ANILLOS DE GALOIS

TESIS QUE PRESENTA

ÁNGEL RAÚL GARCÍA RAMÍREZ

PARA OBTENER EL TÍTULO DE
LICENCIADO EN MATEMÁTICAS

ASESOR: DR. CARLOS ALBERTO LÓPEZ ANDRADE

BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA
Facultad de Ciencias Físico Matemáticas
http://www.fcfm.buap.mx/
Junio 2017

ÁNGEL RAÚL GARCÍA RAMÍREZ : *Anillos de Galois* © Junio 2017.

E-MAIL:
argr_040890@hotmail.com

AGRADECIMIENTOS

Agradezco en primer lugar a mis sinodales, ya que cada uno con su estilo personal, puso a mi disposición su vasto conocimiento para ampliar mi visión y pulir mi trabajo. Al Dr. Juan José Angoa Amador, por la paciencia y tolerancia al escuchar mi resumen de tesis, por su sincero interés y apoyo al aclarar conceptos que necesitaban refuerzo, al Dr. César Bautista Ramos por aceptar la revisión del escrito y por sus observaciones en tanto al estilo de esta tesis y sus conceptos. Finalmente, al Dr. Ivan Fernando Vilchis Montalvo, por su valioso tiempo e integridad al revisar a fondo y con detalle este trabajo, por recordarme la importancia de perseguir la claridad y formalidad en las matemáticas y regalarme un último desafío.

A mi asesor, el Dr. Carlos Alberto López Andrade, por este tiempo de trabajo y de amistad, por enseñarme más que un simple contenido académico, el valor de la perseverancia, la disciplina, el orden, la constancia y por estar siempre allí, al pie del cañón atento de mi avance. Por su tolerancia a mis fallos y por haber influido en mi evolución personal. Aseguro, sin miedo a equivocarme que ha sido usted una gran fuente de inspiración para mi y muchos otros estudiantes.

A mis padres, Mario Raúl y Soledad, quienes caminaron al lado mío durante 17 años siendo mis primeros maestros y amorosas guías, que durante los siguientes años y hasta ahora, me acompañan con el pensamiento y sus bendiciones. A mis hermanas, Graciela, Monserrath y Verónica, tres grandes mujeres y madres de familia, que sonríen cada vez que me ven y que me regalaron la dicha de conocer a mis sobrinos Abraham, Leslie, Mateo y Samantha, que son la nueva alegría de ese hogar que hoy sólo puedo visitar, pase lo que pase, los amo.

A mi amada y fiel compañera Jeny, la mejor de mis amigas, mi soporte durante estos años, quien me apoyo día a día y dirigió mi camino hasta aquí. Gracias amor por todo, las lágrimas, las risas y los enojos, pero sobre todas las cosas, por estar siempre a mi lado.

A mis amigos y amigas: Alberto, Alexis, Arturo, Betsabe, Erik, Gonzalo, Hugo Saúl, Ivan, Jerónimo, Jessica, Jez, Jhonatan O., Jorge, José, Karen G., Luis, Manuel, Mariana, Rafael A., Ricardo, Santiago y Yas. Aquellos que no he mencionado, perdonen mi memoria, pero hay tantas historias y alegrías que nublan al recuerdo. Las palabras están de más, saben bien el gran cariño que les tengo, gracias por regalarme tantas aventuras, por su fidelidad, su regaño oportuno y por abrirme el corazón, una sincera disculpa por el dolor que pude haber causado. *A mis amigos les adeudo la ternura, las palabras de aliento y el abrazo, el compartir con ustedes la factura, que nos presenta la vida paso a paso, [...], la paciencia de soportarme las espinas más agudas, los arrebatos del humor, la negligencia, los temores, vanidades y las dudas, les adeudo también aquel enfado, que perturbara alguna vez nuestra armonía, sabemos bien que no puede ser pecado, el discutir alguna vez por tonterias.*

Es sabido por quienes me conocen, que suelo extender las cosas más allá de lo necesario, y que estos agradecimientos sirvan como evidencia de este rasgo que me representa, pero cuando la vida es tan generosa y da tanto que agradecer, abreviar es imposible. Hoy su servidor, hijo de una mujer que sabiendo lo más básico de matemáticas levantó a una familia y de un hombre que le enseñó a trabajar y desarmar tantas cosas para entender cómo funcionan y cómo repararlas, está frente a grandes profesores y científicos, en compañia de tan buenos amigos, que sin importar que tan lejos llegue, ni que tanto aprenda de sabios y libros, si algún día le preguntasen: ¿Qué se necesita para llegar hasta aquí?, les dirá con el corazón puesto en todos ustedes: "solo se necesita saber sumar, restar, multiplicar, dividir y que no hay nada en este mundo, que no se pueda reparar". Gracias.

INTRODUCCIÓN

En la actualidad, los anillos de Galois han adquirido notoriedad en las áreas de la Teoría de Códigos (cf. [14], [17], [8], [9]) y la Criptografía (cf. [1], [4], [13]), entre otras. La Teoría de Códigos y la Criptografía inmersas en las Matemáticas y en otras disciplinas tales como las Ciencias de la Computación e Ingenieria Eléctrica, están enfocadas en la optimización de la fiabilidad y seguridad de las comunicaciones dígitales. A grandes rasgos, la fiabilidad significa corrección de errores mientras que la seguridad significa prevenir el acceso no autorizado de intrusos.

En los años 90 del siglo pasado, el Lema de Hensel resultó una herramienta muy útil en el estudio de la caracterización de la estructura algebraica de los códigos cíclicos lineales sobre anillos finitos, en particular sobre anillos de Galois (cf. [5], [6], [8], [14]). La representación p-ádica de los elementos de un anillo de Galois es imprescindible en la definición de la función de Gray en esta clase de anillos, así como en la clase de los anillos finitos de cadena (cf. [3]), de las cuales, los primeros son una subclase. Hammons et. al en [5] demostraron que el código de Kerdock es la imagen de Gray de un código cíclico lineal extendido sobre el anillo de Galois $\mathbb{Z}_4$. Ellos usan este hecho para resolver un problema "viejo", explicar la dualidad formal entre dos códigos no lineales binarios, los famosos códigos de Kerdock y Preparata. Este trabajo abrió la puerta al estudio de la Teoría de Códigos Algebraicos sobre anillos finitos, y en particular, sobre los anillos de Galois (cf. [9]).

La presente tesis, tiene como objetivo hacer un estudio general acerca de los anillos de Galois, su estructura, propiedades y su relación con los campos finitos, también llamados campos de Galois.

Los anillos de Galois son extensiones únicas del anillo de clases residuales $\mathbb{Z}_{p^s}$ con p, s enteros positivos y p un número primo. Suelen denotarse por $\mathcal{R} = GR(p^s, m)$, o bien, $\mathcal{R} = GR(p^s, p^{sm})$ dónde la característica del anillo es p^s, su cardinalidad es p^{sm} y el grado de la extensión sobre $\mathbb{Z}_{p^s}$ es m. Éstos son anillos locales con único ideal maximal (p), generado por el elemento $p1$, donde cada ideal es de la forma (p^i) para $1 \leqslant i \leqslant s$, y de campo residual $F = \mathcal{R}/(p)$ isomorfo a $GF(p^m)$, el campo de Galois con p^m elementos.

Este trabajo tiene como base los últimos dos capítulos de la obra de Zhe-Xian Wan [16], presentando un análisis detallado de los resultados allí expuestos, incluyendo los resultados básicos necesarios para que el material sea auto-contenido y está escrito de tal forma que el lector pueda comprender de manera didáctica el contenido de la obra.

Este manuscrito está organizado de la siguiente manera:

El Capítulo 1 esta conformado por definiciones y resultados importantes en teoría de grupos, teoría de anillos y campos, presentando un análisis general pero no superficial sobre los anillos de polinomios con coeficientes en anillos conmutativos y campos, además de presentar generalidades y resultados aunque conocidos muy importantes sobre los campos finitos y los polinomios definidos sobre éstos. Se destacan resultados en este capítulo como el Teorema 1.4.5 de suma importancia en el análisis del grupo de unidades de un anillo de Galois, los Teoremas

1.7.10 y 1.7.11 y la sección 1.8 es clave ya que se exhiben resultados que tendrán paralelismo con propiedades de los anillos de Galois.

En el Capítulo 2 se revisa la estructura del anillo de polinomios $\mathbb{Z}_{p^s}[x]$, se estudian sus ideales y se definen los siguientes epimorfismos. El primero es $\mu : \mathbb{Z}_{p^s} \to \mathbb{F}_p$ y una extensión de éste $- : \mathbb{Z}_{p^s}[x] \to \mathbb{F}[x]$ los cuales se usan en la sección 2.2 para el planetamiento y demostración del Lema de Hensel (Lema 2.2.5), el cual dice:

Lema (de Hensel.). *Sea f un polinomio mónico en $\mathbb{Z}_{p^s}[x]$ y supóngase que $\bar{f} = g_1 g_2 \cdots g_r \in \mathbb{F}_p[x]$ 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) $f = f_1 f_2 \cdots f_r \in \mathbb{Z}_{p^s}[x]$

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

*En la sección 2.3 se define el concepto de polinomio mónico básico irreducible (primitivo), se enuncia un teorema de factorización única y con éstos se demuestra la existencia y unicidad del **Levantamiento de Hensel** de un polinomio mónico irreducible con coeficientes en un campo finito, o de manera explícita:*

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

Definición. Sea $g(x)$ un polinomio mónico sobre $\mathbb{F}_p$. Un polinomio mónico $f(x)$ en $\mathbb{Z}_{p^s}[x]$ con $\bar{f}(x) = g(x)$ 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 $\mathbb{Z}_{p^s}[x]$.

Teorema. *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 $\mathbb{Z}_{p^s}[x]$.*

En la parte final de esta sección, se muestra un algoritmo para hallar el levantamiento de Hensel dado un polinomio que satisface las hipótesis antes mencionadas, dicho algoritmo, desarrollo y justificación pueden encontrarse en [15, Capítulo 15.4,Págs. 418-423]. Se agradece al Dr. Fernando Macías por dar su consentimiento, en su carácter de editor, del uso del material de este capítulo que fue previamente publicado en la obra Matemáticas y sus Aplicaciones 7 (cf. [10]) como trabajo conjunto del tesista y el director de esta tesis.

En el capítulo 3 se desarrolla el objetivo principal de este trabajo, los anillos de Galois, en la sección 3.1 se dan ejemplos de anillos de Galois, como lo son: $\mathbb{Z}_{p^s}$ y $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ donde $h(x)$ es un polinomio mónico básico irreducible, en la secciónes 3.2 3.3 y 3.4 se estudia la estructura de los anillos de Galois, su representación p-ádica y su grupo de unidades, destacando como resultado, un teorema de caracterización de los anillo de Galois. La sección 3.5 se ocupa de las extensiones de anillos de Galois, generalizando el proceso realizado con $\mathbb{Z}_{p^s}$ y exhibiendo análogos de los resultados del Capítulo 2 y en las secciones 3.6 y 3.7 se define el automorfismo generalizado de Frobenius, la traza y norma generalizadas para anillos de Galois y es aquí donde se encuentran grandes similitudes con los conceptos de automorfismos, traza y norma de la teoría de campos finitos.

En la sección 3.8, se lleva a cabo el desarrollo de un ejemplo de un anillo de Galois, concretamente el anillo $\mathrm{GR}(2^2, 2^4)$ *para facilitar la comprensión de los conceptos mostrados en este trabajo. Finalmente, el lector encontrará un apéndice, en éste, se encuentran enunciados y definiciones que sirven como complemento para los temas abordados. Agradecemos de manera anticipada la paciente lectura y atención a los contenidos aquí presentados, se menciona que esta tesis es el primer paso para un futuro trabajo de maestría el cual se enfocará en la Teoría de códigos algebraicos definidos sobre anillos de Galois.*

ÍNDICE GENERAL

1 PRELIMINARES

En este capítulo recordaremos definiciones y resultados importantes en teoría de grupos, teoría de anillos y campos, presentando un análisis general pero no superficial sobre los anillos de polinomios con coeficientes en anillos conmutativos y campos, además de presentar generalidades y resultados aunque conocidos muy importantes sobre los campos finitos y los polinomios definidos sobre éstos.

GRUPOS

Definición 1.1.1. Sea G un conjunto no vacío. Diremos que G es un grupo si existe una función:

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (x, y) & \longmapsto & x * y \end{array}$$

dicha función recibe el nombre de **operación binaria** y satisface para todo $x, y, z \in G$:

1. $(x * y) * z = x * (y * z)$ (Axioma de Asociatividad)
2. existe $e \in G : x * e = e * x = x$ (Axioma del Neutro)
3. para cada $x \in G$ existe $y \in G : x * y = y * x = e$ (Axioma del Inverso)

además, si se cumple que para cada $x, y \in G$, $x * y = y * x$ (Axioma de conmutatividad) diremos que $(G, *)$ es un **grupo abeliano**.

En ocasiones el grupo G es denotado por el par $(G, *)$ para resaltar la importancia de la operación binaria $*$ en la definición de la estructura.

Observación 1.1.2. Algunos resultados conocidos para grupos.

1. El elemento neutro $e \in G$ de un grupo es único y, para cada $x \in G$ el elemento inverso $y \in G$ es único y suele ser denotado por x^{-1}.

2. Sean $g_1, g_2, h \in G$ tales que $g_1 h = g_2 h$ entonces $g_1 = g_2$, análogament, si $h g_1 = h g_2$ se sigue que $g_1 = g_2$. Esta propiedad recibe el nombre de **propiedad cancelativa**.

3. Para todo $x \in G$ el inverso del inverso coincide con x; esto es $(x^{-1})^{-1} = x$.

Estos resultados se pueden verificar facilmente usando las propiedades de la Definición 1.1.1.

Ejemplo 1.1.3. A continuación se exhiben algunos ejemplos de grupos.

1. El par $(\mathbb{Z}, +)$. Los enteros con la suma ordinaria en $\mathbb{Z}$ cumplen la Definición 1.1.1 y decimos que forman un *grupo aditivo* donde $e = 0$ y para cada $z \in \mathbb{Z}$ el *inverso aditivo* de z es $-z$.

2. El par $(\mathbb{Q}-\{0\},\cdot)$. Los racionales con el producto usual de los reales satisfacen tambien la definición anterior y diremos que forman un *grupo multiplicativo*, donde $e=1$ y para cada $p/q\in\mathbb{Q}$ con $p,q\in\mathbb{Z}-\{0\}$, se tiene que , $(p/q)^{-1}=q/p$.

3. El conjunto de las matrices cuadradas con entradas en los números reales $\mathbb{R}$ no singulares, es decir, $\mathcal{M}_{n\times n}(\mathbb{R})=\{A\in M_{n\times n}(\mathbb{R}):\det(A)\neq 0\}$ con el producto usual de matrices forma un grupo multiplicativo en el cual el elemento neutro es $e=I_n$ (*la matriz identidad*) y para cada A con $\det(A)\neq 0$, su inverso es precisamente la matriz inversa de A, es decir A^{-1}.

En el ejemplo 1.1.3 los dos primeros grupos listados son abelianos, mientras que el tercero no lo es.

Definición 1.1.4. Sean $(G,*)$ un grupo, $H\subseteq G$ con $H\neq\emptyset$. Diremos que H es un **subgrupo** de G y denotaremos esto por $H\leqslant G$, si el par $(H,*|_{H\times H})$ es un grupo.

Ejemplo 1.1.5. En cada inciso, exhibimos un grupo y subgrupos del mismo.

1. Es claro que si G es un grupo, entonces $G\leqslant G$ y $\{e\}\leqslant G$ estos reciben el nombre de **subgrupos triviales**.

2. Para el grupo $(\mathbb{Z},+)$ el conjunto $H_1=2\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$. (El conjunto de los numeros pares de $\mathbb{Z}$.)

3. En el grupo de los numeros reales con la suma usual $(\mathbb{R},+)$, el subconjunto $\mathbb{Z}$ es un subgrupo.

Teorema 1.1.6. *Sea $(G,*)$ un grupo y $H\subseteq G$ con $H\neq\emptyset$. Entonces $H\leqslant G$ si y sólo si para todo $a,b\in H$:*

(i) $a*b\in H$

(ii) $a*b^{-1}\in H$

más aún, si G es un grupo abeliano, H también lo es.

Definición 1.1.7. Sean $(G,\cdot)$[1] un grupo y $H\leqslant G$. Para cada $g\in G$ definimos:

(i) La clase lateral derecha del elemento a relativa a H como el conjunto $Ha:=\{ha:h\in H\}$.

(ii) La clase lateral izquierda del elemento a relativa a H como el conjunto $aH:=\{ah:h\in H\}$.

Observación 1.1.8. Sea G un grupo.

- Si G es un grupo aditivo, entonces las clases laterales derechas e izquierdas se denotan por $H+a$ y $a+H$ respectivamente.

- Cabe mencionar que si G no es un grupo abeliano, no necesariamente $Ha=aH$.

1 Usamos la notación multiplicativa para la operación binaria "$\cdot$", es decir, para todo $a,b\in G$, la expresión $a\cdot b$ será representado solo por ab

Ejemplo 1.1.9. Considérese el grupo de permutaciones de tres elementos, es decir, el grupo simétrico:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

por simplicidad, denotémoslo por $S_3 = \{i, \alpha, \beta, \gamma, \delta, \epsilon\}$, donde i es el elemento neutro.

$$\begin{aligned} \gamma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = i \\ \beta\gamma &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \epsilon \\ \gamma\beta &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \delta \end{aligned}$$

Como $\gamma^2 = i$, $H = \{i, \gamma\} \leqslant S_3$. Sin embargo note $\beta H = \{\beta, \epsilon\}$ mientras que $H\beta = \{\beta, \delta\}$, exhibiendo claramente que $\beta H \neq H\beta$.

El ejemplo 1.1.9 y la observación 1.1.8 nos invitan a pensar en las características de los grupos tales que sus clases laterales relativas a un subgrupos H coinciden, es decir, $aH = Ha$ para todo $a \in G$ y $H \leqslant G$, por este motivo, presentamos la siguiente:

Definición 1.1.10. Sean G un grupo, $N \leqslant G$. Si se cumple que para todo $a \in G$: $aN = Na$ entonces diremos que N es **subgrupo normal** de G y denotaremos esto por $N \lhd G$. En general, para cada $a \in G$ diremos que aN es la clase lateral de a relativa a N.

Observación 1.1.11.

1. Es claro que para todo grupo G, $G \lhd G$ y $\{e\} \lhd G$.
2. Si G es un grupo abeliano, $H \leqslant G$ y $a \in G$ tenemos que $aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha$, así, $H \lhd G$, en otras palabras, *todo subgrupo de un grupo abeliano, es normal*.

Teorema 1.1.12. *Sea G un grupo, $a \in G$ y $N \leqslant G$. Luego las siguientes proposiciones son equivalentes:*

(i) $N \lhd G$

(ii) $a^{-1}Na = N$

(iii) $a^{-1}Na \subseteq N$

Definición 1.1.13. Sean G un grupo y $N \lhd G$, el conjunto de las clases laterales relativas a N se denota mediante $G/N := \{aN : a \in G\}$ y se define la función:

$$\begin{array}{rccc} \odot : & G/N \times G/N & \longrightarrow & G/N \\ & (aN, bN) & \longmapsto & (ab)N \end{array}$$

Lema 1.1.14. *El par $(G/N, \odot)$ es un grupo. Más aún, si G es un grupo abeliano, G/N también lo es.*

Demostración. Veamos que $\odot$ está bien definida. Sean $aN, a'N, bN, b'N \in G/N$ tales que $aN = a'N$ y $bN = b'N$. Como $N \leqslant G$ entonces $e \in N$, así, $a = ae \in aN = a'N$, luego existe $n_a \in N$ tal que $a = a'n_a$, análogamente existe $n_b \in N$ tal que $b = b'n_b$, entonces tenemos que, $(ab) = ((a'n_a)(b'n_b)) = (a'(n_ab')n_b)$ por la asociatividad en G. Dado que $nN = N$ siempre que $n \in N$ tenemos que $(a'(n_ab')n_b)N = (a'(n_ab')N$. Como $N \lhd G$, entonces $Nb' = b'N$, luego existe $n \in N$ tal que $n_ab' = b'n$ entonces tenemos que $a'(n_ab')N = a'(b'n)N = (a'b')N$ esto es $(ab)N = (a'b')N$ luego $(aN) \odot (bN) = (a'N) \odot (b'N)$, así, $\odot$ está bien definida. Sean $aN, bN, cN \in G/N$ entonces $(aN \odot bN) \odot (cN) = ((ab)N) \odot (cN) = ((ab)c)N = (a(bc))N$ por la asociatividad en G. Luego $(aN \odot bN) \odot (cN) = (a(bc))N = (aN) \odot ((bc)N) = (aN) \odot (bN \odot cN)$ entonces $\odot$ es asociativa. Afirmamos que $eN = N$ es el neutro de G/N. En efecto, sea $aN \in G/N$ entonces $aN \odot eN = (ae)N = aN = (ea)N = eN \odot aN$, por lo tanto, $N \in G/N$ es el neutro. Finalmente, dado $aN \in G/N$, si elegimos $(a^{-1})N$ tenemos que $aN \odot (a^{-1})N = (aa^{-1})N = eN = N = eN = (a^{-1}a)N = (a^{-1})N \odot aN$ por lo tanto $(a^{-1})N = (aN)^{-1}$ y podemos concluir que $(G/N, \odot)$ es un grupo. Supóngase que G es un grupo abeliano y sean $aN, bN \in G/N$, entonces, $aN \odot bN = (ab)N = (ba)N = bN \odot aN$, así, G/N es un grupo abeliano. □

Lema 1.1.15. *Sean G un grupo y $H \leqslant G$ entonces dos clases laterales son disjuntas o son iguales, es decir, $aH \cap bH = \emptyset$ o $aH = bH$, para todo, $a, b \in G$.*

HOMOMORFISMOS DE GRUPOS

Definición 1.2.1. Sean $(G, *)$ y $(G', \cdot)$ grupos. Si ϕ es una función de G en G' tal que preserva las operaciones entre grupos, es decir, $\phi(x * y) = \phi(x) \cdot \phi(y)$, diremos que ϕ es un **homomorfismo de grupos**, en el caso particular donde $G = G'$, diremos que ϕ es un **endomorfismo**.

Nota. Si ϕ es un homomorfismo de grupos y es una función inyectiva, diremos que es un **monomorfismo**[2]. Por otro lado, si ϕ es una función sobreyectiva (suprayectiva), le llamaremos un **epimorfismo**[3]. En caso de que ϕ sea un función biyectiva, diremos que es un **isomorfismo**, los grupos G y G' se dirán **isomorfos**, y esto se denotará mediante $G \simeq G'$.

Ejemplo 1.2.2. Mostraremos algunos ejemplos de homomorfismos entre grupos.

(i) Sean $G = \mathbb{Z}$ y $G' = 2\mathbb{Z}$. Como vimos, $G' \leqslant G$ así, G' es un grupo. Considérese la función:

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & 2\mathbb{Z} \\ & n & \longmapsto & 2n \end{array}$$

Sean $n, m \in \mathbb{Z}$ entonces $\phi(n+m) = 2(n+m) = 2n + 2m = \phi(n) + \phi(m)$, es decir, ϕ es un homomorfismo. Más aún sabemos que si $2n = 2m$ entonces

2 El concepto de monomorfismo está definido por leyes cancelativas en Teoría de Categorías, sin embargo, para la categoria de grupos, los conceptos de monomorfismo y morfismo inyectivo coinciden.

3 De manera similar a los monomorfismos, el concepto de epimorfismo esta definido por leyes cancelativas, sin embargo, para grupos los epimorfismos y los morfismos suprayectivos coinciden.

$2(n-m) = 0$ y como $2 \neq 0$ tenemos que $n = m$, así, $\phi(n) = \phi(m)$ implica $n = m$, es decir, ϕ es un monomorfismo. Dado $y \in 2\mathbb{Z}$ entonces existe $n \in \mathbb{Z}$ tal que $y = 2n = \phi(n)$, luego ϕ es un epimorfismo, por lo tanto, es un isomorfismo. Por la Definición 1.2.1, $\mathbb{Z} \simeq 2\mathbb{Z}$.

(ii) Considérese a $G = (0, \infty) = \mathbb{R}^+$ con el producto usual entre reales y $G' = \mathbb{R}$ con la suma usual, la función:

$$\begin{array}{rccc} \log: & (\mathbb{R}^+, \cdot) & \longrightarrow & (\mathbb{R}, +) \\ & x & \longmapsto & \log(x) \end{array}$$

satisface que $\log(xy) = \log(x) + \log(y)$, así $\log$ es un homomorfismo y sabemos que $\log$ es una función biyectiva, por lo tanto, $\log$ es un isomorfismo de grupos, así, $\mathbb{R} \simeq (0, \infty)$.

(iii) Sea $H \leqslant G$ entonces la función $\iota : H \longrightarrow G$ tal que $\iota(h) = h$ para toda $h \in H$ es un homomorfismo de grupos, llamado **inclusión** de H en G, además, éste es único.

(iv) Sean $(G, *)$, $(G', \cdot)$ grupos y e' el elemento neutro en G'. Una función $f : G \longrightarrow G'$ que satisface $f(g) = e'$ para todo $g \in G$ es un homomorfismo y recibe el nombre de **homomorfismo neutro** y se denota mediante $f = \overline{e}$.

Es importante notar que el segundo ejemplo muestra como pueden relacionarse dos operaciones binarias diferentes entre grupos mediante un homomorfismo. En lo sucesivo hablaremos de los homomorfismos en general y sus propiedades relacionadas con los subgrupos de un grupo.

Teorema 1.2.3. *Sea ϕ un homomorfismo de $(G, *)$ en $(G', \cdot)$, entonces $\phi(e) = e'$ donde e y e' son los elementos identidad en G y G', respectivamente, y $\phi(a^{-1}) = \phi(a)^{-1}$ para cada $a \in G$.*

Definición 1.2.4. Sean G y G' grupos, ϕ un homomorfismo de G en G'. Definimos

- La **imagen de** ϕ como $\mathrm{Im}\phi := \{\phi(a) : a \in G\}$.
- El **núcleo** o **kernel de** ϕ como $\ker\phi := \{a \in G : \phi(a) = e'\}$.

Un lema que será de utilidad en lo sucesivo, es el siguiente:

Lema 1.2.5. *Sean G, G' grupos y $\phi : G \longrightarrow G'$ un homomorfismo de grupos, entonces:*

(i) *ϕ es suprayectiva si y sólo si $\mathrm{Im}\phi = G'$.*

(ii) *ϕ es un inyectiva si y sólo si $\ker\phi = \{e\}$.*

Definición 1.2.6. Sea G un grupo, $H \leqslant G$ y $a, b \in G$ diremos que a es **congruente con** b **módulo** H si y sólo si $ab^{-1} \in H$, denotaremos esto por $a \equiv b \mod H$.

Observación 1.2.7. Relativo a la Definición 1.2.6.

1. Hemos usado la notación multiplicativa para denotar la operación binaria en G.

2. *La relación de congruencia módulo un subgrupo es una relación de equivalencia*, por consiguiente, induce una partición en G, de modo que $G/\pmod H := \{\overline{a} : a \in G\}$ donde cada $\overline{a} := \{x \in G : x \equiv a \pmod H\}$.

Corolario 1.2.8. *Si G es un grupo y $H \lhd G$ entonces para cada elemento de $G/(\mathrm{mód}\, H)$ tenemos que $\overline{a} = aH$; en virtud de esto, podemos denotar que $G/\pmod H = G/H$, más aún, $aH = bH$ si y sólo si $ab^{-1} \in H$.*

Teorema 1.2.9. *Sean G, G' grupos, $N \lhd G$, entonces:*

(i) *La función $\nu : G \longrightarrow G/N$ que a cada elemento $g \in G$ lo relaciona con la clase lateral gN, es un epimorfismo de grupos y recibe el nombre de **epimorfismo natural** y es tal que $\ker \nu = N$.*

(ii) *Si $\phi : G \longrightarrow G'$ es un homomorfismo de grupos, $\mathrm{Im}\phi \leqslant G'$, $\ker \phi \lhd G$ y la función:*

$$\begin{array}{rccc} \overline{\phi}: & G/\ker\phi & \longrightarrow & \mathrm{Im}\phi \\ & g\ker\phi & \longmapsto & \phi(g) \end{array}$$

es un isomorfismo de grupos.

Demostración. (i) Sean $g_1, g_2 \in G$, luego $\nu(g_1g_2) = (g_1g_2)N = g_1N \odot g_2N = \nu(g_1) \odot \nu(g_2)$ entonces ν es un homomorfismo. Es claro que $\mathrm{Im}\nu \subseteq G/N$ y dado $y \in G/N$ existe $g \in G$ tal que $y = gN = \nu(g)$, así, $y \in \mathrm{Im}\nu$ y $G/N \subseteq \mathrm{Im}\nu$ entonces $\mathrm{Im}\nu = G/N$, esto implica que ν es un epimorfismo. Finalmente, si $g \in \ker \nu$ entonces $\nu(g) = N$, es decir, $gN = N$ lo cual implica que $g \in N$, así, $\ker \nu \subseteq N$, por otro lado, si $g \in N$ tenemos que $gN = N$, luego $\nu(g) = N$, así $g \in \ker \nu$ entonces $\ker \nu \subseteq N$ y por lo tanto, $\ker \nu = N$.

(ii) Sean $y_1, y_2 \in \mathrm{Im}\phi$, entonces existen $g_1, g_2 \in G$ tales que $\phi(g_1) = y_1, \phi(g_2) = y_2$, como $y_1y_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) \in \mathrm{Im}\phi$ y, por el Teorema 1.2.3 $\phi(g_2^{-1}) = (\phi(g_2))^{-1} = y_2^{-1}$, entonces $y_1y_2^{-1} = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1g_2^{-1}) \in \mathrm{Im}\phi$, es decir, $y_1y_2^{-1} \in \mathrm{Im}\phi$, por el Teorema 1.1.6; $\mathrm{Im}\phi \leqslant G'$. Sean $g_1, g_2 \in \ker \phi$ entonces $\phi(g_1) = \phi(g_2) = e'$ luego $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = e'e' = e'$ por lo tanto, $g_1g_2 \in \ker \phi$, entonces $\phi(g_2^{-1}) = \phi(g_2)^{-1} = (e')^{-1} = e'$. entonces $\phi(g_1g_2^{-1}) = e'e' = e'$ por lo tanto, $g_1g_2^{-1} \in \ker \phi$, nuevamente por el Teorema 1.1.6, $\ker \phi \leqslant G$. Sean $g \in \ker \phi$ y $x \in G$ entonces $\phi(xgx^{-1}) = \phi(x)\phi(g)\phi(x)^{-1} = \phi(x)e'\phi(x)^{-1} = \phi(x)\phi(x)^{-1} = e'$, por lo tanto, $xgx^{-1} \in \ker \phi$ es claro que, $x \ker \phi x^{-1} \subseteq \ker \phi$, luego por el Teorema 1.1.12(iii), $\ker \phi \lhd G$. Para ver que $\overline{\phi}$ es un isomorfismo, considere $y \in \mathrm{Im}\phi$ entonces existe $g \in G$ tal que $y = \phi(g)$. Si elegimos $g\ker\phi \in G/\ker\phi$ es claro que $\overline{\phi}(g\ker\phi) = \phi(g) = y$, así $\mathrm{Im}\phi \subseteq \mathrm{Im}\overline{\phi}$. Si $y \in \mathrm{Im}\overline{\phi}$ entonces existe $g\ker\phi$ tal que $\overline{\phi}(g\ker\phi) = y$ pero $\phi(g) = \overline{\phi}(g\ker\phi)$, así $y = \phi(g)$ y en consecuencia, $g \in \mathrm{Im}\phi$, luego $\mathrm{Im}\overline{\phi} \subseteq \mathrm{Im}\phi$ y por lo tanto, $\mathrm{Im}\overline{\phi} = \mathrm{Im}\phi$, por el Lema 1.2.5 ϕ es un epimorfismo. En la prueba del Lema 1.1.14 mostramos que G/N es un grupo con elemento identidad N, en este caso $\ker\phi$ es la identidad de $G/\ker\phi$. Por el Teorema 1.2.3 $\{\ker\phi\} \subseteq \ker\overline{\phi}$. Por otro lado, sea $g\ker\phi \in \ker\overline{\phi}$ entonces $\overline{\phi}(g\ker\phi) = e'$, pero $\overline{\phi}(g\ker\phi) = \phi(g)$, entonces $\phi(g) = e'$ así $g \in \ker\phi$ por lo tanto, $g\ker\phi = \ker\phi$ así $\ker\overline{\phi} \subseteq \{\ker\phi\}$ i.e. $\ker\overline{\phi} = \{\ker\phi\}$, por el Lema 1.2.5 $\overline{\phi}$ es un monomorfismo y por lo tanto, un isomorfismo de grupos. □

Teorema 1.2.10. *Sean* G, G' *grupos,* $\phi : G \longrightarrow G'$ *un epimorfismo de grupos, entonces:*

(i) Si $N \leqslant G$ *entonces* $\phi(N) \leqslant G'$ *y* $N \lhd G$ *implica* $\phi(N) \lhd G'$.

(ii) Sea $N' \leqslant G'$, *entonces* $\phi^{-1}(N') \leqslant G$, $\ker\phi \subseteq \phi^{-1}(N')$, $\phi^{-1}(N')/\ker\phi \simeq N'$ *y* $N' \lhd G'$ *implica que* $\phi^{-1}(N') \lhd G$.

(iii) Si $N \lhd G$, *nombremos* $N' = \phi(N)$ *entonces la función:*

$$\begin{array}{rccc} \phi' : & G/N & \longrightarrow & G'/N' \\ & gN & \longmapsto & \phi(g)N' \end{array}$$

es un homomorfismo de grupos, y si $\ker\phi \subseteq N$ *entonces* $\phi^{-1}(\phi(N)) = N$ *y* ϕ' *es un isomorfismo de grupos.*

PRODUCTO DIRECTO DE GRUPOS

Definición 1.3.1. Sea G un grupo, $H, K \subseteq G$ definimos el producto de H con K como el conjunto $HK := \{hk : h \in H \text{ y } k \in K\}$.

Teorema 1.3.2. *Sea* G *un grupo,* $H \leqslant G$ *y* $N \lhd G$ *entonces:*

(i) $HN \leqslant G$, $N \lhd HN$ *y* $(H \cap N) \lhd H$.

(ii) *La función:*

$$\begin{array}{rccc} \phi : & HN & \longrightarrow & H/(H \cap N) \\ & hn & \longmapsto & h(H \cap N) \end{array}$$

es un homomorfismo de grupos, $\ker\phi = N$ *y* $(HN)/N \simeq H/(H \cap N)$.

En general, no se cumple que si $H, K \leqslant G$ entonces $HK \leqslant G$, en el teorema anterior se requirió de la hipótesis adicional de que alguno de los subgrupos sea normal. Por otro lado un resultado de mucha utilidad y que tiene relación con los subgrupos, es el Teorema de Lagrange, pero antes de enunciarlo requerimos definir algunos conceptos adicionales.

Definición 1.3.3. Sea $(G, *)$ un grupo, $g \in G$ y e la identidad del grupo entonces definimos:

1. $g^1 = g$ y para todo $n \in \mathbb{N}$: $g^{n+1} = g^n * g^1$, y además, $g^0 = e$.

2. Si para todo $n \in \mathbb{N}$ tenemos que $g^n \neq e$ entonces diremos que g es un elemento de **orden infinito** en G y denotaremos esto por $\mathrm{ord}(g) = \infty$, de lo contrario diremos que g es un elemento de **orden finito** en G y diremos que el **orden** g es el mínimo natural m tal que $g^m = e$ y denotamos esto por $\mathrm{ord}(g) = m$.

3. Si $|G| \in \mathbb{N} \cup \{0\}$ diremos que G es un **grupo finito** y llamaremos **orden del grupo** G a la cardinalidad del grupo. Por otro lado si G es un conjunto infinito, diremos que G es un grupo de **orden infinito**.

Lema 1.3.4. *Sea* G *un grupo con elemento identidad* e*, entonces:*

(i) $\mathrm{ord}(e) = 1$ *y para todo* $n \in \mathbb{N}$*:* $(g^n)^{-1} = (g^{-1})^n$ *y denotaremos* $g^{-n} = (g^n)^{-1}$.

(ii) *Si* G *es un grupo finito entonces todo elemento es de orden finito en* G.

(iii) *Si* $\mathrm{ord}(g) = m$ *entonces para cada* $l \in \mathbb{Z}$ *tenemos que* $g^l = g^r$ *para algún* $0 \leqslant r \leqslant m-1$.

(iv) *Si* g *es un elemento de orden finito en* G *tal que* $\mathrm{ord}(g) = m$*, entonces el conjunto* $H = \{e, g, g^2, \ldots, g^{m-1}\}$ *es un subgrupo de* G *de orden* m.

(v) *Para todo* $n \in \mathbb{N}$*:* $g^n = e$ *si y sólo si* $\mathrm{ord}(g) \mid n$.

Teorema 1.3.5 (de Lagrange)**.** *Sea* G *un grupo finito,* $H \leqslant G$ *y denotemos por* $o(G)$ *y* $o(H)$ *a los órdenes de* G *y* H *respectivamente, entonces* $o(H)|o(G)$.

Demostración. Dado que G es un grupo finito, H lo es, por consiguiente, el grupo cociente $G/H = \{gH : g \in G\}$ es finito. Sean $g_1H, g_2H \ldots, g_mH$ para algún $m \in \mathbb{N}$, todos los elementos de G/H. Como G/N es una partición de G, $|G| = \sum_{i=1}^{m} |g_iH|$ ya que las clases H_i y H_j son disjuntas cada vez que $i \neq j$ (ver Lema 1.1.15). Note que $g_iH = \{g_ih_1, g_ih_2, \ldots g_ih_l\}$ con $l = o(H)$, y $g_ih_j = g_ih_k$ implica que $h_j = h_k$, así, todos los elementos de g_iH son distintos entre si y $|g_iH| = o(H)$, es decir, $o(G) = |G| = \sum_{i=1}^{m} |g_iH| = \sum_{i=1}^{m} o(H) = o(H)m$, por lo tanto, $o(H)|o(G)$. □

Definición 1.3.6. Sean G un grupo, $H \leqslant G$. Al número de clases gH inducidas por la relación de congruencia módulo H en G le llamaremos el **índice** de G en H y lo denotaremos por $[G : H]$.

Corolario 1.3.7. *Sea* G *un grupo finito,* $H \leqslant G$ *entonces se cumple:*

(i) $\forall g \in G : (\mathrm{ord}(g)|o(G)$ *y* $g^{o(G)} = e)$.

(ii) $o(G) = [G : H]o(H)$

(iii) *Si* $H \lhd G$ *entonces* $o(G/N) = \dfrac{o(G)}{o(H)}$

(iv) *Si* $N \lhd G$ *entonces* $o(HN) = \dfrac{o(H)o(N)}{o(H \cap N)}$

Demostración. Probaremos solamente el inciso (iv). Sea $N \lhd G$, por el Teorema 1.3.2 tenemos que $HN \leqslant G$, $N \lhd HN$, $(H \cap N) \lhd H$ y $(HN)/N \simeq H/(H \cap N)$ y por el Teorema 1.3.5, tenemos que, $o(HN/N) = o(HN)/o(N)$ y $o(H/(H \cap N)) = o(H)/o((H \cap N))$. Del hecho de que estos grupos cociente son isomorfos, sus órdenes deben ser iguales, despejando $o(HN)$, tenemos que, $o(HN) = o(H)o(N)/o(H \cap N)$. □

Definición 1.3.8. Sean G un grupo, $H_1, H_2, \ldots, H_r \leqslant G$. Diremos que G es **producto directo** de $H_1, H_2, \ldots, H_r$ y denotaremos esto por $G = H_1 \times H_2 \times \cdots \times H_r$ si y sólo si:

i) $H_i \lhd G$ para toda $i \in \{1, 2, \dots r\}$

ii) $G = H_1 H_2 \cdots H_r$

iii) $H_i \cap \prod_{1 \leqslant j \neq i \leqslant r} H_j$

Corolario 1.3.9. *Sea* G *un grupo finito,* $H, K \leqslant G$ *tales que* $G = H \times K$*, entonces* $|G| = |H||K|$.

Demostración. Por la Definición 1.3.8, $H, K \lhd G$, $G = HK$ y $H \cap K = \{e\}$, entonces, por el Corolario 1.3.7(iv),

$$|G| = |HK| = \frac{|H||K|}{|(H \cap K)|} = \frac{|H||K|}{1} = |H||K|. \tag{1.3.1}$$

□

A continuación, estudiaremos algunos grupos con propiedades muy particulares y los resultados obtenidos en éstos serán de suma importancia al analizar los grupos de unidades en un anillo de Galois.

GRUPOS CÍCLICOS Y GRUPOS ABELIANOS FINITOS

A lo largo de esta sección, G denotará a un grupo abeliano finito de orden q, por el Lema 1.3.4 (ii) tenemos que todo elemento $g \in G$ es de orden finito digamos $\mathrm{ord}(g) = m$ y por la parte (iv) de ese mismo lema, el conjunto $\{e, g, g^2, \dots, g^{m-1}\}$ es un subgrupo de G de orden m, sabiendo esto introducimos la siguiente:

Definición 1.4.1. Sea G un grupo y $g \in G$ con $\mathrm{ord}(g) = m$, el subgrupo $H = \{e, g, g^2, \dots, g^{m-1}\}$ se llama **subgrupo cíclico** generado por g y se denotará por $\langle g \rangle$. Más aún, si existe algún $g_0 \in G$ con $G = \langle g_0 \rangle$ diremos que G es un **grupo cíclico** generado por g_0 y g_0 se llamará un **generador** de G.

Lema 1.4.2. *Todo grupo cíclico es abeliano y si* G *es un grupo cíclico, todo subgrupo de* G *es cíclico.*

Teorema 1.4.3. *Sean* G *un grupo finito y* $g \in G$ *con* $\mathrm{ord}(g) = q$ *entonces* $\mathrm{ord}(g^t) = q/\mathrm{mcd}(t, q)$ *para todo* $t \in \mathbb{Z}$.

Corolario 1.4.4. *Sea* G *un grupo cíclico generado por* g *donde* $g \in G$ *es tal que* $\mathrm{ord}(g) = q$. *Para todo* $t \in \mathbb{Z}$, g^t *es un generador de* G *si y sólo si* $\mathrm{mcd}(q, t) = 1$.

Teorema 1.4.5. *Sea* G *un grupo abeliano finito.*

(i) *Si* $o(G) = p$ *entonces* G *es cíclico.*

(ii) *Si* $o(G) = p^n$. *Entonces* G *es cíclico si y sólo si tiene un único subgrupo* H *con* $o(H) = p$.

(iii) *Si* $o(G) = p^n$ *con* $n \geqslant 2$ *y* G *no es cíclico entonces existe* $H \leqslant G$ *y un* $a \in G$ *tal que* $\mathrm{ord}(a) = \max\{\mathrm{ord}(g) : g \in G\}$ *y* $G = \langle a \rangle \times H$.

Demostración. Solamente exhibiremos la parte (iii) de este resultado. Como G es finito, entonces el conjunto $\{ord(g) : g \in G\}$ es un subconjunto finito de los naturales, entonces existen el mínimo y el máximo de éste. Sea pues $a \in G$ tal que $ord(a) = máx\{ord(g) : g \in G\}$, para demostrar esto, haremos inducción sobre n. Si $n = 2$, $o(G) = p^2$ y para $a \in G$ es claro que $ord(a)|p^2$, entonces, $ord(a) \in \{1, p, p^2\}$. Si $ord(a) = 1$ entonces $a = e$ y como $ord(a)$ es máximo entonces todo elemento de G es orden 1, por lo tanto, $G = \{e\}$ lo cual es una contradicción, por otro lado, si $ord(a) = p^2$ entonces $G = \langle a\rangle$ y así, G es cíclico, otra contradicción, por lo tanto, $ord(a) = p$. Por el inciso (ii), al no ser G cíclico, entonces existen al menos dos subgrupos de orden p en G, sean estos $\langle a\rangle$ y P, además tenemos que P debe ser cíclico pues $o(P) = p$, entonces, $P = \langle g\rangle$ para algún $g \in P$. Veamos que $\langle a\rangle \cap \langle g\rangle = \{e\}$. Si existiera $h \in [\langle a\rangle \cap \langle g\rangle] - \{e\}$ entonces $h = a^i$ y $h = g^j$ donde $i, j \in \{1, \dots p-1\}$, entonces $a^i = g^j$, lo cual implica que, $\langle a^i\rangle = \langle g^j\rangle$ y como $mcd(i, p) = mcd(j, p) = 1$, se sigue que $\langle a\rangle = \langle a^i\rangle = \langle g^j\rangle = \langle g\rangle$, lo cual contradice que $\langle a\rangle$ y $P = \langle g\rangle$ son distintos, por lo tanto, $\langle a\rangle \cap P = \{e\}$, entonces, $|\langle a\rangle P| = |\langle a\rangle||P| = p \cdot p = p^2 = |G|$, es decir, $G = \langle a\rangle P$ y como $\langle a\rangle, P \lhd G$, ya que G es abeliano, por la Definición 1.3.8, $G = \langle a\rangle \times P$.

Supóngase que, para todo $m \in \mathbb{N}$ con $2 \leqslant m < n$ si G' es un grupo con $o(G') = p^m$ y no es cíclico, se cumple la conclusión del inciso (iii) y considérese G un grupo con $o(G) = p^n$ que no es cíclico. Por lo anterior, existen al menos dos subgrupos diferentes con orden p y como $ord(a)|o(G) = p^n$ entonces $ord(a) = p^l$ para $l \in \{1, 2, \dots, p^n - 1\}$. Como $\langle a\rangle$ es cíclico, se sigue del inciso (ii) que tiene un único subgrupo de orden p, llamemśle P_a y podemos encontrar otro $P \leqslant G$ con $P \nsubseteq \langle a\rangle$ siempre y cuando $P \neq P_a$, pues si $P \subseteq \langle a\rangle$ por la unicidad de P_a tendríamos que $P = P_a$. Usando el epimorfismo natural:

$$\begin{array}{rccc} \nu: & G & \longrightarrow & G/P \\ & g & \longmapsto & gP \end{array}$$

Veamos que $ord(\nu(a)) = ord(a)$. Como $(\nu(a))^{p^l} = (aP)^{p^l} = a^{p^l}P = eP = P$ entonces $ord(\nu(a))|p^l$ entonces $ord(\nu(a)) = p^k$ con $k \leqslant l$ entonces $(\nu(a))^{p^k} = a^{p^k}P = P$ esto implica que $a^{p^k} \in P$, y como $P = \langle g\rangle$ entonces $a^{p^k} = g^i$ para algún $i \in \{0, 1, \dots, p-1\}$. Si $i > 0$ entonces $(i, p) = 1$ y por lo tanto, existen $j, j' \in \mathbb{Z}$ tales que $ij + j'p = 1$ entonces $ij - 1 = j'p$, es decir, $ij \equiv 1(\mod p)$ entonces $g = g^{ij} = a^{jp^k} \in \langle a\rangle$ esto implica que $P = \langle g\rangle \subseteq \langle a\rangle$ lo cual es una contradicción, por lo tanto, $i = 0$ y así $a^{p^k} = e$ esto es $ord(\nu(a)) = p^l = ord(a)$, por lo tanto, para $aP \in G/P$ tenemos que $ord(aP) = ord(a)$, entonces aP es el elemento de orden máximo en G/P y, como $P \lhd G$ pues G es abeliano, tenemos que $o(G/N) = o(G)/o(P) = p^{n-1}$ y, por la hipotesis inductiva, existe $H' \leqslant G/P$ tal que $G/P = \langle aP\rangle \times H'$. Nombremos $H = \nu^{-1}(H')$, por el Teorema 1.2.10 (ii), $P = \ker(\nu) \subseteq H$ y $H/P \simeq H'$. Tenemos que $\langle a\rangle H \subseteq G$ y dado $x \in G$ entonces $xP \in G/P = \langle aP\rangle \times H'$ entonces $xP = (a^iP)(hP) = (a^ih)P$ con $i \in \{0, 1, \dots, p-1\}$ y $h \in H$ así, $x^{-1}a^ih \in P \subseteq H$ luego, existe $h_0 \in H$ con $x^{-1}a^ih = h_0$ entonces $x^{-1}a^ih(h_0)^{-1} = e$ por lo tanto, $x = a^ih_1$ con $h_1 = h(h_0)^{-1} \in H$ se sigue que $x \in \langle a^i\rangle H$, es decir, $G \subseteq \langle a\rangle H$ y así tenemos que $G = \langle a\rangle H$. Ahora, dado $x \in \langle a\rangle \cap H$ es claro que $xP \in \langle aP\rangle \cap H' = \{P\}$ entonces $xP = P$ y por lo tanto, $x \in P$, así $P \subseteq \langle a\rangle \cap H$. Como $P \subseteq H$ entonces de la contención anterior tenemos que $P \subseteq \langle a\rangle$ o bien $\langle a\rangle \cap H = \{e\}$ puesto que $(\langle a\rangle \cap H)$ es un subgrupo de G contenido en

un subgrupo de orden p, pero la primer contención no se da por ser $P \neq P_a$ por lo tanto, $\langle a \rangle \cap H = \{e\}$, así, $G = \langle a \rangle \times H$. □

Las propiedades de los grupos abelianos finitos son numerosas, sin embargo, para nuestros fines el estudio de los resultados anteriores resulta suficiente, por lo tanto, concluimos esta sección para dar paso al estudio de una nueva estructura.

ANILLOS

Definición 1.5.1. Sean R un conjunto no vacío, $+$ y $\cdot$ dos operaciones binarias sobre R, las cuales llamaremos *suma* y *producto* respectivamente, tales que $(R, +)$ es un grupo abeliano con elemento neutro para la suma denotado por 0 y para todos $x, y, z \in R$ se satisface:

1.	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	(Axioma de Asociatividad)
2a).	$x \cdot (y + z) = x \cdot y + x \cdot z$	(Axioma de Distributividad)
2b).	$x \cdot y = y \cdot x$	(Axioma de Conmutatividad)

y existe un elemento $1_R \neq 0$, tal que, para todo $x \in R$, $x \cdot 1_R = x$, diremos que la quíntupla $(R, +, \cdot, 0, 1_R)$ es un **anillo conmutativo con unidad**. Si R es un conjunto finito, diremos que la quíntupla es un anillo **finito** conmutativo con unidad.

Observación 1.5.2.

1. Usaremos la notación multiplicativa para el producto en R, esto es, $x \cdot y = xy$.

2. Al elemento 1_R se le llama **unidad** del anillo R. Cuando el contexto sea claro, el elemento 1_R, sólo se denotará mediante 1; además éste es único.

3. Para cada $r \in R$, $1 \in \mathbb{N}$, se define $1r = r$ y para todo $n \in \mathbb{N}$ $(n+1)r = nr + r$.

4. La **característica** del anillo R, es el mínimo $n \in \mathbb{N}$ tal que $n1_R = 0$, es decir, la característica del anillo R es el orden del elemento identidad 1_R en el grupo aditivo $(R, +)$ (ver Definición 1.3.3). Se denotará la característica de un anillo mediante $Car(R)$.

5. En lo sucesivo R denotará a un anillo finito conmutativo con unidad 1_R, aunque sólo se refiera a éste como anillo.

Ejemplo 1.5.3. Exhibimos algunos ejemplos de anillos con unidad.

1. La quíntupla $(\mathbb{Z}, +, \cdot, 0, 1)$ es un anillo conmutativo con unidad con la suma y producto usuales de los enteros, y el elemento identidad es $1_{\mathbb{Z}} = 1$.

2. La quíntupla $(\mathbb{Q}, +, \cdot, 0, 1)$ con las operaciones: $(p/q) + (r/s) = (ps + qr)/(qs)$ y $(p/q) \cdot (r/s) = (pr)/(qs)$ para $p, r \in \mathbb{Z}$ y $q, s \in \mathbb{Z} - \{0\}$, es un anillo finito conmutativo con unidad, dónde su elemento identidad es $1_{\mathbb{Q}} = 1 \in \mathbb{Z}$.

Definición 1.5.4. Sean R un anillo, $a \in R$ y $S, I \subseteq R$ no vacíos. Diremos que:

(a) S es un **subanillo** de R si y sólo si $(S, +|_{S\times S}, \cdot|_{S\times S}, 0, 1_R)$ es un anillo conmutativo con unidad.

(b) I es un ideal de R si y sólo si $(I, +) \leqslant (R, +)$ y para todo $r \in R$ y $a \in I$ se tiene que $ar \in I$, y denotaremos esto por $I \leqslant R$.

Puede resultar extraño que denotemos $I \leqslant R$ para un ideal y no para un subanillo (como en el caso de los subgrupos), esto se debe a que existen propiedades similares a las del los subgrupos que los ideales satisfacen mientras que los subanillos no.

Un ideal no es necesariamente un subanillo de R, por ejemplo en $\mathbb{Z}$, no es difícil ver que el conjunto $2\mathbb{Z}$ es un ideal, pero no es un subanillo, puesto que $1 \notin 2\mathbb{Z}$. Por otro lado, no siempre un subanillo es un ideal, en el Ejemplo 1.5.3, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ pero no un ideal, pues tomando $1 \in \mathbb{Z}$ y $1/2 \in \mathbb{Q}$ es claro que $(1/2)(1) = (1/2) \notin \mathbb{Z}$.

Teorema 1.5.5. *Sea R un anillo y $a \in R$, el conjuntos $aR := \{ar | r \in R\}$ es un ideal de R y se denota por $\langle a \rangle$.*

Definición 1.5.6. El ideal $aR = \langle a \rangle$ recibe el nombre de **ideal principal** generado por el elemento a.

Observación 1.5.7. 1. En el anillo $\mathbb{Z}$, el conjunto de los numeros pares es un ideal principal generado por 2, es decir, $\langle 2 \rangle = 2\mathbb{Z}$, más aún, para todo $m \in \mathbb{Z}$, el conjunto $m\mathbb{Z}$ es un ideal principal.

Definición 1.5.8. Sea R un anillo conmutativo con unidad 1:

1. R es un **anillo con divisores de cero** si existen elementos r, s tales que $r \neq 0, s \neq 0$ pero $rs = 0$, a todos los elementos que satisfacen lo anterior se les llama **divisores de cero** y al conjunto formado por los divisores de cero de un anillo lo denotaremos por $\mathcal{D}$. En el caso que $\mathcal{D} = \emptyset$, R se llamará un **dominio entero**, además, si R es un dominio entero y todo ideal de R es generado por algún elemento en R, diremos que éste, es un **dominio de ideales principales**.

2. Un elemento $u \in R$ es una **unidad** de R si existe $v \in R$ tal que $uv = 1$, el conjunto de las unidades de un anillo lo denotaremos por R^*.

3. R satisface la **condición de cadena ascendente** (CCA) en sus ideales si, para un toda colección de ideales $I_1, I_2 \ldots,$, tales que, $I_1 \subseteq I_2 \subseteq \cdots$, existe $m \in \mathbb{N}$ tal que, para todo $k \geqslant m$, $I_k = I_m$.

Corolario 1.5.9. *Sean R un anillo, I un ideal de R, $u \in R^*$. Entonces, $\langle u \rangle = R$ en particular podemos denotar $\langle 1 \rangle = R$, más aún si $u \in I$ entonces $I = R$.*

Ejemplo 1.5.10. Sean $n, m, k \in \mathbb{Z}$, diremos que n es **congruente con** m **módulo** k si $k \mid (n - m)$. En particular, la congruencia módulo un entero es una relación de equivalencia y por tanto induce una partición en $\mathbb{Z}$, así, podemos definir el cociente $\mathbb{Z}/\ (\text{mód } n)$ al cual suele denotarse mediante $\mathbb{Z}/n\mathbb{Z}$ o bien, $\mathbb{Z}_n$ y se le llama conjunto de enteros módulo n. Formalmente, los elementos de $\mathbb{Z}_n$ son clases de equivalencia de la forma $[a] = \{b \in \mathbb{Z} | b \equiv a\ (\text{mód } n)\}$, sin embargo hemos suprimido intencionalmente la notación de clase para facilitar la lectura, se entiende que tanto la suma $\oplus_n$ y el producto $\odot_n$ son operaciones entre clases.

1. Dado $n \in \mathbb{N}$, el conjunto $\mathbb{Z}_n = \{0, 1, \dots n-1\}$ de los enteros módulo n, forman un anillo con divisores de cero con la suma y producto módulo n $(\oplus_n, \odot_n)$ cada vez que n no es un número primo. En efecto, como n no es un número primo, entonces existe $m \in \mathbb{N}$ con $m < n$, $m \neq 1$ y $m \neq n$ tal que $m \mid n$ entonces $n = ml$ para algún $n \in \mathbb{N}$, esto implica que $m, l \in \mathbb{Z}_n$ y $ml \equiv (0 \mod n)$ lo cual nos dice que $m \neq 0, l \neq 0$ y $m \odot_n l = 0$, teniendo que $\mathbb{Z}_n$ es un anillo con divisores del cero.

2. Si $n = p$ con p un número primo, entonces $\mathbb{Z}_p$ es un dominio entero. Supóngase que existen $m, l \in \mathbb{Z}_p$ tales que $m \odot_p l = 0$ esto implica que $p \mid ml$ entonces $p \mid m$ o $p \mid l$ en $\mathbb{Z}$, pues p es un número primo, entonces $m \equiv (0 \mod p)$ o bien $l \equiv (0 \mod p)$ entonces en $\mathbb{Z}_p$ tenemos que $m \odot_p l = 0$ implica que $m = 0$ o $l = 0$ por la Definición 1.5.4, $\mathbb{Z}_p$ es un dominio entero.

Ya se mencionó en la Definición 1.5.8 la existencia de elementos particulares en los anillos y cómo éstos otorgan distintas propiedades al mismo, en virtud de esto incluimos en la siguiente definición algunos elementos más y un concepto que hará simil con la divisibilidad en los enteros.

Definición 1.5.11. Sean R un anillo conmutativo con uno, $p, q, r, s \in R$ diremos que:

a) p **divide** a r en R si y sólo si existe $s \in R$ tal que $r = ps$, si esto pasa lo denotaremos por $p \mid r$.

b) p es un **elemento primo** de R si y sólo si cada vez que $p \mid rs$ en R entonces $p \mid r$ o bien $p \mid s$.

c) p, q son **asociados** en R si existe $u \in R^*$ tal que $p = uq$.

d) $p \in R$ se dice **irreducible** si y sólo si cada vez que $r \mid p$ entonces $r \in R^*$ o r es asociado con p.

Teorema 1.5.12. *Sea* D *un dominio de ideales principales, entonces* D *satisface CCA y todo elemento que no es cero y no es una unidad, puede ser escrito como producto de una cantidad finita de elementos irreducibles.*

Los ideales pueden ser clasificados según algunas propiedades muy especificas que se enuncian a continuación:

Definición 1.5.13. Sean R un anillo conmutativo con uno $r, s \in R$ $P, M, Q \leqslant R$. Diremos que:

a) P es un **ideal primo** de R si y sólo si, $P \neq R$ y cada vez que $rs \in P$ entonces $r \in P$ o $s \in P$.

b) Q es un **ideal primario** de R si y sólo si $Q \neq R$ y cada vez que $rs \in Q$ entonces $r \in Q$ o existe algún $m \in \mathbb{N}$ tal que $s^m \in Q$.

c) M es un **ideal maximal** de R si y sólo si $M \neq R$ y para todo $I \leqslant R$ tal que $M \subseteq I \subseteq R$ entonces $I = M$ o $I = R$.

d) El conjunto $\sqrt{I} := \{r \in R | r^n \in R, \text{ para algún } n \in \mathbb{N}\}$, el cual llamamos **el radical del ideal** I.

Lema 1.5.14. *Sea* D *un dominio de ideales principales y sean* M, P *ideales de* R *entonces:*

(i) P *es un ideal primo si y sólo si* $P = \langle p \rangle$ *para algún elemento* p *primo en* D.

(ii) M *es un ideal maximal si y sólo si* $M = \langle p \rangle$ *par algún elemento irreducible* p *en* D.

Lema 1.5.15. *Sean* R *un anillo conmutativo con elemento unidad* 1 *e* $I, J \leqslant R$*, entonces:*

(i) *Si* $|R| \geqslant 2$*, entonces* $\mathcal{D} \cap R^* = \emptyset$ *y* $R = \mathcal{D} \cup R^* \cup \{0\}$ *y* $(R^*, \cdot)$ *es un grupo abeliano.*

(ii) *Los conjuntos* $I + J = \{i + j | i \in I, j \in J\}$, $I \cap J$ *son también ideales de* R.

(iii) $\sqrt{I}$ *es un ideal.*

Demostración. Veamos solamente la primera y la última de las afirmaciones. (i) Como R es un anillo finito, supongamos que $R = \{0, 1, r_1, r_2, \ldots, r_{n-2}\}$. Si $u \in \mathcal{D} \cap R^*$ entonces existen $v_1, v_2 \in \mathcal{R} - \{0\}$ tales que $v_1 u = 1$ y $v_2 u = 0$ entonces tenemos que $v_1(v_2 u) = 0$, pero también $v_1(v_2 u) = (v_1 v_2)u = (v_2 v_1)u = v_2(v_1 u) = v_2(1) = v_2$ entonces $v_2 = 0$ lo cual es una contradicción, por lo tanto, $\mathcal{D} \cap R^* = \emptyset$. Sea $a \in R - (\mathcal{D} \cup \{0\})$ y considere el ideal $aR = \{0, a, ar_1, \ldots, ar_{n-2}\}$, si tomamos ar_i, ar_j tales que $ar_i = ar_j$ entonces $ar_i - ar_j = 0$ y también $ar_i - ar_j = a(r_i - r_j)$ entonces $r_i - r_j = 0$ puesto que a no es un divisor de cero, por lo tanto, $r_i = r_j$ entonces todos los elementos $0, a, ar_1, \ldots, ar_{n-2}$ son distintos dos a dos así, $|R| = |aR|$ y $aR \subseteq R$, por lo tanto, $aR = R$ y así, existe algún $r_j \in R$ tal que $ar_j = 1$ entonces $a \in R^*$. Sean $u_1, u_2 \in R^*$, entonces existen u_1', u_2' tales que $u_1 u_1' = 1$ y $u_2 u_2' = 1$ entonces para el elemento $u_1 u_2$ basta tomar $v = u_2' u_1'$ entonces $(u_1 u_2)v = (u_1 u_2)(u_2' u_1') = u_1(u_2 u_2')u_1' = u_1 u_1' = 1$, por lo tanto, u_1, u_2 es una unidad de R, así $u_1 u_2 \in R^*$ y $\cdot$ tiene cerradura, la asociatividad y conmutatividad las *heredan de* R es claro que 1 es una unidad de R pues $1 \cdot 1 = 1$ y finalmente, dado $u \in R^*$ afirmamos que $u^{-1} = v$ dónde v es el elemento de R tal que $uv = 1$ por definición de unidad, por lo tanto, $v = u^{-1}$ es también una unidad de R, así R^* tiene inversos y, por lo tanto, $(R^*, \cdot)$ es un grupo.

(iii) Sean $a, b \in \sqrt{I}$, entonces existen $n_a, n_b \in \mathbb{N}$ tales que $a^{n_a}, b^{n_b} \in I$. Por el Teorema del Binomio, $(a - b)^{n_a + n_b} = \sum_{i=0}^{n_a + n_b} \binom{n_a + n_b}{i} (-1)^i a^i b^{n_a + n_b - i}$. Puesto que I es un ideal entonces $(I, +) \leqslant (R, +)$ y para todo $r \in R$ y $t \in I$ entonces $rt \in I$, usando esto, se puede verificar fácilmente que término a término $(a - b)^{n_a + n_b} \in I$, por consiguiente, $a - b \in \sqrt{I}$, es decir, $(\sqrt{I}, +) \leqslant (R, +)$. Por otro lado, sean $r \in R$ y $t \in \sqrt{I}$, entonces existe $n \in \mathbb{N}$ tal que $t^n \in I$, como $I \leqslant R$ entonces $rt^n \in I$, de ahí que, $r^2 t^n \in I$, procediendo de esta manera, multiplicando sucesivamente por R tenemos que $(rt)^n = r^n t^n \in I$, así, $rt \in \sqrt{I}$, por lo tanto, $\sqrt{I} \leqslant R$. □

Teorema 1.5.16. *Todo ideal maximal es un ideal primo.*

Corolario 1.5.17. *Sea* D *un dominio de ideales principales y* $p \in D$ *un elemento irreducible, entonces* p *es un elemento primo.*

Lema 1.5.18. *Sea* R *un anillo conmutativo con unidad y* Q *un ideal* R*, si* $\sqrt{Q}$ *es un ideal primo entonces* $Q \neq R$*, además si* Q *es un ideal primario, entonces* $\sqrt{Q}$ *es un ideal primo.*

Demostración. Supóngase que $\sqrt{Q}$ es un ideal primo, entonces por la Definición 1.5.13 $\sqrt{Q} \neq R$, si $Q = R$ es claro que $1 \in Q$, entonces para $n = 1$ tenemos que $1^n = 1 \in Q$ se sigue que $1 \in \sqrt{Q}$ y, por lo tanto, $\sqrt{Q} = R$ una contradicción, así $Q \neq R$. Por otro lado, si Q es un ideal primario, entonces dados $r, s \in R$ tales que $rs \in \sqrt{Q}$, tenemos que existe $n \in \mathbb{N}$ tal que $(rs)^n \in Q$; como R es conmutativo, tenemos que $(rs)^n = r^n s^n$ luego tenemos que $r^n s^n \in Q$ y como éste es primario entonces $r^s \in Q$ o $(s^n)^m \in Q$ para algún $m \in \mathbb{N}$. Si $r^n \in \mathbb{Q}$ entonces $r \in \sqrt{Q}$, o bien, si $(s^n)^m = s^{nm} \in Q$ entonces también $s \in \sqrt{Q}$, es decir, $rs \in \sqrt{Q}$ implica $r \in \sqrt{Q}$ o $s \in \sqrt{Q}$, por lo tanto, $\sqrt{Q}$ es un ideal primo. □

Definición 1.5.19. Sea D un dominio entero, diremos que D es un **dominio de factorizaciíon única** si y sólo si para todo $r \in D$ con $r \neq 0$ y $r \notin D^*$ existe un número finito de elementos irreducibles $p_1, p_2, \ldots, p_t \in D$, tales que, $r = p_1 p_2 \cdots p_t$ y esta descomposición es un única salvo asociados.

Teorema 1.5.20. *Todo dominio de ideales principales es un dominio de factorización única.*

En esta sección hemos definido algunas propiedades fundamentales de los anillos y nos hemos enfocado a estudiar los dominios enteros, en lo sucesivo nuestro interés estará en los anillos con unidad, dominios enteros y los campos los cuales definimos al comienzo de la siguiente sección.

CAMPOS Y ANILLOS DE POLINOMIOS

En la sección anterior, hemos definido a un anillo conmutativo con unidad como un conjunto distinto del vacío sobre el que definimos dos operaciones binarias, con un elemento neutro para ambas y además, con una de éstas, es un grupo abeliano, mientras que la otra sólo cumple algunas propiedades de la definición de grupo. En esta sección analizaremos una nueva estructura algebraica y su relación con los polinomios.

Definición 1.6.1. Sea F un conjunto no vacío sobre el cual se han definido dos operaciones binarias suma $(+)$ y producto $(\cdot)$, diremos que la terna $(F, +, \cdot)$ es un **campo** si y sólo si:

a) $(F, +)$ es un grupo abeliano con elemento identidad denotado por 0.

b) $(F - \{0\}, \cdot)$ es un grupo abeliano con elemento identidad denotado por 1.

c) Para todo $a, b, c \in F$ se cumple que $a \cdot (b + c) = a \cdot b + a \cdot c$.

Observación 1.6.2.

1. Se usará la notación multiplicativa para el producto en el campo F.
2. Los conceptos de **característica de un campo**, **ideales (ideales principales, maximales, primarios, primos, étc)** del campo F, son análogos a los definidos en la Observación 1.5.2(3), Definición 1.5.4(b) y Definición 1.5.13.

Ejemplo 1.6.3. A continuación se muestran algunos ejemplos de campos.

1. Los numeros reales ($\mathbb{R}$) con las suma y producto usuales entre ellos es un campo.
2. El conjunto de los numeros racionales $\mathbb{Q}$ forman un campo con la suma y el producto definidos como en el Ejemplo 1.5.3 (.2).

Lema 1.6.4. *Todo campo es un dominio entero y todo dominio entero finito es un campo.*

Lema 1.6.5. *Sea* R *un anillo conmutativo con unidad donde sus únicos ideales son* $\langle 0\rangle$ *y* R *entonces* R *es un campo, arecíprocamente los únicos ideales de un campo* F *son* $\langle 0\rangle$ *y* F.

Aunque hemos introducido el concepto de campo, desviaremos nuestra atención de ellos para dar paso al estudio de los anillos de polinomios y anillos euclidianos.

Definición 1.6.6. Sean R un anillo conmutativo con unidad, x una indeterminada y $n \in \mathbb{N}\cup\{0\}$, un **polinomio en la indeterminada** x **con coeficientes en** R es la expresión en símbolos de la forma:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 \tag{1.6.1}$$

donde los a_i, para $i \in \{0, 1, \ldots, n\}$, se llaman **coeficientes** del polinomio, si $a_n \neq 0$, diremos que $f(x)$ es un polinomio de **grado** n, lo cual se denotará por $grad(f(x)) = n$ y a_n se llamará el **coeficiente principal** de $f(x)$, cuando $a_n = 1$, se dice que $f(x)$ es un **polinomio mónico**, aquel polinomio cuyos coeficientes son todos idénticos a 0, se denomina **polinomio nulo** el cual suele denotarse mediante 0 y, si $n = 0$ pero $a_n \neq 0$, decimos que $f(x)$ es un **polinomio constante**[4].

Definición 1.6.7. Sean R un anillo conmutativo con unidad, $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$, dos polinomios en la indeterminada x con coeficientes en R para algunos $n, m \in \mathbb{N}\cup\{0\}$. Entonces:

1. Diremos que dos polinomios son iguales, $f(x) = g(x)$ si y sólo si $n = m$ y $a_i = b_i$ para toda $i \in \{0, 1, \ldots, n\}$.
2. Definimos la suma de polinomios, $f(x) + g(x) = \sum_{i=0}^{l}(a_i + b_i)x^i$ donde $l = \text{máx}\{n, m\}$ y además; $a_i = 0$ y $b_i = 0$ cada vez que $i > n$ o $i > m$ para $i \in \{0, 1, \ldots, l\}$, respectivamente.
3. Definimos el producto de polinomios, $f(x)g(x) = \sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}(a_j b_{i-j})\right)x^i$ donde $a_i = 0$ y $b_{i-j} = 0$ cada vez que $i > n$ o $i - j > m$ para $i \in \{0, 1, \ldots, n + m\}$, respectivamente.

Definición 1.6.8. Sean R un anillo conmutativo con unidad, x una indeterminada y $n \in \mathbb{N}\cup\{0\}$. Definimos el **anillo de polinomios en la indeterminada** x **con coeficientes en** R como el conjunto:

$$R[x] := \left\{ a_n x^n + \cdots + a_2x^2 + a_1x + a_0 \,|\, a_i \in R,\ \forall i \in \{0, 1, \ldots, n\}, n \in \mathbb{N}\cup\{0\}\right\} \tag{1.6.2}$$

acompañado de las operaciones suma de polinomios y producto de polinomios definidas anteriormente.

4 Es decir, los polinomios constantes son polinomios de grado cero y, en particular, son los elementos del anillo R

Observación 1.6.9. No es difícil demostrar que la quíntupla $(R[x], +, \cdot, 0, 1_{R[x]})$ es un anillo conmutativo con unidad, donde $1_{R[x]} = 1_R$ el polinomio constante 1_R. El polinomio nulo es el elemento neutro en el grupo abeliano aditivo $(R[x], +)$ y su grado no está definido, sin embargo, es considerado un polinomio consante. Dado un polinomio $f(x) \in R[x]$ de la forma (1.6.1) tiene por inverso aditivo al polinomio $g(x) = -a_n x^n - a_{n-1}x^{n-1} - \cdots - a_2x^2 - a_1x - a_0 \in R[x]$.

Lema 1.6.10. *Sea* R *un anillo conmutativo con unidad* 1. R *es un dominio entero si y sólo si* $R[x]$ *es un dominio entero, más aún* $\operatorname{grad}(f(x)g(x)) = \operatorname{grad}(f(x)) + \operatorname{grad}(g(x))$, *para cualquier par de polinomios* $f(x), g(x) \in R[x] - \{0\}$.

Definición 1.6.11. Sea F un campo, el conjunto $F[x]$ con las operaciones suma y producto de polinomios, es llamado: **anillo de polinomios en la indeterminada** x **con coeficientes en el campo** F.

Cabe mencionar, que la definición anterior es similar a la Definición 1.6.8, dado que F puede ser considerado un anillo conmutativo con unidad, más aún, es un anillo donde todo elemento tiene un inverso, a los campos también suele llamarséles **anillos con división**.

Definición 1.6.12. Sea D un dominio entero. Diremos que es un *anillo euclidiano* si existe una función: $\delta : D - \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ tal que:

a) Para todo $x, y \in D - \{0\} : \delta(x) \leqslant \delta(xy)$

b) (*Algoritmo de la división*) Para todo $x, y \in D - \{0\}$, existen $r, q \in D - \{0\}$ tales que, $x = qy + r$ donde $r = 0$ o $\delta(r) < \delta(y)$

Teorema 1.6.13. *Todo anillo euclidiano es un dominio de ideales principales.*

Lema 1.6.14. *Sea* F *un campo. El anillo de polinomios* $F[x]$ *es un anillo euclidiano.*

Corolario 1.6.15. *Sean* F *un campo y* $f(x)$ *un polinomio en* $F[x]$.
El conjunto $\langle f(x)\rangle := \{f(x)g(x) \mid g(x) \in F[x]\}$ *es un ideal principal en* $F[x]$, *y:*

(i) $\langle f(x)\rangle$ *es un ideal primo de* $F[x]$ *si y sólo si* $f(x) = 0$ *o* $f(x)$ *es un elemento primo de* $F[x]$.

(ii) $\langle f(x)\rangle$ *es un ideal maximal de* $F[x]$ *si y sólo si* $f(x) = 0$ *o* $f(x)$ *es un elemento irreducible en* $F[x]$.

(iii) *Todo ideal primo* P *de* $F[x]$ *con* $P \neq \langle 0\rangle$ *es un ideal maximal.*

Demostración. Por el Teorema 1.5.5, $\langle f(x)\rangle$ es un ideal prinicipal de $F[x]$. Los inicisos (i) y (ii) se siguen del Lema 1.5.14, por esta razón, demostraremos solamente (iii). Sea I un ideal en $F[x]$ tal que $P \subsetneq I$ y suponga que P es un ideal primo distinto de $\langle 0\rangle$, por el Teorema 1.6.13, $F[x]$ es un dominio de ideales principales, entonces existe $p(x) \in F[x]$ con $P = \langle p(x)\rangle$ y como P es un ideal primo, $p(x)$ es un elemento primo de $F[x]$. Demostraremos que $p(x)$ es irreducible, para esto, sean $g(x), h(x) \in F[x]$ tales que $p(x) = g(x)h(x)$, como $P \neq \langle 0\rangle$ y $P \neq F[x]$ (por ser un ideal primo), $p(x) \neq 0$ y $p(x)$ no es una unidad de $F[x]$. Como, $g(x)h(x) = p(x) \in P$ y P es un ideal primo, $g(x) \in P$ o bien $h(x) \in P$. Supongamos sin pérdida de generalidad que $g(x) \in P$,

entonces existe $q(x) \in F[x]$, tal que $g(x) = p(x)q(x)$, así, $p(x) = p(x)q(x)h(x)$; usando la propiedad cancelativa (pues $F[x]$ es un dominio entero), $q(x)h(x) = 1$, es decir, $h(x)$ es una unidad en $F[x]$. Sea pues $h(x) = u \in F[x]^* = F$, tenemos que $p(x) = ug(x)$, así, $p(x)$ es irreducible y por (ii) de este teorema se concluye que P es maximal. □

Lema 1.6.16. *Sean* R *un anillo euclidiano y* $a \in R - \{0\}$.

1. $\delta(1) = \min\{\delta(x) \mid x \in R - \{0\}\}$.
2. *Si* $\delta(a) = \delta(1)$ *entonces* a *es un unidad.*

Para finalizar esta sección introducimos un concepto que puede parecerle familiar al lector y que será una clave para el estudio de los polinomios sobre campos finitos:

Definición 1.6.17. Sean R un anillo euclidiano, $r, s \in R$. Un elemento $d \in R - \{0\}$, es el **máximo común divisor** de r y s si y sólo si: $d \mid r$, $d \mid s$ y para todo $c \in R - \{0\}$, si $c \mid r$ y $c \mid s$ entonces $c \mid d$.

Lema 1.6.18. *Sean* $r, s \in R$ *un anillo euclidiano, entonces existen* $d \in R - \{0\}$, $\lambda, \mu \in R$ *tales que* $d = \lambda r + \mu s$, $d = (r, s)$ *y* d *es único salvo asociados.*

Demostración. Considérense los ideales principales $I = \langle r \rangle$ y $J = \langle s \rangle$. Por el Lema 1.5.15, $I + J$ es un ideal de R, además por el Teorema 1.6.13, R es dominio de ideales principales luego, existe $d \in R$ tal que $\langle d \rangle = I + J$. Si al menos r o s no son cero, entonces $\langle d \rangle = I + J \neq \langle 0 \rangle$, y así, $d \neq 0$. Como $r, s \in I + J = \langle d \rangle$ entonces $r = dt_1$ y $s = dt_2$ para algunos $t_1, t_2 \in R$, es decir, $d \mid r$ y $d \mid s$. Sea $c \in R - \{0\}$ tal que $c \mid r$ y $c \mid s$ entonces $r = cq_1$ y $s = cq_2$ para algunos $q_1, q_2 \in R$. Note que $d \in I + J$ entonces existen $\lambda, \mu \in R$ tales que $d = \lambda r + \mu s$ como afirmamos, más aún por lo dicho antes tenemos que $d = \lambda r + \mu s = \lambda c q_1 + \lambda c q_2 = c(\lambda q_1 + \mu q_2)$ y entonces $c \mid d$, por lo tanto, $d = (r, s)$. Finalmente, si e es un elemento que satisface 1. y 2. de la Definición 1.6.17, se sigue que $e \mid d$ y $d \mid e$, entonces, $d = ue$ y $e = \nu d$ para algunos $u, \nu \in R - \{0\}$, sustituyendo tenemos que $d = u(\nu d) = (u\nu)d$ y usando cancelación, tenemos que $u\nu = 1$. Por lo tanto, u y ν son unidades, así, d y e son asociados. □

Definición 1.6.19. Sean $r, s \in R$ un anillo euclidiano, diremos que estos elementos son **coprimos** si y sólo si $(r, s) = 1$ o, de manera equivalente si existen $\lambda, \mu \in R$ tales que $\lambda r + \mu s = 1$.

HOMOMORFISMOS DE ANILLOS

En la sección 1.2, estudiamos a los homomorfismos de grupos, su relación con los subgrupos normales y los grupos cociente. Ha llegado el momento de analizar resultados de suma importancia en la teoría de anillos, los **teoremas de isomorfismos**. Éstos serán tratados en la sección presente.

Definición 1.7.1. Sea R un anillo, r, s elementos de R e $I \subseteq R$ un ideal. Diremos que s **es congruente con** r **módulo** I en R si y sólo si $s - r \in I$ y esto lo denotaremos con la expresión:

$$s \equiv r \mod I$$

Es necesario mencionar que se ha definido la congruencia módulo un ideal de un anillo R de manera similar a la congruencia módulo un subgrupo y como es de esperarse, hay propiedades que son *heredadas*, al considerar a $(R, +)$ como un grupo, por ejemplo, que ésta es una relación de equivalencia sobre R e induce una partición allí, que denotaremos mediante R/I, y ésta consta de clases de equivalencia $\overline{r}$, caracterizadas en el siguiente:

Corolario 1.7.2. *Sean R un anillo conmutativo con unidad e $I \leqslant R$. Entonces $R/I = \{r + I \mid r \in R\}$, es decir, $\overline{r} = r + I$; más aún, $r + I = s + I$ si y sólo si $r - s \in I$.*

Definición 1.7.3. Sea R un anillo, $I \leqslant R$, $R/I = \{r + I \mid r \in R\}$, definimos las funciones:

$$\begin{array}{rccc} \oplus: & (R/I) \times (R/I) & \longrightarrow & (R/I) \\ & (r+I, s+I) & \longmapsto & ((r+s)+I) \end{array} \qquad \begin{array}{rccc} \odot: & (R/I) \times (R/I) & \longrightarrow & (R/I) \\ & (r+I, s+I) & \longmapsto & ((rs)+I) \end{array}$$

las cuales llamamos, **suma** y **producto de clases módulo** I respectivamente.

Teorema 1.7.4. *El conjunto R/I con la suma y producto de clases módulo I forman un anillo conmutativo con unidad, el cual es llamado **anillo cociente** o **anillo de clases residuales módulo** I.*

Observación 1.7.5. Considere a R un anillo conmutativo con unidad 1, e $I \leqslant R$.

1. Como en el caso de los grupos cociente, el elemento $I = 0 + I \in R/I$ es el elemento neutro para la suma de clases y $1 + I$ es el elemento unidad de R/I.

   En efecto, $(r + I) \odot (1 + I) = (r1) + I = r + I$ pues 1 es la identidad de R, así, $1 + I$ es el elemento identidad en R/I.

2. En lo sucesivo, denotaremos las operaciones $\oplus$, $\odot$ definidas en R/I por $+$ y $\cdot$ (la suma y producto usuales en R) siempre que el contexto sea claro.

Definición 1.7.6. Sean las quíntuplas $(R, +, \cdot, 0, 1_R)$ y $(R', +', \cdot', 0', 1_{R'})$ anillos. Una función $\phi : R \longrightarrow R'$ es llamada un homomorfismo de anillos si preserva las operaciones entre los anillos, esto es, $\phi(r + s) = \phi(r) +' \phi(s)$ y $\phi(rs) = \phi(r) \cdot' \phi(s)$, para todo $r, s \in R$.

Corolario 1.7.7. *Sean R, R' anillos con elemento identidad 1 y $1'$ respectivamente, ϕ un homomorfismo de anillos entre R y R'. Entonces $\phi(0) = 0'$, $\phi(-r) = -\phi(r)$ y si ϕ es sobreyectiva entonces $\phi(1) = 1'$.*

Definición 1.7.8. Sean R, R' anillos, $\phi : R \longrightarrow R'$ un homomorfismo de anillos, definimos los conjuntos:

$$\begin{aligned} \mathrm{Im}\phi &= \{\phi(r) \mid r \in R\} \\ \ker\phi &= \{r \in R \mid \phi(r) = 0'\} \end{aligned}$$

la **imagen** y el **kernel** de ϕ respectivamente.

Nota. Como en el caso de grupos, los conceptos de monomorfismo, epimorfismo e isomorfismo, son definidos de manera formal en el apéndice A.3, sin embargo, en la teoría de anillos, a pesar de que existe la equivalencia entre los monomorfismos, isomorfismos y los homomorfismos inyectivos y biyectivos respectivamente, en el caso de los epimorfismos y los homomorfismos suprayectivos, dicha equivalencia no existe, por ejemplo, es fácil ver que la inclusión $\iota : \mathbb{Z} \to \mathbb{Q}$ es un epimorfismo y claramente no es una función sobreyectiva entre los anillos $\mathbb{Z}$ y $\mathbb{Q}$. Sin embargo como se demuestra en el Lema A.3.7, un homomorfismo suprayectivo es siempre un epimorfismo, así, en lo sucesivo, diremos epimorfismo para referirnos a un homomorfismo suprayectivo, entendiendo que en general el ser un epimorfismo no implica la suprayectividad.

Además, por lo dicho antes, diremos que ϕ es un monomorfismo de anillos si y sólo si $\ker\phi = \{0\}$ y cada vez que $\mathrm{Im}\phi = G'$, diremos que ϕ es un epimorfismo.

Teorema 1.7.9 (Fundamental de los homomorfismos de anillos)**.** *Sean* R *y* R' *anillos.*

i) Si $I \leqslant R$*, entonces la función:*

$$\begin{array}{rccc} \nu : & R & \longrightarrow & R/I \\ & r & \longmapsto & r + I \end{array}$$

es un epimorfismo de anillos llamado ***epimorfismo natural*** *y es tal que* $\ker\nu = I$.

ii) Si R *y* R' *son anillos con unidad y sean* $1, 1'$ *los elementos identidad en* R *y* R' *respectivamente* $\phi : R \longrightarrow R'$ *un homomorfismo de anillos tal que* $\phi(1) = 1'$*, entonces* $\mathrm{Im}\phi$ *es un subanillo de* R'*,* $\ker\phi \leqslant R$ *y la función:*

$$\begin{array}{rccc} \overline{\phi} : & R/\ker\phi & \longrightarrow & \mathrm{Im}\phi \\ & r + \ker\phi & \longmapsto & \phi(r) \end{array}$$

es un isomorfismo de anillos.

Teorema 1.7.10. *Sea* $\phi : R \longrightarrow R'$ *un homomorfismo suprayectivo de anillos, entonces:*

(i) *Si* I *es un ideal (o subanillo) de* R*, entonces* $\phi(I)$ *es un ideal (o un subanillo) de* R'.

(ii) *Si* I' *es un ideal (o un subanillo) de* R'*, entonces* $\phi^{-1}(I')$ *es un ideal (o un subanillo) de* R*,* $\ker\phi \subseteq \phi^{-1}(I')$ *y* $\phi^{-1}(I')/\ker\phi \simeq I'$.

iii) Si $I \leqslant R$ *entonces nombrando* $\phi(I) = I'$*, la función:*

$$\begin{array}{rccc} \phi' : & R/I & \longrightarrow & R'/I' \\ & r + I & \longmapsto & \phi(r) + I' \end{array}$$

es un homomorfismo de anillos, más aún, si $\ker\phi \subseteq I$ *entonces* $\phi^{-1}(\phi(I)) = I$ *y* ϕ' *es un isomorfismo.*

Demostración. (i) Supongamos que $I \leqslant R$, dados $\rho, \sigma \in \phi(I)$ existen $r, s \in I$, tales que, $\phi(r) = \rho$ y $\phi(s) = \sigma$, es claro que, $\rho - \sigma = \phi(r) - \phi(s) = \phi(r - s)$ entonces $\rho - \sigma \in \phi(I)$, por lo tanto, $(\phi(I), +') \leqslant (R', +')$. Sea $\tau \in R'$, como ϕ es suprayectiva, existe $t \in R$, tal que, $\phi(t) = \tau$ entonces $\tau \cdot' \rho = \phi(t) \cdot' \phi(r) = \phi(tr)$. Luego, como I es un ideal de R,

es claro que, $tr \in I$, así, $\tau \cdot' \rho \in \phi(I)$, por lo tanto, $\phi(I) \leqslant R'$. Por otro lado, si I es un subanillo, considérese $\phi|_I \colon I \longrightarrow R'$, como ϕ es un homomorfismo, $\phi|_I$ lo es también y ya que es suprayectivo, es un epimorfismo. Por el Corolario 1.7.7, $\phi(1) = 1'$ y por el teorema anterior, tenemos que $\operatorname{Im}(\phi|_I) = \phi(I)$ es un subanillo de R'.

(ii) Supóngase que I' es un ideal de R' y sean $r, s \in \phi^{-1}(I')$, entonces $\phi(r), \phi(s) \in I'$, luego $\phi(r) - \phi(s) \in I'$, pues $(I', +') \leqslant (R', +')$; de esto se sigue que $\phi(r-s) \in I'$, por consiguiente, $r - s \in \phi^{-1}(I')$, así, $(\phi^{-1}(I'), +) \leqslant (R, +)$. Ahora, dados $t \in R$ y $r \in \phi^{-1}(I')$ tenemos que $\phi(r) \in I'$ luego, $\phi(t) \cdot' \phi(r) \in I'$ pues I' es un ideal y $\phi(t) \in R'$, es decir, $\phi(tr) \in I'$, así, $tr \in \phi^{-1}(I')$, por lo tanto, $\phi^{-1}(I')$ es un ideal de R. Si I' es un subanillo de R', entonces, $(\phi^{-1}(I'), +) \leqslant (R, +)$, además si $r, s \in \phi^{-1}(I')$ entonces $\phi(r), \phi(s) \in I'$, luego $\phi(r) \cdot' \phi(s) \in I'$ pues éste es un subanillo, por consiguiente, $\phi(rs) \in I'$, es decir, $rs \in \phi^{-1}(I')$, entonces $\phi^{-1}(I')$ es un subanillo de R. Además, si $x \in \ker\phi$ se tiene que, $\phi(x) = 0' \in I'$ ya que $0'$ es el neutro aditivo de $+'$ en R', de ahí que, $x \in \phi^{-1}(I')$, en otras palabras, $\ker\phi \subseteq \phi^{-1}(I')$, por lo anterior, si I' es un subanillo de R' entonces $I = \phi^{-1}(I')$ es un subanillo de R. Considérese la función:

$$\begin{array}{rccc} \phi|_I \colon & I & \longrightarrow & R' \\ & r & \longmapsto & \phi(r) \end{array}$$

por (ii) del Teorema 1.7.9, $\ker(\phi|_I)$ es un ideal de I, $\operatorname{Im}(\phi|_I)$ es un subanillo de R' y entonces $I/\ker(\phi|_I) \simeq \operatorname{Im}(\phi|_I)$, además, note que $\operatorname{Im}(\phi|_I) = \phi(I)$ pues ϕ es sobreyectiva, además, $\phi(I) = \phi(\phi^{-1}(I')) = I'$ nuevamente, por la sobreyectividad de ϕ. Finalmente, si $x \in \ker\phi$ y $x \notin \ker(\phi|_I)$ entonces $\phi(x) = 0$, pero $0 \neq \phi|_I(x) = \phi(x) = 0$, lo cual es una contradicción, por lo tanto, $\ker(\phi|_I) = \ker\phi$, por consiguiente, $\phi^{-1}(I')/\ker\phi \simeq I'$.

(iii) Veamos que ϕ' está bien definida. Considérense $r + I, s + I \in R/I$, tales que $r + I = s + I$, entonces $r - s \in I$, luego $\phi(r-s) \in \phi(I) = I'$, así, $\phi(r) - \phi(s) \in I'$, se sigue que $\phi(r) + I' = \phi(s) + I'$ con lo cual concluimos que $\phi'(r+I) = \phi'(s+I)$, entonces ϕ' está bien definida. Es fácil ver que ϕ' es un homomorfismo de anillos. Ahora supóngase que $\ker\phi \subseteq I$, si $x \in I$, $\phi(x) \in \phi(I)$, luego $x \in \phi^{-1}(\phi(I))$, entonces $I \subseteq \phi^{-1}(\phi(I))$. Por otro lado si $x \in \phi^{-1}(\phi(I))$ se tiene que $\phi(x) \in \phi(I)$, así, existe $y \in I$ tal que $\phi(x) = \phi(y)$ después, $\phi(x) - \phi(y) = 0'$, es decir, $\phi(x-y) = 0'$ entonces, $x - y \in \ker\phi \subseteq I$ luego, $x - y, y \in I$. Como $(I, +) \leqslant (R, +)$ se tiene que $x = (x-y) + y \in I$, es decir, $\phi^{-1}(\phi(I)) \subseteq I$, así tenemos que $\phi^{-1}(\phi(I)) = I$. Dado que ϕ es un sobreyectiva, ϕ' también lo es, y en consecuencia un epimorfismo, y dados $r+I, s+I \in R/I$ tales que $\phi'(r+I) = \phi'(s+I)$ entonces $\phi(r) + I' = \phi(s) + I'$, por el Corolario 1.7.2, $\phi(r) - \phi(s) \in I'$, se sigue que, $\phi(r-s) \in I'$, entonces $r - s \in \phi^{-1}(I') = \phi^{-1}(\phi(I)) = I$, por lo tanto, $r - s \in I$, así, $r + I = s + I$, es decir, ϕ' es inyectiva, por consiguientex, $R/I \simeq R'/I'$. □

Teorema 1.7.11. *Sea R un anillo conmutativo con unidad, R_0 un subanillo de R, I un ideal de R y definamos el conjunto $R_0 + I := \{r_0 + x \mid r_0 \in R_0 \text{ y } x \in I\}$. Entonces:*

(i) *$R_0 + I$ es un subanillo de R, $I \leqslant R_0 + I$ y $R_0 \cap I \leqslant R_0$.*

(ii) *La función:*

$$\begin{array}{rccc} \sigma \colon & R_0 + I & \longrightarrow & R_0/(R_0 \cap I) \\ & r_0 + x & \longmapsto & r_0 + (R_0 \cap I) \end{array}$$

es un homomorfismo de anillos, con $\ker\sigma = I$ y en consecuencia $R_0 + I/I \simeq R_0/(R_0 \cap I)$

Demostración. (i) Si $a, b \in R_0 + I$, existen $r_0, s_0 \in R_0$ y $x_1, x_2 \in I$ tales que $a = r_0 + x_1$ y $b = s_0 + x_2$, entonces $a - b = (r_0 + x_1) - (s_0 + x_2) = (r_0 - s_0) + (x_1 - x_2)$, es claro que $r_0 - s_0 \in R_0$ y $(x_1 - x_2) \in I$. Dado que R_0 es un subanillo y que $(I, +) \leqslant (R, +)$, entonces $a - b \in R_0 + I$, por lo tanto, $(R_0 + I, +) \leqslant (R, +)$. Por otro lado, note que $ab = (r_0 + x_1)(s_0 + x_2) = r_0s_0 + x_1s_0 + r_0x_2 + x_1x_2$, nuevamente, $t_0 = r_0s_0 \in R_0$ pues éste es un subanillo, y como I es un ideal de R, tenemos que, $r_0x_2, s_0x_1, x_1x_2 \in I$ entonces $x = r_0x_2 + s_0x_1 + x_1x_2 \in I$ y por consiguiente, $ab = t_0 + x \in R_0 + I$, así, $R_0 + I$ es un subanillo de R. Como $(R_0, +) \leqslant (R, +)$ es inmediato que $0 \in R_0$ y dado cualquier elemento $x \in I$ podemos reescribir $x = 0 + x \in R_0 + I$, por lo tanto, $I \subseteq R_0 + I$, entonces se verfica que $(I, +) \leqslant (R_0 + I, +)$.Puesto que I es un ideal de R, dados $\chi \in I$, $\rho = r_0 + x \in R_0 + I$, tenemos que $\rho\chi = (r_0 + x)\chi = r_0\chi + x\chi \in I$ pues $I \leqslant R$ entonces $\rho\chi \in I$ y concluimos que $I \leqslant R_0 + I$. Tomemos dos elementos $r_0, s_0 \in R_0 \cap I$, luego $r_0s_0 \in R_0$ y $r_0, s_0 \in I$, como $(R_0, +), (I, +) \leqslant (R, +)$, es claro que, $r_0 - s_0 \in R_0$ y $r_0 - s_0 \in I$, en otras palabras, $r_0 - s_0 \in R_0 \cap I$ entonces $(R_0 \cap I, +) \leqslant (R_0, +)$. Considérense $s_0 \in R_0$, $\chi \in R_0 \cap I$, entonces $s_0\chi \in R_0$ por ser un subanillo y $s_0\chi \in I$ por ser éste un ideal de R, así que, $s_0\chi \in R_0 \cap I$, por lo tanto, $R_0 \cap I$ es un ideal de R_0.

(ii) σ es claramente homomorfismo de anillos. Si $r_0 + x \in \ker\sigma$ entonces $\sigma(r_0 + x) = R_0 \cap I$ y dado que $r_0 + (R_0 \cap I) = \sigma(r_0 + x_1) = (R_0 \cap I) = 0 + (R_0 + I)$, entonces $r_0 - 0 \in R_0 \cap I$, es decir, $r_0 \in I$, por consiguiente, $r_0 + x \in I$ entonces, $\ker\sigma \subseteq I$, además, dado $\chi \in I$ podemos escribir $\chi = 0 + \chi \in R_0 + I$, luego $\sigma(0 + \chi) = 0 + (R_0 \cap I) = R_0 \cap I$, así, $\chi \in \ker\sigma$, luego, $I \subseteq \ker\sigma$, en conclusión $\ker\sigma = I$. Finalmente, si renombramos $S = R_0 + I$, $J = (R_0 \cap I)$, $S' = R_0/J$, dado que σ es sobreyectiva y que $\mathrm{Im}\sigma = S'$, tenemos que $\sigma : S \longrightarrow S'$. Ahora bien, como $\ker\sigma = I$, por (ii) del Teorema 1.7.9, $S/\ker\sigma \simeq \mathrm{Im}\sigma = S' = R_0/J$, es decir, $R_0 + I/I = R_0/(R_0 + I)$ □

Para concluir está sección exhibiremos la estrecha relación existente entre los ideales de un anillo, homomorfismos y el anillo cociente o anillo de clases residuales.

Lema 1.7.12. *Sean* R *un anillo conmutativo con unidad y* M, P *ideales de* R*, entonces:*

i) P es un ideal primo si y sólo si R/P *es un dominio entero.*

ii) M *es un ideal maximal si y sólo si* R/M *es un campo.*

CAMPOS FINITOS

En las secciones previas, hemos estudiado estructuras algebraicas que han culminado en el estudio de los anillos de polinomios, dónde los coeficientes son elementos en un anillo o bien en un campo, en esta sección haremos uso de todo lo estudiado antes para analizar las caracterrísticas de un anillo polinomial con coeficientes en un campo finito.

Definición 1.8.1. Sea $\mathbb{F}$ un conjunto finito no vacío, y $+, \cdot$ dos operaciones binarias definidas sobre $\mathbb{F}$, diremos que la terna $(\mathbb{F}, +, \cdot)$ es un campo finito, si ésta es un campo.

Observación 1.8.2.

1. En el segundo inciso del Ejemplo 1.5.10, vimos que si p es un número primo, el anillo $\mathbb{Z}_p$ es un dominio entero y por el Lema 1.6.4 al ser $\mathbb{Z}_p$ un conjunto finito es un campo finito, llamado usualmente **campo de Galois de orden** p y suele denotarse por $\mathbb{F}_p$.

2. $(\mathbb{F}, +)$ es llamado **grupo aditivo** y $(\mathbb{F}^*, \cdot)$ es el **grupo multiplicativo** del campo $\mathbb{F}$.

3. Si $K \subseteq \mathbb{F}$ con $K \neq \emptyset$, sastisface que $(K, +) \leqslant (\mathbb{F}, +)$ y $(K - \{0\}, \cdot) \leqslant (\mathbb{F}^*, \cdot)$ diremos que K es un **subcampo** o de manera equivalente, si existe algún homomorfismo inyectivo entre K y $\mathbb{F}$, decimos que $\mathbb{F}$ es una **extensión** del campo K, esto se suele denotar como $K \leqslant \mathbb{F}$.

4. Si K es un campo que no tiene subcampos distintos de él mismo y del campo $\{0, 1\}$[5] decimos que es un **campo primo**.

5. Si K es un subcampo de $\mathbb{F}$ entonces podemos considerar a $\mathbb{F}$ como un espacio vectorial sobre el campo K, esto lo denotamos mediante ${}_K\mathbb{F}$ y si éste es un espacio vectorial finito dimensional, la dimensión de $\mathbb{F}$ sobre K se llamará **grado de la extensión** de $\mathbb{F}$ sobre K y lo denotamos por $[\mathbb{F} : K]$, es decir:

$$\dim({}_K\mathbb{F}) = [\mathbb{F} : K]$$

Lema 1.8.3. *$\mathbb{F}_p$ es un campo primo y para todo campo $\mathbb{F}$, el conjunto*

$$\mathbb{P} = \bigcap \{K \mid K \leqslant \mathbb{F} \text{ y } K \text{ es no trivial.}\}$$

es el subcampo primo de $\mathbb{F}$.

Demostración. Sea $F \leqslant \mathbb{F}_p$, entonces $\overline{0}, \overline{1} \in F$, luego los elementos $2\overline{1}, 3\overline{1}, \ldots, (p-1)\overline{1} \in F$, esto implica que, $\mathbb{F}_p \subseteq F$, por lo tanto, $\mathbb{F}_p$ es un campo primo. Sea $\mathbb{F}$ un campo y $\mathbb{P}$ como en las hipótesis. Veamos primero que $\mathbb{P}$ es un subcampo de $\mathbb{F}$. Para esto, sean $a, b \in \mathbb{P}$ entonces para todo $K \leqslant \mathbb{F}$, $a, b \in K$, luego, $a - b \in K$ y si $b \neq 0$, $ab^{-1} \in K^*$, por (3.) de la Observación 1.8.2, de esto se sigue que $a - b \in \mathbb{P}$ y si $b \neq 0$ $a - b \in \mathbb{P} - \{0\}$ entonces $(\mathbb{P}, +) \leqslant (\mathbb{F}, +)$ y $(\mathbb{P} - \{0\}, \cdot) \leqslant (\mathbb{F}^*, \cdot)$; por lo tanto $\mathbb{P}$ es un subcampo de $\mathbb{F}$. Por último, sea $K \leqslant \mathbb{P}$, es claro que $K \leqslant \mathbb{F}$, entonces $\mathbb{P} \subseteq K$ pues $\mathbb{P}$ es la intersección de todos los subcampos no triviales de $\mathbb{F}$ y en consecuencia $K = \mathbb{P}$, es decir, $\mathbb{P}$ es un campo primo. □

Sean K un campo, $M \subseteq K$ no vacío y $\mathbb{F} \leqslant K$. Como K es un subcampo de sí mismo, el conjunto $\{F \leqslant K \mid \mathbb{F} \subseteq F \text{ y } M \subset F\}$, es no vacío puesto que K pertenece a éste y por consiguiente, $L = \bigcap\{F \leqslant K \mid \mathbb{F} \subseteq F \text{ y } M \subset F\}$ es un conjunto no vacío, además, procediendo como al inicio de la demostración del Lema 1.8.3, podemos ver que L es un subcampo de K, al ser la intersección de subcampos. Éste campo tiene propiedades muy particulares que se estudiarán a continuación, pero primero presentamos la siguiente:

5 No es difícil demostrar que este conjunto es un campo. Además éste conjunto y K son llamados **subcampos triviales**.

Definición 1.8.4. Sea $\mathbb{F}$ un subcampo de un campo K y M cualquier subconjunto no vacío de K. El conjunto,

$$\mathbb{F}(M) = \bigcap \{F \leqslant K \mid \mathbb{F} \subseteq F \text{ y } M \subseteq F\}$$

es un campo llamado, **campo extensión de $\mathbb{F}$ obtenido por adjuntar a los elementos de** M.

Si M es un conjunto finito, dígamos $M = \theta_1, \theta_2, \ldots, \theta_n$ entonces denotaremos a $\mathbb{F}(M)$ mediante, $\mathbb{F}(\theta_1, \theta_2, \ldots, \theta_n)$. En el caso que $M = \{\theta\}$ éste campo se denota solamente por $\mathbb{F}(\theta)$ y decimos que es una **extensión simple** de$\mathbb{F}$ definida por el elemento θ sobre $\mathbb{F}$ y por su definición, es el subcampo de K más pequeño que contiene a F y a M.

Ejemplo 1.8.5. Sabemos que $\mathbb{R} \leqslant \mathbb{C}$, por lo anterior, podemos ver que $\mathbb{C} = \mathbb{R}[i]$ es decir, el campo de los números complejos es una extensión simple del campo de los numeros reales, que resulta de adjuntar la unidad imaginaria i a $\mathbb{R}$.

A continuación enunciaremos propiedades que involucran a campos finitos y algunos campos no necesariamente finitos, así que, en lo sucesivo, $\mathbb{F}_q$ denotará exclusivamente un campo finito con q elementos.

Teorema 1.8.6. *Sean $\mathbb{F}_q$ un campo finito y p un número primo. Entonces:*

(i) *La característica de $\mathbb{F}_q$ es un número primo.*

(ii) *Si $K \leqslant \mathbb{F}_q$ tal que $\mid K \mid = r$ entonces $q = r^n$ donde $n = [\mathbb{F}_q : K]$.*

(iii) *El subcampo primo de $\mathbb{F}_q$ es isomorfo a $\mathbb{F}_p$ y en consecuencia $q = p^n$, para algún $n \in \mathbb{N}$.*

(iv) *Para todo $\alpha \in \mathbb{F}_q$ se satisface que $\alpha^q = \alpha$.*

Demostración. (i) Como $\mathbb{F}_q$ es un campo entonces existen elementos neutros de la suma y el producto. Sean 0 y 1 respectivamente, nombremos por el momento $1 = e$ y considérense los elementos $e, 2e, 3e, \ldots \in \mathbb{F}_q$, como $\mathbb{F}_q$ es finito entonces, existen $r, s \in \mathbb{Z}$ tales que $re = se$ con $r \neq s$ entonces $(r-s)e = 0$, así, la característica de $\mathbb{F}_q$ existe y es distinta de cero, se sigue que $1 \neq 0$ y $\mathbb{F}_q^* \neq \emptyset$ (pues $1 \in \mathbb{F}_q^*$), luego la característica de $\mathbb{F}_q$ es al menos 2. Sea p la característica de $\mathbb{F}_q$, y supóngase que no es un número primo, entonces existen r y s enteros mayores que 1 tales que $p = rs$ y desde luego $r, s < p$, entonces $0 = p1 = (rs)1 = (r1)(s1)$ lo cual implica que $(r1) = 0$ o bien $s1 = 0$ pues $\mathbb{F}_q$ es un dominio entero, pero esto contradice que p sea el mínimo entero tal que $p1 = 0$, lo que es una contradicción, por lo tanto, p es un número primo.

(ii) Considérese el espacio vectorial ${}_K\mathbb{F}_q$ y dado que $\mathbb{F}_q$ es un campo finito, ${}_K\mathbb{F}_q$ es finito dimensional. Sea $n = [\mathbb{F}_q : K]$, esto implica que $\mathbb{F}_q$ admite una base de n elementos, dígamos $\beta := \{v_1, v_2, \ldots, v_n\}$, donde cada $v_i \in \mathbb{F}_q$ para $i \in \{1, 2, \ldots, n\}$, así, todo elemento de $a \in \mathbb{F}_q$ es de la forma, $a = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, donde $\alpha_i \in K$ para $i \in \{1, 2, \ldots, n\}$. Dado que $\mid K \mid = r$ entonces, la expresión $a = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, admite r^n posibilidades, es decir, $q = r^n$.

(iii) Sea F el subcampo primo de $\mathbb{F}_q$, entonces $1 \in F$, luego, para cada $m \in \mathbb{N}$ el elemento $m1 = 1 + 1 + \cdots + 1$, pertenece a F. Considérese ahora:

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & F \\ & m & \longmapsto & m1 \end{array}$$

es claro que ϕ es un homomorfismo de anillos y dado que es sobreyectiva, es un epimorfismo. Veamos que $\ker\phi = p\mathbb{Z}$. Tenemos que $\phi(1) = 1$, donde 1 denota a los elementos identidad en los anillos $\mathbb{Z}$ y F. Sea $m \in \ker\phi$ entonces, $\phi(m) = 0$ luego $m1 = 0$, así, $p \mid m$, pues p es la característica de F, por consiguiente, $m \in p\mathbb{Z}$. Ahora, si $m \in p\mathbb{Z}$, es claro que, $p \mid m$ entonces, $m = pk$ para algún $k \in \mathbb{Z}$, lo cual implica que $\phi(m) = m1 = (pk)1 = p(k1) = 0$, entonces, $\ker\phi = p\mathbb{Z}$, por (ii) del Teorema 1.7.9, existe un isomorfismo entre $\mathbb{Z}/\ker\phi$ y F, pero como vimos en la Observación 1.8.2, $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker\phi$, por lo tanto, $\mathbb{F}_p \simeq F$ como afirmamos. Finalmente, es claro que $|F| = |\mathbb{F}_p| = p$ y por (ii) de este teorema $q = p^n$, donde $n = [\mathbb{F}_q : \mathbb{F}_p]$.

(iv) Considérese un elemento $\alpha \in \mathbb{F}_q$ entonces $\alpha = 0$ o bien $\alpha \in \mathbb{F}_q^*$. Si $\alpha = 0$ es claro que $\alpha^q = 0$, por otro lado, si $\alpha \neq 0$ entonces dado que $(\mathbb{F}_q^*, \cdot)$ es un grupo multiplicativo de orden $q-1$, se sigue del Corolario 1.3.7(a) que $\alpha^{q-1} = 1$ y multiplicando por α obtenemos el resultado deseado. □

Como vimos en la sección 1.6, el conjunto $\mathbb{F}_q[x]$ es un anillo de polinomios con coeficientes en el campo $\mathbb{F}_q$. Por el Lema 1.6.14, es un anillo euclidiano, así, por el Teorema 1.6.13, es un dominio de ideales principales y por el Teorema 1.5.20 es un dominio de factorización única. Al tratar con polinomios, la factorización de éstos es un tópico de sumo interés y como $\mathbb{F}_q[x]$ es un DFU, todo elemento admite una descomposición en producto de elementos irreducibles y ésta es única salvo asociados, es decir, para cada $f(x) \in \mathbb{F}_q[x]$, existen $p_1(x), p_2(x), \ldots, p_r(x)$ y $m_1, m_2, \ldots, m_r \in \mathbb{N}$ con $r \in \mathbb{N}$, tales que, $f(x) = (p_1(x))^{m_1}(p_2(x))^{m_2}\cdots(p_r(x))^{m_r}$ donde cada $p_i(x)$ es un elemento irreducible del anillo $\mathbb{F}_q[x]$, con $i \in \{1, 2, \ldots, r\}$. En lo sucesivo, cada vez que un polinomio $p(x)$ es un elemento irreducible, diremos que es un **polinomio irreducible**. Por el Lema 1.5.14, si $p(x)$ es un polinomio irreducible entonces el ideal $\langle p(x)\rangle$ es un ideal maximal de $\mathbb{F}_q[x]$ y luego por el Lema 1.7.12, $\mathbb{F}_q[x]/\langle p(x)\rangle$ es un campo, además, éste es un campo definido por la relación de congruencia módulo un ideal. Por el Corolario 1.7.2, tenemos que para cada clase de equivalencia $[f(x)] \in \mathbb{F}_q[x]/\langle p(x)\rangle$ existe un elemento $r(x) \in \mathbb{F}_q[x]$ tal que $[f(x)] = q(x) + \langle p(x)\rangle$, en virtud de esto se tiene el siguiente:

Corolario 1.8.7. *Si $p(x)$ un polinomio irreducible en $\mathbb{F}_q[x]$ de grado $m \in \mathbb{N} \cup \{0\}$. Entonces:*

$$\frac{\mathbb{F}_q[x]}{\langle p(x)\rangle} = \{[a_0 + a_1x + \cdots + a_{m-1}x^{m-1}] \mid a_i \in \mathbb{F}_q \text{ para } i \in \{0, 1, \ldots, m-1\}\}.$$

y éste es un campo finito con p^{nm} elementos, donde $n \in \mathbb{N}$ y p es un número primo.

en lo sucesivo, se pueden omitir los corchetes que representan a la clase de equivalencia y tomar al polinomio $r(x)$ representante de la clase $r(x) + I$.

Definición 1.8.8. Sean $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}_q[x]$, $n \in \mathbb{N}$ y $\alpha \in \mathbb{F}_q$. Diremos que $\beta \in \mathbb{F}_q$ es la **imagen de** α **bajo f** si resulta de sustituir a x por α en $f(x)$ es decir:

$$\beta = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

también se suele decir que β es "f de α", más aún, diremos que α es una raíz del polinomio $f(x)$ si y sólo si $f(\alpha) = 0$.

Teorema 1.8.9. *Un elemento $\alpha \in \mathbb{F}_q$ es una raíz de un polinomio $f(x) \in \mathbb{F}_q[x]$ si y sólo si $(x-\alpha) \mid f(x)$.*

Definición 1.8.10. Sea α una raíz de un polinomio $f(x) \in \mathbb{F}_q[x]$, si $k \in \mathbb{N}$ es tal que $(x-\alpha)^k \mid f(x)$ pero $(x-\alpha)^{k+1} \nmid f(x)$ entonces diremos que k es la **multiplicidad** de la raíz α. Si $k = 1$, decimos que α es una **raíz simple** y si $k \geqslant 2$, entonces diremos que α es una **raíz múltiple** de $f(x)$.

Corolario 1.8.11. *Sean $f(x) \in \mathbb{F}_q[x]$ un polinomio de grado $n \in \mathbb{N} \cup \{0\}$ y $\alpha_1, \alpha_2, \ldots, \alpha_m$ raíces distintas de $f(x)$ para $m \in \mathbb{N}$, con multiplicidad $k_1, k_2, \ldots, k_m$, respectivamente. Entonces:*

$$(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_m)^{k_m} \mid f(x)$$

y $f(x)$ tiene a lo más n raíces en $\mathbb{F}_q$.

Definición 1.8.12. Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}_q[x]$ para $n \in \mathbb{N} \cup \{0\}$. Entonces definimos la **derivada de** $f(x)$ como el polinomio $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$.

Teorema 1.8.13. *Un elemento $\alpha \in \mathbb{F}_q$ es una raíz múltiple de un polinomio $f(x)$ si y sólo si es raíz de $f(x)$ y $f'(x)$.*

Demostración. Supóngase que α es una raíz múltiple de multiplicidad k, entonces por el Corolario 1.8.11, $(x-\alpha)^k \mid f(x)$ entonces $f(x) = (x-\alpha)^k q(x)$, luego tenemos que $f'(x) = k(x-\alpha)^{k-1}q(x) + (x-\alpha)^k q'(x)$[6], así, $f'(\alpha) = k\left[(\alpha-\alpha)^{k-1}\right]q(\alpha) + (\alpha-\alpha)^k q'(\alpha) = 0$, entonces α es raíz también de $f'(x)$. Por otro lado, si α es raíz de $f(x)$ como de $f'(x)$, por el Teorema 1.8.9, $(x-\alpha) \mid f(x)$ y $(x-\alpha) \mid f'(x)$ luego existen $q_1(x), q_2(x) \in \mathbb{F}_q[x]$, tales que, $f(x) = (x-\alpha)q_1(x)$ y $f'(x) = (x-\alpha)q_2(x)$ así,

$$\begin{aligned}
\Rightarrow\ f'(x) &= (x-\alpha)q_1'(x) + q_1(x)\\
\Rightarrow\ q_1(x) &= (x-\alpha)q_1'(x) - f'(x)\\
\Rightarrow\ q_1(x) &= (x-\alpha)\left[q_1'(x) - q_2(x)\right]\\
\Rightarrow\ f(x) &= (x-\alpha)\left((x-\alpha)\left[q_1'(x) - q_2(x)\right]\right)\\
\Rightarrow\ f(x) &= (x-\alpha)^2\left[q_1'(x) - q_2(x)\right]
\end{aligned}$$

es decir, $(x-\alpha)^2 \mid f(x)$, entonces, α es una raíz múltiple de $f(x)$ con índice de multiplicidad al menos 2. □

Corolario 1.8.14. *Si $\mathbb{F}_q$ es un campo finito y $f(x) \in \mathbb{F}_q[x]$ con grado 2 o 3, entonces $f(x)$ es irreducible si y sólo si no tiene raíces en $\mathbb{F}_q$*

6 Aquí se ha aplicado la fórmula de derivación de un producto $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$, omitimos la demostración de este hecho por motivos de espacio.

Demostración. Si $f(x)$ es irreducible no puede tener una raíz, pues de tenerla, por el Teorema 1.8.9, $(x-\alpha) \mid f(x)$ y $(x-\alpha)$ no es una unidad en $\mathbb{F}_q[x]$. Si $f(x) = g(x)h(x)$ y no tiene raíces entonces $grad(f(x)) = grad(g(x)) + grad(h(x))$, si $grad(f(x))$ entonces tanto $g(x)$ como $h(x)$ son polinomios de grado uno, es decir, $g(x) = g_0 + g_1x$ y $h(x) = h_0 + h_1x$ así los elementos $\alpha = -g_0g_1^{-1}$ y $\beta = -h_0h_1^{-1}$ son raíces de $g(x)$ y $h(x)$ respectivamente y por tanto de $f(x)$, lo que es una contradicción. Si $grad(f(x)) = 3$ entonces al menos $g(x)$ o $h(x)$ son de grado 1, por consiguiente, $f(x)$ tendría una raíz, lo que es imposible, por lo tanto, $f(x)$ es irreducible. □

Ejemplo 1.8.15. 1. Considérese el campo finito $\mathbb{F}_2 = \{0, 1\}$ entonces para el polinomio $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ tenemos que $f(0) = f(1) = 1$ entonces $f(x)$ es irreducible en $\mathbb{F}_2[x]$, pues no tiene raíces en $\mathbb{F}_2$. Busquemos los polinomios irreducibles de grado 3 en $\mathbb{F}_2[x]$, todos los polinomios de grado 3 son:

$$\mathbb{F}_2\left[x^3\right] = \{x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\}$$

$f(x)$	$f(0)$	$f(1)$
x^3	0	1
x^3+1	1	0
x^3+x	0	0
x^3+x+1	1	1
x^3+x^2	0	0
x^3+x^2+1	1	1
x^3+x^2+x	0	1
x^3+x^2+x+1	1	0

Figura 1: Polinomios de grado 3 en $\mathbb{F}_2[x]$ y sus imágenes

usando el corolario anterior, tenemos que los polinomios irreducibles de grado 3 en $\mathbb{F}_2[x]$ son x^3+x+1 y x^3+x^2+1, usando éstos, podemos definir campos finitos a través del anillo polinomial $\mathbb{F}_2[x]$, pero antes de esto, estudiaremos algunos resultados más sobre campos finitos.

Definición 1.8.16. Sea $\mathbb{F}$ una extensión de un campo K y considérese a $\theta \in \mathbb{F}$. Diremos que θ es un **elemento algebraico sobre el campo** K si éste satisface una ecuación polinomial no trivial con coeficientes en K, es decir:

$$c_n\theta^n + c_{n-1}\theta^{n-1} + \cdots + c_1\theta + c_0 = 0$$

donde $c_i \in K$ y no todos son cero para $i \in \{0, 1, \ldots, n\}$, además si todos los elementos de $\mathbb{F}$ son algebraicos sobre K decimos que $\mathbb{F}$ es una **extensión algebraica** de K.

Teorema 1.8.17. *Sea $\mathbb{F}$ un campo.*

(i) *Toda extensión finita de $\mathbb{F}$ es algebraica.*

(ii) *Si $p(x) \in \mathbb{F}$ es un polinomio irreducible de grado $m \geqslant 1$, sobre el campo $\mathbb{F}$, entonces existe una extensión algebraica simple de $\mathbb{F}$ con una raíz de $p(x)$ como elemento que la define.*

Demostración. (i) Sea $\mathcal{K}$ una extensión finita de $\mathbb{F}$ y nombremos $m = [\mathcal{K} : \mathbb{F}]$. Para cada $\theta \in \mathcal{K}$ el conjunto $\{1, \theta, \theta^2, \ldots, \theta^m, \theta^{m+1}\}$ es linealmente dependiente, entonces existen *escalares* $c_i \in \mathbb{F}$ no todos iguales a cero para $i \in \{1, 2, \ldots, m, m+1\}$ tales que $c_0 + c_1\theta + \cdots + c_m\theta^m + c_{m+1}\theta^{m+1} = 0$, por la Definición 1.8.16, θ es algebraico y por lo tanto, $\mathcal{K}$ es una extensión algebraica de $\mathbb{F}$.

(ii) Denotemos por $P = \langle p(x)\rangle$ y $\mathcal{L} = \mathbb{F}[x]/P$ al campo[7] de clases residuales módulo P. Como vimos en el Corolario 1.8.7 la clase de equivalencia $f(x) + P$ corresponde a la clase de un polinomio $[r(x)]$ de grado a lo más $m-1$. Sean $a, b \in \mathbb{F}$, es claro que $a + P = [a]$ y $b + P = [b]$ puesto que un polinomio no puede ser de grado negativo. Considérese la función $\phi : \mathbb{F} \longrightarrow F$ donde $F = \{[a] \mid a \in \mathbb{F}\} \subseteq \mathcal{L}$ y que asocia al polinomio constante a con la clase de equivalencia $[a]$, entonces note que $\phi(a+b) = [a+b] = [a] + [b]$ y también $\phi(ab) = [ab] = [a][b]$ por las operaciones entre clases y del hecho que $grad(ab) = grad(a) + grad(b) = 0 + 0 = 0$ además, $\phi(a) = \phi(b)$ implica que $[a] = [b]$ entonces $a - b \in P = \langle p(x)\rangle$ luego, $(a-b) = p(x)q(x)$ pero $grad(p(x)) \geqslant 1 > grad(a-b)$ así $q(x) = 0$ y en consecuencia $a - b = 0$ por consiguiente $a = b$ y así, ϕ es un monomorfismo. Por (3.) de la Observación 1.8.2, tenemos que $\mathcal{L}$ es una extensión de $\mathbb{F}$. Tomaremos a ϕ como la identificación del elemento $a \in \mathbb{F}$ en el campo residual $\mathcal{L}$, entonces toda clase $[r(x)] \in \mathcal{L}$ tal que $r(x) = [a_0 + a_1x + \cdots + a_{m-1}x^{m-1}] = [a_0] + [a_1][x] + \cdots [a_{m-1}][x]^{m-1}$ puede ser reescrita de la forma, $[r(x)] = a_0 + a_1[x] + \cdots + a_{m-1}[x]^{m-1}$, usando dicha identificación, $[r(x)]$ puede ser considerado como un polinomio en la indeterminada $[x]$ con coeficientes en $\mathbb{F}$. Sea $\mathcal{K}$ un campo tal que contiene a $\mathbb{F} \leqslant \mathcal{L}$ y al elemento $[x] \in \mathcal{L}$, luego $\mathcal{K}$ contiene a $\mathbb{F}([x])$ y entonces $\mathcal{L} \subseteq \mathcal{K}$, para cada campo que cumpla lo antes dicho, es decir,

$$\mathcal{L} \subseteq \bigcap\{\mathcal{K} \mid \mathbb{F} \subset K \text{ y } [x] \in \mathcal{K}\} = \mathbb{F}([x]) \text{ (ver Definición 1.8.4)}$$

y de manera evidente $\mathbb{F}([x]) \subseteq \mathcal{L}$ se puede concluir que $\mathcal{L} = \mathbb{F}([x])$ y así $\mathcal{L}$ es una extensión simple de $\mathbb{F}$ y por ser una extensión finita es claro que $\mathcal{L}$ es una extensión alegbraica por (i) de esta demostración. Finalmente, como $p(x) = c_0 + c_1x + \cdots + c_{m-1}x^{m-1} + c_mx^m$, tenemos que,

$$\begin{aligned} p([x]) &= c_0 + c_1[x] + \cdots + c_{m-1}[x]^{m-1} + c_m[x]^m \\ &= [c_0 + c_1x + \cdots + c_{m-1}x^{m-1} + c_mx^m] \qquad \text{(por la identificación } \phi\text{)} \\ &= p(x) + \langle p(x)\rangle = [0] \end{aligned}$$

es decir, $p([x]) = [0]$, así, $[x]$ es una raíz de $p(x)$ que define a la extensión $\mathcal{L}$. □

Definición 1.8.18. Sea θ un elemento algebraico sobre un campo $\mathbb{F}$, diremos que un polinomio mónico $m(x) \in \mathbb{F}[x]$ es el **polinomio mínimo** de θ si es el único polinomio mónico de grado menor en $\mathbb{F}[x]$ que tiene a θ como raíz, y llamaremos grado de θ sobre $\mathbb{F}$ al grado de su polinomio mínimo.

Teorema 1.8.19. *(Existencia y unicidad del polinomio mínimo) Si θ es un elemento algebraico sobre $\mathbb{F}$ entonces se cumple que:*

(i) *El conjunto $J = \{f(x) \in \mathbb{F} \mid f(\theta) = 0\}$ es un ideal principal en $\mathbb{F}[x]$ y es generado por el polinomio mínimo de θ, $m(x)$.*

7 Le recordamos al lector que $\mathcal{L}$ es un campo pues el ideal $\langle p(x)\rangle$ es maximal.

(ii) $m(x)$ *es irreducible.*

(iii) *Si* $g(x) \in \mathbb{F}[x]$ *entonces* $g(\theta) = 0$ *si y sólo si* $m(x) \mid g(x)$.

Demostración. (i) Sean $f(x), g(x) \in J$ entonces $f(\theta) = g(\theta) = 0$ así, $f(\theta) - g(\theta) = 0$, es decir, $f(x) - g(x) \in J$ se sigue que $(J, +) \leqslant (\mathbb{F}[x], +)$. Por otro lado, sean $f(x) \in J$ y $h(x) \in \mathbb{F}[x]$ entonces $f(\theta)h(\theta) = 0h(\theta) = 0$, es decir, $f(x)h(x) \in J$ y en consecuencia J es un ideal de $\mathbb{F}[x]$. Como $\mathbb{F}[x]$ es un dominio de ideales principales, tenemos que existe algún $m_0(x) \in \mathbb{F}[x]$ tal que $J = \langle m(x) \rangle$, note que $m(x)$ debe ser mónico pues de no serlo tenemos que $m_0(x) = c_n^{-1}(m(x))$ donde c_n es el coeficiente principal de $m(x)$, es un polinomio mónico de grado igual a $m(x)$ tal que $m_0(\theta) = 0$ y $J = \langle m(x) \rangle = \langle m_0(x) \rangle$, así que sin pérdida de generalidad podemos suponer que $m(x)$ es mónico. Veamos que $m(x)$ es el polinomio mínimo de θ. Sea $l(x)$ un polinomio mónico de grado menor tal que $l(\theta) = 0$ entonces $l(x) \in J = \langle m(x) \rangle$, así $l(x) = m(x)q_1(x)$, y por otro lado usando el algoritmo de la división tenemos que $m(x) = l(x)q_2(x) + r(x)$ para algunos $q_2(x), r(x) \in \mathbb{F}$ con $r(x) = 0$ o $grad(r(x)) < grad(l(x))$, evaluando en θ se tiene que $0 = m(\theta) = l(\theta)q_2(\theta) + r(\theta) = r(\theta)$ pero esto es una contradicción pues $l(x)$ es el polinomio de grado menor que tiene a θ como raíz, entonces $r(x) = 0$ y como consecuencia $m(x) = l(x)q_2(x)$ pero entonces $m(x) = m(x)q_1(x)q_2(x)$, de ahí que $m(x)(1 - q_1(x)q_2(x)) = 0$, y tenemos que $q_1(x)q_2(x) = 1$ (pues $\mathbb{F}[x]$ es un dominio entero), es decir, son unidades de $\mathbb{F}[x]$, en particular, son polinomios constantes, pero $l(x) = m(x)q_1(x)$ y tanto $l(x)$ como $m(x)$ son mónicos, entonces $q_1(x) = 1$, análogamente $q_2(x) = 1$ y por lo tanto $l(x) = m(x)$, así $m(x)$ es el polinomio mínimo de θ y éste es único.

(ii) Supóngase que $m(x) = h_1(x)h_2(x)$ donde $grad(m(x)) > grad(h_1(x)), grad(h_2(x)) > 0$, se sigue que $0 = m(\theta) = h_1(\theta)h_2(\theta)$ y nuevamente como $\mathbb{F}[x]$ es un dominio entero tenemos que θ es raíz de $h_1(x)$ o de $h_2(x)$, supongamos que es raíz de $h_1(x)$, tenemos entonces por definición que $h_1(x) \in J$ lo cual implica que $h_1(x) = m(x)q(x)$ para algún, $q(x) \in \mathbb{F}[x]$, y esto implica que $grad(h_1(x)) \geqslant grad(m(x))$ lo cual es una contradicción, análogamente si θ es raíz de $h_2(x)$, por lo tanto, $m(x)$ es irreducible. No es difícil ver que (iii) se sigue de la prueba de (i) con lo cual nuestro resultado queda demostrado. □

Teorema 1.8.20. *Sea* θ *un elemento algebraico de grado* n *sobre* $\mathbb{F}$ *en una extensión* K *y denotemos por* $m(x)$ *al polinomio mínimo de* θ *entonces:*

1. $\mathbb{F}(\theta)$ *es isomorfo a* $\mathbb{F}[x]/\langle m(x) \rangle$.
2. $[\mathbb{F}(\theta) : \mathbb{F}] = n$ *y* $\{1, \theta, \ldots, \theta^{n-1}\}$ *es una base de* ${}_{\mathbb{F}}\mathbb{F}(\theta)$.

Demostración. (i) Considérese $\phi : \mathbb{F}[x] \longrightarrow \mathbb{F}(\theta)$ una función tal que, a cada $f(x) \in \mathbb{F}[x]$ lo relaciona con $f(\theta) \in \mathbb{F}(\theta)$, como en la Definición 1.8.8. Dados $f(x), g(x) \in \mathbb{F}[x]$ tenemos que $\phi(f(x) + g(x)) = f(\theta) + g(\theta) = \phi(f(x)) + \phi(g(x))$, además,$\phi(f(x)g(x)) = f(\theta)g(\theta) = \phi(f(x))\phi(g(x))$, así, ϕ es un homomorfismo de anillos. Note que $\ker\phi = \{f(x) \in \mathbb{F}[x] \mid \phi(f(x)) = 0\} = \{f(x) \in \mathbb{F}[x] \mid f(\theta) = 0\} = \langle m(x) \rangle$ donde $m(x)$ es el polinomio mínimo de θ, por (ii) Teorema 1.7.9 $\mathbb{F}[x]/\langle m(x) \rangle$ es isomorfo a $Im\phi$, donde $Im\phi = \{f(\theta) \mid f(x) \in \mathbb{F}[x]\}$ es decir, el conjunto de todas las expresiones polinomiales en la indeterminada θ con coeficientes en $\mathbb{F}$, entonces $Im\phi \subseteq \mathbb{F}(\theta) \leqslant K$, más aún,

$\mathrm{Im}\phi$ es un campo pues $\mathbb{F}[x]/\langle m(x)\rangle$ lo es, y es claro que $\theta \in \mathrm{Im}\phi$, es decir, $\mathrm{Im}\phi$ es un subcampo de K tal que $\theta \in \mathrm{Im}\phi$, pero $\mathbb{F}(\theta)$ es el campo más pequeño que cumple esta condición entonces $\mathbb{F}(\theta) \subseteq \mathrm{Im}\phi$ y en consecuencia son iguales, por lo tanto, $\mathbb{F}[x]/\langle m(x)\rangle \simeq \mathbb{F}(\theta)$.

(ii) Sea $\alpha \in \mathbb{F}(\theta) = \mathrm{Im}\phi$ entonces existe $f(x) \in \mathbb{F}[x]$ tal que $\alpha = f(\theta)$ y por el algoritmo de la división existen $q(x), r(x) \in \mathbb{F}[x]$ tales que $f(x) = q(x)m(x) + r(x)$ donde $r(x) = 0$ o bien $0 \leqslant grad(r(x)) < grad(m(x)) = n$ así, evaluando en θ tenemos que: $\alpha = f(\theta) = q(\theta)m(\theta) + r(\theta)$, luego $\alpha = r(\theta)$ una combinación lineal de los elementos de $\mathcal{B} = \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ puesto que $r(x)$ es un polinomio de a lo más grado $n-1$ entonces $\mathcal{B}$ genera a $\mathbb{F}(\theta)$ sobre $\mathbb{F}$. Por otro lado, si tomamos $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{F}$ tales que $\lambda_0 + \lambda_1\theta + \cdots \lambda_{n-1}\theta^{n-1} = 0$ entonces el polinomio $\lambda(x) = \lambda_0 + \lambda_1\theta + \cdots \lambda_{n-1}\theta^{n-1}$ tiene a θ como raíz lo que es imposible puesto que $grad(\lambda(x)) < grad(m(x))$ por lo tanto $\lambda(x) = 0$ esto es que $\lambda_i = 0$ para cada $i \in \{0, 1, \ldots, n-1\}$, en conclusión, $\mathcal{B}$ es linealmente independiente y por tanto una base de ${}_{\mathbb{F}}\mathbb{F}(\theta)$. □

El teorema anterior, es de suma importancia dado que ya al ser isomorfos $\mathbb{F}[x]/\langle m(x)\rangle$ y ${}_{\mathbb{F}}\mathbb{F}(\theta)$ todo elemento de $\mathbb{F}(\theta)$ puede ser expresado de manera única en la forma $c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}$ con $c_i \in \mathbb{F}$ para cada $i \in \{0, 1, \ldots, n-1\}$.

Ejemplo 1.8.21. Considérese el polinomio $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ el cual hemos visto que es irreducible, además si tomamos los polinomios de $\mathbb{F}_2[x]$ de grado a lo más 1 es claro que podemos expresar $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ mediante $\{0, 1, [x], [x] + 1\}$, más aún si θ es una raíz del polinomio $p(x)$ tenemos que $\theta^2 + \theta + 1 = 0$ así $\theta^2 = \theta + 1$ y multiplicando por θ llegamos a $\theta^3 = \theta^2 + \theta = 1$, así θ es un elemento de orden 3 en $\mathbb{F}(\theta)$ así, $\mathbb{F}(\theta) = \{0, 1, \theta, \theta^2\} \simeq \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ y también por los calculos previos $\mathbb{F}(\theta) = \{0, 1, \theta, \theta + 1\}$, lo que muestra que estos conjuntos son isomorfos. Verifiquemos que $\mathbb{F}(\theta)$ es un campo.

$+$	0	1	θ	$\theta+1$
0	0	1	θ	$\theta+1$
1		0	$\theta+1$	θ
θ			0	1
$\theta+1$				0

Figura 2: Tabla de Cayley para $(\mathbb{F}(\theta), +)$

$\cdot$	1	θ	$\theta+1$
1	1	θ	$\theta+1$
θ		$\theta+1$	1
$\theta+1$			1

Figura 3: Tabla de Cayley para $(\mathbb{F}(\theta) - \{0\}, \cdot)$

Definición 1.8.22. Sea $f(x)$ un polinomio de grado $n \in \mathbb{N}$, en el anillo de polinomios $\mathbb{F}[x]$, y sea E una extensión de $\mathbb{F}$, diremos que $f(x)$ se **descompone(escinde, factoriza)** en E si existen $\alpha_1, \alpha_2 \ldots, \alpha_n \in E$ tales que:

$$f(x) = c_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in E[x] \tag{1.8.1}$$

donde c_n es el coeficiente principal de $f(x)$. Diremos que E es el **campo de descomposición(factorización, escisión)** de $f(x)$.

Teorema 1.8.23. *Sean α y β dos raíces de un polinomio $f(x) \in \mathbb{F}[x]$ que es irreducible sobre $\mathbb{F}$, entonces $\mathbb{F}(\alpha)$ es isomorfo a $\mathbb{F}(\beta)$ mediante un isomorfismo que deja fijos a los elementos de $\mathbb{F}$.*

Demostración. Como $grad(f(x)) \geqslant 1$ y éste es irreducible entonces existe una extensión alegbraica simple de $\mathbb{F}$ definida por α una raíz de $f(x)$, sea pues $\mathbb{F}(\alpha)$ dicha extensión y dado que β es otra raíz análogamente podemos tomar la extensión algebraica $\mathbb{F}(\beta)$, además consideremos a ambas extensiones como espacios vectoriales sobre $\mathbb{F}$. Ahora, considérese la función:

$$\begin{array}{rccc} \phi: & \mathbb{F}(\alpha) & \longrightarrow & \mathbb{F}(\beta) \\ & f(\alpha) & \longmapsto & f(\beta) \end{array}$$

considerando a los elementos de cada extensión como expresiones polinomiales de grado a lo más $n-1$, como se hizo en la prueba del Teorema 1.8.20 es claro que ϕ es un homomorfismo de anillos. Sea $f(\alpha) \in \ker\phi$ entonces $a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1} = f(\alpha) = 0 + 0\beta + \cdots + 0\beta^{n-1}$ y como $\{1, \beta, \ldots, \beta^{n-1}\}$ es una base para $\mathbb{F}(\beta)$ se sigue que la representación de $f(\alpha)$ es única, por consiguiente,$a_i = 0$ para cada $i \in \{0, 1, \ldots, n-1\}$ por lo tanto $f(\alpha) = 0$, entonces ϕ es un monomorfismo, además, por la forma de los elementos de $\mathbb{F}(\beta)$ y dado que el campo de coeficientes es el mismo, la función ϕ es un epimorfismo y en consecuencia un isomorfismo, por lo tanto, $\mathbb{F}(\alpha)\} \simeq \mathbb{F}(\beta)$. Si $a \in \mathbb{F}$ entonces tenemos que $a = a + 0\alpha + \cdots + 0\alpha^{n-1}$, luego $\phi(a) = a + 0\beta + \cdots + 0\beta^{n-1} = a$ así, ϕ deja fijos a los elementos de $\mathbb{F}$. □

Corolario 1.8.24. *Sea $f(x) \in \mathbb{F}[x]$ un polinomio de grado n, entonces existe E una extensión de $\mathbb{F}$ que es el campo de descomposición de $f(x)$ y éste es único salvo isomorfismos.*

Demostración. Por el Corolario 1.8.11, $f(x)$ tiene a lo más n raíces en $\mathbb{F}$. Sean $\alpha_1, \alpha_2, \ldots, \alpha_m$ con $m \leqslant n$ dichas raíces. Si $m = n$ hemos terminado, de lo contrario, por el Teorema 1.8.9, $(x - \alpha_i) \mid f(x)$ para $i \in \{1, 2, \ldots, m\}$ entonces $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)g_1(x)$ con $grad(g_1(x)) = n - m$. Supongamos, sin pérdida de generalidad que $g_1(x)$ es irreducible[8] sobre $\mathbb{F}[x]$, entonces por el Teorema 1.8.17 existe una extensión algebraica simple de $\mathbb{F}$ definida por una raíz β_1 de $g_1(x)$, sea pues K_1 dicha extensión luego, $g_1(x) = (x-\beta_1)g_2(x)$ y en consecuencia $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)(x-\beta_1)g_2(x) \in K_1[x]$, con $\mathbb{F} \leqslant K_1$. Nuevamente, suponiendo que $g_2(x)$ es irreducible pero ahora sobre $K_1[x]$, existe una extensión algebraica simple K_2 definida por $\beta_2 \in K_2$, una raíz de $g_2(x)$, obteniendo que $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)(x-\beta_1)(x-\beta_2)g_3(x) \in K_2[x]$ y $\mathbb{F} \leqslant K_1 \leqslant K_2$. Procediendo de esta manera se obtiene que:

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\beta_1)(x-\beta_2)\cdots(x-\beta_{n-m-1})h(x) \in K_{n-m-1}[x]$$

donde $h(x)$ es un polinomio de grado uno, luego $h(x) = cx + d = c(x - (-c^{-1}d)$ y así, $\beta_{n-m} = -c^{-1}d$ es una raíz de $h(x)$, por lo tanto, $f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})(x-\alpha_n)$ donde $\alpha_{m+j} = \beta_j$ con $j \in \{1, 2, \ldots, n-m\}$. Note que en cada paso $\mathbb{F} \leqslant K_1 \cdots \leqslant K_{n-m-1}$ entonces nombrando $E = K_{n-m-1}$, éste contiene a todas las raíces de $f(x)$. Cada polinomio $(x-\alpha_i)$ es un polinomio mónico entonces $\prod_{i=1}^{n}(x-\alpha_i)$ es también un polinomio mónico, es decir, el coeficiente de x^n es 1 y como $f(x) = c\prod_{i=1}^{n}(x-\alpha_i)$ es claro que c debe ser el coeficiente de principal de $f(x)$, por la Definición 1.8.22, E es el campo de descomposición de $f(x)$, más aún $\mathbb{F} \leqslant E$ y $\alpha_i \in E$ para $i \in \{1, 2, \ldots, n\}$, usando el isomorfismo del Teorema 1.8.23 para cada raíz de $f(x)$ tenemos que $E \simeq \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. □

8 Si $g_1(x)$ no fuera irreducible, sabemos que es producto de un número finito de polinomios irreducibles y así el procedimiento aplicado en esta prueba se aplicaría a cada factor de $g_1(x)$.

Teorema 1.8.25. *Sea $\mathbb{F}_q$ un campo finito y $F \leqslant \mathbb{F}_q$. Entonces el polinomio $f(x) = x^q - x \in F[x]$ tiene a $\mathbb{F}_q$ como campo de descomposición.*

Demostración. Por el teorema anterior, existe el campo de descomposición de $f(x)$. Como $\mathbb{F}_q$ es un conjunto finito, podemos escribir $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ y usando $iv)$ del Teorema 1.8.6 $\alpha_i^q = \alpha_i$ para $i \in \{1, 2, \ldots, q\}$, pero $f(\alpha_i) = \alpha_i^q - \alpha_i = 0$ entonces α_i es una raíz de $f(x)$ para cada $i \in \{1, 2, \ldots, q\}$, se sigue que $f(x)$ tiene q raíces en $\mathbb{F}_q$ y $grad(f(x)) = q$ entonces $\mathbb{F}_q$ tiene todas las raíces de $f(x)$, luego por el Corolario 1.8.11,

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_q) \mid x^q - x.$$

La igualdad de $x^q - x$ con $\prod_{i=1}^{q}(x - \alpha_i)$ se sigue de que $x^q - x$ es un polinomio mónico, así, por la Definición 1.8.22, $\mathbb{F}_q$ debe ser el campo de descomposición de $x^q - x$. □

Teorema 1.8.26. *Para cada número primo p y cada entero positivo n existe un campo finito con p^n elementos y todo campo finito $\mathbb{F}_q$ con $q = p^n$ elementos es isomorfo al campo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$.*

Demostración. Sea $q = p^n$ y considérese el polinomio $x^q - x \in \mathbb{F}_p[x]$. Como la derivada de éste es $qx^{q-1} - 1$ tenemos que $(qx^{q-1} - 1) = 0 - 1 = -1 \in \mathbb{F}_p$ pues la característica de $\mathbb{F}_p[x]$ es p, así $0(x^q - x) + (-1)(qx^{q-1} - 1) = 1$ y por la Definición 1.6.19, $x^q - x$ y su derivada son coprimos, es decir, su máximo común divisor es 1, luego no tienen raíces múltiples pues de tener alguna, dígamos α, $(x - \alpha) \mid x^q - x$ y $(x - \alpha) \mid qx^{q-1} - 1$, entonces, $(x - \alpha) \mid 1$, lo cual es imposible pues $grad(x - \alpha) = 1 > 0 = grad(1)$, por lo tanto, $x^q - x$ no tiene raíces múltiples, pues no comparte raíces con su derivada. Sea $\mathbb{F} = \{r \in K \mid r^q = r\}$ para K el campo de descomposición de $x^q - x$. Sean $r, s \in \mathbb{F}$ como $(r - s)^q = (r - s)^{p^n}$ entonces aplicando el Teorema A.1.1 repetidas veces tenemos que $(r - s)^q = r^q - s^q = (r - s)$ así $(r - s) \in \mathbb{F}$ y se tiene que $(\mathbb{F}, +) \leqslant (K, +)$. Si $s \neq 0$ es claro que $(s^q)^{-1} = (s^{-1})^q$ por la conmutatividad de K^*, entonces $(rs^{-1})^q = r^q(s^{-1})^q = r^q(s^q)^{-1} = rs^{-1}$ es decir, $rs^{-1} \in \mathbb{F}$ por consiguiente, $(\mathbb{F} - \{0\}, \cdot) \leqslant (K^*, \cdot)$ y por lo tanto $\mathbb{F}$ es un subcampo de K, más aún todo elemento $\alpha \in \mathbb{F}$ satiface que $\alpha^q - \alpha = 0$ es decir, es una raíz de $x^q - x$ y toda raíz de este polinomio es un elemento de $\mathbb{F}$, por lo tanto, $\mathbb{F}$ tiene a todas las raíces de $x^q - x$, luego es isomorfo a K por el Corolario 1.8.24 y así tiene $q = p^n$ elementos. Para concluir, si $\mathbb{F}_q$ es un campo finito entonces tiene característica p primo, su subcampo primo es isomorfo a $\mathbb{F}_p$ y por el Teorema 1.8.25, $\mathbb{F}_q$ es el campo de descomposición de $x^q - x$. □

Teorema 1.8.27. *[Criterio del subcampo] Todo subcampo de $\mathbb{F}_q$ tiene p^m elementos, donde p es un número primo y $m \in \mathbb{N}$ es tal que $m \mid n$ y para todo $m \in \mathbb{N}$ divisor de n, existe un único subcampo de $\mathbb{F}_q$ con p^m elementos.*

Demostración. Como $\mathbb{F}_q$ es finito, su característica es p, luego su campo primo es isomorfo a $\mathbb{F}_p$, podemos decir que $\mathbb{F}_p$ es el subcampo primo, éste tiene p elementos así, el resultado se cumple para $m = 1$. Si $F \leqslant \mathbb{F}$, entonces F es finito y de característica p entonces F posee p^m elementos y esto implica que $\mathbb{F}_p \leqslant F \leqslant \mathbb{F}$. Por el Teorema A.2.1 se sigue que $[\mathbb{F} : \mathbb{F}_p] = [\mathbb{F} : F][F : \mathbb{F}_p]$, es decir, $n = m[F : \mathbb{F}_p]$ de aquí es evidente que $m \mid n$. Por otro lado, si $m \mid n$, por el Corolario A.1.3 el polinomio $x^{p^m-1} - 1$ divide al polinomio $x^{p^n-1} - 1$, multiplicando por el polinomio x, se llega a que $x^{p^m} - x \mid$

$x^{p^n} - x$, no perdamos de vista que ambos polinomios pertenecen a $\mathbb{F}_p[x]$, y por lo anterior, tenemos que $x^{p^n} - x = \left[x^{p^m} - x\right] q(x)$, así toda raíz de $x^{p^m} - x$ es una raíz de $x^{p^n} - x$. Nombrando E_n y E_m a los campos de descomposición de $x^{p^n} - x$ y $x^{p^m} - x$ respectivamente, tenemos que $E_m \leqslant E_n = \mathbb{F}_q$, la igualdad se sigue del Teorema 1.8.25, así, existe un subcampo de $\mathbb{F}_q$ y como $grad\left(x^{p^m} - x\right) = p^m$, éste posee p^m elementos. Finalmente, si existieran dos subcampos K_1, K_2 de $\mathbb{F}_q$ tales que poseen p^m elementos y $K_1 \neq K_2$ entonces $| K_1 \cup K_2 | > p^m$ pero ambos poseen a todas las ráices de $x^{p^m} - x$ y es claro que su unión también, pero lo anterior nos diría que hay más de p^m raíces de $x^{p^m} - x$ en $\mathbb{F}_q$ y esto es una contradicción, por lo tanto, $K_1 = K_2$ y así el subcampo de $\mathbb{F}_q$ con p^m elementos es único. □

Ejemplo 1.8.28. Los subcampos de un campo finito forman retículas con la divisibilidad. Por ejemplo, para $\mathbb{F}_{2^{30}}$ y $\mathbb{F}_{2^{12}}$, usando los divisores de 30 y 12 se tiene, respectivamente:

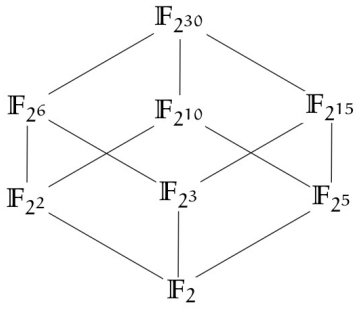

Figura 4: Diagrama de la retícula de los subcampos de $\mathbb{F}_{2^{30}}$.

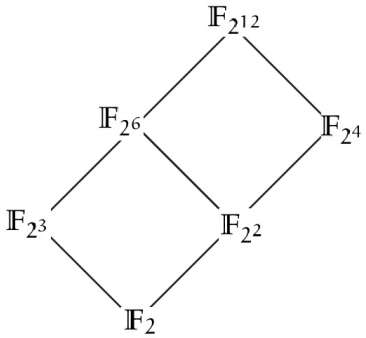

Figura 5: Diagrama de la retícula de los subcampos de $\mathbb{F}_{2^{12}}$.

Teorema 1.8.29. *Para cada campo finito $\mathbb{F}_q$, el grupo multiplicativo $\mathbb{F}_q^*$ de elementos distintos de cero es cíclico.*

Demostración. Si $q = 2$ es claro que $\mathbb{F}_2 = \{0, 1\}$ entonces $\mathbb{F}_2^* = \{1\} = \langle 1 \rangle$ que es cíclico. Ahora, supongamos que $q \geqslant 3$, por el teorema fundamental de la aritmética, sea $h = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ la descomposición en producto de potencias de numeros primos de $q - 1 = ord(\mathbb{F}_q^*)$. Sea $r_i = h/p_i$ para cada $i \in \{1, 2, \ldots, m\}$, luego el polinomio $x^{r_i} - 1$ tiene a lo más r_i raíces en $\mathbb{F}_q$ y como $r_i < h$ para cada $i \in \{1, 2, \ldots, m\}$, podemos afirmar que hay elementos de $\mathbb{F}_q^*$ que no son raíces de los polinomios $x^{r_i} - 1$. Sea $a_i \in \mathbb{F}_q^*$ tal que no es raíz de $x^{r_i} - 1$ y renombremos $a_i^{h/p_i^{e_i}}$ por b_i entonces

$$b_i^{p_i^{e_i}} = \left[a_i^{h/p_i^{e_i}}\right]^{p_i^{e_i}} = a_i^h = a_i^{q-1} = 1 \tag{1.8.2}$$

ya que $o(\mathbb{F}_q^*) = q - 1$, se sigue de (1.8.2) que $ord(b_i) \mid p_i^{e_i}$ luego, $ord(b_i) = p_i^{f_i}$ con $0 \leqslant f_i \leqslant e_i$. Si $b_i^{p_i^{e_i - 1}} = 1$, entonces

$$1 = b_i^{p_i^{e_i-1}} = \left[a_i^{h/p_i^{e_i}}\right]^{p_i^{e_i-1}} = a_i^{h/p_i} = a_i^{r_i} \tag{1.8.3}$$

lo cual implica que $a_i^{r_i} - 1 = 0$, es decir, a_i es raíz de $x^{r_i} - 1$, lo que es una contradicción. Además, si $f_i < e_i - 1$, tenemos que $1 = b_i^{p_i^{f_i}} = \left[a_i^{h/p_i^{e_i}}\right]^{p_i^{f_i}} = a_i^{h/p_i^{e_i-f_i}}$, por consiguiente, $a_i^{h/p_i^{e_i-f_i}} - 1 = 0$, aplicando el Teorema A.1.1 llegamos a, $0 = 0^{p_i^{e_i-f_i-1}} = \left(a_i^{h/p_i^{e_i-f_i}} - 1\right)^{p^{e_i-f_i-1}} = \left(a_i^{h/p_i^{e_i-f_i}}\right)^{p^{e_i-f_i-1}} - 1 = a^{h/p_i} - 1$, es decir, $a_i^{r_i} - 1 = 0$ lo cual es nuevamente una contradicción, por lo tanto, $f_i = e_i$ y así $\operatorname{ord}(b_i) = p_i^{e_i}$ para cada $i \in \{1, 2, \ldots, m\}$. Veamos que el elemento $b = b_1 b_2 \cdots b_m$ tiene orden $h = q - 1$. En efecto, note que $b \in \mathbb{F}_q^*$ y en consecuencia $b^h = 1$, por el Corolario 1.3.7, $\operatorname{ord}(b) \mid h$. Si $\operatorname{ord}(b) < h$ dado que $h = \prod_{i=1}^m p_i^{e_i}$, b debe carecer de al menos un factor $p_j^{f_j}$ con $1 \leqslant f_j < e_j$ con $j \in \{1, 2, \ldots, m\}$, luego $\operatorname{ord}(b) \mid (h/p_j)$ y podemos denotar $h/p_j = k_j \cdot \operatorname{ord}(b)$ para algún $k_j \in \mathbb{N}$. Sin pérdida de generalidad reordenamos los factores de h de tal manera que $j = 1$, entonces $b^{h/p_1} = b^{k_1 \cdot \operatorname{ord}(b)} = \left(b^{\operatorname{ord}(b)}\right)^{k_1} = 1$, luego

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1} \tag{1.8.4}$$

Note que para $2 \leqslant i \leqslant m$ se cumple que $\operatorname{ord}(b_i) = p_i^{e_i} \mid h/p_1$ pues $h/p_1 = p_1^{e_1-1} p_2^{e_2} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i} p_{i+1}^{e_{i+1}} \cdots p_m^{e_m} = \lambda p_i^{e_i}$ con $\lambda = p_1^{e_1-1} \prod_{j \neq i} p_j^{e_j}$ así, $b_i^{h/p_1} = 1$ cuando $2 \leqslant i \leqslant m$, de esto y de (1.8.4) se sigue que $b_1^{h/p_1} = 1$. Finalmente, por lo anterior tenemos que

$$p_1^{e_1} = \operatorname{ord}(b_1) \mid (h/p_1) = p_1^{e_1-1} p_2^{e_2} \cdots p_m^{e_m}$$

lo cual es imposible pues $e_1 - 1 < e_1$ y $(p_i, p_j) = 1$ cada vez que $i \neq j$, pero esto se deduce de suponer que $\operatorname{ord}(b) < h$ por lo tanto $\operatorname{ord}(b) = h = q - 1 = \operatorname{ord}(\mathbb{F}_q^*)$ y en consecuencia $\langle b \rangle = \mathbb{F}_q^*$, así éste último es cíclico. □

Definición 1.8.30. Sea $\mathbb{F}_q$ un campo finito con q elementos, cualquier elemento $\pi \in \mathbb{F}_q$ generador del grupo cíclico $\mathbb{F}_q^*$, es llamado un **elemento primitivo** de $\mathbb{F}_q$, más aún, si un polinomio $f(x) \in \mathbb{F}_q[x]$ tiene a un elemento primitivo como raíz, $f(x)$ recibe el nombre de **polinomio primitivo**.

Corolario 1.8.31. *Sea $\mathbb{F}_q$ un campo finito, entonces*

(i) *Si $\mathbb{F}_r$ es una extensión finita de $\mathbb{F}_q$ entonces es algebraica simple y todo elemento primitivo de $\mathbb{F}_r$, sirve para definir a $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

(ii) *Por cada número natural $m \in \mathbb{N}$, existe un campo finito $\mathbb{F}_q$ y un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m.*

(iii) *El polinomio mínimo de un elemento primitivo de $\mathbb{F}_q$, es un polinomio primitivo.*

Demostración. (i) Por el Teorema 1.8.17, como $\mathbb{F}_r$ es una extensión finita de $\mathbb{F}_q$, es algebraica, además por el teorema anterior $\mathbb{F}_r^*$ es un grupo cíclico luego, existe un elemento primitivo $\pi \in \mathbb{F}_r$, y en consecuencia $\mathbb{F}_q(\pi) = \bigcap\{K \leqslant \mathbb{F}_r \mid \mathbb{F}_q \subseteq K \text{ y } \pi \in K\} \subseteq \mathbb{F}_r$. Por otro lado, como $0 \in \mathbb{F}_q(\pi)$ pues es un campo, y también $\mathbb{F}_r^* \subseteq \mathbb{F}_q(\pi)$ pues tiene como elemento a su generador π, en consecuencia $\mathbb{F}_r = \{0\} \cup \mathbb{F}_r^* \subseteq \mathbb{F}_q(\pi)$, por

lo tanto, $\mathbb{F}_r = \mathbb{F}_q(\pi)$, es decir, es una extensión algebraica, simple y definida por un elemento primitivo sobre $\mathbb{F}_q$.

(ii) Sean p un número primo, $n, m \in \mathbb{N}$ y supongamos que $l = nm$, por el Teorema 1.8.26 existe un campo finito $\mathbb{F}_r$ con $r = p^l$ elementos, por el Criterio del subcampo, como $n \mid l$ entonces existe $\mathbb{F}_q$ un subcampo de $\mathbb{F}_r$ con $q = p^n$ elementos, así $r = q^m$ y $\mathbb{F}_r$ es una extensión del campo $\mathbb{F}_q$. Ahora, por (i) de éste corolario, $\mathbb{F}_r = \mathbb{F}_q(\pi)$ y es una extensión algebraica de $\mathbb{F}_q$, para algún elemento primitivo $\pi \in \mathbb{F}_r$, luego π es un elemento algebraico; entonces por el Teorema 1.8.19 existe $m(x) \in \mathbb{F}_q[x]$ el polinomio mínimo de π el cual es irreducible y $grad(m(x)) = [\mathbb{F}_r : \mathbb{F}_q] = m$.

(iii) Es claro que si π es un elemento primitivo de $\mathbb{F}_q$ dado que es raíz de su polinomio mínimo, entonces este polinomio tiene a un elemento primitivo como raíz, por la Definición 1.8.30, es un polinomio primitivo. □

Observación 1.8.32. Durante las secciones previas y la presente se han introducido de manera formal conceptos, definiciones y notación, sin embargo, en lo sucesivo podriamos omitir alguna formalidad que se desprende como consecuencia inmediata de su defínción, por ejemplo.

1. Si $\alpha \in I = \langle r \rangle$ donde I es un ideal, se sigue que $r \mid \alpha$.
2. Si ϕ es un homomorfismo y $\ker \phi \subseteq \{e\}$, podemos implicar que ϕ es un monomorfismo, la otra contención es inmediata.
3. Si $r \equiv s \pmod{I}$ para I un ideal o un subgrupo[9] y éste es generado por algún elemento $x \in S$ donde S es un anillo o un grupo (respectivamente), podemos denotar que $r \equiv s \pmod{x}$.

Concluimos esta sección con el resultado previo, invitando al lector a profundizar el estudio de los campos finitos consultando [7, Capítulo 2], [16, Capítulos 6,7 y 10].

9 Se hace la distinción pues se definió la congruencia para ambos casos.

2 LEMA DE HENSEL

En este capítulo se estudia la estructura del anillo de polinomios $\mathbb{Z}_{p^s}[x]$, sus ideales, el lema de Hensel y el levantamiento de Hensel.

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.,

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

con la suma y multiplicación usual de clases:

$$\begin{aligned} \overline{r}_1 + \overline{r}_2 &= \overline{r_1 + r_2} \\ \overline{r}_1\,\overline{r}_2 &= \overline{r_1 r_2} \end{aligned} \tag{2.1.1}$$

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

Observación 2.1.1. Por la construcción del anillo cociente $\mathbb{Z}_{p^s}$ tenemos que $\overline{n}\,\overline{m} = \overline{l}$ sí y sólo si $nm \equiv l \mod p^s$.

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

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

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:

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

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:

$$\mathbb{Z}_{p^s} = \{0, 1, \ldots, p^s - 1\}. \tag{2.1.2}$$

El siguiente lema nos será muy útil más adelante.

Lema 2.1.2. *Sean $a \in \mathbb{N}$ y p un número primo. Si $(a, p) = 1$ y $s \in \mathbb{N}$, entonces $ca \equiv 1$ (mód 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 que concluye la demostración. □

Corolario 2.1.3. *En $\mathbb{Z}_{p^s}$ se satisface:*

1. *Si $\overline{a} \in \mathbb{Z}_{p^s}$ y $(a, p) = 1$, entonces $\overline{a}$ es una unidad en $\mathbb{Z}_{p^s}$.*
2. *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 2.1.2 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 2.1.1. 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 que demuestra el resultado.
- Si $(x, p) = p$ entonces $p|x$. Además si q es un primo tal que $q|x$ entonces $q \leqslant p^s - 1$ pues $x \leqslant p^s - 1$. 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 $i = \max\left\{n_j | (x, p^{n_j}) = p^{n_j}\right\}$ como $(x, p) = p$ entonces $n_j \geqslant 1$ 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 $a = q_1^{n_1} q_2^{n_2} \dots q_{j-1}^{n_{j-1}} q_{j+1}^{n_{j+1}} \dots q_k^{n_k}$, entonces $x = ap^i$ y, por lo tanto, $\overline{x} = \overline{a}\overline{p^i}$.

□

Ejemplo 2.1.4. 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:

$$\begin{aligned} 1 \odot 1 &= 1 \\ 2 \odot 5 &= 1 \\ 4 \odot 7 &= 1 \\ 8 \odot 8 &= 1 \end{aligned} \tag{2.1.3}$$

como se afirma en el Corolario 2.1.3. Así $\mathbb{Z}_{p^s}^* = \mathcal{A}$, donde $\mathbb{Z}_{p^s}^*$ denota el grupo de unidades del anillo $\mathbb{Z}_{p^s}$.

Teorema 2.1.5. *Los ideales principales* $\langle\overline{1}\rangle, \langle\overline{p}\rangle, \dots, \langle\overline{p^{s-1}}\rangle, \langle\overline{0}\rangle$, *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 $\mathbb{Z}_{p^s}$ y supóngase que $I \neq \langle\overline{0}\rangle$. Como todos los elementos de I son clases de equivalencia con representantes en $\{0, 1, \dots, p^s - 1\}$, entonces considérese a $m = \min\{n \in \mathbb{N} \mid \overline{n} \in I\}$. 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 $q, r \in \mathbb{Z}$ tales que $i = qm + r$ con $0 \leqslant r < m$, 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 lo que $\langle\overline{m}\rangle \subseteq I$, entonces $I = \langle\overline{m}\rangle$, como queríamos. Dado que $\overline{m} \in I \subseteq \mathbb{Z}_{p^s}$, por el Corolario 2.1.3, existe $a \in \mathbb{Z}$, tal que:

$$\overline{m} = \overline{a}\overline{p^i} \text{ para algún } i \in \{0, \dots, s-1\}. \tag{2.1.4}$$

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 $\overline{ca}\overline{p^i} - \overline{p^i} = \overline{dp^s}\overline{p^i}$, de ahí que, $\overline{ca}\overline{p^i} - \overline{p^i} = \overline{dp^s}\overline{p^i}$, por lo que, $\overline{0} = \overline{c}\overline{a}\overline{p^i} - \overline{p^i} = \overline{c}\,\overline{m} - \overline{p^i}$, 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 (2.1.4), $\langle\overline{m}\rangle \subseteq \langle\overline{p^i}\rangle$, 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 $i \in \{0, 1, \dots s-1\}$. 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, $\langle\overline{p^{i+1}}\rangle \subseteq \langle\overline{p^i}\rangle$, por lo tanto,

$$\langle\overline{0}\rangle \subseteq \langle\overline{p^{s-1}}\rangle \subseteq \dots \subseteq \langle\overline{p^2}\rangle \subseteq \langle\overline{p}\rangle \subseteq \langle\overline{1}\rangle = \mathbb{Z}_{p^s} \tag{2.1.5}$$

de (2.1.5), $\langle\overline{p}\rangle$ es el único ideal maximal, así, $\frac{\mathbb{Z}_{p^s}}{\langle\overline{p}\rangle}$ es un campo finito.

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 $y \in \mathbb{Z}_{p^s}/\langle\overline{p}\rangle$ 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 $0 \leqslant r \leqslant p-1$ entonces, $y = \overline{sp+r} + \langle\overline{p}\rangle = \overline{r} + \overline{s}\,\overline{p} + \langle\overline{p}\rangle = \overline{r} + \langle\overline{p}\rangle$, es decir, $\mathbb{Z}_{p^s}/\langle\overline{p}\rangle = \{\overline{r} + \langle\overline{p}\rangle | r \in \{0, 1 \ldots, p-1\}\}$, es un campo finito con p elementos, por lo tanto, $\mathbb{Z}_{p^s}/\langle\overline{p}\rangle \simeq \mathbb{F}_p$. □

Por el Teorema 2.1.5 se sigue que $\mathbb{Z}_{p^s}$ es un anillo local y finito de cadena, con único ideal maximal $\langle\overline{p}\rangle$.

Lema 2.1.6. *Sean $b \in \mathbb{Z}$ con $b > 1$ y $a \in \mathbb{Z}$. Entonces existen $d_0, d_1 \ldots, d_{n-1}, t \in \mathbb{N}$ con $0 \leqslant d_i \leqslant b-1$ para cada $i \in \{0, 1, \ldots, n-1\}$ tales que:*

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

Por el Lema 2.1.6, 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

$$\begin{aligned} \overline{x} &= \overline{c_0 p^0 + c_1 p^1 + \cdots + c_{s-1} p^{s-1} + t p^s} \\ &= \overline{c_0}\,\overline{p^0} + \overline{c_1 p} + \cdots + \overline{c_{s-1}}\,\overline{p^{s-1}} + \overline{t p^s} \\ &= \overline{c_0}\,\overline{p^0} + \overline{c_1 p} + \cdots + \overline{c_{s-1}}\,\overline{p^{s-1}}, \end{aligned} \tag{2.1.6}$$

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

$$\mu : \mathbb{Z}_{p^s} \longrightarrow \mathbb{F}_p \tag{2.1.7}$$

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 2.1.7. *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

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

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

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

esto es, $\mu(\overline{x}\overline{y}) = \mu(\overline{x})\,\mu(\overline{y})$ 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 $\mu(\overline{x}) = \overline{0}$, 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 $\mu(\overline{x}) = 0$, 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 (2.1.5), 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, $\ker\mu = \langle\overline{p}\rangle$. □

Podemos extender el homomorfismo definido en (2.1.7) como la función:

$$-: \mathbb{Z}_{p^s}[x] \longrightarrow \mathbb{F}_p[x] \tag{2.1.8}$$

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 2.1.8. *La función $-$ es un homomorfismo de anillos.*

Demostración. Recordemos que si $c_i \in \mathbb{Z}_{p^s}$, por (2.1.6) 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 $n < i \leqslant m$. 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 $0 \leqslant l \leqslant m + n$, 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:

$$\sum_{k=0}^{l} \mu(u_k) x^k \text{ con } \mu(u_k) = \left(\mu(c_0)\mu(d_k) + \ldots + \mu(c_k)\mu(d_0)\right) = \mu(e_k),$$

de esto se sigue que $fg(x) = \sum_{k=0}^{l} \mu(e_k) x^k = \sum_{k=0}^{l} \mu(u_k) x^k = \overline{f}(x)\overline{g}(x)$, por lo tanto "$-$" es un homomorfismo. □

Definición 2.1.9. 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:

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

Lema 2.1.10. $Ker - = \ll \overline{p} \gg$.

Demostración. Sea $h(x) = \sum_{i=0}^{n} c_i x^i$. Si $h(x) \in \ker -$ entonces $\overline{h}(x) = \overline{0} \in \mathbb{F}_p$. 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 2.1.8. 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:

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

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

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

con $c_i = \overline{a_i p} \in \langle \overline{p} \rangle$ luego, aplicando "$-$" obtenemos:

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

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

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

Teorema 2.1.11. *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 $0 \leqslant l \leqslant m + n$. Supóngase, sin pérdida de generalidad, que $m > n$ y además, supóngase que $f(x)h(x) \in \ll \overline{p} \gg$ entonces

$$\overline{f(x)h(x)} = 0 \tag{2.1.9}$$

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 demostraremos 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 (2.1.6) 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 (iii) del Teorema 1.7.10, 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, $\overline{\mathbb{P}} \neq \langle 0 \rangle$, por el Corolario 1.6.15, $\overline{\mathbb{P}}$ es un ideal 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 un ideal maximal. □

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

Teorema 2.1.12. *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) Como $\mathbb{Z}_{p^s}[x]$ es un anillo conmutativo con unidad, éste resultado se sigue del Lema 1.5.18.

(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) Supóngase que $\sqrt{Q}$ es un ideal primo y además que $\ll \overline{p} \gg \subsetneq \sqrt{Q}$. Por el Teorema 2.1.11, $\sqrt{Q}$ es maximal y como $\sqrt{Q} \neq \mathbb{Z}_{p^s}[x]$, se sigue del Lema 1.5.18 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 $g(x) \notin \sqrt{Q}$. Considérese el conjunto $\langle g(x)\rangle + \sqrt{Q} := \{t(x)g(x) + q(x) | t(x) \in \mathbb{Z}_{p^s}[x] \text{ y } q(x) \in \sqrt{Q}\}$ el cual es un ideal de $\mathbb{Z}_{p^s}[x]$ pues es la suma de dos ideales de éste anillo.

Sea $q(x) \in \sqrt{Q}$, es claro que $q(x) = t(x)g(x) + q(x)$ con $t(x) = 0$ entonces $q(x) \in \langle g(x)\rangle + \sqrt{Q}$, así, $\sqrt{Q} \subseteq \langle g(x)\rangle + \sqrt{Q}$, 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 $\sqrt{Q}$. Así, $\langle g(x)\rangle + \sqrt{Q} \neq \sqrt{Q}$ y como $\sqrt{Q}$ es maximal, entonces $\langle g(x)\rangle + \sqrt{Q} = \mathbb{Z}_{p^s}[x]$. Por lo anterior, $1 \in \langle g(x)\rangle + \sqrt{Q}$, 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 2.1.13. Sea $f(x) \in \mathbb{Z}_{p^s}$. Diremos que $h(x)$ es un polinomio **primario** si y sólo si $\langle f(x)\rangle$ es un ideal primario de $\mathbb{Z}_{p^s}$.

Lema 2.1.14. *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 2.1.12, 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 $\overline{1} = \overline{h}(x)\overline{f}(x) = \overline{h}(x)\,(g(x))^m = g(x)\left(\overline{h}(x)\,(g(x))^{m-1}\right)$ 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 $(a(x)b(x))^n \in \langle f(x)\rangle$, es decir, existe $q(x) \in \mathbb{Z}_{p^s}$ tal que $(a(x)b(x))^n = (a(x))^n\,(b(x))^n = q(x)f(x)$. Aplicando el epimorfismo (2.1.8) tenemos que $\overline{(a(x))^n\,(b(x))^n} = \overline{q(x)f(x)}$, es decir,

$$\overline{a}(x)^n\overline{b}(x)^n = \overline{q}(x)\overline{f}(x) = \overline{q}(x)\,(g(x))^m$$

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 $(g(x))^m = \overline{f}(x)$ divide a $(\overline{a}(x))^m$, es decir, existe $\overline{c}(x) \in \mathbb{F}_p[x]$ tal que $(\overline{a}(x))^m = \overline{c}(x)\overline{f}(x)$, entonces $\overline{(\overline{a}(x))^m - c(x)f(x)} = \overline{0}$ y como (2.1.8) es epimorfismo tenemos que $\overline{(a(x))^m - c(x)f(x)} = \overline{0}$, de ahí que, $(a(x))^m - c(x)f(x) \in Ker - = \ll \overline{p} \gg$. Entonces existe $d(x) \in \mathbb{Z}_{p^s}[x]$ tal que $(a(x))^m - c(x)f(x) = d(x)\overline{p}$, por lo tanto, $(a(x))^m = c(x)f(x) + d(x)\overline{p}$. Como $p^s \geqslant 2$, elevando la igualdad anterior a p^s obtenemos que $((a(x))^m)^{p^s} = (c(x)f(x) + d(x)\overline{p})^{p^s}$ y, aplicando el Teorema del Binomio tenemos:

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

es decir, $(a(x))^{mp^s} = k(x)f(x) + (d(x))^{p^s}\,(\overline{p})^{p^s}$ pero $s < p^s$ entonces existe $t \in \mathbb{N}$ tal que $p^s = s + t$, luego $(a(x))^{mp^s} = k(x)f(x) + \overline{p}^s\overline{p}^t = k(x)f(x)$ 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 (iii) del Teorema 2.1.12, $\langle f(x)\rangle$ es un ideal primario y, por la Definición 2.1.13, $f(x)$ es un polinomio primario. □

EL LEMA DE HENSEL

En esta sección analizaremos un resultado de suma importancia, además de introducir una demostración muy explicítica, para este propósito, recordaremos la Definición 1.6.19, pero aplicada al anillo de los polinomios $\mathbb{Z}_{p^s}[x]$.

Definición 2.2.1. 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 Definición 2.2.1, $\mathbb{Z}_{p^s}[x]$ puede ser reemplazado por cualquier dominio de ideales principales, por ejemplo, $\mathbb{F}_p[x]$.

Lema 2.2.2. *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 2.2.1 existen $\lambda_1, \lambda_2 \in \mathbb{Z}_{p^s}[x]$ tales que $\lambda_1 f_1 + \lambda_2 f_2 = 1$ y, aplicando (2.1.8) 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 2.2.1, 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 2.2.1, 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 (2.1.8) 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 2.2.3. *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*

1. $f = f_1 f_2 \in \mathbb{Z}_{p^s}[x]$,
2. $\overline{f}_i = g_i$ *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 (2.1.8) 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 2.1.10 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 2.2.2 que h_1 y h_2 son coprimos en $\mathbb{Z}_{p^s}[x]$ luego, por la Definición 2.2.1, existen $\lambda_1\lambda_2 \in \mathbb{Z}_{p^s}[x]$ tales que $\lambda_1 h_1 + \lambda_2 h_2 = 1$. Denotando por ν a $k\overline{p}$ tenemos:

$$f = h_1 h_2 + \nu. \tag{2.2.1}$$

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

$$\begin{aligned} h_{11} &= h_1 + \lambda_2 \nu \\ h_{21} &= h_2 + \lambda_1 \nu \end{aligned}$$

Como $\nu \in \ll \overline{p} \gg$ entonces $\overline{\nu} = \overline{0}$; aplicando (2.1.8) 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:

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

puesto que $\lambda_1 h_1 + \lambda_2 h_2 = 1$ y, usando (2.2.1) en la última igualdad se obtiene que $h_{11}h_{21} = f + \lambda_1\lambda_2\nu^2$, de ahí que, $f - h_{11}h_{21} = -\lambda_1\lambda_2\nu^2$, de manera que:

$$f \equiv h_{11}h_{21} \pmod{\nu^2}.^{1} \tag{2.2.2}$$

Como $(g_1, g_2) = 1$, $\overline{h_{11}} = g_1$ y $\overline{h_{21}} = g_2$, se sigue del Lema 2.2.2 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 (2.2.2) tenemos que $f = h_{11}h_{21} + k_1\nu^2$ para algún $k_1 \in \mathbb{Z}_{p^s}[x]$, entonces repitiendo el proceso t veces definiendo en cada paso a los polinomios:

$$\begin{aligned} h_{1t} &= h_{1t-1} + \lambda_{2t-1}k_{t-1}\nu^{2(t-1)} \\ h_{2t} &= h_{2t-1} + \lambda_{1t-1}k_{t-1}\nu^{2(t-1)} \end{aligned}$$

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 $f = h_{1t-1}h_{2t-1} + k_{t-1}\nu^{2(t-1)}$. Es fácil ver que para $t = s$ al multiplicar los polinomios definidos arriba se tiene:

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

Observe que $\nu^{2s} = (k\overline{p})^{2s} = k^{2s}\overline{p}^s\overline{p}^s = \overline{0}$, 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: $f = f_1 f_2$, $\overline{f_1} = g_1$, $\overline{f_2} = g_2$ 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 2.2.3.

Lema 2.2.4. *Sea* R *un anillo euclidiano y sean* $p_1, p_2, \ldots, p_r \in R$ *coprimos por pares. Entonces, si* $r \geqslant 3$ *se tiene que* $\left(\prod_{i=1}^{r-1} p_i, p_r\right) = 1$.

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

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 2.2.1, 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 2.2.1 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 que queríamos demostrar. □

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

Lema 2.2.5 (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 2.2.3. 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 $\overline{f} = g_1 g_2 \cdots g_r$, donde $g_1, g_2, \ldots, g_r$ son polinomios mónicos y coprimos por pares sobre $\mathbb{F}_p$. Denotemos por $h = g_1 g_2 \cdots g_{r-1}$, es claro que, $h \in \mathbb{F}_p[x]$ y $\overline{f} = h g_r$. Por el Lema 2.2.4, tenemos que $(h, g_r) = 1$ además, por el Lema 2.2.3, 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 $\widehat{h} = f_1 f_2 \cdots f_{r-1}$ y $\overline{f}_i = g_i$ con $i \in (1, 2, \ldots, r-1)$, de ahí que, $f = f_1 f_2 \cdots f_{r-1} f_r \in \mathbb{Z}_{p^s}[x]$ 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 ([11]) para revisar el Lema de Hensel en su versión general sobre anillos conmutativos finitos locales y los artículos [2] y [12] para ver un par de aplicaciones del Lema de Hensel sobre la clase de anillos conmutativos finitos de cadena.

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

1. *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 $\mathbb{F}_p[x]$.

2. *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

$$\overline{f} = g_1^{e_1} g_2^{e_2} \cdots g_r^{e_r}, \tag{2.3.1}$$

para algunos $e_1, e_2, \ldots, e_r \in \mathbb{N}$, por el Lema 2.2.4 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 2.1.14 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:

$$f_1 f_2 \cdots f_r = h_1 h_2 \cdots h_t \tag{2.3.2}$$

son dos factorizaciones de f como producto de polinomios primarios, mónicos coprimos por pares en $\mathbb{Z}_{p^s}[x]$. Se sigue de (2.3.2) 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 $1 \leqslant k_i \leqslant r$ 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 suma 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 $h_{l_j}^{m_j} = c f_j$. Si $j = k_i$ entonces $h_{l_{k_i}}^{m_{k_i}} = c f_{k_i}$ 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 (2.1.8) 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 $\left(h_{j_0}, h_{i_0}\right) = h_{j_0} \neq 1$ en contradicción con el Lema 2.2.2. 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 $r \leqslant t$ y también $t \leqslant r$ así, $r = t$ y re-enumerando $k_i = i$ 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 $\left(f_1, f_j\right) = 1$ 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 2.2.4 $\left(f_2 f_3 \cdots f_r, f_1^{n_1}\right) = 1$. Como $f_1^{n_1} \in \langle h_1 \rangle$ existe algún $c \in \mathbb{Z}_{p^s}[x]$ tal que $f_1^{n_1} = c h_1$. Veamos que el producto $f_2 f_3 \cdots f_r$ y h_1 son coprimos. Dado que $\left(f_2, f_3 \cdots f_r, f_1^{n_1}\right) = 1$ existen $\alpha, \beta \in \mathbb{Z}_{p^s}[x]$ tales que $1 = \alpha f_2 f_3 \cdots f_r + \beta f_1^{n_1} = \alpha f_2 f_3 \cdots f_r + \beta(c h_1)$, sea $\gamma = c\beta$ entonces

$$\alpha f_2 f_3 \cdots f_r + \gamma h_1 = 1, \tag{2.3.3}$$

de ahí que, $(f_2 f_3 \cdots f_r, h_1) = 1$. Multiplicando (2.3.3) 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 (2.3.2), 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 2.3.2. Sea $f(x)$ un polinomio mónico de grado $m \geqslant 1$ 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 2.3.3. *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 $\mathrm{grad}\,(h) = m$, 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 $iv)$ del Teorema 1.8.6 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 2.3.4. *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. Si f tuviera un factor múltiple, dígamos g con $\mathrm{grad}(g) \geqslant 1$, 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 2.3.5. *Sean $\mathbb{F}$ un campo con característica p, i.e., $\mathrm{Car}\,(\mathbb{F}) = p$ 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 el Teorema 1.8.13, 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 2.3.6. *Para cualquier entero $m \geqslant 1$ 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. Por el Corolario 1.8.31 para $m \geqslant 1$ 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 2.3.3, $f_1(x)$ 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 $\mathrm{Car}\,(\mathbb{F}) = p$ 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 2.2.1 y el Lema 2.3.4, $x^{p^m-1}-1$ no tiene factores múltiples. Supongamos que $(f_1(x), g_1(x)) = d(x)$ y $grad(d) \geqslant 1$ 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 $x^{p^m-1}-1 = f_1(x)g_1(x) = k_1(x)k_2(x)\left(d(x)\right)^2$, 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 2.3.2 $f(x)$ 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 2.3.7. 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 2.3.6, 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 2.3.7.

Teorema 2.3.8. *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

$$x^n-1 = \overline{x^n-1} = \overline{f}(x)\overline{h}(x) = g(x)\overline{h}(x). \tag{2.3.4}$$

Como $p \nmid n$, x^n-1 no tiene raíces múltiples en $\mathbb{F}_p[x]$, por el Lema 2.3.5, y de (2.3.4) se sigue que $g(x)$ no tiene raíces múltiples pues de tenerlas entonces serían también raíces de x^n-1, lo cual no puede ocurrir. Más aún, si $x|g(x)$ tenemos que $x|x^n-1$, por (2.3.4), 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 el Lema A.2.6 existe $n \in \mathbb{N}$ tal que $g(x) | x^n-1$ con $n \leqslant p^{grad(g)-1}$. 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 $n = mp^e$. Por el Teorema A.1.1, para $a, b \in \mathbb{F}_p$

$$(a+b)^{p^e} = a^{p^e} + b^{p^e}$$

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 $\mathrm{grad}(g)+\mathrm{grad}(h) = n = mp^e \geqslant 1$. Si $\mathrm{grad}(g) = 1$ 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 $\mathrm{grad}(g) = l > 1$ 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

$$x^m-1 = f(x)f_0(x) \tag{2.3.5}$$

en $\mathbb{Z}_{p^s}[x]$ con $\overline{f}(x) = g(x)$ y $\overline{f_0}(x) = g_0(x)$. Por (2.3.5) 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 2.3.9. *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 $0 \leqslant r < m$. Es facíl 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 $\mathrm{grad}(x^r-1) < \mathrm{grad}(x^m-1)$, por consiguiente, $x^n-1 \equiv x^r-1 \pmod{x^m-1}$. 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 2.3.10. *Sean $s \in \mathbb{N}$ 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 2.3.8, $g(x)$ tiene un levantemiento de Hensel en $\mathbb{Z}_{p^s}[x]$, así que sólo demostraremos 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

$$x^n - 1 = g_1(x)g_2(x)\cdots g_r(x) \tag{2.3.6}$$

en $\mathbb{F}_p[x]$ con $\left(g_i, g_j\right) = 1$ 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, $\left(f_i(x), f_j(x)\right) = 1$ 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 2.1.14, f_i es un polinomio primario sobre $\mathbb{Z}_{p^s}[x]$ para cada i. Como $g(x)|x^n - 1$, $\left(g_i(x), g_j(x)\right) = 1$ si $i \neq j$ y por (2.3.6) tenemos que $g(x) = g_1(x)g_2(x)\cdots g_t(x)$ para algún $1 \leqslant t \leqslant r$, salvo el orden de $g_1(x), g_2(x), \ldots, g_r(x)$ en (2.3.6). 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 2.3.1, 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 $n = k_1n_1$ y $n = k_2n_2$. 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 $n_2|t$ 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 2.3.9, y por el primer caso, debemos concluir que $f^{(1)}(x) = f^{(2)}(x)$. Esto demuestra 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 2.3.11. 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

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

2 El mínimo común múltiplo de n_1 y n_2

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 que

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

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 2.3.12. 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 2.3.13. 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 [12, Definición 3.4] para ver una aplicación del Levantamiento de Hensel sobre la clase de anillos conmutativos finitos de cadena.

3 ANILLOS DE GALOIS

En este capítulo, con la ayuda del material del capítulo que le precede se estudia el tema principal de este trabajo, los anillos de Galois, su estructura, la representación p-ádica de sus elementos, su grupo de unidades, sus extensiones, el automorfismo generalizado de Frobenius, su traza y norma generalizadas.

EJEMPLOS DE ANILLOS DE GALOIS

Definición 3.1.1. Un anillo de Galois R es un anillo conmutativo con unidad 1_R, en el cual el conjunto de sus divisores de cero con el cero añadido forman un ideal principal. En el caso que dicho ideal no es el ideal trivial $\{0\}$, éste es generado por el elemento $p1_R$, para algún número primo p.

Cuando el ideal que se menciona en la definición Definición 3.1.1 es no trivial, se denota mediante $\langle p1_R\rangle$ o $\langle p1\rangle$ cuando el contexto sea claro.

Como se estudió en el capítulo anterior, $\mathbb{Z}_{p^s}$ es un anillo finito conmutativo con unidad, el cual identificamos con el conjunto finito $\{0, 1, \ldots, p^s - 1\}$ y posee elemento unidad $\overline{1}$ y como se ha hecho antes, definimos $1(\overline{1}) = \overline{1}$ y para todo $n \in \mathbb{N}$, $(n+1)\overline{1} = n\overline{1} + \overline{1}$.

Lema 3.1.2. *El ideal principal $\langle\overline{p}\rangle$ de $\mathbb{Z}_{p^s}$, está formado por los divisores de cero de $\mathbb{Z}_{p^s}$ añadiéndole cero.*

Demostración. Sea $\overline{a} \in \langle\overline{p}\rangle$, entonces, existe $\overline{b} \in \mathbb{Z}_{p^s}$ tal que $\overline{a} = \overline{p}\overline{b}$. Multiplicando esta igualdad por $\overline{p^{s-1}}$, tenemos que $\overline{p^{s-1}}\overline{a} = \overline{p^{s-1}}\overline{p}\overline{b} = \overline{p^s}\overline{b} = \overline{0}$ y es claro que $\overline{p^{s-1}} \neq \overline{0}$, entonces, $\overline{a} = \overline{0}$, o bien, $\overline{a}$ es un divisor de cero. Supóngase que $\overline{a}$ es un divisor de cero. Entonces existe $\overline{b} \in \mathbb{Z}_{p^s} - \{0\}$, tal que, $\overline{a}\,\overline{b} = \overline{0}$, luego, $ab \equiv 0 \pmod{p^s}$, es decir, $p^s \mid ab$ y dado que $p \mid p^s$ entonces se sigue que $p \mid a$ o bien $p \mid b$. Si $p \mid a$ hemos terminado. Por otro lado, si $p \mid b$, existen $c, e \in \mathbb{N}$ tales que $b = cp^e$ y $(c, p) = 1$.

Si $e \geqslant s$ entonces $p^s \mid p^e$, entonces $b = p^s p^{e-s} c$, y en consecuencia, $\overline{b} = \overline{0}$, lo que es una contradicción, así, $e < s$ y luego $s = e + f$ para algún $f \in \mathbb{N}$. Entonces, dado que $p^s \mid ab$ se tiene que $ab = p^s k$ para $k \in \mathbb{Z}$, además, $b = cp^e$, por consiguiente, $ac(p^e) = p^{e+f}k$ y como $\mathbb{Z}$ es un dominio entero, tenemos que $ac = p^f k$, pero $(c, p) = 1$ y $p \mid ac$, por lo tanto, $p \mid a$ y luego, $\overline{a} \in \langle\overline{p}\rangle$. □

Con esto, hemos demostrado que $\mathbb{Z}_{p^s}$ satisface la Definición 3.1.1, por lo tanto, es un anillo de Galois. Por otro lado, $\mathbb{F}_p$ es un campo finito y dado que $\mathcal{D} = \emptyset$, entonces el conjunto de sus divisores de cero con el cero añadido forman el ideal $\langle 0\rangle$, es decir, $\mathbb{F}_p$ es un anillo de Galois, de hecho, es el campo de Galois con p elementos. Los anillos de Galois, reciben este nombre, ya que como veremos, comparten propiedades con los

campos de Galois (campos finitos), por consiguiente, todo campo de Galois $GF(q)$ es un anillo de Galois.

Considérese $h(x)$ un polinomio mónico básico irreducible de grado m como en la Definición 2.3.2, entonces el anillo de clases residuales,

$$\mathbb{Z}_{p^s}/\langle h(x)\rangle := \left\{ \left[a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}\right] + \langle h(x)\rangle : a_i \in \mathbb{Z}_{p^s} \text{ y } m = grad(h(x))\right\} \quad (3.1.1)$$

Dado $f(x) \in \mathbb{Z}_{p^s}$, por el algoritmo de la división, existen $g(x), r(x) \in \mathbb{Z}_{p^s}$, tales que $f(x) = g(x)h(x) + r(x)$, con $0 \leqslant grad(r) < grad(h) = m$, entonces $f(x) \equiv r(x)$ (mód $h(x)$) de ahí que el elemento $f(x) + \langle h(x)\rangle$ en el anillo (3.1.1), puede representarse mediante $r(x) + \langle h(x)\rangle$. Por el principio multiplicativo, es claro que $|\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle| = p^{sm}$, el elemento identidad es $1 + \langle h(x)\rangle$ y el neutro aditivo es $\langle h(x)\rangle$. En resumen, $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ es un anillo finito conmutativo con unidad. Dado un número primo p tenemos,

$$\begin{aligned} p\left[1 + \langle h(x)\rangle\right] &= \underbrace{1 + \langle h(x)\rangle + 1 + \langle h(x)\rangle + \cdots + 1 + \langle h(x)\rangle}_{p-veces} \\ &= \underbrace{1 + 1 + \cdots + 1}_{p-veces} + \langle h(x)\rangle = p1 + \langle h(x)\rangle = p + \langle h(x)\rangle \end{aligned}$$

es decir, $\langle p\left[1 + \langle h(x)\rangle\right]\rangle$ se identifica con $\langle p + \langle h(x)\rangle\rangle$.

Lema 3.1.3. *Los divisores de cero con el cero añadido de $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ forman el ideal principal $\langle p + \langle h(x)\rangle\rangle$.*

Demostración. Sea $f(x) + \langle h(x)\rangle \in \langle p + \langle h(x)\rangle\rangle$ entonces existe $g(x) + \langle h(x)\rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ tal que $f(x) + \langle h(x)\rangle = [g(x) + \langle h(x)\rangle]\,[p + \langle h(x)\rangle]$ y considere el elemento $(p^{s-1}) + \langle h(x)\rangle \neq \langle h(x)\rangle$ en $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ entonces

$$[f(x) + \langle h(x)\rangle]\left[p^{s-1} + \langle h(x)\rangle\right] = [g(x) + \langle h(x)\rangle]\,[p + \langle h(x)\rangle]\left[p^{s-1} + \langle h(x)\rangle\right],$$

es claro que $p^{s-1}f(x) + \langle h(x)\rangle = p^s g(x) + \langle h(x)\rangle = \langle h(x)\rangle$, por lo tanto, $f(x) + \langle h(x)\rangle$ es cero o un divisor de cero. Para mostrar que todo divisor de cero pertenece al ideal en cuestión la demostración resulta un poco más elaborada. Para esto, considérese $f(x) + \langle h(x)\rangle$ un divisor de cero en $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ y recordemos que para los epimorfismos (2.1.7) y (2.1.8) se cumple que $\ker(\mu) = \langle \overline{p}\rangle$ y $\ker(-) = \ll \overline{p} \gg$. Demostraremos la siguiente igualdad entre conjuntos[1]: $\overline{\langle h(x)\rangle} = \langle \overline{h}(x)\rangle$. Dado $\overline{f}(x) \in \overline{\langle h(x)\rangle}$ existen $a(x) \in \langle h(x)\rangle$, $b(x) \in \mathbb{Z}_{p^s}[x]$ tales que $\overline{a}(x) = \overline{f}(x)$ y $a(x) = b(x)h(x)$ de ahí que $\overline{f}(x) = \overline{b}(x)\overline{h}(x)$ y por lo tanto $\overline{f}(x) \in \langle \overline{h}(x)\rangle$, es decir, $\overline{\langle h(x)\rangle} \subseteq \langle \overline{h}(x)\rangle$. Como $h(x) \in \langle h(x)\rangle$ entonces $\overline{h}(x) \in \overline{\langle h(x)\rangle}$ y se sigue trivialmente que $\langle \overline{h}(x)\rangle \subseteq \overline{\langle h(x)\rangle}$ y por lo tanto la igualdad. Denotemos al anillo de clases residuales formado por el cociente de $\mathbb{F}_p[x]$ y $\langle \overline{h}(x)\rangle$ mediante $\mathcal{F}(p, m)$ y definimos la función $\phi : \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle \longrightarrow \mathcal{F}(p, m)$ donde cada $f(x) + \langle h(x)\rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ lo relaciona con el elemento $\overline{f}(x) + \langle \overline{h}(x)\rangle$ en $\mathcal{F}(p, m)$. Del hecho de que (2.1.8) es un homomorfismo, se sigue que ϕ lo es, demostremos ahora que $\ker(\phi) = \langle p + \langle h(x)\rangle\rangle$. Sea $f(x) + \langle h(x)\rangle \in \ker(\phi)$ entonces $\phi\left(f(x) + \langle h(x)\rangle\right) = \langle \overline{h}(x)\rangle$, es decir, $\overline{f}(x) + \langle \overline{h}(x)\rangle = \langle \overline{h}(x)\rangle$, así, se concluye que

1 La barra que aparece sobre el ideal indica la imagen directa de sus elementos bajo el epimorfismo $-$.

$\overline{f}(x) \in \langle \overline{h}(x) \rangle$, luego existe $l(x) \in \mathbb{F}_p[x]$ tal que $\overline{f}(x) = l(x)\overline{h}(x)$, como (2.1.8) es un epimorfismo entonces existe $m(x) \in \mathbb{Z}_{p^s}[x]$ de tal manera que $\overline{m}(x) = l(x)$, así, $\overline{f}(x) - l(x)\overline{h}(x) = \overline{f(x) - m(x)h(x)} = 0$, entonces, $f(x) - m(x)h(x) \in \ker(-) = \ll \overline{p} \gg$ de modo que existe $v(x) \in \mathbb{Z}_{p^s}[x]$ tal que $f(x) - m(x)l(x) = pv(x)$, así, pasando a elementos de $\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$ tenemos que $f(x) + \langle h(x) \rangle = pv(x) + \langle h(x) \rangle$ por lo tanto $f(x) + \langle h(x) \rangle \in \langle p + \langle h(x) \rangle \rangle$. Tomando $f(x) + \langle h(x) \rangle \in \langle p + \langle h(x) \rangle \rangle$ se tiene que existe $g(x) + \langle h(x) \rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$ tal que $f(x) + \langle h(x) \rangle = [p + \langle h(x) \rangle][g(x) + \langle h(x) \rangle] = pg(x) + \langle h(x) \rangle$. Entonces $\phi(f(x) + \langle h(x) \rangle) = \phi(pg(x) + \langle h(x) \rangle)$, así,

$$\begin{aligned} \phi(pg(x) + \langle h(x) \rangle) &= \overline{pg(x)} + \langle \overline{h}(x) \rangle \\ &= \mu(p)\,\overline{g}(x) + \langle \overline{h}(x) \rangle \\ &= \langle \overline{h}(x) \rangle \end{aligned}$$

de esto se concluye que: $f(x) + \langle h(x) \rangle \in \ker(\phi)$, como se quería demostrar. Por el Teorema 1.7.9,

$$\frac{\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle}{\langle p + \langle h(x) \rangle \rangle} = \frac{\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle}{\langle p + \langle h(x) \rangle \rangle} \simeq \mathcal{F}(p, m) = \frac{\mathbb{F}_p[x]}{\langle \overline{h}(x) \rangle}. \tag{3.1.2}$$

Como $h(x)$ es mónico básico irreducible, entonces $\overline{h}(x)$ es un polinomio mónico e irreducible en $\mathbb{F}_p[x]$, el ideal $\langle \overline{h}(x) \rangle$ es maximal y en consecuencia $\mathcal{F}(p, m)$ es un campo finito con p^m elementos y $\langle p + \langle h(x) \rangle \rangle$ es también un ideal maximal pero en $\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$. Sabemos por el Lema 1.5.15 que si R es un anillo finito conmutativo con unidad, los elementos son unidades, divisores de cero o bien cero, así que veamos que todo elemento que no pertenece al ideal $\langle p + \langle h(x) \rangle \rangle$ es una unidad. En efecto, considérese $a(x) + \langle h(x) \rangle \notin \langle p + \langle h(x) \rangle \rangle$ fijo y el conjunto $J(a(x)) = \langle a(x) \rangle + \langle p + \langle h(x) \rangle \rangle$, el cual es un ideal por el Lema 1.5.15. Si elegimos $g(x) + \langle h(x) \rangle = 0 + \langle h(x) \rangle$ entonces para todo $r(x) + \langle h(x) \rangle \in \langle p + \langle h(x) \rangle \rangle$ el elemento $a(x) \cdot 0 + r(x) + \langle h(x) \rangle = r(x) + \langle h(x) \rangle$ pertenece al ideal $J(a(x))$ entonces $\langle p + \langle h(x) \rangle \rangle \subseteq J(a(x))$, más aún, como $a(x) + \langle h(x) \rangle$ pertenece a $J(a(x))$ pero no a $\langle p + \langle h(x) \rangle \rangle$ entonces la contención entre estos es propia y del hecho de que $\langle p + \langle h(x) \rangle \rangle$ es un ideal maximal, se concluye que $J(a(x)) = \mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$. Luego, $1 + \langle h(x) \rangle \in J(a(x))$ entonces existen $b(x) + \langle h(x) \rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$ y $r(x) + \langle h(x) \rangle = pc(x) + \langle h(x) \rangle \in \langle p + \langle h(x) \rangle$ tales que $1 + \langle h(x) \rangle = a(x)b(x) + pc(x) + \langle h(x) \rangle$, aplicando el Lema A.1.4.

$$\begin{aligned} (a(x)b(x) + pc(x) + \langle h(x) \rangle)^p &= (a(x)g(x))^p + p^2 c_1(x) + \langle h(x) \rangle \\ (a(x)b(x) + pc(x) + \langle h(x) \rangle)^{p^2} &= (a(x)g(x))^{p^2} + p^3 c_2(x) + \langle h(x) \rangle \\ &\vdots \\ (a(x)b(x) + pc(x) + \langle h(x) \rangle)^{p^{s-1}} &= (a(x)g(x))^{p^{s-1}} + p^s c_{s-1}(x) + \langle h(x) \rangle \\ &= [a(x) + \langle h(x) \rangle] \left[(a(x))^{p^{s-2}} (b(x))^{p^{s-1}} + \langle h(x) \rangle \right] \end{aligned}$$

En cada paso, $c_i(x) + \langle h(x) \rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$ y como $1 + \langle h(x) \rangle = [1 + \langle h(x) \rangle]^{p^{s-1}}$, tenemos que $1 + \langle h(x) \rangle = [a(x) + \langle h(x) \rangle] \left[(a(x))^{p^{s-2}} (b(x))^{p^{s-1}} + \langle h(x) \rangle \right]$, por lo tanto, $a(x) + \langle h(x) \rangle$ es una unidad. Así, $\langle h(x) \rangle$ está formado por los divisores de cero de $\mathbb{Z}_{p^s}[x]/\langle h(x) \rangle$, incluyendo al cero. □

Se sigue del Lema 3.1.3 y la Definición 3.1.1 que, $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ es un anillo de Galois, más aún, el conjunto $\mathcal{R}_{p^s} := \{a + \langle h(x)\rangle : a \in \mathbb{Z}_{p^s}\}$ es un subanillo de $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ y, si definimos la función $\tau : \mathbb{Z}_{p^s} \to \mathcal{R}_{p^s}$ la cual envía a cada elemento $a \in \mathbb{Z}_{p^s}$ a la clase $a + \langle h(x)\rangle \in \mathcal{R}_{p^s}$. No resulta difícil demostrar que τ es un epimorfismo con las operaciones respectivas en cada anillo, así, que demostraremos la inyectividad de éste. Sean $a, b \in \mathbb{Z}_{p^s}$ con $\tau(a) = \tau(b)$ entonces $\tau(a) - \tau(b) = \langle h(x)\rangle$, luego $(a-b) + \langle h(x)\rangle = \langle h(x)\rangle$, es decir, $a - b \in \langle h(x)\rangle$ así, existe $g(x) \in \mathbb{Z}_{p^s}$ tal que $a - b = g(x)h(x)$ pero $grad(a-b) = 0$ lo que ocurre si y sólo si $g(x) = 0$ de ahí que $a = b$ y se tiene la inyectividad de τ y entonces τ es un isomorfismo, por lo tanto, $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ posee un subanillo $(\mathcal{R}_{p^s})$ isomorfo a $\mathbb{Z}_{p^s}$.

Usaremos la notación $\overset{\tau}{=}$ para denotar la igualdad entre dos expresiones cuando en alguna de éstas, se sustituyan elementos de $\mathcal{R}_{p^s}$ por los de $\mathbb{Z}_{p^s}$ y viceversa. Si denotamos por ξ a la expresión $x + \langle h(x)\rangle$ al evaluarla en el polinomio $h(x)$ tenemos que

$$\begin{aligned} h(\xi) &= a_0 + a_1\xi + \cdots + a_m\xi^m \\ &= a_0 + a_1(x + \langle h(x)\rangle) + \cdots + a_m(x + \langle h(x)\rangle)^m \\ &\overset{\tau}{=} a_0 + \langle h(x)\rangle + a_1x + \langle h(x)\rangle + \cdots + a_mx^m + \langle h(x)\rangle \\ &\overset{\tau}{=} (a_0 + a_1x + \cdots + a_mx^m) + \langle h(x)\rangle \\ &= h(x) + \langle h(x)\rangle = \langle h(x)\rangle \end{aligned}$$

en otras palabras $h(\xi) = 0$, luego $\xi \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ es una raíz para el polinomio mónico básico irreducible $h(x)$.

Corolario 3.1.4. *Sea* $f(x) \in \mathbb{Z}_{p^s}[x]$ *tal que* $f(x) \equiv r(x) \pmod{h(x)}$, $\xi = x + \langle h(x)\rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$, *entonces*

1. $r(\xi) \overset{\tau}{=} f(x) + \langle h(x)\rangle$,
2. $r(\xi) \neq \langle h(x)\rangle$,
3. *La representación* $r(\xi)$ *es única.*

Demostración. Por hipótesis $f(x) + \langle h(x)\rangle = r(x) + \langle h(x)\rangle$, con $0 \leqslant grad(r) \leqslant m-1$ sea pues $r(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$, así,

$$\begin{aligned} r(\xi) &= a_0 + a_1(x + \langle h(x)\rangle) + \cdots + a_{m-1}(x + \langle h(x)\rangle)^{m-1} \\ &\overset{\tau}{=} (a_0 + \langle h(x)\rangle) + (a_1x + \langle h(x)\rangle) + \cdots + (a_{m-1}x^{m-1} + \langle h(x)\rangle) \\ &\overset{\tau}{=} \left(a_0 + a_1x + \cdots + a_{m-1}x^{m-1}\right) + \langle h(x)\rangle \\ &= r(x) + \langle h(x)\rangle = f(x) + \langle h(x)\rangle. \end{aligned}$$

Supongamos que $r(\xi) = \langle h(x)\rangle$, entonces $r(x) + \langle h(x)\rangle = \langle h(x)\rangle$, así, $r(x) \in \langle h(x)\rangle$, por consiguiente, $r(x) = g(x)h(x)$ para algún $g(x) \in \mathbb{Z}_{p^s}$, pero esto implica que $m - 1 = grad(r) \geqslant grad(h) = m$, lo que es absurdo. Finalmente, sean $a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}$ y $b_0 + b_1\xi + \cdots + b_{m-1}\xi^{m-1}$ dos representaciones de $r(\xi)$. Considere el polinomio $\lambda(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{m-1} - b_{m-1})x^{m-1} \in \mathbb{Z}_{p^s}[x]$, luego, $\lambda(\xi) = r(\xi) - r(\xi) = \langle h(x)\rangle$ y como $grad(\lambda) < grad(h)$, es claro que, $\lambda(x) = 0$, en consecuencia $a_i = b_i$, para toda $i \in \{0, 1, \ldots, m-1\}$, así, las representaciones son iguales, como queríamos demostrar. □

Del Corolario 3.1.4 se sigue que cada elemento de $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ tiene una única representación en términos de ξ, a ésta se le llama **Respresentación Aditiva de los elementos de un anillo de Galois**, con esta, podemos dar la siguiente:

Definición 3.1.5. Sea $h(x)$ un polinomio mónico básico irreducible de grado $m \in \mathbb{N} \cup \{0\}$. Definimos el conjunto:

$$\mathbb{Z}_{p^s}[\xi] := \left\{ a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} : a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_{p^s}, m = grad(h) \right\}$$

Nótese que el conjunto $\mathbb{Z}_{p^s}[\xi]$ es un anillo con las operaciones siguientes. Dados $a(\xi) = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}$ y $b(\xi) = b_0 + b_1\xi + \cdots + b_{m-1}\xi^{m-1}$, definimos la suma como $a(\xi) + b(\xi) = (a_0 + b_0) + (a_1 + b_1)\xi + \cdots + (a_{m-1} + b_{m-1})\xi^{m-1}$ y, cada vez que, $a(x)b(x) \equiv c(x) \pmod{h(x)}$, para algún $c(x) \in \mathbb{Z}_{p^s}[x]$, entonces definimos el producto $a(\xi)b(\xi) = c(\xi)$, más aún, la función $\hat{\tau} : \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle \to \mathbb{Z}_{p^s}[\xi]$ la cual relaciona a cada elemento $f(x) + \langle h(x)\rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ con $f(\xi) \in \mathbb{Z}_{p^s}[x]$ (su representación aditiva) es un isomorfismo de anillos, por lo tanto, $\mathbb{Z}_{p^s}[\xi]$ es también un anillo de Galois. Si aplicamos a ξ la función ϕ definida en el Lema 3.1.3, obtenemos $\phi(\xi) = \phi(x + \langle h(x)\rangle) = \overline{x} + \langle \overline{h}(x)\rangle \in \mathcal{F}(p, m)$, denotando a este elemento por $\overline{\xi}$ y evaluando en $\overline{h}(x)$

$$\begin{aligned}
\overline{h}(\overline{\xi}) &= \mu(a_0) + \mu(a_1)\overline{\xi} + \cdots + \mu(a_m)\overline{\xi}^m \\
&= \mu(a_0) + \mu(a_1)(\overline{x} + \langle \overline{h}(x)\rangle) + \cdots + \mu(a_m)(\overline{x} + \langle \overline{h}(x)\rangle)^m \\
&\overset{\tau}{=} \mu(a_0) + \langle \overline{h}(x)\rangle + \mu(a_1)(\overline{x} + \langle \overline{h}(x)\rangle) + \cdots + \mu(a_m)(\overline{x} + \langle \overline{h}(x)\rangle)^m \\
&= (\mu(a_0) + \mu(a_1)x + \cdots + \mu(a_m)x^m) + \langle \overline{h}(x)\rangle \\
&= \overline{h}(x) + \langle \overline{h}(x)\rangle = \langle \overline{h}(x)\rangle.
\end{aligned}$$

Tenemos que $\overline{\xi}$ es una raíz para el polinomio $\overline{h}(x)$, en otras palabras, el campo finito $\mathcal{F}(p, m)$ posee una raíz para el polinomio mónico irreducible $\overline{h}(x)$. Siguiendo una construcción similar a la del anillo $\mathbb{Z}_{p^s}[\xi]$ podemos definir al conjunto $\mathbb{F}_p[\overline{\xi}]$, éste es un campo finito isomorfo $\mathcal{F}(p, m)$ y en consecuencia isomorfo a $\mathbb{F}_{p^m}$. De lo anterior dicho podemos también considerar a $\mathbb{F}_p[\overline{\xi}]$ como una extensión del campo finito $\mathbb{F}_p$ y podemos reescribir el epimorfismo (2.1.8) como:

$$\begin{array}{rcl}
- : \mathbb{Z}_{p^s}[\xi] & \longrightarrow & \mathbb{F}_p[\overline{\xi}] \\
a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} & \longmapsto & \mu(a_0) + \mu(a_1)\overline{\xi} + \cdots + \mu(a_{m-1})\overline{\xi}^{m-1}
\end{array} \tag{3.1.3}$$

Corolario 3.1.6. *Definamos las funciones* $\sigma : \mathbb{Z}_{p^s}[x] \to \mathbb{Z}_{p^s}[\xi]$ *y* $\hat{\sigma} : \mathbb{F}_p[x] \to \mathbb{F}_p[\overline{\xi}]$ *tales que para cada* $f(x) \in \mathbb{Z}_{p^s}[x]$ *y* $g(x) \in \mathbb{F}_p[x]$ *los relaciona con* $f(\xi)$ *y* $g(\overline{\xi})$ *las representaciones aditivas de* $f(x) + \langle h(x)\rangle$ *y* $g(x) + \langle \overline{h}(x)\rangle$ *en* $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ *y* $\mathcal{F}(p, m)$ *respectivamente. Entonces el siguiente diagrama es conmutativo.*

$$\begin{array}{ccc}
\mathbb{Z}_{p^s}[x] & \overset{-}{\to} & \mathbb{F}_p[x] \\
\sigma \downarrow & & \downarrow \hat{\sigma} \\
\mathbb{Z}_{p^s}[\xi] & \overset{-}{\to} & \mathbb{F}_p[\overline{\xi}]
\end{array}$$

Demostración. Como $(- \circ \hat{\sigma}) : \mathbb{Z}_{p^s}[x] \to \mathbb{F}_p[\overline{\xi}]$ y $(\sigma \circ -) : \mathbb{Z}_{p^s}[x] \to \mathbb{F}_p[\overline{\xi}]$. Sea $f(x) \in \mathbb{Z}_{p^s}[x]$ tal que $f(x) + \langle h(x)\rangle = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + \langle h(x)\rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$, entonces $(\sigma \circ -)(f(x)) = \overline{\sigma(f(x))} = \overline{f(\xi)} = \mu(a_0) + \mu(a_1)\overline{\xi} + \cdots + \mu(a_{m-1})\overline{\xi}^{m-1}$. Por otro

lado, $(-\circ\hat{\sigma})(f(x)) = \hat{\sigma}\left(\overline{f(x)}\right) = \hat{\sigma}\left(\mu(a_0)+\mu(a_1)x+\cdots+\mu(a_{m-1})x^{m-1}\right) = \mu(a_0)+\mu(a_1)\overline{\xi}+\cdots+\mu(a_{m-1})\overline{\xi}^{m-1}$, por lo tanto, para todo $f(x)\in\mathbb{Z}_{p^s}[x]$ tenemos que $(\sigma\circ-)(f(x)) = (-\circ\hat{\sigma})(f(x))$ como queríamos demostrar. □

Hasta aquí, hemos demostrado que los campos finitos, $\mathbb{Z}_{p^s}$ y $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle = \mathbb{Z}_{p^s}[\xi]$ son anillos de Galois, éste último siempre y cuando $h(x)$ sea un polinomio mónico básico irreducible sobre $\mathbb{Z}_{p^s}$ y además, $Car(\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle) = Car(\mathbb{Z}_{p^s}) = p^s$. En general, cuando un anillo $\mathcal{R}$ es un anillo de Galois con $Car(\mathcal{R}) = p^s$ y $|\mathcal{R}| = p^{sm}$, lo denotaremos por $\mathcal{R} = GR(p^s, p^{sm})$, así, $\mathbb{Z}_{p^s} = GR(p^s, p^s)$, $\mathbb{Z}_{p^s}[\xi] = GR(p^s, p^{sm})$, $\mathbb{F}_p = GR(p,p)$ y $\mathbb{F}_p[\overline{\xi}] = GR(p, p^m)$.

ESTRUCTURA DEL ANILLO DE GALOIS

En esta sección nos daremos a la tarea de mostrar las propiedades fundamentales de los anillos de Galois y dar una caracterización de los mismos.

Lema 3.2.1. *Sea $\mathcal{R}$ un anillo de Galois con unidad 1, cuyos divisores de cero con el cero añadido forman el ideal principal $\langle p1\rangle$ para algún número primo p. Entonces $\langle p1\rangle$ es el único ideal maximal de $\mathcal{R}$, $\mathcal{R}/\langle p1\rangle$ es el campo de Galois $\mathbb{F}_{p^m}$ para algún $m\in\mathbb{N}$ y $Car(\mathcal{R}) = p^s$ para algún $s\in\mathbb{N}$.*

Demostración. Sea M un ideal maximal de $\mathcal{R}$, tal que, $M\nsubseteq\langle p1\rangle$. Entonces existe $m\in M-\langle p1\rangle$, por el Lema 1.5.15, m es una unidad de $\mathcal{R}$, lo cual nos dice que $M=\mathcal{R}$, una contradicción, por lo tanto, $M\subseteq\langle p1\rangle$. Como M es maximal, $M=\langle p1\rangle$, o bien, $\langle p1\rangle = \mathcal{R}$, pero $\langle p1\rangle$ también es maximal, así, $\langle p1\rangle\neq\mathcal{R}$, luego, $M=\langle p1\rangle$. Esto demuestra la unicidad. Sabemos que $\mathcal{R}/\langle p1\rangle$ es un campo finito, por (ii) del Lema 1.7.12, $\mathcal{R}/\langle p1\rangle$ es isomorfo a $\mathbb{F}_{p^m}$ para algún $m\in\mathbb{N}$. Denotemos por "$-$" al epimorfismo natural:

$$\begin{array}{rccc} - : & \mathcal{R} & \longrightarrow & \mathcal{R}/\langle p1\rangle \\ & r & \longmapsto & r+\langle p\rangle. \end{array}$$

Sea $\overline{a}\in\mathcal{R}/\langle p1\rangle$, entonces $p\overline{a} = \overline{p(1a)} = \overline{(p1)a} = \overline{(p1)}\overline{a} = \overline{0}$, así, $\mathcal{R}/\langle p1\rangle$ es de característica finita, $Car(\mathcal{R}/\langle p1\rangle) \mid p$ y como p es primo tenemos que $Car(\mathcal{R}/\langle p1\rangle) = p$. Sea $k = Car(\mathcal{R})$. Entonces $k1=0$, aplicando $-$ tenemos que $\overline{k1} = k\overline{1} = \overline{0}$, entonces $p|k$, luego existen $s,l\in\mathbb{N}$, tales que, $k = p^s l$ con $(l,p)=1$. Si $l>1$, entonces $a = p^s1$ y $b = l1$ son elementos distintos de cero de $\mathcal{R}$, tales que, $ab = (p^s1)(l1) = (p^sl)1 = 0$, en particular, $b\in\langle p1\rangle$. Es decir, existe $\alpha\in\mathcal{R}$ tal que $b = (p1)\alpha$, así, $l1 = (p1)\alpha$, aplicando el epimorfismo, $\overline{(l1)} = \overline{(p1)\alpha}$, luego, $l\overline{1} = \overline{p1}\overline{\alpha} = \overline{0}\in\mathcal{R}/\langle p1\rangle$, y de lo anterior se sigue que $p|l$ y $(p,l)=1$ lo cual es una contradicción, por lo tanto, $l=1$ y se tiene que, $Car(\mathcal{R}) = k = p^s$. □

Lema 3.2.2. *Sea $\mathcal{R}$ un anillo de Galois de característica p^s, donde p es un número primo y sea 1 la identidad de $\mathcal{R}$. Entonces los divisores de cero con cero añadido forman el ideal principal $\langle p1\rangle$ y el conjunto $\mathcal{R}_{p^s} := \{r1 | r\in\mathbb{Z}_{p^s}\}$ es un subanillo de $\mathcal{R}$ isomorfo a $\mathbb{Z}_{p^s}$.*

Demostración. Por la Definición 3.1.1 el conjunto de los divisores de cero con cero añadido de $\mathcal{R}$ forman un ideal principal $\langle q1\rangle$ para algún número primo q. Por el

lema anterior $Car(\mathcal{R}) = q^t$ para algún $t \in \mathbb{N}$ y por hipótesis, $Car(\mathcal{R}) = p^s$, entonces, $p^s = q^t$, luego, $p^s = qq^{t-1}$, así, $q \mid p^s$, por consiguiente, $q \mid p$. Como p, q son numeros primos entonces $q = p$, por lo tanto, $\langle q1\rangle = \langle p1\rangle$. Veamos que $\mathcal{R}_{p^s}$ es un subanillo de $\mathcal{R}$. Para esto, sean $r1, t1 \in \mathcal{R}_{p^s}$, así, $r1 - t1 = (r-t)1$, como $r, t \in \mathbb{Z}_{p^s}$ se sigue que $r - t \in \mathbb{Z}_{p^s}$, así, $r1 - t1 \in \mathcal{R}_{p^s}$ y entonces $(\mathcal{R}_{p^s}, +) \leqslant (\mathcal{R}, +)$. Ahora, $(r1t1) = (rt)1$ y dado que $rt \in \mathbb{Z}_{p^s}$ se sigue que $(r1t1) \in \mathcal{R}_{p^s}$, por lo tanto, $\mathcal{R}_{p^s}$ es un subanillo de $\mathcal{R}$. Finalmente, considérese la función: $[\,] : \mathbb{Z}_{p^s} \longrightarrow \mathcal{R}_{p^s}$, tal que para todo $r \in \mathcal{R}$, $[r] = r1$. No es difícil ver que es un homomorfismo de anillos sobreyectivo. Ahora, veamos que es inyectivo, sean $r, t \in \mathbb{Z}_{p^s}$, tales que, $[r] = [t]$, entonces, $[r] - [t] = 0$, como $[\,]$ es un homomorfismo, se sigue que $[r - t] = 0$, luego, $(r-t)1 = 0$, por lo tanto, $p^s \mid (r-t)$, ya que, $Car(\mathcal{R}) = p^s$. Como $r, t \in \mathbb{Z}_{p^s}$, entonces $r - t \in \mathbb{Z}_{p^s}$, así, $r - t < p^s$, luego, sólo ocurre que $r - t = 0$, por consiguiente, $r = t$ entonces $[\,]$ es biyectivo y por lo tanto, $\mathcal{R}_{p^s} \simeq \mathbb{Z}_{p^s}$. □

Dado un anillo de Galois $\mathcal{R}$ con $Car(\mathcal{R}) = p^s$, donde p es un número primo y $s \in \mathbb{N}$, se tiene que $\langle p1\rangle$ es el único ideal maximal, así que lo representaremos en lo sucesivo como (p), y por el lema previo, podemos considerar a $\mathbb{Z}_{p^s}$ como un subanillo de $\mathcal{R}$.

Lema 3.2.3. *Sea $\mathcal{R}$ un anillo de Galois donde $(p) = \mathcal{D} \cup \{0\}$, $Car(\mathcal{R}) = p^s$ para un número primo p y $s \in \mathbb{N}$. Entonces $\mathcal{R}/(p) \simeq \mathbb{F}_{p^m}$ para algún $m \in \mathbb{N}$ y los ideales principales (p^i) con $0 \leqslant i \leqslant s$, son de cardinalidad $p^{(s-i)m}$ y, en particular $|\mathcal{R}| = p^{sm}$.*

Demostración. Por el Lema 3.2.1, $\mathcal{R}/(p) \simeq \mathbb{F}_{p^m}$ para algún $m \in \mathbb{N}$. Considérese el grupo aditivo $(\mathcal{R}, +)$, entonces los ideales (p^i) con $0 \leqslant i \leqslant s$ son subgrupos aditivos de $(\mathcal{R}, +)$ y para cada $i \in \{0, 1, \ldots, s-1\}$, la función:

$$\begin{array}{rccc} \phi_i : & \mathcal{R} & \longrightarrow & (p^i)/(p^{i+1}) \\ & r & \longmapsto & p^i r + (p^{i+1}) \end{array}$$

es un epimorfismo de grupos. En efecto, como (p^i) es un ideal de $\mathcal{R}$ y $(\mathcal{R}, +)$ es un grupo abeliano entonces $((p^i), +) \lhd (\mathcal{R}, +)$, más áun, si consideramos a (p^i) como un grupo aditivo del hecho que $(p^{i+1}) \subseteq (p^i)$, se consigue que $(p^{i+1}) \lhd (p^i)$, por lo tanto, $(p^i)/(p^{i+1})$ es un grupo abeliano. Sean $r, t \in \mathcal{R}$, entonces $\phi_i(r+t) = p^i(r+t) + (p^{i+1}) = (p^i r + p^i t) + (p^{i+1}) = [p^i r + (p^{i+1})] + [p^i t + (p^{i+1})] = \phi_i(r) + \phi_i(t)$, por lo tanto, ϕ_i es un homomorfismo de grupos, por su definición ϕ_i es un epimorfismo de grupos. Veamos que para todo $i \in \{0, 1, \ldots s-1\}$, $\ker(\phi_i) = (p)$. Sea $\alpha \in \ker(\phi_i)$, entonces $\phi_i(\alpha) = (p^{i+1}) = \overline{0}$. Por otro lado tenemos que $\phi_i(\alpha) = p^i\alpha + (p^{i+1})$, así, $p^i\alpha + (p^{i+1}) = (p^{i+1})$, entonces $p^i\alpha \in (p^{i+1})$, luego existe $\beta \in \mathcal{R}$, tal que, $p^i\alpha = p^{i+1}\beta$, se sigue que $\alpha = p\beta$, entonces $\alpha \in (p)$, por lo tanto, $\ker(\phi_i) \subseteq (p)$. Por otro lado, si $\alpha \in (p)$ entonces existe $\beta \in \mathcal{R}$ tal que: $\alpha = p\beta$, tenemos que $\phi_i(\alpha) = p^i\alpha + (p^{i+1}) = p^i(p\beta) + (p^{i+1}) = p^{i+1}\beta + (p^{i+1}) = (p^{i+1}) = \overline{0}$, por lo tanto, $(p) \subseteq \ker(\phi_i)$ entonces, para todo $i \in \{0, 1, \ldots s-1\}$, $\ker(\phi_i) = (p)$, más aún, $\ker(\phi_i) \lhd \mathcal{R}$, por el Teorema 1.2.9, tenemos **a nivel de grupos** que, $\mathcal{R}/\ker(\phi_i) \simeq \mathrm{Im}\phi_i$. Entonces, $\mathcal{R}/(p) \simeq (p^i)/(p^{i+1})$, así,

$$\left|\frac{\mathcal{R}}{(p)}\right| = \left|\frac{(p)}{(p^2)}\right| = \cdots = \left|\frac{(p^{s-2})}{(p^{s-1})}\right| = \left|(p^{s-1})\right|. \tag{3.2.1}$$

Ya que $\mathcal{R}/(p) \simeq \mathbb{F}_{p^m}$, se deduce que $|\mathcal{R}/(p)| = p^m$ y como $(p^{i+1}) \lhd (p^i)$, para cada $i \in \{0, 1, \ldots, s-1\}$, se sigue que, $(0) \lhd (p^{s-1}) \lhd \ldots \lhd (p) \lhd (1) = \mathcal{R}$; por el Corolario 1.3.7(c),

para cada $i \in \{0, 1, \ldots, s-1\}$, $|(p^i)/(p^{i+1})| = |(p^i)|/|(p^{i+1})|$ y de las igualdades en (3.2.1) tenemos:

$$|(p^i)| = \left|\frac{(p^i)}{(p^{i+1})}\right| |(p^{i+1})| = \underbrace{\left|\frac{(p^i)}{(p^{i+1})}\right| \left|\frac{(p^{i+1})}{(p^{i+2})}\right| \cdots |(p^{s-1})|}_{s-i \text{ términos}} = \underbrace{p^m p^m \cdots p^m}_{s-i \text{ veces}} = p^{(s-i)m}$$

y, en particular $|\mathcal{R}| = |(1)| = |(p^0)| = p^{(s-0)m} = p^{sm}$, como queríamos demostrar. □

Observación 3.2.4. Considerando la notación introducida al final de la sección 3.1, sea $\mathcal{R} = GR(p^s, p^{sm})$ y denotemos al epimorfismo natural de $\mathcal{R}$ en $\mathcal{R}/(p)$ por "$-$" y de manera similar al epimorfismo (2.1.8) podemos extender al epimorfismo, "$-$" a los anillos de polinomios $\mathcal{R}[x]$ y $(\mathcal{R}/(p))[x]$, por simplicidad denotaremos a la extensión también por "$-$" y a las imágenes de los elementos de $r \in \mathcal{R}$ y $f(x) \in \mathcal{R}[x]$ bajo éstos, por $\overline{r}$ y $\overline{f}(x)$ respectivamente.

Lema 3.2.5. *Sea $\mathcal{R} = GR(p^s, p^{sm})$ con p un número primo y $s, m \in \mathbb{N}$. Sea $f(x) \in \mathbb{Z}_{p^s}[x]$ y supóngase que $\overline{f}(\overline{\beta}) = 0$ para algún $\beta \in \mathcal{R}/(p) \simeq \mathbb{F}_{p^m}$ tal que $\overline{f}'(\overline{\beta}) \neq 0$. Entonces existe una única raíz $\alpha \in \mathcal{R}$ de $f(x)$ tal que $\overline{\alpha} = \overline{\beta}$.*

Demostración. Sea β una preimagen de $\overline{\beta}$, ésta existe ya que $-$ es un epimorfismo. Construiremos una sucesión de elementos $\alpha_0, \alpha_1, \ldots, \alpha_{s-1} \in \mathcal{R}$ tales que $\overline{\alpha_i} = \overline{\beta}$ y que $f(\alpha_i) \in (p^{i+1})$ para $i \in \{0, 1, \ldots, s-1\}$. Elegimos $\alpha_0 = \beta$. Entonces $\overline{\alpha_0} = \overline{\beta}$, se sigue que:

$$\begin{aligned}
\overline{f}(\overline{\beta}) = 0 &\Leftrightarrow \overline{a_0} + \overline{a_1}\overline{\beta} + \cdots + \overline{a_n}\overline{\beta}^n = 0 \\
&\Leftrightarrow \overline{a_0} + \overline{a_1\beta} + \cdots + \overline{a_n\beta^n} = 0 \\
&\Leftrightarrow \overline{a_0 + a_1\beta + \cdots + a_n\beta^n} = 0 \\
&\Leftrightarrow a_0 + a_1\alpha_0 + \cdots + a_n\alpha_0^n \in \ker(-) = (p)
\end{aligned}$$

por lo tanto, $f(\alpha_0) \in (p)$. Como $\overline{f}'(\overline{\beta}) \neq 0$ entonces $\overline{f}'(\overline{\alpha_0}) \neq 0$. Así $f'(\alpha_0) \notin (p)$, en otras palabras $f'(\alpha_0)$ es una unidad, denotemos pues $u = f'(\alpha_0)$ así existe $u^{-1} \in \mathcal{R}$ tal que $uu^{-1} = 1 \in \mathcal{R}$. Sea $\alpha_1 = \alpha_0 - (u^{-1}f(\alpha_0)) \in \mathcal{R}$, entonces $\overline{\alpha_1} = \overline{\alpha_0} - \overline{u^{-1}}\,\overline{f(\alpha_0)} = \beta - 0 = \beta$ puesto que $f(\alpha_0) \in (p)$, mostraremos que $f(\alpha_1) \in (p^2)$. En efecto, como $f(\alpha_1) = f(\alpha_0 - (u^{-1}f(\alpha_0)))$, por la fórmula de Taylor (Teorema A.1.5):

$$\begin{aligned}
f(\alpha_1) &= f(\alpha_0) - \frac{f'(\alpha_0)}{1!}(u^{-1}f(\alpha_0)) + \frac{f''(\alpha_0)}{2!}(-u^{-1}f(\alpha_0))^2 - \cdots - (-1)^n\frac{f^{(n)}(\alpha_0)}{n!}(u^{-1}f(\alpha_0))^n \\
&= f(\alpha_0)\left(1 - u(u^{-1}) - \frac{f''(\alpha_0)}{2!}(u^{-1})^2(f(\alpha_0)) - \cdots - (-1)^n\frac{f^{(n)}(\alpha_0)}{n!}(u^{-1})^n(f(\alpha_0))^{n-1}\right) \\
&= f(\alpha_0)\left(1 - 1 + \frac{f''(\alpha_0)}{2!}(u^{-1})^2(f(\alpha_0)) - \cdots - (-1)^n\frac{f^{(n)}(\alpha_0)}{n!}(u^{-1})^n(f(\alpha_0))^{n-1}\right) \\
&= f(\alpha_0)\left(\frac{f''(\alpha_0)}{2!}(u^{-1})^2(f(\alpha_0)) - \cdots - (-1)^n\frac{f^{(n)}(\alpha_0)}{n!}(u^{-1})^n(f(\alpha_0))^{n-1}\right) \\
&= (f(\alpha_0))^2\left(\frac{f''(\alpha_0)}{2!}(u^{-1})^2 - \cdots - (-1)^n\frac{f^{(n)}(\alpha_0)}{n!}(u^{-1})^n(f(\alpha_0))^{n-2}\right)
\end{aligned}$$

Como $f(\alpha_0) \in (p)$ entonces existe $t \in \mathcal{R}$ tal que $f(\alpha_0) = tp$; así $(f(\alpha_0))^2 = t^2p^2$, de ahí que $f(\alpha_1) = p^2\left[t^2\left(\frac{f''(\alpha_0)}{2!}(u^{-1})^2 + \cdots + (-1)^n\frac{f^{(n)}(\alpha_0)}{n!}(u^{-1})^n(f(\alpha_0))^{n-2}\right)\right]$, por lo tanto,

$f(\alpha_1) \in (p^2)$. Procediendo de esta manera para $i \in \{2, 3 \ldots, s-1\}$, se consigue que, $\overline{\alpha_i} = \overline{\beta}$ y $f(\alpha_i) \in (p^{i+1})$ en particular, para $s-1$ se sigue que $\overline{\alpha_{s-1}} = \overline{\beta}$ y $f(\alpha_{s-1}) \in (p^s) = (0)$, así, $f(\alpha_{s-1}) = 0$ y nombrando $\alpha = \alpha_{s-1}$ tenemos una raíz de $f(x)$. Para ver la unicidad, sea $\alpha' \in \mathcal{R}$, tal que, $f(\alpha') = 0$ y $\overline{\alpha'} = \overline{\beta} = \overline{\alpha}$, si $\alpha' \neq \alpha$, entonces $\alpha' - \alpha \neq 0$, pero $\overline{\alpha' - \alpha} = \overline{\alpha'} - \overline{\alpha} = 0$, lo cual implica que $\alpha' - \alpha \in (p) = \ker(-)$, de esto se sigue que $\alpha' - \alpha = pk = p(k1)$, dónde 1 denota a la identidad en $\mathcal{R}$. Usando el epimorfismo del Lema 3.2.2, podemos hallar ρ una preimagen de $(k1)$, por el Corolario 2.1.3, existen $a \in \mathbb{Z}_{p^s}$ e $i \in \mathbb{N}$ tales que $\rho = ap^{i-1}$. Ahora bien, $\alpha' - \alpha = p[ap^{i-1}] = [a]p^i$, denotando $r = [a]$ podemos expresar $\alpha' = \alpha + rp^i$, nuevamente por la fórmula de Taylor, como $\alpha' = \alpha + rp^i$,

$$\begin{aligned} f(\alpha') &= f(\alpha) + \frac{f'(\alpha)}{1!}(rp^i) + \frac{f''(\alpha)}{2!}(rp^i)^2 + \cdots + (-1)^n \frac{f^{(n)}(\alpha)}{n!}(rp^i)^n \\ 0 &= 0 + \frac{f'(\alpha)}{1!}(rp^i) + \frac{f''(\alpha)}{2!}(rp^i)^2 + \cdots + (-1)^n \frac{f^{(n)}(\alpha)}{n!}(rp^i)^n \quad \text{(pues } f(\alpha) = f(\alpha') = 0\text{)} \\ 0 &= f'(\alpha)(rp^i) + \frac{f''(\alpha)}{2!}(rp^i)^2 + \cdots + (-1)^n \frac{f^{(n)}(\alpha)}{n!}(rp^i)^n, \end{aligned}$$

así, despejando el primer término de la suma tenemos que,

$$\begin{aligned} f'(\alpha)(rp^i) &= -\left(\frac{f''(\alpha)}{2!}(rp^i)^2 + \cdots + (-1)^n \frac{f^{(n)}(\alpha)}{n!}(rp^i)^n \right) \\ &= -p^{2i}\left(\frac{f''(\alpha)}{2!}r^2 + \cdots + (-1)^n \frac{f^{(n)}(\alpha)}{n!} r^n p^{(n-2)i} \right) \end{aligned}$$

de esto tenemos que $f'(\alpha)(rp^i) \in (p^{2i}) \subseteq (p^{i+1})$, como $\overline{f}'(\overline{\alpha}) = \overline{f}'(\overline{\beta}) \neq 0$ entonces $f'(\alpha)$ es una unidad, y de $(a, p) = 1$ en $\mathbb{Z}_{p^s}$ y $[a] = r$ se sigue que $(r, p) = 1$ en $\mathcal{R}$, por lo dicho antes, existe $h \in \mathcal{R}$ tal que $hf'(\alpha) = 1$ entonces $rp^i = hf'(\alpha)rp^i \in (p^{i+1})$ esto implica que $r \in (p)$, lo cual es una contradicción, por lo tanto, $\alpha' = \alpha$ y así α es única. □

Teorema 3.2.6. *Sea $\mathcal{R} = GR(p^s, p^{sm})$ con p un número primo y $s, m \in \mathbb{N}$. Entonces para algún polinomio mónico básico irreducible de grado m en $\mathbb{Z}_{p^s}$ se tiene que $\mathcal{R}$ es isomorfo a $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$.*

Demostración. Sea $h(x)$ un polinomio mónico básico irreducible en $\mathbb{Z}_{p^s}[x]$ de grado m, entonces $\overline{h}(x)$ es un polinomio mónico e irreducible de grado m en $\mathbb{F}_p[x]$ entonces por el Lema A.2.4 existe una raíz de $\overline{h}(x)$ en $\mathbb{F}_{p^m}$, más aún todas la raíces de $\overline{h}(x)$ están en $\mathbb{F}_{p^m}$ y son simples, luego por el Lema 3.2.1, $\mathbb{F}_{p^m} \simeq \mathcal{R}/(p)$ y podemos considerar dichas raíces como elementos de $\mathcal{R}/(p)$. Sea $\overline{\beta}$ una raíz de $\overline{h}(x)$, como es simple, $\overline{h}(\overline{\beta}) = 0$ y $\overline{h}'(\overline{\beta}) \neq 0$ entonces por el Lema 3.2.5 existe una única raíz $\alpha \in \mathcal{R}$ de $h(x)$ tal que $\overline{\alpha} = \overline{\beta}$. Considérese ahora la función:

$$\begin{array}{rccc} \psi : & \dfrac{\mathbb{Z}_{p^s}[x]}{\langle h(x)\rangle} & \longrightarrow & \mathcal{R} \\ & f(x) + \langle h(x)\rangle & \longmapsto & f(\alpha) \end{array}$$

Sean $f_1(x) + \langle h(x)\rangle = \sum_{i=0}^{m-1} a_i x^i + \langle h(x)\rangle$ y $f_2(x) + \langle h(x)\rangle = \sum_{i=0}^{m-1} b_i x^i + \langle h(x)\rangle$ con $f_1(x) + \langle h(x)\rangle = f_2(x) + \langle h(x)\rangle$ es claro que $0 + \langle h(x)\rangle = \sum_{i=0}^{m-1} (a_i - b_i)x^i + \langle h(x)\rangle$

entonces el polinomio $l(x) = \sum_{i=0}^{m-1}(a_i - b_i)x^i \in \langle h(x)\rangle$ entonces $\psi(l(x) + \langle h(x)\rangle) = \psi(0 + \langle h(x)\rangle = 0$ pero también $\psi(l(x) + \langle h(x)\rangle) = l(\alpha)$ por lo tanto $l(\alpha) = 0$ así, α es raíz de $l(x)$, además $\overline{l(\alpha)} = \overline{l}(\overline{\alpha}) = \overline{0}$ pero $\overline{h}(\overline{\alpha}) = 0$ y $\overline{h}(x)$ es irreducible en $\mathbb{F}_p[x]$ entonces $\overline{h}(x)|\overline{l}(x)$ pero $grad(l(x)) \leqslant m-1 < m = grad(h(x))$ entonces $\overline{l}(x) = 0$ se sigue que $l(x) = 0$ o $l(x) \in \ll \overline{p} \gg -\{0\}$. Supongamos que $l(x) \neq 0$, como $\overline{h}(x) \mid \overline{l}(x)$ entonces existe $\overline{k}(x) \in \mathbb{F}_p[x]$ tal que $\overline{l}(x) = \overline{k}(x)\overline{h}(x)$ así $\overline{l}(x) - \overline{k}(x)\overline{h}(x) = \overline{0}$ esto es $\overline{l(x) - k(x)h(x)} = \overline{0}$, así, $l(x) - k(x)h(x) \in \ker(-) = \ll \overline{p} \gg$ entonces existe $k_1(x) \in \mathbb{Z}_{p^s}[x]$ tal que $l(x) - k(x)h(x) = pk_1(x)$, así, $l(x) = k(x)h(x) + pk_1(x)$, pero esto implica que $m-1 \geqslant grad(l(x)) = grad(k(x)h(x) + pk_1(x)) = máx\{grad(k(x)h(x)), grad(k_1(x))\} \geqslant grad(h(x)) = m$ lo cual es una contradicción, por lo tanto, $l(x) = 0$. Como $l(x) = 0$ entonces $a_i - b_i = 0$ para toda $i \in \{0, 1, \ldots, m-1\}$, así, $f_1(\alpha) = f_2(\alpha)$ y ψ está bien definida y no es difícil demostrar que es un epimorfismo de anillos y dado $f(x) + \langle h(x)\rangle$ tal que $\psi(f(x) + \langle h(x)\rangle) = 0$ entonces $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} = 0$, aplicando (2.1.8) tenemos que $\overline{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}} = \overline{a_0} + \overline{a_1}\overline{\alpha} + \cdots + \overline{a_{m-1}}\overline{\alpha}^{m-1} = \overline{0}$ de la igualdad anterior tenemos que $\overline{f}(\alpha) = \overline{0}$ y $grad(f(x)) \leqslant m-1 < m = grad(h(x))$ entonces $\overline{h}(x) \mid \overline{f}(x)$ se tiene que $\overline{f}(x) = \overline{0}$, así, $\overline{a_i} = 0$ para cada $i \in \{0, 1, \ldots, m-1\}$, entonces $a_i \in \langle\overline{p}\rangle \subseteq \mathbb{Z}_{p^s} \subseteq \mathcal{R}$ (Lema 3.2.2) entonces $a_i = pb_i^{(1)}$ con $b_i^{(1)} \in \mathcal{R}$ entonces $0 = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} = p\left(b_0^{(1)} + b_1^{(1)}\alpha + \cdots + b_{m-1}^{(1)}\alpha^{m-1}\right)$ luego tenemos que $b_0^{(1)} + b_1^{(1)}\alpha + \cdots + b_{m-1}^{(1)}\alpha^{m-1}$ es un divisor de cero o cero en $\mathcal{R}$, luego, tenemos que $\overline{b_0^{(1)} + b_1^{(1)}\alpha + \cdots + b_{m-1}^{(1)}\alpha^{m-1}} = \overline{0}$, así, $\overline{b_0^{(1)}} + \overline{b_1^{(1)}}\overline{\alpha} + \cdots + \overline{b_{m-1}^{(1)}}\overline{\alpha}^{m-1} = \overline{0}$ procediendo como antes podemos concluir que $b_i^{(1)} = pb_i^{(2)}$ con $b_i^{(2)} \in \mathcal{R}$, en general para $j \in \{1, 2, \ldots, m-2\}$, $b_i^{(j)} = pb_i^{(j+1)}$ entonces $a_i = pb_i^{(1)} = p^2b_i^{(2)} = \cdots = p^jb_i^{(j)} = \cdots = p^sb_i^s$ para $i \in \{0, 1, \ldots, m-1\}$ pero $Car(\mathcal{R}) = p^s$, por lo anterior $a_0 = a_1 = \cdots = a_{m-1} = 0$, por lo tanto, $f(x) + \langle h(x)\rangle = 0 + \langle h(x)\rangle$, así, $\ker(\psi) \subseteq \{\langle h(x)\rangle\}$, por consiguiente, ψ es un monomorfismo y así, un isomorfismo como queríamos demostrar. □

Para conlcuir está sección mostraremos un resultado que nos permite establecer relaciones entre todos los anillos de Galois con la misma cardinalidad y característica.

Corolario 3.2.7. *Sean $\mathcal{R}_1$, $\mathcal{R}_2$ dos anillos de Galois con $Car(\mathcal{R}_1) = Car(\mathcal{R}_2)$ y $|\mathcal{R}_1| = |\mathcal{R}_2|$. Entonces $\mathcal{R}_1 \simeq \mathcal{R}_2$.*

Demostración. Sean $p, s, m \in \mathbb{N}$ con p un número primo y $h_1(x), h_2(x)$ polinomios mónicos, básicos irreducibles en $\mathbb{Z}_{p^s}[x]$ de grado m, por el Teorema 3.2.6, tenemos que, $\mathcal{R}_1 \simeq \mathbb{Z}_{p^s}[x]/\langle h_1(x)\rangle$ y $\mathcal{R}_2 \simeq \mathbb{Z}_{p^s}[x]/\langle h_2(x)\rangle$, además, si ξ_1, ξ_2 son raíces de $h_1(x)$ y $h_2(x)$ respectivamente, entonces $\mathcal{R}_1 \simeq \mathbb{Z}_{p^s}[\xi_1]$ y $\mathcal{R}_2 \simeq \mathbb{Z}_{p^s}[\xi_2]$ luego, considérese la función,

$$\begin{array}{rccc} \phi: & \mathbb{Z}_{p^s}[\xi_1] & \longrightarrow & \mathbb{Z}_{p^s}[\xi_2] \\ & f(\xi_1) & \longmapsto & f(\xi_2) \end{array}$$

donde, $f(\xi_1)$ y $f(\xi_2)$ son las representaciones aditivas de $f(x) + \langle h_1(x)\rangle$ y $f(x) + \langle h_2(x)\rangle$ en $\mathcal{R}_1$ y $\mathcal{R}_2$ respectivamente. Si elegimos $f_1(\xi_1) = \sum_{i=0}^{m-1} a_i\xi_1^i$ y $f_2(\xi_1) = \sum_{i=0}^{m-1} b_i\xi_1^i$ con $f_1(\xi_1) = f_2(\xi_1)$, entonces $a_i = b_i$ para $i \in \{0, 1, \ldots, m-1\}$, puesto que las representaciones aditivas son únicas, por lo tanto, $f_1(\xi_2) = \sum_{i=0}^{m-1} a_i\xi_2^i = \sum_{i=0}^{m-1} b_i\xi_2^i = f_2(\xi_2)$, esto es, $\phi(f_1(\xi_1)) = \phi(f_2(\xi_1))$, y así ϕ está bien definida. Usando las operaciones

dadas en la Definición 3.1.5, tenemos que $\phi(f_1(\xi_1)+f_2(\xi_1)) = \phi([f_1+f_2](\xi_1)) = [f_1+f_2](\xi_2) = f_1(\xi_2)+f_2(\xi_2) = \phi(f_1(\xi_1))+\phi(f_2(\xi_1))$ y supongamos que $f_1(x)f_2(x) \equiv r(x) (\text{mód } [h_1(x), h_2(x)])$[2], entonces $\phi(f_1(\xi_1)f_2(\xi_1)) = \phi(r(\xi_1)) = r(\xi_2) = \phi(f_1(\xi_1))\phi(f_2(\xi_1))$, por lo tanto, ϕ es un homomorfismo de anillos. Más aún, tenemos que $|\mathbb{Z}_{p^s}[\xi_1]| = p^{sm} = |\mathbb{Z}_{p^s}[\xi_2]|$, entonces ϕ es sobreyectiva y por tanto, un epimorfismo. Es claro que $\{0\} \subseteq \ker\phi$ y como $f(\xi_1) \in \ker(\phi)$, se tiene que $\phi(f(\xi_1)) = 0$, entonces $f(\xi_2) = 0$, lo cual implica, $f(\xi_1) = 0$ pues la representación aditiva de 0 es única en ambos anillos, por lo tanto, $\ker(\phi) \subseteq \{0\}$, así, ϕ es un monomorfismo, por lo tanto, es un isomorfismo, por consiguiente, $\mathcal{R}_1 \simeq \mathcal{R}_2$. □

LA REPRESENTACIÓN p-ÁDICA

Teorema 3.3.1. *Sea $\mathcal{R} = GR(p^s, p^{sm})$, entonces:*

(i) *existe un elemento ξ con $ord(\xi) = p^m - 1$, el cual es raíz de un polinomio mónico básico primitivo $h(x)$ con $grad(h(x)) = m$ sobre $\mathbb{Z}_{p^s}$ y que divide a $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$. Más aún, $\mathcal{R} \simeq \mathbb{Z}_{p^s}[\xi]$ y $h(x)$ es el único polinomio de grado m en $\mathbb{Z}_{p^s}[x]$ con ξ como raíz.*

(ii) *Sea $\mathcal{T} := \{0, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$ entonces todo elemento $c \in \mathcal{R}$ puede expresarse de manera única como:*

$$c = a_0 + a_1 p + a_2 p^2 + \cdots + a_{s-1} p^{s-1} \tag{3.3.1}$$

dónde, $a_i \in \mathcal{T}$ para $i \in \{0, 1, \ldots, s-1\}$.

(iii) *Sea $c \in \mathcal{R}$ expresado como en (3.3.1) entonces $c_i \in (p)$ si sólo si $a_0 = 0$ y $c_i \notin (p)$ si y sólo si $a_0 \neq 0$.*

Demostración. (i) Sea $m \in \mathbb{N}$, por el Teorema 2.3.6, existe un polinomio mónico básico primitivo $h(x)$ con $grad(h(x)) = m$ y que divide a $(x^{p^m-1} - 1)$ en $\mathbb{Z}_{p^s}[x]$, entonces $\overline{h}(x)$ es un polinomio mónico y primitivo en $\mathbb{F}_p[x]$. Por el Lema 2.3.4, el polinomio $(x^{p^m} - x)$ no tiene factores múltiples en $\mathbb{F}_p[x]$ y, como $h(x) \mid (x^{p^m-1} - 1)$ entonces $(x^{p^m-1} - 1) = h(x)l(x)$ para algún $l(x) \in \mathbb{Z}_{p^s}[x]$, se sigue que $(x^{p^m} - x) = h(x)l(x)x$ y, aplicando "–" se consigue $(x^{p^m} - x) = \overline{h}(x)\overline{l}(x)x$ en $\mathbb{F}_p[x]$. Como $\mathbb{F}_{p^m}$ es el campo de descomposición de $\overline{h}(x)$, elegimos ξ_p una de las raíces de $\overline{h}(x)$, es claro que ξ_p es un elemento primitivo de $\mathbb{F}_{p^m}$, es decir, $\langle \xi_p \rangle = \mathbb{F}^*_{p^m}$. Si ξ_p fuera una raíz múltiple de $\overline{h}(x)$ entonces para algún $k \in \mathbb{N}$ tendríamos que $(x - \xi_p)^k \mid \overline{h}(x)$, así $\overline{h}(x) = (x - \xi_p)^k \overline{t}(x)$ para algún $\overline{t}(x) \in \mathbb{F}_p[x]$, luego por lo dicho antes tenemos que $(x^{p^m} - x) = \left[(x - \xi_p)^k\right] \overline{t}(x)\overline{l}(x)x$ pero esto contradice que $(x^{p^m} - x)$ no tiene factores múltiples, por lo tanto, ξ_p es una raíz simple y entonces $\overline{h}'(\xi_p) \neq 0$, por el Lema 3.2.5, existe una única raíz $\xi \in \mathcal{R}$ de $h(x)$ tal que $\overline{\xi} = \xi_p$. Tenemos que $x^{p^m-1} - 1 = h(x)l(x)$ en $\mathbb{Z}_{p^s}[x]$, así, $\xi^{p^m-1} - 1 = h(\xi)l(\xi) = 0 \cdot l(\xi) = 0$, luego $\xi^{p^m-1} = 1$, se sigue que, $ord(\xi) \mid p^m - 1$. Si $d = ord(\xi)$, entonces $d \leqslant \xi^{p^m-1}$. Supongamos que $d < \xi^{p^m-1}$, por definición $\xi^d = 1$, aplicando "–", $\overline{\xi}^d = 1$ esto implica que $(\xi_p)^d = 1$ pero esto es una contradicción, pues $ord(\xi_p) = p^m - 1$ entonces $ord(\xi) = p^m - 1$. Por el Teorema 3.2.6,

2 $[h_1(x), h_2(x)]$ es el mínimo común múltiplo de los polinomios.

$\mathcal{R} \simeq \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle = \mathbb{Z}_{p^s}[\xi]$, mediante el isomorfismo ψ con ξ en lugar de α. Sea $\lambda(x)$ un polinomio mónico con $grad(\lambda) = l \leqslant m$ en $\mathbb{Z}_{p^s}[x]$, tal que, $\lambda(\xi) = 0$. Supongamos que $l < m$ entonces aplicando ψ tenemos que $\psi(\lambda + \langle h(x)\rangle) = \lambda(\xi) = 0$, por lo tanto, $\lambda(x) + \langle h(x)\rangle \in \ker(\psi) = \{\langle h(x)\rangle\}$ entonces $h(x)|l(x)$ pero esto ocurre si y sólo si $\lambda(x) = 0$ pues $grad(\lambda(x)) < grad(h(x))$. Si $l = m$ entonces como $\lambda(x)$ y $h(x)$ son mónicos, tenemos que $grad(\lambda(x) - h(x)) < m$ y así $\psi(\lambda(x) - h(x)) = \lambda(\xi) - h(\xi) = 0$, procediendo como antes tenemos que $\lambda(x) - h(x) = 0$, por lo tanto, $\lambda(x) = h(x)$, esto es $h(x)$ es el único polinomio con las características de grado menor o igual que m, con ξ como raíz.

(ii) Sea $0 \leqslant i \leqslant p^m - 2$ entonces $\xi^i(\xi^{p^m-1-i}) = \xi^{p^m-1} = 1$ entonces ξ^i es una unidad para $i \in \{0, 1, \ldots, p^m - 2\}$. Sean ahora $i, j \in \{0, 1, \ldots, p^m - 2\}$ con $i \neq j$, supongamos sin pérdida de generalidad que $i > j$, luego $i = j + k$ para algún $k \in \{0, 1, \ldots, p^m - 2\}$. Si suponemos que $\xi^i = \xi^j$ tenemos que $\xi^{j+k} = \xi^j$, como ξ^j es una unidad, podemos multiplicar por su inverso y así tenemos que, $\xi^k = 1$ y $k < p^m - 1$ lo cual es nuevamente una contradicción pues $ord(\xi) = p^m - 1$, por lo tanto, $\xi^i \neq \xi^j$, entonces $|\mathcal{T}| = \left|\{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}\right| = p^m$. Por el Lema 1.5.15, $\mathcal{R} = \mathcal{R}^* \cup (p)$ con $\mathcal{R}^* \cap (p) = \emptyset$, entonces si $1 - \xi^j \in (p)$, con $1 \leqslant j < p^m - 1$ tenemos que $\overline{0} = \overline{1 - \xi^j} = \overline{1} - \overline{\xi}^j$, por lo tanto, $(\xi_p)^j = \overline{1}$ nuevamente, una contradicción pues $ord(\xi_p) = p^m - 1$, entonces $1 - \xi^j \notin (p)$, esto es $1 - \xi^j$ es una unidad de $\mathcal{R}$, cada vez que $j \in \{1, 2, \ldots, p^m - 2\}$. Más aún, si elegimos $i < j \in \{1, 2, \ldots, p^m - 2\}$ con $j - i \in \{1, 2, \ldots, p^m - 3\}$ entonces ξ^i y $1 - \xi^{j-i}$ son unidades en $\mathcal{R}$, luego el producto es una unidad, entonces $\xi^i(1 - \xi^{j-i}) = \xi^i - \xi^j$ es una unidad de $\mathcal{R}$. Es fácil ver que $a_0 + a_1 p + \cdots + a_{s-1}p^{s-1} \in \mathcal{R}$ y podemos definir el conjunto $\mathbb{T} := \left\{a_0 + a_1 p + \cdots + a_{s-1}p^{s-1} | a_i \in \mathcal{T} \text{ para } i \in \{0, 1, \ldots, s-1\}\right\} \subseteq \mathcal{R}$, por consiguiente, $|\mathbb{T}| \leqslant p^{sm}$. Sean $a_0 + a_1 p + \cdots + a_{s-1}p^{s-1}$, $a'_0 + a'_1 p + \cdots + a'_{s-1}p^{s-1} \in \mathbb{T}$, tales que, $a_0 + a_1 p + \cdots + a_{s-1}p^{s-1} = a'_0 + a'_1 p + \cdots + a'_{s-1}p^{s-1}$. Como $Car(\mathcal{R}) = p^s$ tenemos que:

$$\begin{aligned} p^{s-1}(a_0 + a_1 p + \cdots + a_{s-1}p^{s-1}) &= p^{s-1}(a'_0 + a'_1 p + \cdots + a'_{s-1}p^{s-1}) \\ p^{s-1}a_0 &= p^{s-1}a'_0. \end{aligned} \tag{3.3.2}$$

Si $a_0 = 0$ tenemos que $p^{s-1}a'_0 = 0$, entonces $p \mid a'_0$ en $\mathcal{R}$. Supongamos que $a'_0 \neq 0$ entonces $a'_0 = \xi^j$ para $j \in \{0, 1, \ldots, p^m - 2\}$ y por lo dicho antes $\overline{a'_0} = 0$, así tenemos que $\overline{\xi}^j = 0$ para algún $j \in \{0, 1, \ldots, p^m - 2\}$ lo cual contradice que $\overline{\xi}$ es un elemento primitivo, por esto concluimos que $a'_0 = 0$, es decir, $a_0 = 0$ implica $a'_0 = 0$ así y de manera análoga $a'_0 = 0$ implica $a_0 = a'_0$. Si tanto a_0 como a'_0 no son cero, entonces podemos factorizar de (3.3.2) a p^{s-1} como sigue $p^{s-1}(a_0 - a'_0) = 0$, pero $a_0 - a'_0 = \xi^i - \xi^j$ y como esto es una unidad, existe $u^{-1} \in \mathcal{R}$, tal que, $(a_0 - a'_0)u^{-1} = 1$ entonces, $0 = 0u^{-1} = p^{s-1}(a_0 - a'_0)u^{-1} = p^{s-1}$, otra contradicción, por lo tanto, $a_0 - a'_0 = 0$, en conclusión, $a_0 = a'_0$. Dado que $(\mathcal{R}, +)$ es un grupo, podemos cancelar a_0 y a'_0, así,

$$\begin{aligned} a_1 p + \cdots + a_{s-1}p^{s-1} &= a'_1 p + \cdots + a'_{s-1}p^{s-1} \\ p^{s-2}(a_1 p + \cdots + a_{s-1}p^{s-1}) &= p^{s-2}(a'_1 p + \cdots + a'_{s-1}p^{s-1}) \\ p^{s-1}a_1 &= p^{s-1}a'_1 \end{aligned} \tag{3.3.3}$$

Procediendo como antes, llegamos a que $a_1 = a_1'$ y así sucesivamente, $a_i = a_i'$ para $i \in \{0, 1, \ldots, s-1\}$, luego tenemos que $|\mathbb{T}| = p^{sm}$, entonces $\mathbb{T} = \mathcal{R}$.

(iii) Supongamos que para $c \in \mathcal{R}$ con la representación (3.3.1), $a_0 = 0$ entonces es claro que $c = a_1 p + a_2 p^2 + \cdots + a_{s-1} p^{s-1} = p(a_1 + a_2 p + \cdots + a_{s-1} p^{s-2})$ así $c \in (p)$. Por otro lado, si $c \in (p)$ entonces existe $c' \in \mathcal{R}$ tal que $c = pc'$ y por lo visto antes c' puede ser representado como en (3.3.1) entonces $c = p(b_0 + b_1 p + \cdots + b_{s-1} p^{s-1}) = b_0 p + b_1 p^2 + \cdots + b_{s-2} p^{s-1}$ renombrando $a_i = b_{i-1}$ tenemos que $c = a_0 + a_1 p + \cdots + a_{s-1} p^{s-1}$ con $a_0 = 0$, por lo tanto, $c \in (p)$ si y sólo si $a_0 = 0$ y finalmente esto implica que $c \notin (p)$ si y sólo si $a_0 \neq 0$. □

Definición 3.3.2. Sean $\mathcal{R} = GR(p^s, p^{sm})$, $\xi \in \mathcal{R}$ un elemento distinto de cero tal que $ord(\xi) = p^m - 1$ y éste es raíz de un polinomio mónico básico primitivo $h(x)$ de grado m en $\mathbb{Z}_{p^s}[x]$ y que divide al polinomio $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$. Llamaremos:

a) El **conjunto de Teichmüller** del anillo $\mathcal{R}$ al conjunto $\tau = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$, y

b) para todo $c \in \mathcal{R}$, la **representación p-ádica** de c a la expresión $c = a_0 + a_1 p + \cdots + a_{s-1} p^{s-1}$ con $a_i \in \{0, 1, \ldots, s-1\}$.

Corolario 3.3.3. *Sea $\mathcal{R} = GR(p^s, p^{sm})$ y sea $c \in \mathcal{R}$ con $c = a_0 + a_1 p + \cdots + a_{s-1} p^{s-1}$ para $a_i \in \tau$. Entonces:*

(i) *Todos los elementos con $a_0 \neq 0$ son unidades y forman un grupo multiplicativo de orden $(p^m - 1)(p^{(s-1)m})$ el cual es producto directo del grupo cíclico $\langle \xi \rangle$ con $o(\langle \xi \rangle) = p^m - 1$ y el grupo abeliano $\varepsilon := \{1 + \pi \mid \pi \in (p)\}$ con $o(\varepsilon) = p^{(s-1)m}$.*

(ii) *El orden de ξ^i para $i \in \{0, 1, \ldots, p^m - 2\}$ es un divisor de $p^m - 1$ y el orden de $1 + \pi$ con $\pi \in (p)$ es un divisor de $p^s - 1$. Un elemento cuyo orden es un divisor de $p^m - 1$ en $\mathcal{R}$ es de la forma ξ^i para $i \in \{0, 1, \ldots, p^m - 2\}$, en particular, un elemento cuyo orden es $p^m - 1$ es de la forma ξ^i para $i \in \{0, 1, \ldots, p^m - 2\}$ tal que $mcd(p^m - 1, i) = 1$ y es raíz de un polinomio mónico básico primitivo de grado m que divide a $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$.*

Todos los elementos $c \in \mathcal{R}$ con $a_0 = 0$ son divisores de cero y forman el ideal (p) en $\mathcal{R}$.

Demostración. (i) Como $\mathcal{R}$ es un anillo finito, por (i) del Lema 1.5.15, sus elementos son divisores de cero o bien unidades, por el Teorema 3.3.1, tenemos que $c \in (p)$ si y sólo si $a_0 = 0$ entonces es claro que $R^* = \{c \in \mathcal{R} \mid a_0 \neq 0\}$, más aún, éste es un grupo abeliano con el producto definido en $\mathcal{R}$. Sea $\varepsilon = \{1 + \pi \mid \pi \in (p)\}$ y considere $1 + \pi_1, 1 + \pi_2 \in \varepsilon$, entonces $(1 + \pi_1)(1 + \pi_2) = 1 + \pi_1 + \pi_2 + \pi_1\pi_2$. Nombrando $\pi = \pi_1 + \pi_2 + \pi_1\pi_2 \in (p)$ tenemos que $(1 + \pi_1)(1 + \pi_2) \in (p)$. Si $x \in (p) \cap \varepsilon$ entonces $x = 1 + \pi$ para algún $\pi \in (p)$ y como $((p), +) \leqslant (\mathcal{R}, +)$ entonces $1 = (1 + \pi) + (-\pi) \in (p)$ lo cual es una contradicción, por lo tanto, $(p) \cap \varepsilon = \emptyset$, esto implica que todos los elementos de ε son unidades, entonces $1 \in \varepsilon$, éste es cerrado bajo producto, todo elemento de él tiene un inverso y tanto la asociatividad como la conmutatividad del producto se heredan de $\mathcal{R}$, por lo tanto, $(\varepsilon, \cdot)$ es un grupo abeliano. Definimos la función, $\phi : (p) \to \varepsilon$ tal que para cada $\pi \in (p)$, $\phi(\pi) = 1 + \pi$.

Veamos que ϕ es una biyección. Considérese, $\pi_1, \pi_2 \in (p)$ tales que $\phi(\pi_1) = \phi(\pi_2)$ entonces $1 + \pi_1 = 1 + \pi_2$, luego $\pi_1 = \pi_2$, así, ϕ es inyectiva. Dado $1 + \pi \in \varepsilon$, basta elegir $\pi \in (p)$ y entonces $\phi(\pi) = 1 + \pi$, por lo tanto, es una biyección, esto implica que $|\varepsilon| = |(p)| = p^{(s-1)m}$, por el Lema 3.2.3. Como ξ es un elemento con $ord(\xi) = p^m - 1$ entonces $\langle \xi \rangle$ es un grupo cíclico de orden $p^m - 1$, además, todos los elementos de $\langle \xi \rangle$ y ε son unidades de $\mathcal{R}^*$ entonces $\langle \xi \rangle, \varepsilon \lhd \mathcal{R}^*$ pues son grupos contenidos en $\mathcal{R}^*$ y éste es un grupo abeliano. Considérese un elemento $c \in \mathcal{R}^*$, entonces $c \notin (p)$, así $c = a_0 + a_1 p + \cdots + a_{s-1} p^{s-1}$ con $a_0 \neq 0$, $a_i \in \tau$ para $i \in \{0, 1, \ldots, s-1\}$, luego, $a_0 = \xi^j$ para $j \in \{0, 1, \ldots, p^m - 2\}$, mientras que para $i \in \{1, 2, \ldots, s-1\}$ es claro que $a_i = 0$ o bien $a_i = \xi^k$ para $k \in \{0, 1, \ldots, p^m - 1\}$ en cualquier caso podemos denotar $a_i = 0 \cdot \xi^j$ o $a_i = \xi^{k-j}\xi^j$, entonces $a_i = b_k \xi^i$ donde $b_k \in \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\} = \tau$ para $k \in \{1, 2, \ldots, s-1\}$, factorizando tenemos que $c = \xi^i(1 + b_1 p + b_2 p^2 + \cdots + b_{s-1} p^{s-1})$, es claro que $p^k \in (p)$ para $k \in \{1, 2, \ldots, s-1\}$ entonces $b_k p^k \in (p)$ así que, nombrando $\pi = b_1 p + b_2 p^2 + \cdots + b_{s-1} p^{s-1}$ tenemos que $c = \xi^i(1 + \pi) \in \langle \xi \rangle \cdot \varepsilon$ entonces $R^* \subseteq \langle \xi \rangle \cdot \varepsilon$ y dado que el producto de unidades es siempre una unidad es claro que $\langle \xi \rangle \cdot \varepsilon \subseteq R^*$ concluimos que $R^* = \langle \xi \rangle \cdot \varepsilon$. Sea $c \in (\langle \xi \rangle \cap \varepsilon) - \{1\}$ entonces $c = \xi^i$ para $i \in \{1 \ldots, p^m - 2\}$ y $c = 1 + \pi$ para $\pi \in (p) - \{0\}$, entonces $\xi^i = 1 + \pi$, luego $\xi^i - 1 = \pi$, así, $\overline{\xi^i - 1} = \overline{0}$ se sigue que $\overline{\xi}^i = \overline{1}$ pero $0 < i < p^m - 1 = ord(\overline{\xi})$ lo cual es una clara contradicción, por lo tanto, $\langle \xi \rangle \cap \varepsilon = \{1\}$, concluimos que $R^* = \langle \xi \rangle \times \varepsilon$ y por el Corolario 1.3.9, $|R^*| = (p^m - 1)(p^{(s-1)m})$.

(ii) Para $\xi^i \in \langle \xi \rangle$, por (i) del Corolario 1.3.7, $ord(\xi^i) \mid o(\langle \xi \rangle) = p^m - 1$. Por otro lado, dado $\pi \in (p)$ existe $r \in \mathcal{R}$ tal que $\pi = pr$ entonces, por el Lema A.1.4, $(1 + pr)^{p^{s-1}} = 1 + p^s t$ con $t \in \mathcal{R}$, pero $Car(\mathcal{R}) = p^s$, así, $(1 + \pi)^{p^{s-1}} = 1$, por lo tanto, $ord(1 + \pi) \mid p^{s-1}$. Sea $c \in \mathcal{R}$ tal que $d = ord(c) \mid p^m - 1$; por la descomposición en producto directo existen $a \in \langle \xi \rangle$ y $b \in \varepsilon$ tales que $c = ab$. Si $m = mcm(n_1, n_2)$, entonces $n_1 \mid m$, $n_2 \mid m$ y, dado $M \in \mathbb{Z}$, tal que, $n_1 \mid M$ y $n_2 \mid M$ entonces $m \mid M$. Sean $n_1 = ord(a)$,$n_2 = ord(b)$ y $m = mcm(n_1, n_2)$, entonces $m = n_1 m_1$ y $m = n_2 m_2$, para algunos $m_1, m_2 \in \mathbb{Z}$. Como $a^m = a^{n_1 m_1} = (a^{n_1})^{m_1} = 1^{m_1} = 1$, análogamente $b^m = (b^{n_2})^{m_2} = 1$ entonces $c^m = (ab)^m = a^m b^m = 1$, es decir, $d = ord(c) \mid m$. Por otro lado, $(ab)^d = c^d = 1$, entonces $a^d b^d = 1$ pues $\mathcal{R}$ es un anillo conmutativo, así, $a^d = b^{-d}$ pero $a^d \in \langle \xi \rangle$ y $b^{-d} \in \varepsilon$, luego $a^d \in \langle \xi \rangle \cap \varepsilon = \{1\}$, en otras palabras, $a^d = 1$ y de manera similar llegamos a que $b^d = 1$, entonces $ord(a) = n_1 \mid d$ y $ord(b) = n_2 \mid d$, por lo anterior, $m \mid d$ y $d \mid m$, por lo tanto, $d = m$. Por (i) de este corolario, como $b \in \varepsilon$, se sigue que, $ord(b) \mid p^{s-1}$ y como $ord(b) \mid mcm(ord(a), ord(b)) = d \mid p^m - 1$ tenemos que $ord(b) \mid mcd(p^m - 1, p^{s-1}) = 1$, por lo tanto, $ord(b) = 1$, esto implica que $b = 1$, así, $c = ab = a = \xi^i$ para $i \in \{0, 1, \ldots, p^m - 2\}$. Supóngase que $ord(c) = p^m - 1$ entonces $ord(c) \mid p^m - 1$ y por lo visto antes $c = \xi^i$ para $i \in \{0, 1, \ldots, p^m - 2\}$, como $\langle \xi \rangle$ es un grupo finito con $o(\langle \xi \rangle) = p^m - 1$ entonces $ord(\xi^i) = (p^m - 1)/mcd(p^m - 1, i)$ se sigue que $mcd(p^m - 1, i) = 1$, aplicando el epimorfismo (2.1.8) tenemos que $\overline{\xi}^i$ es un generador de $\langle \overline{\xi} \rangle = \mathbb{F}_{p^m}^*$ puesto que $mcd(p^m - 1, i) = 1$, entonces es un elemento primitivo de $\mathbb{F}_{p^m}$, por el Corolario 1.8.31, el polinomio mínimo de $\overline{\xi}^i$ es un polinomio primitivo, irreducible de grado m en $\mathbb{F}_p[x]$, entonces $m(x) \mid x^{p^m} - x = x(x^{p^m-1} - 1)$ por el Lema A.2.3. Como $m(x)$ es irreducible, tenemos que $m(x) \mid x$ o

$m(x) \mid x^{p^m-1} - 1$. Si $grad(m(x)) = m = 1$ entonces $m(x) = x - 1$, en este caso se cumple trivialmente que la preimagen $l(x) = x - 1 \in \mathbb{Z}_{p^s}[x]$ divide a $x^{p^m-1} - 1 = x^p - 1$. Por otro lado, si $m > 1$ $m(x) \nmid x$ así, $m(x) \mid x^{p^m-1} - 1$; entonces existe $n(x) \in \mathbb{F}_p[x]$ tal que $m(x)n(x) = x^{p^m-1} - 1$, luego como $x^{p^m-1} - 1$ no tiene raíces múltiples los polinomios $m(x)$ y $n(x)$ son coprimos, entonces por el Lema de Hensel, existen polinomios mónicos $h(x)$ y $l(x)$, tales que $h(x)l(x) = x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$, $\overline{h(x)} = m(x)$, $\overline{l(x)} = n(x)$ y entonces $grad(h(x)) = grad(m(x)) = m$, finalmente por el Lema 3.2.5, como $\overline{\xi}^i$ es una raíz simple de $\overline{h(x)}$ entonces existe un único $\alpha \in \mathcal{R}$ tal que $\overline{\alpha} = \overline{\xi}^i$ se sigue que $\alpha = \xi^i$ entonces $c = \xi^i$ es raíz de un polinomio mónico básico irreducible de grado m tal que $h(x) \mid x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$.
(iii) Se sigue de la segunda parte del teorema anterior. □

EL GRUPO DE UNIDADES DE UN ANILLO DE GALOIS

En la sección anterior, vimos cómo representar a los elementos del anillo $\mathcal{R} = GR(p^s, p^{sm})$ y demostramos que el grupo de unidades de éste es el producto directo de dos grupos, uno de ellos al cual llamaremos G_1 es un grupo cíclico generado por el elemento ξ el cual es de orden $p^m - 1$ y es raíz de un polinomio mónico básico primitivo (e irreducible) de grado $m \in \mathbb{N}$ que divide al polinomio $x_1^{p^m-1}$ en $\mathbb{Z}_{p^s}[x]$, el segundo grupo al cual llamaremos en lo sucesivo G_2 es un grupo abeliano cuyo orden es $p^{(s-1)m}$, en esta sección nos dedicaremos a estudiar las propiedades de éste.

Teorema 3.4.1. *Sea* $\mathcal{R} = GR(p^s, p^{sm})$ *entonces:*

$$\mathcal{R}^* = G_1 \times G_2$$

donde G_1 *es un grupo cíclico de orden* $p^m - 1$ *y* G_2 *es un grupo abeliano de orden* $p^{(s-1)m}$ *tal que:*

(i) *Si* p *es impar o* $p = 2$ *y si* $s \leqslant 2$ *es producto directo de* m *grupos cíclicos cada uno de orden* p^{s-1}.

(ii) *Si* $p = 2$ *y* $s \geqslant 3$, *es producto directo de un grupo cíclico de orden* 2, *un grupo cíclico de orden* 2^{s-2} *y* $m - 1$ *grupos cíclicos, cada uno de orden* 2^{s-1}.

Demostración. Cuando $s = 1$ tenemos que $\mathcal{R} = GR(p, p^m) = \mathbb{F}_{p^m}$ el cual es un campo finito y por el Teorema 1.8.29 su grupo de unidades es cíclico, de orden $p^m - 1$ y está generado por un elemento primitivo $\xi \in \mathbb{F}_{p^m}$, además $p^{(s-1)m} = 1$ entonces $G_1 = \langle \xi \rangle$ y $G_2 = \{1\}$. Ahora supóngase que $s \geqslant 2$. Por el Teorema 3.3.1, $\mathcal{R} = \mathbb{Z}_{p^s}[\xi]$ donde ξ es un elemento distinto de cero, cuyo orden es $p^m - 1$ y es raíz de un polinomio mónico básico primitivo $h(x)$ de grado m que divide a $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$ y así, por el Corolario 3.3.3, tenemos que, $\mathcal{R}^* = G_1 \times G_2$, donde $G_1 = \langle \xi \rangle$ es un grupo cíclico de orden $p^m - 1$ y $G_2 = \{1 + \pi \mid \pi \in (p)\}$ es un grupo abeliano de orden $p^{(s-1)m}$, a continuación para analizar la estructura de G_2 distinguimos los siguientes casos:

(i) p es impar. Note que $1+p\xi^i \in G_2$ pues (p) es un ideal, además tenemos que $(1+p\xi^i)^{p^{s-1}} = 1 + a_1\xi^i + a_2\xi^{2i} + \cdots + a_n\xi^{ni}$, donde, $n = p^{s-1}$, por el Lema A.1.6(i), $p^s = p^{(s-1)+1} \mid a_j$, para $1 \leqslant j \leqslant n$, así, $a_j = 0$ para cada $j \geqslant 1$, por lo tanto, $(1+p\xi^i)^{p^{s-1}} = 1$, con $i \in \{0, 1, \ldots, m-1\}$. Supongamos que para numeros naturales $n_0, n_1, \ldots, n_{m-1} \leqslant p^{s-1}$ se satisface:

$$\prod_{i=0}^{m-1} (1+p\xi^i)^{n_i} = 1 \tag{3.4.1}$$

y luego, para cada $i \in \{0, 1, \ldots, m-1\}$ tenemos:

$$\begin{aligned}(1+p\xi^i)^{n_i} &= \sum_{j=0}^{n_i} \binom{n_i}{j} p^j \xi^{ij} = 1 + pn_i\xi^i + \sum_{j=2}^{n_i} \binom{n_i}{j} p^j \xi^{ij} \\ &= 1 + pn_i\xi^i + \sum_{j=0}^{n_i-2} \binom{n_i}{j+2} p^{j+2} \xi^{i(j+2)}\end{aligned} \tag{3.4.2}$$

como $p^2p^j = p^{j+2}$, tomando para cada $i = 0, 1, \ldots, m-1$, $\sigma_i = \sum_{j=0}^{n_i-2} \binom{n_i}{j+2} p^j \xi^{i(j+2)}$, la suma en (3.4.2), se reduce a la forma $p^2\sigma_i$, luego, sustituyendo ésto en (3.4.1):

$$\begin{aligned}1 = \prod_{i=0}^{m-1} (1+p\xi^i)^{n_i} &= \prod_{i=0}^{m-1} (1 + pn_i\xi^i + p^2\sigma_i) \\ &= (1 + pn_0 + p^2\sigma_0)(1 + pn_1\xi + p^2\sigma_1)\cdots(1 + pn_{m-1}\xi^{m-1} + p^2\sigma_{m-1})\end{aligned}$$

multiplicando de forma concreta tenemos que $\prod_{i=0}^{m-1}(1+p\xi^i)^{n_i} = 1 + pn_0 + pn_1\xi^1 + \cdots + pn_{m-1}\xi^{m-1} + p^2\sigma$ donde $\sigma \in \mathcal{R}$ y nuevamente, por (3.4.1):

$$\begin{aligned} 1 + pn_0 + pn_1\xi^1 + \cdots + pn_{m-1}\xi^{m-1} + p^2\sigma &= 1 \\ pn_0 + pn_1\xi^1 + \cdots + pn_{m-1}\xi^{m-1} + p^2\sigma &= 0 \\ p\left(n_0 + n_1\xi^1 + \cdots + n_{m-1}\xi^{m-1} + p\sigma\right) &= 0 \\ p\left(\sum_{i=0}^{m-1} n_i\xi^i + p\sigma\right) &= 0 \end{aligned} \tag{3.4.3}$$

es decir, $\sum_{i=0}^{m-1} n_i\xi^i + p\sigma$ es un divisor de cero, así, pertenece al ideal maximal, $(p) = \ker(-)$, entonces, aplicando el epimorfismo (2.1.8) a dicha suma, se consigue que $\overline{\sum_{i=0}^{m-1} n_i\xi^i + p\sigma} = \overline{0}$, como éste es un homomorfismo se sigue que, $\sum_{i=0}^{m-1} \overline{n_i}\,\overline{\xi}^i = \overline{0}$ y se llega a la expresión $a_0 + a_1\overline{\xi} + \cdots + a_{m-1}\overline{\xi}^{m-1} = \overline{0}$ donde $a_i = \overline{n_i}$ para $i \in \{0, 1, \ldots, m-1\}$. Considérese el polinomio $l(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}[x]$, por lo anterior, se tiene que, $\overline{\xi} \in \mathbb{F}_{p^m}$ es raíz de $l(x)$ en $\mathbb{F}_{p^m}$. Si $l(x) \neq 0$, dado que el polinomio mínimo de $\overline{\xi}$ es de grado m en $\mathbb{F}_p[x]$, se llega a una contradicción. Luego, ocurrre que $l(x) = 0$, así, $\overline{n_i} = \overline{0}$, por consiguiente, $p \mid n_i$, para cada $i = 0, 1, \ldots, m-1$. Sea $e \in \mathbb{N}$ tal que $p^{e+1} \mid n_i$ pero $p^{e+2} \nmid n_i$, entonces $n_i = p^{e+1}r_i$ con $mcd(p, r_i) = 1$ y por (i) del Lema A.1.6, $p^{e+3} \mid \sum_{j=2}^{n_i} \binom{n_i}{j} p^j$

con $i \in \{0, 1, \ldots, m-1\}$; entonces: $(1+p\xi^i)^{n_i} = 1 + p^{e+2}r_i\xi^i + p^{e+3}\alpha_i$, para algún $\alpha_i \in \mathcal{R}$, y sustituyendo en (3.4.1), el producto $\prod_{i=0}^{m-1}(1 + p^{e+2}r_i\xi^i + p^{e+3}\sigma_i)$ se convierte en,

$$(1+p^{e+2}r_0+p^{e+3}\sigma_0)(1+p^{e+2}r_1\xi+p^{e+3}\sigma_1)\cdots(1+p^{e+2}r_{m-1}\xi^{m-1}+p^{e+3}\sigma_{m-1}) = 1$$

, lo cual, multiplicando de forma concreta, se convierte, para algún $\alpha \in \mathcal{R}$ en:

$$\begin{aligned}
1 &= 1 + p^{e+2}r_0 + p^{e+2}r_1\xi + p^{e+2}r_2\xi^2 + \cdots + p^{e+2}r_{m-1}\xi^{m-1} + p^{e+3}\alpha \\
0 &= p^{e+2}r_0 + p^{e+2}r_1\xi + p^{e+2}r_2\xi^2 + \cdots + p^{e+2}r_{m-1}\xi^{m-1} + p^{e+3}\alpha \\
0 &= p^{e+2}\left(r_0 + r_1\xi + r_2\xi^2 + \cdots + r_{m-1}\xi^{m-1} + p\alpha\right) \\
0 &= p^{e+2}\left(\sum_{i=0}^{m-1} r_i\xi^i + p\alpha\right) \qquad (3.4.4)
\end{aligned}$$

, entonces $\sum_{i=0}^{m-1} r_i\xi^i + p\alpha \in (p)$, aplicando el epimorfismo (2.1.8) se consigue,

$$\sum_{i=0}^{m-1} \overline{r_i}\overline{\xi}^i = \overline{0}. \qquad (3.4.5)$$

Como $n_i \leqslant p^{s-1}$ y $p^{e+1} \mid n_i$, entonces $e+1 \leqslant s-1$, es decir, $e+2 \leqslant s$. Si $e+2 \neq s$, de la expresión (3.4.5) y que el polinomio mínimo de $\overline{\xi}$ es de grado m, tenemos que $\overline{r_i} = \overline{0}$, lo cual implica que, $r_i \in (p)$, pero, $\mathrm{mcd}(p, r_i) = 1$, claramente, una contradicción. Entonces, $e+2 = s$, luego, $e+1 = s-1$, así, $p^{s-1} \mid n_i$ y $n_i \leqslant p^{s-1}$; se concluye que, $n_i = p^{s-1}$. Además, ya habíamos visto que $(1+p\xi^i)^{p^{s-1}} = 1$ y mostramos que la única forma de obtener a la unidad como producto de potencias de elementos de ésta forma es si todos son 1, más aún, el entero positivo mínimo que satisface $(1+p\xi^i)^{n_i} = 1$ es p^{s-1}, en otras palabras, $\mathrm{ord}(1+p\xi^i) = p^{s-1}$, para $i \in \{0, 1, \ldots, m-1\}$. Sea $H_i = \langle 1+p\xi^i\rangle$ para cada $i \in \{0, 1, \ldots, m-1\}$, entonces $H_i \lhd G_2$ y $|H_i| = p^{s-1}$ pues es un grupo cíclico con generador de orden p^{s-1}. Si consideramos $c \in H_i \cap (H_1H_2\cdots H_{i-1}H_{i+1}\cdots H_{m-1})$, existen enteros $n, n_0, n_1, \ldots, n_{i-1}, n_{i+1}, \ldots, n_{m-1} \leqslant p^{s-1}$ tales que:

$$\begin{aligned}
(1+p\xi^i)^n &= (1+p)^{n_0}\cdots(1+p\xi^{i-1})^{n_{i-1}}(1+p\xi^{i+1})^{n_{i+1}}\cdots(1+p\xi^{m-1})^{n_{m-1}} \\
1 &= (1+p)^{n_0}\cdots(1+p\xi^{i-1})^{n_{i-1}}(1+p\xi^i)^{-n}(1+p\xi^{i+1})^{n_{i+1}}\cdots(1+p\xi^{m-1})^{n_{m-1}} \\
1 &= (1+p)^{n_0}\cdots(1+p\xi^{i-1})^{n_{i-1}}(1+p\xi^i)^{n_i}(1+p\xi^{i+1})^{n_{i+1}}\cdots(1+p\xi^{m-1})^{n_{m-1}}
\end{aligned}$$

donde, tomando $n_i = n$ lo anterior equivale a: $\prod_{i=0}^{m-1}(1+p\xi^i)^{n_i} = 1$ con $n_i \leqslant p^{s-1}$ para $i \in \{0, 1, \ldots, m-1\}$ en cuyo caso demostramos que $n_i = p^{s-1}$ y así, $c = (1+p\xi^i)^{p^{s-1}} = 1$, por consiguiente, $H_i \cap (H_1H_2\cdots H_{i-1}H_{i+1}\cdots H_{m-1}) = \{1\}$, por el Corolario 1.3.9, $\left|\prod_{i=0}^{m-1}\langle 1+p\xi^i\rangle\right| = \prod_{i=0}^{m-1} p^{(s-1)} = p^{(s-1)m} = o(G_2)$ entonces $G_2 = H_1H_2\cdots H_{m-1}$ y por la Definición 1.3.8, concluimos, $G_2 = \prod_{i=0}^{m-1}\langle 1+p\xi^i\rangle$.

(ii) $p = 2$, $s = 2$. En este caso, $\mathcal{R} = GR(4, 4^m)$, así, $o(G_2) = p^{(s-1)m} = 2^m$, entonces para todo elemento $g = 1+2\pi \in G_2$, tenemos que, $(1+2\pi)^2 = 1+4\pi+4\pi^2 = 1$, por lo tanto, $\mathrm{ord}(g) = 2$ para todo $g \in G_2$. Si $m = 1$ el orden de $G_2 = 2$ entonces G_2 es cíclico

y es producto directo de $m = 1$ grupos de orden $2^{s-1} = 2$. Por otro lado, si $m \geqslant 2$ considérense g_1, g_2 tales que $g_1 \neq 1$, $g_2 \neq 1$ y $g_1 \neq g_2$ esto es posible ya que $2^m \geqslant 4$, entonces $\langle g_1 \rangle$ y $\langle g_2 \rangle$ son dos subgrupos de orden $p = 2$, y además $\langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$, de lo contrario, $g_1 = g_2$ lo cual no ocurre, por (b) del Teorema 1.4.5, G_2 no es cíclico, así, por (c) del mismo teorema $G_2 = H \times \langle g_0 \rangle$ donde $o(\langle g_0 \rangle) = 2$, entonces $o(H) = 2^{m-1}$, y procediendo de esta manera se consigue que, $G_2 = \prod_{i=0}^{m-1} \langle g_i \rangle$

(iii) $p = 2, s \geqslant 3$. Considere el conjunto $N = \{\overline{a}^2 + \overline{a} \mid \overline{a} \in \mathbb{F}_{2^m}\} \subseteq \overline{\mathcal{R}}$, entonces dados $x, y \in N$ existen $a, b \in \mathbb{F}_{2^m}$ tales que $x = \overline{a}^2 + \overline{a}$, $y = \overline{b}^2 + \overline{b}$, es claro que, $x + y = \overline{a}^2 + \overline{a} + \overline{b}^2 + \overline{b} = \left(\overline{a}^2 + \overline{b}^2\right) + (\overline{a} + \overline{b})$. Como $Car(\mathbb{F}_{2^m}) = 2$, se sigue que, dados $\alpha, \beta \in \mathbb{F}_{2^m}$, luego, $\alpha^2 + \beta^2 = (\alpha + \beta)^2$ y $\alpha = -\alpha$. Si $\overline{c} = \overline{a} + \overline{b}$, entonces $x + y = \overline{c}^2 + \overline{c} \in N$, por consiguiente, $x - y \in N$, es decir, $(N, +) \lhd (\mathbb{F}_{2^m}, +)$, pues, $(\mathbb{F}_{2^m}, +)$ es un grupo abeliano. Considérese la función:

$$\begin{aligned} \phi : \mathbb{F}_{2^m} &\longrightarrow N \\ \overline{a} &\longmapsto \overline{a}^2 + \overline{a} \end{aligned}$$

Sean $\overline{a}, \overline{b} \in \mathbb{F}_{2^m}$, así $\phi\left(\overline{a} + \overline{b}\right) = \left(\overline{a} + \overline{b}\right)^2 + (\overline{a} + \overline{b}) = (\overline{a}^2 + \overline{a}) + (\overline{b}^2 + \overline{b}) = \phi(\overline{a}) + \phi(\overline{b})$ es decir, ϕ es un homomorfismo de grupos y por su forma es un epimorfismo, así, $Im\phi = N$ y $\ker \phi \lhd \mathbb{F}_{2^m}$. Luego, para $\overline{a} \in \ker \phi$ tenemos que $\overline{a}^2 + \overline{a} = \phi(\overline{a}) = \overline{0}$, entonces $\overline{a}(\overline{a} + \overline{1}) = 0$, luego, $\overline{a} = \overline{0}$, o bien, $\overline{a} = \overline{1}$, pues $\mathbb{F}_{2^m}$ es un dominio entero de característica 2, entonces, $ker\phi = \{\overline{0}, \overline{1}\}$. Por (ii) del Teorema 1.2.9, $|\mathbb{F}_{2^m}/ker\,\phi| = |Im\phi|$, luego, por el Teorema 1.3.5 $o(\ker \phi) \mid o(\mathbb{F}_{2^m})$, es decir, $|\mathbb{F}_{2^m}|/|ker\phi| = |Im\phi|$, por consiguiente, $|\mathbb{F}_{2^m}|/|Im\phi| = |\ker \phi| = 2$. Como se dijo antes, $Im\phi = N$, entonces, $[\mathbb{F}_{2^m} : N] = 2$, así, $N \neq \emptyset$ y existe $\overline{b} \in \mathbb{F}_{2^m} - N$. Como (2.1.8) es un epimorfismo elegimos $b \in \mathcal{R}$ una preimagen de este elemento. Por el Teorema 3.3.1, en $\mathcal{R} = GR(2^s, 2^{sm})$ existe un elemento ξ distinto de cero de orden $2^m - 1$, raíz de un polinomio mónico básico primitivo de grado m y que divide a $x^{2^m-1} - 1$ en $\mathbb{Z}_{2^s}[x]$ y, $\mathcal{R} = \mathbb{Z}_{2^s}[\xi]$, es decir, dado $\alpha \in \mathcal{R}$; $\alpha = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}$ con $a_i \in \mathbb{Z}_{2^s}$, para $i \in \{0, 1, \ldots, m-1\}$. Considérense los elementos $(1 + 2 + 2^2 + \cdots + 2^{s-1})$, $1 + 2\xi^i$ con $i \in \{1, 2, \ldots, m-1\}$ y $1 + 4b \in \mathcal{R}$ los cuales pertenecen a G_2. Renombrando $\alpha = 1 + 2 + 2^2 + \cdots + 2^{s-1}$, tenemos que $2\alpha = 2 + 2^2 + 2^3 + \cdots + 2^{s-1}$, así,

$$\begin{aligned} 2\alpha - \alpha &= 2 + 2^2 + 2^3 + \cdots + 2^{s-1} - (1 + 2 + 2^2 + \cdots + 2^{s-1}) \\ \alpha &= 2 + 2^2 + 2^3 + \cdots + 2^{s-1} - 1 - 2 - 2^2 - 2^3 - \cdots - 2^{s-1} \\ \alpha &= -1 \end{aligned}$$

tenemos pues que $\alpha^2 = 1$, es decir, $(1 + 2 + 2^2 + \cdots + 2^{s-1})^2 = 1$, usando (ii) y (iii) del Lema A.1.6, tenemos que $(1 + 2\xi^i)^{2^{s-1}} = 1$ y $(1 + 4b)^{2^{s-2}} = 1$. Supóngase como se hizo al inicio de esta prueba que, para números naturales $n_0 \leqslant 2, n_1, \ldots, n_{m-1} \leqslant 2^{s-1}, n \leqslant 2^{s-2}$, se cumple que,

$$(1 + 2 + 2^2 + \cdots + 2^{2-1})^{n_0} \prod_{i=1}^{m-1} (1 + 2\xi^i)^{n_i} (1 + 4b)^n = 1 \tag{3.4.6}$$

como se vió en (3.4.2), la expresión no depende del valor de p entonces el desarrollo es similar para $(1 + 2\xi^i)^{n_i}$ con $i \in \{1, 2, \ldots, m-1\}$, es decir, $(1 + 2\xi^i)^{n_i} = 1 + 2n_i\xi^i + 4c_i$,

$(1+4b)^n = 1+4nb+8c$ para algunos $c, c_i \in \mathcal{R}$ con $i \in \{1,2,\dots,m-1\}$. Si $n_0 = 1$ entonces, (3.4.6) se convierte en:

$$\begin{aligned}
1 &= (1+2+2^2+\cdots+2^{s-1}) \prod_{i=1}^{m-1} (1+2n_i\xi^i+4c_i)(1+4nb+8c) \\
1 &= (1+2+4(1+2+\cdots+2^{s-3})) \prod_{i=1}^{m-1} (1+2n_i\xi^i+4c_i)(1+4nb+8c) \\
1 &= (1+2n_0\xi^0+4c') \left(1+2\sum_{i=1}^{m-1} n_i\xi^i+4c''\right)(1+4nb+8c) \\
1 &= 1+2\sum_{i=0}^{m-1} n_i\xi^i+4d \\
0 &= 2\left(\sum_{i=0}^{m-1} n_i\xi^i+2d\right)
\end{aligned} \tag{3.4.7}$$

con $c' = 1+2+\cdots+2^{s-3}$ y algunos $c'', d \in \mathcal{R}$, los cuales se obtienen al multiplicar de manera concreta a lo largo de, (3.4.7), igual que antes, tenemos que, $\sum_{i=0}^{m-1} n_i\xi^i + 2d \in (2)$, así, aplicando el (2.1.8), tenemos que, $\sum_{i=1}^{m-1} \overline{n_i}\overline{\xi}^i = 0$, nuevamente, ya que el polinomio mínimo de $\overline{\xi}$ es de grado m, $\overline{n_0} = 0$, es decir, $2 \mid n_0$ y $n_0 = 1$, una contradicción, por lo tanto, $n_0 = 2$, así, (3.4.6), se reduce a, $\prod_{i=1}^{m-1}(1+2\xi^i)^{n_i}(1+4b)^n = 1$, procediendo de la misma manera, se tiene que, $\sum_{i=1}^{m-1} \overline{n_i}\overline{\xi}^i = 0$, es decir, $2 \mid n_i$ para $i \in \{1,2,\dots,m-1\}$. Sea $e \in \mathbb{N}$ tal que $2^{e+1} \mid n_i$ y $2^{e+1} \mid 2n$, entonces $n = 2^e r$ y $n_i = 2^{e+1}r_i$, usando nuevamente (ii) y (iii) del Lema A.1.6 con $e+1$ en lugar de e, tenemos que, $(1+2\xi^i)^{n_i} = 1+2n_i\xi^i+\binom{n_i}{2}2^2\xi^{2i}+2^{e+3}c_i$ y $(1+4b)^n = 1+4nb+2^{e+3}c$. Como $\binom{n_i}{2}2^2 = \left(2^2 n_i!\right)/\left((2)!(n_i-1)!\right) = 2(n_i)(n_i-1) = (2^{e+2}r_i)(2^{e+1}r_i-1)$, entonces $(1+2\xi^i)^{n_i} = 1+2^{e+2}r_i\xi^i+(2^{e+2}r_i)(2^{e+1}r_i-1)\xi^{2i}+2^{e+3}c_i$, así,

$$\begin{aligned}
\prod_{i=1}^{m-1} \left[1+2^{e+2}r_i\xi^i+(2^{e+2}r_i)(2^{e+1}r_i-1)\xi^{2i}+2^{e+3}c_i\right](1+4nb+2^{e+3}c) &= 1 \\
1+2^{e+2}\sum_{i=1}^{m-1}\left(r_i\xi^i+r_i(2^{e+1}r_i-1)\xi^{2i}\right)+2^{e+2}rb+2^{e+3}c &= 1 \\
2^{e+2}\left[\sum_{i=1}^{m-1}\left(r_i\xi^i+r_i(2^{e+1}r_i-1)\xi^{2i}\right)+rb+2c\right] &= 0
\end{aligned}$$

procediendo como antes, tenemos que, $e \leqslant s-2$ y si $e < s-2$ entonces $e+2 < s$ así, $\sum_{i=1}^{m-1}\left(r_i\xi^i+r_i(2^{e+1}r_i-1)\xi^{2i}\right)+rb+2c \in (p)$ y aplicando el epimorfismo (2.1.8) tenemos que $\sum_{i=1}^{m-1}\left(\overline{r_i}\overline{\xi}^i-\overline{r_i}\overline{\xi}^{2i}\right)+\overline{r}\,\overline{b} = \overline{0}$. Ya que para todo $i \in \{0,1,\dots,m-1\}$, $\overline{r_i}, \overline{r} \in \mathbb{F}_2 = \{\overline{0},\overline{1}\}$, si $\overline{r} = \overline{1}$ entonces $\overline{b} = \sum_{i=1}^{m-1}\left(\overline{r_i}\overline{\xi}^i-\overline{r_i}\overline{\xi}^{2i}\right)$, como $\overline{r_i} = \overline{r_i}^2$, se

sigue que, $\overline{b} = \sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i - \sum_{i=1}^{m-1} \overline{r_i}^2\overline{\xi}^{2i}$ y como $Car(\mathbb{F}_2) = 2$ tenemos que, $\overline{b} = \sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i - \left[\sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i\right]^2 \in N$ pero esto contradice que $\overline{b} \notin N$, por lo tanto, $\overline{r} = \overline{0}$, así,

$$\begin{aligned}\sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i - \left[\sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i\right]^2 &= 0\\ \sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i \left[1 - \sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i\right] &= 0\end{aligned}$$

entonces $\sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i = 0$, o bien, $1 - \sum_{i=1}^{m-1} \overline{r_i}\overline{\xi}^i = 0$ las cuales contradicen el hecho de que el polinomio mínimo de $\overline{\xi}$ sobre $\mathbb{F}_2$ es de grado m, luego se concluye que, $e = s-2$, entonces $n = 2^{s-2}r$, $n_i = 2^{s-1}r_i$, pero $2 \leqslant 2^{s-2}$ y $n \leqslant 2^{s-2}$, por lo tanto, $n_0 = 2$, $n_i = 2^{s-1}$ y $n = 2^{s-2}$. Finalmente definimos $H_0 = \langle 1 + 2 + \cdots + 2^{s-1}\rangle$, $H = \langle 1 + 4b\rangle$ y para $i \in \{1, 2, \ldots, m-1\}$; $H_i = \langle 1 + 2\xi^i\rangle$, análogamente al primer caso de esta demostración, $H_0, H_i, H \lhd G_2$, la intersección de cada H_i y el producto de los restantes es $\{1\}$ y $|H_0(H_1H_2\cdots H_{m-1})H| = |H_0||H_1H_2\cdots H_{m-1}||H| = (2)(2^{(m-1)(s-1)})(2^{s-2}) = 2^{m(s-1)} = o(G_2)$, por lo tanto, $G_2 = H_0 \times H_1 \times \cdots \times H_{m-1} \times H$. □

EXTENSIONES EN ANILLOS DE GALOIS

Ya hemos analizado la construcción del anillo de Galois $GR(p^s, p^{sm})$ a tráves del anillo de polinomios $\mathbb{Z}_{p^s}[x]$, en esta sección hablaremos de la construcción de anillos de Galois como extensiones de otros anillos de Galois.

Definición 3.5.1. Sean R y R' anillos, diremos que R' es una extensión del anillo R si y sólo si $R \subseteq R'$, es decir, R es una extensión de todos sus subanillos.

Teorema 3.5.2. *Sean $\mathcal{R}' = GR(p^s, p^{sn})$ y $\mathcal{R} = GR(p^s, p^{sm})$. Si $\mathcal{R}'$ es una extensión del anillo $\mathcal{R}$ entonces $m \mid n$.*

Demostración. Considérese la función $- : \mathcal{R}' \longrightarrow \mathcal{R}'/(p)$ donde (p) es el ideal generado por cero y todos los divisores de cero de $\mathcal{R}'$, así, $\ker - = (p)$, por el Teorema 1.7.11, $\mathcal{R} + (p)$ es un subanillo de $\mathcal{R}'$ y $(p) \leqslant \mathcal{R} + (p)$. Como $\mathcal{R} = GR(p^s, p^{sm})$, cero y los divisores de cero del anillo forman un ideal principal, llamemósle $(p)'$ y demostraremos que $(p)' = \mathcal{R} \cap (p)$. Si $x \in (p)' \subseteq \mathcal{R}$ entonces existe $r' \in \mathcal{R}$ tal que $x = pr'$, pero $\mathcal{R} \subseteq \mathcal{R}'$ entonces $x = pr'$, para algún $r' \in \mathcal{R}'$, así, $x \in (p)$, por lo tanto, $x \in \mathcal{R} \cap (p)$. Por otro lado, si $x \in \mathcal{R} \cap (p)$ entonces $x \in \mathcal{R}$ y existe un $r \in \mathcal{R}'$ tal que $x = pr$, luego, $p^{s-1}x = p^{s-1}(pr) = 0$ entonces x es un divisor de cero de $\mathcal{R}$ o $x = 0$, entonces $x \in (p)'$, por lo tanto $(p)' = \mathcal{R} \cap (p)$. Por (iii) del Teorema 1.7.11, tenemos que, $\mathcal{R} + (p)/(p)$ es isomorfo a $\mathcal{R}/(p)'$ y éste, a su vez, es isomorfo a $\mathbb{F}_{p^m}$. Dado que $\mathcal{R} \subseteq \mathcal{R}'$, $(p) \leqslant \mathcal{R}'$ y $(p) \leqslant \mathcal{R} + (p)$ entonces, $\mathcal{R} + (p)'/(p)' \subseteq \mathcal{R}'/(p)$ pero éste último es isomorfo $\mathbb{F}_{p^n}$, por lo tanto, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, es decir, $m \mid n$. □

Teorema 3.5.3. *Sea $\mathcal{R} = GR(p^s, p^{sm})$ con $m \mid n$ para $n \in \mathbb{N}$. Entonces existe un anillo de Galois $\mathcal{R}' \simeq GR(p^s, p^{sn})$ tal que $\mathcal{R} \subseteq \mathcal{R}'$.*

Demostración. Como $n \in \mathbb{N}$ existe $h_n(x) \in \mathbb{Z}_{p^s}[x]$ polinomio mónico básico primitivo de grado n y así, nombrando $\mathcal{R}' = \mathbb{Z}_{p^s}[x]/\langle h_n(x)\rangle$ éste es isomorfo a $GR(p^s, p^{sn})$. Por otro lado, tenemos que $\mathcal{R} = GR(p^s, p^{sm}) \simeq \mathbb{Z}_{p^s}[x]/\langle h_m(x)\rangle$ donde $h_m(x)$ es un polinomio mónico básico primitivo de grado m en $\mathbb{Z}_{p^s}[x]$, por el Teorema 3.3.1, existen elementos $\xi_1 \in \mathcal{R}$ y $\xi_2 \in \mathcal{R}'$ raíces de polinomios mónicos básicos primitivos de grados m y n respectivamente, $\mathcal{R} = \mathbb{Z}_{p^s}[\xi_1]$ y $\mathcal{R}' = \mathbb{Z}_{p^s}[\xi_2]$, luego, aplicando el epimorfismo $-$ tenemos que $\overline{\mathbb{Z}_{p^s}[\xi_1]} = \mathbb{F}_{p^m}$ y $\overline{\mathbb{Z}_{p^s}[\xi_2]} = \mathbb{F}_{p^n}$, como $m \mid n$ entonces $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, finalmente, al ser $-$ un epimorfismo es claro que las preimágenes de los campos finitos preservan la contención. Así, podemos concluir que $\mathcal{R} \subseteq \mathcal{R}'$. □

La existencia de las extensiones de un anillo de Galois, nos permiten generalizar los resultados estudiados en las secciones previas, sin embargo, una propiedad muy importante de las extensiones de un anillo de Galios, es la unicidad.

Corolario 3.5.4. *Sean $\mathcal{R}' = GR(p^s, p^{sn})$ y $m \in \mathbb{N}$, tal que $m \mid n$ entonces, existe un único anillo de Galois $\mathcal{R} = GR(p^s, p^{sm})$ tal que $\mathcal{R} \subseteq \mathcal{R}'$.*

Demostración. Ya hemos visto que para $m \in \mathbb{N}$ existe $\mathcal{R} = GR(p^s, p^{sm})$ y por hipótesis suponga que $n = ml$, por el Teorema 3.5.3 existe un anillo de Galois $\mathcal{R}' = GR(p^s, p^{sml})$ tal que $\mathcal{R} \subseteq \mathcal{R}'$, se sigue de $n = ml$ que $\mathcal{R}' \simeq GR(p^s, p^{sn})$. Suponga que existe otro anillo $\mathcal{R}'' \simeq GR(p^s, p^{sm})$ tal que $\mathcal{R}'' \subseteq \mathcal{R}'$, por el Teorema 3.3.1 existen elementos $\eta \in \mathcal{R}$ y $\zeta \in \mathcal{R}''$ distintos de cero cuyo orden es $p^m - 1$ y que son raíces de polinomios mónicos básicos irreducibles de grado m y que dividen a $x^{p^m-1} - 1$ en $\mathbb{Z}_{p^s}[x]$, así, $\mathcal{R} = \{a_0 + a_1 p + \cdots + a_{s-1}p^{s-1} \mid a_i \in \tau_0, \text{ con } i \in \{0, 1, \ldots, m-1\}\}$ y $\mathcal{R}'' = \{b_0 + b_1 p + \cdots + b_{s-1}p^{s-1} \mid b_i \in \tau_1, \text{ con } i \in \{0, 1, \ldots, m-1\}\}$, para los cuales se tiene que, $\tau_0 = \{0, 1, \eta, \eta^2, \ldots, \eta^{p^m-2}\}$ y $\tau_1 = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^m-2}\}$. Como $\mathcal{R}'^*$ es un grupo finito, tiene un único subgrupo G cuyo orden es $p^n - 1$ y dado que $m \mid n$, $p^m - 1 \mid p^n - 1$, así, existe un único $H \leqslant G$ con $o(H) = p^m - 1$. De lo anterior, se sigue que, $o(\langle\eta\rangle) = o(\langle\zeta\rangle) = p^m - 1 = o(H)$, por lo tanto, $\langle\eta\rangle = \langle\zeta\rangle$, entonces $\eta = \zeta^i$ para $i \in \{0, 1, \ldots, p^m - 2\}$ con $mcd(p^m - 1, i) = 1$, por consiguiente, $\tau_0 = \tau_1$ y en consecuencia $\mathcal{R} = \mathcal{R}''$. □

Hemos demostrado la existencia y la unicidad de extensiones del anillo de Galois $GR(p^s, p^{sm})$ para cada entero que tenga a m como divisor propio, en vista de esto, podemos extender las propiedades de nuestro anillo de Galois, sin embargo antes de continuar caracterizaremos los ideales de un anillo de Galois en paralelismo con el Teorema 2.1.5

Teorema 3.5.5. *Sea $\mathcal{R} = GR(p^s, p^{sm})$, los ideales $(0), (1), (p), (p^2), \ldots, (p^{s-1})$ son los únicos ideales de $\mathcal{R}$, (p) es el único ideal maximal de $\mathcal{R}$ y $\mathcal{R}/(p) \simeq \mathbb{F}_{p^m}$.*

Demostración. Sean $I \leqslant \mathcal{R}$ con $I \neq (0)$ y $c \in I$. Por (i) del Teorema 3.3.1, $c = a_0 + a_1 p + \cdots + a_{s-1}p^{s-1}$. Si $a_0 \neq 0$ entonces c es una unidad de ser así $I = \mathcal{R} = (1)$, por el contrario, si $a_0 = 0$ entonces podemos elegir $j = \min\{i \in \{1, 2, \ldots, s-1\} \mid a_i \neq 0\}$, luego, $c = p^j(a_j + a_{j+1}p + \cdots + a_{s-1}p^{s-j-1})$, así, $c \in (p^j)$, entonces $I \subseteq (p^j)$, ahora como $a_j \neq 0$ el elemento $r = a_j + a_{j+1}p + \cdots + a_{s-1}p^{s-j-1}$ es una unidad de $\mathcal{R}$, sea pues r^{-1} su inverso así tenemos que $cr^{-1} = p^j r r^{-1} = p^j$ como I es un ideal, $p^j = cr^{-1} \in I$ entonces $p^j \in I$, luego, $(p^j) \subseteq I$, concluimos que $I = (p^j)$ para algún $j \in \{0, 1, \ldots, s-1\}$, como tenemos la cadena descendente $(0) \subseteq (p^{s-1}) \subseteq (p^{s-2}) \subseteq \cdots \subseteq (p^2) \subseteq (p) \subseteq$

$(1) = \mathcal{R}$ se tiene que (p) es maximal. Ahora bien, sea M un ideal maximal de $\mathcal{R}$ entonces $M \neq R$ y por lo demostrado antes existe $i \in \{1, 2, \ldots, s-1\}$ tal que $M = (p^i)$ entonces $M = (p^i) \subseteq (p) \subseteq \mathcal{R}$, y por la maximalidad de M tenemos que $M = (p)$, de manera inmediata se sigue que $\mathcal{R}/(p) \simeq \mathbb{F}_{p^m}$. □

En el teorema previo, hemos encontrado una similitud entre los ideales de un anillo de Galois y los ideales del anillo $\mathbb{Z}_{p^s}$, esto nos permite extender resultados demostrados en $\mathbb{Z}_{p^s}$, ahora, para un anillo de Galois. Podemos también, contemplar el epimorfismo (2.1.7), como el epimorfismo natural entre $\mathcal{R}$ y $\mathcal{R}/(p) = \mathbb{F}_{p^m}$ y denotárlo mediante "-" como a (2.1.8), incluso podemos referirnos a éste cuando sea conveniente. Además, se define el anillo de polinomios en la indeterminada x con coeficientes en $\mathcal{R}$ como se hizo antes para cualquier anillo $\mathcal{R}[x]$, así, de manera equivalente a los Teoremas 2.1.11, 2.1.12 y el Lema 2.2.2 tenemos:

Teorema 3.5.6. *El ideal $(p)[x] = p\mathcal{R}[x]$ del anillo $\mathcal{R}[x]$ es primo, todo ideal primo de $\mathcal{R}[x]$ contiene a $(p)[x]$ y si lo contiene propiamente entonces es maximal.*

Teorema 3.5.7. *Sea $Q \leqslant \mathcal{R}[x]$.*

i) Si Q es un ideal primario de $\mathcal{R}[x]$ entonces $\sqrt{Q}$ es un ideal primo.

ii) $(p)[x] \subseteq \sqrt{Q}$

iii) Si $\sqrt{Q}$ es un ideal primo que contiene a $(p)[x]$ propiamente, entonces Q es primario.

Lema 3.5.8. *Sea $f(x)$ un polinomio en $\mathcal{R}[x]$ y suponga que $\overline{f}(x) = (\overline{g}(x))^l$ donde $\overline{g}(x)$ es un polinomio irreducible en $\mathbb{F}_{p^m}[x]$ y $l \in \mathbb{N}$. Entonces $\langle f(x) \rangle$ es un ideal primario en $\mathcal{R}[x]$.*

Las demostraciones de estos teoremas y lema son iguales a las desarrolladas en sus análogos y se omiten. También podemos extender conceptos como divisibilidad, coprimalidad y otros entre polinomios al anillo de polinomios $\mathcal{R}[x]$, de la siguiente manera:

Definición 3.5.9. Sean $f(x), g(x) \in \mathcal{R}[x]$ diremos que:

1. $g(x)$ **divide** a $f(x)$ si existe $h(x) \in \mathcal{R}[x]$ tal que $f(x) = g(x)h(x)$ y denotaremos esto por $g(x) \mid f(x)$.

2. $f(x)$ y $g(x)$ son **coprimos** en $\mathcal{R}[x]$ si se satisface que $f(x)\mathcal{R}[x] + g(x)\mathcal{R}[x] = \mathcal{R}[x]$, donde $f(x)\mathcal{R}[x], g(x)\mathcal{R}[x]$ son los ideales principales de $\mathcal{R}[x]$ generados por $f(x)$ y $g(x)$ respectivamente.

3. $f(x)$ es un polinomio **primario** en $\mathcal{R}[x]$ si el ideal $f(x)\mathcal{R}[x]$ es un ideal primario de $\mathcal{R}[x]$.

En vista de la definición anterior tenemos el siguiente:

Lema 3.5.10. *Sean $f_1(x), f_2(x) \in \mathcal{R}[x]$. Entonces $f_1(x)$ y $f_2(x)$ son coprimos en $\mathcal{R}[x]$ si y sólo si $\overline{f_1}(x)$ y $\overline{f_2}(x)$ son coprimos en $\mathbb{F}_{p^m}[x]$.*

Una generalización para el **Lema de Hensel** está dada por:

Lema 3.5.11 (de Hensel). *Sea* $f(x)$ *un polinomio mónico en* $\mathcal{R}[x]$ *y suponga que* $\overline{f}(x) = g_1(x)g_2(x)\cdots g_r(x)$, *para* $g_1(x), g_2(x), \ldots, g_r(x)$ *polinomios mónicos, coprimos por pares en* $\overline{\mathcal{R}}[x] = \mathbb{F}_{p^m}[x]$. *Entonces existen polinomios mónicos coprimos por pares* $f_1(x), f_2(x), \ldots, f_r(x) \in \mathcal{R}[x]$ *tales que:*

$$f(x) = f_1(x)f_2(x)\cdots f_r(x)$$

y $\overline{f_i}(x) = g_i(x)$ *para cada* $i \in \{1, 2, \ldots, r\}$.

También, análogo a nuestro teorema de factorización única tenemos:

Teorema 3.5.12. *Sea* $f(x)$ *un polinomio mónico de grado* $l \geqslant 1$ *en* $\mathcal{R}[x]$. *Entonces:*

(i) $f(x)$ *puede ser factorizado como producto de algunos, dígamos* r *polinomios primarios mónicos coprimos por pares* $f_1(x), f_2(x), \ldots, f_r(x)$ *sobre* $\mathcal{R}$, *es decir:*

$$f(x) = f_1(x)f_2(x)\cdots f_r(x)$$

y para cada $i = 1, 2, \ldots, r$, $\overline{f_i}(x)$ *es potencia de algún polinomio mónico irreducible sobre* $\mathbb{F}_{p^m}[x]$.

(ii) Sean $f(x) = f_1(x)f_2(x)\cdots f_r(x) = h_1(x)h_2(x)\cdots h_t(x)$ *dos factorizaciones de* $f(x)$ *en producto de polinomios primarios mónicos coprimos por pares en* $\mathcal{R}[x]$, *entonces* $r = t$ *y salvo re-ordenamiento* $f_i(x) = h_i(x)$ *para* $i = 1, 2, \ldots r$.

Definición 3.5.13. Sea $f(x) \in \mathcal{R}[x]$ un polinomio mónico de grado $l \geqslant 1$, si $\overline{f}(x)$ es un polinomio irreducible (o primitivo) en $\mathbb{F}_{p^m}[x]$, $f(x)$ será llamado polinomio **mónico básico irreducible**(o **mónico básico primitivo** respectivamente) sobre $\mathcal{R}$.

En lo sucesivo, para cada $h(x) \in \mathcal{R}[x]$, adopateremos la notación $(h(x))$ para denotar al ideal $h(x)\mathcal{R}[x]$ de $\mathcal{R}[x]$.

Teorema 3.5.14. *Para todo entero* $l \geqslant 1$ *existe un polinomio monico básico irreducible (o mónico básico primitivo) de grado* l *que divide a* $x^{p^{ml}-1} - 1$ *en* $\mathcal{R}[x]$.

Teorema 3.5.15. *Sea* $h(x)$ *un polinomio mónico básico irreducible de grado* l *sobre* $\mathcal{R}$. *Entonces el anillo de clases residuales* $\mathcal{R}[x]/(h(x))$ *es un anillo de Galois de característica* p^s *y cardinalidad* p^{sml} *y contiene a* $\mathcal{R}$ *como subanillo. Es decir,* $\mathcal{R}[x]/(h(x)) \simeq GR(p^s, p^{sml})$. *Denotando* $\xi = x + (h(x))$, *entonces* $h(\xi) = 0$ *y todos los elementos de* $R[x]/(h(x))$ *pueden ser expresados de manera única en la forma:*

$$a_0 + a_1\xi + \cdots + a_{l-1}\xi^{l-1}; \text{ para } a_0, a_1, \ldots, a_{l-1} \in \mathcal{R} \tag{3.5.1}$$

y denotaremos al anillo $\mathcal{R}[x]/(h(x))$ *por* $\mathcal{R}[\xi]$.

También, tenemos los siguientes teoremas análogos al Lema 3.2.5, Teorema 3.2.6 y Teorema 3.3.1.

Lema 3.5.16. *Sean* $\mathcal{R} = GR(p^s, p^{sm})$, $\mathcal{R}' = GR(p^s, p^{sml})$ *con* $\mathcal{R} \subseteq \mathcal{R}'$, $f(x) \in \mathcal{R}'[x]$ *y suponga que* $\overline{f}(x)$ *tiene una raíz* $\overline{\beta} \in \mathbb{F}_{p^{ml}}$ *tal que* $\overline{f}'(\overline{\beta}) \neq 0$. *Entonces existe una única raíz* $\alpha \in \mathcal{R}'$ *del polinomio* $f(x)$ *con la propiedad de* $\overline{\alpha} = \overline{\beta}$.

Teorema 3.5.17. *Sea $\mathcal{R}'$ un anillo de Galois de característica p^s y cardinalidad p^{sml}, donde p es un número primo, $s, m, l \in \mathbb{N}$. Entonces $\mathcal{R}'$ es isomorfo al anillo de clases residuales $\mathcal{R}[x]/(h(x))$ del anillo $\mathcal{R} = GR(p^s, p^{sm})$ y un polinomio mónico básico irreducible $h(x)$ de grado l en $\mathcal{R}[x]$.*

Teorema 3.5.18. *(i) En el anillo de Galois $GR(p^s, p^{sml})$ existe un elemento $\xi \neq 0$, de orden $p^{ml} - 1$, el cual es raíz de un polinomio mónico básico primitivo $h(x)$ de grado l y que divide a $x^{p^{ml}-1} - 1$ en $\mathcal{R}[x]$ donde $\mathcal{R} = GR(p^s, p^{sm})$, más aún $GR(p^s, p^{sml}) = \mathcal{R}[\xi]$ y $h(x)$ es el único polinomio mónico en $\mathcal{R}[x]$ de grado menor o igual que l y que tiene a ξ como raíz.*

(ii) Sea $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^{ml}-2}\}$, entonces cualquier elemento $c \in GR(p^s, p^{sml})$ puede ser escrito de manera única como:

$$c = a_0 + a_1 p + a_2 p^2 + \cdots + a_{s-1} p^{s-1} \text{ donde } a_0, a_1, \ldots a_{s-1} \in \mathcal{T} \tag{3.5.2}$$

más aún, c es invertible si y sólo si $a_0 \neq 0$ y es divisor de cero si y sólo si $a_0 = 0$.

Corolario 3.5.19. *Sean $\xi \in \mathcal{R}' = GR(p^s, p^{sml})$ un elemento distinto de cero de orden $p^{ml} - 1$, el cual es raíz de un polinomio mónico básico primitivo $h(x)$ de grado l y que divide a $x^{p^{ml}-1} - 1$ en $\mathcal{R}[x]$ donde $\mathcal{R} = GR(p^s, p^{sm})$ entonces el elemento:*

$$\eta = \xi^{(p^{ml}-1)/(p^m-1)} \in \mathcal{R}'$$

es tal que $ord(\eta) = p^m - 1$ y si $\mathcal{T}' = \{0, 1, \eta, \eta^2, \ldots, \eta^{p^m-2}\}$ entonces $\mathcal{R} = \{a_0 + a_1 p + \cdots + a_{s-1} p^{s-1} \mid a_i \in \mathcal{T}' \text{ para } i \in \{0, 1, \ldots, s-1\}\}$.

Demostración. Denotemos $n = ml$, así, $\eta^{p^m-1} = \left(\xi^{(p^n-1)/(p^m-1)}\right)^{p^m-1}$ y esto es igual a, $\xi^{p^n-1} = 1$. Entonces $ord(\eta) \mid p^m - 1$. Si $d = ord(\eta)$, $\eta^d = 1$, y tenemos que $\xi^{(d(p^n-1))/(p^m-1)} = 1$, entonces $p^n - 1 = ord(\xi) \mid d\left(\frac{p^n-1}{p^m-1}\right)$ entonces existe $k \in \mathbb{Z}$ tal que $d\left(\frac{p^n-1}{p^m-1}\right) = k(p^n - 1)$, y haciendo operaciones en enteros, tenemos que, $d = k(p^m - 1)$, es decir, $p^m - 1 \mid d$, por consiguiente, $ord(\eta) = d = p^m - 1$, luego los elementos $0, 1, \eta, \ldots, \eta^{p^m-2}$ son todos distintos y $\langle\eta\rangle$ es un grupo cíclico de orden $p^m - 1$ y la cardinalidad del conjunto $\mathcal{T}'$ es p^m. Finalmente, por el Corolario 3.5.4, existe un único anillo de Galois $\mathcal{R} = GR(p^s, p^{sm})$ y con $\mathcal{R} \subseteq \mathcal{R}'$. Si consideramos el conjunto $\mathcal{S} = \{a_0 + a_1 p + \cdots + a_{s-1} p^{s-1} \mid a_i \in \mathcal{T}' \text{ para } i \in \{0, 1, \ldots, s-1\}\}$, éste es un anillo de Galois con característica p^s por el principio multiplicativo su cardinalidad es p^{sm} luego, por la unicidad (bajo isomorfismos) de $\mathcal{R}$, tenemos que $\mathcal{R} \simeq \mathcal{S}$, es decir, $\mathcal{R} = \{a_0 + a_1 p + \cdots + a_{s-1} p^{s-1} \mid a_i \in \mathcal{T}' \text{ para } i \in \{0, 1, \ldots, s-1\}\}$, como queríamos demostrar. □

AUTOMORFISMOS DE ANILLOS DE GALOIS

Ya hemos estudiado en las secciones previas, la estructura de los anillos de Galois y cómo éstos pueden extender sus propiedades a anillos que los contienen, en esta

sección estudiaremos una clase muy particular de funciones entre anillos de Galois, a las cuales llamaremos *automorfismos*, pero antes de esto veamos el siguiente:

Lema 3.6.1. *Sean* $\mathcal{R}' = GR(p^s, p^{sml})$ *que contiene a* $\mathcal{R} = GR(p^s, p^{sm})$ *como subanillo,* $\xi \in \mathcal{R}' - \{0\}$ *tal que* $ord(\xi) = p^{ml} - 1$ *y que es raíz de un polinomio mónico básico primitivo (irreducible)* $h(x)$ *de grado* $l \in \mathbb{N}$ *que divide a* $x^{p^{ml}-1} - 1$ *en* $\mathcal{R}[x]$ *y tal que* $\mathcal{R}' = \mathcal{R}[\xi]$. *Entonces los elementos* $\xi, \xi^{p^m}, \dots \xi^{p^{m(l-1)}} \in \mathcal{R}'$ *son todas las raíces de* $h(x)$.

Demostración. Como $h(x)$ es un polinomio mónico básico primitivo (irreducible) en $\mathcal{R}[x]$ entonces por la Definición 3.5.13 el polinomio $\overline{h}(x) \in \mathbb{F}_{p^m}[x]$ es un polinomio mónico y primitivo (irreducible), más aún, como $grad(h(x)) = l$ y $h(\xi) = 0$ entonces $grad(\overline{h}(x)) = l$ y $\overline{h}(\overline{\xi}) = 0$, luego $\overline{\xi}$ es un elemento primitivo de $\mathbb{F}_{p^m}$ y como $ord(\overline{\xi}) = ord(\xi) = p^{ml} - 1$ entonces $\overline{\xi}, \overline{\xi}^{p^m}, \overline{\xi}^{p^{m(l-1)}}$ son todas las raíces de $\overline{h}(x)$ (ver Lema A.2.4). Dado que el grado de $\overline{h}(x) = l$ y los elementos $\xi^{p^{mi}}$ con $i \in \{0, 1, \dots, l-1\}$ son l entonces todas las raíces son simples, es decir, $\overline{h}'\left(\xi^{p^{mi}}\right) \neq 0$, por el Lema 3.5.16, existen, para cada $i \in \{0, 1, \dots, l-1\}$ únicas raíces de $h(x)$, $\alpha_i \in \mathcal{R}'$, tales que $\overline{\alpha}_i = \overline{\xi}^{p^{mi}}$. Dado que $h(x) \mid x^{p^{ml}-1} - 1$ en $\mathcal{R}[x]$, existe $k(x) \in \mathcal{R}[x]$, tal que, $x^{p^{ml}-1} - 1 = h(x)k(x)$, así, evaluando tenemos que $\alpha_i^{p^{ml}-1} - 1 = 0$ por ser raíz de $h(x)$, por consiguiente, $\alpha_i^{p^{ml}-1} = 1$, de ahí que, $ord(\alpha_i) \mid p^m - 1$, por (ii) del Corolario 3.3.3, $\alpha_i = \xi^{l_i}$, para $l_i \in \{0, 1, \dots, p^{ml} - 2\}$. Aplicando el epimorfismo (2.1.8), tenemos, $\overline{\xi}^{p^{mi}} = \overline{\alpha}_i = \overline{\xi}^{l_i}$, entonces, $l_i = p^{mi}$, por lo tanto, $\alpha_i = \xi^{p^{mi}}$. De lo anterior, $\alpha_0 = \xi$, $\alpha_1 = \xi^{p^m}, \dots, \alpha_{l-1} = \xi^{p^{m(l-1)}}$ son l—raíces de $h(x)$ y $h(x) = (x - \xi)\left(x - \xi^{p^m}\right) \cdots \left(x - \xi^{p^{m(l-1)}}\right)$. Como $grad(h(x)) = l$, $\xi, \xi^{p^m}, \dots \xi^{p^{m(l-1)}} \in \mathcal{R}'$ son todas las raíces de $h(x)$. □

Definición 3.6.2. Sean $\mathcal{R}' = GR(p^s, p^{sml})$, que contiene a $\mathcal{R} = GR(p^s, p^{sm})$ como subanillo, $\xi \in \mathcal{R}' - \{0\}$ con $ord(\xi) = p^{ml} - 1$ y tal que es raíz de un polinomio mónico básico primitivo (irreducible) $h(x)$ de grado $l \in \mathbb{N}$ que divide a $x^{p^{ml}-1} - 1$ en $\mathcal{R}[x]$. Considérese que $\mathcal{R}' = \mathcal{R}[\xi]$, con esto se define la función: $\Phi : \mathcal{R}[\xi] \longrightarrow \mathcal{R}[\xi]$ tal que:

$$\Phi\left(a_0 + a_1\xi + \cdots + a_{l-1}\xi^{l-1}\right) = a_0 + a_1\xi^{p^m} + \cdots + a_{l-1}\xi^{(l-1)p^m} \tag{3.6.1}$$

Teorema 3.6.3. Φ *es un automorfismo de* $\mathcal{R}'$ *tal que* $\alpha \in \mathcal{R}$ *si y sólo si* $\Phi(\alpha) = \alpha$

Demostración. Considérense las funciones ϕ_1, ϕ_2, definidas como:

$$\begin{array}{rcl} \phi_1 : \mathcal{R}[x]/(h(x)) & \longrightarrow & \mathcal{R}[\xi] \\ \sum_{i=0}^{l-1} a_i x^i + (h(x)) & \longmapsto & \sum_{i=0}^{l-1} a_i \xi^i \end{array} \qquad \begin{array}{rcl} \phi_2 : \mathcal{R}[x]/(h(x)) & \longrightarrow & \mathcal{R}\left[\xi^{p^m}\right] \\ \sum_{i=0}^{l-1} a_i x^i + (h(x)) & \longmapsto & \sum_{i=0}^{l-1} a_i \xi^{i(p^m)} \end{array}$$

no es difícil ver que ϕ_1 y ϕ_2 son homomorfismos de anillos, por el Lema 3.6.1, ξ^{p^m} es también una raíz del polinomio $h(x)$, así, $\mathcal{R}\left[\xi^{p^m}\right]$ es un anillo de Galois con característica p^s y cardinalidad p^{sml}, es decir, $|\mathcal{R}[\xi]| = \left|\mathcal{R}\left[\xi^{p^m}\right]\right|$ y $\mathcal{R}\left[\xi^{p^m}\right] \subseteq \mathcal{R}[\xi]$, por lo tanto, son iguales y se sigue que ϕ_1 como ϕ_2 son epimorfismos. Tomando $[\alpha](x) = \sum_{i=0}^{l-1} a_i x^i + (h(x)), [\beta](x) = \sum_{i=0}^{l-1} b_i x^i + (h(x)) \in \mathcal{R}[x]/(h(x))$, es claro que $[\alpha + \beta](x) = \sum_{i=0}^{l-1} (a_i + b_i)x^i + (h(x))$, ahora suponga que $\phi_1([\alpha](x)) = \phi_1([\beta](x))$ entonces $0 = \phi_1([\alpha](x)) - \phi_1([\beta](x)) = \phi_1([\alpha - \beta](x))$, por consiguiente:

$$(a_0 - b_0) + (a_1 - b_1)\xi + \cdots + (a_{l-1} - b_{l-1})\xi^{l-1} = 0 + 0\xi + \cdots + 0\xi^{(l-1)} \tag{3.6.2}$$

dado que la *representación aditiva* en un anillo de Galois es única entonces se deduce de (3.6.2) que $(a_i - b_i) = 0$ para cada $i \in \{0, 1, \ldots, l-1\}$; de manera análoga suponiendo que $\phi_2([\alpha](x)) = \phi_2([\beta](x))$ se llega a:

$$(a_0 - b_0) + (a_1 - b_1)\xi^{p^m} + \cdots + (a_{l-1} - b_{l-1})\xi^{(l-1)p^m} = 0 + 0\xi^{p^m} + \cdots + 0\xi^{(l-1)p^m} \tag{3.6.3}$$

nuevamente por la unicidad de la *representación aditiva* y de (3.6.3), $(a_i - b_i) = 0$ para $i \in \{0, 1, \ldots, l-1\}$ por lo tanto $[\alpha](x) = [\beta](x)$ y se concluye que ϕ_1 y ϕ_2 son monomorfismos y por consiguiente isomorfismos. Por lo anterior dicho, tenemos que, $\Psi = \left[\phi_2 \circ (\phi_1)^{-1}\right] : \mathcal{R}[\xi] \longrightarrow \mathcal{R}\left[\xi^{p^m}\right] = \mathcal{R}[\xi]$ es un isomorfismo y es evidente que tanto Φ como Ψ tienen el mismo dominio además, para todo $a_0 + a_1\xi + \cdots a_{l-1}\xi^{l-1} \in \mathcal{R}[\xi]$ tenemos que:

$$\begin{aligned}
\Psi(a_0 + a_1\xi + \cdots a_{l-1}\xi^{l-1}) &= \phi_2\left((\phi_1)^{-1}(a_0 + a_1\xi + \cdots a_{l-1}\xi^{l-1})\right) \\
&= \phi_2\left(a_0 + a_1x + \cdots a_{l-1}x^{l-1} + (h(x))\right) \\
&= a_0 + a_1\xi^{p^m} + \cdots a_{l-1}\xi^{(l-1)p^m} \\
&= \Phi(a_0 + a_1\xi + \cdots a_{l-1}\xi^{l-1})
\end{aligned}$$

por lo tanto $\Phi = \Psi$ con lo cual tenemos que Φ es un automorfismo de $\mathcal{R}' = \mathcal{R}[\xi]$. Sea $\alpha \in \mathcal{R}$, entonces $\alpha = \alpha + 0\xi + \cdots + 0\xi^{l-1}$, así $\Phi(\alpha) = \alpha$, se sigue que $\alpha \in \mathcal{R}$ implica $\Phi(\alpha) = \alpha$. Por otro lado, supongamos que $\Phi(\alpha) = \alpha$ para $\alpha \in \mathcal{R}'$, por el Teorema 3.5.18, $\alpha = a_0 + a_1p + a_2p^2 + \cdots + a_{s-1}p^{s-1}$ con $a_i \in \mathcal{T} = \langle\xi\rangle \cup \{0\}$ para $i \in \{0, 1, \ldots, s-1\}$. Note que $\Phi(\xi) = \xi^{p^m}$ y **deja fijos** a los elementos del subanillo. $\mathcal{R}$[3] Luego, como $p \in \mathcal{R}$, tenemos que, $\Phi(p^j) = p^j$ para $j \in \{0, 1, \ldots, s-1\}$, así,

$$\Phi(a_0 + a_1p + a_2p^2 + \cdots + a_{s-1}p^{s-1}) = a_0^{p^m} + a_1^{p^m}p + a_2^{p^m}p^2 + \cdots + a_{s-1}^{p^m}p^{s-1} \tag{3.6.4}$$

dado que la representación p-ádica es única, $\Phi(\alpha) = \alpha = a_0 + a_1p + a_2p^2 + \cdots + a_{s-1}p^{s-1}$ y de (3.6.4) tenemos que $a_i^{p^m} = a_i$, para cada $i \in \{0, 1, \ldots, s-1\}$. Supongamos que $a_i = 0$ entonces $a_i^{p^m} = 0$, por otro lado si $a_i^{p^m} = 0$, dado que $a_i \in \langle\xi\rangle \cup \{0\}$ entonces $a_i = 0$ o $a_i = \xi^j$ para $j \in \{0, 1, \ldots, p^{ml} - 2\}$. Suponiedo que $a_i \neq 0$ entonces $0 = a_i^{p^m} = (\xi^j)^{p^m}$, aplicado el epimorfismo (2.1.8) se obtiene que:

$$\begin{aligned}
\overline{0} &= \overline{(\xi^j)^{p^m}} \\
\overline{0} &= \overline{\xi^{j(p^m)}} \\
\overline{0} &= \overline{\xi}^{j(p^m)} = \overline{\xi}\left(\overline{\xi}^{jp^m - 1}\right)
\end{aligned} \tag{3.6.5}$$

dado que $\overline{\xi}$ es un elemento primitivo en $\mathbb{F}_{p^{ml}}$ entonces ξ es un unidad de éste campo luego la expresión (3.6.5), da lugar a una contradicción, por lo tanto $a_i = 0$, de esto se concluye que $a_i = 0$ si y sólo si $a_i^{p^m} = 0$. Ahora supongamos que $a_i \neq 0$, como $a_i = a_i^{p^m}$ y a_i es invertible, pues $a_i \in \langle\xi\rangle$ se sigue que $a_i^{p^m - 1} = 1$ entonces existe $j_i \in \{0, 1, \ldots, p^{ml} - 2\}$ tal que $\left(\xi^{j_i}\right)^{p^m - 1} = a_i^{p^m - 1} = 1$ es decir $\xi^{j_i(p^m - 1)} = 1$ por consiguiente $p^{ml} - 1 = \mathrm{ord}(\xi) \mid (j_i(p^m - 1))$ entonces existe un $t_i \in \mathbb{Z}$ tal que $j_i(p^m - 1) =$

3 Pues ya se demostró que si $r \in \mathcal{R}$ entonces $\Phi(r) = r$.

$t_i(p^{ml}-1)$, se sigue que $j_i = t_i\left(p^{ml}-1/p^m-1\right)$, usando η como en el Corolario 3.5.19 tenemos que, para cada $i \in \{0,1,\ldots,s-1\}$; $a_i = \xi^{j_i} = \xi^{t_i\left(p^{ml-1}/p^m-1\right)} = \eta^{t_i}$ entonces, renombrando $b_0 = a_0 = \eta^{t_0}$, $b_1 = \eta^{t_1}, \ldots, b_{s-1} = a_{s-1} = \eta^{t_{s-1}}$ podemos reescribir a α como $\alpha = b_0 + b_1 p + \cdots + b_{s-1}p^{s-1}$ donde $b_i \in \mathcal{T}'$ como en el Corolario 3.5.19, es decir, $\alpha \in \mathcal{R}$, en resumen, dado que $\Phi(\alpha) = \alpha$ esto implica que $\alpha \in \mathcal{R}$, por lo tanto $\alpha \in \mathcal{R}$ si y sólo si $\Phi(\alpha) = \alpha$ como queríamos demostrar. □

Un automorfismo de un anillo de Galois $\mathcal{R}'$ que deja fijos a los elementos de un subanillo $\mathcal{R}$ de $\mathcal{R}'$ es llamado **autormorfismo de** $\mathcal{R}'$ **sobre** $\mathcal{R}$, más aún el automorfismo del teorema anterior es llamado *automorfismo generalizado de Frobenius*, haciendo una clara referencia al automorfismo de Frobenius, definido entre campos finitos.

Definición 3.6.4. Sean $\mathcal{R}' = GR(p^s, p^{sml})$ y $\mathcal{R} = GR(p^s, p^{sm})$ un subanillo de $\mathcal{R}'$ tal que $\mathcal{R}' = \mathcal{R}[\xi]$ para p un número primo, $n, m, l \in \mathbb{N}$ definimos:

(i) El automorfismo generalizado de Frobenius de $\mathcal{R}'$ sobre $\mathcal{R}$ como la función:

$$\begin{array}{rccc} \Phi: & \mathcal{R}' & \longrightarrow & \mathcal{R} \\ & \sum_{i=0}^{l-1} a_i\xi^i & \longmapsto & \sum_{i=0}^{l-1} a_i\xi^{i(p^m)} \end{array}$$

(ii) $\Phi^0 = id_{\mathcal{R}'}$, $\Phi^{t+1} = \Phi^t \circ \Phi$ y $\Phi^{-t} = \left(\Phi^{-1}\right)^t$ para cada $t \in \mathbb{N}$.

(iii) El conjunto $Gal(\mathcal{R}'/\mathcal{R}) := \{\tau : \mathcal{R}' \to \mathcal{R}' \mid \tau \text{ es automorfismo de } \mathcal{R}' \text{ sobre } \mathcal{R}\}$ es el **grupo de Galois** de $\mathcal{R}'$ sobre $\mathcal{R}$.

A continuación presentamos algunos resultados sobre el grupo de Galois de un anillo de Galois y su estrecha relación con el automorfismo generalizado de Frobenius, el grupo de Galois de un campo finito y el automorfismo de Frobenius.

Lema 3.6.5. *Sea $\tau \in Gal(\mathcal{R}'/\mathcal{R})$. Definimos un automorfismo inducido por (2.1.8); $\overline{\tau}$ de $\overline{\mathcal{R}'} = \mathbb{F}_{p^{ml}}$ de la siguiente manera:*

$$\begin{array}{rccc} \overline{\tau}: & \mathbb{F}_{p^{ml}} & \longrightarrow & \mathbb{F}_{p^{ml}} \\ & a & \longmapsto & \overline{\tau}(a) = \overline{\tau(\alpha)} \end{array}$$

donde $\overline{\alpha} = a$ para algún $\alpha \in \mathcal{R}'$. Entonces $\overline{\tau}$ está bien definida y $\overline{\tau} \in Gal(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$.

Demostración. Sea $a \in \mathbb{F}_{p^{ml}}$, como (2.1.8) es un epimorfismo de $\mathcal{R}'$ en $\mathcal{R}'/(p)' = \mathbb{F}_{p^{ml}}$; existe $\alpha \in \mathcal{R}'$ tal que $\overline{\alpha} = a$. Veamos que $\overline{\tau}$ está bien definida. Sean $\alpha, \alpha' \in \mathcal{R}'$ con $\overline{\alpha} = \overline{\alpha}$, entonces $\overline{\alpha - \alpha'} = \overline{\alpha} - \overline{\alpha'} = a - a = \overline{0} \in \mathbb{F}_{p^{ml}}$, es decir, $\alpha - \alpha' \in \ker(-) = (p)' \subseteq \mathcal{R}'$, así, existe $\pi \in \mathcal{R}'$ tal que $\alpha - \alpha' = p\pi$, luego $\tau(\alpha) - \tau(\alpha') = \tau(\alpha - \alpha') = \tau(p\pi) = p\tau(\pi)$, ya que $p \in \mathcal{R}$ y $\tau \in Gal(\mathcal{R}'/\mathcal{R})$. Luego, $\tau(\alpha) = \tau(\alpha') + p\tau(\pi)$, por consiguiente, $\overline{\tau(\alpha)} = \overline{\tau(\alpha') + p\tau(\pi)} = \overline{\tau(\alpha')} + \overline{0}\,\overline{\tau(\pi)}$, es decir, $\overline{\tau(\alpha)} = \overline{\tau(\alpha')}$ entonces $\overline{\tau}$ está bien definida. Por otro lado, consideremos $a, b \in \mathbb{F}_{p^{ml}}$, luego existen $\alpha, \beta \in \mathcal{R}'$ tales que $\overline{\alpha} = a$ y $\overline{\beta} = b$ entonces $a + b = \overline{\alpha + \beta}$ y $ab = \overline{\alpha\beta}$, tenemos que:

$$\begin{aligned} \overline{\tau}(a+b) &= \overline{\tau(\alpha+\beta)} \\ &= \overline{\tau(\alpha) + \tau(\beta)} \\ &= \overline{\tau(\alpha)} + \overline{\tau(\beta)} = \overline{\tau}(a) + \overline{\tau}(b) \end{aligned} \qquad \begin{aligned} \overline{\tau}(ab) &= \overline{\tau(\alpha\beta)} \\ &= \overline{\tau(\alpha)\tau(\beta)} \\ &= \overline{\tau(\alpha)}\,\overline{\tau(\beta)} = \overline{\tau}(a)\overline{\tau}(b) \end{aligned}$$

de lo anterior, se sigue que $\overline{\tau}$ es un homomorfismo de anillos, y por su definición es claro que es un epimorfismo. Si $\overline{\tau}(a) = \overline{0}$ entonces existe $\alpha \in \mathcal{R}'$ tal que $\overline{\tau(\alpha)} = \overline{0}$, así $\tau(\alpha) \in \ker(-) = (p)'$, luego existe $\pi \in \mathcal{R}'$ tal que $\tau(\alpha) = p\pi$ y como la característica de $\mathcal{R}'$ es p^s entonces $(\tau(\alpha))^s = p^s\pi^s = 0$, lo cual es equivalente a $\tau(\alpha^s) = 0$, entonces $\alpha^s \in (p)'$ y aplicando (2.1.8) tenemos que $\overline{\alpha}^s = \overline{\alpha^s} = \overline{0} \in \mathbb{F}_{p^{ml}}$ y cómo éste es un dominio entero, es claro que $a = \overline{\alpha} = 0$, así $\ker\overline{\tau} = \{0\}$, por consiguiente $\overline{\tau}$ es un monomorfismo y por lo ya visto antes, un automorfismo. Finalmente, considere el subanillo $\mathcal{R}$, éste es un anillo de Galois y por tanto sus divisores de cero con el cero forman un ideal principal (p) y por el Teorema 3.5.2; $(p) = \mathcal{R} \cap (p)'$. Considere la restricción de (2.1.8) a $\mathcal{R}$, dada por $- \mid_{\mathcal{R}} \colon \mathcal{R} \longrightarrow \mathcal{R}/(p) = \mathbb{F}_{p^m}$, la cual por simplicidad denotaremos también por $-$. Sea $a \in \mathbb{F}_{p^m}$, por lo anterior, existe $\alpha \in \mathcal{R}$ con $\overline{\alpha} = a$, se sigue que $\overline{\tau}(a) = \overline{\tau(\alpha)} = \overline{\alpha}$ pues $\tau \in \mathrm{Gal}(\mathcal{R}'/\mathcal{R})$, en otras palabras $\overline{\tau}(a) = a$, así $\overline{\tau}$ es un automorfismo de $\mathbb{F}_{p^{ml}}$ que *deja fijos* a los elementos de $\mathbb{F}_{p^m}$, por definición $\overline{\tau} \in \mathrm{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$, con lo cual hemos demostrado nuestro lema. □

Lema 3.6.6. *Sea Φ el automorfismo generalizado de Frobenius de $\mathcal{R}' = \mathrm{GR}(p^s, p^{sml})$ sobre $\mathcal{R} = \mathrm{GR}(p^s, p^{sm})$, entonces Φ es generador de un grupo cíclico de orden l, con la composición de funciones como operación.*

Demostración. Sea $\xi \in \mathcal{R}'$, entonces $\Phi^2(\xi) = \Phi(\Phi(\xi)) = \Phi\left(\xi^{p^m}\right) = \left(\xi^{p^m}\right)^{p^m} = \xi^{p^{2m}}$ luego, $\Phi^3(\xi) = \Phi\left(\Phi^2(\xi)\right) = \Phi\left(\xi^{p^{2m}}\right) = \left(\xi^{p^{2m}}\right)^{p^m} = \xi^{p^{3m}}$; siguiendo de esta manera, es claro que para cada $i \in \mathbb{N}$, $\Phi^i(\xi) = \xi^{p^{im}}$. Como Φ es un automorfismo de $\mathcal{R}'$ es claro que el dominio de Φ^l coincide con el dominio de $\mathrm{id}_{\mathcal{R}'}$, más aún para todo $\alpha \in \mathcal{R}' = \mathcal{R}[\xi]$, con $\alpha = \sum_{j=0}^{l-1} a_j\xi^j$ se tiene que:

$$\begin{aligned}
\Phi^l(\alpha) &= a_0 + a_1\Phi^l(\xi) + \cdots + a_{l-1}\Phi^l(\xi^{l-1}) \\
&= a_0 + a_1\Phi^l(\xi) + \cdots + a_{l-1}\left(\Phi^l(\xi)\right)^{l-1} && (\Phi \in \mathrm{Gal}(\mathcal{R}'/\mathcal{R})) \\
&= a_0 + a_1\xi^{p^{ml}} + \cdots + a_{l-1}\left(\xi^{p^{ml}}\right)^{l-1} \\
&= a_0 + a_1\xi + \cdots + a_{l-1}\xi^{l-1} \\
&= \alpha = \mathrm{id}_{\mathcal{R}'}(\alpha) && (\mathrm{ord}(\xi) = p^{ml} - 1)
\end{aligned}$$

es decir $\Phi^l = \mathrm{id}_{\mathcal{R}'}$. Sea $0 < t < l$ con $\Phi^t = \mathrm{id}'_{\mathcal{R}}$ entonces en particular $\Phi^t(\xi) = \xi^{p^{mt}}$ y $\Phi^t(\xi) = \xi$, luego $\xi^{p^{mt}} = \xi$, es decir, $\xi^{p^{mt}-1} = 1$, pero $t < l$ de lo cual se sigue que $mt < ml$, así $p^{mt} - 1 < p^{ml} - 1 = \mathrm{ord}(\xi)$ lo que es una contradicción, entonces l es el entero más pequeño tal que $\Phi^l = \mathrm{id}_{\mathcal{R}'}$ por consiguiente $\mathrm{ord}(\Phi) = l$, considerando a Φ como un elemento del grupo de las funciones biyectivas con la composición como operación binaria; finalmente, nombrando $1 = \mathrm{id}_{\mathcal{R}'}$, tenemos que $\langle\Phi\rangle := \{1, \Phi, \Phi^2, \ldots, \Phi^{l-1}\}$ es un grupo cíclico de orden l, bajo la composición de funciones. □

Teorema 3.6.7. *Sea Φ el automorfismo generalizado de Frobenius de $\mathcal{R}'$ sobre $\mathcal{R}$. Entonces $\overline{\Phi}$ es el automorfimo de Frobenius de $\mathbb{F}_{p^{ml}}$ sobre $\mathbb{F}_{p^m}$, más aún:*

(i) $\mathrm{Gal}(\mathcal{R}'/\mathcal{R}) = \langle\Phi\rangle$

(ii) La función:

$$\begin{array}{rccc} \mathcal{F}: & \mathrm{Gal}(\mathcal{R}'/\mathcal{R}) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m}) \\ & \tau & \longmapsto & \overline{\tau} \end{array}$$

es un isomorfismo de grupos.

Demostración. (i) Por definición, Φ es un automorfismo de $\mathcal{R}'$ sobre $\mathcal{R}$, luego $\Phi \in \mathrm{Gal}(\mathcal{R}'/\mathcal{R})$, por el lema anterior $\overline{\Phi} \in \mathrm{Gal}(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m})$, luego, $\overline{\Phi}: \mathbb{F}_{p^{ml}} \longrightarrow \mathbb{F}_{p^{ml}}$ es un automorfismo que deja fijos a los elementos de $\mathbb{F}_{p^m}$. Por otro lado, sea $\sigma: \mathbb{F}_{p^{ml}} \longrightarrow \mathbb{F}_{p^{ml}}$ el automorfismo de Frobenius de $\mathbb{F}_{p^{ml}}$ sobre $\mathbb{F}_{p^m}$, es claro que $\mathrm{dom}\,\overline{\Phi} = \mathrm{dom}\,\sigma$, además tenemos que, dado $b \in \mathbb{F}_{p^{ml}}$, existe $\beta \in \mathcal{R}'$ tal que $\overline{\beta} = b$ y para $\xi \in \mathcal{R}'$, así:

$$\overline{\Phi}\left(\overline{\xi}\right) = \overline{\Phi(\xi)} = \overline{\xi^{p^m}} = \overline{\xi}^{p^m} = \sigma\left(\overline{\xi}\right)$$

además, considerando a $\mathbb{F}_{p^{ml}}$ como una extensión de $\mathbb{F}_{p^m}$, es decir, $\mathbb{F}_{p^{ml}} = \mathbb{F}_{p^m}\left[\overline{\xi}\right]$ tenemos que para todo $b = b_0 + b_1\overline{\xi} + \cdots + b_{n-1}\overline{\xi}^{n-1} \in \mathbb{F}_{p^m}\left[\overline{\xi}\right]$, entonces

$$\begin{aligned} \sigma(b) &= \sigma\left(b_0 + b_1\overline{\xi} + \cdots + b_{l-1}\overline{\xi}^{l-1}\right) \\ &= b_0 + b_1\sigma(\overline{\xi}) + \cdots + b_{l-1}\sigma\left(\overline{\xi}^{l-1}\right) \\ &= b_0 + b_1\sigma(\overline{\xi}) + \cdots + b_{l-1}\sigma(\overline{\xi})^{l-1} && \left(\sigma \in \mathrm{Gal}\left(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m}\right)\right) \\ &= b_0 + b_1\overline{\Phi}(\overline{\xi}) + \cdots + b_{l-1}\overline{\Phi}(\overline{\xi})^{l-1} \\ &= b_0 + b_1\overline{\Phi}(\overline{\xi}) + \cdots + b_{l-1}\overline{\Phi}\left(\overline{\xi}^{l-1}\right) \\ &= \overline{\Phi}\left(b_0 + b_1\overline{\xi} + \cdots + b_{l-1}\overline{\xi}^{l-1}\right) = \overline{\Phi}(b) && \left(\overline{\Phi} \in \mathrm{Gal}\left(\mathbb{F}_{p^{ml}}/\mathbb{F}_{p^m}\right)\right) \end{aligned}$$

es decir, para todo $b \in \mathbb{F}_{p^{ml}}$: $\sigma(b) = \overline{\Phi}(b)$ se tiene que $\overline{\Phi}$ es el automorfismo de Frobenius. Por otro lado, recordemos que $\xi \in \mathcal{R}'$ es raíz de un polinomio mónico básico primitivo de grado l y que divide a $x^{p^{ml}-1} - 1$ en $\mathcal{R}[x]$, denotemóslo por $h(x) = h_0 + h_1x + \cdots + h_{l-1}x^{l-1} + x^l$ y entonces $h(\xi) = 0$, más aún $\tau(h(\xi)) = \tau(0) = 0$, de manera equivalente:

$$\begin{aligned} 0 = \tau(h(\xi)) &= \tau\left(h_0 + h_1\xi + \cdots + h_{l-1}\xi^{l-1} + x^l\right) \\ &= h_0 + h_1\tau(\xi) + \cdots + h_{l-1}\tau\left(\xi^{l-1}\right) + \tau\left(\xi^l\right) \\ &= h_0 + h_1\tau(\xi) + \cdots + h_{l-1}\tau(\xi)^{l-1} + \tau(\xi)^l && (\tau \in \mathrm{Gal}(\mathcal{R}'/\mathcal{R})) \\ &= h(\tau(\xi)) \end{aligned}$$

luego, $\tau(\xi)$ es una raíz para $h(x)$, por el Lema 3.6.1, $\tau(\xi) = \xi^{p^{mj}}$ para $j \in \{0, 1, \ldots, l-1\}$; por consiguiente dado $\alpha \in \mathcal{R}'$ es claro que $\alpha = a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{l-1}\xi^{l-1}$con $a_i \in \mathcal{R}$ para $i \in \mathcal{R}$, entonces:

$$\begin{aligned}
\tau(\alpha) &= \tau\left(a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{l-1}\xi^{l-1}\right) \\
&= a_0 + a_1\tau(\xi) + a_2\tau\left(\xi^2\right) + \cdots + a_{l-1}\tau\left(\xi^{l-1}\right) \\
&= a_0 + a_1\tau(\xi) + a_2(\tau(\xi))^2 + \cdots + a_{l-1}\left(\tau(\xi)\right)^{l-1} \\
&= a_0 + a_1\xi^{p^{mj}} + a_2\left(\xi^{p^{mj}}\right)^2 + \cdots + a_{l-1}\left(\xi^{p^{mj}}\right)^{l-1} \\
&= a_0 + a_1\xi^{p^{mj}} + a_2\xi^{2p^{mj}} + \cdots + a_{l-1}\xi^{(l-1)p^{mj}} \\
&= a_0 + a_1\Phi^j(\xi) + \Phi^j\left(\xi^2\right) + \cdots + a_{l-1}\Phi^j\left(\xi^{l-1}\right) \\
&= \Phi^j\left(a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{l-1}\xi^{l-1}\right) \\
&= \Phi^j(\alpha)
\end{aligned}$$

por lo tanto $\tau = \Phi^j$ para algún $j \in \{0, 1, \ldots, l-1\}$, por consiguiente $Gal(\mathcal{R}'/\mathcal{R}) \subseteq \langle\Phi\rangle$ y dado que $\Phi \in Gal(\mathcal{R}'/\mathcal{R})$ se obtiene que $Gal(\mathcal{R}'/\mathcal{R}) = \langle\Phi\rangle$.

(ii) Sean $\Phi^i, \Phi^j \in Gal(\mathcal{R}'/\mathcal{R})$ luego $\mathcal{F}\left(\Phi^i \circ \Phi^j\right) = \mathcal{F}\left(\Phi^{i+j}\right) = \sigma^{i+j}$ ya que $\overline{\Phi} = \sigma$, entonces $\mathcal{F}\left(\Phi^i \circ \Phi^j\right) = \sigma^i \circ \sigma^j = \mathcal{F}\left(\Phi^i\right) \circ \mathcal{F}\left(\Phi^j\right)$, es decir, $\mathcal{F}$ es un homomorfismo de grupos. Si ocurre que $\mathcal{F}\left(\Phi^i\right) = id_{\mathbb{F}_{q^d}}$ entonces $\sigma^i = id_{\mathbb{F}_{q^d}}$ luego $l = ord(\sigma) \mid i$ en consecuencia $i = kl$ para algún $k \in \mathbb{N}$, luego $\Phi^i = \Phi^{lk} = id_{\mathcal{R}'}$ y así $\ker\mathcal{F} \subseteq \{id_{\mathcal{F}}\}$, evidentemente $\{id_{\mathcal{F}}\} \subseteq \ker\mathcal{F}$ y entonces $\mathcal{F}$ es un monomorfismo. Por su definición ésta función es un epimorfismo, así es un isomorfismo como afirmamos. □

Corolario 3.6.8. *Sea Φ el automorfismo generalizado de Frobenius de $\mathcal{R}' = GR(p^s, p^{sn})$ sobre $\mathcal{R} = GR(p^s, p^{sm})$, suponga que $n = md$. Entonces*

i) Φ^d es el automorfismo de Frobenius de $\mathcal{R}'$ sobre $\mathcal{R}'' = GR(p^s, p^{smd})$ y $Gal(\mathcal{R}'/\mathcal{R}'') = \langle\Phi^d\rangle$ es un grupo cíclico de orden l.

ii) Para todo $a \in \mathcal{R}''$, $\Phi(a) \in \mathcal{R}''$. Si denotamos la restricción de Φ a $\mathcal{R}''$ por $\Phi\mid_{\mathcal{R}''}$, entonces la función

$$\begin{array}{rccc} \Phi\mid_{\mathcal{R}''}: & \mathcal{R}'' & \longrightarrow & \mathcal{R}'' \\ & \alpha & \longmapsto & \Phi(\alpha) \end{array}$$

está bien definida, es el automorfismo de Frobenius de $\mathcal{R}''$ sobre $\mathcal{R}$ y $Gal(\mathcal{R}''/\mathcal{R}) = \langle\Phi\mid_{\mathcal{R}''}\rangle$ es un grupo cíclico de orden d.

Demostración. Note que $\overline{\mathcal{R}} = \mathbb{F}_{p^m}$, $\overline{\mathcal{R}'} = \mathbb{F}_{p^n}$ y $\overline{\mathcal{R}''} = \mathbb{F}_{p^{md}}$, por el teorema anterior $\overline{\Phi} = \sigma$ y los grupos de Galois $Gal(\mathcal{R}'/\mathcal{R})$ y $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^{md}})$ son isomorfos, entonces el Corolario A.4.3 es un análogo a éste corolario. (i) Como $md \mid n$ entonces por lo dicho antes y i) del Corolario A.4.3 $Gal(\mathbb{F}_{q^n}/\mathbb{F}_{q^{md}}) = \langle\sigma^d\rangle$, tomando la preimagen de estos conjuntos bajo la función $\mathcal{F}$ tenemos que $Gal(\mathcal{R}'/\mathcal{R}'') = \langle\Phi^d\rangle$ y éste es un grupo cíclico de orden $n/md = l$. (ii) Aplicando un razonamiento similar al del inciso previo, usando la preimagen de $\sigma\mid_{\mathbb{F}_{q^{md}}}$, la función $\Phi\mid_{\mathcal{R}''}$ está bien definida y como $Gal(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^m}) = \langle\sigma\mid_{\mathbb{F}_{q^{md}}}\rangle$ entonces $Gal(\mathcal{R}''/\mathcal{R}) = \langle\Phi\mid_{\mathcal{R}''}\rangle$ es un grupo cíclico de orden d. □

TRAZA Y NORMA GENERALIZADAS

Ya se ha notado antes que los anillos de Galois poseen propiedades afines a los campos finitos, en esta última sección analizaremos el concepto de traza y norma generalizadas.

Definición 3.7.1. Sean $\mathcal{R} = GR(p^s, p^{sm})$, $\mathcal{R}' = GR(p^s, p^{sml})$ tal que $\mathcal{R} \subseteq \mathcal{R}'$ y Φ el automorfismo generalizado de Frobenius de $\mathcal{R}'$ sobre $\mathcal{R}$. Definimos para cada $\alpha \in \mathcal{R}'$

$$Tr_{\mathcal{R}'/\mathcal{R}}(\alpha) = \alpha + \Phi(\alpha) + \cdots + \Phi^{l-1}(\alpha)$$
$$N_{\mathcal{R}'/\mathcal{R}}(\alpha) = \alpha\Phi(\alpha)\cdots\Phi^{l-1}(\alpha)$$

la **traza y norma generalizadas de** $\alpha \in \mathcal{R}'$ **relativa a** $\mathcal{R}$, respectivamente. Cuando $\mathcal{R}'$ y $\mathcal{R}$ son claros en el contexto, escribimos Tr y N para referirnos a la traza y norma generalizadas respectivamente.

Teorema 3.7.2. *Para $\alpha, \beta \in \mathcal{R}'$ y $\lambda \in \mathcal{R}$ tenemos:*

i) $Tr(\alpha) \in \mathcal{R}$

ii) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$

iii) $Tr(\lambda\alpha) = \lambda Tr(\alpha)$

iv) $Tr(\lambda) = l\lambda$

v) $Tr(\Phi(\alpha)) = Tr(\alpha)$

i)' $N(\alpha) \in \mathcal{R}$

ii)' $N(\alpha\beta) = N(\alpha)N(\beta)$

iii)' $N(\lambda\alpha) = \lambda^l N(\alpha)$

iv)' $N(\lambda) = \lambda^l$

v)' $N(\Phi(\alpha)) = N(\alpha)$

Demostración. La demostración es análoga a la prueba del Teorema A.5.2 y por esa razón se omite. □

Teorema 3.7.3. *Sea $\mathcal{R} = GR(p^s, p^{sm})$ un subanillo de $\mathcal{R}' = GR(p^s, p^{sml})$ y éste a su vez, un subanillo de $\mathcal{R}'' = GR(p^s, p^{smld})$. Entonces para todo $\alpha \in \mathcal{R}''$*

$$Tr_{\mathcal{R}''/\mathcal{R}}(\alpha) = Tr_{\mathcal{R}'/\mathcal{R}}\left(Tr_{\mathcal{R}''/\mathcal{R}'}(a)\right) \text{ y } N_{\mathcal{R}''/\mathcal{R}}(a) = N_{\mathcal{R}'/\mathcal{R}}\left(N_{\mathcal{R}''/\mathcal{R}'}(a)\right)$$

Demostración. Esta demostración es completamente análoga a la prueba del Teorema A.5.3 y por esa razón se omite. □

DESARROLLO DEL ANILLO DE GALOIS $GR(2^2, 2^4)$

A continuación, se aplican los conceptos más importantes estudiados a lo largo del Capítulo 3 en el anillo de Galois $GR(2^2, 2^4)$, de manera que el lector pueda apreciar la implementación de éstos de manera concreta, y que su conocimiento de las propiedades antes enunciadas, no sea sólo teórica. A la vez se invita a que el lector realice un ejemplo particular para mejorar la comprensión de los conceptos vistos en este trabajo.

Considérese $GR(2,4) = \mathbb{Z}_4 = \{0,1,2,3\}$ con único ideal maximal $\langle 2\rangle = 2\mathbb{Z}_4$ y el polinomio $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$, aplicando el epimorfismo (2.1.8) tenemos que

$\overline{h}(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$, luego dado que $\overline{h}(0) = \overline{h}(1) = 1$, no tiene raíces en $\mathbb{F}_2$ y por ser de grado 2, es irreducible, entonces es un polinomio mónico básico irreducible y entonces tenemos que $\mathbb{Z}_4[x]/\langle h(x)\rangle = GR(2^2, 2^4)$, además tomando a θ una raíz de $\overline{h}(x)$, tenemos:

$$\theta^2 + \theta + 1 = 0 \Rightarrow \theta^2 = \theta + 1 \Rightarrow \theta^3 = \theta^2 + \theta = 1$$

de aquí se sigue que $h(x)$ es un polinomio mónico básico primitivo también, puesto que $\mathbb{F}_{2^2}^* = (\theta)$ y denotando $R = GR(2^2, 2^4) = \mathbb{Z}_4[x]/(h(x))$, tenemos, por el Teorema 3.3.1 que existe un elemento $\xi \in R$ de orden 3, $h(\xi) = 0$, $h(x) \mid x^3 - 1$ en $\mathbb{Z}_4[x]$, $\overline{\xi} = \theta$ y $R \simeq \mathbb{Z}_4[\xi]$. En efecto dado que

$$\begin{aligned}\left(x^2 + x + 1\right)(x + 3) &= x^3 + x^2 + x + 3x^2 + 3x + 3\\ &= x^3 + 3\\ &= x^3 - 1\end{aligned}$$

por lo tanto $h(x) \mid x^3 - 1$. Ahora, tomando ξ una raíz de $h(x)$ tenemos que $\xi^2 + \xi + 1 = 0$, entonces $\xi^2 = 3\xi + 3$ y luego $x^3 = 3\xi^2 + 3\xi = (\xi + 1) + 3\xi = 1$, así $ord(\xi) = 3$, se sigue que $\overline{\xi} = \theta$ y así el conjunto de Teichmüller de R está dado por $\mathcal{T} = \{0, 1, \xi, \xi^2\} = \{0, 1, \xi, 3\xi + 3\}$, y por el isomorfismo antes mencionado, podemos denotar:

$$R = \{0, 1, 2, 3, \xi, \xi + 1, \xi + 2, \xi + 3, 2\xi, 2\xi + 1, 2\xi + 2, 2\xi + 3, 3\xi, 3\xi + 1, 3\xi + 2, 3\xi + 3\}$$

y todo elemento de R puede representarse de manera única mediante $c = a_0 + a_1 \cdot 2$ con $a_0, a_1 \in \mathcal{T}$, es decir, los elementos de R tienen su representación $2-ádica$.

0	$0 + 0(2)$	ξ	$\xi + 0(2)$	2ξ	$0 + \xi(2)$	3ξ	$\xi + \xi(2)$
1	$1 + 0(2)$	$\xi + 1$	$[3\xi + 3] + [3\xi + 3](2)$	$2\xi + 1$	$1 + \xi(2)$	$3\xi + 1$	$[3\xi + 3] + 1(2)$
2	$0 + 1(2)$	$\xi + 2$	$\xi + 1(2)$	$2\xi + 2$	$0 + [3\xi + 3](2)$	$3\xi + 2$	$\xi + [3\xi + 3](2)$
3	$1 + 1(2)$	$\xi + 3$	$[3\xi + 3] + \xi(2)$	$2\xi + 3$	$1 + [3\xi + 3](2)$	$3\xi + 3$	$3\xi + 3 + 0(2)$

Figura 6: Representación 2-ádica de los elementos de $GR(4, 16)$

es fácil verificar que las representaciones son correctas aplicando aritmética módulo 4. Por otro lado, como el ideal maximal de $R = GR(4, 16)$ es $\langle 2\rangle = \{0, 2, 2\xi, 2\xi + 2\}$, tenemos que $R^* = \{1, 3, \xi, \xi + 1, \xi + 2, \xi + 3, 2\xi + 1, 2\xi + 3, 3\xi, 3\xi + 1, 3\xi + 2, 3\xi + 3\}$ es el grupo de unidades del anillo de Galois $GR(4, 16)$, en este caso note que $p = 2$ y $s = 2$, entonces por el Teorema 3.4.1 R^* es producto directo de $G_1 = \langle \xi\rangle$ un grupo cíclico de orden $p^m - 1 = 2^2 - 1 = 3$ y un grupo abeliano G_2 el cual es producto directo de $m = 2$ grupos cíclicos cada uno de orden $p^{(s-1)} = 2^{2-1} = 2$. En dicho teorema nos inidica que podemos denotar $G_2 = \{1 + \pi \mid \pi \in (2)\} = \{1, 3, 2\xi + 1, 2\xi + 3\}$ luego note que

$$\begin{aligned}1 &= (1)(1)\\ 3 &= (1)(3)\\ 2\xi + 1 &= (1)(2\xi + 1)\\ 2\xi + 3 &= (3)(2\xi + 1)\end{aligned}$$

es decir, todo elemento de G_2 es producto de los elementos de los grupos cíclicos $\langle 3\rangle$ y $\langle 2\xi+1\rangle$ los cuales son tales $\langle 3\rangle \cap \langle 2\xi+1\rangle = \{1\}$ y esto implica que $G_2 = \langle 3\rangle \times \langle 2\xi+1\rangle$, y en consecuencia tenemos que $R^* = \langle \xi\rangle \times (\langle 3\rangle \times \langle 2\xi+1\rangle)$ como afirmamos. Además si consideramos a $GR(4,4) = \mathbb{Z}_4$ como subanillo de $GR(4,16)$ podemos definir el automorfismo generalizado de Frobenius considerando $p = 2$, $m = 1$, $s = 2$ y $l = 2$ en la Definición 3.6.2 como sigue:

$$\begin{aligned} \Phi : GR(4,16) &\longrightarrow GR(4,16) \\ a_0 + a_1\xi &\longmapsto a_0 + a_1\xi^2 \end{aligned}$$

donde, $\xi^2 = 3\xi + 3$. Entonces, las imágenes de cada elemento en $GR(4,16)$ bajo Φ es:

α	$\Phi(\alpha)$	α	$\Phi(\alpha)$	α	$\Phi(\alpha)$	α	$\Phi(\alpha)$
0	0	ξ	$3+3\xi$	2ξ	$2+2\xi$	3ξ	$1+\xi$
1	1	$1+\xi$	3ξ	$1+2\xi$	$3+2\xi$	$1+3\xi$	$2+\xi$
2	2	$2+\xi$	$1+3\xi$	$2+2\xi$	2ξ	$2+3\xi$	$3+\xi$
3	3	$3+\xi$	$2+3\xi$	$3+2\xi$	$1+2\xi$	$3+3\xi$	ξ

Es bueno prestar antención que estamos en el caso de un anillo de Galois $GR(p^s, p^{sml})$ con un subanillo $GR(p^s, p^{sm})$ donde $p = 2, s = 2, m = 1, l = 2$, así que, podemos definir la traza y la norma generalizada de todo elemento en $GR(4,16)$, así,

$$\begin{aligned} Tr : GR(4,16) &\longrightarrow GR(4,16) \\ a_0 + a_1\xi &\longmapsto (a_0 + a_1\xi) + \left(a_0 + a_1\xi^2\right) \end{aligned} \qquad \begin{aligned} N : GR(4,16) &\longrightarrow GR(4,16) \\ a_0 + a_1\xi &\longmapsto (a_0 + a_1\xi)\left(a_0 + a_1\xi^2\right) \end{aligned}$$

como en la Definición 3.7.1.

A RESULTADOS COMPLEMENTARIOS

En este apéndice enunciaremos resultados que fueron omitidos de algunas secciones, por cuestiones de espacio. Si R es un anillo con unidad 1_R, usaremos solamente 1 para denotar a dicho elemento, el elemento $p1 \in R$ con $p \in \mathbb{N}$ un número primo, se expresa a menudo solamente por p cuando el contexto es claro, y en general para cada $n \in \mathbb{Z}$, $n1$ se suele denotar solo por n.

ALGUNAS PROPIEDADES ADICIONALES EN ANILLOS CONMUTATIVOS

Teorema A.1.1. *Sea p un número primo.*

(i) $p \mid \binom{p}{i}$ *cada vez que* $1 \leqslant i \leqslant p-1$.

(ii) *Si R es un anillo con unidad de característica p entonces, para todo $r, s \in R$ $(r+s)^p = r^p + s^p$ y $(r-s)^p = r^p - s^p$.*

(iii) *Si R es un anillo con unidad de característica p, un número primo. Entonces, para todo $r, s \in R$ y para todo $n \in \mathbb{N}$, se cumple que $(r \pm s)^{p^n} = r^{p^n} \pm s^{p^n}$*

Demostración. (i) Sabemos que $\binom{p}{i} = p!/(i!)(p-i)!$ y que éste es un número natural. Despejando $p!$ tenemos que $p! = \binom{p}{i}[(i!)(p-i)!]$ y es evidente que $p \mid p! = \binom{p}{i}[(i!)(p-i)!]$, luego por la primalidad de p, éste divide a alguno de los tres factores, pero $p \nmid i!$ puesto que $i < p$ y de manera similar $p \nmid (p-i)!$ por lo tanto sólo ocurre que $p \mid \binom{p}{i}$.

(ii) Por el por el Teorema del Binomio:

$$(r+s)^p = \sum_{i=0}^{p} \binom{p}{i} r^{p-i}s^i = r^p + \sum_{i=1}^{p-1} \binom{p}{i} r^{p-i}s^i + s^p = r^p + s^p \tag{A.1.1}$$

en la expresión (A.1.1) la igualdad se sigue de que la característica de R es p y de la primera parte de este teorema, puesto que todo el término de la suma es idéntico a cero al estar multiplicado por un múltiplo de p. Finalmente note que $r = (r-s)+s$ entonces $r^q = [(r-s)+s]^q = (r-s)^q + s^q$ por lo demostrado anteriormente, restando de ambos lados s^q se obtiene el resultado deseado.

(iii) Hagamos inducción sobre n, el caso $n = 1$ ya se demostró en el apartado anterior. Supongamos que para $n \in \mathbb{N}$ el resultado es válido y veamos que se cumple para $n+1$. Como

$$(r+s)^{p^{n+1}} = \left((r+s)^{p^n}\right)^p = \left(r^{p^n} + s^{p^n}\right)^p = r^{p^{n+1}} + s^{p^{n+1}}$$

con lo cual el resultado queda demostrado en el caso de la suma, para el otro caso, basta con proceder como en el inciso anterior. □

Lema A.1.2. *Sean* p *un elemento en un anillo* R *y* $n, m \in \mathbb{N}$ *con* $n \geqslant m$*, entonces* $p^n - 1 = c(p^m - 1) - (p^r - 1)$ *para algúnos* $c, r \in \mathbb{N}$ *con* $0 \leqslant r < m$ *y en consecuencia* $(p^m - 1) \mid (p^n - 1)$ *si y sólo si* $m \mid n$.

Demostración. Como $\mathbb{Z}$ es un anillo euclidiano, entonces para n y m existen $q, r \in \mathbb{N}$ tales que $n = qm + r$ con $0 \leqslant r < m$ entonces $p^n - 1 = p^{qm+r} - 1$ y entonces haciendo la división larga obtenemos que

$$\begin{aligned} p^{qm+r} - 1 &= (p^{(q-1)m+r})(p^m - 1) + p^{(q-1)m+r} - 1 \\ &= (p^{(q-1)m+r})(p^m - 1) + (p^{(q-2)m+r})(p^m - 1) + p^{(q-2)m+r} - 1 \\ &= (p^{(q-1)m+r} + p^{(q-2)m+r})(p^m - 1) + p^{(q-2)m+r} - 1 \\ &\vdots \end{aligned}$$

procediendo de esta forma q veces llegamos a la expresión

$$p^n - 1 = \sum_{i=1}^{q-1} \left(p^{(q-i)m+r}\right)(p^m - 1) + p^r - 1 \tag{A.1.2}$$

luego, nombrando c a la suma, se obtiene la primera parte de éste lema. Ahora, si $m \mid n$ entonces como $n = qm + r$, sólo puede ocurrir que $r = 0$, así, $p^r = 1$ y sustituyendo en (A.1.2); $p^n - 1 = c(p^m - 1) + 1 - 1 = c(p^m - 1)$, en otras palabras, $p^m - 1 \mid p^n - 1$. Análogamente, si $p^m - 1 \mid p^n - 1$, $p^r - 1 = 0$, esto implica que $r = 0$, por lo que, $m \mid n$ como queríamos demostrar. □

Corolario A.1.3. *Sean* $n, m \in \mathbb{N}$ *con* $n \geqslant m$*, entonces* $m \mid n$ *si y sólo si* $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$.

Lema A.1.4. *Sean* R *un anillo conmutativo con unidad,* $r, s \in R$*,* p *un número primo y* $l \in \mathbb{N}$*. Entonces,* $(r + ps)^{p^l} = r^{p^l} + p^{l+1}t$*; para algún* $t \in R$.

Demostración. Haremos inducción sobre l. Como p es un número primo, entonces $p \geqslant 2$, así $p = 2 + q$ para $q \geqslant 0$ y $q \in \mathbb{Z}$. Si $l = 1$ entonces, por el Teorema del Binomio:

$$\begin{aligned} (r + ps)^p &= \sum_{i=0}^{p} \binom{p}{i} (r)^{p-i}(ps)^i = r^p + \sum_{i=1}^{p-1} \binom{p}{i} (r)^{p-i}(ps)^i + (ps)^p \\ &= r^p + p^2 s \sum_{i=1}^{p} b_i (r)^{p-i}(ps)^{i-1} + p^2 s^2 (ps)^q \\ &= r^p + p^2 s \sum_{i=1}^{p} b_i (r)^{p-i}(ps)^{i-1} + s^2 (ps)^q \quad \text{(por (i) del Teorema A.1.1)} \\ &= r^p + p^2 t, \end{aligned}$$

claramente, t ocupa el lugar de la suma en la penúltima igualdad. Supóngase que para $l \in \mathbb{N}$, el resultado se cumple, verifiquemos que para $l+1$ también. Escribiendo:

$$\begin{aligned}
(r+ps)^{p^{l+1}} &= \left((r+ps)^{p^l}\right)^p \\
&= \left(r^{p^l} + p^{l+1}t_1)\right)^p && \text{(con } t_1 \in R\text{. Por hipótesis inductiva)} \\
&= (\rho + p\sigma)^p && \text{(con } \rho = r^{p^l},\ \sigma = p^l t_1\text{)} \\
&= \rho^p + p^2 t_2 && \text{(por el caso } l = 1\text{)} \\
&= r^{p^{l+1}} + p^{l+2}t && (t = t_1 t_2 \in R)
\end{aligned}$$

□

Teorema A.1.5. *[Fórmula de Taylor] Sea* R *un anillo conmutativo con unidad y considere un polinomio* $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ *en* $R[x]$*. Para todo* $b \in R$ *y* $n \in \mathbb{N}$ *se cumple que:*

$$f(x+b) = f(x) + \frac{f'(x)}{1!}b + \frac{f''(x)}{2!}b^2 + \cdots + \frac{f^{(n)}(x)}{n!}b^n$$

Demostración. Veamos que para todo $k \in \mathbb{N}$, si $1 \leqslant k \leqslant n$ entonces la $k-$ésima derivada de x^n es $\frac{n!}{(n-k)!}x^{n-k}$. En efecto, sea $n \in \mathbb{N}$ fijo y suponga que $k = 1$, entonces tenemos que, derivando una vez $(x^n)' = nx^{n-1}$, recordemos que $n! = n((n-1)!)$ entonces $n!/(n-1)! = n$, entonces se cumple el resultado para $k = 1$. Ahora, supongamos que para cada $l < k$ el resultado es válido, veamos que éste se cumple para k. Para ver esto, calculemos $(x^n)^{(k)} = \left((x^n)'\right)^{(k-1)} = \left(nx^{n-1}\right)^{(k-1)}$, luego por la hipótesis inductiva para $k-1 < k$,

$$(x^n)^{(k)} = n\left(\frac{(n-1)!}{((n-1)-(k-1))!}x^{(n-1)-(k-1)}\right) = \frac{n(n-1)!}{(n-k)!}x^{n-k} = \frac{n!}{(n-k)!}x^{n-k} \quad \text{(A.1.3)}$$

como habíamos afirmado. En particular, para $k = n$ se tiene que $(x^n)^{(n)} = n!$. Además, para cada $n \in \mathbb{N}$, por el Teorema del Binomio, $(x+b)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}b^k$ y note que $\binom{n}{k}x^{n-k} = \frac{n!}{k!(n-k)!}x^{n-k} = \frac{1}{k!}\left(\frac{n!}{(n-k)!}x^{n-k}\right)$ por consiguiente, de (A.1.3), se sigue que,

$$(x+b)^n = \sum_{k=0}^{n}\frac{(x^n)^{(k)}(x)}{k!}b^k \quad \text{(A.1.4)}$$

Usando lo anterior, como $f(x+b) = a_0 + a_1(x+b) + a_2(x+b)^2 + \cdots + a_n(x+b)^n$ entonces

$$\begin{aligned}
f(x+b) &= a_0 + a_1 \sum_{k=0}^{1} \frac{(x)^{(k)}(x)}{k!} b^k + \sum_{k=0}^{2} \frac{(x^2)^{(k)}(x)}{k!} b^k + \cdots + \sum_{k=0}^{2} \frac{(x^n)^{(k)}(x)}{k!} b^k \\
&= a_0 + a_1 \left(\frac{x}{0!} + \frac{(x)'}{1!} b \right) + a_2 \left(\frac{x^2}{0!} + \frac{(x^2)'}{1!} b + \frac{(x^2)''}{2!} b^2 \right) + \cdots \\
&\quad + a_n \left(\frac{x^n}{0!} + \frac{(x^n)'}{1!} b + \cdots + \frac{(x^n)^{(n)}}{n!} b^n \right) \\
&= a_0 + a_1(x+b) + a_2 \left(x^2 + 2xb + \frac{2!}{2!} b^2 \right) + \cdots + a_n \left(x^n + nx^{n-1} b + \cdots + \frac{n!}{n!} b^n \right) \\
&= (a_0 + a_1 x + \cdots + a_n x^n) + \frac{1}{1!} \left(a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \right) b + \cdots \\
&\quad + \frac{1}{2!} \left(2a_2 + 6a_3 x + \cdots + n(n-1) a_n x^{n-2} \right) b^2 + \cdots + \frac{1}{n!} \left(n! a_n \right) b^n \\
&= f(x) + \frac{f'(x)}{1!} b + \frac{f''(x)}{2!} b^2 \cdots + \frac{f^{(n)}(x)}{n!} b^n \qquad \text{como queríamos demostrar.}
\end{aligned}$$

□

Lema A.1.6. *Sean x una indeterminada, $p \geqslant 3$ un número primo y $n \in \mathbb{N}$. Nombremos a_t, b_t, c_t a los coeficientes de x^t en el desarrollo de las expresiones $(1+px)^n$, $(1+2x)^n$ y $(1+4x)^n$, respectivamente. Luego, si*

i) $p^e \mid n$, *entonces* $p^{e+1} \mid a_1$ *y* $p^{e+2} \mid a_t$ *para* $2 \leqslant t \leqslant n$.

ii) $2^e \mid n$, *entonces* $2^{e+1} \mid b_t$ *para* $t = 1, 2$ *y* $2^{e+2} \mid b_t$ *para* $3 \leqslant t \leqslant n$.

iii) $2^e \mid n$, *entonces* $2^{e+2} \mid c_1$ *y* $2^{e+3} \mid c_t$ *con* $2 \leqslant t \leqslant n$.

iv) $4 \mid c_t$ *para* $1 \leqslant t \leqslant n$.

Demostración. Note que en general tenemos:

$$\binom{n}{t} = \frac{n!}{(n-t)!t!} = \frac{n}{t} \left(\frac{(n-1)!}{((n-1)-(t-1))!(t-1)!} \right)) = \frac{n}{t} \binom{n-1}{t-1} \tag{A.1.5}$$

y por el Teorema del Binomio, $(1+\alpha x)^n = \sum_{i=0}^{n} \binom{n}{i} \alpha^i x^i$, demostremos ahora el resultado.

(i) Supóngase que $\alpha = p$, $a_1 = np$ y $a_t = \binom{n}{t} p^t$, para $2 \leqslant t \leqslant n$. Como $p^e \mid n$ existe algún $n' \in \mathbb{Z}$ tal que $n = n' p^e$ así tenemos que $a_1 = n' p^e p = n' p^{e+1}$ por tanto $p^{e+1} \mid a_1$. Suponga que $p^f \mid t$ pero que $p^{f+1} \nmid t$ para $f \in \mathbb{N} \cup \{0\}$, entonces $t = p^f t'$ con $mcd(p, t') = 1$. De (A.1.5) tenemos que $t\binom{n}{t} = n\binom{n-1}{t-1}$, entonces $t \mid n\binom{n-1}{t-1} = p^e n' \binom{n-1}{t-1}$ y $t' \mid t$ luego $t' \mid n' \binom{n-1}{t-1}$ pues $mcd(p, t') = 1$ se sigue que $(n'/t')\binom{n-1}{t-1} \in \mathbb{Z}$, una vez más usando (A.1.5) tenemos que:

$$a_t = \frac{n}{t} \binom{n-1}{t-1} p^t = \frac{n' p^{e+t}}{t' p^f} \binom{n-1}{t-1} = \left(p^{e-f+t} \right) \frac{n'}{t'} \binom{n-1}{t-1} \tag{A.1.6}$$

así, por (A.1.6) $p^{e-f+t} \mid a_t$. Ahora, si $f = 0$ es claro que $t \geqslant 2 + f$ y si $f > 0$ entonces $p^f \geqslant f + 2$ pues p es un primo impar, además como $p^f \mid t$ se sigue que $t \geqslant p^f \geqslant f + 2$,

en ambos casos podemos ver que $-f+t \geqslant 2$ por lo tanto $e-f+t \geqslant e+2$ así, $p^{e+2} \mid p^{e-f+t} \mid a_t$ para $2 \leqslant t \leqslant n$.

(ii) Ahora sean, $\alpha = 2$, $b_1 = 2n$, $b_2 = 4\binom{n}{2}$ y $b_t = 2^t\binom{n}{t}$, para $3 \leqslant t \leqslant n$. Como $2^e \mid n$ entonces $n = 2^e n'$ para algún $n' \in \mathbb{Z}$, luego $2^{e+1} \mid 2^{e+1}n' = b_1$, además por (A.1.5) tenemos que,

$$b_2 = 4\left(\frac{2^e n'}{2}\right)\binom{n-1}{1} = 2^{e+1}(n-1)n'$$

es decir, $p^{e+1} \mid b_1, b_2$. Por otro lado, supongamos que $2^f \mid t$ pero $2^{f+1} \nmid t$, es decir $t = 2^f t'$ con $mcd(2, t') = 1$. Procediendo como antes demostramos que $(n'/t')\binom{n-1}{t-1} \in \mathbb{Z}$ y con (A.1.6) para $p = 2$ tenemos:

$$b_t = \frac{n}{t}\binom{n-1}{t-1}2^t = \frac{2^{e+t}n'}{2^f t'}\binom{n-1}{t-1} = \left(2^{e-f+t}\right)\frac{n'}{t'}\binom{n-1}{t-1} \tag{A.1.7}$$

se sigue que $2^{e-f+t} \mid b_t$, ahora, como $t \geqslant 3$ si $0 \leqslant f \leqslant 1$ entonces $e-f \geqslant e-1$ y así $e-f+t \geqslant e+2$, luego $2^{e+2} \mid 2^{e-f+t} \mid b_t$. Finalmente, para $f \geqslant 2$ es claro que $2^f > f+2$ y dado que $t \geqslant 2^f$ se sigue que $t > f+2$ así $e-f+t > e+2$ por lo tanto $2^{e+2} \mid 2^{e-f+t} \mid b_t$.

(iii) Considérense, $\alpha = 4$ $c_1 = 4n = 2^2 n$ y $c_t = \binom{n}{t}4^t = \binom{n}{t}2^{2t}$, para $2 \leqslant t \leqslant n$. Como en (ii) usemos $n = 2^e n'$ y $t = 2^f t'$ con $mcd(2, t') = 1$ entonces $c_1 = 2^2(2^e)n' = 2^{e+2}n'$ en conclusión $2^{e+2} \mid c_1$ y también como $t \geqslant 2$ entonces $2t \geqslant 4$, usando ésto y (A.1.7) se sigue que,

$$c_t = \frac{n}{t}\binom{n-1}{t-1}2^{2t} = \frac{2^{e+2t}n'}{2^f t'}\binom{n-1}{t-1} = \left(2^{e-f+4}\right)\frac{n'}{t'}\binom{n-1}{t-1}$$

una vez más, $(n'/t')\binom{n-1}{t-1} \in \mathbb{Z}$ entonces $2^{e-f+2t} \mid c_t$, finalmente es claro que para $f = 0, 1$ $e-f+2t > e+3$ entonces $2^{e+3} \mid c_t$ y para $f \geqslant 2$ podemos proceder como en la parte final de ii) para llegar a que $2^{e-f+t} > 2^{e+2}$ y como $t > 1$ sumando a la desigualdad anterior se tiene que $e-f+2t > e+3$ por lo tanto $2^{e+3} \mid c_t$ para $2 \leqslant t \leqslant n$.

(iv) Finalmente, como en (iii), $2^{e+2} \mid c_t$ para $1 \leqslant t \leqslant n$, es evidente que $4 \mid 4(2^e) = 2^{e+2}$ y podemos concluir que $4 \mid c_t$. □

MÁS PROPIEDADES SOBRE CAMPOS FINITOS

Teorema A.2.1. *Sean* $\mathbb{F}$ *un campo finito,* $L, K \leqslant \mathbb{F}$ *tales que* $L \leqslant K$ *entonces*

$$[\mathbb{F} : L] = [\mathbb{F} : K][K : L].$$

En la sección 1.8 se estudiaron generalidades sobre los campos finitos y se finalizó con un teorema que asegura la existencia de polinomios irreducibles con coeficientes en un campo finito, en los presentes resultados nos sumergiremos en el estudio de sus propiedades.

Teorema A.2.2. *Sean* $f(x)$ *un polinomio irreducible con coeficientes en un campo finito* $\mathbb{F}_q$ *y* α *una raíz de éste. Para todo polinomio* $h(x) \in \mathbb{F}_q[x]$*, se tiene que* $h(\alpha) = 0$ *si y sólo si* $f(x) \mid h(x)$.

Demostración. Supongamos que c es el coeficiente principal del polinomio $f(x)$, veamos que el polinomio mónico, $m(x) = c^{-1}f(x)$ es el polinomio mínimo del elemento α en $\mathbb{F}_q[x]$. Sea $m_1(x)$ el polinomio mínimo de α en $\mathbb{F}_q[x]$, como $m(\alpha) = c^{-1}f(\alpha) = 0$, por el Teorema 1.8.19 $m_1(x) \mid m(x)$, luego, $m(x) = q(x)m_1(x)$ para $q(x) \in \mathbb{F}_q[x]$. Si $\operatorname{grad}(q(x)) = 0$ entonces es un polinomio constante y, como $m(x)$ y $m_1(x)$ son mónicos, es claro que $q(x) = 1$, así, $m(x) = m_1(x)$. Sin embargo, suponiendo que $\operatorname{grad}(q(x)) > 0$ entonces tenemos que $f(x) = am(x) = aq(x)m_1(x)$ y $\operatorname{grad}(q(x)) < \operatorname{grad}(f(x))$ lo cual contradice que $f(x)$ sea irreducible, por lo tanto $m(x) = m_1(x)$. Ahora, si $h(x) \in \mathbb{F}_q[x]$ es un polinomio tal que $h(\alpha) = 0$, es claro que $m(x) \mid h(x)$ entonces $f(x) = am(x) \mid h(x)$. Si $f(x) \mid h(x)$ entonces $h(x) = q(x)f(x)$, con $q(x) \in \mathbb{F}_q[x]$; evaluando α tenemos que $h(\alpha) = q(\alpha)f(\alpha) = 0$, pues α es raíz de $f(x)$. □

Lema A.2.3. *Sea* $f(x)$ *un polinomio irreducible con coeficientes en un campo finito* $\mathbb{F}_q$*. Si* $\operatorname{grad}(f(x)) = m$ *entonces* $f(x) \mid x^{q^n} - x$ *si y sólo si* $m \mid n$.

Demostración. Supongamos que $f(x) \mid x^{q^n} - x$, como $f(x)$ es irreducible, por el Teorema 1.8.17, existe una extensión de $\mathbb{F}_q$ definida por una raíz de $f(x)$, sea pues $\mathbb{F}_q(\alpha)$ esta extensión, por el Teorema 1.8.20, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Note que $\alpha^{q^n} - \alpha = q(\alpha)f(\alpha) = 0$ donde $q(\alpha)$ es la imagen de α bajo algún $q(x) \in \mathbb{F}_q[x]$[1], entonces α es también raíz de $x^{q^n} - x$, por consiguiente pertenece al campo de descomposición de dicho polinomio, el cual es, por el Teorema 1.8.25, $\mathbb{F}_{q^n}$, así por el Teorema A.2.1 $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)]m$, por lo tanto $m \mid n$. Si $m \mid n$, por el Criterio del subcampo $\mathbb{F}_{q^m} \leqslant \mathbb{F}_{q^n}$. Considere a α una raíz de $f(x)$ en $\mathbb{F}_q(\alpha)$ como antes y así, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, es decir $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ ya que los subcampos son únicos, pero se sigue que $\alpha \in \mathbb{F}_{q^n}$, luego $\alpha^{q^n} = \alpha$ es inmediato observar que α es raíz de $x^{q^n} - x$ y por el teorema anterior $f(x) \mid x^{q^n} - x$. □

Lema A.2.4. *Si* $f(x)$ *es un polinomio irreducible en* $\mathbb{F}_q[x]$ *con* $\operatorname{grad}(f(x)) = m > 0$*, entonces* $f(x)$ *tiene una raíz* θ *en* $\mathbb{F}_{q^m}$ *y todas las raíces de* $f(x)$ *son simples y están dadas por los* m *distintos elementos* $\theta, \theta^q, \theta^{q^2}, \ldots, \theta^{q^{m-1}} \in \mathbb{F}_{q^m}$.

Demostración. Si θ es una raíz de $f(x)$ en el campo de escisión de $f(x)$, entonces como ya vimos antes, $[\mathbb{F}_q(\theta) : \mathbb{F}_q] = m$, por el Criterio del subcampo $\mathbb{F}_q(\theta) = \mathbb{F}_{q^m}$ y en consecuencia $\theta \in \mathbb{F}_{q^m}$, con lo cual la primera afirmación queda demostrada. Para la segunda, veamos primero que si $\theta \in \mathbb{F}_{q^m}$ es tal que $f(\theta) = 0$ entonces $f(\theta^q) = 0$, en efecto, considere a $f(x) = c_m x^m + \cdots + c_1 x + c_0$ con $c_j \in \mathbb{F}_q$ para $j \in \{0, 1, \ldots, m-1, m\}$, así:

$$\begin{aligned} f(\theta^q) &= c_m(\theta^q)^m + \cdots + c_1(\theta)^q + c_0 \\ &= c_m^q(\theta^m)^q + \cdots + c_1^q(\theta)^q + c_0^q && (c_j^q = c_j, \text{ pues } c_j \in \mathbb{F}_q) \\ &= (c_m\theta^m + \cdots + c_1\theta + c_0)^q && (\text{por el Teorema A.1.1, pues } q = p^l) \\ &= (f(\theta))^q = 0 \end{aligned}$$

1 Esto puesto que $f(x) \mid x^{q^n} - x$

ahora, como $f(\theta^q) = 0$, usando el mismo argumento se demuestra que $f\left(\theta^{q^2}\right) = 0$, así, sucesivamente hasta $f\left(\theta^{q^{m-1}}\right) = 0$, entonces los elementos θ^i son raíces de $f(x)$ para $i \in \{0, 1, \ldots, m-1\}$. Suponga que para $i, k \in \{0, 1, \ldots, m-1\}$ con $i < k$ $\theta^{q^i} = \theta^{q^k}$, entonces se sigue que

$$\left(\theta^{q^i}\right)^{q^{m-k}} = \left(\theta^{q^k}\right)^{q^{m-k}}$$

aplicando leyes de los exponentes, se obtiene $\theta^{q^{i+m-k}} = \theta^{q^m} = \theta$, luego $\theta^{q^{i+m-k}} - \theta = 0$, entonces θ es raíz de $x^{m-(k-i)} - x$. Note que $m-(k-i) < m$ pero, por el Teorema A.2.2, $f(x) \mid x^{q^{m-(k-i)}} - x$ y por el Lema A.2.3, $m \mid m-(k-i)$ lo cual es una contradicción, así $i = k$. Por lo tanto todas las raíces son distintas y al ser m, éstas son todas raíces simples. □

Los resultados siguientes son consecuencias inmediatas de lo ya revisado e incluso sus demostraciones son parte de los resultados previos.

Corolario A.2.5. *Sea $f(x)$ un polinomio irreducible en $\mathbb{F}_q[x]$ de grado $m \in \mathbb{N}$. Entonces*

(i) *El campo de descomposición de $f(x)$ es $\mathbb{F}_{q^m}$.*

(ii) *Dos polinomios irreducibles en $\mathbb{F}_q[x]$ con el mismo grado, tienen campos de descomposición isomorfos.*

(iii) *Si E es una extensión de $\mathbb{F}_q$, entonces todo elemento $a \in E$ satisface que $a^q = a$ si y sólo si $a \in \mathbb{F}_q$.*

Demostración. (i) y (ii) se siguen del lema anterior y el Teorema 1.8.23, así que, demostraremos (iii). Supóngase que $a^q = a$, entonces a es raíz de $x^q - x \in \mathbb{F}[x]$, para $\mathbb{F} \leqslant \mathbb{F}_q$, luego a pertenece al campo de descomposición de $f(x)$, por el Teorema 1.8.25 éste es $\mathbb{F}_q$, por lo tanto, $a \in \mathbb{F}_q$. La suficiencia se sigue del Teorema 1.8.6. □

Lema A.2.6. *Sea $f(x)$ un polinomio en $\mathbb{F}_p[x]$ un polinomio de grado $m \geqslant 1$, tal que $f(0) \neq 0$. Entonces existe $n \in \mathbb{N}$ tal que $n \leqslant p^m - 1$ y $f(x) \mid x^n - 1$.*

Demostración. El anillo de clases residuales $\mathbb{F}_p[x]/\langle f(x)\rangle$ posee al menos una clase distinta de cero $(1 + \langle f(x)\rangle)$ y a lo más $p^m - 1$. Si consideramos el conjunto $\{x^j + \langle f(x)\rangle \mid j \in \{0, 1, \ldots, m-1\}\}$, podemos observar que éste contiene p^m clases distintas de cero, pues si alguna fuera cero entonces $x^j \in \langle f(x)\rangle$, es decir $f(x) \mid x^j$ con $j < m = \mathrm{grad}(f(x))$ lo cual es una contradicción. Pero lo anterior implica que existen $r, s \in \{0, 1, \ldots, m-1\}$ tales que $x^r + \langle f(x)\rangle = x^s + \langle f(x)\rangle$ y $r \neq s$, de lo contrario ya habría p^m clases distintas de cero, lo cual no puede ser. Supongamos sin pérdida de generalidad que $0 \leqslant r < s \leqslant p^{m-1}$, dado que $x^r - x^s \in \langle f(x)\rangle$ entonces podemos denotar $x^r \equiv x^s \pmod{f(x)}$, así podemos elegir $0 < n = s - r \leqslant p^m - 1$ y entonces $x^n \equiv 1 \pmod{f(x)}$, es decir, existe $n \leqslant p^m - 1$ tal que $f(x) \mid x^n - 1$. □

CONCEPTO FORMAL DE MONOMORFISMO, EPIMORFISMO E ISOMORFISMO

A lo largo de este trabajo, los homomorfimos de grupos y anillos fueron usados con frecuencia. Hemos considerado necesario hacer mención de las definiciones precisas de **monomorfismo**, **epimorfismo** e isomorfismo en la teoría de grupos y anillos, para tener una visión más general del concepto. Usaremos la notación multiplicativa para la composición de funciones, como se hace en la literatura relacionada a la Teoría de Categorias, esto es, $f \circ g = fg$.

Definición A.3.1. Sean G y G' grupos y $\phi : G \to G'$ un homomorfismo de grupos. Decimos que ϕ es

1. un **monomorfismo de grupos** si para cada grupo H y cada par de homomorfismos de grupos $\alpha : H \to G$ y $\beta : H \to G$ tales que $\phi\alpha = \phi\beta$, entonces se tiene que $\alpha = \beta$.

2. un **epimorfismo de grupos** si para cada grupo H y cada par de homomorfismos de grupos $\alpha : G' \to H$ y $\beta : G' \to H$ tales que $\alpha\phi = \beta\phi$, entonces se tiene que $\alpha = \beta$.

3. un **bimorfismo de grupos** si es monomorfismo y epimorfismo de grupos.

4. un **isomorfismo de grupos** si existe un homomorfismo $\psi : G' \to G$ tal que $\phi\psi = id_{G'}$ y $\psi\phi = id_G$. Además decimos que G y G' son **isomorfos** cuando existe un isomorfismo $\phi : G \to G'$ y denotamos esto por $G \simeq G'$.

Nótese que se definen los monomorfismos y epimorfismos de grupos en términos de leyes cancelativas como ya se dijo en la nota siguiente a la Definición 1.2.1, y como es de esperarse mostraremos las equivalencias allí mencionadas.

Lema A.3.2. *Sean $(G, *)$, $(G', \cdot)$ grupos, y $\phi : G \to G'$ un homomorfismo de grupos. Entonces ϕ es un monomorfismo de grupos si y sólo si ϕ es inyectiva.*

Demostración. Veamos que si ϕ es un monomorfismo de grupos entonces $\ker\phi = \{e\}$. Para esto, considérense $H = \ker\phi$ y los homomorfismos $\alpha = \iota : H \to G$ y $\beta = \overline{e} : H \to G$, la inclusión de $\ker\phi$ en G y el homomorfismo neutro respectivamente. Entonces, para todo $k \in \ker\phi$:

$$(\phi\alpha)(k) = \phi(\alpha(k)) = \phi(k) = e = \phi(e) = \phi(\beta(k)) = (\phi\beta)(k).$$

Por lo tanto, $\phi\alpha = \phi\beta$ y ya que, ϕ es un monomorfismo, se sigue que $\alpha = \beta$, por consiguiente, para toda $k \in \ker\phi$, $k = \alpha(k) = \beta(k) = e$, es decir, $\ker\phi = \{e\}$, por el Lema 1.2.5 se tiene que ϕ es inyectiva. Por otro lado, si ϕ es inyectiva, considérense H un grupo, $\alpha : H \to G$ y $\beta : H \to G$ tales que $\phi\alpha = \phi\beta$, entonces para todo $h \in H$ tenemos que:

$$(\phi\alpha)(h) = (\phi\beta)(h) \Rightarrow \phi(\alpha(h)) = \phi(\beta(h)) \tag{A.3.1}$$

dado que ϕ es inyectiva, se sigue de la expresión (A.3.1) que $\alpha(h) = \beta(h)$ para toda $h \in H$, entonces $\alpha = \beta$,por lo tanto, ϕ es un monomorfismo. □

Antes de demostrar la segunda equivalencia veamos un lema que será de utilidad para este efecto.

Lema A.3.3. *Si* $H \leqslant G$ *tal que* $H \neq G$. *Entonces existen un grupo* L *y homomorfismos de grupos distintos* α *y* β *de* G *en* L *tales que* $\alpha(H) = \beta(H)$.

Lema A.3.4. *Sean* $(G, *)$, $(G', \cdot)$ *grupos y* $\phi : G \to G'$ *un homomorfismo de grupos. Entonces* ϕ *es suprayectiva si y sólo si* ϕ *es un epimorfismo.*

Demostración. Sean H un grupo, $\alpha : G' \to H$ y $\beta : G' \to H$ tales que $\alpha\phi = \beta\phi$. Sea $g' \in G'$ entonces existe $g \in G$ tal que $\phi(g) = g'$, pues ϕ es suprayectiva, luego

$$\alpha(g') = \alpha(\phi(g)) = (\alpha\phi)(g) = (\beta\phi)(g) = \beta(\phi(g)) = \beta(g')$$

para cada $g' \in G'$, por lo tanto, $\alpha = \beta$, es decir, ϕ es un epimorfismo. Supóngase ahora que ϕ es un epimorfismo y que $\phi(G) \neq G'$. Como $\phi(G) \leqslant G'$, por el Lema A.3.3, existen H un grupo y dos homomorfismos distintos α y β de G' en H tales que $\alpha(\phi(G)) = \beta(\phi(G))$, pero esto implica que $\alpha(\phi) = \beta(\phi)$ y como ϕ es un epimorfismo se sigue que $\alpha = \beta$, lo que es una contradicción, así, $\phi(G) = G'$, por lo tanto ϕ es suprayectiva. □

Lema A.3.5. *Sean* $(G, *)$, $(G', \cdot)$ *grupos y* $\phi : G \to G'$ *un homomorfismo de grupos. Entonces* ϕ *es un isomorfismo si y sólo si es biyectiva.*

Demostración. Supóngase que ϕ es un isomorfismo, entonces existe un homomorfismo $\psi : G' \to G$ tal que, $\psi\phi = id_G$ y $\phi\psi = id_{G'}$. Sean $x, y \in G$ tales que $\phi(x) = \phi(y)$, luego por hipótesis $x = id_G(x) = \psi\phi(x) = \psi(\phi(y)) = id_G(y) = y$, es decir, ϕ es inyectiva. Considérese ahora $y \in G'$, como $y = id_{G'}(y) = \phi(\psi(y))$, sin embargo, $\psi : G' \to G$, es decir, $\psi(y) \in G$, llamémosle x, entonces existe $x \in G$ tal que $\phi(x) = y$, por lo tanto, ϕ es suprayectiva y en consecuencia, biyectiva.

Supóngase que ϕ es un homomorfismo biyectivo, entonces existe una función $\phi^{-1} : G' \to G$ tal que $\phi\phi^{-1} = id_{G'}$ y $\phi^{-1}\phi = id_G$. Resta ver que ϕ^{-1} es un homomorfismo de grupos. Sean $x, y \in G'$ entonces existen únicos $g, h \in G$ tales que $\phi(g) = x$ y $\phi(h) = y$, así:

$$\phi^{-1}(xy) = \phi^{-1}(\phi(g)\phi(h)) = \phi^{-1}(\phi(g * h)) = g * h = \phi^{-1}(x) * \phi^{-1}(y)$$

así, tenemos que ϕ^{-1} es un isomorfismo, más aún, como ϕ es inyectiva y suprayectiva, por los Lemas A.3.2 y A.3.4, ϕ es un monomorfismo y epimorfismo, por consiguiente, es un bimorfismo. □

Definición A.3.6. Sean $(R, +, \cdot, 0, 1_R)$ y $(S, +', \cdot', 0', 1_S)$ anillos conmutativos con unidad y $\phi : R \to S$ un homomorfismo de anillos. Decimos que ϕ es

1. un **monomorfismo de anillos** si para cada anillo R' y cada par de homomorfismos de anillos $\alpha : R' \to R$ y $\beta : R' \to R$ tales que $\phi\alpha = \phi\beta$, entonces se tiene que $\alpha = \beta$.

2. un **epimorfismo de anillos** si para cada anillo R' y cada par de homomorfismos de anillos $\alpha : S \to R'$ y $\beta : S \to R'$ tales que $\alpha\phi = \beta\phi$, entonces se tiene que $\alpha = \beta$.

3. un **isomorfismo de anillos** si existe un homomorfismo $\psi : S \to R$ tal que $\phi\psi = id_S$ y $\psi\phi = id_R$. Además decimos que R y S son **isomorfos** cuando existe un isomorfismo $\phi : R \to S$ y denotamos esto por $R \simeq S$.

Lema A.3.7. *Sean R, S anillos y $\phi : R \to S$ un homomorfismo de anillos.Entonces*

(i) *ϕ es un monomorfismo si y sólo si ϕ es un homomorfismo inyectivo.*

(ii) *Si ϕ es una función suprayectiva, entonces es un epimorfismo.*

(iii) *ϕ es un isomorfismo si y sólo si es un homomorfismo biyectivo.*

Demostración. (i) Sea $f : R \to S$ un monomorfismo que no es inyectivo, luego existen $r_1, r_2 \in R$ con $r_1 \neq r_2$ pero $f(r_1) = f(r_2)$. También considere los homomorfismos $\alpha : \mathbb{Z}[x] \to R$ y $\beta : \mathbb{Z}[x] \to R$ definidos por $\alpha(t(x)) = r_1$ y $\beta(t(x)) = r_2$ para cada $t(x) \in \mathbb{Z}[x]$. Sea $t(x) \in R$ entonces $f(\alpha(t(x)) = f(r_1) = f(r_2) = f(\beta(t(x))$, se sigue que $f\alpha = f\beta$ y como f es un monomorfismo, se sigue que, $\alpha = \beta$, esto implica que, $r_1 = r_2$, lo que es una contradicción, así f debe ser inyectiva. Supóngase que ϕ es un homomorfismo inyectivo y sean R' un anillo, α y β homomorfismos de anillos de R' en R tales que $\phi\alpha = \phi\beta$, de manera análoga al caso de grupos, usando la expresión (A.3.1) y tomando $h \in R'$, se sigue que, $\alpha(h) = \beta(h)$, es decir, $\alpha = \beta$, por lo tanto ϕ es un monomorfismo.

(ii) Sean ϕ un homomorfismo de anillos suprayectivo, R' un anillo y dos homomorfismos α y β de S en R', tales que $\alpha\phi = \beta\phi$. Considérese $s \in S$, como ϕ es suprayectiva entonces existe $r \in R$, tal que $\phi(r) = s$. Por otro lado,

$$\alpha(s) = \alpha(\phi(r)) = \alpha\phi(r) = \beta\phi(r) = \beta(\phi(r)) = \beta(s)$$

es decir, $\alpha = \beta$, por lo tanto, ϕ es un epimorfismo.

(iii) La biyectividad se sigue de la definición de isomorfismo, como en el Lema A.3.5. Supóngase que ϕ es un homomorfismo de anillos biyectivo, de manera similar al Lema A.3.5, veamos que ϕ^{-1} es un homomorfismo de anillos. Como ϕ es biyectiva, extonces dados $s_1, s_2 \in S$ existen únicos $r_1, r_2 \in R$ tales que $\phi(r_1) = s_1$ y $\phi(r_2) = s_2$, así,

$$\begin{aligned}\phi^{-1}(s_1 +' s_2) &= \phi^{-1}(\phi(r_1) +' \phi(r_2)) = \phi^{-1}(\phi(r_1 + r_2)) \\ &= \phi^{-1}\phi(r_1 + r_2) = r_1 + r_2 = \phi^{-1}(s_1) + \phi^{-1}(s_2)\end{aligned}$$

, por otro lado,

$$\begin{aligned}\phi^{-1}(s_1 \cdot' s_2) &= \phi^{-1}(\phi(r_1) \cdot' \phi(r_2)) = \phi^{-1}(\phi(r_1 r_2)) \\ &= \phi^{-1}\phi(r_1 r_2) = r_1 r_2 = \phi^{-1}(s_1)\phi^{-1}(s_2)\end{aligned}$$

por lo tanto, ϕ^{-1} es un homomorfismo de anillos, así, ϕ es un isomorfismo. □

AUTOMORFISMOS

En las secciones 3.6 y 3.7 de este trabajo, se estudian los automorfismos, la traza y la norma generalizadas, en algunos de éstos, se hizo referencia a que las demostraciones eran análogas al caso de un campo finito, por tanto se muestran a continuación las demostraciones y los conceptos clave relacionados.

Definición A.4.1. Sea $\mathbb{F}_{q^n}$ una extensión de un campo finito $\mathbb{F}_q$.

1. Si $\alpha \in \mathbb{F}_q$, entonces los elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}} \in \mathbb{F}_{q^n}$ son llamados **los conjugados** de α respecto a $\mathbb{F}_q$.
2. Una función $\psi : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ es un **automorfismo**[2] si y sólo si es un isomorfismo, además, ψ se dirá un **automorfismo de** $\mathbb{F}_{q^n}$ **sobre** $\mathbb{F}_q$ si para todo $a \in \mathbb{F}_q$ se tiene que $\psi(a) = a$.
3. El conjunto $\{\psi \mid \psi \text{ es un automorfismo de } \mathbb{F}_{q^n} \text{ sobre } \mathbb{F}_q\}$ es llamado el **grupo de Galois** de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y lo denotamos mediante $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

Teorema A.4.2. *Sea $\mathbb{F}_{q^n}$ un campo finito. La función:*

$$\begin{array}{rccc} \sigma: & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ & a & \longmapsto & a^q \end{array}$$

*es un automorfismo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, llamado **automorfismo de Frobenius** y es tal que:*

(i) *El conjunto $G = \{id_{\mathbb{F}_{q^n}}, \sigma, \ldots, \sigma^{n-1}\}$, donde $\sigma^{j+1} = \sigma^j \circ \sigma$ para $j = 2, \ldots, n-1$ forma un grupo cíclico de orden n con la composición de funciones como operación binaria.*

(ii) $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \sigma \rangle$.

Demostración. Sean $a, b \in \mathbb{F}_{q^n}$ entonces $\sigma(a+b) = (a+b)^q = a^q + b^q$ pues $q = p^l$, es decir $\sigma(a+b) = \sigma(a) + \sigma(b)$, también $\sigma(ab) = (ab)^q = a^q b^q$ por la conmutatividad de $\mathbb{F}_{q^n}$, entonces $\sigma(ab) = \sigma(a)\sigma(b)$ y así σ es un homomorfismo. Si tenemos que $\sigma(a) = 0$ entonces $a^q = 0$, lo cual implica que $a = 0$, o bien, a es un divisor de cero, pero esto no puede ser ya que $\mathbb{F}_{q^n}$ es un campo, así sólo ocurre que $a = 0$ y por tanto $\ker \sigma = \{0\}$, luego σ es un monomorfismo. Puesto que $\mathbb{F}_{q^n}$ es un conjunto finito y σ es inyectiva, se sigue que σ es un epimorfismo y en consecuencia un automorfismo de $\mathbb{F}_{q^n}$. Ahora, dado un elemento $\alpha \in \mathbb{F}_q$, tenemos que, por el Teorema 1.8.6 $\sigma(\alpha) = \alpha^q = \alpha$, es decir σ es un automorfismo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y así $\sigma \in Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

(i) Sabemos que las funciones biyectivas de un conjunto X en sí mismo, forman un grupo con la composición de funciones, donde el elemento identidad es $e = id_X$. Si elegimos $X = \mathbb{F}_{q^n}$ entonces σ es un elemento de este grupo. Veamos que $ord(\sigma) = n$, para esto, note que $dom(\sigma^n) = dom(\sigma) = \mathbb{F}_{q^n} = dom(id_{\mathbb{F}_{q^n}})$. Note que dado $a \in \mathbb{F}_{q^n}$, $\sigma^2(a) = \sigma(\sigma(a)) = (a^q)^q = a^{q^2}$, entonces $\sigma^3(a) = \sigma(\sigma^2(a)) = \left(a^{q^2}\right)^q = a^{q^3}$, en general note que $\sigma^j(a) = a^{q^j}$ con $j \in \mathbb{N}$ y si $j = n$ entonces $\sigma^n(a) = a^{q^n} =$

2 La definición de un automorfismo es más general, sin embargo se enuncia para campos finitos por utilidad.

$a = id_{\mathbb{F}_{q^n}}(a)$, entonces $\sigma^n = id_{\mathbb{F}_{q^n}}$, o en otras palabras $ord(\sigma) = n$ y así $\langle\sigma\rangle$ es un subgrupo cíclico de orden n y en lo sucesivo, podemos denotar $1 = id_{\mathbb{F}_{q^n}}$.

(ii) Ya que $\sigma \in Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$ entonces $\langle\sigma\rangle \subseteq Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Considere a ψ un automorfismo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y b un elemento primitivo en $\mathbb{F}_{q^n}$, luego existe su polinomio mínimo $m(x)$ el cual es mónico, irreducible y de grado n sobre $\mathbb{F}_q$. Suponga que $m(x) = x^n + c_{m-1}x^{m-1} + \cdots + c_2x^2 + c_1x + c_0$, luego $m(b) = b^n + c_{m-1}b^{m-1} \cdots + c_2b^2 + c_1b + c_0 = 0$, así,

$$\begin{aligned} 0 &= \psi(b^n + c_{m-1}b^{m-1} \cdots + c_2b^2 + c_1b + c_0) \\ &= \psi(b)^m + c_{m-1}\psi(b)^{m-1} \cdots + c_2\psi(b)^2 + c_1\psi(b) + c_0 \end{aligned}$$

la última igualdad es consecuencia de que $c_i \in \mathbb{F}_q$ para $i \in \{0, 1, \ldots, n-1\}$ y $\psi \in Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Además también se deduce que $\psi(b)$ es una raíz de $m(x)$, y como éste último es irreducible, el Lema A.2.4, nos dice que $\psi(b) = b^{q^j}$ para algún $j \in \{0, 1, \ldots, n-1\}$, es decir, $\psi = \sigma^j \in \langle\sigma\rangle$, por lo tanto $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \subseteq \langle\sigma\rangle$, lo cual nos lleva a la igualdad deseada. □

Corolario A.4.3. *Sea σ el automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ y considere a $d \in \mathbb{N}$ tal que $d \mid n$. Entonces*

(i) *σ^d es el automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_{q^d}$ y $Gal(\mathbb{F}_{q^n}/\mathbb{F}_{q^d}) = \langle\sigma^d\rangle$ es un grupo cíclico de orden n/d.*

(ii) *Para todo $a \in \mathbb{F}_{q^d}$, $\sigma(a) \in \mathbb{F}_{q^d}$. Si denotamos la restricción de σ a $\mathbb{F}_{q^d}$ por $\sigma|_{\mathbb{F}_{q^d}}$, entonces la función,*

$$\begin{aligned} \sigma|_{\mathbb{F}_{q^d}}: \ \mathbb{F}_{q^d} &\longrightarrow \mathbb{F}_{q^d} \\ a &\longmapsto \sigma(a) \end{aligned}$$

está bien definida, es el automorfismo de Frobenius de $\mathbb{F}_{q^d}$ sobre $\mathbb{F}_q$ y $Gal(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle\sigma|_{\mathbb{F}_{q^d}}\rangle$ es un grupo cíclico de orden d.

Demostración. (i) Por el teorema anterior, $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ son todos los automorfismos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, entonces $\sigma^d(a) = a^{q^d}$ para todo $a \in \mathbb{F}_{q^n}$. Ya aclaramos que σ^d es un automorfismo y note que si $a \in \mathbb{F}_{q^d}$ entonces $a = 0$ o bien $a \in \mathbb{F}_{q^d}^*$. Si $a = 0$ es evidente que $a^{q^d} = 0 = a$, y como $\mathbb{F}_{q^d}^*$ es un grupo (cíclico) de orden $q^d - 1$ entonces $a^{q^d-1} = 1$ y en consecuencia $\sigma^d(a) = a^{q^d} = a$, luego por lo visto antes, σ^d es el automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_{q^d}$ y por el teorema anterior $Gal(\mathbb{F}_{q^n}/\mathbb{F}_{q^d}) = \langle\sigma^d\rangle$ y como $\langle\sigma^q\rangle \lhd \langle\sigma\rangle$, por el Teorema de Lagrange $o\left(\langle\sigma^d\rangle\right) = [\mathbb{F}_{q^n} : \mathbb{F}_{q^d}] = n/d$ como afirmamos.

(ii) Si $a \in \mathbb{F}_{q^d}$, por la cerradura del producto es claro que $a^q \in \mathbb{F}_{q^d}$, así $\sigma|_{\mathbb{F}_{q^d}}(a) = \sigma(a) = a^q \in \mathbb{F}_{q^d}$, esto implica que $\sigma|_{\mathbb{F}_{q^d}}\left(\mathbb{F}_{q^d}\right) \subseteq \mathbb{F}_{q^d}$. Es claro que $dom\left(\mathbb{F}_{q^d}\right) = \mathbb{F}_{q^n} \cap \mathbb{F}_{q^d} = \mathbb{F}_{q^d}$, luego podemos escribir, $\sigma|_{\mathbb{F}_{q^d}}: \mathbb{F}_{q^d} \longrightarrow \mathbb{F}_{q^d}$. Por otro lado, sea $a \in \mathbb{F}_{q^d}$ tal que $\sigma|_{\mathbb{F}_{q^d}}(a) = a^q$ y $\sigma|_{\mathbb{F}_{q^d}}(a) = b^q$, para $b \in \mathbb{F}_q^n$. Luego, como $b^q \in \mathbb{F}_{q^n}$ y σ es un epimorfismo, entonces existe $\lambda \in \mathbb{F}_{q^n}$ tal que $\sigma(\lambda) = b^q = \sigma(a)$ pero σ es inyectiva, luego $a^q = \lambda^q = b^q$, por lo tanto $a^q = b^q$, así $\sigma|_{\mathbb{F}_{q^d}}$

está bien definida. Además, sean $a, b \in \mathbb{F}_{q^d}$ tales que $\sigma|_{\mathbb{F}_{q^d}}(a) = \sigma|_{\mathbb{F}_{q^d}}(b)$ esto implica que $\sigma(a) = \sigma(b)$ y de la inyectividad de σ tenemos que $a = b$, entonces $\sigma|_{\mathbb{F}_{q^d}}$ es inyectiva y nuevamente como $\mathbb{F}_{q^d}$ es un conjunto finito en combinación a lo dicho antes, tenemos que $\sigma|_{\mathbb{F}_{q^d}}$ es un automorfismo. Finalmente, para todo elemento $\alpha \in \mathbb{F}_q$ es claro que $\sigma|_{\mathbb{F}_{q^d}}(\alpha) = \alpha^q = \alpha$, por lo tanto $\sigma|_{\mathbb{F}_{q^d}}$ deja fijos a los elementos de $\mathbb{F}_q$, entonces éste es el automorfismo de Frobenius de $\mathbb{F}_{q^d}$ sobre $\mathbb{F}_q$, por lo tanto $\langle \sigma|_{\mathbb{F}_{q^d}} \rangle = Gal\left(\mathbb{F}_{q^d}/\mathbb{F}_q\right)$ y nuevamente, por el Teorema de Lagrange $o\left(\langle \sigma|_{\mathbb{F}_{q^d}} \rangle\right) = [\mathbb{F}_{q^d} : \mathbb{F}_q] = d$. □

TRAZA Y NORMA

Definición A.5.1. Sea $\mathbb{F}_q$ un campo finito y $a \in \mathbb{F}_{q^n}$. Definimos respectivamente la **traza** y la **norma** de α relativa a $\mathbb{F}_q$ mediante:

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = a + a^q + \cdots + a^{q^{n-1}}$$
$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = aa^q \cdots a^{q^{n-1}}$$

cuando el contexto sea claro, podemos omitir los subíndices $\mathbb{F}_{q^n}/\mathbb{F}_q$ y nos referimos a estas funciones solamente como traza y norma respectivamente.

En la sección 3.8 se hizo un análisis de propiedades de la norma y traza generalizada, aludiendo a la similitud en un par de resultados clásicos sobre estas funciones. Presentamos a continuación el desarrollo de las demostraciones de esas propiedades.

Teorema A.5.2. *Para $a, b \in \mathbb{F}_{q^n}$ y $l \in F_q$ tenemos:*

i) $Tr(a) \in \mathbb{F}_q$	*i)'* $N(a) \in \mathbb{F}_q$
ii) $Tr(a+b) = Tr(a) + Tr(b)$	*ii)'* $N(ab) = N(a)N(b)$
iii) $Tr(la) = lTr(a)$	*iii)'* $N(la) = l^n N(a)$
iv) $Tr(l) = nl$	*iv)'* $N(l) = l^n$
v) $Tr(a^q) = Tr(a)$	*v)'* $N(a^q) = N(a)$

Demostración. (i), (i)' Apliquemos el automorfismo de Frobenius a la traza y norma. Esto es $\sigma(Tr(a)) = \sigma\left(a + a^q + \cdots + a^{q^{n-1}}\right) = \sigma(a) + (\sigma(a))^q + \cdots + (\sigma(a))^{q^{n-1}}$ y $\sigma(N(a)) = \sigma\left(aa^q \cdots a^{q^{n-1}}\right) = \sigma(a)(\sigma(a))^q \cdots (\sigma(a))^{q^{n-1}}$, recuerde que $(\sigma(a))^{q^j} = a^{q^{j+1}}$ y $a^{q^n} = a$ luego, reordenando términos se tiene que

$$\sigma(Tr(a)) = a + a^q + \cdots + a^{q^{n-1}} = Tr(a)$$
$$\sigma(N(a)) = aa^q \cdots a^{q^{n-1}} = N(a)$$

por (iii) del Corolario A.2.5 se tiene que $Tr(a), N(a) \in \mathbb{F}_q$.

(ii), (ii)′ Note que $p \mid q^j$ para toda $j \in \{1, 2, \ldots, n-1\}$, entonces por el Teorema A.1.1

$$\begin{aligned}
\mathrm{Tr}(a+b) &= (a+b) + (a+b)^q \cdots + (a+b)^{q^{n-1}} \\
&= (a+b) + (a^q + b^q) + \cdots + \left(a^{q^{n-1}} + b^{q^{n-1}}\right) \\
&= \left(a + a^q + \cdots + a^{q^{n-1}}\right) + \left(b + b^q + \cdots + b^{q^{n-1}}\right) \\
&= \mathrm{Tr}(a) + \mathrm{Tr}(b) \\
\mathrm{N}(ab) &= (ab)(ab)^q \cdots (ab)^{q^{n-1}} \\
&= ab a^q b^q \cdots a^{q^{n-1}} b^{q^{n-1}} \\
&= \left(a a^q \cdots a^{q^{n-1}}\right)\left(b b^q \cdots b^{q^{n-1}}\right) \\
&= \mathrm{N}(a)\mathrm{N}(b)
\end{aligned}$$

como afirmamos.

(iii), (iii)′ Para ver esto, considere $l \in \mathbb{F}_q$ entonces podemos ver que $\mathrm{Tr}(la) = la + (la)^q + \cdots + (la)^{q^{n-1}}$ y $\mathrm{N}(la) = (la)(la)^q \cdots (la)^{q^{n-1}}$, como $l^q = l$ entonces $l^{q^j} = l$ para cada $j \in \{1, 2, \ldots, n-1\}$ luego,

$$\begin{aligned}
\mathrm{Tr}(a) &= la + la^q + \cdots + la^{q^{n-1}} = l\left(a + a^q + \cdots + a^{q^{n-1}}\right) = l\mathrm{Tr}(a) \\
\mathrm{N}(a) &= la(la^q) \cdots \left(la^{q^{n-1}}\right) = l^n\left(a a^q \cdots a^{q^{n-1}}\right) = l^n \mathrm{N}(a)
\end{aligned}$$

(iv), (iv)′ Resulta evidente que $\mathrm{Tr}(1) = n$ y $\mathrm{N}(1) = 1$ entonces aplicando (iii) y (iii)′ respectivamente tenemos que $\mathrm{Tr}(1) = \mathrm{Tr}(l1) = l\mathrm{Tr}(1) = ln = nl$ y $\mathrm{N}(1) = \mathrm{N}(l1) = l^n\mathrm{N}(1) = l^n$.(v), (v)′ Procediendo como en los incisos (i) y (i)′ se pueden reordenar los términos para obtener el resultado deseado. □

Teorema A.5.3. *Sea* $\mathbb{F}_{q^n}$ *y* d *un divisor de* n. *Entonces para todo* $a \in \mathbb{F}_{q^n}$

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = \mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a)\right) \text{ y } \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = \mathrm{N}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\left(\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a)\right)$$

Demostración. Por el Corolario A.4.3 si σ es el automorfismo de Frobenius, tenemos que $\mathrm{ord}(\sigma) = n$, $\mathrm{ord}\left(\sigma^d\right) = n/d$ y si denotamos por $\hat{\sigma}$ a la restricción de σ en $\mathbb{F}_{q^d}$ entonces $\mathrm{ord}(\hat{\sigma}) = d$. Además, como $d \mid n$ existe $l \in \mathbb{N}$ tal que $n = ld$, o de otra forma $n/d = l$ y por el teorema anterior, para todo $a \in \mathbb{F}_{q^n}$; $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a) \in \mathbb{F}_{q^d}$, y así la expresión, $\mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a)\right)$ está bien definida y luego,

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a)\right) &= \sum_{i=0}^{d-1} \hat{\sigma}^i\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a)\right) \\
&= \sum_{i=0}^{d-1} \hat{\sigma}^i\left(\sum_{j=0}^{l-1} \sigma^{jd}(a)\right) \\
&= \sum_{i=0}^{d-1} \sigma^i\left(\sigma^0(a) + \sigma^d(a) + \cdots + \sigma^{(n/d-1)d}(a)\right) \qquad (l = n/d) \\
&= \sum_{i=0}^{d-1} \left(\sigma^i(a) + \sigma^{d+i}(a) + \cdots + \sigma^{(n-d)+i}(a)\right)
\end{aligned}$$

evaluando $i = 0, 1, \ldots, d-1$, reordenando términos y usando que $\sigma^0 = id$, tenemos:

$$Tr_{\mathbb{F}_{q^d}/\mathbb{F}_q}\left(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(a)\right) = a + \sigma(a) + \cdots + \sigma^{d-1}(a) + \cdots + \sigma^{d}(a) + \sigma^{n-1}(a) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a)$$

como queríamos demostrar, note que para la norma la prueba es similar y es bueno que el lector lo intente. □

BIBLIOGRAFÍA

[1] Carlet C., Ku-Cauich y Tapia Recillas H., *Bent Functions on a Galois Rings and systematic authentication codes*. Advances in Mathematics of communications Vol. 6 NO. 2 249-258 (2012).

[2] 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.

[3] 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.

[4] Gómez-Calderon J. and Mullen G. L., *Galois rings and algebaic cryptography*, Acta Arithmetica 59 (1991) No. 4, 317-328.

[5] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The Z_4-linearity of kerdock, preparata, goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[6] 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.

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

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

[9] 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.

[10] García Ramírez, A. R., López-Andrade, C. A. (2016) El lema de Hensel y el levantamiento de Hensel, En F. Macías Romero (Ed.), Matemáticas y sus aplicaciones 7 (1a ed., Cap. 2, pp. 53-81, ISBN: 978-607-525-135-6). Textos Científicos, Fomento Editorial de la Benemérita Universidad Autónoma de Puebla, México.

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

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

[13] F. Özbudck and Z. Saygi, *Some constructions of systematic authentication codes using Galois rings*. Desing Codes Cryptography, 41, 343-357 (2006).

[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.