{114} = \overline{0} + \overline{23} + \overline{03}^2 + \overline{13}^3 + \overline{13}^4.$$

Lemma 2.3. *Let R be a commutative ring with unity. Then R is a SPIR if and only if it is not an integral local principal ideal ring.*

P r o o f. If R is a SPIR, $\mathrm{Nil}(R) \neq 0$ is its maximal ideal. Let $\mathrm{Nil}(R) = \pi R$. Then π is nilpotent, then R is not integral. Conversely, if R is not an integral local principal ideal ring, let πR be its maximal ideal and suppose that π is not nilpotent. Lemma 2.1 shows that for any element $x \in R$ there exist a unique integer p and a unique family $(x_i)_{0 \leqslant i \leqslant p}$ in k such that $x = \sum_{i=0}^{p} x_i \pi^i$ and x_p is a unit. Since R is not integral, there exist $x \neq 0$ and $y \neq 0$ such that $xy = 0$. By Proposition 2.1 we have $x = \sum_{i=0}^{p} x_i \pi^i$ and $y = \sum_{i=0}^{q} y_i \pi^i$. Then the $(p+q)$-th entry is $x_p y_q$, which is a unit. By the unicity of Hensel's development, we should get $x_p y_p = 0$. This is a contradiction. Then π is nilpotent. This shows that $\pi R = \mathrm{Nil}(R)$ and R contains a unique prime ideal. Hence, R is a special principal ideal ring. □

Lemma 2.4. *Let k be a field. Then $R = k[X]/(X^e)$ is a SPIR of length e with k its residual field and XR its maximal ideal.*

P r o o f. Since k is a field, $k[X]$ is a principal ideal ring and so is R. Moreover, let $s \notin XR$. Then there exist $a \in k[X]$ and $b \in k$ such that $s = \overline{aX + b}$ and $b \neq 0$. We have that $\overline{aX}$ is a nilpotent element in R and $\overline{b}$ is a unit in R. Then s is a unit in R. Therefore, R is a local ring and XR is its maximal ideal and its index of nilpotency is e. Since R is not integral, it is a SPIR of length e. □

E x a m p l e 2.5. $\mathbb{C}[X]/(X^e)$ and $\mathbb{R}[X]/(X^e)$ are two SPIRs of length e.

Lemma 2.6 (Lemma 23, [4])**.** *Let $(R, \pi R, k, e)$ be a SPIR and $f(X) = a_n X^n + \ldots + a_1 X + a_0 \in R[X]$. The following statements are equivalent:*

(1) *f is regular (if $xf = 0$, then $x = 0$, where $x \in R$).*
(2) *f is primitive ($(a_n, \ldots, a_1, a_0) = R$).*
(3) *There is $i \in \{0, \ldots, n\}$ such that a_i is unit.*
(4) *$f_0 \neq 0$ (f_0 obtained by Hensel's development 2.1).*
(5) *$\overline{f} \neq \overline{0}$ in $k[X]$.*

Lemma 2.7. *Let $(R, \pi R, k, e)$ be a SPIR of length e. Then the ideals of R are*

$$0 = \pi^e R \subset \pi^{e-1} R \subset \ldots \subset \pi R \subset R.$$

P r o o f. Let k be a positive integer $0 < k < e$, and I be an ideal of R such that $\pi^{k+1}R \subseteq I \subsetneq \pi^k R$. Then for any element $x \in I$, $x = \pi^k x'$ for some $x' \in R$. If $x' \in \pi R$, then $x \in \pi^{k+1}R$. Else, we get that x' is a unit in R, thus $\pi^k \in I$ and $I = \pi^k R$, which is impossible. Therefore, $I = \pi^{k+1}R$. It follows that the ideals of R are all of the form $\pi^k R$. □

Since R contains a finite number of ideals, it is a complete ring (see [6], page 182). As well, Theorem 2.3 in [9] shows that R is a Henselian ring, that is, a ring in which Hensel's lemma holds (see [1]).

Lemma 2.8 (Hensel's lemma, Theorem 7.18 in [6])**.** *Let R be a complete local Noetherian ring and f be in $R[x]$ such that $\overline{f} = g_1 \dots g_k$ in $k[x]$, where $g_1, \dots, g_k$ are pairwise coprime polynomials in $k[x]$. Then there is $G_1, \dots, G_k \in R[x]$ such that $f = G_1 \dots G_k \in R[x]$, $\overline{G_i} = g_i$ for all $i \in \{1, \dots, k\}$.*

3. Main results

Theorem 3.1. *Let $(R, \pi R, k, 2)$ be a SPIR of length 2 with πR its maximal ideal and k its residual field. A primitive polynomial f is irreducible in $R[X]$ if and only if it satisfies one of the following statements:*

(1) *There exist f_0 and f_1 in $k[X]$ and $p \geqslant 2$ a positive integer such that $f = f_0^p + \pi f_1$, f_0 is an irreducible polynomial in $k[X]$ and f_0 does not divide f_1.*
(2) *$\overline{f}$ is irreducible in $k[X]$.*

P r o o f. Let $f = f_0^p + \pi f_1$ be Hensel's development 2.1 such that f_0 is an irreducible polynomial in $k[X]$ and f_0 does not divide f_1. Let $f = gh$ with $g = g_0 + \pi g_1$ and $h = h_0 + \pi h_1$ being Hensel's development 2.1 of g and h. Then

$$f_0^p = g_0 h_0, \quad f_1 = g_0 h_1 + g_1 h_0.$$

Since f_0 is irreducible, g_0 and h_0 are either units or are divisible by f_0. If g_0 and h_0 are both divisible by f_0, then f_0 divides f_1; this is a contradiction since we have assumed that f_0 does not divide f_1. Then either g_0 is a unit or h_0 is a unit. Therefore, by Proposition 2.1 either g is a unit or h is a unit. Thus, f is irreducible in $R[X]$.

For the second statement, suppose now that $\overline{f}$ is irreducible in $k[X]$. Let $f = gh$ for some polynomials g and h in $R[X]$. By Hensel's development 2.1, $f = f_0 + \pi f_1$, $g = g_0 + \pi g_1$ and $h = h_0 + \pi h_1$. Then

$$f_0 = g_0 h_0, \quad f_1 = g_0 h_1 + g_1 h_0.$$

Since $\overline{f}$ is irreducible in $k[X]$, f_0 is irreducible, then either g_0 is a unit or h_0 is a unit. Therefore, by 2.1 either g is a unit or h is a unit. It follows that f is irreducible.

Conversely, suppose f is irreducible in $R[X]$ and assume $\overline{f}$ is not irreducible in $k[X]$. If $\overline{f}$ is not primary, Hensel's lemma 2.8 yields that f is not irreducible. This contradicts the fact that f is irreducible.

Suppose f is irreducible in $R[X]$. Then there exists an irreducible polynomial f_0 in $k[X]$ such that $\overline{f} = f_0^p$ for a positive integer $p \geqslant 2$. Then Hensel's development 2.1 proves that $f = f_0^p + \pi f_1$ for a polynomial $f_1 \in k[X]$. It is enough to prove that f_0 does not divide f_1. Contrariwise, we put:

$$F = \frac{f_1}{f_0}, \quad g = f_0, \quad h = f_0^{p-1} + \pi F.$$

Then f is not irreducible since $f = gh$ and neither g nor h is a unit. This is a contradiction. So f_0 does not divide f_1. □

Corollary 3.2. *Let $(R, \pi R, k, 2)$ be a SPIR of length 2 with πR its maximal ideal, and k its residual field. We fix an irreducible polynomial f_0 in $k[X]$. Then irreducible polynomials in $R[X]$ such that f_0 divides $\overline{f}$ are*

(1) *$f = uf_0$, where u is a unit in $R[X]$,*
(2) *$f = u(f_0^p + \pi f_1)$, where p is a positive integer, f_1 is a coprime with f_0 in $k[X]$ and u is a unit in $R[X]$.*

Corollary 3.3. *Let $R = \mathbb{C}[Y]/(Y^2)$. Irreducible polynomials of $R[X]$ are*

(1) *$f = u(X + a)$, where $a \in \mathbb{C}$ and u is a unit in $R[X]$,*
(2) *$f = u((X - a)^p + Yf')$, where $a \in \mathbb{C}$, p is a positive integer, f' is a polynomial in $\mathbb{C}[X]$ such that $f'(a) \neq 0$ and u is a unit in $R[X]$.*

Corollary 3.4. *Let $R = \mathbb{R}[Y]/(Y^2)$. Irreducible polynomials of $R[X]$ are*

(1) *$f = u(X + a)$, where $a \in \mathbb{R}$ and u is a unit in $R[X]$,*
(2) *$f = u((X - a)^p + Yf')$, where $a \in \mathbb{R}$, p is a positive integer, f' is a polynomial in $\mathbb{R}[X]$ such that $f'(a) \neq 0$ and u is a unit in $R[X]$,*
(3) *$f = u(X^2 + aX + b)$, where $a, b \in \mathbb{R}$ such that $a^2 - 4b < 0$ and u is a unit in $R[X]$,*
(4) *$f = u((X^2 + aX + b)^p + Yf')$, where $a, b \in \mathbb{R}$ such that $a^2 - 4b < 0$, p is a positive integer, f' is a polynomial in $\mathbb{R}[X]$ which is not divisible by $X^2 + ax + b$ and u is a unit in $R[X]$.*

We can prove, by the same way as in the proof of the Theorem 3.1, a general result for every length e of R:

Theorem 3.5. *Let $(R, \pi R, k, e)$ be a SPIR of length e with πR its maximal ideal, and k its residual field. Let f be a primitive polynomial in $R[X]$. If $\overline{f}$ is irreducible in $k[X]$, then f is irreducible in $R[X]$.*

P r o o f. Assume $\overline{f}$ is irreducible in $k[X]$. Let $f = gh$ for some polynomials g and h in $R[X]$. By Hensel's development 2.1, $f = f_0 + \ldots + \pi^{e-1} f_{e-1}$, $g = g_0 + \ldots + \pi^{e-1} g_{e-1}$ and $h = h_0 + \ldots + \pi^{e-1} h_{e-1}$. Put $F = f_1 + \ldots + \pi^{e-2} f_{e-1}$, $G = g_1 + \ldots + \pi^{e-2} g_{e-1}$ and $H = h_1 + \ldots + \pi^{e-2} h_{e-1}$. Then

$$f_0 = g_0 h_0, \quad f_1 = g_0 H + G h_0.$$

Since $\overline{f}$ is irreducible in $k[X]$, f_0 is irreducible, then either g_0 is a unit or h_0 is a unit. Therefore, by Hensel's development 2.1, either g is a unit or h is a unit. It follows that f is irreducible. □

Corollary 3.6. *Let $R = \mathbb{C}[Y]/(Y^e)$ for a positive integer $e > 1$. For any $a \in \mathbb{C}$ and any $g \in R[X]$ satisfying $g(a) \neq 0$, the polynomial $f = (X - a) + Yg$ is irreducible in $R[X]$.*

Corollary 3.7. *Let $R = \mathbb{R}[Y]/(Y^e)$ for a positive integer $e > 1$. For any $a, b \in \mathbb{C}$ verifying $a^2 - 4b < 0$, for any $g \in R[X]$ satisfying $g(a) \neq 0$ and for any $h \in R[X]$ not divisible by $(X^2 + aX + b)$, polynomials $f = (X - a) + Yg$ and $f' = (X^2 + aX + b) + Yh$ are irreducible in $R[X]$.*

References

[1] *G. Azumaya*: On maximally central algebras. Nagoya Math. J. *2* (1951), 119–150. zbl MR doi
[2] *E. R. Berlekamp*: Algebraic Coding Theory. McGraw-Hill, New York, 1968. zbl MR doi
[3] *W. C. Brown*: Matrices Over Commutative Rings. Pure and Applied Mathematics 169. Marcel Dekker, New York, 1993. zbl MR
[4] *M. E. Charkani, B. Boudine*: On the integral ideals of $R[X]$ when R is a special principal ideal ring. São Paulo J. Math. Sci. *14* (2020), 698–702. zbl MR doi
[5] *B. Chor, R. L. Rivest*: A knapsack-type public key cryptosystem based on arithmetic in finite fields. IEEE Trans. Inf. Theory *34* (1988), 901–909. zbl MR doi
[6] *D. Eisenbud*: Commutative Algebra: With a View Toward Algebraic Geometry. Graduate Texts in Mathematics 150. Springer, Berlin 1995. zbl MR doi
[7] *D. Hachenberger, D. Jungnickel*: Irreducible polynomials over finite fields. Topics in Galois Fields. Algorithms and Computation in Mathematics 29. Springer, Cham, 2020, pp. 197–239. doi
[8] *M. O. Rabin*: Probabilistic algorithms in finite fields. SIAM J. Comput. *9* (1980), 273–280. zbl MR doi
[9] *C. Rotthaus*: Excellent rings, Henselian rings and the approximation property. Rocky Mt. J. Math. *27* (1997), 317–334. zbl MR doi

Author's address: *Brahim Boudine*, Faculty of Sciences Dhar El Mahraz, University Sidi Mohamed Ben Abdellah, Fez, Morocco, e-mail: brahimboudine.bb@gmail.com.