Universidad Autónoma del Estado de Hidalgo
Instituto de Ciencias Básicas e Ingeniería
Área Académica de Matemáticas y Física

Irreducibilidad de polinomios y el polígono de Newton

Tesis que para obtener el grado de

Maestra en Matemáticas

presenta

Annel Ayala Velasco

bajo la dirección de

Dr. Fernando Barrera Mora

Pachuca, Hidalgo, Enero de 2019

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
Instituto de Ciencias Básicas e Ingeniería
School of Engineering and Applied Sciences

Mineral de la Reforma, Hgo., a 28 de noviembre de 2018

Número de control: ICBI-D/1149/2018
Asunto: Autorización de impresión de tesis.

MTRO. JULIO CÉSAR LEINES MEDECÍGO
DIRECTOR DE ADMINISTRACIÓN ESCOLAR DE LA UAEH

Por este conducto le comunico que el comité revisor asignado a la C. Annel Ayala Velasco, alumna de la Maestría en Matemáticas con número de cuenta 215025, autoriza la impresión del proyecto de tesis titulado "Irreducibilidad de polinomios y el polígono de Newton" en virtud de que se han efectuado las revisiones y correcciones pertinentes.

A continuación se registran las firmas de conformidad de los integrantes del comité revisor.

PRESIDENTE	Dr. Rafael Villarroel Flores
SECRETARIO	Dr. Gabriel Villa Salvador
VOCAL	Dr. Fernando Barrera Mora
SUPLENTE	Dr. Ricardo Cruz Castillo

Sin otro particular reitero a Usted la seguridad de mi atenta consideración.

Atentamente
"Amor, Orden y Progreso"

Dr. Óscar Rodolfo Suárez Castillo
Director del ICBI

ORSC/POJM

Ciudad del Conocimiento
Carretera Pachuca-Tulancingo km 4.5 Colonia
Carboneras, Mineral de la Reforma, Hidalgo,
México. C.P. 42184
Teléfono: +52 (771) 71 720 00 ext. 2231
Fax 2109
direccion_icbi@uaeh.edu.mx

Dedicatoria

A mi madre y a la memoria de mi padre.

Agradecimientos

Primeramente quiero agradecer a lo más importante que tengo en mi vida: mi familia. Porque son mi motivación y porque gracias a ellos he aprendido a luchar en la vida.
También quiero agradecer a mi asesor, al Dr. Fernando Barrera Mora, por ser un excelente guía en esta etapa y por el tiempo que me ha dedicado para hablar de la vida.
De igual manera quiero agradecer a mi amiga Betzabé Topete Galván, por las observaciones que hizo a mi trabajo y porque gracias a que compartimos esta etapa juntas tendré muy buenos recuerdos de la maestría. Así mismo, a mi estimado Adán Ángeles Romero, compañero y amigo de la maestría, por los entrañables momentos que compartimos.
Finalmente, quiero hacer un agradecimiento muy especial a mi jurado de tesis, los doctores Gabriel Villa Salvador y Rafael Villarroel Flores, por sus valiosas observaciones que hicieron mejorar este trabajo.

Resumen

En este trabajo analizamos algunos criterios de irreducibilidad de polinomios, más concretamente, centramos la discusión en polinomios de la forma $f(x) = x^{2^n} + rx^{2n-1} + s \in \mathbb{Z}[x]$. La motivación de esta exposición se debe a los resultados que E. Driver, P. A Leonard y K. S Williams exponen en [5], en donde muestran condiciones necesarias y suficientes para que polinomios de la forma $f(x) = x^{2^n} + rx^{2n-1} + s \in \mathbb{Z}[x]$, con $n = 2$, sean irreducibles sobre $\mathbb{Z}$ pero reducibles módulo p para todo primo p. Debido a que no existe un criterio general de irreducibilidad para trinomios, se ha tenido la necesidad de explorar nuevos métodos, por ejemplo, criterios que utilizan la teoría del polígono de Newton. Este método que se define sobre campos locales se emplea para entender propiedades de polinomios.

Con el propósito de mostrar un criterio de irreducibilidad para los polinomios $f(x)$ descritos antes, presentamos algunas propiedades del polígono de Newton. Con este fin, estudiamos a los campos locales desde un punto de vista topológico, además, dado que cualquier campo local de característica 0 es isomorfo a una extensión finita del campo de los números p-ádicos, y si es de característica $p > 0$, es isomorfo al campo de las series de Laurent $K((x))$ sobre un campo finito K [16], fijamos la atención en el campo de los números p-ádicos.

In this work, we present some irreducibility criteria for polynomials, more precisely, we study polynomials of the form $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$. The motivation of this exposition is due to some results that E. Driver, P. A Leonard and K. S Williams present in [5], they consider conditions under which $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$, but reducible module p for every prime p, when $n = 2$. Since there is not a general irreducibility criteria for trinomials, there has been need to explore new methods, for example, criteria that use Newton's polygon theory. This method is defined over local fields and it is used to understand the properties of polynomials.

With the purpose to show an irreducibility criterion for polynomials $f(x)$ mentioned above, we present some properties of Newton's polygon, for which we study

local fields from a topological point of view. Furthermore, since any local field of characteristic 0 is isomorphic to a finite extension of the p-adic numbers and, if it is of characteristic $p > 0$, is isomorphic to the Laurent series $K((x))$ over a finite field K [16], we study the p-adic numbers.

Índice general

Introducción

Gauss en *Disquisitiones Arithmeticae* menciona que uno de los resultados más importantes de la teoría de números es el Teorema Fundamental de la Aritmética; en este resultado se establece que todo entero se escribe, de forma única, como producto de números primos. Este resultado caracteriza algunas clases de anillos en los que la aritmética tiene analogías con la de los enteros. Con este antecedente, es de gran importancia, desde el punto de visto teórico como práctico, decidir si un número entero es primo. A partir de esto, uno de los problemas más importantes en teoría de números, es determinar si un entero es primo, para lo cual se han desarrollado varios criterios de divisibilidad.

Dado que el anillo de polinomios con coeficientes en un campo es un dominio de factorización única, entonces se puede plantear el Teorema Fundamental de la Aritmética para polinomios, más concretamente, todo polinomio $f(x) \in K[x]$ se escribe como producto de polinomios irreducibles de forma única. Recordemos que un polinomio es reducible sobre K si se escribe como producto de polinomios con coeficientes en K de grado menor, en otro caso se dice que es irreducible. La importancia de construir polinomios irreducibles, desde el punto de vista algebraico es, que a partir de ellos se construyen extensiones finitas de campos. Dado que $K[x]$ es un dominio de ideales principales, entonces los irreducibles generan ideales maximales, por lo que $\dfrac{K[x]}{(f(x))}$ es un campo, el cual es isomorfo a $K(\alpha)$, donde α es raíz de $f(x)$. Por otro lado, cuando F/K es una extensión finita y separable, por el Teorema del Elemento Primitivo Lagrange- Galois [1, Teorema 7.1.2] se tiene que $F = K(\alpha)$, donde α es raíz de un polinomo irreducible.
Al igual que en los números enteros racionales, en el anillo de polinomios con coeficientes en un campo se han formulado criterios que permiten decidir si un polinomio es irreducible. El más conocido y de los más remotos, atribuido a Ferdinand Eisenstein en el año 1846, es el criterio que lleva su nombre, el cual se plantea sobre dominios de factorización única. Este resultado esencialmente reduce el problema de factorización de polinomios a factorización de elementos de un anillo. Muchos de los criterios de irreducibilidad de polinomios son parciales, es decir, se aplican a polinomios con algunas restricciones. El único criterio general es el de Capelli, pues muestra condiciones necesarias y suficientes para que un binomio sobre un campo arbitrario K sea irreducible [11]. No existen criterios de manera global, aunque si hay criterios parciales. Por ejemplo, el criterio de Polya, el cual aplica para polinomios $f(x)$ en los cuales sea posible encontrar una cota para una cantidad finita de valores de x, esta cota debe satisfacer las

condiciones planteadas en [3]. Otro tema que ha sido de gran interés es la relación que existe entre los números primos y polinomios irreducibles, aún existen muchas conjeturas sobre la similitud que hay entre ellos. Por ejemplo, el hecho de producir una cantidad infinita de primos a partir de un polinomio irreducible. Cuando el polinomio es lineal primitivo, es decir, sus coeficientes son primos relativos, entonces por el Teorema de Dirichlet sobre progresiones aritméticas, este produce una cantidad infinita de números primos. Para cuando el polinomio produce una cantidad finita de primos se puede concluír que el polinomio es irreducible [17], más aún, bajo ciertas condiciones, basta que el polinomio produzca un número primo para decidir irreducibilidad [17, Theorem 2].

A. Schinzel en [20] presenta una buena cantidad de criterios de irreducibilidad para polinomios en varias variables sobre campos que tienen las propiedades de ser algebraicamente cerrados y finitamente generados. En este trabajo estamos interesados en criterios de irreducibilidad de polinomios en una variable. Para polinomios en varias variables, los criterios de irreducibilidad se relacionan directamente con aspectos geométricos.

El interés de este trabajo es, entre otras cosas, explorar criterios de irreducibilidad sobre los números racionales en casos especiales de familias de polinomios, más concretamente, en polinomios de la forma $f(x) = x^{2^n} + rx^{2^{n-1}} + s$ cuyos coeficientes son enteros. Se tiene, por el Lema de Gauss [1, Teorema 2.1.7], que $f(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si lo es en $\mathbb{Z}[x]$. Existen diversos criterios de irreducibilidad para trinomios los cuales pueden abordar el problema planteado previamente; sin embargo, ninguno es general. Sólo si $n = 2$ o $n = 1$ se sabe exactamente cuándo $f(x)$ es irreducible [5].

El objetivo de abordar esta clase de polinomios se deriva del trabajo que E. Driver, P. A. Leonard y K. S. Williams exponen en [5], en donde analizan condiciones bajo las cuales polinomios de la forma $x^4 + rx^2 + s$ son irreducibles sobre $\mathbb{Z}$ pero reducibles módulo p para todo primo p, más aún, puesto que todo número entero m es producto de potencias de números primos, digamos $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, entonces por el Teorema Chino del Residuo, el problema de decidir reducibilidad módulo m es equivalente a mostrar reducibilidad módulo $p_i^{e_i}$ para todo i, por lo que, de igual modo, encuentran condiciones para las cuales $x^4 + rx^2 + s$ sea irreducible sobre $\mathbb{Z}$ pero reducible módulo m para todo entero positivo m. Podemos observar que si un polinomio mónico es reducible sobre $\mathbb{Z}$ también lo es módulo p para todo primo p, consecuentemente se tiene que si $f(x)$ es un polinomio irreducible módulo p para algún primo p, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$. El recíproco está muy lejos de ser cierto, de hecho, si $f(x)$ es irreducible sobre $\mathbb{Z}$, este puede ser reducible módulo p para todo primo p. Ejemplos de este tipo son los polinomios que E. Driver, P. A. Leonard y K. S. Williams exponen en [5]. De igual modo, M. A. Lee, demuestra en [14] que la familia de polinomios $x^4 + 2(1-a)x^2 + (1+a)^2$, donde a es un entero libre de cuadrado, diferente de 1 y -1, es irreducible sobre $\mathbb{Q}$ pero reducible módulo p para todo primo p. Diversas propiedades algebraicas giran en torno de estos polinomios, pues se sabe que su grupo de Galois es el 4-grupo de Klein, un grupo cíciclo de cuatro elementos o el grupo diédrico de orden 8, [10].

Los polinomios $f(x) = x^{2^n} + rx^{2^{n-1}} + s$ en los que centraremos la discusión en este trabajo se obtienen a partir de la composición de $x^4 + rx^2 + s$ con $x^{2^{n-2}}$ para todo $n > 2$. Como consecuencia de lo anterior, usaremos lo expuesto en [5] para obtener resultados de tales polinomios. Debido a que no existe un criterio general para trinomios, se ha tenido la necesidad de explorar nuevos métodos, por ejemplo criterios que utilizan la teoría del Polígono de Newton. Este método que se define sobre campos locales se emplea para entender propiedades de polinomios tales como información sobre sus raíces y de sus factores irreducibles. Una de las aplicaciones más conocidas de este útil método es la demostración del Criterio de Eisenstein. En este trabajo presentamos propiedades del Polígono de Newton con el propósito de mostrar un criterio de irreducibilidad para $f(x)$. El resultado primordial para la justificación de dicho criterio fue planteado por primera vez por Dumas [4]. En este reporte damos una justificación alterna a este resultado partiendo de casos particulares y usando las ideas que se plantean en [9].

A continuación daremos a conocer el contenido de la tesis. El trabajo se divide en tres capítulos. El objetivo del primero es mostrar la notación, terminología y conceptos básicos que serán necesarios para la exposición. Introducimos el concepto de valuación, la cual es una función particular definida sobre un campo K. Estas funciones permiten, entre otras cosas, construir un subanillo de K denominado anillo de valuación, cuyas propiedades algebraicas son de gran importancia, de igual modo permiten establecer una norma sobre K y, consecuentemente, conceptos tales como convergencia de sucesiones de Cauchy y completez. En este primer capítulo partiremos de una valuación sobre un campo K para definir una norma y construir un campo completo, extensión de K, mostrando de igual manera propiedades y relaciones de los anillos de valuación de cada uno de los campos. Lo anterior es con la finalidad de poder introducir la definición de campo local.

El capítulo dos tiene como objetivo explorar a los campos locales desde un punto de vista topológico. En primer lugar definimos una familia de subconjuntos, la cual resulta una base para la topología de K, más aún, demostraremos que K es un espacio de Hausdorff. Uno de los principales resultados que exponemos es, dado K un campo local y R su anillo de valuación, entonces K es totalmente disconexo, no discreto y localmente compacto, además el anillo de valuación y sus ideales son conjuntos compactos de K, para esto usaremos de manera fundamental el Teorema de Tychonoff y el hecho de que cualquier elemento en K se escribe de forma única como suma de elementos de un subconjunto fijo del anillo de valuación.

Puesto que se sabe que cualquier campo local de característica 0 es isomorfo a una extensión finita del campo de los números p-ádicos y, si es de característica $p > 0$, es isomorfo al campo de las series de Laurent $K((x))$ sobre un campo finito K [16], fijamos la atención en el campo de los números p-ádicos, por esta razón desarrollamos algunas de las propiedades más elementales de dicho campo.

Iniciaremos con el concepto de orden de un número racional, lo cual nos permitirá definir una valuación, denominada valuación p-ádica y, apartir de ello, construir el campo de los números p-ádicos como el campo completo, extensión de $\mathbb{Q}$, bajo la norma inducida por la valuación p-ádica. Una de las propiedades importantes

de valuaciones sobre $\mathbb{Q}$ que exponemos es el Teorema de Ostrowski, el cual establece que toda norma no trivial sobre $\mathbb{Q}$ es equivalente a una norma inducida por una valuación p-ádica o a la norma usual valor absoluto. Así también, mostramos uno de los métodos más empleados para aproximar raíces de polinomios sobre el campo de los números p-ádicos: el Lema de Hensel. Para finalizar este capítulo desarrollamos una sección dedicada a extensiones de normas sobre campos locales, en dicha sección justificamos que toda norma sobre los números p-ádicos se extiende de manera única a cualquier extensión finita. Los resultados expuestos en este capítulo fueron citados de [7], [12] y [8].

Finalmente, estructuramos el capítulo 3 en cuatro secciones. En la primera mostramos algunos de los criterios más conocidos de irreducibilidad, empezando con el criterio de Capelli, el cual es válido para binomios. Para trinomios presentamos los criterios de Nagell y Perron. De igual modo, para polinomios de grado arbitrario exponemos los criterios de Eisenstein y Polya. Así mismo, introduciendo el concepto y desarrollando propiedades del índice de Newton, planteamos un criterio que, además de establecer condiciones para decidir irreducibilidad, determina información sobre los factores irreducibles de un polinomio. El último criterio que mostramos establece una relación entre números primos y polinomios irreducibles, para su justificación será necesario plantear un lema que señala propiedades de las raíces, este último criterio puede extenderse a campos de funciones sobre campos finitos tal como lo plantea R. Murty en [17].

Dedicamos la segunda sección a estudiar el polígono de Newton de un polinomio. Primero mostramos el concepto y en seguida cómo se construye. Puesto que el polígono de Newton se puede considerar como una función lineal a trozos, la primera proposición de esta sección estable una conexión que existe entre las raíces y las pendientes del polígono, para la justificación de este resultado iniciamos retomando las ideas de [9] y finalizamos con una idea alterna, usando propiedades de rectas paralelas. La generalización de este resultado la obtuvimos de [12, Lemma 4, p. 97]. Dumas establece por primera vez una relación entre el polígono de un polinomio y los polígonos de sus factores. Partiendo de casos particulares justificamos este resultado, para ello empezamos mostrando un lema que A. Jorza prueba en [9]. Usando la misma técnica de A. Jorza extendemos el lema previo a un caso más general, se trata del Teorema 3.2.5, pág. 52. Para el caso general, Teorema 3.2.6, pág. 53, usamos los resultados que se plantean sobre los segmentos del polígono de un polinomio y sus raíces. Para finalizar esta sección usando [4, pág. 371] demostraremos el criterio de Eisenstein.

En la tercera sección exploramos a los polinomios de la forma $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$. Para cuando $n = 2$ todos los resultados y demostraciones que exponemos fueron citados de [5], salvo el Teorema 3.3.8, pág. 58, en el cual, retomando algunas ideas de [5] presentamos una demostración diferente. Cuando $n = 3$, logramos encontrar un criterio de irreducibilidad, Teorema 3.3.10, pág. 59, usando propiedades del Polígono de Newton, dicho criterio puede generalizarse para cualquier $n > 3$, Teorema 3.3.14, pág. 64. De igual modo, obtenemos propiedades de $f(x)$ usando el hecho de que es composición de los polinomios $x^{2^k} + rx^{2^{k-1}} + s$ y $x^{2^{n-k}}$.

Finalmente, en la última sección presentamos observaciones finales y preguntas que surgieron durante el desarrollo de este trabajo; esas preguntas ya no fue posible abordar por aspectos de tiempo.
A lo largo del trabajo algunos resultados serán presentados sin demostración debido a que sus pruebas son extensas o no ilustran algunas de las técnicas que estamos empleando, no obstante, daremos las referencias donde pueden consultarse.

CAPÍTULO 1

Notación, terminología y conceptos básicos

En este capítulo presentamos la notación, terminología y resultados básicos que serán necesarios para la exposición del presente trabajo. El objetivo principal es mostrar propiedades de campos sobre los cuales se definen funciones llamadas valuaciones. Dichas funciones permiten establecer el concepto de norma en un campo y, en consecuencia, conceptos tales como sucesiones de Cauchy, convergencia y completez, dicho de otra manera, aspectos topológicos que son de gran utilidad para explorar resultados algebraicos.

1.1. Notación y conceptos básicos

Introducimos a continuación la notación y algunos conceptos que usaremos en el desarrollo del trabajo.

Emplearemos de manera sistemática el concepto de campo, el cual se da por conocido. Utilizaremos la notación usual de inclusión de conjuntos $\subseteq$, así como la de pertenencia $\in$, unión $\cup$, intersección $\cap$ y, dado un conjunto A, $|A|$ denota la cardinalidad de A. El símbolo $\hookrightarrow$ indica inmersión de conjuntos y A^∞ es el conjunto de sucesiones $(a_0, a_1, a_2, \ldots)$, donde $a_i \in A$ para toda i.

Dada una función f y un conjunto A, la expresión $f|_A$ es la función restringida al conjunto A y $f(A)$ la imagen de f sobre A.

Los símbolos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ denotarán a los números naturales, enteros, racionales, reales y complejos respectivamente. Así mismo, $\mathbb{R}^+$, $\mathbb{Z}^+$ y $\mathbb{Q}^+$ representan a los elementos no negativos de cada conjunto.

En algunas ocasiones llamaremos a los números enteros como enteros racionales, esto para diferenciarlos de los enteros algebraicos de un campo numérico.

Al máximo común divisor de los enteros a y b lo denotaremos por $\mathrm{mcd}(a, b)$; en caso de que sean primos relativos esto significará que $\mathrm{mcd}(a, b) = 1$. Si a y b son enteros tales que a divide a b lo expresaremos como $a \mid b$ y si a no divide a b escribiremos $a \nmid b$.

Dado un entero a y un primo impar p, el símbolo de Legendre, denotado $\left(\frac{a}{p}\right)$, se define como sigue:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & si \quad p \text{ divide a } a, \\ -1 & si \quad x^2 \not\equiv a \ mód\, p \text{ para toda } x, \\ 1 & si \quad x^2 \equiv a \ mód\, p \text{ para algún } x. \end{cases} \tag{1.1.1}$$

Algunas propiedades del símbolo de Legendre que necesitaremos en el trabajo las presentamos en el siguiente teorema:

Teorema 1.1.1. *Sea a un entero y p un primo, entonces*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mód \ p,$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$
3. *Si* $a \equiv b \ mód \ p,$ *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$
4. $\left(\frac{l^2a}{p}\right) = \left(\frac{a}{p}\right)$ *para todo entero* l *tal que* $p \nmid l.$

Demostración. 1. Si $p \mid a$, entonces $a \equiv 0$ mód p, por lo que $\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}}$ mód p.
Si $p \nmid a$, por el Pequeño Teorema de Fermat tenemos $a^{p-1} \equiv 1$ mód p, de manera que

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \text{ mód } p, \tag{1.1.2}$$

de ahí que $a^{\frac{p-1}{2}} \equiv \pm 1$ mód p. Usaremos el Hecho 2 de [2, pág. 1] en lo que sigue. Si $a^{\frac{p-1}{2}} = 1$, entonces $x^2 \equiv a$ mód p tiene solución. Si $a^{\frac{p-1}{2}} \equiv -1$, entonces $x^2 \equiv a$ mód p no tiene solución. En ambos casos $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \text{ mód } p$.
2. Por el inciso anterior $\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. Supongamos que $a \equiv b$ mód p. Si $\left(\frac{a}{p}\right) = 1$, entonces $x^2 \equiv a \equiv b$ mód p, para algún x, de modo que $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. De la misma forma si $\left(\frac{a}{p}\right) = -1$ o $\left(\frac{a}{p}\right) = 0$ podemos concluír que $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
4. Supongamos que $\left(\frac{a}{p}\right) = 1$, entonces $x^2 \equiv a$ mód p, para algún x, de manera que $(lx)^2 \equiv l^2 a$ mód p, por lo que $\left(\frac{a}{p}\right) = \left(\frac{l^2a}{p}\right)$. Si $\left(\frac{a}{p}\right) = -1$, entonces $x^2 \not\equiv a$ mód

p, para todo x. Supongamos que $\left(\frac{l^2a}{p}\right) = 1$, entonces existe x tal que $x^2 = l^2a$ mód p, puesto que $\text{mcd}(l, p) = 1$, existen $z, y \in \mathbb{Z}$ tales que $zl + yp = 1$, de modo que $zl \equiv 1$ mód p, así $\frac{1}{l} \equiv z$ mód p (en el sentido que l y z son inversos uno del otro), lo cual implica que $(zx)^2 \equiv a$ mód p, lo cual es una contradicción pues $x^2 \not\equiv a$ mód p, para todo x, consecuentemente $\left(\frac{l^2a}{p}\right) = -1$. Cuando $\left(\frac{l^2a}{p}\right) = 0$ entonces $p \mid a$, en consecuencia $p \mid l^2a$, de modo que $\left(\frac{l^2a}{p}\right) = 0$.

□

Por un anillo, entenderemos un anillo conmutativo con identidad; en caso de que aparezcan anillos más generales lo mencionaremos. Si R es un anillo usaremos las expresiones Rx y (x) para denotar al ideal principal de R generado por el elemento x. Si I es un ideal de R, $\frac{R}{I}$ denotará al anillo cociente. El anillo de polinomios con coeficientes en R será denotado por $R[x]$. Si $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ tal que $a_n = 1$, diremos que $f(x)$ es un polinomio mónico. Un ideal P de R es primo, si cuando $ab \in P$, entonces al menos uno de a o b pertenece a P. Cuando R es campo, usualmente lo denotaremos por K y en este caso si α y α' son raíces del mismo polinomio irreducible diremos que α y α' son conjugados. Dado un campo K, $\overline{K}$ denotará la cerradura algebraica de K y $K^* = K \setminus \{0\}$ al grupo multiplicativo de K. A los campos finitos de cardinalidad igual a q los denotaremos por $\mathbb{F}_q$.
Finalmente, recordamos algunas definiciones y resultados topológicos que emplearemos en el capítulo 2.

Definición 1.1.2. Una topología sobre un conjunto X es una colección τ de subconjuntos de X con las siguientes propiedades:

1. $\emptyset$ y X pertenecen al conjunto τ.
2. La unión de los elementos de cualquier subcolección de τ está en τ.
3. La intersección de los elementos de cualquier subcolección finita de τ está en τ.

Un conjunto X para el que se ha definido una topologiá se llama espacio topológico.

Si X es un espacio topológico con una topología τ, diremos que un conjunto U es abierto de X si pertenece a τ. Llamaremos al conjunto U cerrado si $X \setminus U$ es abierto en X. Si U es un conjunto abierto que contiene a un elemento x, diremos que U es una vecindad de x.

Definición 1.1.3. Si X es un conjunto, una base para una topología sobre X es una colección $\mathcal{B}$ de subconjuntos de X (llamados elementos básicos) tales que:

1. Para cada x en X, hay al menos un elemento básico B que contiene a x.

2. Si x pertenece a la intersección de dos elementos básicos B_1 y B_2, entonces existe un elemento básico B_3 que contiene a x y $B_3 \subseteq B_1 \cap B_2$.

Definición 1.1.4. Una subbase S para una topología sobre X es una colección de subconjuntos de X cuya unión es igual a X. La topología generada por la subbase S se define como la colección τ de todas las uniones de intersecciones finitas de elementos de S.

Recordaremos la siguiente colección de términos para un espacio topológico X:

1. Diremos que X es un espacio Hausdorff, si para cada par de elementos diferentes de X x_1 y x_2, existen conjunto abiertos disjuntos U_1 y U_2 que contienen a x_1 y x_2, respectivamente.

2. Una separación de X es un par U y V de conjuntos abiertos disjuntos no triviales de X cuya unión es X. El espacio X se dice que es conexo si no existe separación de X.

3. Diremos que X es totalmente disconexo si sus únicos subespacios conexos son los conjuntos que consisten de un punto y el vacío.

4. Una colección $\mathcal{A}$ de subconjuntos del espacio X se dice que cubre a A o es una cubierta de A, si la unión de los elementos de $\mathcal{A}$ coincide con X. Se dice que $\mathcal{A}$ es una cubierta abierta de X si los elementos de $\mathcal{A}$ son conjuntos abiertos.

5. El espacio X se dice que es compacto si cada cubierta abierta de $\mathcal{A}$ admite una subcubierta finita que también cubre a X.

6. Diremos que X es localmente compacto en x si existe un subespacio de X compacto que contiene una vecindad de x. Si X es localmente compacto en cada uno de sus puntos, diremos que X es localmente compacto.

7. El espacio X se dice discreto si todo conjunto de X que consiste de un solo elemento es abierto.

Sean $\{X_\alpha\}_{\alpha\in J}$ una familia indexada de espacios topológicos y sea $\pi_\beta : \prod_{\alpha\in J} X_\alpha \to X_\beta$ la función que asigna a cada elemento del espacio producto su coordenada $\beta-$ésima,

$$\pi_\beta((x_\alpha)_{\alpha\in J}) = x_\beta;$$

π_β se denomina proyección asociada con el índice β.
Uno de los resultados que emplearemos en este trabajo es el teorema de Tychonoff, el cual enunciamos después de la siguiente definición:

Definición 1.1.5. Denotemos por S_β a la colección

$$S_\beta = \{\pi_\beta^{-1}(U_\beta) \mid U_\beta \text{ es abierto en } X_\beta\}$$

y denotemos por S a la unión de esas colecciones,

$$S = \bigcup_{\beta \in J} S_\beta.$$

La topología generada por la subbase S se denomina topología producto. En esta topología $\prod_{\alpha \in J} X_\alpha$ se denomina espacio producto

Teorema 1.1.6 (Teorema de Tychonoff)**.** *Sea* $\{Y_\alpha \mid \alpha \in A\}$ *una familia de espacios, entonces* $\prod_\alpha Y_\alpha$ *es compacto si y sólo si* Y_α *lo es para toda* α*.*

Demostración. La demostración de este resultado puede consultarse en [6, Theorem 1.4]. □

1.2. Localización de un anillo

Iniciaremos recordando algunos conceptos básicos de anillos y anillos de valuación.

Definición 1.2.1. Sea R un anillo y $S \subseteq R$. Diremos que S es multiplicativamente cerrado si satisface:

1. el elemento 1 pertenece a S,
2. si $a, b \in S$, entonces $ab \in S$.

Ejemplo 1. Si P es un ideal primo de R, entonces $S = R \setminus P$ es multiplicativamente cerrado. En efecto, sean $a, b \in S$. Si $ab \notin S$, entonces $ab \in P$, pero por definición de ideal primo $a \in P$ o $b \in P$, lo cual no es posible. Por lo que, $ab \in S$.

Sea R un anillo y S un subconjunto multiplicativamente cerrado de R que no contiene a cero. Consideremos al conjunto $R \times S$ y definamos en este conjunto la siguiente relación:

$$(r, s) \sim (a, t), \text{ si existe } u \in S \text{ tal que } u(rt - as) = 0.$$

Se tiene que $\sim$ es una relación de equivalenca. En efecto:

1. (Reflexividad) $(a, b) \sim (a, b)$, pues $1(as - as) = 0$.
2. (Simetría) Si $(a, b) \sim (c, d)$, entonces existe $u \in S$ tal que $u(ad - cb) = 0$. Multiplicando a la igualdad anterior por -1 se tiene $u(cb - ad) = 0$, de modo que $(c, d) \sim (a, b)$.

3. (Transitividad) Si $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$, entonces existen $u_1, u_2 \in S$ tales que $u_1(ad-bc)=0$ y $u_2(cf-de)=0$. Multiplicando por u_2u y su_1 a las ecuaciones anterior, respectivamente, obtenemos $u_2uu_1(ad-bc)=0$ y $su_1u_2(cf-de)=0$, sumando estas igualdades se obtiene $u_1u_2d(af-be)=0$. Tomando $u=u_1u_2d$ concluimos que $(a,b) \sim (e,f)$.

Al conjunto de clases de equivalencia de $R \times S$ bajo la relación $\sim$ definida antes lo denotaremos como $R_S = \dfrac{R \times S}{\sim}$ y los elementos por $\dfrac{a}{s} := [(a,b)]$.
Se definen en R_S las siguientes operaciones:

$$\frac{a}{s} + \frac{b}{t} := \frac{at+bs}{ts}, \tag{1.2.1}$$

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}. \tag{1.2.2}$$

Si $\dfrac{a_1}{b_1} = \dfrac{a_2}{b_2}$ y $\dfrac{c_1}{d_1} = \dfrac{c_2}{d_2}$, entonces existen $u_1, u_2 \in S$ tales que $u_1(a_1b_2 - a_2b_1)=0$ y $u_2(c_1d_2 - c_2d_1)=0$, si multiplicamos a las ecuaciones previas por $d_1d_2u_2$ y $u_1b_1b_2$, respectivamente, y sumando se tiene $u_1u_2(b_2d_2(a_1d_1+c_1b_1) - b_1d_1(a_2d_2+c_2b_2))=0$. Ahora, multiplicando a $u_1(a_1b_2 - a_2b_1)=0$ y $u_2(c_1d_2 - c_2d_1)=0$ por $c_1d_2u_2$ y $a_2b_1u_1$, respectivamente, y restando, obtenemos $u_1u_2(a_1c_1b_2d_2 - a_2c_2b_1d_1)=0$. Lo anterior justifica que las operaciones definidas previamente están bien definidas.
Se verifica sin dificultad que el conjunto R es un anillo con identidad y la función $f_s : R \to R_S$ definida por $f(x) = \dfrac{x}{1}$ es un monomorfismo de anillos, de modo que $R \hookrightarrow R_S$.
Sean R un dominio entero y $S = R \setminus \{0\}$, se tiene que el conjunto S es multiplicativamente cerrado y R_S es un campo. Para demostrar que R_S es campo, basta mostrar que todo elemento de $R_S \setminus \{0\}$ admite un inverso multiplicativo. Sea $\dfrac{a}{b} \in R_S \setminus \{0\}$, entonces $a \neq 0$, de modo que $\dfrac{b}{a} \in R_S$. Además, $\dfrac{a}{b} \cdot \dfrac{b}{a} = \dfrac{ab}{ab} = \dfrac{1}{1} = 1$, pues $ab - ab = 0$.

Definición 1.2.2. Al anillo R_S en la construcción anterior se le denomina anillo local en S. Si R es un dominio entero y $S = R \setminus \{0\}$, al campo construido anteriormente se le llama el campo de cocientes del dominio entero R.

Sean R en un anillo, $\mathfrak{P}$ ideal primo de R y $S = R \setminus \mathfrak{P}$, la localización de R en S se denotará por $R_{\mathfrak{P}}$.

Proposición 1.2.3. *Si R en un anillo y $\mathfrak{P}$ ideal primo de R, entonces $R_{\mathfrak{P}}$ tiene un único ideal máximo $\mathfrak{P}R_{\mathfrak{P}}$.*

Demostración. Esta demostración puede consultarse en [8, Proposición 1.3] □

Ejemplo 2. Sea $R = \mathbb{Z}$ y (p) el ideal primo de R generado por p, donde p es un número primo. Se tiene que $\mathbb{Z}_{(p)} = \left\{ \dfrac{a}{b} \mid \text{mcd}(b,p) = 1 \right\}$ y $(p)\mathbb{Z}_{(p)} = \left\{ p^n \dfrac{a}{b} \mid \dfrac{a}{b} \in \mathbb{Z}_{(p)} \text{ y } n > 0 \right\}$.

Definición 1.2.4. Un anillo R se dice local si contiene un único ideal máximo. En particular, si el anillo es local y de ideales principales diremos que es de valuación discreta.

Definición 1.2.5. Sean R y R' anillos tales que $R \subseteq R'$. Un elemento $\alpha \in R'$ se dice entero sobre R si existe $f(x) \in R[x]$ mónico tal que $f(\alpha) = 0$. Cuando R sea un dominio entero, R' el campo de cocientes de R y todo elemento de R' entero sobre R diremos que R es íntegramente cerrado.

Algunas de las propiedades básicas de un anillo de valuación discreta son las siguientes:

Proposición 1.2.6. *Sea R es un anillo de valuación discreta y $\pi \in R$ tal que $\mathfrak{P} = R\pi$ es el ideal máximo de R. Se tienen las siguientes propiedades:*

1. *R es un anillo noetheriano.*
2. *Todo elemento de R es de la forma $u\pi^k$, para algún entero no negativo k y u unidad en R.*
3. *Todo ideal no cero de R es de la forma $R\pi^k$, para algún k.*
4. *R es íntegramente cerrado.*
5. *R tiene un único ideal primo distinto de $\{0\}$.*

Demostración.

1. Puesto que R es de ideales principales, entonces todo ideal es finitamente generado, por lo tanto R es un anillo noetheriano.

2. Se tiene que R es un dominio de factorización única por ser de ideales principales [1, Teorema 1.5.3], es decir, todo elemento no cero de R es producto finito de elementos irreducibles. Sea M el ideal máximo de R, entonces $M = R\pi$, con π irreducible. Sea $a \in R$, si a no es unidad entonces $(a) \subseteq R\pi$, de modo que $a = r_0\pi$ con $r_0 \in R$, si r_0 es unidad hemos terminado, de otra forma, $(r_0) \subseteq R\pi$ obteniendo que $r_0 = r_1\pi$ para algún $r_1 \in R$, de manera que $r = r_1\pi^2$, procediendo de la misma forma se tiene que $r = r_{k-1}\pi^k$ para algún $k \in \mathbb{N}$. Dado que R es un dominio de factorización única, entonces r_{k-1} es unidad para algún k, por lo tanto $a = u\pi^k$, con u unidad de R y $k \in \mathbb{N}$.

3. Sea I ideal no cero de R, entonces $I = Rx$ para algún $x \in R$. Por el inciso 2 se tiene que $x = \pi^k u$, donde u es unidad de R. Por lo tanto, $I = R\pi^k$.

4. Sean K el campo de fracciones de R y $\dfrac{a}{b} \in K$ un entero, es decir, $\dfrac{a}{b}$ es raíz de un polinomio $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in R[x]$. Se tiene $\left(\dfrac{a}{b}\right)^n + a_{n-1}\left(\dfrac{a}{b}\right)^{n-1} + \ldots + a_1\left(\dfrac{a}{b}\right) + a_0 = 0$. Puesto que R es un dominio de factorización única, entonces podemos suponer que a, b no tienen factores irreducibles en común no triviales. Despejando $\left(\dfrac{a}{b}\right)^n$ y multiplicando por

b^n se tiene $a^n = b\left(\sum_{i=0}^{n} a_i\right)$, de manera que b divide a a^n y, puesto que a y b no tienen factores irreducibles en comun, entonces b es unidad de R. Por lo tanto, $\frac{a}{b} = ua \in R$, con u unidad de R.

5. Debemos probar que el único ideal primo no cero de R es $R\pi$. Sea $R\pi^k$ un ideal de R con $k > 1$. Se tiene que $\pi^{k-1}\pi = \pi^k \in R\pi^k$, sin embargo $\pi^{k-1}, \pi \notin R\pi^k$, por lo tanto $R\pi^k$ no es ideal primo. De modo que, el único ideal primo de R es $R\pi$.

□

1.3. Valuaciones

En esta sección introducimos el concepto de valuación y algunas de sus propiedades. En el desarrollo del trabajo que estamos presentando y en general, en teoría de números el concepto de valuación juega un papel muy relevante.

Definición 1.3.1. Sea K un campo, una valuación v es una función $v : K^* \to \mathbb{R}$ que satisface:

1. para todos $a, b \in K^*$, $v(ab) = v(a) + v(b)$,
2. para todos $a, b \in K^*$ tales que $a + b \in K^*$, $v(a + b) \geq \min\{v(a), v(b)\}$,
3. existe $a \in K^*$ tal que $v(a) \neq 0$.

Se define $v(0) = \infty$.

Proposición 1.3.2. *Sean K un campos y v una valuación sobre K, entonces para todos $a, b \in K^*$ se tiene:*

1. *para todo $a \in K^*$, $v(a) = v(-a)$, $v(1) = 0$ y $v(a^{-1}) = -v(a)$,*
2. *si $v(a) \neq v(b)$, entonces $v(a + b) = \min\{v(a), v(b)\}$,*
3. *si $a_1, a_2, \ldots, a_n$ son elementos de K^*, entonces $v\left(\sum_{i=1}^{n} a_i\right) \geq \min_{1 \leq i \leq n}\{v(a_i)\}$ y la igualdad se cumple si $v(a_i) \neq v(a_j)$ para todos $i \neq j$,*
4. *si $\sum_{i=1}^{n} a_i = 0$, entonces $v(a_i) = v(a_j)$ para algunos $i \neq j$.*

Demostración. 1. Notemos que $v(-a) = v((-1)a) = v(-1) + v(a)$, entonces debemos justificar que $v(-1) = 0$. Se tiene que $v(-1) = v(-1(1)) = v(-1) + v(1)$). De esto se tiene que $v(1) = 0$, entonces $0 = v(1) = v((-1)(-1)) = v(-1) + v(-1) = 2v(-1)$, lo que implica $v(-1) = 0$.

2. Si $v(a) \neq v(b)$, podemos suponer que $v(a) < v(b)$, de modo que, por definición de valuación, $v(a+b) \geq v(a)$. Si demostramos que $v(a) \geq v(a+b)$ entonces tenemos la conclusión del inciso 2.

   Se tiene $v(a) \geq \text{mín}\{v(a+b), v(-b)\} = v(a+b)$, como se quería.

3. Procediendo por inducción, si $n = 1$ no hay nada que probar. Si $n = 2$ el resultado se tiene por definición de valuación. Cuando $n = 3$, $v(a_1+a_2+a_3) \geq \text{mín}\{v(a_1+a_2), v(a_3)\} \geq \text{mín}\{\text{mín}\{v(a_1), v(a_2)\}, v(a_3)\} \geq \text{mín}\{v(a_1), v(a_2), v(a_3)\}$.

   Sea $n > 3$, por hipótesis de inducción se tiene

   $$v\left(\sum_{i=1}^{n} a_i\right) \geq \text{mín}\left\{v\left(\sum_{i=1}^{n-1} a_i\right), a_n\right\} \geq \text{mín}\left\{\min_{1\leq i\leq n-1}\{v(a_i)\}, v(a_n)\right\} = \min_{1\leq i\leq n}\{v(a_i)\}.$$

   Ahora, supongamos $v(a_i) \neq v(a_j)$ para todo $i \neq j$ y $v(a_1) = \min_{1\leq i\leq n}\{v(a_i)\}$, entonces $v\left(\sum_{i=1}^{n} a_i\right) \geq v(a_1)$. Por demostrar que $v(a_1) \geq v\left(\sum_{i=1}^{n} a_i\right)$.

   Observemos que
   $v(a_1) = v\left(a_1 + \sum_{i=2}^{n} a_i - \sum_{i=2}^{n} a_i\right) \geq \text{mín}\left\{v\left(a_1 + \sum_{i=2}^{n} a_i\right), v\left(-\sum_{i=2}^{n} a_i\right)\right\} =$
   $v\left(a_1 + \sum_{i=2}^{n} a_i\right) = v(\sum_{i=1}^{n} a_i)$, pues de lo contrario
   $v(a_1) \geq v\left(-\sum_{i=2}^{n} a_i\right) \geq \min_{2\leq i\leq n}\{v(a_i)\}$, lo cual no es posible.

4. Notemos que $\infty = v\left(\sum_{i=1}^{n} a_i\right) \geq \min_{1\leq i\leq n}\{v(a_i)\}$. Si $\min_{1\leq i\leq n}\{v(a_i)\} = \infty$, entonces $v(a_i) = \infty$ para todo i, de manera que $a_i = 0$ para todo i. Luego, $v(a_i) = v(a_j)$ para todos i y j.

   Si $\min_{1\leq i\leq n}\{v(a_i)\} < \infty$, entonces existen $i \neq j$ tales que $v(a_i) \neq v(a_j)$, pues de lo contrario, usando el inciso anterior, $\infty = v\left(\sum_{i=1}^{n} a_i\right) = \min_{1\leq i\leq n}\{v(a_i)\}$, contradiciendo que $\min_{1\leq i\leq n}\{v(a_i)\} < \infty$.

□

Definición 1.3.3. Una norma o valor absoluto en un campo K es una función $|\ |: K \to \mathbb{R}$ tal que:

1. para todo $x \in K$, $|x| \geq 0$, con $|x| = 0$, solamente cuando $x = 0$.
2. para todos $x, y \in K$, $|xy| = |x||y|$, y
3. $|x+y| \leq |x| + |y|$.

Diremos que $|\ \ |$ es no Arquimediana, si $|x+y| \leq \text{máx}\{|x|,|y|\}$, para todos $x, y \in K$.
Sean K un campo, $v : K^* \to \mathbb{R}$ una valuación y $0 < c < 1$, entonces v define una norma $|\ |_v : K \to \mathbb{R}$ dada por:

$$|x|_v = c^{v(x)}. \tag{1.3.1}$$

En efecto:

1. Para todo $x \in K$, $|x|_v \geq 0$.

2. $|x|_v = 0$ si y sólo si $c^{v(x)} = 0$ si y sólo si $v(x) = \infty$ si y sólo si $x = 0$.

3. Conisderemos la función $f(x) = c^x = e^{x\ln(c)}$, entonces $f'(x) = \ln(c)c^x < 0$, por lo cual que f es decreciente. Ahora, dado que $v(x+y) \geq \text{mín}\{v(x), v(y)\}$, se tiene

$$|x+y|_v = c^{v(x+y)} \leq c^{\text{mín}\{v(x),v(y)\}} = \text{máx}\{|x|_v, |y|_v\}.$$

   Por lo que, $|x+y|_v \leq |x|_p + |y|_v$, para todos $x, y \in K$.

Observación 1.3.4. *Si $|\ \ |$ es una norma inducida por una valuación v, entonces $|\ \ |$ es no arquimediana.*

Definición 1.3.5. Decimos que dos normas $|\ |$ y $|\ |_1$ en un campo K son equivalentes si cuando $|x| < 1$, entonces $|x|_1 < 1$. Cuando $|\ |$ y $|\ |_1$ son equivalentes lo denotamos por $|\ | \sim |\ |_1$.

Teorema 1.3.6. *Sean $|\ \ |$ y $|\ \ |_1$ dos normas no triviales en un campo K. Entonces $|\ \ | \sim |\ \ |_1$ si y sólo si, existe $a \in \mathbb{R}^+ \setminus \{0\}$ tal que $|x| = |x|_1^a$ para todo $x \in K$.*

Demostración. Supongamos que $|\ |$ y $|\ |_1$ son equivalentes. Dado que $|\ |$ y $|\ |_1$ son no triviales, entonces existe $y \in K$ tal que $|y| > 1$ y $|y|_1 > 1$. Sea $a = \dfrac{\ln(|y|_1)}{\ln(|y|)}$ y consideremos a la función real $f(t) = |y|^t$, la cual es creciente. Para cada $x \in K^*$ existe $b_x \in \mathbb{R}$ tal que $|x| = f(b_x) = |y|^{b_x}$. Sea $\left\{\dfrac{m_i}{n_i}\right\} \subset \mathbb{Q}$ tal que $\dfrac{m_i}{n_i} \to b_x$ cuando $i \to \infty$ y $b_x < \dfrac{m_i}{n_i}$ para todo i. Entonces $|x| = |y|^{b_x} < |y|^{\frac{m_i}{n_i}}$, de manera que $\left|\dfrac{x^{n_i}}{y^{m_i}}\right| < 1$, y puesto que $|\ \ |$ y $|\ \ |_1$ son equivalentes entonces $\left|\dfrac{x^{n_i}}{y^{m_i}}\right|_1 < 1$, así $|x|_1 < |y|_1^{\frac{m_i}{n_i}}$, tomando límite cuando $i \to \infty$ en la desigualdad anterior se tiene que $|x|_1 \leq |y|_1^{b_x}$.
Ahora, sea $\left\{\dfrac{m_i}{n_i}\right\} \subset \mathbb{Q}$ tal que $\dfrac{m_i}{n_i} \to b_x$ cuando $i \to \infty$ y $b_x > \dfrac{m_i}{n_i}$ para todo i, entonces $|x| = |y|^{b_x} > |y|^{\frac{m_i}{n_i}}$, de manera que $\left|\dfrac{x^{n_i}}{y^{m_i}}\right| > 1$, y puesto que $|\ |$ y $|\ |_1$ son

equivalentes entonces $\left|\frac{x^{n_i}}{y^{m_i}}\right|_1 > 1$, así $|x|_1 > |y|_1^{\frac{m_i}{n_i}}$, tomando límite cuando $i \to \infty$ en la desigualdad anterior se tiene que $|x|_1 \geq |y|_1^{b_x}$. Por lo tanto, si $|x| = |y|^{b_x}$ entonces $|x|_1 = |y|_2^{b_x}$ para todo $x \in K^*$. Tomando logaritmos se tiene $\ln(|x|) = b_x \ln(|y|)$ y $\ln(|x|_1) = b_x \ln(|y|_1)$, de modo que $\frac{\ln(|x|)}{\ln(|x|_1)} = \frac{\mathrm{In}(|y|)}{\ln(|y|_1)} = \frac{1}{a} > 0$, de donde obtenemos que $|x|_1 = |x|^a$, con $a > 0$, para todo $x \in K$. □

Teorema 1.3.7. *Sea $|\ |$ una norma no arquimediana en K, $R = \{x \in K : |x| \leq 1\}$ y $\mathfrak{B} = \{x \in K : |x| < 1\}$. Entonces R es un anillo local con único ideal máximo $\mathfrak{B}$ y K es su campo de cocientes. El anillo R es de valuación discreta si y sólo si $|K^*| \cong \mathbb{Z}$.*

Demostración. Probaremos que R es anillo local. Dado que $|1| = 1$, entonces $1 \in R$. Sean $x, y \in R$, se tiene que $|x + y| \leq \text{máx}\{|x|, |y|\} \leq 1$, de manera que $x + y \in R$. Así también, $|xy| = |x||y| \leq 1$. Por lo cual R es un anillo. De igual modo se muestra que $\mathfrak{B}$ es un ideal de R.
Sea $x \in R \setminus \mathfrak{B}$, entonces $1 = |x|$. Se tiene que $1 = |x^{-1}x| = |x^{-1}||x| = |x^{-1}|$, de manera que $x^{-1} \in R$, en consecuencia, todo elemento $x \in R \setminus \mathfrak{B}$ es unidad. Así, $\mathfrak{B}$ es el único ideal máximo de R.
Si $x \in K \setminus R$, entonces $|x| > 1$, de manera que $|x^{-1}| < 1$, por lo cual $x^{-1} \in R$, consecuentemente, K es el campo de cocientes de R.
Ahora, supongamos que R es un dominio de valuación discreta, de lo cual se tiene que $\mathfrak{B} = (\pi)$. Si $x \in K^*$, entonces $x \in R$ o $x^{-1} \in R$, pues K es el anillo de cocientes de R, de manera que $x = \pi^k u_1$ con $u_1 \in R$ unidad y $k \in \mathbb{Z}$. En consecuencia, $|x| = |\pi^k u_1| = |\pi|^k$, de donde se obtiene que $|K^*| = \langle |\pi| \rangle \cong \mathbb{Z}$.
Recíprocamente, supongamos que $|K^*| \cong \mathbb{Z}$ y sea $\varphi : |K^*| \to \mathbb{Z}$ un isomorfismo de grupos abelianos. Dado que φ es un isomorfismo, existe $x \in K^*$ tal que $\varphi(|x|) = 1$. Notemos que x puede ser elegido en R, pues $-\varphi$ es también un isomorfimo de grupos, y por tanto existe un elemento en K^*, a saber, x^{-1} tal que $-\varphi(|x^{-1}|) = -(-\varphi(|x|)) = \varphi(|x|) = 1$, y $x^{-1} \in R$. Ahora, puesto que $\varphi(|x|^n) = n$ para todo $n \in \mathbb{N}$, entonces $\mathbb{N} \subseteq \varphi(|R^*|)$. Notemos que $x \in \mathfrak{B}$, pues de lo contrario $|x| = 1$ y $\varphi(|x|) = \varphi(1) = 0$, lo cual no es posible.
Si $y \in K^*$ entonces $\varphi(|y|) = n \cdot 1 = n\varphi(|x|) = \varphi(|x|^n)$, de modo que $\varphi(|y|) - \varphi(|x|^n) = \varphi(|y||x|^{-n}) = 0$, de ahí que $|yx^{-n}| = 1$, en consecuencia $yx^{-n} = u$, con u unidad, de donde obtenemos que $y = x^n u$. Supongamos que $y \in R$, con $y = x^n u$ y u unidad de R. Demostraremos que $n \geq 0$. Dado que $y \in R$ y u es unidad de R, entonces $x^n = yu^{-1} \in R$. Si $n < 0$, se tiene $x^{-n}y = u$, de modo que x^{-n} es unidad en R, de manera que $0 = \varphi(|x^{-n}|) = -n\varphi(|x|) = -n$, lo cual no es posible. Por lo que, si $y \in R$, entonces $y = x^n u$, con $n \geq 0$ y u unidad de R, y en consecuencia $\mathfrak{B} = (x)$.

□

Proposición 1.3.8. *Si $|\ |$ es una norma inducida por una valuación v sobre un campo K, entonces*

$$R = \{x \in K : |x| \leq 1\} = \{x \in K : v(x) \geq 0\} \text{ y}$$
$$\mathfrak{B} = \{x \in K : |x| < 1\} = \{x \in K : v(x) > 0\}.$$

Demostración. Sea $c \in \mathbb{R}$, $0 < c < 1$, tal que $|x| = c^{v(x)}$ para todo $x \in K^*$.
Si $x \in R$, entonces $|x| = c^{v(x)} \leq 1$, de modo que $v(x) \geq 0$, pues $0 < c < 1$. Recíprocamente, si $x \in K^*$ es tal que $v(x) \geq 0$, entonces $|x| = c^{v(x)} \leq 1$, por lo que $x \in R$.
Ahora, si $x \in \mathfrak{B}$ entonces $|x| = c^{v(x)} < 1$ de manera que $v(x)$ no puede ser cero, pues de lo contrario $|x| = 1$. Así, $v(x) > 1$. Recíprocamente, si $v(x) > 1$, entonces $|x| < 1$.

□

Puesto que $\mathfrak{B}$ es el ideal máximo de R, entonces $\dfrac{R}{\mathfrak{B}}$ es un campo, el cual se denomina campo residual del anillo de valuación R.

1.4. Completaciones

Como ya se discutió en la sección anterior, una valuación sobre un campo K define una norma. En esta sección construiremos la completación de un campo cuya norma es inducida por una valuación. Demostraremos que dicha completación es un campo, extensión de K, y presentaremos algunos resultados básicos.
Empezamos recordando la definición de sucesión de Cauchy.

Definición 1.4.1. Sea K un campo con valuación v y $|\ |_v$ una norma inducida por tal valuación. Decimos que $\{x_i\}_{i\in\mathbb{N}} \subset K$ es una sucesión Cauchy, si para todo $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que $|x_n - y_m|_v < \epsilon$, siempre que $m, n \geq N$.

Dos sucesiones Cauchy $\{a_i\}$, $\{b_i\}$ son equivalentes, y se denota por $\{a_i\} \sim \{b_i\}$, si

$$|a_i - b_i|_v \to 0 \text{ cuando } i \to \infty.$$

Sea $\hat{K} = \dfrac{\{\{x_i\} \subset K \mid \{x_i\} \text{ es una sucesión Cauchy}\}}{\sim}$, es decir, el conjunto de clases de equivalencia de sucesiones Cauchy.
Si $\overline{\{x_i\}} \in \hat{K}$, entonces $\{x_i\}$ es una sucesión Cauchy en K, de modo que $||x_n|_v - |x_m|_v| \leq |x_n - x_m|_v \leq \epsilon$ para todo $n, m \geq N_0$ para algún N_0, en consecuencia $\{|x_n|_v\}_{n\in\mathbb{N}}$ es una sucesión Cauchy en $\mathbb{R}$, por lo que $\lim\limits_{n\to\infty} |x_n|_v$ existe.
Sea $x \in \hat{K}$, con $x = \overline{\{x_i\}}$ y $\{x_i\} \subset K$, se define en $\hat{K}$ la función $|\ | : \hat{K} \to \mathbb{R}$ dada por

$$|x| := \lim_{i\to\infty} |x_i|_v.$$

La cual está bien definida por lo discutido previamente.

Proposición 1.4.2. *El conjunto $\hat{K}$ es un campo, extensión de K, y la función $|\ | : \hat{K} \to \mathbb{R}$ es una norma.*

Demostración. Se tiene que $K \hookrightarrow \hat{K}$ mediante el mapeo $x \mapsto \overline{\{x\}}$. Además, $\{x\} \sim \{x'\}$ si y sólo si $x = x'$. Denotaremos por x al elemento $\overline{\{x\}}$ de $\hat{K}$, donde $x \in K$. Se tiene que $1_{\hat{K}} = \overline{\{1\}}$ y $0_{\hat{K}} = \overline{\{0\}}$.

Definamos en $\hat{K}$ las operaciones suma y producto como sigue. Para $a = \overline{\{a_i\}}, b = \overline{\{b_i\}} \in \hat{K}$, $a+b := \overline{\{a_i\}}+\overline{\{b_i\}} = \overline{\{a_i+b_i\}}$ y $a\cdot b := \overline{\{b_i\}}\cdot\overline{\{b_i\}} = \overline{\{a_i\cdot b_i\}}$, las cuales no dependen de los representantes, pues si $\{a_i\} \sim \{a_i'\}$ y $\{b_i\} \sim \{b_i'\}$, entonces

$$|a_i + b_i - (a_i' + b_i')|_p \leq |a - a_i'|_p + |b_i - b_i'|_p \to 0$$

cuando $i \to \infty$. También,

$$|a_ib_i - a_i'b_i'|_v = |a_ib_i - a_i'b_i' + a_i'b_i - a_i'b_i|_v \leq |b_i|_v|a_i - a_i'|_v + |a_i'|_v|b_i - b_i'|_v \to 0$$

cuando $i \to \infty$.
Ahora debemos probar que si $a = \overline{\{x_n\}} \in \hat{K}$, $a \neq 0_{\hat{K}}$, existe $b \in \hat{K}$ tal que $ab = 1$. Puesto que $a \neq 0_{\hat{K}}$, entonces $\{x_n\} \not\sim \{0\}$, de modo que existen $\epsilon_0 > 0$ y $N_0 \in \mathbb{N}$ tales que $|x_n|_v > \epsilon$ para todo $n \geq N_0$. Sean $\{x_n^{-1}\}_{n\geq N_0} \subset K$, $\epsilon > 0$ y $\epsilon' < \epsilon\epsilon_0^2$, entonces $|x_n| > \epsilon_0$ para todo $n \geq N_0$ y $|x_n - x_m| < \epsilon'$ para todos $n, m \geq N'$, y para algún N', de manera que

$$|x_n^{-1} - x_m^{-1}| = \left|\frac{x_x - x_m}{x_nx_m}\right| = \left|\frac{1}{x_nx_m}\right| |x_n - x_m| \leq \frac{1}{\epsilon_0^2}\epsilon' < \frac{1}{\epsilon_0^2}\epsilon_0^2\epsilon = \epsilon$$

para todos $n, m \geq N$, donde N=máx$\{N_0, N'\}$, de modo que $\{x_n^{-1}\}_{n\geq N_0}$ es de Cauchy.
Sea

$$y_n = \begin{cases} 0 & si \quad n < N_0 \\ \\ x_n^{-1} & si \quad n \geq N_0 \end{cases},$$

entonces $\{y_n\} \sim \{x_n^{-1}\}$, pues para todo $\epsilon > 0$, $|y_n - x_n^{-1}| = 0 < \epsilon$ para todo $n \geq N_0$. Además, $\{x_n\}\{y_n\} = \{x_ny_n\} \sim \{1\} = 1_{\hat{K}}$, por lo tanto $\overline{\{x_n\}}^{-1} = \overline{\{y_n\}}$. En consecuencia $\hat{K}$ es campo.
Por último, debemos probar que $|\ |$ es una norma. Dado que $\lim\limits_{n\to\infty} |x_n|_v$ existe, demostraremos que esta definición no depende del representante $\{x_n\}$ de $\overline{\{x_n\}}$. Sea $\{y_n\} \in \overline{\{x_n\}}$, entonces $\lim\limits_{i\to\infty} |x_n - y_n|_v = 0$, pues $\{y_n\} \sim \{x_n\}$, por lo tanto para todo $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que $||x_n|_v - |y_n|_v| \leq |x_n - y_n|_v < \epsilon$ para todo $n \leq N$, de modo que $\lim\limits_{n\to\infty}(|x_n|_v - |y_n|_v) = 0$.
Finalmente, las primeras propiedades de la definición de norma se siguen fácilmente usando que $|\ |_v$ es norma. Mostraremos únicamente la desigualdad del triángulo. Se tiene que

$$\begin{aligned} |\overline{\{x_n\}} + \overline{\{y_n\}}| &= |\overline{\{x_n + y_n\}}| \\ &= \lim_{n\to\infty} |x_n + y_n|_v \\ &\leq \lim_{n\to\infty} [\text{máx}\{|x_n|_v, |y_n|_v\}] \\ &= \text{máx}\{\lim_{n\to\infty} |x_n|_v, \lim_{n\to\infty} |y_n|_v\} \\ &= \text{máx}\{|\overline{\{x_n\}}|, |\overline{\{y_n\}}|\} \end{aligned}$$

para todo $\overline{\{x_n\}}, \overline{\{y_n\}} \in \hat{K}$. □

Sea $\{\alpha_n\}_{n\in\mathbb{N}} \subset \hat{K}$ una sucesión Cauchy. Se tiene que $\alpha_n = \{\alpha_j^{(n)}\}_{j\in\mathbb{N}}$ para todo $n \in \mathbb{N}$ y, dado que $\{\alpha_n\}_{n\in\mathbb{N}} \subset \hat{K}$ es una sucesión Cauchy, entonces para todo $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que para todos $n, m > N$

$$|\alpha_n - \alpha_m| = |\{\alpha_j^{(n)}\} - \{\alpha_j^{(m)}\}| = |\{\alpha_j^{(n)} - \alpha_j^{(m)}\}| = \lim_{j\to\infty} |\alpha_j^{(n)} - \alpha_j^{(m)}| < \epsilon. \quad (1.4.1)$$

Sea $\alpha = \{\alpha_j^{(j)}\}_{j\in\mathbb{N}}$. Se tiene que $|\alpha_n^{(n)} - \alpha_m^{(m)}| \leq |\alpha_n^{(n)} - \alpha_m^{(n)}| + |\alpha_m^{(n)} - \alpha_m^{(m)}| < \epsilon$, para todo $n, m > N$, para algún $N \in \mathbb{N}$, esto porque $\alpha_n = \{\alpha_j^{(n)}\}$ es de Cauchy y por la Ecuación (1.4.1). De modo que $\alpha \in \hat{K}$.
Ahora, probaremos que $\alpha_n \to \alpha$, cuando $n \to \infty$, es decir, $\lim_{n\to\infty} |\alpha - \alpha_n| = 0$. Notemos que $|\alpha_n - \alpha| = |\{\alpha_j^{(n)}\} - \{\alpha_j^{(j)}\}| = |\{\alpha_j^{(n)} - \alpha_j^{(j)}\}| = \lim_{j\to\infty} |\alpha_j^{(n)} - \alpha_j^{(j)}|$, por otro lado $|\alpha_j^{(n)} - \alpha_j^{(j)}| \leq |\alpha_j^{(n)} - \alpha_j^{(m)}| + |\alpha_j^{(m)} - \alpha_j^{(j)}| < \epsilon$.

Se define en $\hat{K}$ la valuación $\tilde{v} : \hat{K}^* \to \mathbb{R}$ como sigue. Si $a = \overline{\{x_n\}} \in \hat{K}$, se declara $\tilde{v}(a) = \lim_{n\to\infty} v(x_n)$. Debemos verificar que $\lim_{n\to\infty} v(x_n) \in \mathbb{R} \cup \{\infty\}$.
Se tiene que $|c^{v(x_n)} - c^{v(x_m)}| = ||x_n|_v - |x_m|_v| \leq |x_n - x_m|_v \leq \epsilon$ para todos $n, m \geq N_0$ y $N_0 \in \mathbb{N}$, entonces $\{c^{v(x_n)}\}_{n\in\mathbb{N}}$ es una sucesión Cauchy en $\mathbb{R}$, y por tanto $\lim_{n\to\infty} c^{v(x_n)}$ existe. Ahora, $\tilde{v}(a) = \lim_{n\to\infty} v(x_n) = \lim_{n\to\infty} \log_c(c^{v(x_n)}) \in \mathbb{R} \cup \{\pm\infty\}$. Si $\lim_{n\to\infty} v(x_n) = -\infty$, entonces $|a| = \lim_{n\to\infty} |x_n|_v = \lim_{n\to\infty} c^{v(x_n)} = c^{-\infty} = \infty$, lo cual no es posible. Luego, $\tilde{v}(a) \in \mathbb{R} \cup \{\infty\}$. Las propiedades de valuación se siguen directamente usando que v lo es.

Observación 1.4.3. *Si $x \in K$, entonces $\tilde{v}(x) = \lim_{n\to\infty} v(x) = v(x)$. De manera que $\tilde{v}|_K = v$.*

Observación 1.4.4. *Sea $v : K \to \mathbb{R}$ tal que $\mathrm{Im}(v) \subset (\mathbb{Z} \cup \{\infty\})$, entonces $Im(\tilde{v}) \subset (\mathbb{Z} \cup \{\infty\})$ pues para todo $a \in \hat{K}$, $\tilde{v}(a) = \lim_{n\to\infty} v(x_n)$, y $v(x_n) \in (\mathbb{Z} \cup \{\infty\})$.*

Teorema 1.4.5. *Sea $|\ |$ una norma no arquimediana en K cuyo anillo de valuación R es de valuación discreta, entonces el anillo de valuación $\hat{R}$ de $\hat{K}$ es de valuación discreta y el ideal máximo de $\hat{R}$ puede ser generado por el mismo elemento que genera al ideal máximo de R.*

Demostración. Por el Teorema 1.3.7 basta demostrar que $|\hat{K}| \cong \mathbb{Z}$.
Sea $\alpha \in \hat{K}^*$, entonces $\alpha = \overline{\{a_n\}}_{n\in\mathbb{N}}$, con $a_n \in K$ para todo n. Sea $\pi \in R$ tal que $\mathfrak{B} = (\pi)$ es el ideal máximo de R y $0 < c < 1$ tal que $|\pi| = c$. Dado que $\alpha \neq 0$ y $a_n \in K$ podemos suponer que $a_n = \pi^{k_n} u_n$, con $k_n \in \mathbb{Z}$ para todo n y u_n unidad de R. Así, $0 \neq |\alpha| = \lim_{n\to\infty} |a_n| = \lim_{n\to\infty} |\pi^{k_n} u_n| = \lim_{n\to\infty} c^{k_n}$. La única manera en la que $\lim_{n\to\infty} c^{k_n}$ sea finito no cero es que $k_n = k$ para todo $n \geq N$, para algún $N \in \mathbb{N}$ fijo. Por tanto $|a_n| = |a_N|$ para todo $n \geq N$ y $|\alpha| = \lim_{n\to\infty} |a_n| = |a_N| = c^k$. De modo que $|\alpha| = |a_N| \in |K^*| \cong \mathbb{Z}$. Luego, $|\hat{K}^*| \cong \mathbb{Z}$.
Sea $\hat{\mathfrak{B}} = x\hat{R}$, con $x \in \hat{R}$, el ideal máximo de $\hat{R}$. Por lo anterior se tiene que $|x| = c^r$, para algún $r \neq 0 \in \mathbb{Z}$, pues $x \in \hat{\mathfrak{B}}$ y por tanto $|x| \neq 0$. Puesto que

$|\pi| = c$, entonces $\left|\dfrac{\pi^r}{x}\right| = \dfrac{|\pi|^r}{|x|} = \dfrac{c^r}{c^r} = 1$, de modo que $\dfrac{\pi^r}{x}$ es unidad de $\hat{R}$, es decir $\dfrac{\pi^r}{x} = u$, con u unidad de R, así pues $x = \pi^r u^{-1}$, de donde obtenemos que $\hat{B} = x\hat{R} = \pi^r \hat{R}$. Ahora, dado que $\pi\hat{R} \subseteq \hat{\mathfrak{B}} = \pi^r \hat{R}$, se sigue que $r = 1$, como se quería. □

Corolario 1.4.6. *En el contexto del Teorema 1.4.5, todo elemento $\alpha \in \hat{K}$ puede ser representado por una sucesión $\{a_n\} \subset K$ tal que $|a_n|$ es constante para todo n.*

Corolario 1.4.7. *Las unidades en $\hat{R}$ son elementos $\overline{\{a_n\}}$ en $\hat{K}$ para los cuales $|a_n| = 1$ para todo n.*

Demostración. Se tiene por el Corolario 1.4.6 que todo elemento en $\hat{R}$ se representa por una sucesión $\{a_n\} \subset K$ tal que $|a_n|$ es constante para todo n. Dado que $\overline{\{a_n\}} \in \hat{R}$, se tiene $|a_n| \leq 1$. Si $\overline{\{a_n\}}$ es unidad entonces $|a_n| = 1$ para todo n.

□

Proposición 1.4.8. $\dfrac{R}{\mathfrak{B}^n} \cong \dfrac{\hat{R}}{\hat{\mathfrak{B}}^n}$ *para todo entero positivo n.*

Demostración. Se tiene que $\hat{\mathfrak{B}} \cap R = \mathfrak{B}$, por lo tanto $\hat{\mathfrak{B}}^n \cap R = \mathfrak{B}^n$. Además, por un teorema de isomorfismo

$$\frac{R + \hat{\mathfrak{B}}^n}{\hat{\mathfrak{B}}^n} \cong \frac{R}{R \cap \hat{\mathfrak{B}}^n} = \frac{R}{\mathfrak{B}^n}.$$

Para concluír la prueba basta demostrar que $R + \hat{\mathfrak{B}}^n = \hat{R}$ para todo $n \geq 1$.
Sea $\alpha = \overline{\{a_n\}}_{n\in\mathbb{N}} \in \hat{R} \setminus \hat{\mathfrak{B}}$, entonces α es unidad de $\hat{R}$. Por el Corolario 1.4.7 se tiene que $|a_n| = 1$ para todo n. Ahora, dado que $\{a_n\}_{n\in\mathbb{N}}$ es Cauchy, existe $N \in \mathbb{N}$ tal que $|a_{n+1} - a_n| < \dfrac{1}{2}$ para todo $n \geq N$. Sin pérdida de generalidad podemos suponer que $N = 1$.
Se tiene que $a_{n+1} - a_n \in \mathfrak{B}\ \forall\ n$, de modo que $a_{n+1} \equiv a_n$ mód $\mathfrak{B}$, así pues $a_n \equiv a_1$ mód $\mathfrak{B}$, de donde obtenemos $\overline{\{a_n\}}_{n\in\mathbb{N}} \equiv \overline{\{a_1\}}$ mód $\hat{\mathfrak{B}}$, con $a_1 \in R$. Así pues, $\alpha = a_1 + y$ con $y \in \hat{\mathfrak{B}}$. Por lo tanto, $\alpha \in \hat{R} \subseteq R + \hat{\mathfrak{B}}$, consecuentemente $\hat{R} = R + \hat{\mathfrak{B}} = R + \pi\hat{R}$. Si multiplicamos por π a la última ecuación obtenemos $\pi\hat{R} = \pi R + \pi^2\hat{R}$, esto es, $\hat{\mathfrak{B}} = \mathfrak{B} + \hat{\mathfrak{B}}^2$. De modo que

$$\hat{R} = R + \hat{\mathfrak{B}} = R + \mathfrak{B} + \hat{\mathfrak{B}}^2 = R + \hat{\mathfrak{B}}^2.$$

Finalmente, por inducción obtenemos que $\hat{R} = R + \hat{\mathfrak{B}}^n$ para todo $n \geq 1$. □

Teorema 1.4.9. *Todo elemento $\alpha \in \hat{K}^*$ tiene una representación única de la forma*

$$\alpha = \pi^r \sum_{i\geq 0} s_i \pi^i, \tag{1.4.2}$$

donde $s_i \in S$ y S es un conjunto de representantes, que incluye al 0, de $\dfrac{R}{\mathfrak{B}}$, $s_0 \neq 0$.

Demostración. Sea S un conjunto de representantes de $\dfrac{R}{\mathfrak{B}}$ que incluye al 0. Por la Proposición 1.4.8 podemos suponer que S es un conjunto de representantes de $\dfrac{\hat{R}}{\hat{\mathfrak{B}}}$.
Dado que $\hat{R}$ es un dominio de valuación discreta y $\hat{K}$ es su campo de cocientes, entonces todo elemento $\alpha \in \hat{K}^*$ tiene una representación única de la forma $\alpha = \pi^r u$, con u unidad de $\hat{R}$, por lo que solo resta probar que u se representa como $u = \sum_{i\geq 0} s_i \pi^i$.
Se tiene que existe un único $s_0 \in S$ tal que $u \equiv s_0$ mód $\mathfrak{B}$, o bien, $u \equiv s_0$ mód $\pi\hat{R}$, con $s_0 \neq 0$, pues u es unidad y de esto $u \notin \hat{\mathfrak{B}}$. Entonces $u = s_0 + x_1\pi$, con $x_1 \in \hat{R}$. Ahora, para x_1 existe un único $s_1 \in S$ tal que $x \equiv s_1$ mód $\pi\hat{R}$, de modo que $x_1 = s_1 + x_2\pi$, para algún $x_2 \in \hat{R}$. Así pues,
$u = s_0 + x_1\pi = s_0 + (s_1 + x_2\pi)\pi = s_0 + s_1\pi + x_2\pi^2$. Siguiendo de esta manera obtenemos una sucesión de sumas parciales $b_n = \sum_{i=0}^{n} s_i\pi^i$ que converge a u, pues $|u - b_n| = |x_{n+1}\pi^{n+1}| = |x_{n+1}|c^{n+1} \to 0$ cuando $n \to \infty$. De manera que $u = \sum_{i\geq 0} s_i\pi^i$.
Para demostrar unicidad supongamos que $\alpha = \pi^{m_1}\sum_{i\geq 0} s_i\pi^i = \pi^{m_2}\sum_{i\geq 0} r_i\pi^i$, entonces $|\alpha| = m_1 = m_2$, de manera que $\sum_{i\geq 0} s_i\pi^i = \sum_{i\geq 0} r_i\pi^i$.
Se tiene

$$s_0 - r_0 + s_1\pi + s_2\pi^2 + \cdots = r_1\pi + r_2\pi^2 + \cdots,$$

notemos que la expresión de la derecha tiene valuación mayor que uno, de modo que $s_0 - r_0 = 0$. Procediendo de la misma forma obtenemos que $r_i = s_i$ para todo $i \geq 1$.

□

1.5. Extensiones finitas de campos completos

Sea F una extensión de K y v' una valuación de F. Sea $v = v'|_K$, entonces v es una valuación de K. Si v es una valuación de K, cualquier valuación v' de F tal que $v'|_K = v$, recibe el nombre de extensión de v.
Sean R', $\mathfrak{P}'$ y $\mathfrak{t}$ el anillo de valuación, ideal máximo y campo residual de F, respectivamente. Entonces

$$R = R' \cap K, \quad \mathfrak{P} = \mathfrak{P}' \cap R, \tag{1.5.1}$$

de modo que, por un teorema de isomorfismo se tiene

$$\mathfrak{t} = \frac{R}{\mathfrak{P}} = \frac{R}{\mathfrak{P}' \cap R} \cong \frac{R + \mathfrak{P}'}{\mathfrak{P}'} \subseteq \frac{R'}{\mathfrak{P}'} = \mathfrak{t}'. \tag{1.5.2}$$

De manera que

$$\mathfrak{t} \hookrightarrow \mathfrak{t}'. \tag{1.5.3}$$

Puesto que $v = v'|_K$, entonces $v(K^*) \subseteq v'(F^*)$. Sean

$$e = e(v'/v) = [v'(F^*) : v(K^*)], \quad f = f(v'/v) = [\mathfrak{t}' : \mathfrak{t}],$$

donde e es el índice del grupo y f el grado de la extensión $\mathfrak{t}'/\mathfrak{t}$.
A e y f se les denominan índice de ramificación y grado relativo, respectivamente.

Lema 1.5.1. *Sea F/K una extensión de campos completos. Supongamos que $f < \infty$, entonces F/K es una extensión finita y*

$$[F : K] = ef. \tag{1.5.4}$$

Demostración. La demostración de este Lema puede consultarse en [7] □

En seguida mostramos un resultado importante que establece condiciones para que una valuación se extienda de manera única.

Proposición 1.5.2. *Sea v una valuación de un campo completo K y F una extensión algebraica de K. Entonces v se extiende de manera única a una valuación v' de F y $v = v'|_K$. En particular, si F/K es finita, entonces F también es un campo completo, y*

$$v'(x) = \frac{1}{n} v(N_{F/K}(x)), \quad \textit{para todo } x \in F, \tag{1.5.5}$$

donde $n = [F : K]$ es el grado de la extensión y $N_{F/K}$ es la función norma de la extensión F/K.

Demostración. La demostración de esta proposición puede consultarse en [22]. □

CAPÍTULO 2

Campos locales y números p-ádicos

En este capítulo estudiaremos campos locales desde un punto de vista topológico. Definiremos una familia de subconjuntos en un caso especial de campos completos, la cual resultará una base para la topología. Justificaremos que, con esa familia de subconjuntos, un campo local es un espacio Hausdorff, entre otras propiedades.
Dentro de los resultados importantes en la teoría de campos locales es su clasificación pues se sabe que cualquier campo local de característica 0 es isomorfo a una extensión finita del campo de los números p-ádicos y, si es de característica $p > 0$, es isomorfo al campo de las series de Laurent $K((x))$ sobre un campo finito K [16].
Con el propósito de entender los campos locales de característica 0, centraremos la atención en los números p-ádicos.

2.1. La topología definida por una valuación

Empezamos esta sección con la definición de campo local. Recordemos que dado un campo K con anillo de valuación R e ideal máximo $\mathfrak{B}$, su campo residual es $\frac{R}{\mathfrak{B}}$.

Definición 2.1.1. Un campo K es un campo local si es completo con respecto a una norma inducida por una valuación no arquimediana y su campo residual es finito.

Sea K un campo local con valuación $v : K \to \mathbb{Z}$. Para cada $x \in K$ y $\alpha \in \mathbb{R}$ sea

$$N(x, \alpha) = \{y \mid y \in K, v(y - x) > \alpha\}.$$

Se tiene que para cada $\alpha \in \mathbb{R}$, $x \in N(x, \alpha)$.

Proposición 2.1.2. *La familia de subconjuntos $N(x, \alpha)$, $\alpha \in \mathbb{R}$ y $x \in K$, forman una base para K, la cual define una topología Hausdorff.*

Demostración. Sea $x \in K$. Dado que para cada $\alpha \in \mathbb{R}$, $x \in N(x, \alpha)$, solo resta demostrar que si $x \in N(y, \beta) \cap N(z, \alpha)$, entonces existen $w \in K$ y $\gamma \in \mathbb{R}$ tales que $x \in N(w, \gamma) \subset N(y, \beta) \cap N(z, \alpha)$.

Sea $\gamma = \text{máx}\{\beta, \alpha\}$. Notemos que $x \in N(x, \gamma)$. Ahora, demostraremos que $N(x, \gamma) \subset N(y, \beta) \cap N(z, \alpha)$. Sea $w \in N(x, \gamma)$, entonces $v(w - x) > \gamma$. Se tiene que

$$v(w - y) = v(w - x + x - y) \geq \text{mín}\{v(w - x), v(x - y)\} > \text{mín}\{\gamma, \beta\} = \beta,$$

$$v(w - z) = v(w - x + x - z) \geq \text{mín}\{v(w - x), v(x - z)\} > \text{mín}\{\gamma, \alpha\} = \alpha,$$

de modo que $w \in N(y, \beta) \cap N(z, \alpha)$ y, en consecuecia,

$$N(x, \gamma) \subset N(y, \beta) \cap N(z, \alpha).$$

Ahora debemos probar que, con la topología que define la base anterior, K es un espacio Hausdorff.
Sean $x, y \in K$ y $\alpha = v(x - y)$. Se tiene que $x \in N(x, \alpha), y \in N(y, \alpha)$.
Supongamos que existe $w \in N(x, \alpha) \cap N(y, \alpha)$, entonces $v(x - w) > \alpha$ y $v(y - w) > \alpha$. Por otro lado,

$$v(x - y) = v(x - w + w - y) \geq \text{mín}\{v(x - w), v(w - y)\} > \alpha = v(x - y),$$

lo cual no es posible. Por consiguiente $N(x, \alpha) \cap N(y, \alpha) = \emptyset$.

□

2.2. Propiedades topológicas de un campo local

Proposición 2.2.1. *El anillo de valuación R es un conjunto cerrado de K y los ideales $\mathfrak{B}^n$ son conjuntos abiertos y cerrados de K.*

Demostración. Probaremos que el anillo de valuación R es cerrado. Sea $x \in R^c = \{y \in K \mid v(y) < 0\}$. Afirmamos que $x \in N(x, 0) \subset R^c$. Si existe $z \in N(x, \alpha) \cap R$, entonces $v(x - y) > 0$. Por otro lado puesto que $v(x) < 0$ y $v(y) \geq 0$ se tiene $v(x - y) = \text{mín}\{v(x), v(y)\} = v(x) < 0$, lo cual es una contradicción. Luego, $x \in N(x, 0) \subset R^c$, es decir, R es un conjunto cerrado.
Ahora, demostraremos que $\mathfrak{B}$ es un conjunto abierto y cerrado de K. Sea $x \in \mathfrak{B}$. Mostraremos que $N(x, 0) \subset \mathfrak{B}$. Supongamos que existe $y \in \mathfrak{B}^c = \{y \in K \mid v(y) \leq 0\}$ tal que $y \in N(x, 0)$. Entonces $v(x - y) > 0$. Puesto que $v(x) > 0$ y $v(y) \leq 0$ se tiene que $v(x - y) = \text{mín}\{v(x), v(y)\} = v(y) \leq 0$, lo cual es una contradicción. Por lo que $N(x, 0) \subset \mathfrak{B}$, es decir, $\mathfrak{B}$ es abierto.
Para demostrar que $\mathfrak{B}$ es un conjunto cerrado, probaremos que $\mathfrak{B}^c$ es abierto. Sea $x \in \mathfrak{B}^c$. Argumentando de manera similar se tiene que $N(x, 0) \subset \mathfrak{B}^c$. Luego, $\mathfrak{B}$ es cerrado.
Análogamente se demuestra que los ideales $\mathfrak{B}^n$, con $n > 1$, son conjuntos abiertos y cerrados de K. □

Proposición 2.2.2. *La familia de subconjuntos $\{\mathfrak{B}^n\}_{n \in \mathbb{N}}$ es una base de vecindades abiertas de $0 \in K$.*

Demostración. Se tiene $v(0) > n$ para todo $n \in \mathbb{N}$, de manera que $0 \in \mathfrak{B}^n$ para toda $n \in \mathbb{N}$. Sea U una vecindad de 0. Debemos hallar m tal que $\mathfrak{B}^m \subset U$. Dado que la familia de subconjuntos $N(x, \alpha)$, $\alpha \in \mathbb{R}$ y $x \in K$, forman una base para K, podemos suponer que $0 \in N(x, \alpha) \subseteq U$ para algún $x \in K$ y $\alpha \in \mathbb{R}$. Puesto que $0 \in N(x, \alpha)$, entonces $v(x) > \alpha$. Sea $m \in \mathbb{N}$ tal que $m > \alpha$, y consideremos al conjunto $\mathfrak{B}^m$. Si $y \in \mathfrak{B}^m$, entonces $v(y) \geq m > \alpha$. Por otro lado, $v(y - x) \geq \text{mín}\{v(x), v(y)\} > \alpha$, de modo que $y \in N(x, \alpha)$. En consecuencia, $\mathfrak{B}^m \subset N(x, \alpha)$. □

Si K es un campo local, su campo residual es finito. Sea S un conjunto de representantes de $\dfrac{R}{\mathfrak{B}}$ en K.
Se tiene que S^∞ es el conjunto de todas las sucesiones $(s_0, s_1, s_2, \ldots)$, donde $s_n \in S$ para todo n, así

$$S^\infty = \prod_{n=0}^{\infty} S_n, \quad \text{con} \;\; S_n = S.$$

Se introduce sobre S^∞ la topología producto de los espacios discretos S_n.

Corolario 2.2.3. *El mapeo*

$$(s_0, s_1, s_2, \ldots) \mapsto \sum_{n=0}^{\infty} s_n \pi^n$$

define un homeomorfismo biyectivo de S^∞ al anillo de valuación R de K.

Demostración. La demostración de este resultado puede consultarse en [7, pág. 11] □

La topología que emplearemos sobre K en el siguiente resultado es la que se definió previamente.

Teorema 2.2.4. *Sea (K, v) un campo local. Entonces K es un campo totalmente disconexo, no discreto y localmente compacto. Además, el anillo de valuación R y los ideales $\mathfrak{B}^n$ son conjuntos compactos de K.*

Demostración. Se tiene que el conjunto de ideales $\mathfrak{B}^n$ forman una familia de vecindades de $0 \in K$, de modo que si $x \in K$, entonces $x + \mathfrak{B}^n$ forman una base de vecindades de $x \in K$, por esto, para demostrar que K es totalmente disconexo es suficiente probar que la componente conexa de 0, denotado por $C(0)$, es $C(0) = \{0\}$.
Supongamos que existe $y \in C(0) \setminus \{0\}$. Se tiene que $\bigcap_{n \geq 1} \mathfrak{B}^n = \{0\}$, pues si $x \in \mathfrak{B}^n$ para todo $n \geq 1$, entonces $v(x) \geq n$, por lo que $v(x) = \infty$, es decir, $x = 0$. De esto se tiene que existe $m \in \mathbb{N}$ tal que $0 \in \mathfrak{B}^m$ y $y \notin \mathfrak{B}^m$. También tiene que $\mathfrak{B}^m$ y $(\mathfrak{B}^m)^c$ son conjuntos abiertos disjuntos de K tales que $C(0) \subset \mathfrak{B}^m \cup (\mathfrak{B}^m)^c$, de manera que $C(0) = (\mathfrak{B}^m \cap C(0)) \cup ((\mathfrak{B}^m)^c \cap C(0))$ así que $C(0)$ es disconexo, lo cual no es posible. En consecuencia $C(0) = \{0\}$.
Sea $S \subset R$ un conjunto de representantes de $\dfrac{R}{\mathfrak{B}}$. Puesto que K es un campo local se tiene que S es un conjunto finito. Por otro lado, por el Corolario 2.2.3,

$R \cong \prod_{n=0}^{\infty} S_n$, $S_n = S$. Dado que S es un conjunto finito, entonces S es compacto. Luego, por el Teorema de Tychonoff se tiene que R es compacto. Puesto que los ideales $\mathfrak{B}^n$ son conjuntos cerrados y están contenidos en R, el cual es compacto, entonces $\mathfrak{B}^n$ es compacto para todo $n \geq 1$. Por lo que K es localmente compacto, pues para cada $x \in K$ se tiene que los conjuntos $x + \mathfrak{B}^n$ forman una base local de vecindades compactas.
Para demostrar que K es no discreto supongamos que $\{0\}$ es abierto. Puesto que los ideales $\mathfrak{B}^n$ son una base de vecindades de $\{0\}$, existe $n \in \mathbb{N}$ tal que $\mathfrak{B}^n = (\pi^n) = \{0\}$, de manera que $\pi^n = 0$, lo cual es imposible. Consecuentemente, $\{0\}$ no es abierto. □

2.3. El campo de los números p-ádicos

En esta sección daremos una introducción al campo de los números p-ádicos. Para construir este campo partiremos del concepto de orden de un número y, con esto, definiremos una valuación en $\mathbb{Q}$. Teniendo lo anterior, emplearemos los resultados del capítulo 1, sección 3, para construir un campo completo extensión de $\mathbb{Q}$.

Definición 2.3.1. Sea p un número primo. Para cualquier $a \in \mathbb{Z}$, se define el orden de a, $\mathrm{ord}_p(a)$, como el entero más grande m tal que $a \equiv 0$ mód p^m.

Para cualquier racional $x = \dfrac{a}{b}$, se define

$$\mathrm{ord}_p(x) := \mathrm{ord}_p(a) - \mathrm{ord}_p(b). \tag{2.3.1}$$

Sea $v_p : \mathbb{Q} \to \mathbb{R}$, definida por

$$v(x)_p = \mathrm{ord}_p(x). \tag{2.3.2}$$

Proposición 2.3.2. *v_p es una valuación en $\mathbb{Q}$.*

Demostración. Demostraremos las siguientes condiciones para todo $x, y \in \mathbb{Q}$:

1. $v(xy)_p = v(x)_p + v(y)_p$.
2. $v(x+y)_p \geq \mathrm{mín}\{v(x)_p, v(y)_p\}$.

1. Sean $x = \dfrac{a}{b}$ y $y = \dfrac{c}{d}$. Si $x = y = 0$ se tiene que $v_p(xy) = \infty$ y $v_p(x) + v_p(y) = \infty$. Si $x = 0$ y $y \neq 0$ entonces $v(xy)_p = \infty$ y $v_p(x) + v_p(y) = \infty$. De igual modo, si $x \neq 0$ y $y = 0$, $v_p(xy) = 0$ y $v_p(x) + v_p(y) = \infty$.
Supongamos que $x, y \neq 0$, $a = p^{n_a} a_1, b = p^{n_b} b_1, c = p^{n_c} c_1$ y $c = p^{n_c} c_1$, donde $p \nmid a_1 b_1 c_1 d_1$, entonces

$$\begin{aligned} \mathrm{ord}_p(xy) &= \mathrm{ord}_p\left(\frac{ac}{bd}\right) \\ &= \mathrm{ord}_p(ac) - \mathrm{ord}_p(bd) = (n_a + n_c) - (n_b + n_d) \\ &= (n_a - n_b) + (n_c - n_d) \\ &= \mathrm{ord}_p(x) + \mathrm{ord}_p(y). \end{aligned}$$

Así, $v_p(xy) = v_p(x) + v_p(y)$.
2. Sean x y y como en el inciso anterior. Probaremos que $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$. Si $x = 0$ o $y = 0$, se prueba directamente la desigualdad. Supongamos que $x \neq 0$, $y \neq 0$ y $v_p(y) = \text{mín}\{v_p(x), v_p(y)\}$, es decir, $\text{ord}_p(y) \leq \text{ord}_p(x)$, entonces $n_c - n_d \leq n_a - n_b$.
Se tiene que

$$\begin{aligned} x + y = \frac{a}{b} + \frac{c}{d} &= \frac{p^{n_a}a_1}{p^{n_b}b_1} + \frac{p^{n_c}c_1}{p^{n_d}d_1} \\ &= \frac{p^{n_a+n_d}a_1d_1 + p^{n_b+n_c}c_1b_1}{p^{n_b+n_d}b_1d_1} \\ &= \frac{p^{n_b+n_c}(p^{n_a+n_d-(n_b+n_c)}a_1d_1 + c_1b_1)}{p^{n_b+n_d}b_1d_1}. \end{aligned}$$

De manera que $\text{ord}_p(x+y) \geq n_b + n_c - (n_b + n_d) = n_c - n_d = \text{ord}_p(y)$, consecuentemente $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

□

Observación 2.3.3. *La imagen de v_p es $\mathbb{Z}$. Cuando una valuación v sobre un campo K es tal que $v(K) \cong \mathbb{Z}$, se denomina discreta.*

Observación 2.3.4. *Denotaremos por $|\ |_p$ a la norma en $\mathbb{Q}$ inducida por v_p, la cual se obtiene como en (1.3.1), pág.16.*

El siguiente resultado clasifica a todas las normas sobre $\mathbb{Q}$ pues establece que cualquier norma es equivalente a una norma inducida por una valuación p-ádica, o bien, a la norma usual de valor absoluto.

Teorema 2.3.5 (Ostrowski)**.** *Toda norma no trivial sobre $\mathbb{Q}$ es equivalente a $|\ |_p$ para algún primo p o a la norma usual de valor absoluto.*

Demostración. Sea $|\ | : \mathbb{Q} \to \mathbb{R}$ una norma. Puesto que $|\ |$ es no trivial se tienen dos posibilidades: existe $n \in \mathbb{N}$ tal que $|n| > 1$ o, para todo $n \in \mathbb{N}$, $|n| \leq 1$. Probaremos que, en el primer caso, la norma es equivalente a la norma usual de valor absoluto y, en el segundo caso, la norma es equivalente a una norma p-ádica.
Caso 1. Consideremos la función $f(t) = n_0^t$ y sea n_0 el menor entero positivo tal que $|n_0| > 1$. Se tiene que existe $\alpha > 0$ tal que $f(\alpha) = n_0^\alpha = |n_0|$. Notemos que para todo $n \in \mathbb{N}$, existen $a_0, a_1, \ldots, a_s$ con $0 \leq a_i < n_0$, $a_s \neq 0$, tales que $n = a_0 + a_1n_0 + \cdots + a_sn_0^s$. Se tiene que $n_0^s \leq n < n_0^{s+1}$. De modo que

$$|n| = |a_0 + a_1n_0 + \cdots + a_sn_0^s| \leq |a_0| + |a_1||n_0| + \cdots + |a_s||n_0^s|,$$

puesto que $|n_0| = n_0^\alpha$ y n_0 es el mínimo entero positivo tal que $|n_0| > 1$, entonces $|a_i| \leq 1$ para todo i y

$$|n| \leq 1 + n_0^\alpha + \cdots + n_0^{\alpha s} = n_0^{\alpha s}\left(1 + \frac{1}{n^\alpha} + \cdots + \frac{1}{n_0^{\alpha s}}\right) \leq n_0^{\alpha s}\sum_{s=0}^{\infty}\left(\frac{1}{n_0^\alpha}\right)^s = n_0^{\alpha s}C \leq n^\alpha C,$$

en donde $C = \sum_{s=0}^{\infty} \left(\frac{1}{n_0^{\alpha}}\right)^s$, esta serie converge pues $\frac{1}{n_0^{\alpha}} = \frac{1}{|n_0|} < 1$, la última desigualdad se sigue del hecho de que $n_0^s \leq n < n_0^{s+1}$. Por lo que tomando $n = k^m$ se tiene $|k^m| \leq k^{\alpha m} C$, entonces $|k| \leq k^{\alpha} \sqrt[m]{C}$, tomando límite cuando $m \to \infty$ se tiene $|k| \leq k^{\alpha}$ para todo $k \geq 1$, de lo cual se tiene

$$|n| \leq n^{\alpha}, \text{ para todo } n \geq 1. \tag{2.3.3}$$

En particular la desigualdad anterior se cumple para $n_0^{s+1} - n$, de modo que

$$|n_0^{s+1} - n| \leq (n_0^{s+1} - n)^{\alpha}. \tag{2.3.4}$$

Por otro lado se tiene

$$|n_0^{s+1}| = |n + n_0^{s+1} - n| \leq |n| + |n_0^{s+1} - n|. \tag{2.3.5}$$

Usando (2.3.4), (2.3.5) y el hecho de que $|n_0| = n_0^{\alpha}$ obtenemos

$$|n| \geq |n_0^{s+1}| - |n_0^{s+1} - n| \geq n_0^{\alpha(s+1)} - (n_0^{s+1} - n)^{\alpha} = n_0^{\alpha(s+1)} \left(1 - \left(1 - \frac{1}{n_0^s}\right)^{\alpha}\right) \geq n^{\alpha} M,$$

pues $n_0^{s+1} > n$, y donde $M = \left(1 - \left(1 - \frac{1}{n_0^s}\right)^{\alpha}\right)$. De manera que $|n| \geq n^{\alpha} M$. Tomando $n = k^m$, se tiene $|k^m| \geq k^{\alpha m} M$ lo cual implica $|k| \geq k^{\alpha} \sqrt[m]{M}$, y tomando límite cuando $m \to \infty$ se tiene $|k| \geq k^{\alpha}$ para todo $k \leq 1$, en particular para n. De modo que $|n| = n^{\alpha}$ para todo entero $n \geq 1$.
Si $n < 0$, entonces $|n| = |-n| = (-n)^{\alpha}$.
Sea $x \in \mathbb{Q}^*$, entonces $x = \frac{a}{b}$, con $a, b \in \mathbb{Z}$, de manera que $\left|\frac{a}{b}\right| = \frac{|a|}{|b|} = \left|\frac{a}{b}\right|^{\alpha}$. De modo que $|\ |$ es equivalente al valor absoluto usual en $\mathbb{Q}$.
Caso 2. Supongamos que $|n| \leq 1$ para todo $n \in \mathbb{N}$. Puesto que $|\ |$ es no trivial entonces existe $n \in \mathbb{N}$ tal que $|n| < 1$. Sea $p = \text{mín}\{x \in \mathbb{N} | |x| < 1\}$, entonces p es primo, pues de lo contrario $p = ab$, con $0 < a, b < 1$, por lo que $|a|, |b| \geq 1$ y $1 > |p| = |ab| = |a||b| \geq 1$, lo cual no es posible.
Sea $m \in \mathbb{Z}$ tal que $\text{mcd}(m, p) = 1$, supongamos que $|m| < 1$ entonces existe $t \in \mathbb{N}$ tal que $|m|^t, |p|^t < \frac{1}{2}$, y puesto que $\text{mcd}(m, p) = 1$, existen $r, s \in \mathbb{N}$ tales que $1 = rp^t + sm^t$, por lo que $1 = |1| = |rp^t + sm^t| < \frac{1}{2}(|r| + |s|) \leq 1$, lo cual no es posible, en consecuencia $|m| = 1$. Así, dado $x \in \mathbb{Q}$, con $x = p^a \frac{a}{b}$, $\text{mcd}(mn, p) = 1$, entonces $|x| = |p^a||\frac{a}{b}| = |p^a| = c^a$, donde $c = |p| < 1$, de esto obtenemos que $|\ |$ es equivalente a $|\ |_p$. □

Con el concepto de norma inducida por una valuación p-ádica que introducimos previamente, podemos definir al campo de los números p-ádicos como sigue:

Definición 2.3.6. Sea p un número primo. El campo de los números p-ádicos, denotado por $\mathbb{Q}_p$, es la completación de $\mathbb{Q}$ bajo la norma $|\ |_p$. El anillo de valuación de $\mathbb{Q}_p$ lo denotaremos por $\mathbb{Z}_p$ y se llama el anillo de los enteros p-ádicos.

Sea $v_p : \mathbb{Q} \to \mathbb{Z}$ una valuación p-ádica. Se tiene que el anillo de valuación de $\mathbb{Q}$ es $R = \left\{ \frac{a}{b} \in \mathbb{Q} \mid x = p^n \frac{a}{b},\ con\ n \geq 0\ y\ \text{mcd}(ab, p) = 1 \right\} = \mathbb{Z}_{(p)}$ y su ideal máximo es $\mathfrak{B} = (p)\mathbb{Z}_{(p)}$. Demostraremos que $\frac{\mathbb{Z}_{(p)}}{(p)\mathbb{Z}_{(p)}} \cong \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$.

Sea $\varphi : \frac{\mathbb{Z}}{p\mathbb{Z}} \to \frac{\mathbb{Z}_{(p)}}{(p)\mathbb{Z}_{(p)}}$, definida por

$$\varphi(r + p\mathbb{Z}) = \frac{r}{1} + (p)\mathbb{Z}_{(p)}. \tag{2.3.6}$$

Demostraremos que φ es un isomorfismo de campos. Primero justificaremos que la función esta bien definida. Sean $r + p\mathbb{Z} = r_1 + p\mathbb{Z}$, con $r \neq r_1$, entonces $r - r_1 + p\mathbb{Z} = p\mathbb{Z}$, de modo que

$$\varphi(r - r_1 + p\mathbb{Z}) = (p)\mathbb{Z}_{(p)}.$$

Por lo anterior, $r - r_1 + (p)\mathbb{Z}_{(p)} = (p)\mathbb{Z}_{(p)}$, de ahí que $\varphi(r + p\mathbb{Z}) = \varphi(r_1 + p\mathbb{Z})$, de lo cual se tiene que φ esta bien definida.

Sean $r + p\mathbb{Z}$ y $r_1 + p\mathbb{Z}$ elementos de $\frac{\mathbb{Z}}{p\mathbb{Z}}$, entonces $\varphi((r + p\mathbb{Z}) + (r_1 + p\mathbb{Z})) = \varphi(r+r_1+p\mathbb{Z}) = r+r_1+(p)\mathbb{Z}_{(p)} = r+(p)\mathbb{Z}_{(p)}+r_1+(p)\mathbb{Z}_{(p)} = \varphi(r+p\mathbb{Z})+\varphi(r_1+p\mathbb{Z})$. Por otro lado, $\varphi((r + p\mathbb{Z})(r_1 + p\mathbb{Z})) = \varphi(rr_1 + p\mathbb{Z}) = rr_1 + (p)\mathbb{Z}_{(p)} = (r + (p)\mathbb{Z}_{(p)})(r_1+(p)\mathbb{Z}_{(p)}) = \varphi(r+p\mathbb{Z})\varphi(r_1+p\mathbb{Z})$, de manera que φ es un homomorfismo.

Sea $r + p\mathbb{Z} \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ tal que $\varphi(r + p\mathbb{Z}) = (p)\mathbb{Z}_{(p)}$, entonces $r + (p)\mathbb{Z}_{(p)} = (p)\mathbb{Z}_{(p)}$, de modo que $r = b$ con $b \in (p)$. En consecuencia $r + p\mathbb{Z} = p\mathbb{Z}$, de lo cual se tiene que φ es inyectiva.

Sea $\frac{c}{s}+(p)\mathbb{Z}_{(p)}$, con $s \notin (p)$, entonces existen $x \in \mathbb{Z}$ y $y \in (p)$ tales que $1 = xs+y$, pues $(s) + (p) = \mathbb{Z}$, por lo que $x + \frac{y}{s} = \frac{1}{s}$. Por tanto $cx + \frac{cy}{s} = \frac{c}{s}$, de donde obtenemos $\varphi(cx + p\mathbb{Z}) = \frac{c}{s} + (p)\mathbb{Z}_{(p)}$. De modo que φ es suprayectiva.

Lo anterior demuestra que φ es un isomorfismo de campos, como se quería.

Sea R el anillo de valuación de $\mathbb{Q}_p$ y $\mathfrak{B}$ su ideal máximo. Se tiene por la Proposición 1.4.8 que

$$\frac{R}{\mathfrak{B}} \cong \frac{\mathbb{Z}_{(p)}}{(p)\mathbb{Z}_{(p)}} \cong \mathbb{F}_p. \tag{2.3.7}$$

De modo que el campo residual de $\mathbb{Q}_p$ es finito, lo cual implica que $\mathbb{Q}_p$ es un campo local y, por (1.5.3), página 22, y [8, Lema 6.5], se tiene que cualquier extensión finita de $\mathbb{Q}_p$ es también un campo local.

El siguiente resultado carecteriza a los campos locales.

Teorema 2.3.7. *Sea K un campo local tal que su campo residual es de característica p, entonces:*

1. *K es de característica 0 si y sólo si es una extensión finita de $\mathbb{Q}_p$,*

2. *K es de característica p si y sólo si es una extensión finita del campo de series de Laurent $\mathbb{F}_p((T))$.*

Demostración. La demostración de este teorema puede consultarse en [7, Teorema 2.9]. □

Uno de los métodos más usados en el campo de los números p-ádicos para aproximar raíces de polinomios es el Lema de Hensel, también llamado Lema p-ádico de Newton, pues su demostración es esencialmente el método de Newton para encontrar raíces de polinomios con coeficientes reales.

Teorema 2.3.8 (Lema de Hensel)**.** *Sea $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$ con derivada $f'(x) = nx^{n-1} + (n-1)x^{n-2} + \cdots + a_1$, y sea $c_0 \in \mathbb{Z}_p$ tal que $f(c_0) \equiv 0$ (mód p) y $f'(c_0) \not\equiv 0$ (mód p). Entonces existe un único entero p-ádico c tal que $f(c) = 0$ y $c_0 \equiv c$ (mód p).*

Demostración. La idea de la demostración es construir un número p-ádico c tal que $f(c) \equiv 0$ mód p^n para todo n, lo cual implicaría que $f(c) = 0$. Para esto construiremos una sucesión única de números enteros $\{b_i\}$ tal que se cumplan las siguientes condiciones para todo k:

(a) $f(b_k) \equiv 0 \pmod{p^{k+1}}$,

(b) $b_k \equiv b_{k-1} \pmod{p^k}$,

(c) $0 \leq b_k < p^{k+1}$.

Procediendo por inducción. Si $k = 1$, supongamos que $c_0 = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \cdots$, donde $0 \leq \lambda_i < p$. Tomando $b_0 = \lambda_0$, se tiene que $b_0 \equiv c_0$ mód p, $0 \leq b_0 < p$ y , por hipótesis, $f(b_0) \equiv f(c_0) \equiv 0$ mód p. Por (b) y (c) queremos hallar $0 \leq b_1 < p^2$ tal que $b_1 \equiv b_0$ mód p^2. Sea $b_1 = b_0 + c_1 p$ para algún $0 < c_1 < p$. Se tiene que $b_1 \equiv b_0$ mód p y $0 \leq b_1 < p^2$, pues $b_0 + c_1 \leq (p-1) + (p-1)p = (p-1)(p+1) = p^2 - 1 < p^2$. Ahora, definiendo $a_n = 1$, se tiene

$$\begin{aligned} f(b_1) = f(b_0 + c_1 p) &= \sum_{i=0}^{n} a_i (b_0 + c_1 p)^i \\ &= \sum_{i=0}^{n} a_i (b_0^i + i c_1 p b_0^{i-1} + p^2 Q), \text{ donde } Q \in \mathbb{Z}_p \\ &\equiv \sum_{i=0}^{n} a_i (b_0^i + i c_1 p b_0^{i-1}) \pmod{p^2} \\ &= \sum_{i=0}^{n} a_i b_0^i + \sum_{i=0}^{n} i a_i c_1 p b_0^{i-1} \pmod{p^2} \\ &= f(b_0) + c_1 p f'(b_0) \pmod{p^2}. \end{aligned}$$

Dado que $b_0 \equiv c_0$ mód p, entonces $f(b_0) \equiv f(c_0) \equiv 0$ mód p y $f'(b_0) \equiv f'(c_0) \not\equiv 0$ mód p. Así, $f(b_0) = bp$ para algún $b \in \mathbb{Z}$. Puesto que existen únicos $q, \beta \in$

$\mathbb{Z}$, con $0 \leq \beta < p$, tales que $b = qp + \beta$, entonces $f(b_0) \equiv \beta p$ mód p^2. Para que (a) se cumpla, es decir, $f(b_1) \equiv 0$ mód p^2, debemos resolver la congruencia $\beta p + f'(b_0)c_1 p \equiv 0$ mód p^2 o equivalentemente

$$\beta + f'(b_0)c_1 \equiv 0 \text{ mód } p, \text{ para } c_1. \tag{2.3.8}$$

Se tiene por (2.3.8) que $c_1 \equiv \dfrac{-\beta}{f'(b_0)}$ mód p y, puesto que existe un único $\gamma \in \mathbb{Z}$, con $0 \leq \gamma < p$, tal que $\gamma \equiv \dfrac{-\beta}{f'(b_0)}$ mód p, entonces podemos elegir $c_1 = \gamma$. Así, dada la elección de c_1, se tiene que b_1 satisface (a), (b) y (c).
Inductivamente supongamos que hemos construído $b_0, b_1, \ldots, b_{k-1}$ tales que satisfacen (a), (b) y (c). Queremos hallar b_k con las mismas propiedades que $b_0, b_1, \ldots, b_{k-1}$. Sea $b_k = b_{k-1} + c_k p^k$, para algún $0 \leq c_k < p$, de manera que b_k cumple (a) y (b). Sólo falta verificar (c):

$$\begin{aligned} f(b_k) &= f(b_{k-1} + c_k p^k) \\ &= \sum_{i=0}^{n} a_i (b_{k-1} + c_k p^k)^i \\ &\equiv \sum_{i=0}^{n} a_i (b_{k-1}^i + i c_1 p^k b_{k-1}^{i-1}) \text{ mód } p^k \\ &= f(b_{k-1}) + c_k p f'(b_{k-1}) \text{ mód } p^k \end{aligned}$$

Sabemos que $f(b_{k-1}) \equiv 0$ mód p^n. Así, $f(b_{k-1}) = \beta p^k$, para algún $\beta \in \mathbb{Z}$. Para que $f(b_n) \equiv 0$ mód p^{k+1}, debemos resolver la congruencia $\beta p^k + f'(b_{k-1})c_k p^k$ mód p^{k+1} para c_k, o equivalentemente, $\beta + f'(b_{k-1})c_k$ mód p. Puesto que $b_{k-1} \equiv b_{k-2} \equiv \ldots \equiv b_1 \equiv b_0$ mód p, se tiene que $f'(b_{k-1}) \equiv f'(b_0) \not\equiv 0$ mód p. De modo que podemos resolver la congruencia para c_k, así $c_k \equiv \dfrac{-\beta}{f'(b_{k-1})}$ mód p. Dado que existe un único $r \in \mathbb{Z}$, con $0 \leq r < p$, tal que $r \equiv \dfrac{-\beta}{f'(b_{k-1})}$ mód p, podemos elegir $c_k = r$ y la congruencia $\beta + f'(b_{k-1})c_k$ mód p se cumple. Luego, b_k satisface (1), (2) y (3).
Sea $c = b_0 + c_1 p + c_2 p^2 + \cdots$. Notemos que $c \equiv b_n$ mód p^{n+1} para todo n. Luego, $f(c) \equiv f(b_n) \equiv 0$ mód p^{n+1} $n \geq 1$, lo cual implica que $f(c) = 0$. Además, la unicidad de c se obtiene de la unicidad de la sucesión $\{b_i\}$. □

2.4. Extensiones de normas sobre campos locales

Sea F/K una extensión de campos y $|\ |$ una norma sobre F. Notemos que si restringimos $|\ |$ a K, entonces $|\ |$ es una norma; sin embargo, si $|\ |$ es una norma sobre K, no se sabe si $|\ |$ puede extenderse a F. Si $|\ |_p$ es una norma

p-ádica de $K = \mathbb{Q}_p$, demostraremos en esta sección que cuando F/K es una extension finita, $|\ |_p$ siempre se puede extender de manera única a F. También mostraremos algunos resultados importantes de normas definidas sobre campos que son extensión de campos localmente compactos.
Sea K un campo con norma no arquimediana $|\ \ |$, es decir, $|\ \ |$ satisface las condiciones establecidas en la Definición 1.3.3. Sea V un espacio vectorial de dimensión finita sobre F. Una norma sobre V es una función $|\ |_V : V \to \mathbb{R}$ que satisface:

1. para todo $x \in V$, $|x|_V \geq 0$ y $|x|_V = 0$ si y sólo si $x = 0$,
2. para todos $x \in V$ y $a \in K$, $|ax|_V = |a||x|_V$,
3. para todos $x, y \in V$, $|x + y|_V \leq |x|_V + |y|_V$.

Por ejemplo, si F/K es una extensión finita de campos y $|\ |_F$ es una norma extensión de $|\ \ |$, entonces $|\ |_F$ también es una norma sobre F como espacio vectorial.

Definición 2.4.1. Diremos que dos normas sobre un campo K son equivalentes si definen la misma topología.

El siguiente resultado muestra una propiedad importante de las normas definidas en espacios vectoriales sobre campos localmente compactos.

Teorema 2.4.2. *Si V un espacio vectorial de dimensión finita sobre un campo K localmente compacto, entonces todas las normas en V son equivalentes.*

Demostración. Para demostrar este resultado usaremos el hecho: dos normas $|\ |_1$ y $|\ \ |_2$ son equivalente si y sólo si existen constantes positivas c_1, c_2 tales que $c_1|x|_1 \leq |x|_2 \leq c_2|x|_1$, para todo $x \in V$, [13, pág. 75]. Sea $\{v_1, v_2, \ldots, v_n\}$ una base para V y $|\ \ |$ una norma sobre K. Sea $x \in V$ con $x = a_1v_1 + \cdots + a_nv_n$. Definamos $|\ |_{sup} : V \to \mathbb{R}$ como

$$|av_1 + \cdots + a_nv_n|_{sup} = \max_{1 \leq i \leq n}(|a_i|). \tag{2.4.1}$$

Se tiene que $|\ \ |_{sup}$ definida como antes es una norma, pues para todos $x, y \in V$ y $\alpha \in K$, con $x = a_1v_1 + \cdots a_nv_n$ y $y = b_1v_1 + \cdots + b_nv_n$, $|x|_{sup} = \max\{|a_i|\} \geq 0$, $|\alpha x|_{sup} = \max\{|\alpha a_i|\} = \max\{|\alpha||a_i|\} = |\alpha| \max\{|a_i|\} = |\alpha||x|_{sup}$ y
$|x + y|_{sup} = \max\{|a_i + b_i|\} \leq \max\{|a_i| + |b_i|\} \leq \max\{|a_i|\} + \max\{|b_i|\} = |x|_{sup} + |y|_{sup}$.
Ahora, sea $|\ \ |_v$ otra norma sobre V. Notemos que

$$|x|_v \leq |a_1||v_1|_v + \cdots + |a_n||v_n|_v \leq n(\max\{|a_i|\}) \max\{|v_i|_v\}, \tag{2.4.2}$$

consecuentemente $|\ \ |_v \leq c_2|\ \ |_{sup}$, donde $c_2 = n \max\{|v_i|_v\}$. Sólo resta justificar que existe una constante c_1 tal que $c_1|\ \ |_{sup} \leq |\ \ |_v$.
Sea

$$U = \{x \in V \mid |x|_{sup} = 1\}.$$

Demostraremos que existe $\epsilon > 0$ tal que $|x|_v > \epsilon$ para todo $x \in U$. Supongamos que el hecho anterior es falso, es decir, para todo $\epsilon > 0$ existe $x \in U$ tal que $|x| < \epsilon$, en particular esto se cumple para $\epsilon_m = \dfrac{1}{m}$ entonces hay una sucesión $\{x_m\} \subset U$ tal que $|x_m|_v \to 0$ cuando $m \to \infty$. Puesto que U es compacto [12, pág. 59], la sucesión $\{x_m\}$ admite una subsucesión $\{x_{m_j}\}$ convergente, y converge a un elemento $x \in U$.
Se tiene que

$$|x|_v \leq |x - x_{m_j}|_v + |x_{m_j}|_v \leq c_2|x - x_{m_j}|_{sup} + |x_{m_j}|_v \to 0,$$

pues $x_{m_j} \to x$ y $|x_m|_v \to 0$. De modo que $|x|_v = 0$, así $x = 0$, lo cual no es posible, pues $x \in U$. Con esto concluímos que existe $\epsilon > 0$ tal que $|x|_v \geq \epsilon$ para todo $x \in U$.
Notemos que si $x \in U$, entonces $|x|_{sup} \leq \dfrac{1}{c_1}|x|_v$, donde $c_1 = \epsilon$, pues $|x|_{sup} = 1$ y $|x|_v \geq \epsilon$. Ahora, sea $x \notin U$, $x = a_1v_1 + \cdots + a_nv_n$, y j tal que $|a_j| = \text{máx}\{|a|_i\}$, entonces $\dfrac{x}{a_j} \in U$, pues $\left|\dfrac{x}{a_j}\right|_{sup} = \dfrac{|x|_{sup}}{|a_j|} = \dfrac{|a_j|}{|a_j|} = 1$. De manera que $\left|\dfrac{x}{a_j}\right|_v \geq \epsilon = c_1$, en consecuencia $c_1|a_j| = c_1|x|_{sup} \leq |x|_v$. En cualquiera de los dos casos se tiene $c_1|x|_{sup} \leq |x|_v$ para toda $x \in V$.

□

Corolario 2.4.3. *Sean $|\ |$ una norma sobre K y $V = F$ un campo, que es una extensión finita de K, entonces existe a lo más una norma sobre F que extiende a $|\ |$.*

Demostración. Se tiene que F es un espacio vectorial sobre K de dimensión finita. Por el Teorema 2.4.2 cualesquiera dos normas $|\ |_1$ y $|\ |_2$ son equivalentes, es decir, existen constantes positivas c_1, c_2 tales que $c_1|x|_1 \leq |x|_2 \leq c_2|x|_1$, para todo $x \in F$.
Sea $x \in F$. Supongamos que $|x|_1 \neq |x|_2$, si $|x|_2 < |x|_1$ entonces $\left|\dfrac{1}{x}\right|_1 < \left|\dfrac{1}{x}\right|_2$, de manera que siempre podemos elegir $x \in F$ tal que $|x|_1 \neq |x|_2$ y $|x|_1 < |x|_2$. Sea $x_0 \in F$ que satisfaga las condiciones anteriores.
Se tiene

$$|x_0|_2 \leq c_2|x_0|_1 \quad y \quad |x_0|_1 < |x_0|_2. \tag{2.4.3}$$

De esto obtenemos que $1 < \dfrac{|x_0|_2}{|x_0|_1} \leq c_2$, entonces existe $N \in \mathbb{N}$ suficientemente grande tal que $c_2 < \dfrac{|x_0^N|_2}{|x_0^N|_1}$, de ahí que $c_2|x_0^N|_1 < |x_0^N|_2$, lo cual no es posible pues $|x|_2 \leq c_2|x|_1$ para todo $x \in F$. Consecuentemente $|x|_1 = |x|_2$, para todo $x \in F$. □

Sean F/K una extensión finita y Galois, $\alpha \in F$ y $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in K[x]$ el irreducible de α. Si $N_{F/K} : F \to K$ es la función norma, entonces $N_{F/K}(\alpha) = \prod_{i=1}^{n} \alpha_i$, donde α_i son los conjugados de $\alpha = \alpha_1$ sobre K.

Sea $|\ |$ una norma sobre K y supongamos que $|\ |$ puede extenderse a una norma en F. Se tiene por el Corolario 2.4.3 que $|\ |$ se extiende de manera única a F, digamos a $|\ |_1$. Sean α_j un conjugado de α, para algún $j = 1, \cdots, n$ y σ un K-automorfismo tal que $\sigma(\alpha) = \alpha_j$. Definamos $|\ |' : F \to \mathbb{R}$ como $|x|' = |\sigma(x)|_1$, para toda $x \in F$. Se demuestra sin dificultad que $|\ |'$ es una norma extensión de $|\ |$, de manera que $|\ |_1 = |\ |'$. Así $|\alpha|_1 = |\alpha|' = |\sigma(\alpha)|_1 = |\alpha_j|_1$, de modo que podemos concluir que la norma de α coincide con la norma de cada uno de sus conjugados.

Notemos que $N_{F/K}(\alpha) \in K$, así $|N_{F/K}(\alpha)| = |N_{F/K}(\alpha)|_1 = \left|\prod_{i=1}^{n} \alpha_i\right|_1 = \prod_{i=1}^{n} |\alpha_i|_1 = \prod_{i=1}^{n} |\alpha|_v = |\alpha|_1^n$, en consecuencia

$$|\alpha|_1 = \sqrt[n]{N_{F/K}(\alpha)}. \tag{2.4.4}$$

Las propiedades de la norma $N_{F/K}$ que emplearemos para la demostración del siguiente teorema pueden consultarse en [8, pág. 19].

Teorema 2.4.4. *Sea $K/\mathbb{Q}_p$ una extensión finita. Entonces existe una norma sobre K que extiende a $|\ |_p$.*

Demostración. Sea $n = [K : \mathbb{Q}_p]$. Consideremos a $|\ | : K \to \mathbb{R}$ definida por

$$|\alpha| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(\alpha)|_p} \tag{2.4.5}$$

demostraremos que $|\ |$ es una norma extensión de $|\ |_p$.

Si $a \in \mathbb{Q}_p$, entonces $N_{F/\mathbb{Q}_p}(a) = a^n$, de manera que $|a| = \sqrt[n]{|N_{K/\mathbb{Q}_p(a)}|_p} = \sqrt[n]{|a^n|_p} = |a|_p$ para toda $a \in \mathbb{Q}_p$.

Sean $\alpha, \beta \in K$, puesto que $N_{K/\mathbb{Q}_p}$ es multiplicativa se tiene $|\alpha\beta| = |N_{K/\mathbb{Q}_p}(\alpha\beta)|_p = |N_{K/\mathbb{Q}_p}(\alpha)N_{K/\mathbb{Q}_p}(\beta)|_p = |N_{K/\mathbb{Q}_p}(\alpha)|_p |N_{K/\mathbb{Q}_p}(\beta)|_p$. Ahora, sea $\alpha \in K$ tal que $|\alpha| = 0$, entonces $|N_{K/\mathbb{Q}_p}(\alpha)| = 0$, esto ocurre si y sólo si $N_{K/\mathbb{Q}_p}(\alpha) = 0$, pues $|\ |_p$ es una norma sobre K, pero $N_{K/\mathbb{Q}}(\alpha) = 0$ sólo si $\alpha = 0$. Para finalizar solo resta demostrar que $|\alpha + \beta| \leq |\alpha| + |\beta|$. Justificaremos que $|\ |$ es no arquimediana, es decir,

$$|\alpha + \beta| \leq \text{máx}\{|\alpha|, |\beta|\}. \tag{2.4.6}$$

Supongamos que $|\beta| \geq |\alpha|$ y consideremos $\gamma = \dfrac{\alpha}{\beta}$, entonces demostrar (2.4.6) es equivalente a mostrar

$$|1 + \gamma| \leq 1. \tag{2.4.7}$$

Para justificar lo anterior usaremos el siguiente hecho: sea $|\ |$ definida como antes sobre K, entonces $|1 + \gamma| \leq 1$ para todo $\gamma \in K$ tal que $|\gamma| \leq 1$, [12, pág. 62].

Puesto que $|\beta| \leq |\alpha|$, entonces $|\gamma| = \left|\dfrac{\alpha}{\beta}\right| \leq 1$, de manera que (2.4.7) se sigue del hecho anterior. □

Consideremos $\overline{\mathbb{Q}_p}$ la cerradura algebraica de $\mathbb{Q}_p$, se tiene que $\overline{\mathbb{Q}_p}$ es la unión de todas las extensiones finitas de $\mathbb{Q}_p$. Puesto que para cada extensión finita de $\mathbb{Q}_p$ $|\ |_p$ tiene una única extensión, Teorema 2.4.4, entonces $|\ |_p$ se extiende de manera única a $\overline{\mathbb{Q}_p}$. Más precisamente, si $\alpha \in \overline{\mathbb{Q}_p}$, entonces α es raíz de un polinomio mónico irreducible sobre $\mathbb{Q}_p$, digamos $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Se define $|\ | : \overline{\mathbb{Q}_p} \to \mathbb{R}$ como $|\alpha| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(\alpha)|_p}$, donde K es una extensión finita Galois de $\mathbb{Q}$ que contiene a α y $|\ | : K \to \mathbb{Q}$ es la norma sobre K que extiende a $|\ |_p$. La demostración de que $|\ |$ es una norma sigue las mismas líneas que la prueba del Teorema 2.4.4.

El resultado anterior se puede extender a cualquier campo completo con una valuación discreta, [[19], Proposición 3, paág, 28]. El Corolario 2, pág. 29 a esta proposición es de utilidad para garantizar unicidad al extender una valuación.

CAPÍTULO 3

Criterios de irreducibilidad y polígono de Newton

En este capítulo enunciaremos algunos criterios de irreducibilidad para polinomios. El único criterio general que presentamos es el de Capelli, pues establece condiciones necesarias y suficientes para que un binomio sea irreducible. Para trinomios mostramos resultados parciales, los criterios de Nagell y de Perron. Para polinomios de grado $n > 3$ discutimos los de Eisenstein, Polya y un resultado que establece una conexión entre polinomios irreducibles y números primos.
Con el propósito de mostrar propiedades de polinomios y desarrollar un criterio de irreducibibilidad para aquellos de la forma $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$, en la segunda sección estudiamos al Polígono de Newton y sus propiedades elementales. Para finalizar exploramos a los polinomios $f(x) = x^{2^n} + rx^{2^{n-1}} + s$, empezando con los resultados que E. Driver, P. A. Leonard and K. S. Williams exponen en [5], en donde encuentran condiciones para que $f(x)$, con $n = 2$, sea irreducible en $\mathbb{Z}[x]$ pero reducible módulo p, para cualquier número primo p.

3.1. Algunos criterios de irreducibilidad

Sean K un campo y $f(x) = bx^n - ax^m \in K[x]$, $b \neq 0$, $n > m$. Para que $f(x)$ sea irreducible sobre K necesariamente $m = 0$ y $a \neq 0$ o $n = 1$ y $m = 0$. De modo que, en lo que sigue centraremos la atención en binomios de la forma $f(x) = x^n - a$.

Teorema 3.1.1. *Sean K un campo, $a \in K$ y $m, n \in \mathbb{N}$ tales que* $\text{mcd}(m, n) = 1$. *Entonces $x^{mn} - a$ es irreducible sobre K si y sólo si, $x^n - a$ y $x^m - a$ son irreducibles sobre K.*

Demostración. Supongamos que $x^{mn} - a$ es irreducible sobre K. Si $y^n - a$ es reducible entonces $y^n - a = q(y)g(y)$, con $\deg(q) > 0$ y $\deg(g) > 0$, tomando $y = x^m$ se tiene que $x^{nm} - a = q(x^m)g(x^m)$, es decir, $x^{mn} - a$ es reducible sobre K lo cual no es posible, por lo que $x^n - a$ es irreducible. De igual manera se demuestra que $x^m - a$ es irreducible.
Recíprocamente, supongamos que $x^n - a$ y $x^m - a$ son irreducibles sobre K. Sea u una raíz de $x^{nm} - a = 0$, entonces u^n y u^m son raíces de $x^m - a = 0$ y $x^n - a = 0$, respectivamente, de modo que $[K(u^n) : K] = m$ y $[K(u^m) : K] = n$.

Puesto que $K(u^n, u^m) = K(u^n)K(u^m)$ y $\text{mcd}(n, m) = 1$, entonces $[K(u^n, u^m), K] = nm$.
Se tiene que $K(u^n, u^m) = K(u)$ pues $u = u^{rn+sm} = u^{rn}u^{sm}$, para $r, s \in \mathbb{Z}$ tales que $rn+sm = 1$. En consecuencia $[k(u^n, u^m) : K] = [K(u) : K] = nm$, de manera que $x^{nm} - a$ es irreducible. □

Sea $f(x) = x^n - a \in K[x]$, donde $n = p_1^{e_1}p_2^{e_2}\cdots_k^{e_k}$ es la factorización en primos de n. Se tiene, por el resultado anterior, que $f(x)$ es irreducible si y sólo si $x^{p_i^{e_1}} - a$ es irreducible para toda i. El siguiente criterio establece cuándo un binomio de la forma $x^{p^n} - a \in K[x]$ es irreducible.

Teorema 3.1.2 (Criterio de Capelli)**.** *Sea p un primo y a un elemento en K tal que no es raíz p-ésima en K. Entonces*

1. *Si p es impar, $x^{p^n} - a$ es irreducible sobre K para todo n.*
2. *Si $p = 2$ y la característica es 2, $x^{2^n} - a$ es irreducible sobre K para todo n.*
3. *Si $p = 2$, y la característica no es 2, $x^{2^n} - a$ es irreducible sobre K si y sólo si $-4a \notin K^4$.*

Demostración. Demostraremos 1 y 2. Para esto, primero mostraremos que $x^p - a$ es irreducible sobre K. Supongamos lo contrario, sea $f(x)$ un factor irreducible de $x^p - a$ donde el grado k de $f(x)$ es tal que $0 < k < p$. Sea $u = a^{\frac{1}{p}}$, entonces todas las raíces de $x^p - a$ son de la forma ζu, donde ζ es raíz p-ésima de la unidad. Sea c el término constante de $f(x)$, entonces $\pm c = \eta u^k$, donde $\eta^p - 1 = 0$. Puesto que $\text{mcd}(p, k) = 1$ existen $r, s \in \mathbb{Z}$ tales que $rk + sp = 1$, de modo que

$$u = u^{rk}u^{sp} = \left(\frac{\pm c}{\eta}\right)^r a^s, \tag{3.1.1}$$

de donde obtenemos $u\eta^r = (\pm c)a^s$. Esto implica que $u\eta^r \in K$. Puesto que la p-ésima potencia de $u\eta^r$ es a, entonces se tiene una contradicción pues, por hipótesis, a no es una p-ésima potencia. Consecuentemente $x^p - a$ es irreducible sobre K.
Sea v una raíz de $x^{p^n} - a$ y consideremos $u = v^{p^{n-1}}$. Se tiene que u es raíz de $x^p - a$, el cual es irreducible por lo anterior, de modo que $[K(u) : K] = p$. Si probamos que $[K(v) : K(u)] = p^{n-1}$, entonces $[K(v) : K] = [K(v) : K(u)][K(u) : K] = p^{n-1}p = p^n$, lo cual implicaría que $x^{p^n} - a$ es irreducible sobre K.
Demostraremos lo anterior por inducción sobre n. Si $n = 1$, $x^p - a$ es irreducible. Supongamos $n = 2$, entonces v es raíz de $x^p - u \in K(u)[x]$, puesto que u es raíz de $x^p - a \in K[x]$, entonces por el Teorema 50 [11, pág. 60] se tiene que u no es una raíz p-ésima en $K(u)$ de modo que $x^p - u$ es irreducible sobre $K(u)$, lo cual implica que $[K(v) : K] = [K(v) : K(u)][K(u) : K] = p^2$, obteniendo el caso $n = 2$. Supongamos que el resultado es cierto para $n - 1$, es decir todo polinomio de la forma $x^{p^{n-1}} - a$, donde a no es una p-potencia sobre K, es irreducible, se tiene que v es raíz de $x^{p^{n-1}} - u \in K(u)$, pues $u = v^{p^{n-1}}$, puesto que u no es una p-potencia sobre $K(u)$, Teorema 50 [11, pág. 60], se tiene, por hipótesis de

inducción que $x^{p^{n-1}} - u \in K(u)$ es irreducible, obteniendo $[K(v) : K] = [K(v) : K(u)][K(u) : K] = p^n$. Con lo anterior queda justificado los incisos 1 y 2.
Ahora, supongamos que $p = 2$ y que la característica K no es 2. Supongamos que $x^{2^n} - a$ es irreducible y $-4a$ es una cuarta potencia en K. Sea $-4a = \alpha^4$, puesto que la característica de K no es 2, entonces $-a = \dfrac{\alpha}{4}$, de ahí que $a = -\dfrac{4}{4} \cdot \dfrac{\alpha^4}{4} = -4\left(\dfrac{\alpha}{2}\right)^4$. Sea $y = x^{2^{n-2}}$, entonces

$$x^{2^n} - a = y^4 + 4\left(\frac{\alpha}{2}\right)^4 = \left(y^2 + \alpha y + \frac{\alpha^2}{2}\right)\left(y^2 - \alpha y + \frac{\alpha^2}{2}\right), \tag{3.1.2}$$

lo cual es una contradicción pues $x^{2^n} - a$ es irreducible.

Recíprocamente, supongamos que $-4a$ no es una cuarta potencia en K. Sea v una raíz de $x^{2^n} - a$ y $u = v^{2^{n-1}}$. Se tiene que $[K(u) : K] = 2$, pues $u^2 - a = 0$, de modo que debemos probar $[K(v) : K(u)] = 2^{n-1}$. Cuando $n = 2$, por el Teorema 50 [11, pág. 60] el resultado es cierto pues $-4a$ no es una cuarta potencia de K. Para $n > 2$, usando un argumento inductivo análogo al caso anterior, el resultado se obtiene del Teorema 50 [11, pág. 60], para eso debemos justificar que $-4u$ no es una cuarta potencia en $K(u)$. Si suponemos lo contrario, entonces $-u$ es un cuadrado en $K(u)$. Ahora, considerando al K-automorfismo de $K(u)$ que manda $-u$ a u, entonces concluímos que u es un cuadrado sobre $K(u)$, lo cual por el Teorema 50 [11, pág. 60] no es posible, pues $-4a$ no es una cuarta potencia.
□

En seguida presentaremos algunos criterios para decidir irreducibilidad de trinomios con coeficientes en los enteros.
Empezaremos con el criterio de Nagell, citado en [18], el cual enuncia lo siguiente:

Teorema 3.1.3. *Sea $f(x) = x^n + qx^p + r \in \mathbb{Z}[x]$, $1 \leq p \leq n-1$, si*

1. *$|q| > 1 + |r|^{n-1}$ y*
2. *Si $h|n$, $h > 1$, entonces $|r|$ no es una h potencia,*

entonces $f(x)$ es irreducible sobre $\mathbb{Q}$. En particular se tiene que $|r| > 1$.

En el resultado anterior se tiene que $|r| > 1$. Para cuando $|r| = 1$ existen criterios tomando $p = 1$, como los que se muestran en seguida.

Teorema 3.1.4. *1. (Perron, [18]). El polinomio $f(x) = x^n + ax \pm 1 \in \mathbb{Z}[x]$ es irreducible para $|a| \geq 3$. Cuando $|a| = 2$, $f(x)$ es irreducible o tiene un factor de la forma $x \pm 1$. En el último caso, el segundo factor de $f(x)$ es irreducible sobre $\mathbb{Z}$.*

2. (Selmer, [18]). Si $|a| = 1$, entonces

a) *Los polinomios $f(x) = x^n - x - 1$ son irreducibles para todo n.*

b) *Los polinomios* $f(x) = x^n + x + 1$ *son irreducibles para cuando* $n \not\equiv 2$ *mód 3. Cuando* $n \equiv 2$ *mód 3,* $f(x)$ *tiene de factor a* $x^2 + x + 1$ *y el segundo factor es irreducible.*

La demostración del siguiente criterio lo presentaremos en la siguiente sección página 54.

Teorema 3.1.5 (Criterio de Eisenstein)**.** *Sea* R *un dominio de factorización única,* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$ *primitivo y supongamos que existe un primo* $\pi \in R$ *tal que* $\pi \nmid a_n$, $\pi \mid a_i$ *para todos* $i = 0, \ldots, n-1$ *y* $\pi^2 \nmid a_0$. *Entonces* $f(x)$ *es irreducible.*

Existen diversos criterios de irreducibilidad de polinomios en una variable que se extienden de manera natural a polinomios en varias variables. Por ejemplo, los resultados que surgen del criterio de Polya [3, Theorem 1.1, Theorem 1.3].

Teorema 3.1.6 (Citado en [3])**.** *Sea* $f(x) \in \mathbb{Z}[x]$, *con* $n = deg(f(x))$. *Supongamos que existen* $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ *tales que* $f(x_i) \neq 0$ *y*

$$|f(x_i)| < \frac{[n/2]!}{2^{[n/2]}},$$

para todo $i = 1, \ldots, n$, *entonces* $f(x)$ *es irreducible sobre* $\mathbb{Q}$.

En [21], Stefanescu discute el concepto de índice de Newton de un polinomio para presentar un criterio de irreducibilidad. Esta útil herramienta, entre otras cosas, permite obtener información sobre los factores irreducibles de un polinomio.

Definición 3.1.7 (Índice de Newton)**.** Sea K un campo con valuación v y$f(x) = a_0 x^d + a_1 x^{d-1} + \ldots a_{d-1}x + a_d \in K[x]$. Se define el índice de Newton de f como:

$$e(f) := \max_{0 \leq i \leq d} \frac{v(a_0) - v(a_i)}{i}.$$

Proposición 3.1.8. *Si* $f_1, f_2 \in A[x]$, *entonces* $e(f_1 f_2) = \max\{e(f_1), e(f_2)\}$.

Demostración. La demostración de este resultado puede consultarse en [21, Proposition 2.1]. □

Teorema 3.1.9. *Sean* A *un dominio de valuación discreta,* v *una valuación en* A *y* $f(x) = a_0 x^d + a_1 x^{d-1} + \ldots a_{d-1}x + a_d \in A[x]$. *Supongamos que* $v(a_0) = 0$ *y que existe* $s \in \{1, 2, \ldots, d\}$ *tal que las siguientes condiciones se cumplen:*

(1) $\dfrac{v(a_s)}{s} < \dfrac{v(a_i)}{i}$, *para todo* $i \neq s$,

(2) $sv(a_d) - dv(a_s) = 1$,

entonces f *es irreducible en* $A[x]$ *o tiene un factor cuyo grado es un múltiplo de* s.

Demostración. Supongamos que $f(x) = f_1(x)f_2(x)$, con $\deg(f_1)$, $\deg(f_2) > 0$ y $f_1(x), f_2(x) \in A[x]$. Denotemos $d = deg(f)$, $d_1 = deg(f_1)$, $d_2 = deg(f_2)$, $m = v(a_d)$, $a = v(a_s)$, $m_1 = v(f_1(0))$ y $m_2 = v(f_2(0))$. Con la notación anterior, reescribiendo (2) se tiene $sm - ad = 1$. Además, por la condición (1), $e(f) = -\dfrac{v(a_s)}{s} = -\dfrac{a}{s}$. Ahora, por la Proposición 3.1.8,

$$-\frac{a}{s} = e(f) = e(f_1) \geq -\frac{v(f_1(0))}{d_1} = -\frac{m_1}{d_1},$$

de manera que $ad_1 \leq sm_1$. Por otro lado, como

$$d = deg(f_1f_2) = deg(f_1) + deg(f_2) = d_1 + d_2$$

y

$$m = v(a_d) = v(f_1(0)f_2(0)) = v(f_1(0)) + v(f_2(0)) = m_1 + m_2,$$

entonces $a(d-d_2) = ad_1 \leq sm_1 = s(m-m_2)$, y puesto que $sm-ad = 1$ entonces $sm_2 - ad_2 \leq 1$.
Ahora, como $-\dfrac{a}{s} = e(f) \geq e(f_2) \geq -\dfrac{m_2}{d_2}$, entonces $0 \leq sm_2 - ad_2$. De manera que $0 \leq sm_2 - ad_2 \leq 1$. Puesto que $sm_2 - ad$ es un número entero, se tiene que $sm_2 - ad = 0$ o $sm_2 - ad = 1$, veamos qué ocurre en cada caso:

1. Supongamos que $sm_2 - ad_2 = 0$. Por la condición 2) del teorema $sm-da = 1$, de modo que a y s son primos relativos. Por lo tanto, $s \mid d_2$.

2. Supongamos que $sm_2 - ad_2 = 1$. Reemplazando m_2 por $m - m_1$ y d_2 por $d - d_1$ se tiene $s(m - m_1) - a(d - d_1) = 1$. Dado que $sm - ad = 1$, entonces $sm_1 - ad_1 = 0$, además como a y s son primos relativos obtenemos que $s \mid d_1$.

□

Presentamos el siguiente lema que será necesario para la demostración del Teorema 3.1.11.

Lema 3.1.10. *Sea $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Suponga que $a_n \geq 1, a_{n-1} \geq 0$ y $|a_i| \leq H$ para todo $i = 0, 1, \ldots, n-2$, donde H es una constante positiva. Si $\alpha \in \mathbb{C}$ y $f(\alpha) = 0$, entonces α tiene parte real no positiva o satisface*

$$|\alpha| < \frac{1 + \sqrt{1 + 4H}}{2} \tag{3.1.3}$$

Demostración. Sea $z \in \mathbb{C}$ tal que $|z| > 1$ y $\mathrm{Re}(z) > 0$. Se tiene

$$\begin{aligned}
\left|\frac{f(z)}{z^n}\right| &= \left|\frac{a_n z^n}{z^n} + \frac{a_{n-1}z^{n-1}}{z^n} + \cdots + \frac{a_0}{z^n}\right| \\
&= \left|a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n}\right| = \left|a_n + \frac{a_{n-1}}{z} - \left(-\frac{a_{n-2}}{z^2}\cdots - \frac{a_0}{z^n}\right)\right| \\
&\geq \left|a_n + \frac{a_{n-1}}{z}\right| - \left|\frac{a_{n-2}}{z^2}\cdots + \frac{a_0}{z^n}\right| \geq \left|a_n + \frac{a_{n-1}}{z}\right| - \left(\left|\frac{a_{n-2}}{z^2}\right| + \cdots + \left|\frac{a_0}{z^n}\right|\right) \\
&= \left|a_n + \frac{a_{n-1}}{z}\right| - \frac{|a_{n-2}|}{|z|^2} - \cdots - \frac{|a_0|}{|z|^n} \geq \left|a_n + \frac{a_{n-1}}{z}\right| - \frac{H}{|z|}\left(\frac{1}{|z|} + \cdots + \frac{1}{|z|^{n-1}}\right) \\
&= \left|a_n + \frac{a_{n-1}}{z}\right| - \frac{H}{|z|}\left(\frac{1 - \frac{1}{|z|^n}}{1 - \frac{1}{|z|}} - 1\right) = \left|a_n + \frac{a_{n-1}}{z}\right| - \frac{H}{|z|}\left(\frac{|z|^n - |z|}{|z|^n(|z|-1)}\right) \\
&= \left|a_n + \frac{a_{n-1}}{z}\right| - \frac{|z|^{n-1}-1}{|z|^{n-1}}\left(\frac{H}{|z|^2 - |z|}\right) > \left|a_n + \frac{a_{n-1}}{z}\right| - \frac{H}{|z|^2 - |z|} \\
&\geq Re(a_n + \frac{a_{n-1}}{z}) - \frac{H}{|z|^2 - |z|} > 1 - \frac{H}{|z|^2 - |z|} \geq 0 \iff 1 \geq \frac{H}{|z|^2 - |z|} \\
&\iff |z|^2 - |z| \geq H \iff 4|z|^2 - 4|z| + 1 \geq 1 + 4H \iff 2|z| - 1 \geq 1 + 4H \\
&\iff |z| \geq \frac{1 + \sqrt{1+4H}}{2}.
\end{aligned}$$

Sea $\alpha \in \mathbb{C}$ raíz de $f(x)$. Si $|\alpha| \leq 1$, entonces $|\alpha| < \dfrac{1+\sqrt{1+4H}}{2}$.
Si $|\alpha| > 1$, entonces $\mathrm{Re}(\alpha) \leq 0$ o $\mathrm{Re}(\alpha) > 0$. Si pasa lo primero hemos concluído. Supongamos lo segundo. Puesto que $|\alpha| > 1$ y $\mathrm{Re}(\alpha) > 0$ tomando $z = \alpha$ por lo observado antes $\left|\dfrac{f(z)}{z^n}\right| > 0$ si y sólo si $|z| \geq \dfrac{1+\sqrt{1+4H}}{2}$, dado que $f(\alpha) = 0$ entonces $|\alpha| < \dfrac{1+\sqrt{1+4H}}{2}$. □

Existen diversas conjeturas que establecen relaciones entre los números primos y polinomios irreducibles. Por ejemplo, el hecho de producir una cantidad infinita de números primos a partir de un polinomio irreducible. Con lo anterior, surge una pregunta interesante: ¿Qué se puede decir de un polinomio si este produce números primos? Si $f(x)$ produce una cantidad infinita, entonces $f(x)$ es irreducible, pues de lo contrario, supongamos que $f(x) = g(x)h(x)$, y sea $\{x_i\}_{i\geq 1} \subset \mathbb{Z}$ tal que $f(x_i) = p_i$, donde p_i es primo y $f(x_i) \neq f(x_j)$ para todo $i \neq j$. Se tiene, sin pérdida de generalidad, que $h(x_i) = \pm 1$ para una cantidad infinita de x_i, lo cual no es posible, pues esto implica que $h(x) \pm 1$ tiene una cantidad infinita de raíces.
En relación con la pregunta anterior existen resultados que indican irreducibilidad de un polinomio si este produce una cantidad finita de números primos. Incluso basta que un polinomio produzca un primo para decidir si es irreducible. Por ejemplo, Cohn [17] establece un resultado que se enuncia como sigue: Si p es un

número primo con expasión decimal

$$p = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0,$$

entonces el polinomio

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

es irreducible en $\mathbb{Z}[x]$.
Este criterio fue generalizado por Brillhart, Filaseta y Odlizko [17] para cualquier base b, como se muestra a continuación. No presentamos el caso cuando $b = 2$, sin embargo, la demostración puede consultarse en [17].

Teorema 3.1.11. *Sea $b > 2$ y p un número primo con expasión b-ádica*

$$p = a_m b^m + a_{m-1}b^{m-1} + \ldots + a_1 b + a_0$$

Entonces el polinomio $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 b + a_0$ es irreducible en $\mathbb{Q}[x]$.

Demostración. Notemos que el contenido de $f(x)$ es 1, es decir, $\text{mcd}(a_0, a_1, \ldots, a_n)$=1, pues de lo contrario si d =$\text{mcd}(a_0, a_1, \ldots, a_n)$, con $d > 1$, entonces $p = a_n b^n + a_{n-1}b^{n-1} + \ldots + a_1 x + a_0 = dq$, para algún $q \in \mathbb{Z}$, lo cual no es posible pues p es un número primo. De modo que $f(x)$ es un polinomio primitivo.
Por el Lema de Gauss, puesto que $f(x)$ es primitivo, para mostrar que $f(x)$ es irreducible en $\mathbb{Q}$ basta con demostrar que lo es en $\mathbb{Z}$.
Supongamos que $f(x) = g(x)h(x)$, con $g(x), h(x) \in \mathbb{Z}[x]\setminus\mathbb{Z}$. Puesto que $f(b) = p$, se tiene $g(b) = \pm 1$ o $h(b) = \pm 1$. Vamos a suponer que $g(b) = \pm 1$.
Escribamos a $g(x) = c\prod(x-\alpha_i)$, donde α_i es raíz de $f(x)$ y c es un número entero y es el coeficiente principal de $g(x)$. Por el Lema 3.1.10 todo cero α de $f(x)$ tiene parte real no positiva o $|\alpha| < \dfrac{1+\sqrt{1+4(b-1)}}{2}$.
Supongamos que $\alpha = x + iy$ es un cero de $f(x)$ y tiene parte real no positiva.
Ubicando los puntos (x, y), $(x, 0)$ y $(b, 0)$ en el plano, se tiene un triángulo rectángulo cuyos catetos e hipotenusa miden $|\alpha - x|$, $|b - x|$ y $|\alpha - b|$, respectivamente, de manera que, por el Teorema de Pitágoras, $|\alpha - x|^2 + |b - x|^2 = |\alpha - b|^2$, consecuentemente $|\alpha - b|^2 \geq |b - x|$, por lo que

$$|\alpha - b| \geq |b - x| = b - x > b.$$

Ahora, si α es un cero de $f(x)$ tal que $|\alpha| < \dfrac{1+\sqrt{1+4(b-1)}}{2}$, puesto que $b > 2$, se tiene

$$|\alpha| < \frac{1+\sqrt{1+4(b-1)}}{2} \leq b - 1,$$

en efecto,

$$\frac{1+\sqrt{1+4(b-1)}}{2} \leq b-1 \Leftrightarrow 1+\sqrt{1+4(b-1)} \leq 2(b-1) \Leftrightarrow$$
$$\sqrt{1+4(b-1)} \leq 2(b-1)-1 \Leftrightarrow 1+4(b-1) \leq 4(b-1)^2-4(b-1)+1 \Leftrightarrow$$
$$1 \leq b-1-1 \Leftrightarrow 3 \leq b.$$

En cualquiera de los casos anteriores se tiene que o bien $|b-\alpha| \geq b > 1$ o $|b-\alpha| \geq b-|\alpha| > b-(b-1) = 1$, de modo que

$$|g(b)| = |c\prod(b-\alpha_i)| \geq \prod |b-\alpha_i| > 1,$$

lo cual es una contradicción pues $g(b) = \pm 1$. Por lo tanto $f(x)$ es irreducible en $\mathbb{Z}$.

□

El resultado anterior puede extenderse a campos de funciones sobre campos finitos, tal como lo plantea Ram Murty en [17].

3.2. Polígono de Newton

El Polígono de Newton es un concepto que se emplea en teoría de números para explorar propiedades de polinomios en cuanto a irreducibilidad. Algunos de los resultados que se derivan de aplicar el polígono de Newton, para decidir irreducibilidad, permiten obtener información sobre raíces y factores irreducibles. Partiendo de esto se obtienen criterios de irreducibilidad. Por ejemplo, bien conocido Criterio de Eisenstein se puede obtener como un caso especial, como veremos al final de esta sección.

3.2.1. Propiedades del Polígono de Newton

Sea K_v un campo local con valuación $v : K_v \to \mathbb{Z} \cup \{\infty\}$, $\overline{K_v}$ su cerradura algebraica y $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K_v[x]$, con $a_0 a_n \neq 0$. Consideremos al conjunto

$$P = \{(i, v(a_i)) \mid v(a_i) \neq 0\} \subset \mathbb{R}^2.$$

Definición 3.2.1. El polígono de Newton de $f(x)$ con respecto a la valuación v es la cubierta convexa inferior del conjunto P.

Construcción del polígono de Newton:
El primer vértice del polígono de Newton es el punto de coordenadas $(0, v(a_0))$; las coordenadas del siguiente vértice $(i_1, v(a_{i1}))$ satisfacen $\dfrac{v(a_{i1})-v(a_0)}{i_1-0} = \min\limits_{1\leq j\leq n}\left\{\dfrac{v(a_j)-v(a_0)}{j-0}\right\}$. En general, si $(i_k, v(a_{ik}))$ es un vértice del polígono de Newton, el siguiente vértice $(i_{k+1}, v(a_{ik+1}))$ satisface $\dfrac{v(a_{ik+1})-v(a_{ik})}{i_{k+1}-i_k} = \min\limits_{i_k<j\leq n}\left\{\dfrac{v(a_j)-v(a_{ik})}{j-i_k}\right\}$. Ver Figura 3.1, pág. 47.

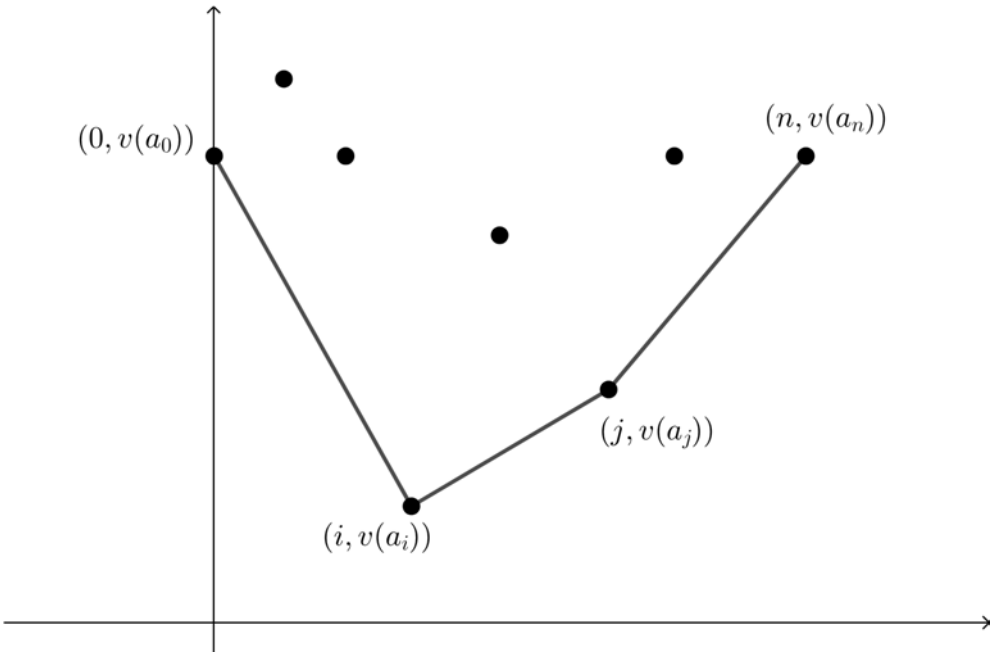


Figura 3.1: Polígono de Newton de $f(x)$ con respecto a la valuación v.

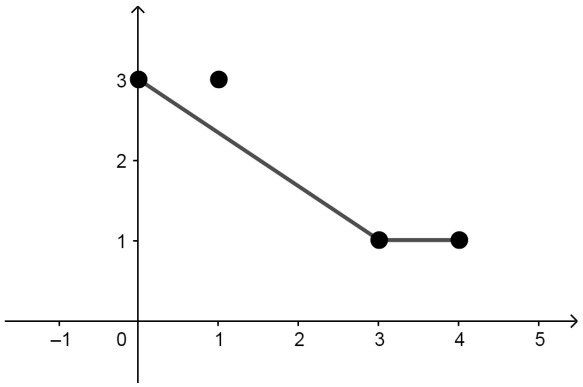


Figura 3.2: Polígono de Newton de $f(x)$ con respecto a la valuación 2-ádica.

Ejemplo 3. Sea $f(x) = 2x^4 + 6x^3 + 8x + 8 \in \mathbb{Q}[x]$ y consideremos v la valuación 2-ádica. Para este ejemplo, el conjunto P es $P = \{(0,3), (1,3), (3,1), (4,1)\}$. De modo que el polígono de Newton de $f(x)$ con respecto a la valuación v es como se muestra en la Figura 3.2.

El polígono de Newton de un polinomio $f(x)$ puede ser considerado como una función lineal a trozos. Algunos autores usan la expresión $NP(f)(x)$. Más adelante presentaremos resultados en los cuales adoptaremos la misma notación.
A continuación presentamos un resultado que establece una conexión entre las raíces de un polinomio y las pendientes de los segmentos del polígono de Newton de éste.

Proposición 3.2.2. *Sea $f(x) = f_0 + f_1 x + \cdots + f_n x^n \in K_v[x]$. Si $u \in \overline{K_v}$ es raíz de $f(x)$, entonces existe un segmento del polígono de Newton de $f(x)$ de pendiente*

igual a $-v(u)$.

Demostración. La hipótesis sobre u implica que $f_0 + f_1u + \cdots + f_nu^n = 0$. Sea i tal que $v(f_iu^i) \leq v(f_ju^j)$ para todo $j = 0, 1, \ldots, n$. Si $v(f_ku^k) \neq v(f_lu^l)$ para todo $k \neq l$, entonces

$$v(f_0 + f_1u + \cdots + f_nu^n) = \text{mín}\{v(f_ku^k)\} = v(f_iu^i) = v(0) = \infty,$$

lo cual no es posible, de modo que existe $j \neq i$ tal que $v(f_iu^i) = v(f_ju^j)$. De lo anterior se obtiene

$$\frac{v(f_j) - v(f_i)}{j - i} = -v(u).$$

De modo que $-v(u)$ es la pendiente de la recta que pasa por los puntos $P_i = (i, v(f_i))$ y $P_j = (j, v(f_j))$, cuya ecuación es $y = -v(u)(x - i) + v(f_i)$.
Notemos que la recta anterior interseca el eje vertical en $y = v(f_iu^i)$, pues si $x = 0$ entonces $y = iv(u) + v(f_i) = v(f_iu^i)$.
Probaremos que todos los puntos del polígono de Newton de $f(x)$ están en la recta $y = -v(u)(x - i) + v(f_i)$ o en el semiplano superior determinado por ésta, lo cual implicaría que esta recta contiene un segmento del polígono de Newton de $f(x)$.
Sea $P_k = (k, v(f_k))$ y consideremos la coordenada $(0, v(f_ku^k))$. Se tiene por hipótesis sobre i, que $v(f_iu^i) \leq v(f_ku^k)$. Además, la recta que pasa por P_k y $(0, v(f_ku^k))$ tiene pendiente

$$m = \frac{v(f_ku^k) - v(f_k)}{-k} = \frac{v(f_k) + kv(u) - v(f_k)}{-k} = -v(u),$$

de modo que la recta $y = -v(u)(x - i) + v(f_i)$ es paralela a la recta que pasa por los puntos P_k y $(0, v(f_ku^k))$, esto implica necesariamente que P_k está sobre la recta $y = -v(u)(x - i) + v(f_i)$ o en el semiplano superior determinado por ésta, pues de lo contrario se tendría una situación como se muestra en la Figura 3.3, lo cual no es posible. □

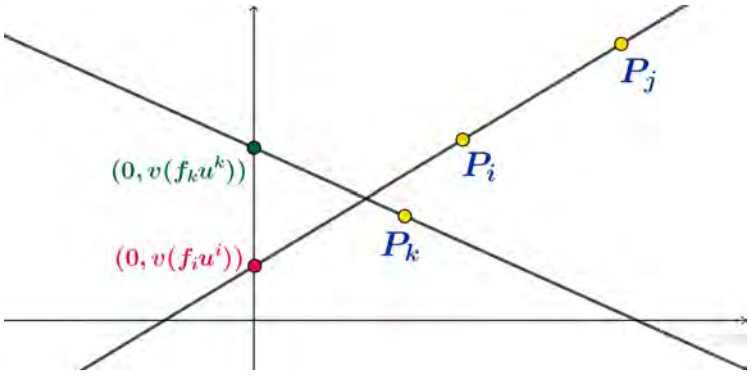


Figura 3.3

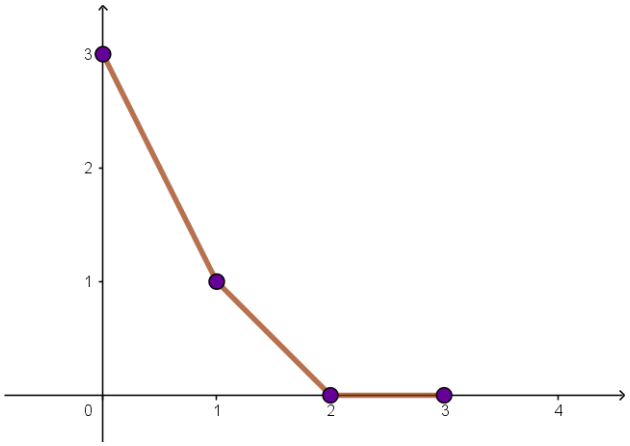


Figura 3.4

Ejemplo 4. Sea $f(x) = x^3 + 16x^2 + 69x + 54 = (x+1)(x+6)(x+9)$. El polígono de Newton de $f(x)$ con respecto a la valuación 3-ádica es el que se muestra en la Figura 3.4.
Notemos que los segmentos del polígono de $f(x)$ tienen pendientes -2, -1 y 0, las cuales coinciden con el negativo de las valuaciones de sus raíces, $v(-1) = 0$, $v(-6) = 1$ y $v(-9) = 2$.

La conexión que mostramos previamente entre las raíces y el polígono de Newton es más general, como se muestra en seguida, pues para cada pendiente de los segmentos del polígono de Newton, existen una o varias raíces que satisfacen el enunciado de la Proposición 3.2.2.

Lema 3.2.3. *Sean* $f(x) = \left(1 - \frac{x}{\alpha_1}\right)\left(1 - \frac{x}{\alpha_1}\right)\cdots\left(1 - \frac{x}{\alpha_n}\right)$, $\alpha_i \in \overline{K_v}$ *y* $\lambda_i = v\left(\frac{1}{\alpha_i}\right)$ *para* $i = 1, 2, \ldots, n$. *Si el polígono de Newton de* $f(x)$ *tiene un segmento de pendiente* λ *y longitud* l, *entonces existen* l *elementos de* $\{\lambda_1, \ldots, \lambda_n\}$ *que son iguales a* λ.

Demostración. Ordenando a los $\lambda_1, \ldots, \lambda_n$ podemos suponer que $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Si $\lambda_1 = \cdots = \lambda_r \leq \lambda_{r+1}$, demostraremos que el primer segmento del polígono de Newton de $f(x)$ es el que une a los puntos $(0,0)$ y $(r, r\lambda_1)$. Si $f(x) = a + a_1x + a_2x^2 + \cdots + a_nx^n$, cada a_i se expresa en términos de los elementos $\frac{1}{\alpha_j}$ vía las funciones simétricas; de manera más precisa, a_i es suma de productos de $\frac{1}{\alpha_j}$, donde cada sumando es de la forma $\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}$, con $k_j \in \{1, \ldots, n\}$, $k_j \neq k_l$ para todo $j \neq l$. Si $1 \leq i \leq r-1$ y $\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}$ es un sumando de a_i, entonces

$$v\left(\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}\right) = v\left(\frac{1}{\alpha_{k_1}}\right) + \cdots + v\left(\frac{1}{\alpha_{k_i}}\right) = \lambda_{k_1} + \cdots + \lambda_{k_i} \geq i\lambda_1,$$

de manera que

$$v(a_i) \geq \text{mín}\left\{v\left(\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}\right)\right\} \geq i\lambda_1,$$

de modo que el punto $(i, v(a_i))$ se encuentra arriba del punto $(i, i\lambda_1)$, y en consecuencia en la línea que une a los puntos (0,0) y $(r, r\lambda_1)$ o en el semiplano superior determinado por ésta.

Si $i = r$, entonces a_r tiene un sumando de valuación $r\lambda_1$, a saber, $\frac{1}{\alpha_1\alpha_2\cdots\alpha_r}$, los demás factores tienen valuación $> r\lambda_1$, pues en $\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_r}}$ al menos un α_{k_j} pertenece al conjunto $\{\alpha_{r+1}, \ldots, \alpha_n\}$, por lo que $v(a_r) = r\lambda_1$.

Si $i > r$, entonces todo sumando de a_i tiene valuación $> i\lambda_1$, así que$v(a_i) > i\lambda_1$.

De manera que el polígono de Newton tiene un segmento que une a los puntos $(0, 0)$ y $(r, r\lambda_1)$.

Discutamos el caso cuando $\lambda_s < \lambda_{s+1} = \cdots = \lambda_{s+r} < \lambda_{r+s+1}$. Demostraremos que el polígono de Newton de $f(x)$ tiene un segmento que une a los puntos $(s, \lambda_1 + \cdots + \lambda_s)$ y $(s + r, \lambda_1 + \lambda_2 + \cdots + \lambda_s + r\lambda_{s+1})$.

Notemos que a_s tiene un sumando con valuación $\lambda_1 + \lambda_2 + \cdots + \lambda_s$, el cual es $\frac{1}{\alpha_1\alpha_2\cdots\alpha_s}$, los demás sumandos tienen valuación $> \lambda_1 + \lambda_2 + \cdots + \lambda_s$, pues si $\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_s}}$ es un sumando de a_s, con $k_i \in \{1, \ldots, n\}$ y $\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_s}} \neq \frac{1}{\alpha_1\alpha_2\cdots\alpha_s}$, entonces al menos un α_{k_j} pertenece al conjunto $\{\alpha_{s+1}, \ldots, \alpha_n\}$, de modo que $v(a_s) = \lambda_1 + \cdots + \lambda_s$.

Si $s < i < s + r$, todo sumando de a_i tiene valuación mayor que $\lambda_1 + \cdots + \lambda_s$, pues un sumando de a_i es de la forma $\frac{1}{\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_i}}$, en el cual al menos un α_{kj} pertenece al conjunto $\{\alpha_{s+1}, \ldots, \alpha_n\}$, por lo tanto $v(a_i) > \lambda_1 + \lambda_2 + \cdots + \lambda_s$.

Consideremos a a_{s+r} y notemos que a_{r+s} tiene un sumando de valuación $\lambda_1 + \cdots + \lambda_s + r\lambda_{s+1}$, a saber, $\frac{1}{\alpha_1\alpha_2\cdots\alpha_s\alpha_{s+1}\cdots\alpha_{s+r}}$, el resto de los sumandos tienen valuación $> \lambda_1 + \cdots + \lambda_s + r\lambda_{s+1}$, de modo que $v(a_{r+s}) = \lambda_1 + \cdots + \lambda_s + r\lambda_{s+1}$.

Ahora, si $i > s + r$, todos los sumandos de a_i tienen valuación $> \lambda_1 + \cdots + \lambda_s + r\lambda_{s+1}$, y en consecuencia $v(a_i) > \lambda_1 + \cdots + \lambda_s + r\lambda_{s+1}$.

Lo anterior prueba que el polígono de Newton de $f(x)$ tiene un segmento que une a los puntos $(s, \lambda_1 + \cdots + \lambda_s)$ y $(r + s, \lambda_1 + \cdots + \lambda_s + r\lambda_{s+1})$.

□

Dorwart en [4] establece que el polígono de un producto de polinomios es la concatenación de los polígonos de sus factores, es decir, los segmentos del polígono de un producto son los segmentos de los polígonos de sus factores, donde las pendientes se ordenan de menor a mayor. Para ilustrar mejor el resultado anterior presentamos el siguiente ejemplo:

Ejemplo 5. Sea $f(x) = x^5 + 6x^4 + 2x^3 - 4x^2 + 40x + 32 \in \mathbb{Q}[x]$ y v la valuación 2-ádica. Se tiene que $f(x) = (x^2 + 6x + 4)(x^3 - 2x + 8)$ y los polígonos de

$f(x), x^2 + 6x + 4$ y $x^3 - 2x + 8$ son como se muestran en las Figuras 3.5 y Figuras (a) y (b). Además, los segmentos del polígono de $f(x)$ son precisamente los segmentos de los polígonos de sus factores, y las pendientes están ordenadas de menor a mayor.

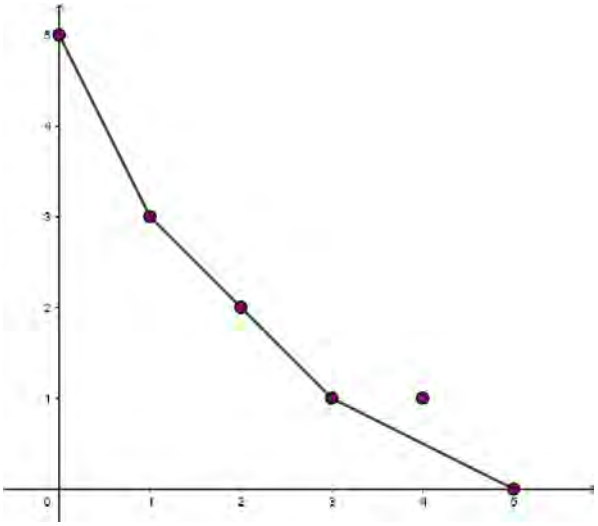
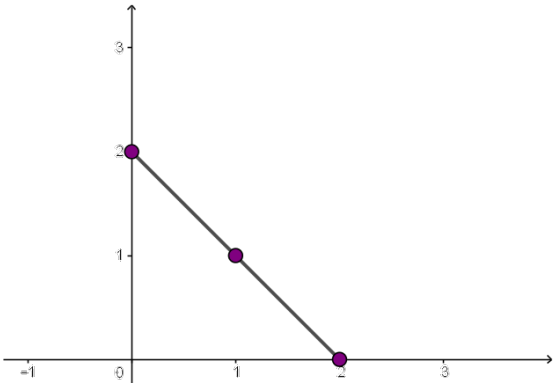
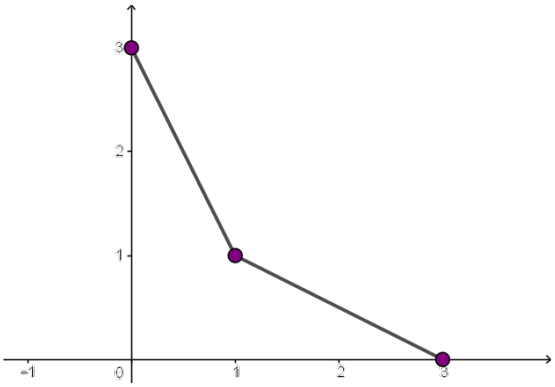


Figura 3.5: Polígono de $f(x)$.



(a) Polígono de Newton de $x^2 + 6x + 4$ con respecto a la valuación v.



(b) Polígono de Newton de $x^3 - 2x + 8$ con respecto a la valuación v.

Discutiremos el resultado citado previamente empezando con algunos casos particulares.
Iniciaremos mostrando el siguiente caso, cuando las pendientes de uno de los factores son menores o iguales que las pendientes del segundo factor. La demostración se obtuvo de [9].

Lema 3.2.4. *Sean* $f(x) = f_d x^d + f_{d-1}x^{d-1} + \cdots + f_1 x + f_0$ *y* $g(x) = g_e x^e + g_{e-1}x^{e-1} + \cdots + e_1 x + e_0$ *elementos de* $K_v[x]$ *tales que todas las pendientes de* $NP(f)$ *son menores o iguales que todas las pendientes de* $NP(g)$*, entonces*

$$NP(fg)(x) = \begin{cases} NP(f)(x) + NP(g)(0), & si \quad x \in [0, d] \\ NP(f)(d) + NP(g)(x - d), & si \quad x \in [d, d + e] \end{cases}$$

Demostración. Se tiene que $(fg)(x) = \sum_{i=0}^{d+e} h_i x^i$, donde $h_i = \sum f_j g_{i-j}$.
Si $i \in [0, d]$, entonces $v(h_i) = v(g_0 f_i + \cdots + g_j f_{i-j} + \cdots)$ y $v(g_0 f_i) = v(g_0) + v(f_i) \geq NP(g)(0) + NP(f)(i)$, con igualdad si $v(f_i) = NP(f)(i)$. Para $j > 0$, $v(g_j f_{i-j}) = v(g_j) + v(f_{i-j}) \geq NP(g)(j) + NP(f)(i-j) > NP(g)(0) + NP(f)(i)$ pues por hipótesis sobre las pendientes de $NP(f)$ y $NP(g)$ se tiene

$$\frac{NP(g)(j) - NP(g)(0)}{j - 0} > \frac{NP(f)(i) - NP(f)(i-j)}{i - (i-j)},$$

de ahí que $NP(g)(j) + NP(f)(i-j) > NP(g)(0) + NP(f)(i)$. De lo anterior obtenemos que $NP(fg)(x) = NP(g)(0) + NP(f)(x)$, si $x \in [0, d]$.
Ahora, supongamos que $i \in [d, d+e]$, entonces $h_i = f_d g_{i-d} + \cdots + f_{d-j} g_{i+j-d} + \cdots$ y $v(f_d g_{i-d}) = v(f_d) + v(g_{i-d}) \geq NP(f)(d) + NP(g)(i-d)$ con igualdad si $v(g_{i-d}) = NP(g)(i-d)$. Para $j > 0$, $v(f_{d-j} g_{i+j-d}) = v(f_{d-j}) + v(g_{i+j-d}) \geq NP(f)(d-j) + NP(g)(i+j-d) > NP(f)(d) + NP(g)(i-d)$ pues por hipótesis sobre las pendientes de $NP(f)$ y de $NP(g)$ se tiene que

$$\frac{NP(g)(i+j-d) - NP(g)(i-d)}{i+j-d-(i-d)} > \frac{NP(f)(d) - NP(f)(d-j)}{id - (d-j)},$$

de ahí que $NP(f)(d-j) + NP(g)(i+j-d) > NP(f)(d) + NP(g)(i-d)$. De lo anterior obtenemos que $NP(fg)(x) = NP(g)(0) + NP(f)(x)$ si $x \in [0, d]$. □

Usando las ideas de la demostración anterior, demostramos un caso más general, como se muestra a continuación.

Teorema 3.2.5. *Sean $f(x) = f_d x^d + f_{d-1} x^{d-1} + \cdots + f_1 x + f_0$ y $g(x) = g_e x^n + g_{e-1} x^{e-1} + \cdots + g_1 x + g_0$ en $K[x]$. Supongamos que el polígono de Newton de $f(x)$ consiste de un segmento de pendiente m. Además, supongamos que el polígono de Newton de $g(x)$ consiste de k segmentos, con pendientes $m_1, m_2, \ldots, m_k$ y $m_1 < m_2 < \cdots < m_k$. Si $m_1 < m_2 < \cdots < m_l \leq m \leq m_{l+1} < \cdots < m_k$, entonces el polígono de Newton de $(fg)(x)$ es*

$$NP(fg)(x) = \begin{cases} NP(f)(0) + NP(g)(x), & si \quad x \in [0, i_l] \\ NP(f)(x - i_l) + NP(g)(i_l), & si \quad x \in [i_l, i_l + d] \\ NP(f)(d) + NP(g)(x - d), & si \quad x \in [i_l + d, e + d] \end{cases},$$

donde el j-ésimo segmento del polígono de Newton de $g(x)$ es el que une a los puntos $(i_{j-1}, v(g_{ij-1}))$ y $(i_j, v(g_{i_j}))$; el primer segmento es el que une a los puntos $(0, v(g_0))$ y $(i_1, v(g_{i_1}))$.

Demostración. Sea $(fg)(x) = \sum_{i=0}^{d+e} h_i x^i$, donde $h_i = \sum f_j g_{i-j}$.
Si $0 \leq i \leq i_l$, entonces $h_i = f_0 g_i + f_1 g_{i-1} + \cdots + f_j g_{i-j} + \cdots$.
Se tiene que

$$v(f_0 g_i) = v(f_0) + v(g_i) \geq NP(f)(0) + NP(g)(i),$$

con igualdad si $i \in \{i_1, i_2, \ldots, i_l\}$, y

$$v(f_j g_{i-l}) = v(f_j) + v(g_{i-l}) \geq NP(f)(j) + NP(g)(i-1) > NP(f)(0) + NP(g)(i-j),$$

pues por hipótesis sobre las pendientes de los polígonos de $f(x)$ y $g(x)$ se tiene que

$$\frac{NP(f)(j) - NP(f)(0)}{j} > \frac{NP(g)(i) - NP(g)(i-j)}{i - (i-j)}.$$

De modo que $NP(fg)(x) = NP(f)(0) + NP(g)(x)$, para todo $x \in [0, i_l]$.
Si $i_l < i \leq i_l + d$, entonces $h_i = g_{il} f_{i-i_l} + \cdots + g_{i_l - j} f_{i+j-i_l} + \cdots$.
Observemos que

$$v(g_{il} f_{i-i_l}) \geq NP(g)(i_l) + NP(f)(i - i_l),$$

con igualdad si $i = i_l + d$, y

$$v(g_{i_l - j} f_{i+j-i_l}) \geq NP(g)(i_l - j) + NP(f)(i + j - i_l) > NP(g)(i_l) + NP(f)(i - i_l),$$

pues por hipótesis

$$\frac{NP(f)(i + j - i_l) - NP(f)(i - i_l)}{i + j - i_l - (i - i_l)} > \frac{NP(g)(i_l) - NP(g)(i - i_l)}{i_l - (i_l - j)}.$$

De lo anterior obtenemos que $NP(fg)(x) = NP(f)(x - i_l) + NP(g)(i_l)$, para todo $x \in (i_l, i_l + d]$.
Si $i_l + d < i \leq d + e$, entonces $h_i = f_d g_{i-d} + \cdots + f_{d-j} g_{i-d+j} + \cdots$.
Notemos que

$$v(f_d g_{i-d}) \geq NP(f)(d) + NP(g)(i - d),$$

con igualdad si $i \in \{i_{l+1} + d, i_{l+2} + d, \ldots, d + e\}$, además

$$v(f_{d-j} g_{i-d+j}) \geq NP(f)(d - j) + NP(g)(1 - d + j) > NP(f)(d) + NP(g)(i - d),$$

pues $\dfrac{NP(g)(i - d + j) - NP(g)(i - d)}{i - d + j - (i - d)} > \dfrac{NP(f)(d) - NP(f)(d - j)}{d - (d - j)}$.
De manera que $NP(fg)(x) = NP(f)(d) + NP(g)(x - d)$, para todo
$x \in (i_l + d, d + e]$. □

Teorema 3.2.6. *Si $f(x)$ y $g(x)$ son elementos de $K_v[x]$, entonces el polígono de Newton de $fg(x)$ es la concatenación de los polígonos de $f(x)$ y de $g(x)$.*

Demostración. Se tiene que el polígono de Newton de $f(x)$ es el polígono de $\dfrac{f(x)}{a_n}$, con un desplazamiento en dirección del eje vertical de $v(a_n)$. De modo que podemos suponer que los polinomios $f(x)$ y $g(x)$ son mónicos.
Se tiene que

$$f(x) = \left(\frac{x}{\alpha_1} - 1\right)\left(\frac{x}{\alpha_2} - 1\right)\cdots\left(\frac{x}{\alpha_n} - 1\right), \quad g(x) = \left(\frac{x}{\beta_1} - 1\right)\left(\frac{x}{\beta_2} - 1\right)\cdots\left(\frac{x}{\beta_m} - 1\right),$$

con $\alpha_i, \beta_j \in \overline{K_v}$, para todo $i = 1, \ldots, n$ y $j = 1, \ldots, m$.
Sean $\lambda_i = v\left(\frac{1}{\alpha_i}\right)$ y $\mu_j = v\left(\frac{1}{\beta_j}\right)$; por el Lema 3.2.3 sabemos que las pendientes de los polígonos de $f(x)$ y $g(x)$ son precisamente λ_i y μ_j, respectivamente. Supongamos que k de $\lambda_1, \lambda_2, \ldots, \lambda_n, \mu_1, \ldots, \mu_m$ son iguales, digamos a λ, entonces por el Lema 3.2.3 el polígono de $(fg)(x)$ tiene un segmento de longitud k y pendiente λ. Esto demuestra que el polígono de Newton de $(fg)(x)$, es la concatenación de los polígonos $f(x)$ y $g(x)$. □

Sea $f(x) \in K_v[x]$, con $\deg(f) = n$, y polígono de Newton como se muestra en la Figura 3.6.

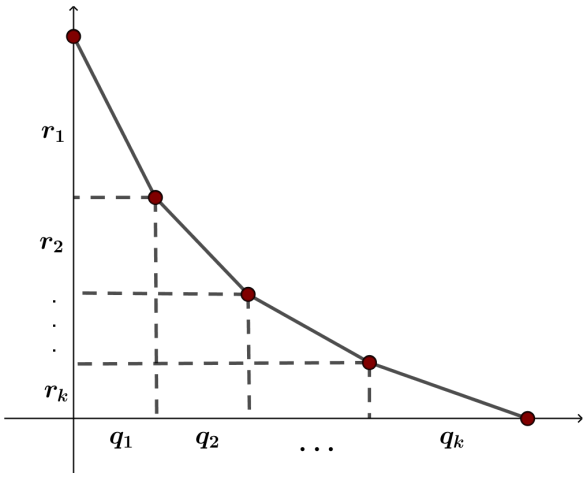


Figura 3.6: Polígono de Newton de $f(x)$.

Se tiene que $q_1+q_2+\cdots+q_k = n$ y $r_1+r_2+\cdots+r_k = v(a_0)$, además $q_i, r_i \in \mathbb{Z}$ para todo i, de modo que existe el máximo común divisor de r_i y q_i, al cual llamaremos $e_i = \text{mcd}(q_i, r_i)$.
Sea $q_i = e_i\lambda_i$ y $r_i = e_i t_i$, con $\text{mcd}(\lambda_i, t_i) = 1$. Un resultado citado en [4, pág. 371], establece que los posibles factores irreducibles de $f(x)$ tienen grado m, donde m es de la forma

$$m = \sum_{j=1}^{k} q_i\lambda_i,$$

donde $q_i \in \{0, 1, \ldots, e_i\}$.
Para los polinomios que satisfacen las condiciones del criterio de Eisenstein, su polígono de Newton consiste de un segmento que une a los puntos $(0, 1)$ y $(n, 0)$. De lo cual se tiene que $k = 1$, $r_1 = 1$, $q_1 = n$, $e_1 = 1$ y $\lambda_1 = n$. De manera que $m = 0$ o $m = n$, de donde se obtiene que $f(x)$ es irreducible.

3.3. Polinomios de la forma $f(x) = x^{2^n} + rx^{2^{n-1}} + s$.

E. Driver, P. A. Leonard y K. S. Williams en [5] analizan polinomios de la forma $f(x) = x^4 + rx^2 + s \in \mathbb{Z}[x]$. El objetivo principal de su trabajo es presentar

polinomios $f(x)$ que sean irreducibles en $\mathbb{Z}[x]$ pero reducibles módulo p para todo primo p. Además, muestran propiedades algebraicas de tales polinomios, por ejemplo, mencionan que su grupo de Galois es el 4-grupo de Klein. También, usando el teorema Chino del Residuo encuentran una familia de polinomios $f(x)$ que son irreducibles en $\mathbb{Z}[x]$ pero cuya reducción módulo n es reducible para todo entero $n > 1$.
Con el propósito de estudiar a los polinomios de la forma $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$, $n > 1$, presentaremos algunos de los resultados que E. Driver, P. A. Leonard and K. S. Williams exponen en [5].
Iniciaremos con un teorema que muestra condiciones necesarias y suficientes para que $f(x)$, con $n = 2$, sea reducible en $\mathbb{Z}[x]$.

Teorema 3.3.1. *Sean $r, s \in \mathbb{Z}$. El polinomio $f(x) = x^4 + rx^2 + s$ es reducible en $\mathbb{Z}[x]$ si y sólo si existen enteros a, c y e que satisfacen:*

1. $c + e - a^2 - r = 0$,
2. $a(e - c) = 0$,
3. $ce - s = 0$.

Si esto se cumple, entonces $f(x) = (x^2 + ax + c)(x^2 - ax + e)$.

Demostración. Supongamos que $f(x)$ es reducible en $\mathbb{Z}[x]$. Entonces $f(x)$ tiene un factor lineal, $x - m$ o un factor cuadrático $x^2 + ax + c$. Si $f(x)$ tiene un factor de la forma $x - m$ entonces m y $-m$ son raíces, de modo que $f(x)$ es divisible por $x^2 - m^2$. Por lo anterior podemos concluir que si $f(x)$ es reducible, necesariamente tiene un factor cuadrático. De esto se tiene que $f(x) = (x^2 + ax + c)(x^2 + tx + e)$, para algunos enteros t y e. Desarrollando el producto anterior se llega a

$$f(x) = x^4 + (t + a)x^3 + (e + at + c)x^2 + (ae + ct)x + ec.$$

Comparando coeficientes obtenemos que $a = -t$, $e + at + c = e - a^2 + c = r$, $ae + ct = ae - ca = 0$ y $ce = s$, obteniendo 1, 2 y 3 del teorema, además, puesto que $a = -t$, entonces se tiene $f(x) = (x^2 + ax + d)(x^2 - ax + e)$.
Recíprocamente, si 1, 2 y 3 del teorema se cumplen, entonces

$$(x^2 + ax + c)(x^2 - ax + e) = x^4 + (e - a^2 + c)x^2 + (ae - ac)x + ec = x^4 + rx^2 + s,$$

de modo que $f(x)$ es reducible en $\mathbb{Z}[x]$. □

Se tiene que $r^2 - 4s$ es el discriminante del polinomio $x^2 + rx + s \in \mathbb{Z}[x]$. Por otro lado, el hecho de que $x^2 + rx + s$ sea irreducible en $\mathbb{Z}[x]$ depende de si $r^2 - 4s$ es o no un cuadrado. De manera que, es natural preguntarse ¿qué sucede con $f(x)$ si $r^2 - 4s$ es o no un cuadrado? Los siguientes dos colorarios responden a la pregunta.

Corolario 3.3.2. *Si $r^2 - 4s = t^2$, para algún $t \in \mathbb{Z}$, entonces $f(x)$ es reducible en $\mathbb{Z}[x]$ y $f(x) = \left(x^2 + \left(\frac{r+t}{2}\right)\right)\left(x^2 + \left(\frac{r-t}{2}\right)\right)$.*

Demostración. Si $r^2 - 4s = t^2$, entonces $s = \left(\frac{r+t}{2}\right)\left(\frac{r-t}{2}\right)$, de manera que $f(x) = x^4 + rx^2 + s = x^4 + rx^2 + \left(\frac{r+t}{2}\right)\left(\frac{r-t}{2}\right) = \left(x^2 + \left(\frac{r+t}{2}\right)\right)\left(x^2 + \left(\frac{r-t}{2}\right)\right)$. □

Corolario 3.3.3. *Si $r^2 - 4s$ no es un cuadrado, entonces $f(x)$ es reducible en $\mathbb{Z}[x]$, si y sólo si existe $c \in \mathbb{Z}$ tal que $c^2 = s$, $2c - r = a^2$, para algún $a \in \mathbb{Z}$.*
Si esto se cumple, entonces $f(x) = (x^2 + ax + c)(x^2 - ax + c)$.

Demostración. Supongamos que $f(x)$ es reducible en $\mathbb{Z}[x]$, entonces existen $a, c, e \in \mathbb{Z}$ tales que $c + e - a^2 - r = 0$, $a(e - c) = 0$ y $ec - s = 0$. Puesto que $a(e - c) = 0$ se tiene que $a = 0$ o $e = c$. Si $a = 0$, entonces $c + e = r$, de modo que $r^2 - 4s = (c + e)^2 - 4(ce) = (c - e)^2$, lo cual no es posible pues por hipótesis $r^2 - 4s$ no es un cuadrado. Luego, $s = ce = c^2$ y $2c - r = a^2$.
Recíprocamente, si $c^2 = s$ y $2c - r = a^2$, entonces $c, e, a \in \mathbb{Z}$, con $e = c$, satisfacen las condiciones del Teorema 3.3.1, por lo tanto $f(x)$ es reducible en $\mathbb{Z}[x]$. □

El siguiente resultado es similar al Teorema 3.3.1 para polinomios $f(x)$ módulo p^k, con p un número primo y k entero positivo. La demostración del teorema es análoga a la del Teorema 3.3.1.

Teorema 3.3.4. *Sea p un número primo y k un entero positivo. El polinomio $f(x) = x^4 + rx^2 + s \in \mathbb{Z}[x]$ es reducible módulo p^k si y sólo si existen enteros a, c y e tales que:*

1. $c + e - a^2 - r \equiv 0 \pmod{p^k}$,
2. $a(e - c) \equiv 0 \pmod{p^k}$,
3. $ce - s \equiv 0 \pmod{p^k}$.

Si esto se cumple, entonces $f(x) = (x^2 + ax + c)(x^2 - ax + e) \pmod{p^k}$.

Observación 3.3.5. *Sea p un primo impar.*

1. *Si $s \equiv 0 \pmod{p}$, con $k = 1, a = c = 0$ y $e = r$ se tiene*

$$\begin{gathered} c + e - a^2 - r = 0, \\ a(e - c) = 0 \text{ y} \\ ce - s = -s \equiv 0 \pmod{p}, \end{gathered}$$

de modo que

$$x^4 + rx^2 + s \equiv (x^2 + ax + c)(x^2 - ax + e) = x^2(x^2 + r) \pmod{p}.$$

2. *Si $r^2 - 4s \equiv 0 \pmod{p}$, con $k = 1, a = 0, c = e \equiv \frac{r}{2} \pmod{p}$ se tiene*

$$c + e - a^2 - r = 2e - r \equiv 2 \cdot \frac{r}{2} - r = 0 \text{ mód } p,$$
$$a(e - c) = 0 \text{ y } ce - s \equiv \frac{r^2}{4} - s \equiv 0 \text{ mód } p,$$

pues $r^2 - 4s \equiv 0$ mód p. *Por lo tanto*

$$\begin{aligned} x^4 + rx^2 + s &\equiv (x^2 + ax + c)(x^2 - ax + e) \\ &\equiv \left(x^2 + \frac{r}{2}\right)\left(x^2 + \frac{r}{2}\right) \\ &= \left(x^2 + \frac{r}{2}\right)^2 \text{ mód } p. \end{aligned}$$

Usando el símbolo de Legendre, Carlitz [5] presenta un teorema, el cual presentamos a continuación, que muestra condiciones de reducibilidad módulo p de polinomios de la forma $f(x) = x^4 + rx^2 + s$, si $r^2 - 4s$ no es un cuadrado. Este resultado será empleado para demostrar cuándo $f(x)$ es reducible módulo p, para todo primo p, Teorema 3.3.8.

Teorema 3.3.6. *Si p es un primo impar y $r, s \in \mathbb{Z}$ tales que $s \not\equiv 0$ mód p y $r^2 - 4s \not\equiv 0$ mód p, entonces:*

1. *$f(x)$ es el producto de dos polinomios lineales mónicos distintos y un polinomio cuadrático irreducible módulo p si y sólo si*

$$\left(\frac{s}{p}\right) = -1 \qquad y \qquad \left(\frac{r^2 - 4s}{p}\right) = 1.$$

2. *$f(x)$ es el producto de cuatro factores lineales mónicos distintos módulo p si y sólo si*

$$\left(\frac{s}{p}\right) = 1, \qquad \left(\frac{r^2 - 4s}{p}\right) = 1 \qquad y \qquad \left(\frac{-r - 2t}{p}\right) = 1.$$

   donde t es un número entero tal que $s \equiv t^2$ mód p.

3. *$f(x)$ es el producto de dos polinomios cuadráticos mónicos irreducibles distintos módulo p si y sólo si*

$$\left(\frac{s}{p}\right) = 1, \qquad \left(\frac{r^2 - 4s}{p}\right) = 1 \qquad y \qquad \left(\frac{-r - 2t}{p}\right) = -1.$$

   donde t es un número entero tal que $s \equiv t^2$ mód p, o

$$\left(\frac{s}{p}\right) = 1 \qquad y \qquad \left(\frac{r^2 - 4s}{p}\right) = -1.$$

4. *$f(x)$ es irreducible módulo p si y sólo si*

$$\left(\frac{s}{p}\right) = -1 \qquad y \qquad \left(\frac{r^2-4s}{p}\right) = -1.$$

donde $\left(\frac{*}{p}\right)$ *significa el símbolo de Legendre.*

El siguiente lema será usado en la demostración del Teorema 3.3.8.

Lema 3.3.7. *Si* $\Pi = \{p_1, p_2, \ldots, p_k\}$ *es un conjunto no vacío de números primos y* $\epsilon : \Pi \to \{1, -1\}$ *una función, entonces existen infinitos primos* p *tales que*

$$\chi_p(p_i) = \epsilon(p_i),$$

para todo $i = 1, \ldots, k$, *donde* $\chi_p(p_i) = \left(\frac{p_i}{p}\right)$.

Demostración. La demostración de este lema puede consultarse en [23, Lema 4.4]. □

Teorema 3.3.8. *Sean* r *y* s *enteros tales que* r^2-4s *no es un cuadrado. Entonces el polinomio* $f(x) = x^4 + rx^2 + s$ *es reducible módulo* p *para todo primo* p, *si y sólo si* $s = t^2$, *para algún entero* t.

Demostración. Supongamos que $s = t^2$, $t \in \mathbb{Z}$ y que p es un primo impar.
Si $s \equiv 0$ mód p o $r^2 - 4s \equiv 0$ mód p, por la Observación 3.3.5 se tiene que $f(x)$ es reducible. Si $s \not\equiv 0$ mód p y $r^2 - 4s \not\equiv 0$ mód p, entonces $\left(\frac{s}{p}\right) = 1$, pues $s = t^2$, de modo que $f(x)$ es reducible, Teorema 3.3.6, incisos 2 y 3.
Veamos que ocurre con $p = 2$. Existen únicamente 4 polinomios en $\mathbb{F}_2[x]$ de la forma $f(x) = x^4 + rx^2 + s$, a saber x^4, $x^4 + 1$, $x^4 + x^2$, $x^4 + x^2 + 1$. Se tiene que $(x^4 + rx^2 + s) \equiv (x^2 + rx + s)^2$ mód 2, de modo que los polinomios planteados previamente son reducibles módulo 2.
Recíprocamente, supongamos que $f(x) = x^4 + rx^2 + s$ es reducible módulo p para todo primo p. Supongamos además que s no es un cuadrado.
Sea $m = m^2 p_1 p_2 \cdots p_k$ y $r^2 - 4s = n^2 q_1 q_2 \cdots q_l$. Para primos p y q, usando propiedades del símbolo de Legendre se tiene que

$$\left(\frac{s}{p}\right) = \left(\frac{p_1 p_2 \cdots p_k}{p}\right) = \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\cdots\left(\frac{p_k}{p}\right)$$

y

$$\left(\frac{r^2-4s}{q}\right) = \left(\frac{q_1 q_2 \cdots q_k}{q}\right) = \left(\frac{q_1}{q}\right)\left(\frac{q_2}{q}\right)\cdots\left(\frac{q_l}{q}\right).$$

Además, dado que s y $r^2 - 4s$ no son cuadrados, por el Teorema 4.2 de [23] existen infinitos primos p tales que

$$\left(\frac{s}{p}\right) = -1 \quad \text{y} \quad \left(\frac{r^2-4s}{q}\right) = -1.$$

Sean p_0 y q_0 números primos tales que cumplan las condiciones anteriores, respectivamente.
Sea $\Pi = \{p_1, p_2, \ldots, p_k, q_1, \ldots, q_l\}$ y $\epsilon : \Pi \to \{\pm 1\}$ definida como

$$\epsilon(x) = \begin{cases} \left(\dfrac{x}{p_0}\right) & \text{si} \quad x = p_i \quad \text{para algún} \quad i \in \{1, 2, \ldots k\} \\ \\ \left(\dfrac{x}{q_0}\right) & \text{si} \quad x = q_j \quad \text{para algún} \quad j \in \{1, 2, \ldots, l\} \end{cases}$$

Por el Lema 3.3.7 existen infinitos primos p tales que $X_p(x) = \epsilon(x)$ para todo $x \in \Pi$, donde $X_p(x) = \left(\dfrac{x}{p}\right)$. Sea w un número primo tal que $X_w(x) = \epsilon(x)$ para todo $x \in \Pi$, entonces $\left(\dfrac{q_j}{w}\right) = \left(\dfrac{q_j}{q_0}\right)$ para todo $j \in \{1, 2, \ldots, l\}$ y $\left(\dfrac{p_i}{w}\right) = \left(\dfrac{p_i}{p_0}\right)$ para todo $i \in \{1, 2, \ldots, k\}$, de modo que $\left(\dfrac{s}{w}\right) = \left(\dfrac{r^2 - 4s}{w}\right) = -1$. Por el Teorema 3.3.6, inciso 4, $f(x)$ es irreducible módulo w, lo cual es una contradicción pues $f(x)$ es reducible módulo p, para todo primo p. Luego, s es un cuadrado perfecto. □

Mostramos en seguida uno de los teoremas principales que se plantea en [5], el cual muestra condiciones necesarias y suficientes para que un polinomio de la forma $x^4 + rx^2 + s$ sea irreducible en $\mathbb{Z}[x]$ pero reducible módulo p para cualquier primo p. La demostración se obtiene usando los Teoremas 3.3.1 y 3.3.8, y los Colorarios 3.3.2 y 3.3.3.

Teorema 3.3.9. *Sea $f(x) = x^4 + rx^2 + s \in \mathbb{Z}[x]$. Entonces $f(x)$ es irreducible en $\mathbb{Z}[x]$ pero reducible módulo p para todo primo p, si y sólo si s es un cuadrado y $r^2 - 4s$, $2\sqrt{s} - r$ y $-2\sqrt{s} - r$ no son cuadrados.*

Ejemplo 6. Sea $n \in \mathbb{Z}$, que no es un cuadrado. Si $n \neq -3^m q$, $\text{mcd}(3, q) = 1$ y m impar, entonces $f(x) = x^4 + nx^2 + n^2$ es irreducible en $\mathbb{Z}[x]$ pero reducible módulo p para todo primo p, pues $s = n^2$ y $r^2 - 4s = -3n^2$, $2\sqrt{s} - r = n$ y $-2\sqrt{s} - r = -3n$ no son cuadrados.

En lo que sigue analizaremos polinomios $x^{2^n} + rx^{2^{n-1}} + s$, con $n = 3$. El primer resultado es un criterio de irreducibilidad. En la demostración del teorema usaremos teoría del polígono de Newton.

Teorema 3.3.10. *Sean $f(x) = x^8 + rx^4 + s \in \mathbb{Z}[x]$, $r = p_1^{e_1} \cdots p_l^{e_l}$ y $s = p_1^{a_1} \cdots p_l^{a_l}$, con p_i primo y $e_i, a_i \in \mathbb{Z}$ para todo $i \in \{1, \ldots l\}$. Supongamos que existe $i \in \{1, \ldots l\}$ tal que $a_i \leq 2e_i$ y $a_i \not\equiv 0$ mód 2, entonces $f(x)$ es irreducible.*

Demostración. Sean p_i el primo para el cual a_i cumple la hipótesis y v la valuación p_i-ádica. El polígono de Newton, con valuación v, de $f(x)$, es la envolvente convexa inferior de los puntos $(0, 0), (4, e_i), (8, a_i)$. Puesto que $a_i \leq 2e_i$, entonces $\dfrac{a_i}{8} \leq \dfrac{e_i}{4}$,

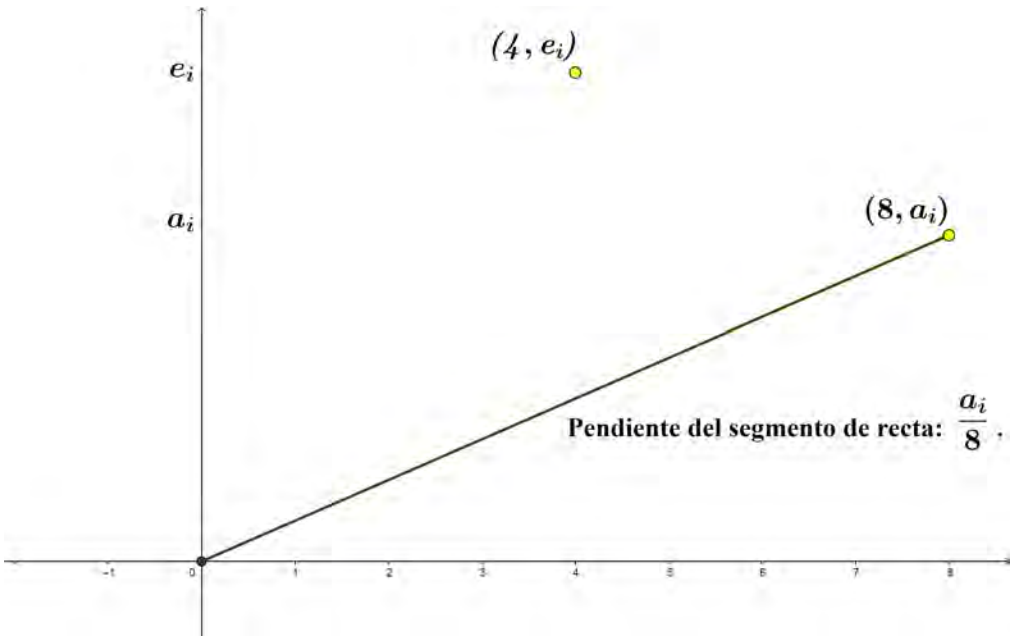


Figura 3.7: Polígono de Newton de $x^8 + rx^4 + s$.

de modo que el polígono de Newton de $f(x)$ es un segmento de recta, como se muestra en la Figura 3.7.
Si $f(x)$ es reducible, existen solamente tres posibles factorizaciones para $f(x)$ en $\mathbb{Z}[x]$: como producto de dos polinomios, uno de grado 6 y otro de grado 2; como producto de dos polinomios de grado 4; y como producto de un polinomio de grado 3 y uno de grado 5. Si $f(x)$ tuviese un factor lineal, digamos $x - m$, entonces $x + m$ también lo es, pues por la forma de $f(x)$ si m es raíz $-m$ también es raíz.
Supongamos que

$$f(x) = (x^2 + b_1x + b_2)(x^6 + d_1x^5 + d_2x^4 + d_3x^3 + d_4x^2 + d_5x + d_6),$$

con $b_j = q_j p_i^{\beta_j}, d_k = t_k p_i^{\alpha_k}, q_j, \beta_j, t_k, \alpha_k \in \mathbb{Z}$ para todo $j \in \{1, 2\}$ y $k \in \{1, 2, 3, 4, 5, 6\}$. Puesto que el polígono de Newton de un producto es la concatenación de los polígonos de los factores y dado que el polígono de Newton de $f(x)$ consiste de un segmento de recta, entonces los polígonos de $x^2 + b_1x + b_2$ y $x^6 + d_1x^5 + d_2x^4 + d_3x^3 + d_4x^2 + d_5x + d_6$ consisten de un segmento de recta, como se muestra en las Figuras 3.8 y 3.9, pág. 61.
De lo anterior obtenemos que $\frac{\beta_2}{2} = \frac{\alpha_6}{6} = \frac{a_i}{8}$, de modo que $\beta_2 = \frac{a_i}{4}$ y $\alpha_6 = \frac{3}{4}a_i$, lo cual contradice la elección de $\beta_2, \alpha_6 \in \mathbb{Z}$, pues $a_i \not\equiv 0$ mód 4.
Ahora supongamos que

$$f(x) = (x^4 + b_1x^3 + b_2x^2 + b_3x + b_4)(x^4 + d_1x^3 + d_2x^2 + d_3x + d_4),$$

con $b_j = q_j p_i^{\beta_j}, d_j = t_j p_i^{\alpha_j}$, $q_j, \beta_j, t_j, \alpha_j \in \mathbb{Z}$ para todo $j \in \{1, 2, 3, 4\}$, de manera análoga al caso anterior concluimos que los polígonos de los factores de $f(x)$

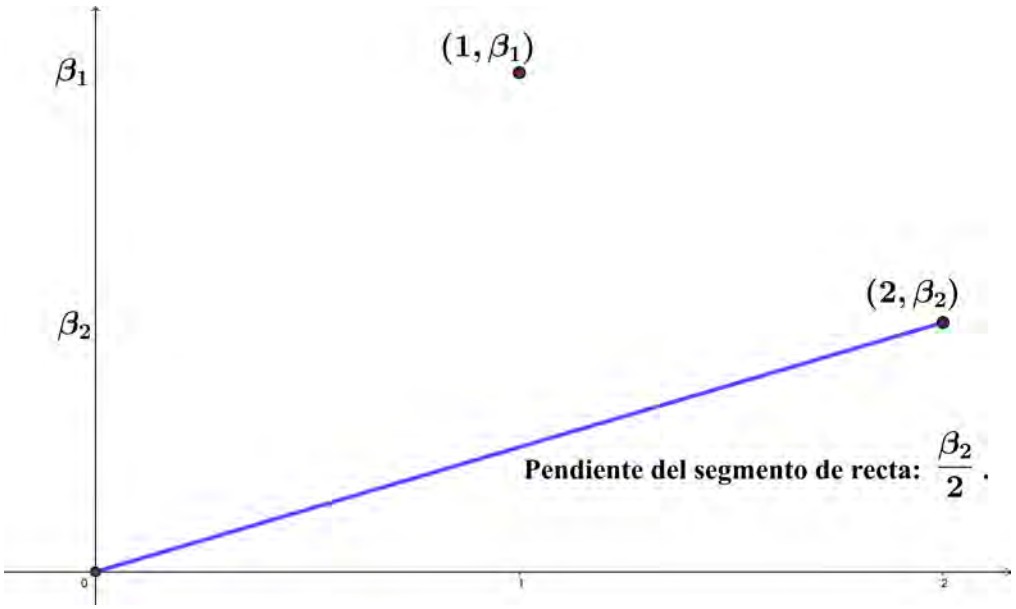


Figura 3.8: Polígono de Newton de $x^2 + b_1x + b_2$.

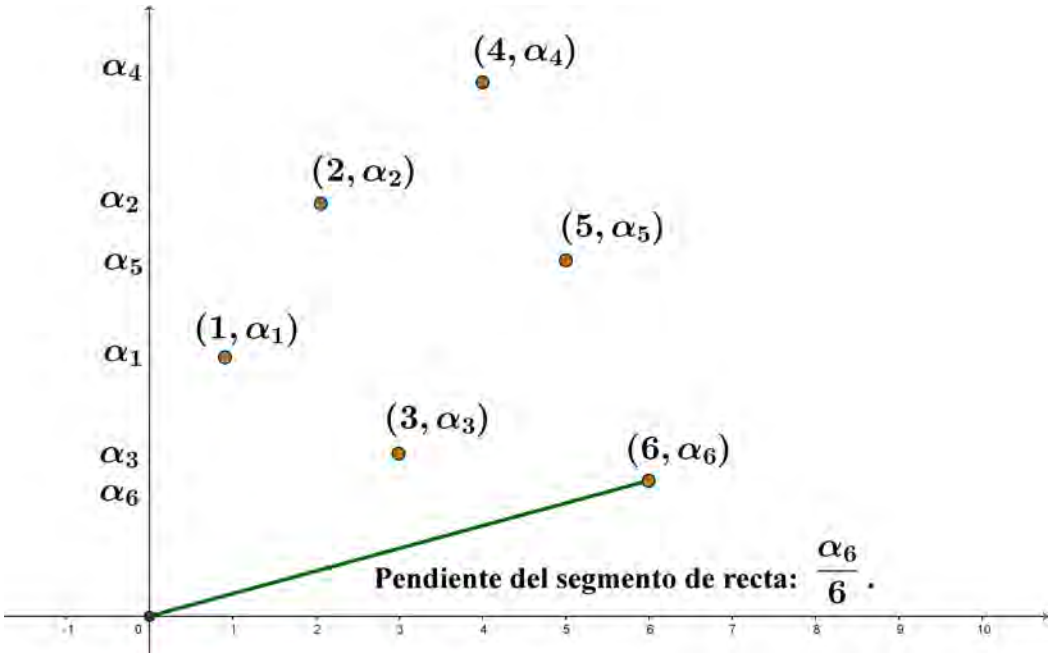


Figura 3.9: Polígono de Newton de $x^6 + d_1x^5 + d_2x^4 + d_3x^3 + d_4x^2 + d_5x + d_6$.

consisten de un segmento de recta, Figuras 3.10 y 3.11, pág. 62, de modo que $\frac{\alpha_4}{4} = \frac{\beta_4}{4} = \frac{a_i}{8}$, por lo tanto $\alpha_4 = \frac{a_i}{2}$ y $\beta_4 = \frac{a_i}{2}$, lo cual contradice la elección de $\alpha_4, \beta_4 \in \mathbb{Z}$, pues $a_i \not\equiv 0$ mód 2.
Similarmente, si suponemos que

$$f(x) = (x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5)(x^3 + d_1x^2 + d_2x + d_3),$$

con $b_j = q_j p_i^{\beta_j}, d_k = t_k p_i^{\alpha_k}$, $q_j, \beta_j, t_k, \alpha_k \in \mathbb{Z}$ para todo $j \in \{1, 2, 3, 4, 5\}$ y $k \in$

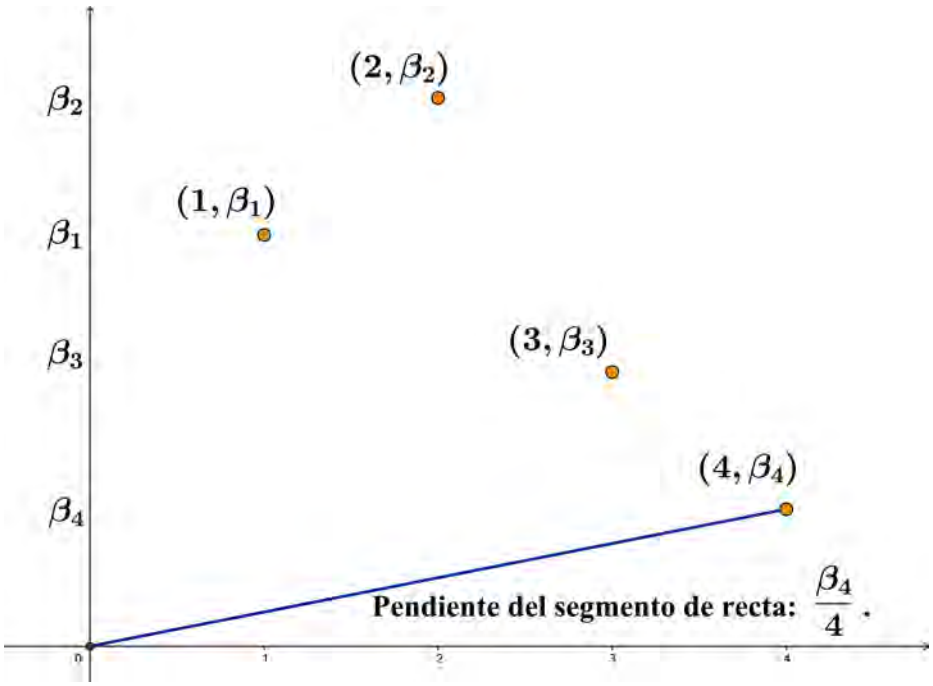


Figura 3.10: Polígono de Newton de $x^4 + b_1x^3 + b_2x^2 + b_3x + b_4$.

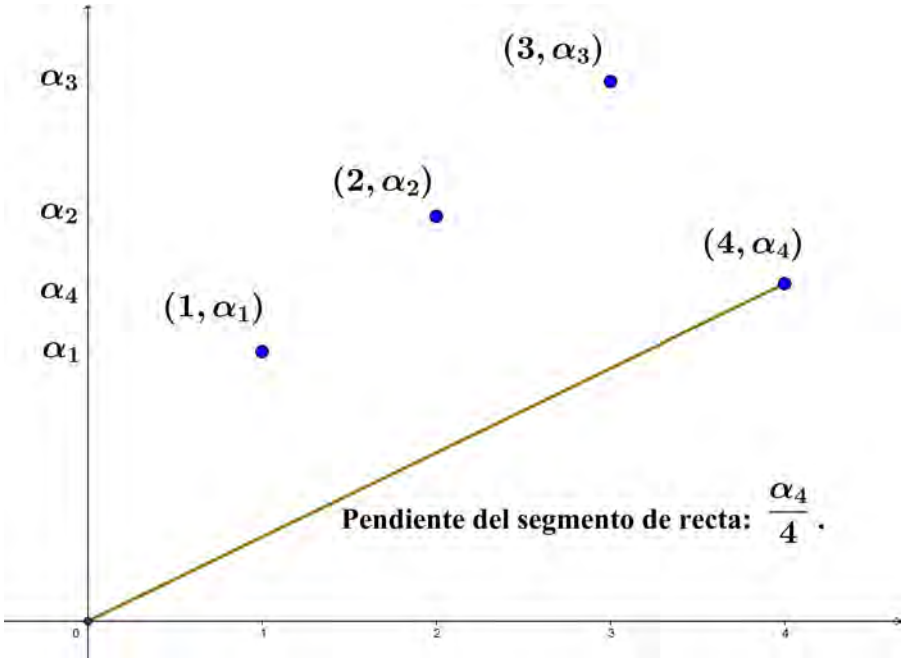


Figura 3.11: Polígono de Newton de $x^4 + d_1x^3 + d_2x^2 + d_3x + d_4$.

$\{1, 2, 3\}$, entonces los polígonos de Newton de $x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$ y $x^3 + d_1x^2 + d_2x + d_3$ consisten de un segmento, Figuras 3.12 y 3.13, pág. 63, de modo que $\frac{\beta_5}{5} = \frac{a_i}{8}$ y $\frac{\alpha_3}{3} = \frac{a_i}{8}$, así pues $\alpha_3 = \frac{3}{8}a_i$ y $\beta_5 = \frac{5}{8}a_i$, lo cual contradice la elección de $\alpha_3, \beta_5 \in \mathbb{Z}$, pues $a_i \not\equiv 0$ mód 2.
Por lo tanto, $f(x) = x^8 + rx^4 + s$ es irreducible en $\mathbb{Z}[x]$. □

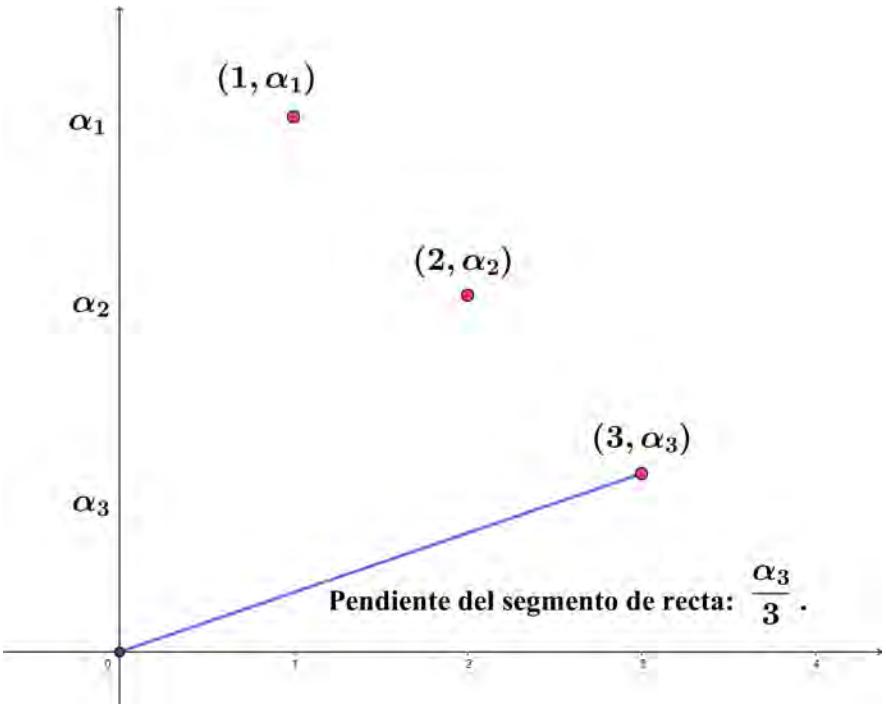


Figura 3.12: Polígono de Newton de $x^3 + d_1x^2 + d_2x + d_3$.

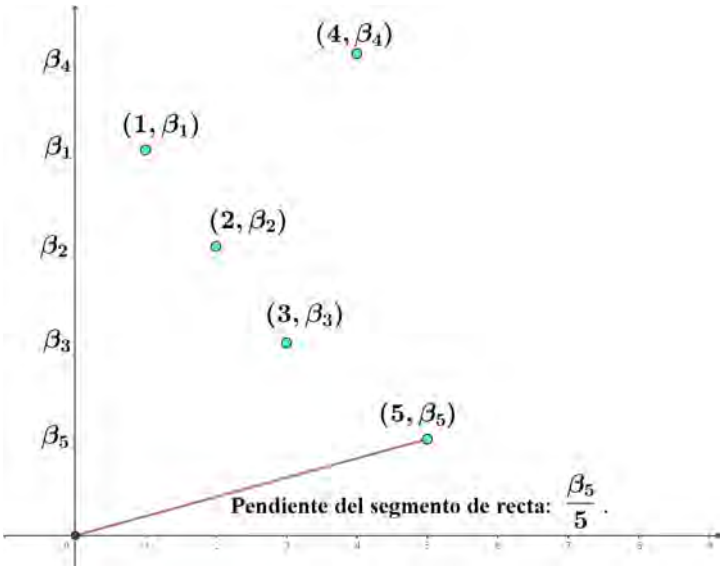


Figura 3.13: Polígono de Newton de $x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$.

Del Teorema 3.3.1 obtenemos el siguiente corolario:

Corolario 3.3.11. *Las siguientes condiciones son equivalentes:*

1. $f(x) = x^8 + rx^2 + s \in \mathbb{Z}[x]$ *se factoriza como producto de dos polinomios de la forma* $x^4 + \alpha x^2 + \beta \in Z[x]$,

2. $x^4 + rx^2 + s$ *es reducible en* $\mathbb{Z}[x]$,

3. *existen* $a, c, e \in \mathbb{Z}$ *tales que*

   a) $c + e - a^2 = r$,

   b) $ce = s$,

   c) $a(e - c) = 0$.

Tomando un cambio de variable $y = x^2$ en $f(x) = x^8 + rx^4 + s$, obtenemos y^4+ry^2+s, de modo que, si y^4+ry^2+s es reducible en $\mathbb{Z}[y]$, digamos $y^4+ry^2+s = q_1(y)q_2(y)$, entonces $f(x) = x^8+rx^2+s = q_1(x^2)q_2(x^2)$, es decir, $f(x)$ es reducible. Veamos qué ocurre cuando $y^4 + ry^2 + s$ es irreducible.

Proposición 3.3.12. *Sean* $f(x), g(x) \in K[x]$*, con* $deg(f) = n$ *y* $f(x)$ *irreducible. Entonces el grado de cada factor irreducible de* $(f \circ g)(x)$ *es divisible por* n*.*

Demostración. Sean $h(x) \in K[x]$ un factor irreducible de $(f \circ g)(x)$ y β una raíz de $h(x)$.
Sea $\alpha = g(\beta)$, puesto que $h(\beta) = 0$ entonces

$$(f \circ g)(\beta) = f(g(\beta)) = f(\alpha) = 0,$$

de manera que α es raíz de $f(x)$.
Dado que $\alpha = g(\beta) \in K(\beta)$ y $[K(\alpha) : K] = n$, pues, por hipótesis, $f(x)$ es irreducible se tiene

$$\deg(h) = [K(\beta) : K] = [K(\beta) : K(\alpha)][K(\alpha) : K] = [K(\beta) : K(\alpha)] \cdot n.$$

□

Usando la proposición anterior se tiene el siguiente corolario.

Corolario 3.3.13. *Sea* $f(x) = x^8 + rx^4 + s \in \mathbb{Z}[x]$*. Si* $x^4 + rx^2 + s$ *es irreducible en* $\mathbb{Z}[x]$*, entonces* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$ *o se factoriza como producto de dos polinomios irreducibles de grado* 4*.*

El Teorema 3.3.10 puede extenderse a polinomios de la forma $x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$, con $n > 3$, como se muestra a continuación:

Teorema 3.3.14. *Sea* $f(x) = x^{2^n} + rx^{2^{n-1}} + s$*,* $r = p_1^{e_1} \cdots p_l^{e_l}$*,* $n > 3$*, y* $s = p_1^{a_1} \cdots p_l^{a_l}$*, con* p_i *primo y* $e_i, a_i \in \mathbb{Z}$ *para todo* $i \in \{1, \ldots, l\}$*. Supongamos que existe* $i \in \{1, \ldots l\}$ *tal que* $a_i \leq 2e_i$ *y* $a_i \not\equiv 0$ *mód* 2*, entonces* $f(x)$ *es irreducible.*

Demostración. Sea i que satisface las condiciones del teorema. Si $f(x)$ se pudiese factorizar tendría dos factores de grados $2^{n-1} + j$ y $2^{n-1} - j$, para algún $j = 0, \ldots, 2^{n-1} - 1$. Dado que $a_i \leq 2e_i$, el polígono de Newton de $f(x)$ consiste de un segmento, con pendiente igual a $\dfrac{a_i}{2^n}$, además si suponemos

$$f(x) = (x^{2^{n-1}+j}+b_1x^{2^{n-1}+j-1}+\cdots+b_{2^{n-1}+j-1})(x^{2^{n-1}-j}+d_1x^{2^{n-1}+j-1}+\cdots+d_{2^{n-1}-j-1}),$$

donde $b_r = p_i^{\beta_r} q_r$, $a_k = p_i^{\alpha_k} t_k$, $p_i \nmid q_r t_k$, $\beta_r, \alpha_k, q_r, t_k \in \mathbb{Z}$ entonces los polígonos de los factores consisten también de un segmento, con pendientes

$$\frac{\beta_{2^{n-1}+j}}{2^{n-1}+j} \quad y \quad \frac{\alpha_{2^{n-1}-j}}{2^{n-1}-j}.$$

De modo que

$$\frac{a_i}{2^n} = \frac{\beta_{2^{n-1}+j}}{2^{n-1}+j} = \frac{\alpha_{2^{n-1}-ij}}{2^{n-1}-j}.$$

Así pues

$$\beta_{2^{n-1}+j} = \frac{a_i(2^{n-1}+j)}{2^n}, \quad \alpha_{2^{n-1}-j} = \frac{a_i(2^{n-1}-j)}{2^n}.$$

Dado que $\beta_{2^{n-1}+j}, \alpha_{2^{n-1}-j} \in \mathbb{Z}$ y $a_i \not\equiv 0$ mód 2, entonces

$$2^n \mid (2^{n-1}-j) \quad y \quad 2^n \mid (2^{n-1}+j),$$

esto no tienen lugar ya que

$$2^{n-1} - j < 2^n \;\; y \;\; 2^{n-1} + j < 2^{n-1} + 2^{n-1} - 1 = 2^n - 1 < 2^n.$$

Por lo tanto $f(x)$ es irreducible. □

Sea $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$ y $y = x^{2^{n-k}}$, haciendo un cambio de variable en $f(x)$ se tiene $y^{2^k} + ry^{2^{k-1}} + s$, de modo que, si $y^{2^k} + ry^{2^{k-1}} + s$ es reducible para algún $1 \leq k \leq n$, entonces $f(x)$ también es reducible. En consecuencia, se tiene el siguiente corolario:

Corolario 3.3.15. *Si $f(x)$ es irreducible, necesariamente $x^{2^k} + rx^{2^{k-1}} + s$ es irreducible para toda $1 \leq k \leq n$.*

Ahora supongamos que $x^{2^k} + rx^{2^{k-1}} + s$ es irreducible para toda $1 \leq k \leq n-1$, entonces por la Proposición 3.3.12 cada factor irreducible de $f(x)$ es divisible por 2^k, para toda $1 \leq k \leq n-1$, de manera que si $h(x)$ es un factor propio irreducible de $f(x)$, entonces $\deg(h) = 2^{n-1}$ y, consecuentemente, de ser $f(x)$ reducible en $\mathbb{Z}[x]$ este se factoriza como producto de dos polinomios de grado 2^{n-1}.
Usando la Proposición 3.3.12 y, planteando el Corolario 3.3.13 a polinomios $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$, obtenemos lo siguiente:

Corolario 3.3.16. *Si $x^{2^{n-1}} + rx^{2^{n-2}} + s$ es irreducible en $\mathbb{Z}[x]$, entonces $f(x)$ es irreducible en $\mathbb{Z}[x]$ o es producto de dos polinomios irreducibles de grado 2^{n-1}.*

3.4. Observaciones y conclusiones finales

En ese trabajo presentamos un pequeño recuento de algunos criterios de irreducibilidad para polinomios en una indeterminada.
Así mismo, estudiamos al polígono de Newton y sus propiedades elementales. Justificamos que el polígono de un polinomio es la concatenación de los polígonos de sus factores. Para esto iniciamos presentando un caso especial, del cual retomando las ideas justificamos un caso más general.

Con la finalidad de abordar a la familia de polinomios de la forma $f(x) = x^{2^n} + rx^{2^{n-1}} + s \in \mathbb{Z}[x]$, presentamos los resultados que se exponen en [5], en donde se muestran condiciones bajo las cuales $f(x)$, con $n = 2$, es irreducible en $\mathbb{Z}[x]$ pero reducible módulo p, para todo primo p. Cuando $n > 2$, pudimos establecer un criterio de irreducibilidad, para ello utilizamos propiedades del polígono de Newton. Por cuestiones de tiempo ya no fué posible abordar completamente el problema de encontrar condiciones para que los polinomios que se construyen con dicho criterio sean reducibles módulo p para cualquier primo p.
Pudimos concluir que si $f(x)$ es irreducible, necesariamente $x^{2^k} + rx^{2^{k-1}} + s$ es irreducible para toda $1 < k < n$, sin embargo, no obtuvimos el resultado general del recíproco.
Finalmente, una idea interesante que ya no fue posible abordar, por cuestiones de tiempo, es la generalización de lo que se probó para 2, más precisamente, estudiar los polinomios $f(x) = x^{p^n} + rx^{p^{n-1}} + s \in \mathbb{Z}[x]$, donde p es número primo impar.

Bibliografía

[1] F. Barrera Mora, *Notas de anillos, módulos, campos y teoría de Galois*, no publicado, 2015.

[2] F. Barrera Mora, *Notas de campos numéricos*, no publicado, revisado en 2016.

[3] N. Bonciocat, Y. Bugeaud, M. Cipe and M. Mignotte, *Some Pólya- Type Irreducibility Criteria for Multivariate Polynomials*, Communications in Algebra, 10(2005), 3733-3744.

[4] H. L. Dorwart y W. College, *Irreducibility of polynomials*, The American Mathematical Monthly, 42(1935), 369-381.

[5] E. Driver, P. A. Leonard and K. S. Williams, *Irreducible quartic polynomials with factorizations modulo p*, The American Mathematical Monthly, 10(2005), 876-890.

[6] J. Dugundji, *Topology*, Allyn and Bacon, Inc, USA, 1976.

[7] K. Iwasawa, *Local Class Field Theory*, Oxford University Press, New York, 1986.

[8] G. J. Janusz, *Algebraic number theory*, Academic Press, Inc, New York, 1973.

[9] A. Jorza, *Newton Polygons and Factoring polynomials over Local Fields*, https://www3.nd.edu/ ajorza/notes/newton_polygons.pdf.

[10] L. C. Kappe and B. Warren, *An Elementary Test for the Galois of a Quartic Polynomial*, The American Mathematical Monthly, 2(1986), 133-137.

[11] I. Kaplansky, *Fields and Rings*, The University of Chicago Press, USA, 1972.

[12] N. Koblitz, *p-ádic Numbers, p-ádic Analysis, and Zeta Functions*, Springer-Verlag, New York, 1984.

[13] E. Kreyszig, *Introductory Functional Analysis with Applications*, Wiley, United States, 1989.

[14] M. A. Lee, *Some irreducible polynomials which are reducible mod p for all p*, The American Mathematical Monthly, 10(1969), 1125.

[15] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand, 8(1960), 65-70.

[16] J. S. Milne, *Algebraic number theory*, http://www.jmilne.org/math/CourseNotes/ANT.pdf, págs. 125-126.

[17] M. Ram Murty, *Prime numbers and Irreducible polynomials*, The American Mathematical Monthly, 5(2002), 452-458.

[18] E. Selmer, *On the irreducibility of certain trinomials*, Math. Scand, 4(1956), 287-302.

[19] J. P. Serre, *Local Fields*, Springer-Verlag New York Inc. 1979.

[20] A. Schinzel, *Polynomials with Especial Regard to Reducibility*, Cambridge University Press, 2000.

[21] D. Stefanescu, *On the factorization of polynomials over discrete valuation domains*, Analele Stiintifice ale Universitatii Ovidius Constanta, Seria Matematica, 1(2014), 273-280.

[22] B. L. van der Waerden, *Algebra I*, Springer- Verlag, New York, 1964.

[23] S. Wright, *Quadratic Residues and Non-residues*, Springer, Michigan, U.S.A., 2016.