Universidad del Atlántico

MATUA

Revista MATUA Páginas: 102–107

Facultad de Ciencias Básicas
©Programa de Matemáticas
Vol. VII , № 1, (2020)

Received 16 Jul 2020; Approved 01 Oct 2020

Algunas propiedades de $\mathbb{Z}_n[x]$ siendo n no necesariamente primo

Some properties of $\mathbb{Z}_n[x]$ being n not necessarily prime

Primitivo Acosta-Humánez

Instituto Superior de Formación Docente Salomé Ureña - ISFODOSU

primitivo.acosta-humanez@isfodosu.edu.do

Resumen

En este artículo se presentan algunos resultados originales y elementales relacionados con algunas propiedades de polinomios mónicos con coeficientes en $\mathbb{Z}_n$, siendo n no necesariamente primo. En particular se introduce una función para calcular el número de raíces de tales polinomios. Este artículo está basado en la tesis de grado ”Grupos Diedros y del Tipo (p,q)”([2]), presentada por el autor bajo la dirección de Jairo Charris Castañeda y Jesús Hernando Pérez (Pelusa).

Palabras claves:
Anillos, polinomios, teorema chino del resto.

Abstract

In this paper we present some originals and elementary results related with some properties of monic polynomials with coefficients belonging to $\mathbb{Z}_n$, where n is not prime. In particular we introduce a function to compute the number of roots of such polynomials. This paper is based on the BS thesis ”Grupos Diedros y del Tipo (p,q)”([2]), written by the author under the supervision of Jairo Charris Castañeda and Jesús Hernando Pérez (Pelusa).

Keywords:
Rings, polynomials, chinese remainder theorem.

1. Introduction

This paper is an slightly improvement, translated to English, of the first part of the bachelor dissertation [2]), which was published recently in the book ”Memorias Grandes Maestros de la Matemática en Colombia", edited by Ivan Castro and Fernando Zalamea, see [1]. Other sequel paper correspond to [3] and see also [4, 5, §11].

We understand the readers are familiarized with some basic concepts related to number theory and group theory, see [4, 5]. We start setting the following notations: by φ we means the Euler's totient function, also called the Euler's φ function. By $U(\mathbb{Z}_n)$ we means the multiplicative group of the roots of unity in $\mathbb{Z}_n$.

Concerning the results of the paper, we can say that each one of them is elementary and original. To present the results we start introducing the notation $ch(f, n, m)$ to mean the number of the roots of the polynomial $f(x) \in \mathbb{Z}_n$, being $\mathrm{grad}(f(x)) = m \geq 0$. To honor Jairo Charris, teacher, friend and mentor, the notation $ch(f, n, m)$ is read as *the Charris of polynomial f of degree m belonging to $\mathbb{Z}_n[x]$*.

The main results of this paper are summarized as follows:

Theorem 2.1 *Let $k = \prod_{i=1}^{r} k_i$ such that k_i is a positive integer for $i = 1, 2, \ldots, r$, $\gcd(k_i, k_j) = 1$, then, $ch(f, k, n) = \prod_{i=1}^{r} ch(f, k_i, n)$.*

Theorem 2.2 *Let q, be no necessarily prime, p be a prime and $U(\mathbb{Z}_q)$ be the multiplicative group of roots of unity in $\mathbb{Z}_{||}$. Then $p|\varphi(q)$, if and only if, there exists $a \in \mathbb{Z}$ such that $\overline{a} \in U(||)$ and $|\overline{a}| = p$, and we can suppose that $1 \leq a \leq q$. Furthermore, if $H = [\overline{a}]$, then, $H = [\overline{a}^l]$ for all $1 \leq l \leq p-1$ with $\gcd(l, p) = 1$. Finally, if $U(\mathbb{Z}_q)$ is cyclic and $b \in \mathbb{Z}$ is such that $\overline{b} \in U(\mathbb{Z}_q)$ and that $|\overline{b}| = p$, there exist $1 \leq l \leq p-1$ with $\gcd(l, p) = 1$ such that $b \equiv a^l (\mod q)$.*

Theorem 2.3 *If q is prime, then, $U(\mathbb{Z}_q)$ is cyclic, also $U(\mathbb{Z}_q) = \mathbb{Z}_q^* = \mathbb{Z}_q - \{0\}$.*

Theorem 2.4 *The group $U(\mathbb{Z}_q)$ is a cyclic group if and only if q is some of the numbers $2, 4, p^k$ either $2p^k$ with p odd prime.*

Theorem 2.5 *Let G a group of order pq where $p < q$ are prime numbers. Then $p|q-1$, if and only if, there exists $\overline{a} \in \mathbb{Z}_q^*$ such that $|\overline{a}| = p$, and we can suppose that $1 \leq a < q$. If besides, $H = [\overline{a}]$ is subgroup $\mathbb{Z}_q^*$ generate for $\overline{a}$, then, $H = [a^l]$ for all $1 \leq l \leq p-1$ with $gcd(l, p) = 1$. Finally, if $b \in \mathbb{Z}$ is such that $\overline{b} \in U(\mathbb{Z}_q)$ and that $|\overline{b}| = p$, there exist $1 \leq l \leq p-1$ with $\gcd(l, p) = 1$ such that $b \equiv a^l (\mod q)$.*

We hope that this paper can motivate students to wonderful world of polynomials in $\mathbb{Z}_n[x]$.

2. Some properties of $\mathbb{Z}_n[x]$.

In this section we analyze some properties of $\mathbb{Z}_n$.

Let $n \geq 1$ an integer, not necessarily prime, and consider the ring $(\mathbb{Z}_n, +, \cdot)$. Consider $f(x), g(x) \in \mathbb{Z}_n[x]$, where $g(x)$ is monic. Then there $q(x) \in \mathbb{Z}_n[x]$ and $r(x) \in \mathbb{Z}_n[x]$, with $deg(r(x)) < deg(g(x))$, such that

$$f(x) = q(x)g(x) + r(x)$$

If $deg(g(x)) > deg(f(x))$, then for $g(x)$ monic we have that $q(x) = 0$ and $r(x) = f(x)$. From elsewhere $deg(g(x)) \leq deg(f(x))$ and $g(x)$ is monic then

$$f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{n} b_i x^i$$

with $a_n \neq 0, b_m = 1, m \leq n$, where $m = deg(g(x))$ and $n = deg(f(x))$. To proceed by induction on $n = deg(f(x))$, if $n = 0$, then $m = 0$, $f(x) = a_0$, $g(x) = 1$. Let $q(x) = a_0 \cdot 1 = a_0$ and $r(x) = 0$, then, $deg(r(x)) < deg(g(x))$ and $f(x) = q(x)g(x) + r(x) = a_0 \cdot 1 + 0 = a_0$. Now suppose that the lemma is true for polynomials of degree less that $n = deg(f(x))$. A simple calculation shows that the polynomial $(a_n x^{n-m})g(x)$ have degree n and leading coefficient a_n. So

$$f(x) - (a_n x^{n-m})g(x) = \sum_{i=0}^{n} a_i x^i - \sum_{i=0}^{m} a_n b_i x^{n-m+i}, b_m = 1$$

is a polynomial of degree less that n. By hypothesis of induction there polynomials $q'(x)$ and $r(x)$ such that

$$f(x) - (a_n x^{n-m})g(x) = q'(x)g(x) + r(x) \text{ and } deg(r(x)) < deg(g(x)),$$

however, if $q(x) = a_n x^{n-m} + q'(x)$, then

$$f(x) = (a_n x^{n-m})g(x) + q'(x)g(x) + r(x) = q(x)g(x) + r(x).$$

Now see the uniqueness of $q(x)$ and $r(x)$. Suppose that $f(x) = q_1(x)g(x) + r_1(x)$ and that $f(x) = q_2(x)g(x) + r_2(x)$, then $(q_1(x) - q_2(x))g(x) = (r_2(x) - r_1(x))$ and as $b_m = 1$, $deg((q_1(x) - q_2(x))g(x)) = deg(q_1(x) - q_2(x)) + deg(g(x)) = deg(r_2(x) - r_1(x))$

$$deg(r_2(x) - r_1(x)) \leq \text{máx}(deg(r_1(x)), deg(r_2(x))) < deg(g(x))$$

is true, if and only if, $deg(q_1(x) - q_2(x)) = -\infty = deg(r_2(x) - r_1(x))$, which indicates that $q_1(x) - q_2(x) = 0$ and $r_2(x) - r_1(x) = 0$; therefore $q_1(x) = q_2(x)$ and $r_2(x) = r_1(x)$ Let $f(x) \in \mathbb{Z}_n[x], a \in \mathbb{Z}_n$. Then $f(x) = q(x)(x - a) + f(a)$, where $q(x) \in \mathbb{Z}_n[x]$ and n not necessarily prime If $f(x) = 0$ then $q(x) = 0$. Suppose that $f(x) \neq 0$. The previous lemma says that exist polynomials uniques $q(x), r(x) \in \mathbb{Z}_n[x]$ and n not necessarily prime such that $f(x) = q(x)(x - a) + r(x)$ and $deg(r(x)) < deg(x - a) = 1$, then $r(x) = r$ is a polynomial constant (possibly zero)

$$\text{if } q(x) = \sum_{j=0}^{n-1} b_j x^j \text{ then } f(x) = q(x)(x - a) + r;$$

$$f(x) = -b_o a + b_{n-1} x^n + r + \sum_{k=1}^{n-1} (-b_k a + b_{k-1}) x^k$$

where

$$f(a) = -b_o a + b_{n-1} a^n + r + \sum_{k=1}^{n-1} (-b_k a + b_{k-1}) a^k$$

$$= -\sum_{k=0}^{n-1} b_k a^{k+1} + \sum_{k=1}^{n} b_{k-1} a^k + r = -\sum_{k=1}^{n} b_{k-1} a^k + \sum_{k=1}^{n} b_{k-1} a^k + r = r.$$

Then $f(x) = q(x)(x-a) + f(a)$. Can see that if $f(x) \in \mathbb{Z}_n[x]$ and $deg(f(x)) = m \geq 1$, then not necessarily $f(x)$ has at most m roots in $\mathbb{Z}_n[x]$. Sufficient to consider the following counterexample: if $f(x) = (2x+2)^2 \in \mathbb{Z}_4[x]$ and $deg(f(x)) = 2$, then, $f(x)$ has four roots $0, 1, 2, 3 = \mathbb{Z}_4[x]$. If n is prime, the assertion is true as shown in the following lemma.

Also shows that when n is not prime, $x^m - \overline{1}$ has at most m distinct roots in $\mathbb{Z}_n$. simply take the following counterexample, if $f(x) = x^2 - 1 \in \mathbb{Z}_8[x]$, $f(x)$ is roots $1, 3, 5, 7$. If n is prime, the assertion is true, as shown in the following lemma. In what follows in this chapter, the notation will be used $ch(f, n, m)$ to indicated the number of roots of polynomial $f(x) \in \mathbb{Z}_n$ with $deg(f(x)) = m \geq 0$. This notation is adopted as a tribute to Professor Charris.

The following theorem is an application of Chinese Remainder Theorem, and generalizes the two previous lemmas.

Theorem 2.1. *Let* $k = \prod_{i=1}^{r} k_i$ *such that* k_i *is a positive integer for* $i = 1, 2, \ldots, r$, $\gcd(k_i, k_j) = 1$*, then,* $ch(f, k, n) = \prod_{i=1}^{r} ch(f, k_i, n)$.

suppose that $f(a) = 0$ with $a \in \mathbb{Z}_{k_i}$ for each $i = 1, 2, \ldots, r$. For the Chinese Remainder Theorem, there exist a integer a such that $a \equiv a_i(modk_i)$ for each $i = 1, 2, \ldots, r$ and a is unique module k. Therefore, for each $i = 1, 2, \ldots, r$ we have $f(a) \equiv f(a_i) \equiv 0(modk_i)$ and as any solution of the congruence polynomial $f(x) \equiv 0(modk)$ is solution of the system $f(x) \equiv 0(modk_i)$ for each $i = 1, 2, \ldots, r$, then $f(a) = 0,\ a \in \mathbb{Z}_k$. And so we can build all the roots of $f(x) \in \mathbb{Z}_k$ and we can choose a_1 of $ch(f, k_1, n)$ forms, a_2 of $ch(f, k_2, n)$ forms and successively $ch(f, k, n) = \prod_{i=1}^{r} ch(f, k_i, n)$, as we wanted to test If $k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where p_i is prime, $i = 1, \ldots, r$ we can take $k_i = p_i^{\alpha_i}$ in the previous theorem and we see that the problem of finding roots of a polynomial of $\mathbb{Z}_n[x]$ is reduced to use the fundamental theorem of arithmetic. Similarly shows that ch is a homomorphism (of monoids by setting f y n) of $\mathbb{Z}^+$ to $\mathbb{Z}^+$

Let $k = \prod_{i=1}^{r} k_i$ such that k_i is a integer positive for each $i = 1, \ldots, r$, $\gcd(k_i, k_j) = 1$ for $i \neq j$, then, the number of roots of the unity in $\mathbb{Z}_k$ is the product number of roots of the unity in $\mathbf{Z}_{k_i}$ for each $i = 1, 2 \ldots, r$. sufficient to take in the theorem previous a $x^m - 1$ in place of $f(x)$ If $k \geq 3$, $f(x) = x^2 - 1$, then $ch(f, 2^k, 2) = 4$ Is consequence immediate of theorem 1.1. and of corollary 1.1. Given $m \geq 1$, $k \geq 1$ and p a prime number odd, then, $x^m - \overline{1}$ has at most m roots different in $\mathbb{Z}_n$, if and only if, n is any of the numbers $2, 4, p^k$ either $2p^k$. $\varphi(2) = 1$, $\varphi(4) = 2$, $\varphi(p^k) = \varphi(2p^k) = (p-1)p^{k-1}$. the converse is an immediate consequence of corollary 2.1. Let G an abelian finite group and for each $n \in \mathbb{Z}^+$, are G^n and G_n two subsets of G, defined as follows:

$$G^n = \{a^n \mid a \in G\}, \quad G_n = \{a \in G \mid a^n = e\},$$

then G^n and G_n are both subgroups G and

$$G/G_n \approx G^n.$$

$a^n,\ b^n \in G^n$, then $b^{-n} = (b^n)^{-1} \in G^n$ and therefore, $(b^{-1}a)^n = a^n(b^{-1})^n = a^n(b^n)^{-1} \in G$ and therefore, $G^n \leq G$. The same form, if $a,\ b \in G_n$, then $a^n = e$, $b^n = e$, $b^{-n} = (b^{-1})^n = (b^n)^{-1} = e$ and consequence, $(b^{-1}a)^n = a^n(b^{-1})^n = a^n(b^n)^{-1} = e \in G_n$ and therefore, $G_n \leq G$. $f : G \to G'$ such that $a \mapsto a^n$, then $Im(f) = G^n$ and $Ker(f) = G_n$, applying the first isomorphism theorem must be $G/Ker(f) \approx Im(f)$ and therefore $G/G_n \approx G^n$ If, in the lemma 2.5. $n| \circ (G)$, then, also, $n| \circ (G_n)$ Is consequence of lemma 1.5. and theorem of classification of abelian finite groups. Let G, G^n and G_n defined as on the lemma 1.5, G abelian. If for all $n \in \mathbb{Z}$, $n \geq 1$ have that $\circ(G_n) \leq n$, then $\circ(G_n) = n$ for all n such that $n|\circ(G)$ For the lemma 2.6 have that $\circ(G_n) = nk$ for some $k \in \mathbb{Z}^+$ an as $\circ(G_n) \leq n$, then $k = 1$ and $\circ(G_n) = n$ Let p prime and G a $p-$abelian group. Then, for all $n \in \mathbb{Z}^+$, $\circ(G_n) \leq n$, then G is cyclic Is consequence of the fact that $\circ(G) = p^m$ for some $m \geq 1$ and that for all prime p, all $p-$ subgroup of Sylow of G is cyclic. Generalizing the previous theorem for any abelian finite group, have: If G is an abelian finite group such that for all $n \in \mathbb{Z}^+$, $\circ(G_n) \leq n$, then G is cyclic. As G is a abelian group finite such that for all $G_n = \{a \in G | a^n = e\}$ where the number of elements fails to n, then $G = [a] = \{a^n | n \in \mathbb{Z}\}$ with $G_n \leq G$ If G is a cyclic finite group, then, $\circ(G_n) \leq n$ and if $n| \circ (G)$ then $\circ(G_n) = n$ $G = [a] = \{a^n | n \in \mathbb{Z}\}$ and as $G_n = \{a \in [a] | a^n = e\}$ and therefore $\circ(G_n) \leq n$. Now, if $n| \circ (G)$, then, $\circ(G) = n[a]$ and so $\circ(G_n) = n$ If G is a cyclic finite group, for all $n \in \mathbb{Z}$, $n \geq 1$, such that $n| \circ (G)$, G have an unique subgroup H of order n, which is cyclic $G = [a] = \{a^n | n \in \mathbb{Z}\}$, then, $\circ(G) = |a| = m$, where $n|m$ and therefore $|a^n| = \frac{m}{n}$. Let $d = \frac{m}{n}$, then $H = [a^d]$ is a subgroup of order n. Suppose now that exist b such that $H = [a^b]$ is a subgroup of order n, where b is the smallest positive integer such that $a^b \in H$. As $\frac{m}{d} = n = \circ(H) = |a^b|$, then $d|b$ and therefore $H = [a^b] \leq [a^d]$, where $\circ([a^d]) = n = \circ(H)$ and so $H = [a^d]$.

Theorem 2.2. *Let q, be no necessarily prime, p be a prime and $U(\mathbb{Z}_q)$ be the multiplicative group of roots of unity in $\mathbb{Z}_{\shortparallel}$. Then $p|\varphi(q)$, if and only if, there exists $a \in \mathbb{Z}$ such that $\overline{a} \in U(\shortparallel)$ and $|\overline{a}| = p$, and we can suppose that $1 \leq a \leq q$. Furthermore, if $H = [\overline{a}]$, then, $H = [\overline{a}^l]$ for all $1 \leq l \leq p-1$ with $\gcd(l,p) = 1$. Finally, if $U(\mathbb{Z}_q)$ is cyclic and $b \in \mathbb{Z}$ is such that $\overline{b} \in U(\mathbb{Z}_q)$ and that $|\overline{b}| = p$, there exist $1 \leq l \leq p-1$ with $\gcd(l,p) = 1$ such that $b \equiv a^l (\mod q)$.*

Is consequence of the definition of $U(\mathbb{Z}_q)$ an of order of $U(\mathbb{Z}_q)$

Theorem 2.3. *If q is prime, then, $U(\mathbb{Z}_q)$ is cyclic, also $U(\mathbb{Z}_q) = \mathbb{Z}_q^* = \mathbb{Z}_q - \{0\}$.*

Is consequence of lemma 1.2 and of fact that $U(\mathbb{Z}_q)$ is generate any of its element Note that, under the hypothesis of the theorem above, if $p < q$ and $p|q-1$, the equation $x^p = \overline{1}$ have a set complete of different solutions in $\mathbb{Z}_q^*$(i.e, p different solutions, the only possible.)
can easily see that $U(\mathbb{Z}_{14})$ is cyclic, while $U(\mathbb{Z}_{16})$ is not cyclic. Now we generalize the theorem 1.3.

Theorem 2.4. *The group $U(\mathbb{Z}_q)$ is a cyclic group if and only if q is some of the numbers $2, 4, p^k$ either $2p^k$ with p odd prime.*

Suppose that q is none of the above forms. We can considerate 2 cases:

1. $q = 2^r \prod_{i=1}^{k} p_i^{\alpha_i}$ with $k \geq 2$ or with $k = 1$ and $r \geq 2$.
2. $q = 2^k$ with $k \geq 3$.

see that in neither case $U(\mathbb{Z}_q)$ is cyclic. In the first case, $p_1^{\alpha_1} > 2$ and $q/p_1^{\alpha_1} > 2$, then $2|\varphi(p_1^{\alpha_1})$ and $2|\varphi(q/p_1^{\alpha_1})$. As $a^{\varphi(p_1^{\alpha_1})} \cong 1(\mod p_1^{\alpha_1})$ y $a^{\varphi(q/p_1^{\alpha_1})} \equiv 1(\mod q/p_1^{\alpha_1})$ have that $a^{\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(q/p_1^{\alpha_1})} \cong 1(\mod p_1^{\alpha_1})$ y $a^{\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(q/p_1^{\alpha_1})} \cong 1(\mod q/p_1^{\alpha_1})$ and therefore $a^{\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(q/p_1^{\alpha_1})} \equiv 1(\mod q)$. Then if $a \in U(q)$, then $|a| \leq \frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(q/p_1^{\alpha_1}) = \frac{\varphi(q)}{2} < \varphi(q)$ and therefore $U(q)$ can't be cyclic. In the second case, if $\gcd(a,q) = 1$, where $n = 2^k$, then, a is odd of the form $a = 1 + 2b$ and we have $a^2 = 1 + 4b + b^2 = 1 + 2^3c$, $a^4 = 1 + 2^4d$, $a^8 = 1 + 2^5e$, in general for an argument inductive, if $j \geq$, then $a^{2^{j-2}} = 1 + 2^j g \equiv 1(\mod 2^j)$. and therefore, $a^{2^{k-2}} \equiv 1(\mod 2^k)$ and if $a \in U(2^k)$, then, $|a| \leq 2^{k-2} < 2^{k-1} = \varphi(2^k)$, which implies that $U(2^k)$ can't be cyclic.
to prove the converse, you have to clarament that $U(2) = \{1\}$, $U(4) = \{1, 3\}$ are cyclic groups. Also for the theorem 1.3, $U(p)$ is cyclic. We see now that $U(p^k)$ is cyclic if $k > 1$. Let $k = q + 1$. Should be found in $U(p^{q+1})$ an element of order $\varphi(p^{q+1}) = (p-1)p^q$. Choosing $a^p(p+1)$ where a is a generator of $U(p)$, $t = |a^p(p+1)|$ in $U(p^{q+1})$, then $t|U(p^{q+1}) = (p-1)p^q$. As $a^p(p+1) \equiv a^p \equiv a(\mod p)$, then, $|a| = p-1$ in $U(p)$ and $(a^p(p+1))^t \equiv 1(\mod p^{q+1}) \equiv 1(\mod p)$, since $t|(p-1)p^q$ and $p-1|t$, then, $t = p^k(p-1)$, As $(a^p(p+1))^{p^{q-1}(p-1)} \equiv (1+p)^{p^{q-1}(p-1)} \mod p^{q+1}$, then $(a^p(p+1))^{p^{q-1}(p-1)} \not\equiv 1(\mod p^{q+1})$ since $1+p$ have order p^q in $U(p^{q+1})$. Therefore $t \nmid p^{q-1}(p-1)$, and necessarily $t = p^q(p-1)$ as wanted

Theorem 2.5. *Let G a group of order pq where $p < q$ are prime numbers. Then $p|q-1$, if and only if, there exists $\overline{a} \in \mathbb{Z}_q^*$ such that $|\overline{a}| = p$, and we can suppose that $1 \leq a < q$. If besides, $H = [\overline{a}]$ is subgroup $\mathbb{Z}_q^*$ generate for $\overline{a}$, then, $H = [a^l]$ for all $1 \leq l \leq p-1$ with gcd$(l,p) = 1$. Finally, if $b \in \mathbb{Z}$ is such that $\overline{b} \in U(\mathbb{Z}_q)$ and that $|\overline{b}| = p$, there exist $1 \leq l \leq p-1$ with $\gcd(l,p) = 1$ such that $b \equiv a^l(\mod q)$.*

Is consequence of theorems 1.2. and 1.4.

Referencias

[1] P.B Acosta-Humánez, *Algunas observaciones sobre polinomios mónicos con coeficientes en el anillo* $\mathbb{Z}_n$, in Memorias Grandes Maestros de la Matemática en Colombia 02 Jairo Charris, Editors Ivan Castro and Fernando Zalamea, 2018, pp. 213–223.

[2] P.B Acosta-Humánez, *Grupos Diedros y del Tipo* (p,q) . Trabajo de Grado presentado como requisito para optar al título de Matemático, Bogotá, Universidad Sergio Arboleda, 2004.

[3] P.B Acosta-Humánez, *Teoremas de isomorfía en grupos diedros*. Lecturas Matemáticas, **24** (2003), 123–136

[4] J. Charris, B. Aldana and P.B. Acosta-Humánez, *Algebra I. Fundamentos y Teoría de los Grupos*, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 2005.

[5] J. Charris, B. Aldana and P.B. Acosta-Humánez, *Algebra. Fundamentos, Grupos, Anillos, Cuerpos y Teoría de Galois*, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 2013.