Matemáticas y sus aplicaciones 7, Textos Científicos, Fomento Editorial de la Benemérita Universidad Autónoma de Puebla, ISBN: 978-607-525-135-6

Capítulo 2

El lema de Hensel y el levantamiento de Hensel

Ángel Raúl García Ramírez, Carlos Alberto López Andrade
FCFM, BUAP

Resumen

El Lema de Hensel es una herramienta utilizada en la teoría de números, geometría y topología algebraica, siendo la factorización de polinomios el objetivo principal de su uso. Desarrollado por Kurt Hensel quien introdujo los números p-ádicos, nos muestra un método para hallar factorizaciones de polinomios mónicos, factorizándolos sobre un campo finito de característica un primo p y después "levantando" dicha factorización sobre un anillo de clases residuales módulo una potencia de ese primo. Recientemente esta herramienta y el levantamiento de Hensel se han empleado en la Teoría de Códigos Algebraicos. En este trabajo se exhibe la demostración del Lema de Hensel para polinomios mónicos sobre el anillo $\mathbb{Z}_{p^s}$, así como del levantamiento de Hensel.

1 Introducción

En 1904 Kurt Hensel introdujo los números p-ádicos y el lema de Hensel en el artículo Neue Grundlagen der Arithmetik (cf. [6]). Cuatro años más tarde, en su libro Theorie der algebraischen Zahlen, Hensel mostró una versión más general de su lema. Recientemente, en los años 90 del siglo pasado, esta herramienta ha sido muy útil en el estudio de la caracterización de la estructura algebraica de los códigos cíclicos lineales sobre anillos finitos, por ejemplo; sobre anillos de Galois (cf. [5], [14], [7]) y sobre anillos finitos de cadena (cf. [3], [13], [11]). El levantamiento de Hensel está relacionado con la representación p-ádica de los elementos de un anillo de Galois ó de un anillo finito de cadena y tal representación es imprescindible en la definición de la función de Gray en esta clase de anillos finitos ([4], [1], [2], [17], [9], [10]). Se demostró en [5] a través de Hammons, et. al., que el código de Kerdock es la imagen de Gray de un código cíclico lineal extendido sobre $\mathbb{Z}_4$. Ellos usan este hecho para resolver un problema "viejo" dando la explicación de la dualidad formal entre dos códigos no lineales binarios, los famosos códigos de Kerdock y Preparata.

Definiciones y conceptos fundamentales sobre el anillo $\mathbb{Z}_{p^s}$, propiedades de los polinomios y de la divisibilidad en $\mathbb{Z}_{p^s}[x]$ son dados en la sección 2, la demostración

del Lema de Hensel se encuentra desarrollada en la sección 3 y finalmente la demostración del Levantamiento de Hensel se exhibe en la sección 4. Cabe mencionar que este capítulo de libro está inspirado en la lectura de la obra de Wan ([16]).

2 El anillo de polinomios $\mathbb{Z}_{p^s}[x]$

Sea p cualquier número primo, $s \in \mathbb{N}$ y $\mathbb{Z}_{p^s}$ el anillo de enteros módulo p^s, i.e.,

$$\mathbb{Z}_{p^s} = \frac{\mathbb{Z}}{p^s\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{p^s - 1}\}$$

con la suma y multiplicación usual de clases:

$$\begin{aligned} \overline{r}_1 + \overline{r}_2 &= \overline{r_1 + r_2} \\ \overline{r}_1 \, \overline{r}_2 &= \overline{r_1 r_2} \end{aligned} \tag{1}$$

para cada $\overline{r}_1, \overline{r}_2 \in \mathbb{Z}_{p^s}$.

Observación 2.1. Por la construcción del anillo cociente $\mathbb{Z}_{p^s}$ tenemos que $\overline{a}\overline{b} = \overline{c}$ sí y sólo si $ab \equiv c \mod p^s$.

Considérese el conjunto $\mathcal{S} = \{0, 1, \ldots, p^s - 1\} \subseteq \mathbb{N} \cup \{0\}$ y la función:

$$\begin{aligned} \phi : \mathbb{Z}_{p^s} &\longrightarrow \mathcal{S} \\ \overline{r} &\mapsto r \end{aligned}$$

Es claro que ϕ es biyectiva, entonces podemos inducir la estructura de anillo en el conjunto $\mathcal{S}$ definiendo las operaciones $\oplus$ y $\odot$ en $\mathcal{S}$ de la manera siguiente:

$$\begin{aligned} s_1 \oplus s_2 &:= \phi\left(\overline{r}_1 + \overline{r}_2\right) \\ s_1 \odot s_2 &:= \phi(\overline{r}_1 \cdot \overline{r}_2) \end{aligned}$$

para cada $s_1, s_2 \in \mathcal{S}$ siempre que $s_1 = \phi(\overline{r}_1)$ y $s_2 = \phi(\overline{r}_2)$ para algunos $\overline{r}_1$ y $\overline{r}_2$ en $\mathbb{Z}_{p^s}$.

Dadas estas operaciones, ϕ es un *isomorfismo* y, con esta identificación, usaremos cuando sea conveniente que:

$$\mathbb{Z}_{p^s} = \{0, 1, \ldots, p^s - 1\}. \tag{2}$$

Recordar que: (a, b) denota al máximo común divisor de a y b, i.e., $(a, b) = mcd(a, b)$.

El siguiente lema nos será muy útil más adelante.

Lema 2.2. *Sean $a \in \mathbb{N}$ y p un número primo. Si $(a,p) = 1$ y $s \in \mathbb{N}$, entonces $ca \equiv 1 \pmod{p^s}$ para algún $c \in \mathbb{Z}$.*

Demostración. Haremos inducción sobre s. Veamos que el resultado es válido para $s = 1$. Como $(a,p) = 1$, entonces existen $c, d \in \mathbb{Z}$ tales que $ca + dp = 1$. Así $ca - 1 = -dp$ es decir, $p|\,(ca-1)$, por lo tanto,

$$ca \equiv 1 \pmod{p^1}.$$

Supóngase que el resultado se cumple para s y demostremos que se cumple para $s+1$. Por hipótesis, existen $k_1, k_2, l_1, l_2 \in \mathbb{Z}$ tales que:

$$\begin{aligned} k_1 a + k_2 p &= 1, \\ l_1 a + l_2 p^s &= 1. \end{aligned}$$

Multiplicando las igualdades anteriores tenemos que:

$$\begin{aligned} 1 &= k_1 l_1 a^2 - k_1 l_2 a p^s + k_2 l_1 p a - k_2 l_2 p^{s+1} \\ &= (k_1 l_1 a - k_1 l_2 p^s + k_2 l_1 p)\, a + (-k_2 l_2)\, p^{s+1} \\ &= ca + dp^{s+1} \end{aligned}$$

donde $c = k_1 l_1 a - k_1 l_2 p^s + k_2 l_1 p$ y $d = -k_2 l_2$. Entonces $ca - 1 = -dp^{s+1}$, es decir,

$$ca \equiv 1 \pmod{p^{s+1}},$$

lo cual concluye la prueba. □

Corolario 2.3. *En $\mathbb{Z}_{p^s}$ se satisface:*

i) Si $\overline{a} \in \mathbb{Z}_{p^s}$ y $(a,p) = 1$, entonces $\overline{a}$ es una unidad en $\mathbb{Z}_{p^s}$.

ii) Para todo $\overline{x} \in \mathbb{Z}_{p^s}$ con $\overline{x} \neq 0$, existen $\overline{a} \in \mathbb{Z}_{p^s}$ e $i \in \mathbb{N} \cup \{0\}$ tales que $(a,p) = 1$ y $\overline{x} = \overline{a}\overline{p^i}$.

Demostración. Sea $\overline{a} \in \mathbb{Z}_{p^s}$ con $(a,p) = 1$, por el Lema 2.2 existe $c \in \mathbb{N}$ tal que $ca \equiv 1 \pmod{p^s}$ entonces $\overline{c} \cdot \overline{a} = \overline{1}$, debido a la Observación 2.1. Por lo tanto, $\overline{a}$ es una unidad de $\mathbb{Z}_{p^s}$. Ahora bien, considérese $\overline{x} \in \mathbb{Z}_{p^s}$ con $\overline{x} \neq \overline{0}$, usando la identificación anterior se sigue que $x \in \mathbb{N}$. Se tienen dos casos:

- Si $(x,p) = 1$ entonces sea $a = x$, de ahí que, $\overline{x} = \overline{a}\overline{p^0}$, lo cual prueba el resultado.

- Si $(x,p) = p$ entonces $p|x$. Además si q es un primo tal que $q|x$ entonces $q \leq p^s - 1$ pues $x \leq p^s - 1$. Por el teorema fundamental de la aritmética, existen $q_1, q_2, \ldots, q_k \in \mathbb{N}$ números primos y $n_1, n_2, \ldots, n_k \in \mathbb{N}$ tales que:

$$x = q_1^{n_1} q_2^{n_2} \ldots q_k^{n_k}$$

como $p|x$ entonces $p = q_j$ para algún $j \in \{1, 2, \ldots, k\}$. Sea

$$i = máx \left\{ n_j | \, (x, p^{n_j}) = p^{n_j} \right\}.$$

Como $(x,p) = p$ entonces $n_j \geq 1$ y por consiguiente este conjunto es no vacío, entonces:

$$\begin{aligned} x &= q_1^{n_1} q_2^{n_2} \ldots q_{j-1}^{n_{j-1}} p^i q_{j+1}^{n_{j+1}} \ldots q_k^{n_k} \\ &= \left(q_1^{n_1} q_2^{n_2} \ldots q_{j-1}^{n_{j-1}} q_{j+1}^{n_{j+1}} \ldots q_k^{n_k} \right) p^i \end{aligned}$$

donde $a = q_1^{n_1} q_2^{n_2} \ldots q_{j-1}^{n_{j-1}} q_{j+1}^{n_{j+1}} \ldots q_k^{n_k}$, entonces $x = ap^i$ y, por lo tanto, $\overline{x} = \overline{a}\overline{p^i}$. □

Ejemplo 2.4. Sean $p = 3$, $s = 2$ entonces $\mathbb{Z}_{3^2} = \{0,1,2,3,4,5,6,7,8\}$, si definimos el conjunto $\mathcal{A} := \{a \in \mathbb{Z}_{p^s} : (a,p) = 1\}$; en este caso tenemos que $\mathcal{A} = \{1,2,4,5,7,8\}$ luego:

$$\begin{aligned} 1 \odot 1 &= 1 \\ 2 \odot 5 &= 1 \\ 4 \odot 7 &= 1 \\ 8 \odot 8 &= 1 \end{aligned} \tag{3}$$

como se afirma en el Corolario 2.3. Así $\mathbb{Z}_{p^s}^* = \mathcal{A}$, donde $\mathbb{Z}_{p^s}^*$ denota el grupo de unidades del anillo $\mathbb{Z}_{p^s}$.

El siguiente teorema caracteriza a los ideales en el anillo $\mathbb{Z}_{p^s}$.

Teorema 2.5. *Los ideales principales* $\langle \overline{1} \rangle, \langle \overline{p} \rangle, \ldots, \langle \overline{p^{s-1}} \rangle, \langle \overline{0} \rangle$*, son todos los ideales de* $\mathbb{Z}_{p^s}$*.* $\langle \overline{p} \rangle$ *es el único ideal maximal de* $\mathbb{Z}_{p^s}$ *y* $\frac{\mathbb{Z}_{p^s}}{\langle \overline{p} \rangle} \simeq \mathbb{F}_p$*.*

Demostración. Sea I un ideal de $\mathbb{Z}_{p^s}$. Suponga que $I \neq \langle \overline{0} \rangle$. Sea m el natural más pequeño que es representante de las clases de I, veamos que $I = \langle \overline{m} \rangle$. Sea $\overline{i} \in I$ entonces $\overline{i} \in \mathbb{Z}_{p^s}$. Por el algoritmo euclidiano de la división, existen $q, r \in \mathbb{Z} : i = qm + r$ con $0 \leq r < m$, entonces $r = i - qm$, de ahí que, $\overline{r} = \overline{i} - \overline{q}\,\overline{m} \in I$, por consiguiente, $\overline{r} \in I$ y $r < m$ lo cual contradice la minimalidad de m, así $\overline{r} = \overline{0}$, en otras palabras, $\overline{i} = \overline{q}\,\overline{m}$, entonces $\overline{i} \in \langle \overline{m} \rangle$, en consecuencia, $I \subseteq \langle \overline{m} \rangle$. Es claro que

$\overline{m} \in I$, por consiguiente $\langle \overline{m} \rangle \subseteq I$, entonces $I = \langle \overline{m} \rangle$, como queríamos. Dado que $\overline{m} \in I \subseteq \mathbb{Z}_{p^s}$, por el Corolario 2.3, existe $a \in \mathbb{Z}$, tal que:

$$\overline{m} = \overline{a}\overline{p^i} \text{ para algún } i \in \{0, \ldots, s-1\}. \tag{4}$$

Como $(a, p) = 1$ tenemos que $ca \equiv 1 \pmod{p^s}$ para algún $c \in \mathbb{Z}$, así, $ca - 1 = dp^s$ con $d \in \mathbb{Z}$, entonces $cap^i - p^i = dp^s p^i$, de ahí que, $\overline{cap^i} - \overline{p^i} = \overline{dp^s p^i}$, por lo que

$$\begin{aligned} \overline{0} &= \overline{c}\overline{ap^i} - \overline{p^i} \\ &= \overline{c}\,\overline{m} - \overline{p^i} \end{aligned}$$

de manera que, $\overline{c}\,\overline{m} = \overline{p^i}$. Entonces $\overline{p^i} \in \langle \overline{m} \rangle$ luego $\langle \overline{p^i} \rangle \subseteq \langle \overline{m} \rangle$, y por (4), $\langle \overline{m} \rangle \subseteq \langle \overline{p^i} \rangle$, de ahí que, $\langle \overline{m} \rangle = \langle \overline{p^i} \rangle$. Por consiguiente, queda demostrado que todo ideal I de $\mathbb{Z}_{p^s}$ es de la forma $I = \langle \overline{p^i} \rangle$ para algún $i \in \{0, 1, \ldots s-1\}$. Además, como $\overline{p^i} \in \langle \overline{p^i} \rangle$ y $\overline{p} \in \mathbb{Z}_{p^s}$ entonces $\overline{p^i} \cdot \overline{p} = \overline{p^{i+1}} \in \langle \overline{p^i} \rangle$, así, $\langle \overline{p^{i+1}} \rangle \subset \langle \overline{p^i} \rangle$, por lo tanto,

$$\langle \overline{0} \rangle \subseteq \langle \overline{p^{s-1}} \rangle \subseteq \ldots \subseteq \langle \overline{p^2} \rangle \subseteq \langle \overline{p} \rangle \subseteq \langle \overline{1} \rangle = \mathbb{Z}_{p^s}. \tag{5}$$

Ahora veamos que $\langle \overline{p} \rangle$ es un ideal maximal. Sea J un ideal de $\mathbb{Z}_{p^s}$ tal que:

$$\langle \overline{p} \rangle \subseteq J \subseteq \mathbb{Z}_{p^s}, \tag{6}$$

luego, existe algún i con $i \in \{0, 1, \ldots, s-1\}$ tal que $J = \langle \overline{p^i} \rangle$. Tenemos que: si $i = 1$ entonces $J = \langle \overline{p^i} \rangle = \langle \overline{p} \rangle$, o bien, si $1 < i \leq s-1$ entonces $J = \langle \overline{p^i} \rangle \subseteq \langle \overline{p} \rangle$ debido a (5), entonces, por (6), $J = \langle \overline{p} \rangle$, o bien, si $i = 0$ entonces $J = \langle \overline{p^0} \rangle = \langle \overline{1} \rangle = \mathbb{Z}_{p^s}$. En cualquier caso, se concluye que $J = \langle \overline{p} \rangle$ o $J = \mathbb{Z}_{p^s}$. Por lo tanto, $\langle \overline{p} \rangle$ es un ideal maximal, y por (5), es el único ideal maximal de $\mathbb{Z}_{p^s}$, en consecuencia, $\frac{\mathbb{Z}_{p^s}}{\langle \overline{p} \rangle}$ es un campo.

Recordemos que:

i) $\frac{\mathbb{Z}_{p^s}}{\langle \overline{p} \rangle} = \{\overline{x} + \langle \overline{p} \rangle : \overline{x} \in \mathbb{Z}_{p^s}\}$

ii) $\langle \overline{p} \rangle = \{\overline{c}\,\overline{p} : \overline{c} \in \mathbb{Z}_{p^s}\}$

Sea $y \in \frac{\mathbb{Z}_{p^s}}{\langle \overline{p} \rangle}$ entonces existe $\overline{x} \in \mathbb{Z}_{p^s}$ tal que $y = \overline{x} + \langle \overline{p} \rangle$, dividiendo a x por p tenemos que existen $r, s \in \mathbb{Z}$ tales que $x = sp + r$ con $0 \leq r \leq p-1$ entonces

$$\begin{aligned} y &= \overline{sp + r} + \langle \overline{p} \rangle \\ &= \overline{r} + \overline{s}\,\overline{p} + \langle \overline{p} \rangle \\ &= \overline{r} + \langle \overline{p} \rangle \end{aligned}$$

es decir:

$$\frac{\mathbb{Z}_{p^s}}{\langle \overline{p} \rangle} = \{\overline{r} + \langle \overline{p} \rangle | r \in \{0, 1 \ldots, p-1\}\}$$

así, $\frac{\mathbb{Z}_{p^s}}{\langle \overline{p} \rangle}$ es un campo finito con p elementos, por lo tanto, $\frac{\mathbb{Z}_{p^s}}{\langle \overline{p} \rangle} \simeq \mathbb{F}_p$. □

Lema 2.6. *Sean $b \in \mathbb{Z}$ con $b > 1$ y $a \in \mathbb{N}$. Entonces existen $d_0, d_1 \ldots, d_{n-1}, t \in \mathbb{Z}$ con $0 \leq d_i \leq b-1$ para cada $i \in \{0, 1, \ldots, n-1\}$ tales que:*

$$a = d_0 b^0 + d_1 b^1 + \cdots + d_{n-1} b^{n-1} + t b^n$$

Demostración. Dividiendo a por b tenemos que, existen $d_0, s_0 \in \mathbb{Z}$ tales que $a = s_0 b + d_0$ con $0 \leq d_0 \leq b-1$. Si dividimos ahora, s_0 por b, obtenemos $d_1, s_1 \in \mathbb{Z}$ tales que $s_0 = s_1 b + d_1$ entonces:

$$\begin{aligned} a &= (s_1 b + d_1)\, b + d_0 \\ &= s_1 b^2 + d_1 b + d_0 \end{aligned}$$

con $0 \leq d_1 \leq b-1$. Procediendo de esta manera $n-1$ veces, tenemos:

$$a = s_{n-1} b^n + d_{n-1} b^{n-1} + d_{n-2} b^{n-2} + \cdots + d_1 b + d_0$$

con $d_i \in \{0, 1 \ldots, b-1\}$ para $i \in \{0, 1 \ldots, n-1\}$, observese que la sucesión de cocientes satisface:

$$a > s_0 > s_1 > \ldots \geq 0$$

debido a que la sucesión $s_0, s_1, \ldots$ es una sucesión decreciente de enteros no negativos. Tomando, $t = s_{n-1}$ se concluye que:

$$a = d_0 b^0 + d_1 b^1 + \cdots + d_{n-1} b^{n-1} + t b^n$$

como queríamos. □

Por el Lema 2.6, dado $x \in \{0, 1, \ldots, p^s - 1\}$ tenemos que:

$$x = c_0 p^0 + c_1 p^1 + \cdots + c_{s-1} p^{s-1} + t p^s$$

con $c_i \in \{0, 1 \ldots, p-1\}$ para cada $i \in \{0, 1 \ldots, s-1\}$ entonces

$$\begin{aligned} \overline{x} &= \overline{c_0 p^0 + c_1 p^1 + \cdots + c_{s-1} p^{s-1} + t p^s} \\ &= \overline{c_0}\,\overline{p^0} + \overline{c_1 p} + \cdots + \overline{c_{s-1}}\,\overline{p^{s-1}} + \overline{t p^s} \\ &= \overline{c_0}\,\overline{p^0} + \overline{c_1 p} + \cdots + \overline{c_{s-1}}\,\overline{p^{s-1}}, \end{aligned} \tag{7}$$

puesto que $\overline{p^s} = \overline{0} \in \mathbb{Z}_{p^s}$. Definamos ahora la función:

$$\mu : \mathbb{Z}_{p^s} \longrightarrow \mathbb{F}_p \tag{8}$$

dada por $\mu(\overline{x}) = \mu\left(\overline{c_0}\,\overline{p^0} + \overline{c_1 p} + \cdots + \overline{c_{s-1}}\,\overline{p^{s-1}}\right) = c_0$, para cada $\overline{x} \in \mathbb{Z}_{p^s}$.

Lema 2.7. *La función μ es un homomorfismo de anillos con $Ker\,\mu = \langle \overline{p} \rangle$.*

Demostración. Sean $\overline{x} = \sum_{i=0}^{s-1} \overline{c_i}\overline{p^i}, \overline{y} = \sum_{i=0}^{s-1} \overline{d_i}\,\overline{p^i} \in \mathbb{Z}_{p^s}$, entonces

$$\overline{x} + \overline{y} = \sum_{i=0}^{s-1} \left(\overline{c_i} + \overline{d_i}\right) \overline{p^i} = \sum_{i=0}^{s-1} \left(\overline{c_i + d_i}\right) \overline{p^i},$$

de ahí que,

$$\begin{aligned} \mu\left(\overline{x} + \overline{y}\right) &= \mu\left(\sum_{i=0}^{s-1} \left(\overline{c_i + d_i}\right) \overline{p^i}\right) = c_0 + d_0 \\ &= \mu\left(\sum_{i=0}^{s-1} \overline{c_i}\,\overline{p^i}\right) + \mu\left(\sum_{i=0}^{s-1} \overline{d_i}\overline{p^i}\right) = \mu\left(\overline{x}\right) + \mu\left(\overline{y}\right), \end{aligned}$$

esto es, $\mu\left(\overline{x} + \overline{y}\right) = \mu\left(\overline{x}\right) + \mu\left(\overline{y}\right)$ para toda $\overline{x}, \overline{y} \in \mathbb{Z}_{p^s}$. Por otro lado,

$$\begin{aligned} \mu\left(\overline{x}\,\overline{y}\right) &= \mu\left(\left(\overline{c_0} + \overline{c_1}\,\overline{p} + \overline{c_2}\overline{p^2} + \ldots + \overline{c_{s-1}}\overline{p^{s-1}}\right) \sum_{i=0}^{s-1} \overline{d_i}\,\overline{p^i}\right) \\ &= \mu\left(\overline{c_0}\left(\sum_{i=0}^{s-1} \overline{d_i}\,\overline{p^i}\right) + \ldots + \overline{c_{s-1}}\left(\sum_{i=0}^{s-1} \overline{d_i}\,\overline{p^i}\right) \overline{p^{s-1}}\right) \\ &= \mu\left(\overline{c_0}\,\overline{d_0} + \overline{c_0}\left(\sum_{i=1}^{s-1} \overline{d_i}\,\overline{p^i}\right) + \ldots + \overline{c_{s-1}}\left(\sum_{i=0}^{s-1} \overline{d_i}\,\overline{p^i}\right) \overline{p^{s-1}}\right) \\ &= \mu\left(\overline{c_0 d_0} + \overline{c_0}\left(\sum_{i=1}^{s-1} \overline{d_i}\,\overline{p^i}\right) + \ldots + \overline{c_{s-1}}\left(\sum_{i=0}^{s-1} \overline{d_i}\,\overline{p^i}\right) \overline{p^{s-1}}\right) \\ &= c_0 d_0 = \mu\left(\sum_{i=0}^{s-1} \overline{c_i}\overline{p^i}\right) \mu\left(\sum_{i=0}^{s-1} \overline{d_i}\,\overline{p^i}\right) = \mu\left(\overline{x}\right) \mu\left(\overline{y}\right) \end{aligned}$$

esto es, $\mu\left(\overline{x}\overline{y}\right) = \mu\left(\overline{x}\right) \mu\left(\overline{y}\right)$ para toda $\overline{x}, \overline{y} \in \mathbb{Z}_{p^s}$. Por lo tanto, μ es un homomorfismo.

Sea $\overline{x} \in \langle \overline{p} \rangle$, entonces existe $\overline{c} \in \mathbb{Z}_{p^s}$ tal que $\overline{x} = \overline{c}\,\overline{p}$. Entonces $\overline{x} = \overline{0}\,\overline{p^0} + \overline{c}\,\overline{p} + \cdots + \overline{0}\,\overline{p^{s-1}}$, luego $\mu\left(\overline{x}\right) = \overline{0}$, por lo tanto $\overline{x} \in Ker\,\mu$, de ahí que, $\langle \overline{p} \rangle \subseteq Ker\,\mu$. Ahora bien, sea $\overline{x} \in Ker\,\mu$ entonces $\mu\left(\overline{x}\right) = 0$, luego $\overline{x} = \overline{0} + \overline{c_1}\,\overline{p} + \ldots + \overline{c_{s-1}}\overline{p^{s-1}}$. Como $\overline{c_i}\overline{p^i} \in \langle \overline{p^i} \rangle \subseteq \langle \overline{p} \rangle$, por (5), para cada $i \in \{1, \ldots, s-1\}$, esto es, $\overline{c_i}\overline{p^i} \in \langle \overline{p} \rangle$ para cada $i \in \{1, 2, \ldots, s-1\}$, así, $\overline{x} \in \langle \overline{p} \rangle$ entonces $Ker\,\mu \subseteq \langle \overline{p} \rangle$. Por lo tanto, $Ker\,\mu = \langle \overline{p} \rangle$. □

$\mathcal{R}[x]$ denota el anillo de polinomios en la indeterminada x con coeficientes en el anillo $\mathcal{R}$, esto es, el conjunto

$$\mathcal{R}[x] = \left\{ f(x) = \sum_{i=0}^{n} c_i x^i : c_i \in \mathcal{R}, i \in \{0, \ldots, n\} \text{ para algún } n \in \mathbb{N} \right\} \tag{9}$$

es un anillo con las operaciones habituales de suma y multiplicación de polinomios.

Podemos extender el homomorfismo definido en (8) de la manera siguiente: sea la función

$$\bar{\cdot} : \mathbb{Z}_{p^s}[x] \longrightarrow \mathbb{F}_p[x] \tag{10}$$

dada por $-(f(x)) = \sum_{i=0}^{n} \mu(c_i) x^i$ para cada $f(x) \in \mathbb{Z}_{p^s}[x]$ y denotamos por $\overline{f}(x)$ la imagen de $f(x)$ bajo " $-$ ".

Como una consecuencia directa del lema anterior tenemos:

Corolario 2.8. *La función $-$ es un homomorfismo de anillos.*

Demostración. Recordemos que si $c_i \in \mathbb{Z}_{p^s}$, por (7) tenemos que:

$$c_i = d_{i0} + d_{i1}p + \ldots + d_{i(s-1)}p^{s-1} \text{ con } d_{ik} \in \{0, 1, \ldots, p-1\}$$

Sean $f(x), g(x) \in \mathbb{Z}_{p^s}[x]$ entonces $f(x) = \sum_{i=0}^{n} c_i x^i$ y $g(x) = \sum_{i=0}^{m} d_i x^i$, con $c_i, d_i \in \mathbb{Z}_{p^s}$ para cada i. Sin pérdida de generalidad, supóngase que $m > n$ entonces $f(x) + g(x) = \sum_{i=0}^{m} (c_i + d_i) x^i$ con $c_i = 0$ para cada $n < i \leq m$. Entonces

$$\begin{aligned}
\overline{f+g}(x) &= \sum_{i=0}^{m} \mu(c_i + d_i) x^i \\
&= \sum_{i=0}^{m} (c_{i0} + d_{i0}) x^i \\
&= \sum_{i=0}^{m} c_{i0} x^i + \sum_{i=0}^{m} d_{i0} x^i \\
&= \sum_{i=0}^{n} c_{i0} x^i + \sum_{i=0}^{m} d_{i0} x^i \\
&= \sum_{i=0}^{n} \mu(c_i) x^i + \sum_{i=0}^{m} \mu(d_i) x^i \\
&= \overline{f}(x) + \overline{g}(x).
\end{aligned}$$

Sabemos que $f(x)g(x) = \sum_{k=0}^{l} e_k x^k$ donde $e_k = c_0 d_k + c_1 d_{k-1} + \ldots + c_k d_0$ y $0 \leq l \leq m+n$, entonces

$$\begin{aligned}\mu(e_k) &= \mu(c_0 d_k + c_1 d_{k-1} + \ldots + c_k d_0) \\ &= \mu(c_0)\mu(d_k) + \mu(c_1)\mu(d_{k-1}) + \ldots + \mu(c_k)\mu(d_0).\end{aligned}$$

Por otro lado, tenemos que:

$$\begin{aligned}\overline{f}(x)\overline{g}(x) &= \left(\sum_{i=0}^{n} \mu(c_i)x^i\right)\left(\sum_{i=0}^{m} \mu(d_i)x^i\right) \\ &= \left(\mu(c_0) + \mu(c_1)x + \ldots + \mu(c_n)x^n\right)\left(\mu(d_0) + \mu(d_1)x + \ldots + \mu(d_m)x^m\right),\end{aligned}$$

pero esto lo podemos expresar como $\sum_{k=0}^{l} \mu(u_k)x^k$ con

$$\mu(u_k) = (\mu(c_0)\mu(d_k) + \ldots + \mu(c_k)\mu(d_0)) = \mu(e_k),$$

de esto se sigue:

$$\overline{fg}(x) = \sum_{k=0}^{l} \mu(e_k)x^k = \sum_{k=0}^{l} \mu(u_k)x^k = \overline{f}(x)\overline{g}(x),$$

por lo tanto, "$-$" es un homomorfismo. □

Definición 2.9. Sea $\overline{p} \in \mathbb{Z}_{p^s} \subseteq \mathbb{Z}_{p^s}[x]$, el ideal generado por $\overline{p} \in \mathbb{Z}_{p^s}[x]$ se denota por $\ll \overline{p} \gg$ y se define como:

$$\ll \overline{p} \gg := \left\{f(x)\overline{p} : f(x) \in \mathbb{Z}_{p^s}[x]\right\}.$$

Lema 2.10. *$Ker - = \ll \overline{p} \gg$.*

Demostración. Sea $h(x) = \sum_{i=0}^{n} c_i x^i$. Si $h(x) \in Ker -$ entonces $\overline{h}(x) = \overline{0} \in \mathbb{Z}_{p^s}$. Pero $\overline{h}(x) = \sum_{i=0}^{n} \mu(c_i)x^i$, es decir $\mu(c_i) = 0$ con $i \in \{0, 1, \ldots, n\}$, entonces $c_i \in Ker\,\mu = \langle\overline{p}\rangle$, por el Lema 2.8. Así, existen $\overline{m_0}, \overline{m_1}, \ldots, \overline{m_n} \in \mathbb{Z}_{p^s}$ tales que $c_i = \overline{m_i}\,\overline{p}$, de ahí que:

$$h(x) = \sum_{i=0}^{n} c_i x^i = \sum_{i=0}^{n} \left(\overline{m_i}\,\overline{p}\right) x^i = \left(\sum_{i=0}^{n} \overline{m_i} x^i\right)\overline{p} = g(x)\overline{p}$$

con $g(x) = \sum_{i=0}^{n} \overline{m_i} x^i$, luego $h(x) \in \ll \overline{p} \gg$, por consiguiente, $Ker - \subseteq \ll \overline{p} \gg$. Ahora bien, si $h(x) \in \ll \overline{p} \gg$ entonces existe $g(x) \in \mathbb{Z}_{p^s}[x]$ tal que $h(x) = g(x)\overline{p}$,

sea $g(x) = \sum_{i=0}^{n} a_i x^i$ entonces

$$\begin{aligned} h(x) &= \sum_{i=0}^{n} a_i \overline{p} x^i \\ &= \sum_{i=0}^{n} c_i x^i \text{ con } c_i = \overline{a_i p} \in \langle \overline{p} \rangle \end{aligned}$$

aplicando "$-$" obtenemos:

$$\overline{h}(x) = \sum_{i=0}^{n} \mu(c_i) x^i = \sum_{i=0}^{n} 0 x^i = \overline{0}$$

luego, $h(x) \in Ker -$, de ahí que, $\ll \overline{p} \gg \subseteq Ker -$, por lo tanto, $Ker - = \ll \overline{p} \gg$. $\square$

Algunas veces denotaremos a $f(x)$ en $\mathbb{Z}_{p^s}[x]$ o $\mathbb{F}_p[x]$ simplemente por f.

Teorema 2.11. *El ideal $\ll \overline{p} \gg$ es un ideal primo de $\mathbb{Z}_{p^s}[x]$, todo ideal primo de $\mathbb{Z}_{p^s}[x]$ contiene a $\ll \overline{p} \gg$, más aún, si un ideal primo contiene a $\ll \overline{p} \gg$ propiamente, entonces dicho ideal es maximal.*

Demostración. Sean $f(x), h(x) \in \mathbb{Z}_{p^s}[x]$ tales que $f(x) = \sum_{i=0}^{n} a_i x^i$ y $h(x) = \sum_{i=0}^{m} b_i x^i$ con $a_n \neq 0 \neq b_m$, de ahí que, los grados de $f(x)$ y $g(x)$ son n y m respectivamente, lo cual denotamos por $grad(f(x)) = n$ y $grad(h(x)) = m$, entonces se tiene que $f(x)h(x) = \sum_{k=0}^{l} c_k x^k$ donde $c_k = \sum_{s=0}^{k} a_s b_{k-s}$ y si $f(x)h(x) \neq 0$ entonces $grad(f(x)h(x)) = l$ con $0 \leq l \leq m+n$. Supóngase, sin pérdida de generalidad, que $m > n$ y además, supóngase que $f(x)h(x) \in \ll \overline{p} \gg$ entonces

$$\overline{f(x)h(x)} = 0 \tag{11}$$

dado que $Ker - = \ll \overline{p} \gg$, pero $\overline{f(x)h(x)} = \sum_{k=0}^{l} \mu(c_k) x^k$ entonces $\mu(c_k) = 0$ para cada $k \in \{0, 1, \ldots, l\}$. Como $\mu(c_k) = \mu(a_0)\mu(b_k) + \ldots + \mu(a_k)\mu(b_0) \in \mathbb{F}_p$ para cada $k \in \{0, 1, \ldots, l\}$ tenemos que para $k = 0$, $0 = \mu(c_0) = \mu(a_0)\mu(b_0)$, pero $\mathbb{F}_p$ es un dominio entero, así $\mu(a_0) = 0$ o $\mu(b_0) = 0$. Supóngase que $\mu(a_0) \neq 0$, entonces $\mu(b_0) = 0$. Ahora bien, cuando $k = 1$, $0 = \mu(c_1) = \mu(a_1)\mu(b_0) + \mu(a_0)\mu(b_1) = \mu(a_0)\mu(b_1)$ puesto que $\mu(b_0) = 0$ y como $\mu(a_0) \neq 0$ tenemos que $\mu(b_1) = 0$, procediendo de esta manera, establecemos que $\mu(b_k) = 0$ para cada $k \in \{0, 1, \ldots, m\}$ de ahí que $\overline{h(x)} = 0$, por consiguiente, $h(x) \in \ll \overline{p} \gg$. Por otro lado, supóngase que $\mu(b_0) \neq 0$ entonces $\mu(a_0) = 0$ y de manera análoga se tiene que $\overline{f(x)} = 0$, en consecuencia, $f(x) \in \ll \overline{p} \gg$, de ahí que, si $f(x)h(x) \in \ll \overline{p} \gg$ entonces $f(x) \in \ll \overline{p} \gg$ o bien $h(x) \in \ll \overline{p} \gg$. Por lo tanto, $\ll \overline{p} \gg$ es un ideal primo de $\mathbb{Z}_{p^s}[x]$. Sea $\mathbb{P}$ un ideal primo de $\mathbb{Z}_{p^s}$. Como $\overline{p} \cdot \overline{p^{s-1}} = \overline{p^s} = \overline{0} \in \mathbb{P}$, entonces

$\overline{p} \in \mathbb{P}$ o $\overline{p^{s-1}} \in \mathbb{P}$, ya que $\mathbb{P}$ es un ideal primo. Si $\overline{p} \in \mathbb{P}$ entonces $\ll \overline{p} \gg \subseteq \mathbb{P}$, ahora bien, si $\overline{p^{s-1}} \in \mathbb{P}$, entonces $\overline{p^{s-2}} \cdot \overline{p} = \overline{p^{s-1}} \in \mathbb{P}$, de ahí que, $\overline{p} \in \mathbb{P}$ o $\overline{p^{s-2}} \in \mathbb{P}$, una vez más, si $\overline{p} \in \mathbb{P}$ concluimos que $\ll \overline{p} \gg \subseteq \mathbb{P}$, o bien, si $\overline{p^{s-2}} \in \mathbb{P}$ se procede como antes, y continuando de esta manera se concluye que $\overline{p} \in \mathbb{P}$, por lo tanto, $\ll \overline{p} \gg \subseteq \mathbb{P}$. Ahora probaremos que si $\mathbb{P}$ es un ideal primo y $\ll \overline{p} \gg \subsetneq \mathbb{P}$ entonces $\mathbb{P}$ es maximal. Veamos primero que $-$ es un epimorfismo. Sean $g(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_p[x]$ y $f(x) = \sum_{i=0}^{n} b_i x^i \in \mathbb{Z}_{p^s}[x]$, se establecio en (7) que para cada $i \in \{0, 1, \ldots, n\}$, $b_i = c_{i0} + c_{i1}p + c_{i2}p^2 + \ldots + c_{i(s-1)}p^{s-1}$ donde $c_{ij} \in \mathbb{F}_p$ para cada $i \in \{0, \ldots, n\}$, $j \in \{1, 2, \ldots, s-1\}$. Sean los b_i's de tal forma que $c_{i0} = a_i$ para cada $i \in \{0, 1 \ldots, n\}$ entonces

$$\overline{f}(x) = \sum_{i=0}^{n} \mu(b_i)x^i = \sum_{i=0}^{n} c_{i0}x^i = \sum_{i=0}^{n} a_i x^i = g(x)$$

así, $-$ es sobre y por tanto epimorfismo. Si denotamos por $\overline{\mathbb{P}}$ a la imagen de $\mathbb{P}$ bajo $-$ y a $-^{-1}(\overline{\mathbb{P}})$ como la imagen inversa de $\overline{\mathbb{P}}$ bajo $-$ entonces $-^{-1}(\overline{\mathbb{P}}) = \mathbb{P}$ y por un teorema de isomorfismos (ver [16, Theorem 12.7, iii)]) la función:

$$\psi : \frac{\mathbb{Z}_{p^s}[x]}{\mathbb{P}} \longrightarrow \frac{\mathbb{F}_p[x]}{\overline{\mathbb{P}}}$$

es un isomorfismo de anillos. Por lo tanto $\dfrac{\mathbb{Z}_{p^s}[x]}{\mathbb{P}} \simeq \dfrac{\mathbb{F}_p[x]}{\overline{\mathbb{P}}}$.

Como $\mathbb{P}$ es un ideal primo entonces $\mathbb{P} \neq \mathbb{Z}_{p^s}[x]$. Si $\overline{\mathbb{P}} = \mathbb{F}_p[x]$, por lo anterior, se tiene que: $-^{-1}(\overline{\mathbb{P}}) = -^{-1}(\mathbb{F}_p[x]) = \mathbb{Z}_{p^s}[x]$, la última igualdad debido a que $-$ es sobreyectiva, de ahí que, $\mathbb{P} = \mathbb{Z}_{p^s}[x]$, lo cual es una contradicción, por consiguiente, $\overline{\mathbb{P}} \neq \mathbb{F}_p[x]$. Sean $f_0(x), g_0(x) \in \mathbb{F}_p[x]$ tales que $f_0(x)g_0(x) \in \overline{\mathbb{P}}$ entonces existen $f(x), g(x) \in \mathbb{Z}_{p^s}[x]$ con $\overline{f}(x) = f_0(x)$ y $\overline{g}(x) = g_0(x)$, luego $\overline{f(x)g(x)} \in \overline{\mathbb{P}}$, de ahí que, $f(x)g(x) \in \mathbb{P}$, pero $\mathbb{P}$ es un ideal primo por lo que $f(x) \in \mathbb{P}$ o $g(x) \in \mathbb{P}$. Si $f(x) \in \mathbb{P}$ entonces $f_0(x) = \overline{f}(x) \in \overline{\mathbb{P}}$ o bien, si $g(x) \in \mathbb{P}$ entonces $g_0(x) = \overline{g}(x) \in \overline{\mathbb{P}}$, por consiguiente, $\overline{\mathbb{P}}$ es un ideal primo de $\mathbb{F}_p[x]$. Sin embargo, $\overline{\mathbb{P}} \neq \langle 0 \rangle$, debido a que, $\ll \overline{p} \gg \subsetneq \mathbb{P}$, ya que, existe $h(x) \in \mathbb{Z}_{p^s}[x]$ tal que $h(x) \in \mathbb{P}$ pero $h(x) \notin \ll \overline{p} \gg$, entonces $\overline{h}(x) \in \overline{\mathbb{P}}$ y $\overline{h}(x) \neq \overline{0}$, por lo tanto, $\overline{\mathbb{P}} \neq \langle 0 \rangle$, en consecuencia, por [16, Theorem 12.27], $\overline{\mathbb{P}}$ es maximal, así $\dfrac{\mathbb{F}_p[x]}{\overline{\mathbb{P}}}$ es un campo y como $\dfrac{\mathbb{Z}_{p^s}[x]}{\mathbb{P}} \simeq \dfrac{\mathbb{F}_p[x]}{\overline{\mathbb{P}}}$ se concluye que $\mathbb{P}$ es maximal. □

A continuación estudiaremos otro tipo de ideales, estos son los ideales primarios de $\mathbb{Z}_{p^s}[x]$, para este propósito se enuncia la definición siguiente:

Definición 2.12. Sean $\mathcal{R}$ un anillo, $I \subseteq \mathcal{R}$ un ideal y $r, s \in \mathcal{R}$. Diremos que:

- I es un ideal **primario** si y sólo si $rs \in I$ implica que $r \in I$ o existe un $n \in \mathbb{N}$ tal que $s^n \in I$.

- El **radical de** I se denota por $\sqrt{I}$ y es el conjunto:

$$\sqrt{I} := \{r \in \mathcal{R} \mid \exists n \in \mathbb{N} : r^n \in I\}.$$

Lema 2.13. *Sea $\mathcal{R}$ un anillo con unidad, e I un ideal tal que $\sqrt{I}$ es un ideal primo. Entonces $I \neq \mathcal{R}$.*

Demostración. Es claro $\sqrt{I} \neq \mathcal{R}$, puesto que $\sqrt{I}$ es un ideal primo. Si $I = \mathcal{R}$, se sigue que, $1 \in I$, luego dado $n = 1 \in \mathbb{N}$, se tiene que, $1^n = 1 \in I$, de ahí que, $1 \in \sqrt{I}$ entonces $\sqrt{I} = \mathcal{R}$, lo cual es una contradicción. □

Teorema 2.14. *Sea Q un ideal de $\mathbb{Z}_{p^s}[x]$.*

i) Si Q es un ideal primario de $\mathbb{Z}_{p^s}[x]$ entonces $\sqrt{Q}$ es un ideal primo.

ii) $\ll \overline{p} \gg \subseteq \sqrt{Q}$

iii) Si $\sqrt{Q}$ es un ideal primo y $\ll \overline{p} \gg \subsetneq \sqrt{Q}$ entonces Q es un ideal primario.

Demostración. Sea Q un ideal de $\mathbb{Z}_{p^s}[x]$.

i) Supongamos que Q es primario, entonces $Q \neq \mathbb{Z}_{p^s}[x]$. Sean $f(x), g(x) \in \mathbb{Z}_{p^s}[x]$ tales que $f(x)g(x) \in \sqrt{Q}$, entonces existe un $n \in \mathbb{N}$ tal que $(f(x)g(x))^n \in Q$, i.e., $(f(x))^n \cdot (g(x))^n \in Q$. Como Q es primario, se sigue que $(f(x))^n \in Q$ o existe $m \in \mathbb{N}$ de manera que $((g(x))^{nm} \in Q$. Si $(f(x))^n \in Q$ entonces $f(x) \in \sqrt{Q}$, o bien, $(g(x))^{nm} \in Q$ entonces $g(x) \in \sqrt{Q}$, pues $nm \in \mathbb{N}$. Por lo tanto, $\sqrt{Q}$ es un ideal primo.

ii) Como $\overline{p^s} = 0$ y Q es un ideal, entonces $\overline{p^s} \in Q$, pero $(\overline{p})^s = \overline{p^s} \in Q$, es decir., existe $s \in \mathbb{N}$ tal que $((\overline{p})^s \in Q)$, por lo tanto, $\overline{p} \in \sqrt{Q}$ y, en consecuencia, $\ll \overline{p} \gg \subseteq \sqrt{Q}$.

iii) Suponga que $\sqrt{Q}$ es un ideal primo y además que $\ll \overline{p} \gg \subsetneq \sqrt{Q}$. Por el Teorema 2.11, $\sqrt{Q}$ es maximal y como $\sqrt{Q} \neq \mathbb{Z}_{p^s}[x]$, se sigue del Lema 2.13 que $Q \neq \mathbb{Z}_{p^s}[x]$. Sean $f(x), g(x) \in \mathbb{Z}_{p^s}[x]$ tales que $f(x)g(x) \in Q$. Suponga ahora que para todo $m \in \mathbb{N}$ se cumple que $((g(x))^m \notin Q)$ entonces $g(x) \notin \sqrt{Q}$.

Definimos $\mathcal{J}(g(x)) := \{t(x)g(x) + q(x) \mid t(x) \in \mathbb{Z}_{p^s}[x] \text{ y } q(x) \in \sqrt{Q}\}$ y sean $l(x), k(x) \in \mathcal{J}(g(x))$, entonces existen $t_1(x), t_2(x) \in \mathbb{Z}_{p^s}[x]$ y $q_1(x), q_2(x) \in \sqrt{Q}$ tales que $l(x) = t_1(x)g(x) + q_1(x)$ y $k(x) = t_2(x)g(x) + q_2(x)$, de ahí que,

$$\begin{aligned} l(x) - k(x) &= t_1(x)g(x) + q_1(x) - t_2(x)g(x) - q_2(x) \\ &= (t_1(x) - t_2(x))\, g(x) + (q_1(x) - q_2(x)) \\ &= t(x)g(x) + r(x) \end{aligned}$$

con $t(x) = t_1(x) - t_2(x) \in \mathbb{Z}_{p^s}[x]$ y $r(x) = q_1(x) - q_2(x) \in \sqrt{Q}$ entonces $l(x) - k(x) \in \mathcal{J}(g(x))$, por lo tanto, $(\mathcal{J}(g(x)), +) < (\mathbb{Z}_{p^s}[x], +)$. Ahora, si $h(x) \in \mathcal{J}(g(x))$ y $k(x) \in \mathbb{Z}_{p^s}[x]$, entonces existen $q(x) \in \sqrt{Q}$ y $t(x) \in \mathbb{Z}_{p^s}[x]$ tales que $h(x) = t(x)g(x) + q(x)$, así $k(x)h(x) = k(x)t(x)g(x) + k(x)q(x) = s(x)g(x) + r(x)$ con $s(x) = k(x)t(x) \in \mathbb{Z}_{p^s}[x]$ y $r(x) = k(x)q(x) \in \sqrt{Q}$, por consiguiente, $k(x)h(x) \in \mathcal{J}(g(x))$, en consecuencia, $\mathcal{J}(g(x))$ es un ideal. Sea $q(x) \in \sqrt{Q}$, es claro que $q(x) = t(x)g(x) + q(x)$ con $t(x) = 0$ entonces $q(x) \in \mathcal{J}(g(x))$, así, $\sqrt{Q} \subseteq \mathcal{J}(g(x))$, también tenemos que si $t(x) \in \mathbb{Z}_{p^s}[x]$ con $t(x) \neq 0$ y $t(x) \notin \sqrt{Q}$ entonces $t(x)g(x) + q(x) \notin \sqrt{Q}$, pues de lo contrario, $t(x)g(x) + q(x) - q(x) = t(x)g(x) \in \sqrt{Q}$ y $\sqrt{Q}$ es un ideal primo pero ni $t(x)$ ni $g(x)$ pertenecen a $sqrtQ$. Así, $\mathcal{J}(g(x)) \neq \sqrt{Q}$ y como $\sqrt{Q}$ es maximal, entonces $\mathcal{J}(g(x)) = \mathbb{Z}_{p^s}[x]$. Por lo anterior, $1 \in \mathcal{J}(g(x))$, entonces existen $t(x) \in \mathbb{Z}_{p^s}[x]$ y $q(x) \in \sqrt{Q}$ tales que $1 = t(x)g(x) + q(x)$ y como $q(x) \in \sqrt{Q}$ entonces existe $n \in \mathbb{N}$ tal que $(q(x))^n \in Q$ entonces

$$\begin{aligned}
1^n &= (t(x)g(x) + q(x))^n \\
&= \sum_{i=0}^{n} \binom{n}{i} (t(x))^{n-i} (g(x))^{n-i} (q(x))^i \\
&= g(x) \sum_{i=0}^{n} \binom{n}{i} (t(x))^{n-i} (g(x))^{n-i-1} (q(x))^i \\
&= g(x) \underbrace{\sum_{i=0}^{n-1} \binom{n}{i} (t(x))^{n-i} (g(x))^{n-i-1} (q(x))^i}_{T(x)} + (q(x))^n,
\end{aligned}$$

esto es, $1 = T(x)g(x) + (q(x))^n$, multiplicando por $f(x)$ obtenemos que $f(x) = T(x)f(x)g(x) + f(x)(q(x))^n$, luego, como $f(x)g(x) \in Q$, $(q(x))^n \in Q$ y Q es un ideal, se sigue que $f(x) \in Q$. Por lo tanto, Q es un ideal primario. □

Definición 2.15. Sea $h(x) \in \mathbb{Z}_{p^s}$. Diremos que $h(x)$ es un polinomio **primario** si y sólo si $\langle h(x) \rangle$ es un ideal primario de $\mathbb{Z}_{p^s}$.

Lema 2.16. *Sea $f(x)$ un polinomio de $\mathbb{Z}_{p^s}[x]$, supóngase que $\overline{f}(x) = (g(x))^m$ donde $g(x)$ es un polinomio irreducible en $\mathbb{F}_p[x]$ y $m \in \mathbb{N}$. Entonces $f(x)$ es un polinomio primario.*

Demostración. Como $\langle f(x) \rangle$ es un ideal de $\mathbb{Z}_{p^s}[x]$, por *ii)* del Teorema 2.14, se tiene que $\ll \overline{p} \gg \subseteq \sqrt{\langle f(x) \rangle}$. Dado que $(f(x))^1 \in \langle f(x) \rangle$ entonces $f(x) \in \sqrt{\langle f(x) \rangle}$ y $\overline{f}(x) \neq 0$, entonces $\ll \overline{p} \gg \subsetneq \sqrt{\langle f(x) \rangle}$. Veamos que $\sqrt{\langle f(x) \rangle}$ es un ideal primo. Si $1 \in \langle f(x) \rangle$ entonces existe $h(x) \in \mathbb{Z}_{p^s}[x]$ de tal manera que $1 = h(x)f(x)$ entonces $\overline{1} =$

$\overline{h}(x)\overline{f}(x) = \overline{h}(x)\left(g(x)\right)^m = g(x)\left(\overline{h}(x)\left(g(x)\right)^{m-1}\right)$ pero esto implica que $g(x)$ es una unidad, lo cual es una contradicción ya que $g(x)$ es irreducible, entonces $\overline{1} \notin \langle f(x)\rangle$, se sigue que, $\langle f(x)\rangle \neq \mathbb{Z}_{p^s}[x]$ y así $\sqrt{\langle f(x)\rangle} \neq \mathbb{Z}_{p^s}[x]$. Sean ahora $a(x), b(x) \in \mathbb{Z}_{p^s}[x]$ y suponga que $a(x)b(x) \in \sqrt{\langle f(x)\rangle}$, entonces existe $n \in \mathbb{N}$ tal que $\left(a(x)b(x)\right)^n \in \langle f(x)\rangle$, es decir, existe $q(x) \in \mathbb{Z}_{p^s}$ tal que $\left(a(x)b(x)\right)^n = \left(a(x)\right)^n\left(b(x)\right)^n = q(x)f(x)$. Aplicando el epimorfismo (10) tenemos que $\overline{\left(a(x)\right)^n\left(b(x)\right)^n} = \overline{q(x)f(x)}$, i.e.,

$$\begin{aligned}\overline{a}(x)^n\overline{b}(x)^n &= \overline{q}(x)\overline{f}(x)\\ &= \overline{q}(x)\left(g(x)\right)^m\end{aligned}$$

de la última igualdad se tiene que $g(x)$ divide al producto $\overline{a}(x)^n\overline{b}(x)^n$ y, como $g(x)$ es irreducible entonces divide a $\overline{a}(x)$ o bien a $\overline{b}(x)$. Supóngase que $g(x)|\overline{a}(x)$ entonces $\left(g(x)\right)^m = \overline{f}(x)$ divide a $\left(\overline{a}(x)\right)^m$, es decir, existe $\overline{c}(x) \in \mathbb{F}_p[x]$ tal que $\left(\overline{a}(x)\right)^m = \overline{c}(x)\overline{f}(x)$, entonces $\left(\overline{a}(x)\right)^m - \overline{c(x)f(x)} = \overline{0}$ y como (10) es epimorfismo tenemos que $\overline{\left(a(x)\right)^m - c(x)f(x)} = \overline{0}$, de ahí que, $\left(a(x)\right)^m - c(x)f(x) \in Ker- = \ll \overline{p} \gg$. Entonces existe $d(x) \in \mathbb{Z}_{p^s}[x]$ tal que $\left(a(x)\right)^m - c(x)f(x) = d(x)\overline{p}$, por lo tanto, $\left(a(x)\right)^m = c(x)f(x) + d(x)\overline{p}$. Como $p^s \geq 2$, elevando la igualdad anterior a p^s obtenemos que $\left(\left(a(x)\right)^m\right)^{p^s} = \left(c(x)f(x) + d(x)\overline{p}\right)^{p^s}$ y, aplicando el teorema del binomio tenemos:

$$\begin{aligned}\left(a(x)\right)^{mp^s} &= \sum_{i=0}^{p^s}\binom{p^s}{i}\left(c(x)f(x)\right)^{p^s-i}\left(d(x)\overline{p}\right)^i\\ &= \underbrace{\left[\sum_{i=0}^{p^s-1}\binom{p^s}{i}\left(c(x)\right)^{p^s-i}\left(f(x)\right)^{p^s-i-1}\left(d(x)\overline{p}\right)^i\right]}_{k(x)} f(x) + \left(d(x)\overline{p}\right)^{p^s}\end{aligned}$$

es decir, $\left(a(x)\right)^{mp^s} = k(x)f(x) + \left(d(x)\right)^{p^s}\left(\overline{p}\right)^{p^s}$ pero $s < p^s$ entonces existe $t \in \mathbb{N}$ tal que $p^s = s + t$, luego $\left(a(x)\right)^{mp^s} = k(x)f(x) + \overline{p}^s\overline{p}^t = k(x)f(x)$ puesto que $\overline{p}^s = \overline{0}$, de ahí que, $a(x) \in \sqrt{f(x)}$. Análogamente si $g(x)$ divide a $\overline{b}(x)$ se concluye que $b(x) \in \sqrt{\langle f(x)\rangle}$. Por lo tanto $\sqrt{\langle f(x)\rangle}$ es un ideal primo. Luego, por la parte *iii)* del Teorema 2.14, $\langle f(x)\rangle$ es un ideal primario y, por la Definición 2.15, $f(x)$ es un polinomio primario. □

3 El Lema de Hensel

Definición 3.1. Sean $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$. Diremos que f_1 y f_2 son **coprimos** en $\mathbb{Z}_{p^s}[x]$ si existen $\lambda_1, \lambda_2 \in \mathbb{Z}_{p^s}[x]$ tales que

$$\lambda_1 f_1 + \lambda_2 f_2 = 1.$$

Cabe mencionar que en la Defincíón 3.1, $\mathbb{Z}_{p^s}[x]$ puede ser reemplazado por $\mathbb{F}_p[x]$.

Lema 3.2. *Sean $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$. Entonces f_1 y f_2 son coprimos en $\mathbb{Z}_{p^s}[x]$ si y sólo si $\overline{f}_1, \overline{f}_2$ son coprimos en $\mathbb{F}_p[x]$.*

Demostración. Sean f_1 y f_2 polinomios coprimos en $\mathbb{Z}_{p^s}[x]$, entonces por la Definición 3.1 existen $\lambda_1, \lambda_2 \in \mathbb{Z}_{p^s}[x]$ tales que $\lambda_1 f_1 + \lambda_2 f_2 = 1$ y, aplicando (10) tenemos que $\overline{\lambda_1 f_1 + \lambda_2 f_2} = \overline{1}$, es decir, $\overline{\lambda_1}\,\overline{f_1} + \overline{\lambda_2}\,\overline{f_2} = \overline{1}$, una vez más, por la Definición 3.1, se concluye que $\overline{f_1}$ y $\overline{f_2}$ son coprimos en $\mathbb{F}_p[x]$. Recíprocamente, sean $\overline{f}_1$ y $\overline{f}_2$ coprimos en $\mathbb{F}_p[x]$, luego por la Definición 3.1, existen $\mu_1, \mu_1 \in \mathbb{F}_p[x]$ tales que $\mu_1\overline{f}_1 + \mu_2\overline{f}_2 = \overline{1}$, pero (10) es un epimorfismo, entonces existen $\lambda_1, \lambda_2 \in \mathbb{Z}_{p^s}[x]$ con $\mu_1 = \overline{\lambda}_1$ y $\mu_2 = \overline{\lambda}_2$ tales que $\overline{\lambda}_1\overline{f}_1 + \overline{\lambda}_2\overline{f}_2 = \overline{1}$, es decir, $\overline{\lambda_1 f_1 + \lambda_2 f_2} = \overline{1}$, luego $\overline{\lambda_1 f_1 + \lambda_2 f_2 - 1} = \overline{0}$, de la última igualdad, se sigue que, $\lambda_1 f_1 + \lambda_2 f_2 - 1 \in Ker - =\ll \overline{p} \gg$, entonces existe $k \in \mathbb{Z}_{p^s}[x]$ tal que $\lambda_1 f_1 + \lambda_2 f_2 - 1 = k\overline{p}$, de ahí que, $\lambda_1 f_1 + \lambda_2 f_2 = 1 + k\overline{p}$. Definimos $\sigma = \sum_{i=0}^{s-1} \left(-k\overline{p}^{\,i}\right)$, luego tenemos que, $\sigma\left(\lambda_1 f_1 + \lambda_2 f_2\right) = \sigma\left(1 + k\overline{p}\right)$, es decir,

$$\begin{aligned}
\left(\sigma\lambda_1\right) f_1 + \left(\sigma\lambda_2\right) f_2 &= \sigma + \sigma k\overline{p} \\
&= \sigma + \left(\sum_{i=0}^{s-1} \left(-k\overline{p}\right)^i\right) k\overline{p} \\
&= \sigma + \left(\left(-k\overline{p}\right)^0 + \left(-k\overline{p}\right)^1 + \cdots + \left(-k\overline{p}\right)^{s-1}\right) k\overline{p} \\
&= \sigma + \left(1 - k\overline{p} + \cdots + (-1)^{s-1} k^{s-1}\overline{p}^{s-1}\right) k\overline{p} \\
&= \sigma + k\overline{p} - k^2\overline{p}^2 + \ldots + (-1)^{s-2} k^{s-1}\overline{p}^{s-1} + (-1)^{s-1} k^s\overline{p}^s \\
&= 1 - k\overline{p} + k^2\overline{p}^2 + \cdots + (-1)^{s-1} k^{s-1}\overline{p}^{s-1} \\
&\quad + k\overline{p} - k^2\overline{p}^2 + \ldots + (-1)^{s-2} k^{s-1}\overline{p}^{s-1} + (-1)^{s-1} k^s\overline{p}^s \\
&= 1
\end{aligned}$$

ya que $\overline{p}^s = 0$, de ahí que, $\left(\sigma\lambda_1\right) f_1 + \left(\sigma\lambda_2\right) f_2 = 1$, por lo tanto, f_1 y f_2 son coprimos en $\mathbb{Z}_{p^s}[x]$. □

Lema 3.3. *Sea $f \in \mathbb{Z}_{p^s}[x]$ un polinomio mónico, supóngase que $\overline{f} = g_1 g_2 \in \mathbb{F}_p[x]$, donde $g_1, g_2 \in \mathbb{F}_p[x]$ son polinomios mónicos coprimos. Entonces existen $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$ polinomios mónicos coprimos tales que*

i) $f = f_1 f_2 \in \mathbb{Z}_{p^s}[x]$,

ii) $\overline{f}_i = g_i$ *para* $i \in \{1, 2\}$.

Demostración. Sea $f \in \mathbb{Z}_{p^s}[x]$ un polinomio mónico, tal que $\overline{f} = g_1 g_2$, donde $(g_1, g_2) = 1$ en $\mathbb{F}_p[x]$, entonces $\overline{f} - g_1 g_2 = \overline{0}$. Como (10) es un epimorfismo, existen $h_1, h_2 \in \mathbb{Z}_{p^s}[x]$ tales que $\overline{h}_1 = g_1$ y $\overline{h}_2 = g_2$, así $\overline{f} - \overline{h}_1\overline{h}_2 = \overline{f - h_1 h_2} = \overline{0}$; por el Lema 2.10 tenemos que $f - h_1 h_2 \in \ll \overline{p} \gg$, es decir existe $k \in \mathbb{Z}_{p^s}$ tal que $f - h_1 h_2 = k\overline{p}$. Por consiguiente, $f = h_1 h_2 + k\overline{p}$. Como g_1 y g_2 son coprimos en $\mathbb{F}_p[x]$, se sigue del Lema 3.2 que h_1 y h_2 son coprimos en $\mathbb{Z}_{p^s}[x]$ luego, por la Definición 3.1, existen $\lambda_1\lambda_2 \in \mathbb{Z}_{p^s}[x]$ tales que $\lambda_1 h_1 + \lambda_2 h_2 = 1$. Denotando por v a $k\overline{p}$ tenemos:

$$f = h_1 h_2 + v. \tag{12}$$

Definimos en $\mathbb{Z}_{p^s}[x]$ los polinomios siguientes:

$$h_{11} = h_1 + \lambda_2 v$$
$$h_{21} = h_2 + \lambda_1 v$$

Como $v \in \ll \overline{p} \gg$ entonces $\overline{v} = \overline{0}$; aplicando (10) a cada polinomio, tenemos que $\overline{h_{11}} = \overline{h}_1 = g_1$ y $\overline{h_{21}} = \overline{h}_2 = g_2$ además, al multiplicar estos polinomios obtenemos:

$$\begin{aligned} h_{11}h_{21} &= h_1 h_2 + \lambda_1 h_1 v + \lambda_2 h_2 v + \lambda_1\lambda_2 v^2 \\ &= h_1 h_2 + (\lambda_1 h_1 + \lambda_2 h_2)\, v + \lambda_1\lambda_2 v^2 \\ &= h_1 h_2 + v + \lambda_1\lambda_2 v^2, \end{aligned}$$

puesto que $\lambda_1 h_1 + \lambda_2 h_2 = 1$ y, usando (12) en la última igualdad se obtiene que $h_{11}h_{21} = f + \lambda_1\lambda_2 v^2$, de ahí que, $f - h_{11}h_{21} = -\lambda_1\lambda_2 v^2$, de manera que:

$$f \equiv h_{11}h_{21} \pmod{v^2}.^1 \tag{13}$$

Como $(g_1, g_2) = 1$, $\overline{h_{11}} = g_1$ y $\overline{h_{21}} = g_2$, se sigue del Lema 3.2 que h_{11} y h_{21} son coprimos, es decir existen λ_{11}, λ_{21} tales que $\lambda_{11}h_{11} + \lambda_{21}h_{21} = 1$. Por (13) tenemos que $f = h_{11}h_{21} + k_1 v^2$ para algún $k_1 \in \mathbb{Z}_{p^s}[x]$, entonces repitiendo el proceso t veces definiendo en cada paso a los polinomios:

$$h_{1t} = h_{1t-1} + \lambda_{2t-1}k_{t-1}v^{2(t-1)}$$
$$h_{2t} = h_{2t-1} + \lambda_{1t-1}k_{t-1}v^{2(t-1)}$$

donde $\overline{h_{1t}} = g_1$, $\overline{h_{2t}} = g_2$, $\lambda_{1t-1}h_{1t-1} + \lambda_{2t-1}h_{2t-1} = 1$ y $f = h_{1t-1}h_{2t-1} + k_{t-1}v^{2(t-1)}$. Es fácil ver que para $t = s$ al multiplicar los polinomios definidos arriba se tiene:

$$f \equiv h_{1s}h_{2s} \pmod{v^{2s}}.$$

[1] Usamos la notación de congruencia modular ya que $v^2 | f - h_{11}h_{21}$.

Observe que $v^{2s} = (k\overline{p})^{2s} = k^{2s}\overline{p}^s\overline{p}^s = \overline{0}$, es decir, $f \equiv h_{1s}h_{2s} \pmod{\overline{p}^s}$, en otras palabras, $f - h_{1s}h_{2s} = \overline{0}$ y, por lo tanto, $f = h_{1s}h_{2s}$. Finalmente, renombrando $f_1 = h_{1s}$ y $f_2 = h_{2s}$ tenemos que: $f = f_1f_2$, $\overline{f_1} = g_1$, $\overline{f_2} = g_2$ y $(f_1, f_2) = 1$, con lo cual queda demostrado el lema. □

A continuación mostraremos un resultado que nos será muy útil en la generalización del Lema 3.3.

Lema 3.4. *Sea R un anillo euclidiano y sean $p_1, p_2, \ldots, p_r \in R$ coprimos por pares. Entonces, si $r \geq 3$ se tiene que $\left(\prod_{i=1}^{r-1} p_i, p_r\right) = 1$.*

Demostración. Haremos inducción sobre r. Supongamos que $r = 3$. Sean $p_1, p_2, p_3 \in R$ tales que $(p_i, p_j) = 1$ para $i \neq j$ con $i, j \in \{1, 2, 3\}$ entonces, por la Definición 3.1, tenemos que existen $a_1, a_2, b_1, b_2 \in R$ tales que $a_1p_1 + a_2p_3 = 1$ y $b_1p_2 + b_2p_3 = 1$. Multipicando estas igualdades tenemos:

$$\begin{aligned} 1 &= (a_1p_1 + a_2p_3)(b_1p_2 + b_2p_3) \\ &= a_1b_1p_1p_2 + a_1b_2p_1p_3 + a_2b_1p_2p_3 + a_2b_2p_3^2 \\ &= (a_1b_1)\, p_1p_2 + (a_1b_2p_1 + a_2b_1p_2 + a_2b_2p_3)\, p_3 \\ &= \lambda_1p_1p_2 + \lambda_2p_3 \end{aligned}$$

donde $\lambda_1 = a_1b_1, \lambda_2 = a_1b_2p_1 + a_2b_1p_2 + a_2b_2p_3 \in R$, por lo tanto, $(p_1p_2, p_3) = 1$. Supóngase que este resultado se cumple para r, veamos que es válido para $r+1$. Sean $p_1, p_2, \ldots, p_r, p_{r+1} \in R$ tales que $(p_i, p_j) = 1$ para $i \neq j$ con $i, j \in \{1, 2, \ldots, r+1\}$, en particular tenemos que $(p_r, p_{r+1}) = 1$ y, por la hipótesis inductiva, tenemos que $\left(\prod_{i=1}^{r-1} p_i, p_{r+1}\right) = 1$ así, por la Definición 3.1 se tiene que existen $c_1, c_2, d_1, d_2 \in R$ tales que:

$$\begin{aligned} c_1p_r + c_2p_{r+1} &= 1, \\ d_1p_1p_2\cdots p_{r-1} + d_2p_{r+1} &= 1, \end{aligned}$$

multiplicando las igualdades obtenemos:

$$\begin{aligned} 1 &= c_1d_1\prod_{i=1}^{r-1} p_ip_r + c_1d_2p_rp_{r+1} + c_2d_1\prod_{i=1}^{r-1} p_ip_{r+1} + c_2d_2p_{r+1}^2 \\ &= (c_1d_1)\prod_{i=1}^{r} p_i + \left(c_1d_2p_r + c_2d_1\prod_{i=1}^{r-1} p_i + c_2d_2p_{r+1}\right)p_{r+1} \\ &= \mu_1\prod_{i=1}^{r} p_i + \mu_2p_{r+1} \end{aligned}$$

donde $\mu_1 = c_1d_1, \mu_2 = c_1d_2p_r + c_2d_1\prod_{i=1}^{r-1} p_i + c_2d_2p_{r+1} \in R$, de ahí que, $\mu_1\prod_{i=1}^{r} p_i + \mu_2p_{r+1} = 1$, por lo tanto, $(\prod_{i=1}^{r} p_i, p_{r+1}) = 1$, lo cual queríamos demostrar. □

Ahora demostraremos uno de los resultados más importantes de este trabajo, el famoso **Lema de Hensel**.

Lema 3.5 (Lema de Hensel)**.** *Sea f un polinomio mónico en $\mathbb{Z}_{p^s}[x]$ y supóngase que $\overline{f} = g_1g_2\cdots g_r \in \mathbb{F}_p[x]$ donde $g_1, g_2, \ldots, g_r$ son polinomios mónicos y coprimos por pares sobre $\mathbb{F}_p$. Entonces existen polinomios mónicos y coprimos por pares $f_1, f_2, \ldots, f_r$ sobre $\mathbb{Z}_{p^s}$ tales que:*

i) $f = f_1f_2\cdots f_r \in \mathbb{Z}_{p^s}[x]$

ii) $\overline{f}_i = g_i$ *para cada* $i \in \{1, 2, \ldots, r\}$

Demostración. Haremos inducción sobre el número de factores, r. Para el caso $r = 2$, ver la demostración del Lema 3.3. Ahora, supóngase que el resultado es válido para $r-1$ factores y veamos que es válido para r factores. Sea $f \in \mathbb{Z}_{p^s}[x]$ un polinomio mónico tal que $\overline{f} = g_1g_2\cdots g_r$, donde $g_1, g_2, \ldots, g_r$ son polinomios mónicos y coprimos por pares sobre $\mathbb{F}_p$. Denotemos por $h = g_1g_2\cdots g_{r-1}$, es claro que, $h \in \mathbb{F}_p[x]$ y $\overline{f} = hg_r$. Por el Lema 3.4, tenemos que $(h, g_r) = 1$ además, por el Lema 3.3, tenemos que existen $\widehat{h}, f_r \in \mathbb{Z}_{p^s}[x]$ polinomios mónicos coprimos tales que $f = \widehat{h}f_r$, donde $\overline{\widehat{h}} = h$ y $\overline{f}_r = g_r$. Pero $\overline{\widehat{h}} = h = \prod_{i=1}^{r-1} g_i$, por la hipótesis inductiva existen $f_1, f_2 \ldots, f_{r-1} \in \mathbb{Z}_{p^s}[x]$ polinomios mónicos coprimos por pares tales que $\widehat{h} = f_1f_2\cdots f_{r-1}$ y $\overline{f}_i = g_i$ con $i \in (1, 2, \ldots, r-1)$, de ahí que, $f = f_1f_2\cdots f_{r-1}f_r \in \mathbb{Z}_{p^s}[x]$ y $\overline{f}_i = g_i$ para cada $i \in \{1, 2, \ldots, r\}$, con lo cual queda demostrado el lema de Hensel. □

Concluimos esta sección mencionando que el lector interesado puede consultar el libro de McDonald ([12]) para revisar el Lema de Hensel en su versión general sobre anillos conmutativos finitos locales y los artículos [3] y [13] para ver un par de aplicaciones del Lema de Hensel sobre la clase de anillos conmutativos finitos de cadena.

4 Polinomios Básicos irreducibles y el levantamiento de Hensel

A continuación, se demostrará un teorema de factorización "única" para polinomios con coeficientes en el anillo $\mathbb{Z}_{p^s}$.

Teorema 4.1. *Sea f un polinomio mónico en $\mathbb{Z}_{p^s}[x]$ con $grad(f) \geq 1$. Entonces:*

i) f puede ser factorizado de la manera siguiente:

$$f = f_1 f_2 \cdots f_r$$

donde $f_1, f_2, \ldots, f_r$ son polinomios mónicos, primarios y coprimos por pares en $\mathbb{Z}_{p^s}[x]$, más aún, para cada $i \in \{1, 2, \ldots, r\}$, $\overline{f}_i$ es una potencia de algún polinomio mónico irreducible en $\mathbb{F}_p[x]$.

ii) Esta factorización es única salvo el orden.

Demostración. Sea $f \in \mathbb{Z}_{p^s}[x]$ entonces $\overline{f} \in \mathbb{F}_p[x]$, como $\mathbb{F}_p[x]$ es un *dominio de factorización única* existen $g_1, g_2, \ldots, g_r \in \mathbb{F}_p[x]$ polinomios mónicos irreducibles coprimos por parejas tales que

$$\overline{f} = g_1^{e_1} g_2^{e_2} \cdots g_r^{e_r}, \tag{14}$$

para algunos $e_1, e_2, \ldots, e_r \in \mathbb{N}$, por el Lema 3.4 tenemos que si $i \neq j$ entonces $\left(g_i^{e_i}, g_j^{e_j}\right) = 1$ para $i, j \in \{1, 2, \ldots, r\}$, además, debido al Lema de Hensel, tenemos que existen polinomios mónicos, coprimos por pares $f_1, f_2, \ldots, f_r \in \mathbb{Z}_{p^s}[x]$ tales que $f = f_1 f_2 \cdots f_r$ y $\overline{f_i} = g_i^{e_i}$ para cada $i \in \{1, 2, \ldots r\}$, y por el Lema 2.16 se sigue que para cada i, f_i es un polinomio primario en $\mathbb{Z}_{p^s}[x]$, con lo cual queda demostrada la primera afirmación. Ahora bien, supóngase que:

$$f_1 f_2 \cdots f_r = h_1 h_2 \cdots h_t \tag{15}$$

son dos factorizaciones de f como producto de polinomios primarios, mónicos coprimos por pares en $\mathbb{Z}_{p^s}[x]$. Se sigue de (15) que $f_1 f_2 \cdots f_r \in \langle h_i \rangle$ para cada $i \in \{1, 2, \ldots, t\}$ y como $\langle h_i \rangle$ es un ideal primario, existen $k_i \in \mathbb{Z}$ con $1 \leq k_i \leq r$ y $n_i \in \mathbb{N}$ tales que $f_{k_i}^{n_i} \in \langle h_i \rangle$. Veamos que k_i es único para cada $i \in \{1, 2, \ldots, t\}$. Sean $k_i' \neq k_i$ y $n_i' \in \mathbb{N}$ tales que $f_{k_i'}^{n_i'}, f_{k_i}^{n_i} \in \langle h_i \rangle$, es claro que $\left(f_{k_i'}, f_{k_i}\right) = 1$ entonces existen $a, b \in \mathbb{Z}_{p^s}[x]$ tales que $a f_{k_i} + b f_{k_i'} = 1$, como $1^{n_i + n_i' - 1} = \left(a f_{k_i} + b f_{k_i'}\right)^{n_i + n_i' - 1}$ tenemos que:

$$1 = \sum_{j=0}^{n_i + n_i' - 1} \binom{n_i + n_i' - 1}{j} a^j f_{k_i}^j b^{n_i + n_i' - 1 - j} f_{k_i'}^{n_i + n_i' - 1 - j}$$

al desarrollar la sumatoria siempre tendremos presentes a los factores $f_{k_i}^{n_i}$ y $f_{k_i'}^{n_i'}$ los cuales son elementos del ideal $\langle h_i \rangle$, entonces $1 \in \langle h_i \rangle$ lo cual es una contradicción pues h_i es primario, por lo tanto $k_i = k_i'$. De manera similar, para cada $j \in \{1, 2 \ldots, r\}$ existe un único l_j con $l_j \in \{1, 2, \ldots, t\}$ tal que $h_{l_j}^{m_j} \in \langle f_j \rangle$, así,

para cada $k_i \in \{1, 2, \ldots, r\}$ tenemos que $h_{l_j}^{m_j} = cf_j$. Si $j = k_i$ entonces $h_{l_{k_i}}^{m_{k_i}} = cf_{k_i}$ así $h_{l_{k_i}}^{m_{k_i} n_i} = c^{n_i} f_{k_i}^{n_i} \in \langle h_i \rangle$, es decir, $h_{l_{k_i}}^{m_{k_i} n_i} \in \langle h_i \rangle$ luego existe un $\lambda \in \mathbb{Z}_{p^s}[x]$ tal que $h_{l_{k_i}}^{m_{k_i} n_i} = \lambda h_i$, aplicando el epimorfismo (10) tenemos que $\overline{h}_{l_{k_i}}^{m_{k_i} n_i} = \overline{\lambda}\,\overline{h}_i$, en otras palabras, $\overline{h}_{l_{k_i}}^{m_{k_i} n_i} \in \langle \overline{h}_i \rangle$. Así tenemos que $l_{k_i} = i$ para cada $i \in \{1, 2, \ldots r\}$ pues de lo contrario dado l_{k_i} existirían j_0, i_0 distintos tales que $j_0 = l_{k_i} = i_0$ pero $(h_{j_0}, h_{i_0}) = h_{j_0} \neq 1$ en contradicción con el Lema 3.2. Usando lo anterior, definimos las siguiente funciones:

$$\begin{array}{ccc} \{1, 2, \ldots, t\} & \longrightarrow & \{1, 2, \ldots, r\} \\ i & \longmapsto & k_i \end{array}$$

$$\begin{array}{ccc} \{1, 2, \ldots, r\} & \longrightarrow & \{1, 2, \ldots, t\} \\ j & \longmapsto & l_j \end{array}$$

las cuales son inyectivas, de ahí que $r \leq t$ y también $t \leq r$ así, $r = t$ y reenumerando $k_i = i$ para cada $i \in \{1, 2, \ldots, r\}$ tenemos que $l_j = k_i = i$ entonces $f_i^{n_i} \in \langle h_i \rangle$ y $h_i^{m_i} \in \langle f_i \rangle$. Si $j \neq 1$ tenemos que $(f_1, f_j) = 1$ entonces $\left(\overline{f}_1, \overline{f}_j\right) = 1$, luego $\overline{f}_2 \overline{f}_3 \cdots \overline{f}_r$ y $\overline{f}_1^{n_1}$ son coprimos y por el Lema 3.4 $(f_2 f_3 \cdots f_r, f_1^{n_1}) = 1$. Como $f_1^{n_1} \in \langle h_1 \rangle$ existe algun $c \in \mathbb{Z}_{p^s}[x]$ tal que $f_1^{n_1} = ch_1$. Veamos que el producto $f_2 f_3 \cdots f_r$ y h_1 son coprimos. Dado que $(f_2, f_3 \cdots f_r, f_1^{n_1}) = 1$ existen $\alpha, \beta \in \mathbb{Z}_{p^s}[x]$ tales que $1 = \alpha f_2 f_3 \cdots f_r + \beta f_1^{n_1} = \alpha f_2 f_3 \cdots f_r + \beta(ch_1)$, sea $\gamma = c\beta$ entonces

$$\alpha f_2 f_3 \cdots f_r + \gamma h_1 = 1, \tag{16}$$

de ahí que, $(f_2 f_3 \cdots f_r, h_1) = 1$. Multiplicando (16) por f_1 se obtiene que $\alpha f_1 f_2 \cdots f_r + \gamma h_1 f_1 = f_1$, es decir, $\alpha h_1 h_2 \cdots h_r + \gamma h_1 f_1 = f_1$, usando (15), entonces $f_1 = h_1 (\alpha h_2 h_3 \cdots h_r + \gamma f_1)$, por lo anterior, se tiene que h_1 divide a f_1. Procediendo de manera similar con $h_1^{m_1}$, se establece que f_1 divide a h_1 y como $(f_1, h_1) = 1$ se sigue que $f_1 = h_1$, análogamente se concluye que $f_i = h_i$ para toda $i \in \{1, 2, \ldots, r\}$. □

Definición 4.2. Sea $f(x)$ un polinomio mónico de grado $m \geq 1$ en $\mathbb{Z}_{p^s}[x]$. Si $\overline{f}(x) \in \mathbb{F}_p[x]$ es irreducible (o primitivo), diremos que $f(x)$ es un **polinomio mónico básico irreducible**(o mónico básico primitivo) en $\mathbb{Z}_{p^s}[x]$.

Los siguientes lemas, serán de suma importancia en la demostración de los resultados más relevantes de esta sección.

Lema 4.3. *Si $\mathbb{F}_q$ es un campo finito con q elementos, entonces todo polinomio irreducible $h(x) \in \mathbb{F}_q[x]$ de grado m divide a $x^{q^m} - x$.*

Demostración. Como $h(x)$ es irreducible con $grad\,(h) = m$, entonces el conjunto:

$$\mathbb{F} = \frac{\mathbb{F}_q[x]}{\langle h(x)\rangle} := \{[f(x)] = f(x) + \langle h(x)\rangle | f(x) \in \mathbb{F}_p[x]\}$$

es un campo finito con q^m elementos y por [8, Lemma 2.3] se tiene que, $[x] \in \mathbb{F}$ implica que $[x]^{q^m} = [x]$, entonces $[0] = [x]^{q^m} - [x] = [x^{q^m} - x]$, es decir, $x^{q^m} - x \in \langle h(x)\rangle$, por lo tanto, $h(x)|x^{q^m} - x$. □

Lema 4.4. *Sea f un polinomio no nulo de grado positivo sobre un campo finito $\mathbb{F}$. Si $(f, f') = 1$ entonces f no tiene factores múltiples.*

Demostración. Suponga que f tiene al menos un factor múltiple, dígamos g con $grad(g) \geq 1$, es decir, $f = g^2h$ para algún $h \in \mathbb{F}[x]$. Entonces $f' = 2gg'h + h'g^2$ factorizando a g tenemos que $f' = g\,(2g'h + h'g)$, de manera que, g divide a f y f'. Sea $d = (f, f')$ entonces $g|d$, de ahí que, $d \neq 1$. □

Lema 4.5. *Sean $\mathbb{F}$ un campo con característica p, i.e., $Car\,(\mathbb{F}) = p$ y $n \in \mathbb{N}$. Si $p \nmid n$ entonces el polinomio $x^n - 1 \in \mathbb{F}_p[x]$ no tiene raíces múltiples.*

Demostración. Sea r una raíz múltiple de $h(x) = x^n - 1$ en $\mathbb{F}_p[x]$. Es claro que $r \neq 0$ y, por [8, Theorem 1.68], también es raíz de $h'(x) = nx^{n-1}$. Entonces $nr^{n-1} = 0$, esto es, $(nr)r^{n-2} = 0$ pero $\mathbb{F}_p$ es un dominio entero y $r \neq 0$, de ahí que, $nr = 0$, por lo tanto, $p|n$. □

Teorema 4.6. *Para cualquier entero $m \geq 1$ existe un polinomio mónico básico irreducible de grado m sobre $\mathbb{Z}_{p^s}$ el cual divide a $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$.*

Demostración. Sea $\mathbb{F}_p$ un campo finito con p elementos. En [8, Corollary 2.11] se muestra que para $m \geq 1$ existe $f_0(x)$ un polinomio irreducible de grado m sobre $\mathbb{F}_p$. Si $f_0(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ entonces $f_1(x) = a_m^{-1} f_0(x)$ es un polinomio mónico irreducible de grado m en $\mathbb{F}_p[x]$. Por el Lema 4.3, $f_1(x)$ divide a $x^{p^m} - x$ en $\mathbb{F}_p[x]$. Como $f_1(x)$ es irreducible y $x^{p^m} - x = x\left(x^{p^m-1} - 1\right)$ entonces $f_1(x)|x$ ó $f_1(x)|x^{p^m-1} - 1$. Supongamos que $m = 1$ y sea $f(x) = x - 1 \in \mathbb{Z}_{p^s}[x]$ tal que $\overline{f}(x) = f_1(x)$ entonces $f_1(x)|\left(x^{p^m-1} - 1\right)$ en $\mathbb{F}_p[x]$ ya que $\overline{f}(x) = f_1(x) = x - 1$, así que $\overline{f}(x) = x - 1$ en $\mathbb{F}_p[x]$ es un polinomio mónico e irreducible tal que $f(x)|\left(x^{p^m-1} - 1\right)$ en $\mathbb{Z}_{p^s}[x]$, como deseabamos. Por otro lado, si $m > 1$ entonces $f_1(x)$ no puede dividir a x entonces $f_1(x)$ divide a $x^{p^m-1} - 1$ en $\mathbb{F}_p[x]$. Así, existe $g_1(x) \in \mathbb{F}_p[x]$ tal que $x^{p^m-1} - 1 = f_1(x)g_1(x)$, observe que la derivada de $x^{p^m-1} - 1$ es el polinomio $p^m x^{p^m-2} - x^{p^m-2}$ y como $Car\,(\mathbb{F}) = p$ entonces $p^m x^{p^m-2} - x^{p^m-2} = -x^{p^m-2}$. Ahora bien, si consideramos los polinomios $\lambda_1 = -1$ y $\lambda_2 = -x$ se sigue que $\lambda_1\left(x^{p^m-1} - 1\right) + \lambda_2\left(-x^{p^m-2}\right) = -x^{p^m-1} + 1 + x^{p^m-1} = 1$,

así, por la Definición 3.1 y el Lema 4.4, $x^{p^m-1}-1$ no tiene factores múltiples. Supongamos que $(f_1(x), g_1(x)) = d(x)$ y $grad(d) \geq 1$ entonces $f_1(x) = k_1(x)d(x)$ y $g_1(x) = k_2(x)d(x)$ para algunos $k_1(x), k_2(x) \in \mathbb{F}_p[x]$, entonces como $x^{p^m-1}-1 = f_1(x)g_1(x) = k_1(x)k_2(x)\,(d(x))^2$, tenemos que, $x^{p^m-1}-1$ tiene a $d(x)$ como factor múltiple, lo cual es una contradicción, por consiguiente, $(f_1(x), g_1(x)) = d(x)$ con $grad(d) = 1$ pero $f_1(x)$ es mónico, de ahí que, $(f_1(x), g_1(x)) = 1$, entonces por el Lema de Hensel existen polinomios mónicos y coprimos $f_2(x)$ y $g_2(x)$ en $\mathbb{Z}_{p^s}[x]$ tales que $x^{p^m-1}-1 = f_2(x)g_2(x)$ en $\mathbb{Z}_{p^s}[x]$ con $\overline{f_2}(x) = f_1(x)$ y $\overline{g_2}(x) = g_1(x)$. Si escogemos $f(x) = f_2(x)$ se satisface que $\overline{f(x)} = f_1(x)$ un polinomio mónico e irreducible en $\mathbb{F}_p[x]$ y por la Definición 4.2 $f(x)$ es un polinomio mónico básico irreducible con $grad(f) = grad(f_1) = m$ y que divide a $x^{p^m-1}-1$ en $\mathbb{Z}_{p^s}$ como queríamos demostrar. □

Definición 4.7. Sea $g(x)$ un polinomio mónico sobre $\mathbb{F}_p$. Un polinomio mónico $f(x)$ en $\mathbb{Z}_{p^s}[x]$ con $\overline{f}(x) = g(x)$ es llamado un ***Levantamiento de Hensel*** para $g(x)$ si y sólo si existe $n \in \mathbb{N}$ tal que si $p \nmid n$ entonces $f(x) | (x^n - 1)$ en $\mathbb{Z}_{p^s}[x]$.

En el Teorema 4.6, tenemos que $\overline{f}(x) = f_1(x)$ y si $p|p^m - 1$ entonces existirá un $k \in \mathbb{N}$ tal que $p^m - 1 = kp$ entonces $p^m - kp = 1$, en otras palabras, $(p, p^m) = 1$ lo cual es absurdo, así existe $n = p^m - 1 \in \mathbb{N}$ tal que $p \nmid n$ y $f(x) | (x^n - 1)$ en $\mathbb{Z}_{p^s}[x]$. por lo tanto, $f(x)$ es el levantamiento de Hensel de $f_1(x)$.

Sin embargo, no todo polinomio mónico básico irreducible es un levantamiento de Hensel. Por ejemplo, para el polinomio $x + 2 \in \mathbb{Z}_4[x]$ se tiene $\overline{x+2} = x \in \mathbb{F}_2[x]$. Veamos que $x + 2$ no es un levantamiento de Hensel para x. Sea $n \in \mathbb{N}$, si $2 \nmid n$ entonces existe $k \in \mathbb{N}$ tal que $n = 2k+1$, como $x^{2k+1}-1 = (x^{2k} - 2x^{2k-1})(x+2)-1$ tenemos que el residuo de la división de $x^{2k+1}-1$ por $x+2$ es -1, esto es, $x^{2k+1} - 1 \equiv -1 \pmod{x+2}$, por lo tanto, $x + 2 \nmid x^n - 1$, lo cual contradice la Definición 4.7.

Teorema 4.8. *Sea $s \in \mathbb{N}$. Un polinomio mónico $g(x) \in \mathbb{F}_p[x]$ tiene un levantamiento de Hensel $f(x) \in \mathbb{Z}_{p^s}$ si y sólo si $g(x)$ no tiene raíces múltiples y $x \nmid g(x)$ en $\mathbb{F}_p[x]$.*

Demostración. Supóngase que $f(x)$ es un levantamiento de Hensel para $g(x)$ sobre $\mathbb{Z}_{p^s}$, entonces $\overline{f}(x) = g(x)$ y existe $n \in \mathbb{N}$ tal que $p \nmid n$ y $f(x)|x^n - 1$, así, tenemos que, $x^n - 1 = f(x)h(x)$ para algún $h(x) \in \mathbb{F}_p[x]$ entonces

$$x^n - 1 = \overline{x^n - 1} = \overline{f}(x)\overline{h}(x) = g(x)\overline{h}(x). \tag{17}$$

Como $p \nmid n$, $x^n - 1$ no tiene raíces múltiples en $\mathbb{F}_p[x]$, por el Lema 4.5, y de (17) se sigue que $g(x)$ no tiene raíces múltiples pues de tenerlas entonces serían tambien raíces de $x^n - 1$, lo cual no puede ocurrir. Más aún, si $x|g(x)$ tenemos que

$x|x^n-1$, por (17), es decir, 0 es raíz de x^n-1 lo cual tampoco puede ocurrir. Por lo tanto, $x \nmid g(x)$. Recíprocamente, supongamos que $g(x)$ no tiene raíces múltiples y que $x \nmid g(x)$ en $\mathbb{F}_p[x]$, entonces $g(0) \neq 0$. Por [8, Lemma 3.1], existe $n \in \mathbb{N}$ tal que $g(x)|x^n-1$ con $n \leq p^{grad(g)-1}$. Tenemos que $(n,p)=1$ o bien $p|n$, entonces existen $m \in \mathbb{N}$ y $e \in \mathbb{N} \cup \{0\}$ con $(m,p)=1$ tales que $n = mp^e$. Como $p|\binom{p^e}{i}$ para $i \in \{1,2,\ldots,p^e-1\}$ y $Car(\mathbb{F}_p)=p$ entonces $\binom{p^e}{i}=0$ para $i \in \{1,2,\ldots,p^e-1\}$ en $\mathbb{F}_p$, aplicando el teorema del binomio para $a,b \in \mathbb{F}_p$ se tiene que:

$$\begin{aligned}(a+b)^{p^e} &= \sum_{i=0}^{p^e} \binom{p^e}{i} a^{p^e-i}b^i \\ &= a^{p^e} + \sum_{i=1}^{p^e-1} \binom{p^e}{i} a^{p^e-i}b^i + b^{p^e} \\ &= a^{p^e} + b^{p^e}.\end{aligned}$$

Por lo anterior, $(x^m)^{p^e} = ((x^m-1)+1)^{p^e} = (x^m-1)^{p^e}+1$, i.e., $(x^m)^{p^e} = (x^m-1)^{p^e}+1$, de ahí que, $(x^m-1)^{p^e} = (x^m)^{p^e}-1 = x^{mp^e}-1 = x^n-1$. Como $g(x)|\,(x^n-1)$ entonces $g(x)h(x) = (x^m-1)^{p^e}$ para algún $h(x) \in \mathbb{F}_p[x]$ y $grad\,(g)+grad\,(h) = n = mp^e \geq 1$. Si $grad\,(g)=1$ entonces $g(x)=x-1$, ya que $g(x)$ es mónico y 1 es raíz común de $g(x)$ y x^n-1, además $x-1|x^m-1$, por consiguiente, $g(x)|x^m-1$. Por otro lado, como $g(x)h(x) = (x^m-1)\,(x^m-1)^{p^e-1}$ y $g(x)$ no tiene raíces múltiples, si $grad\,(g)=l>1$ entonces $g(x)|x^m-1$, ya que de lo contrario, tendría a 1 como raíz múltiple. En ambos casos tenemos que existe $m \in \mathbb{N}$ tal que $p \nmid n$ y $g(x)|x^m-1$ en $\mathbb{F}_p[x]$, es decir, existe $g_0(x) \in \mathbb{F}_p[x]$ de tal manera que $x^m-1 = g(x)g_0(x)$ y como $p \nmid m$, x^m-1 no tiene factores múltiples, así $(g(x),g_0(x))=1$ en $\mathbb{F}_p[x]$, por el Lema de Hensel, existen $f(x), f_0(x) \in \mathbb{Z}_{p^s}[x]$ polinomios mónicos, coprimos entre si tales que

$$x^m-1 = f(x)f_0(x) \tag{18}$$

en $\mathbb{Z}_{p^s}[x]$ con $\overline{f}(x)=g(x)$ y $\overline{f_0}(x)=g_0(x)$. Por (18) se deduce que $f(x)|x^m-1$ en $\mathbb{Z}_{p^s}[x]$ con $p \nmid m$, por lo tanto, f es el levantamiento de Hensel de $g(x)$. □

Este teorema y el siguiente lema son fundamentales en la demostración de la unicidad del levantamiento de Hensel.

Lema 4.9. *Sean $m,n \in \mathbb{N}$. $x^m-1|x^n-1$ si y sólo si $m|n$.*

Demostración. Por el algoritmo de la división, existen $s,r \in \mathbb{Z}$ tales que $n = sm+r$ con $0 \leq r < m$. Es faćil verificar, mediante la división larga de x^n-1 por x^m-1, que:

$$x^n-1 = \left(x^{(s-1)m+r} + x^{(s-2)m+r} + \cdots + x^r\right)(x^m-1) + x^r - 1,$$

dado que $n = sm + r$ con $grad(x^r - 1) < grad(x^m - 1)$, por consiguiente, $x^n - 1 \equiv x^r - 1$ (mód $x^m - 1$). Si $m|n$ entonces $r = 0$, luego, $x^r - 1 = 0$ y de lo anterior se sigue que $x^m - 1|x^n - 1$. Por otro lado, si $x^m - 1|x^n - 1$ tenemos que $x^r - 1 = 0$, es decir, $x^r = 1$ entonces $r = 0$, por lo tanto. $m|n$, como queríamos demostrar. □

Teorema 4.10. *Sea $s \in \mathbb{N}$ y $g(x)$ un polinomio mónico en $\mathbb{F}_p[x]$ sin raíces múltiples tal que $x \nmid g(x)$ en $\mathbb{F}_p[x]$. Entonces $g(x)$ tiene un único levantamiento de Hensel en $\mathbb{Z}_{p^s}[x]$.*

Demostración. Por el Teorema 4.8, $g(x)$ tiene un levantemiento de Hensel en $\mathbb{Z}_{p^s}[x]$, así que sólo probaremos la unicidad. Sean $f^{(1)}(x)$ y $f^{(2)}(x)$ dos levantamientos de Hensel de $g(x)$ en $\mathbb{Z}_{p^s}[x]$ entonces

i) $f^{(1)}$ y $f^{(2)}$ son polinomios mónicos.

ii) $\overline{f^{(1)}}(x) = g(x) = \overline{f^{(2)}}(x)$.

iii) Existen $n_1, n_2 \in \mathbb{N}$ tales que $p \nmid n_1, p \nmid n_2$ con $f^{(1)}(x)|x^{n_1} - 1$ y $f^{(2)}(x)|x^{n_2} - 1$ en $\mathbb{Z}_{p^s}[x]$.

De *ii*) y *iii*) se sigue que $g(x)|x^{n_1} - 1$ y $g(x)|x^{n_2} - 1$ en $\mathbb{F}_p[x]$. Así, tenemos dos casos: $n_1 = n_2$ y $n_1 \neq n_2$. Supóngase que $n = n_1 = n_2$, como $\mathbb{F}_p[x]$ es un *dominio de factorización única* tenemos que existen $h_1(x), h_2(x), \ldots, h_r(x)$ polinomios mónicos e irreducibles en $\mathbb{F}_p[x]$ y $e_1, e_2 \ldots, e_r \in \mathbb{N}$ tales que $x^n - 1 = h_1^{e_1}(x)h_2^{e_2}(x) \cdots h_r^{e_r}(x)$. Sea $g_i(x) = h_i^{e_i}(x)$ para cada $i \in \{1, 2, \ldots, r\}$ entonces

$$x^n - 1 = g_1(x)g_2(x) \cdots g_r(x) \tag{19}$$

en $\mathbb{F}_p[x]$ con $(g_i, g_j) = 1$ para cada $i \neq j$, luego, por el Lema de Hensel, existen $f_1(x), f_2(x), \ldots, f_r(x) \in \mathbb{Z}_{p^s}[x]$ tales que $x^n - 1 = f_1(x)f_2(x) \cdots f_r(x)$ en $\mathbb{Z}_{p^s}[x]$ con $f_i(x)$ mónico, $(f_i(x), f_j(x)) = 1$ si $i \neq j$, y $\overline{f_i}(x) = g_i(x) = h_i(x)^{e_i} \in \mathbb{F}_p[x]$ para cada $i \in \{1, 2, \ldots, r\}$. Por el Lema 2.16, f_i es un polinomio primario sobre $\mathbb{Z}_{p^s}[x]$ para cada i. Como $g(x)|x^n - 1$, $(g_i(x), g_j(x)) = 1$ si $i \neq j$ y por (19) tenemos que $g(x) = g_1(x)g_2(x) \cdots g_t(x)$ para algún $1 \leq t \leq r$, salvo el orden de $g_1(x), g_2(x), \ldots, g_r(x)$ en (19). Finalmente, nombrando a $f(x) = f_1(x)f_2(x) \cdots f_t(x)$, $f(x)$ es el único polinomio tal que $\overline{f}(x) = \overline{f^{(1)}}(x) = \overline{f^{(2)}}(x) = g(x)$ y $f(x)|x^n - 1$, por el Teorema 4.1, en otras palabras, $f^{(1)}(x) = f^{(2)}(x)$. Por otro lado, si $n_1 \neq n_2$, sea $n = [n_1, n_2]$[2], entonces $n_1|n$ y $n_2|n$, de ahí que, existen $k_1, k_2 \in \mathbb{N}$ tales que $n = k_1 n_1$ y $n = k_2 n_2$. Nuevamente ocurre que $(p, k_1) = 1$ o $k_1 = kp^e$ y $(p, k_2) = 1$ o $k_2 = k'p^{e'}$ con $(p, k) = (p, k') = 1$ y $e, e' \in \mathbb{N}$. Sea $t = kk'n_1n_2$ entonces $p \nmid t$ pero $n_1|t$ y $n_2|t$

[2]El mínimo común múltiplo de n_1 y n_2

entonces $x^{n_1}-1|x^t-1$ y $x^{n_2}-1|x^t-1$ en $\mathbb{Z}_{p^s}[x]$, por el Lema 4.9, y por el primer caso, debemos concluir que $f^{(1)}(x)=f^{(2)}(x)$. Esto prueba la unicidad del levantamiento de Hensel. □

Algoritmo 1 Hensel's Step [15, Algorithm 15.10]

Entrada: p un número primo, polinomios $f\in\mathbb{Z}_{p^2}[x]$ y $g,h,s,t\in\mathbb{F}_p[x]$ tales que: $\overline{f}=gh$, g,h mónicos, $grad(f)=grad(g)+grad(h)$, $grad(t)<grad(g)$, $grad(s)<grad(h)$ y $sg+th=1$ en $\mathbb{F}_p[x]$.

Salida: Polinomios $g^*,h^*,s^*,t^*\in\mathbb{Z}_{p^2}[x]$ tales que: $f=g^*h^*$ con g^*,h^* mónicos, $\overline{g^*}=g$, $\overline{h^*}=h$, $\overline{s^*}=s$ y $\overline{t^*}=t$.

1: Calcule el polinomio $e=f-gh$ en $\mathbb{Z}_{p^2}$.
2: Hallar polinomios $q,r\in\mathbb{Z}_{p^2}[x]$ tales que $se=qh+r$.
3: Defina los polinomios $g_0=g(q+1)+te$, $h_0=h+r$ y $u=sg_0+th_0-1$.
4: Hallar polinomios $v.w\in\mathbb{Z}_{p^2}[x]$ tales que: $su=vh_0+w$.
5: Obtener $g^*=g_0$, $h^*=h_0$, $s^*=s-w$ y $t^*=t(1-u)-vg_0$.

En el siguiente ejemplo aplicamos el Algoritmo 1 para factorizar el polinomio dado.

Ejemplo 4.11. Factorizar el polinomio $f=x^3+4x+8\in\mathbb{Z}_{3^2}[x]$.

Es claro que $\overline{f}=x^3+x+2\in\mathbb{F}_3[x]$ y además 2 es una raíz de $\overline{f}$, entonces $x-2$ divide a $\overline{f}$ en $\mathbb{F}_3[x]$, realizando la división se obtiene que $\overline{f}=(x-2)(x^2+2x+2)$, de ahí que, $g=x-2$ y $h=x^2+2x+2$. Aplicando el algoritmo de Euclides se tiene que

$$(2x+2)(x-2)+(1)(x^2+2x+2)=1$$

así $s=2x+2$ y $t=1$. Calculamos en $\mathbb{Z}_9[x]$ el polinomio $e=f-gh=x^3+4x+8-\left(x^3-2x-4\right)=6x+3$. Entonces $se=3x^2+6$ y, al dividir por h se obtiene que

$$se=3\left(x^2+x+2\right)-6x,$$

de ahí, se sigue que $q=3$ y $r=-6x\in\mathbb{Z}_9$. Luego se calculan los polinomios $g_0=x-5$ y $h_0=x^2-4x+2$ y definimos $u=sg_0+th_0-1=3x^2-3x$. Nuevamente al dividir su por h_0 tenemos que

$$su=(6x+6)(x^2-4x+2)+(6x-3)$$

Finalmente, se concluye que $v=6x+6$ y $w=6x-3$. Realizando los últimos

calculos se obtiene que

$$\begin{array}{ll} g^* = x-5 & \overline{g^*} = x-2 \\ h^* = x^2-4x+2 & \overline{h^*} = x^2-x+2 = x^2+2x+2 \\ s^* = -4x+5 & \overline{s^*} = -x+2 \quad = 2x+2 \\ t^* = 4 & \overline{t^*} = 1 \end{array}$$

Además,

$$\begin{aligned} s^*g^* + t^*h^* &= (-4x+5)(x-5) + (4)(x^2-4x+2) \\ &= -4x^2+7x-7+4x^2-7x+8 \\ &= 1 \end{aligned}$$

como esperabamos.

Algoritmo 2 Método de Graeffe [16, Theorem 13.12]

Entrada: Un polinomio $f_2(x) \in \mathbb{F}_2[x]$ de grado n sin raíces múltiples y tal que $f_2(0) \neq 0$.

Salida: Un polinomio $f(x)$ el levantamiento de Hensel de $f_2(x)$.

1: Escriba $f_2(x) = e(x) - d(x)$ donde $e(x)$ sólo contiene términos de f_2 con exponenete par y $d(x)$ con los de exponenete impar.

2: Calcule en $\mathbb{Z}_4[x]$ el polinomio

$$f(x^2) = \begin{cases} +\left[(e(x))^2 - (d(x))^2\right] & \text{si } grad(e) > grad(d) \\ -\left[(e(x))^2 - (d(x))^2\right] & \text{si } grad(e) < grad(d) \end{cases}$$

3: Cambie x^2 por x en $f(x^2)$.

En los siguientes dos ejemplos se emplea el Algoritmo 2 para realizar el levantamiento de Hensel del polinomio dado.

Ejemplo 4.12. Calcular el levantamiento de Hensel para el polinomio $f_2(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Obsérvese que $e(x) = 1$ y $d(x) = x^3 + x$ entonces tenemos que $grad(d) > grad(e)$, así

$$\begin{aligned} f(x^2) &= -\left[(1)^2 - \left(x^3+x\right)^2\right] \\ &= -\left[-x^6 - 2x^4 - x^2 + 1\right] \\ &= x^6 + 2x^4 + x^2 - 1. \end{aligned}$$

Luego, haciendo el cambio de x^2 por x en $f(x^2)$ tenemos que $f(x) = x^3+2x^2+x-1$. Veamos que es el levantamiento de Hensel de f_2.

$$\overline{f}(x) = \overline{x^3 + 2x^2 + x - 1} = x^3 + x - 1 = x^3 + x + 1 = f_2(x).$$

Además, se tiene tras hacer la división larga que

$$x^3 + 2x^2 + x - 1 \equiv 0 \pmod{x^7 - 1}$$

como queríamos probar.

Ejemplo 4.13. Calcular el levantamiento de Hensel para $g_2(x) = x^4+x^3+x^2+x+1$. Tenemos pues que $e(x) = x^4+x^2+1$ y $d(x) = x^3+x$ así $grad(e) > grad(d)$ entonces

$$\begin{aligned} g(x^2) &= \left[\left(x^4 + x^2 + 1\right)^2 - \left(x^3 + x\right)^2\right] \\ &= \left[x^8 + 2x^6 + x^4 + 2x^4 + 2x^2 + 1 - x^6 - 2x^4 - x^2\right] \\ &= x^8 + x^6 + x^4 + x^2 + 1 \end{aligned}$$

de ahí que $g(x) = x^4 + x^3 + x^2 + x + 1$. Tenemos que

$$\overline{g}(x) = \overline{x^4 + x^3 + x^2 + x + 1} = x^4 + x^3 + x^2 + x + 1 = g_2(x)$$

Además, se tiene tras hacer la división larga que

$$x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{x^5 - 1}$$

por lo tanto, g es el levantamiento de Hensel de g_2.

Concluimos esta sección invitando al lector interesado a consultar el artículo [13, Definición 3.4]) para ver una aplicación del Levantamiento de Hensel sobre la clase de anillos conmutativos finitos de cadena.

Agradecimientos

Agradecemos al árbitro su amable revisión y valiosos comentarios al trabajo.

Bibliografía

[1] A. Bonnecaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41** (1995), 366–377.

[2] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), 1250–1255.

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

[4] M. Greferath and S. E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory **45** (1999), 2522–2524.

[5] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}\_4$*-linearity of kerdock, preparata, goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[6] K. Hensel, *Neue Grundlagen der Arithmetik*, Journal für die reine und angewandte Mathematik, 127 (1904), 51–84. http://eudml.org/doc/149178

[7] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the integers modulo* p^m, Finite Fields and Their Applications **3** (1997), no. 4, 334–352.

[8] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, (Great Britain: Cambridge University Press, 1994).

[9] S. Ling and J. T. Blackford, $\mathbb{Z}_{p^{k+1}}$*-linear codes*, IEEE Trans. Inform. Theory **48** (2002), no. 9, 2592–2605.

[10] C. A. López-Andrade and H. Tapia-Recillas, *On the linearity and quasi-cyclicity of the gray image of codes over a galois ring*, Groups, Algebras and Applications, vol. CONM/537, AMS, (2011), pp. 255–268.

[11] C. A. López-Andrade and H. Tapia-Recillas, *On the cyclicity of the gray image of a class of linear cyclic codes over a finite chain ring*, International Journal of Pure and Applied Mathematics, **80** (2012), no. 2, 181–190.

[12] B. R. McDonald, *Finite Rings with Identity* in Pure and Applied Mathematics, Marcel Dekker, New York, 1974.

[13] E. Martínez-Moro and I. F. Rua, *Multivariable Codes over Finite Chain Rings: Serial Codes*, SIAM J. Discrete Math., **20**(4), (2006) 947–959.

[14] V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* $\mathbb{Z}\_4$, IEEE Trans. Inform. Theory **42** (1996), 1594–1600.

[15] J. von zur Gathen and G. Jurgen, *Modern computer alegbra*, (New York: Cambridge University Press, 2003).

[16] Z. X. Wan, *Lectures on finite fields and Galois rings*, (Beijing: World Scientific Pub. Co. Inc., 2003).

[17] J. Wolfmann, *Binary images of cyclic codes over* $\mathbb{Z}_4$, IEEE, Trans. Inform. Theory **47** (2001), 1773–1779.

Facultad de Ciencias Físico Matemáticas, BUAP
Avenida San Claudio y 18 Sur, Colonia San Manuel,
Puebla, Pue. C.P. 72570

argr_040890@hotmail.com
clopez@fcfm.buap.mx