Extensiones de cuerpos sobre el cuerpo de los números *p*-ádicos

Vianey Landinez Garcia

Trabajo de Grado para optar al título de Matemática

Directora

Adriana Alexandra Albarracín Mantilla

Doctora en Matemáticas

Universidad Industrial de Santander

Facultad de Ciencias

Escuela de Matemáticas

Bucaramanga

2023

Dedicatoria

Dedico este trabajo a Dios y al regalo más grande que me entregó, mi hija Ailyn Valeria, la persona más importante en mi vida, la que me dio más fuerzas, motivos para luchar y salir adelante.

Por ella y para ella todo mi esfuerzo y dedicación.

Agradecimientos

Agradezco a Dios primeramente, a mi hija como fuente de inspiración, a mi novio que siempre me apoyó en todo momento, a mis profesores y a mi familia. También agradezco a mis amigos y compañeros por las vivencias de estos inolvidables años de universidad.

Un reconocimiento y agradecimiento importante lo realizo a mi directora de trabajo de grado, por dedicar su tiempo, experiencia y conocimiento en la guía de mi proyecto.

Tabla de Contenido

Resumen

Título: Extensiones de cuerpos sobre el cuerpo de los números p-ádicos [*]

Autor: Vianey Landinez Garcia [**]

Palabras Clave: Extensiones de cuerpos, Polinomio mínimo, Grado de la extensión, Números p-ádicos, Lema de Hensel, Extensiones p-ádicas.

Descripción: Dado F un cuerpo y $p(x)$ un polinomio no constante en $F[x]$. Es posible encontrar una extensión de cuerpos de F que contiene todas las raíces de $p(x)$, llamado el cuerpo de descomposición de $p(x)$. En el caso $F = \mathbb{Q}_p$ con p-primo, el cuerpo de los números p-ádicos forman una extensión de cuerpos de los números racionales descritos por primera vez en 1897, por Kurt Hensel un matemático alemán. Dado que $\mathbb{Q}_p$ no es algebraicamente cerrado es necesario el Lema de Hensel, un resultado fundamental que proporciona un método para construir raíces aproximadas de un polinomio.

En este proyecto consta tres secciones, la primera parte se hará un breve resumen de la teoría de las extensiones de cuerpos, la segunda se ilustra la construcción del cuerpo de los números p-ádicos y las propiedades necesarias para describir el lema de Hensel y el lema de Newton, que permitirá resolver ecuaciones sobre $\mathbb{Q}_p$ y la tercera que muestra algunas propiedades de las extensiones p-ádicas.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. EEscuela de Matemáticas. Directora: Adriana Alexandra Albarracín Mantilla, Doctora en Matemáticas.

Abstract

Title: Fields extensions on the field of p-adic numbers [*]

Author: Vianey Landinez Garcia [**]

Keywords: Fields extensions, minimal polynomial, Degree of the extension, p-adics numbers, Hensel's lemma, p-adics extensions.

Description: Let F a field and $p(x)$ a not constant polynomial in $F[x]$. It is possible to find a fields extension of F that contains all the roots of $p(x)$, called the decomposition field of $p(x)$. In the case $F = \mathbb{Q}_p$ with p-prime, the field of the p-adic numbers form a fields extension of the rational numbers first described in 1897, by Kurt Hensel a German mathematician. Since $\mathbb{Q}_p$ is not algebraically closed, Hensel's Lemma is necessary, a fundamental result that provides a method for constructing approximate roots of a polynomial. This project consists of three sections, the first part will provide a brief summary of the theory of fields extensions, the second illustrates the construction of the field of p-adic numbers and the properties necessary to describe Hensel's lemma and Newton's lemma, which will allow solving equations on $\mathbb{Q}_p$ and the third shows some properties of p-adic extensions.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Directora: Adriana Alexandra Albarracín Mantilla, Doctora en Matemática.

Introducción

Los cuerpos finitos han sido estudiados desde siglos atrás por diferentes matemáticos, en particular por Evariste Galois, fue a partir de sus estudios, que se llegó a comprender que la solubilidad de una ecuación polinomial "por radicales" estaba ligada a la naturaleza del grupo de permutaciones de las raíces de la ecuación. Alrededor de 1940, Artin y otros matemáticos cambiaron el enfoque al estudio de las extensiones de cuerpos: al cuerpo base que incluye los coeficientes del polinomio $p(x)$ se le adjuntan las raíces de la ecuación $p(x) = 0$, (Maldonado, 2015). El teorema principal que une los dos conceptos, el de grupo de permutaciones y el de extensión de cuerpo, establece una correspondencia de Galois entre los subgrupos del grupo de permutaciones y los cuerpos intermedios de la extensión, (Leinster, 2022).

Dado F un cuerpo y $p(x)$ un polinomio no constante en $F[x]$. Es posible encontrar una extensión de cuerpos de F que contiene todas las raíces de $p(x)$, llamado el cuerpo de descomposición de $p(x)$, (Jara, 2018). Estos resultados tienen diferentes aplicaciones en campos, de evidente interés para el mundo industrial y financiero, entre otros, como son la criptografía o los códigos correctores de errores,(Huguet, 2013). En el caso $F = \mathbb{Q}_p$ con p-primo, el cuerpo de los números p-ádicos forman una extensión de cuerpos de los números racionales descritos por primera vez en 1897 por el matemático alemán Kurt Hensel, que vivió entre 1861 y 1941, reconocido principalmente por su trabajo en teoría de números y álgebra,(López, 2019). Hensel investigaba en su artículo sobre las analogías entre las estructuras de $\mathbb{Z}$ y su cuerpo de fracciones $\mathbb{Q}$, con las del

anillo de polinomios $\mathbb{C}[x]$ y su cuerpo de fracciones $\mathbb{C}(x)$, (Monsalve, 2018). $\mathbb{Q}_p$ tiene la propiedad de que es un cuerpo completo con la norma p-ádica, esto nos permite el desarrollo del análisis p-ádico, análogo al análisis real.(Albarracín, 2022)

Dado que $\mathbb{Q}_p$ no es algebraicamente cerrado es necesario el Lema de Hensel, un resultado fundamental que proporciona un método para construir raíces aproximadas de un polinomio. Este proyecto de grado consta de tres secciones, la primera donde se mostrará un breve resumen de la teoría de las extensiones de cuerpos, con ejemplos y las demostraciones de algunos resultados, y la segunda se ilustra la construcción del cuerpo de los números p-ádicos y las propiedades necesarias para describir el lema de Hensel y el lema de Newton (Echevarría, 2016), que permitirá resolver ecuaciones sobre $\mathbb{Q}_p$ y la tercera que muestra algunas propiedades de las extensiones p-ádicas y ejemplos ilustrativos para hacer más fácil su compresión. Este trabajo de tipo monográfico guiará al lector interesado en el tema de extensiones p-ádicas de cuerpos.

1. Preliminares

En este capítulo se mostrarán varios resultados relacionados con extensiones de cuerpos, casi todos sin demostración pero ilustrados con ejemplos que permitirán evidenciar dichos resultados. Esto con el fin de facilitar la comprensión del tercer capítulo que habla sobre extensiones p-ádicas, (Lezama, 2017).

1.1. Cuerpos

Definición 1.1.1. *Sea R un anillo con unitario $1 \in R$. Se dice que $r \in \mathbb{R}$ es una **unidad** si existe un elemento $s \in R$ tal que $r \cdot s = s \cdot r = 1$. El conjunto de unidades de R se denota por $\mathscr{U}(R)$ y es un grupo con respecto a la multiplicación.*

Ejemplo 1.1.1. *1. Las unidades de $\mathbb{Z}$ son 1 y -1.*

2. Las unidades de $\mathbb{Z}[i]$ son 1, -1, i y $-i$.

Lema 1.1.1. *Sea R un anillo unitario conmutativo, entonces $a \in \mathscr{U}(R)$ si y sólo si $(a) = R$; es decir, que el generado de a es R.*

Definición 1.1.2. *Un **cuerpo** es un anillo unitario conmutativo F tal que $\mathscr{U}(F) = F/\{0\}$. Se dice que un cuerpo es finito si tiene un número finito de elementos.*

Ejemplo 1.1.2. *1. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.*

2. $K = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ es un cuerpo.

El inverso multiplicativo de $a+b\sqrt{2}$ es $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. En efecto,

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in K.$$

De ahí que el inverso de $a+b\sqrt{2}$ está en K.

3. *Dado un dominio de entero, $\mathscr{D}$, (esto es, un anillo conmutativo con unidad tal que $ab = 0$ entonces $a = 0$ ó $b = 0$), el cuerpo de fracciones de $\mathscr{D}$ es el conjunto de expresiones de la forma r/s con $r,s \in \mathscr{D}$, $s \neq 0$, bajo la relación de equivalencia $r/s \sim t/u \Leftrightarrow ru = ts$.*

Definición 1.1.3. *Sea F un cuerpo. Un subcuerpo de F es un subconjunto no vacío $K \subseteq F$ tal que, con las operaciones de F, tiene estructura de cuerpo no trivial. Se llama* ***subcuerpo primo*** *de F a la intersección de todos los subcuerpos de F.*

Definición 1.1.4. *Sea F un cuerpo y suponga que existe $n \in \mathbb{Z}^+$ tal que $n \cdot 1 = 0$. Al menor entero con tal propiedad se le llama la característica del cuerpo.*

Ejemplo 1.1.3. 1. *$\mathbb{R}$ y $\mathbb{Q}$ tienen característica cero.*

2. *$\mathbb{F}_p$ tiene característica p.*

Se sigue que si F es un cuerpo. Entonces la característica de F es cero o un número primo p. En el primer caso el subcuerpo primo de F es isomorfo a $\mathbb{Q}$ y en el segundo, isomorfo a $\mathbb{F}_p$.

Demostración: Suponga que F tiene característica $p \neq 0$ y que no es un número primo, entonces

se puede factorizar como $p = p_1 \cdot p_2$, con $1 < p_1, p_2 < p$. Entonces

$$(p_1 \cdot 1)(p_2 \cdot 1) = (p_1 \cdot p_2) \cdot 1 = 0,$$

luego por ser F un cuerpo no contiene divisores de cero, así $p_1 \cdot 1 = 0$ o $p_2 \cdot 1 = 0$, que contradice que p es el menor entero positivo que cumple con dicha condición.

Para demostrar la otra parte del teorema, suponga que F tiene característica cero, por definición $n \cdot 1_F \neq 0$ para todo $n \geq 0$. Sea el homomorfismo $\varphi : \mathbb{Q} \to F$ definido por $m/n \mapsto (m \cdot 1_F)/(n \cdot 1_F)$ (que está bien definido pues $\phi : n \mapsto n \cdot 1_F$ es un homomorfismo). Ahora φ es inyectivo por lo tanto $im(\varphi) \cong \mathbb{Q}$. Pero $im(\varphi)$ es un subcuerpo de F, y ya que $\mathbb{Q}$ no tiene subcuerpos, este es el subcuerpo primo.

Ahora, suponga que la característica de F es $p > 0$, p: primo, el homomorfismo $\psi : \mathbb{Z} \to F$ tiene kernel (p), por definición. Por el primer teorema de isomorfismos de anillos $im(\psi) \cong \mathbb{Z}/(p) = \mathbb{F}_p$. Pero $im(\psi)$ es un subcuerpo de F, y ya que $\mathbb{F}_p$ no tiene subcuerpos, este es el subcuerpo primo. □

Como consecuencia se obtiene que:

Todo cuerpo finito tiene característica p, donde p es un número primo.

Teorema 1.1.1. *Un dominio euclídeo es un domino de ideales principales. Si R es un dominio de ideales principales y a ∈ R, entonces (a) es un ideal maximal si y sólo si a es un elemento primo.*

Dado que en el anillo de polinomios, cada polinomio es caracterizado por su grado, se tiene que:

Lema 1.1.2. *Si F es un cuerpo, $F[x]$ es un dominio euclídeo. Si $p(x)$ y $q(x) \in F[x]$ con $q(x) \neq 0$, entonces existen dos polinomios $c(x)$ y $r(x)$ tales que $p(x) = q(x)c(x) + r(x)$ con $gr(r(x)) < gr(q(x))$, donde gr es el grado del polinomio.*

Definición 1.1.5. *Sea F un cuerpo. La **clausura algebraica** de F es un cuerpo que contiene a F, tal que todo polinomio con coeficientes en F tiene todas sus raíces en el y que es minimal con esta propiedad.*

El siguiente teorema establece una conexión entre los cuerpos finitos y los enteros módulo p, este garantiza la existencia de cuerpos finitos.

Teorema 1.1.2. *Sea $F = \mathbb{F}_q$ un cuerpo finito con q elementos. Existe un primo p tal que F contiene al cuerpo $\mathbb{F}_p$ de los enteros módulo p.*

Caracterización de los cuerpos finitos Para todo primo p y todo número natural m existe un cuerpo finito con $q = p^m$ elementos. Tal cuerpo es único salvo isomorfismo.

1.2. Extensiones finitas

Definición 1.2.1. *Sean F y K dos cuerpos. Se dice que F es una extensión de K, si K es un subcuerpo de F, es decir $K \subseteq F$, en este caso se denota por F/K.*

Ejemplo 1.2.1. 1. *Los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ son extensiones de $\mathbb{Q}$.*

2. *El cuerpo $\mathbb{C}$ es una extensión de $\mathbb{R}$.*

3. *Sea K un cuerpo y $p(x) \in K[x]$ un polinomio irreducible. Entonces $F = K[x]/(p(x))$ es un cuerpo que contiene a K, así F/K es una extensión de cuerpos.*

Definición 1.2.2. *Sea F/K una extensión de cuerpos, se dice que F/K es **finitamente generada**, si existe un subconjunto $S \subseteq F$ finito tal que $F = K(S)$, es decir, es el menor subcuerpo que contiene a K y a S. Se dice que es **simple** si existe $u \in F$ tal que $F = K(u)$.*

Ejemplo 1.2.2.

1. *La extensión $\mathbb{C}/\mathbb{R}$ es una extensión simple dado que $\mathbb{C} = \mathbb{R}(i)$.*
2. *El cuerpo $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ es una extensión de $\mathbb{Q}$.*
3. *Sea K un cuerpo y $K(x) = \left\{ \dfrac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ g(x) \neq 0\ y\ x \in K \right\}$ el cuerpo de cocientes del anillo de polinomios de $K[x]$. Entonces $K(x)/K$ es una extensión simple.*

Definición 1.2.3. *Sea F una extensión de K. Se denomina grado de la extensión a la dimensión de F considerado como espacio vectorial sobre K, y se denota por $[F : K] = dim_K(F)$; la extensión es finita si su grado es finito.*

Ejemplo 1.2.3.

1. *$[\mathbb{C} : \mathbb{R}] = 2$, pues $\{1, i\}$ es una base de $\mathbb{C}$ como $\mathbb{R}-$espacio vectorial.*
2. *$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, ya que la base es $\{1, \sqrt{2}\}$.*

Lema 1.2.1. *Sea F un cuerpo y $p(x)$ un polinomio irreducible sobre F de grado n. Dado el cuerpo $F[x]/(p(x))$, entonces $1 + (p(x)), x + (p(x)), x^2 + (p(x)), \ldots, x^{n-1} + (p(x))$, es una $F-$base de $F[x]/(p(x))$ y $[F[x]/(p(x)) : F] = n$, donde n es el grado del polinomio.*

El siguiente teorema, permite calcular el grado de una extensión finita.

Teorema 1.2.1 (**Transitividad de índices**). *Sea F una extensión finita de E y E una extensión finita de K, entonces F es una extensión finita de K y además,*

$$[F : K] = [F : E][E : K]$$

.

Ejemplo 1.2.4. *1. Si F es una extensión de K, entonces $[F : K] = 1$ si, y sólo si, $F = K$.*

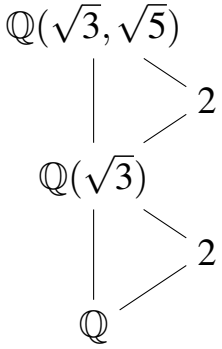
2. Sea $p(x) = x^4 - 8x^2 + 15 \in \mathbb{Q}[x]$, entonces

$$p(x) = (x^2 - 3)(x^2 - 5) = (x + \sqrt{3})(x - \sqrt{3})(x + \sqrt{5})(x - \sqrt{5}),$$

es reducible en $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ pero no sobre $\mathbb{Q}$. Por lo tanto, la extensión $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ tiene grado 4.

En efecto, dado que $\sqrt{3}$ es algebraico sobre $\mathbb{Q}$ con polinomio minimal $p(x) = x^2 - 3$, el grado de la extensión es $2 = gr(p(x))$. Al mismo tiempo, $\sqrt{5}$ es algebraico sobre $\mathbb{Q}(\sqrt{3})$ con polinomio minimal $q(x) = x^2 - 5$, de ahí que $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$.

$$[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2\cdot 2 = 4.$$



1.3. Extensiones algebraicas y trascendentes

En esta sección se clasificarán las extensiones de cuerpos en algebraicas (finitas) o trascendentes.

Definición 1.3.1. *Sea F/K una extensión de cuerpos. Se dice que un elemento $u \in F$ es algebraico sobre K si existe un polinomio no nulo $p(x) \in K[x]$ tal que $p(u) = 0$.*

*Si u no es algebraico sobre K, se dice que u es **trascendente** sobre K.*

Ejemplo 1.3.1.

1. *Considere la extensión $\mathbb{R}/\mathbb{Q}$. Se tiene entonces que tanto $\sqrt{2}$, $\sqrt[3]{2}$, como i son algebraicos sobre $\mathbb{Q}$, pues son ceros de los polinomios x^2-2, x^3-2 y x^2+1 respectivamente.*

2. *En la extensión $\mathbb{R}/\mathbb{Q}$ los números e y π son trascendentes sobre $\mathbb{Q}$, pues no existe un polinomio $p(x)$ con coeficientes en $\mathbb{Q}$ tal que $p(\pi) = 0 = p(e)$.*

3. *El número $\alpha = \sqrt{2+\sqrt{5}}$ es algebraico sobre $\mathbb{Q}$, pues $\alpha^2 = 2+\sqrt{5}$, o sea $\alpha^2 - 2 = \sqrt{5}$,*

$(\alpha^2-2)^2=5$, *y entonces* $\alpha^4-4\alpha^2-1=0$. *Por consiguiente* α *es raíz del polinomio* $p(x)=x^4-4x^2-1\in\mathbb{Q}[x]$.

El siguiente resultado caracteriza un polinomio irreducible.

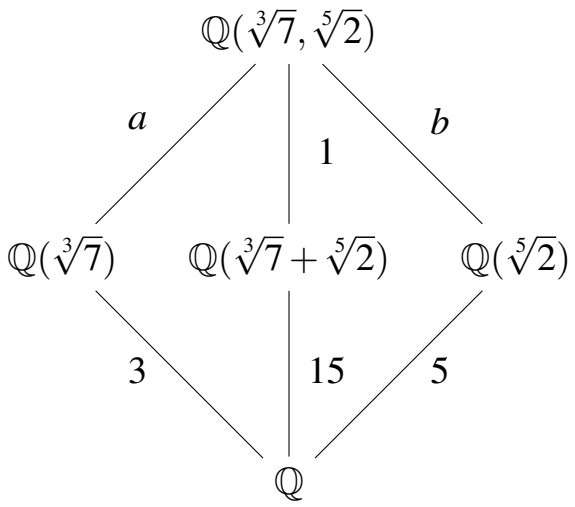
Teorema 1.3.1. *Sea F/K una extensión de cuerpos con $u\in F$ un elemento algebraico sobre K. Entones, existe un único polinomio mónico irreducible $p(x)\in K[x]$ tal que $p(u)=0$. Además, si $q(x)\in K[x]$ es tal que $q(u)=0$, entonces $p(x)$ divide a $q(x)$. Se denotará por* $\text{mín}(u,K)$ *y de denominará* ***polinomio mínimo****.*

Ejemplo 1.3.2. *1.* $\text{mín}(\sqrt{2},\mathbb{Q})=x^2-2$.

2. $\text{mín}(\sqrt[4]{2},\mathbb{Q}(\sqrt{2}))=x^2-\sqrt{2}$. *En general,* $\text{mín}(\sqrt[4]{u},\mathbb{Q}(\sqrt{u}))=x^2-\sqrt{u}$.

3. $\text{mín}(\sqrt{1+\sqrt{3}},\mathbb{Q})=x^4-2x^2-2$. *Dado que, tomando* $\alpha=\sqrt{1+\sqrt{3}}$, *entonces* $\alpha^2-1=\sqrt{3}$, *por lo tanto* $(\alpha^2-1)^2-3=\alpha^4-2\alpha^2-2=0$. *Así* α *es raíz del polinomio* x^4-2x^2-2 *que es irreducible en* $\mathbb{Q}$. *Usando el criterio de Eisenstein, para* $p=2$, *se tiene que* $p\mid -2$, *que* $p\nmid 1$ *y* $p^2\nmid -2$. *Por lo tanto* $p(x)$ *es irreducible sobre* $\mathbb{Q}$.

4. $\text{mín}(\sqrt[3]{7},\mathbb{Q}(\sqrt[5]{2}))$. *Observe el siguiente diagrama:*



Sea $[\mathbb{Q}(\sqrt[3]{7},\sqrt[5]{2}):\mathbb{Q}]=n$*, luego, tenemos que:*

$$\begin{aligned}[\mathbb{Q}(\sqrt[3]{7},\sqrt[5]{2}):\mathbb{Q}] &= [\mathbb{Q}(\sqrt[3]{7},\sqrt[5]{2}):\mathbb{Q}(\sqrt[3]{7})]\cdot[\mathbb{Q}(\sqrt[3]{7}):\mathbb{Q}]\\ n &= [\mathbb{Q}(\sqrt[3]{7},\sqrt[5]{2}):\mathbb{Q}(\sqrt[3]{7})]\cdot 3\\ n &= a\cdot 3,\end{aligned}$$

y

$$\begin{aligned}[\mathbb{Q}(\sqrt[3]{7},\sqrt[5]{2}):\mathbb{Q}] &= [\mathbb{Q}(\sqrt[3]{7},\sqrt[5]{2}):\mathbb{Q}(\sqrt[5]{2})]\cdot[\mathbb{Q}(\sqrt[5]{2}):\mathbb{Q}]\\ n &= b\cdot 5.\end{aligned}$$

Así entonces se tiene que $3\cdot a=5\cdot b$*, además* $3|b$ *y* $5|a$*. Tomando el polinomio* $p=x^3-7\in\mathbb{Q}(\sqrt[5]{2})[x]$ *donde* $\sqrt[3]{7}$ *es uno de sus ceros, se tiene que el grado del polinomio mínimo es menor o igual a* 3*, sin embargo, se sabe que* $3|b$ *por lo tanto* $b=3$ *y entonces* $a=5$*; así*

$n = 15$*, el grado del polinomio mínimo.*

El siguiente resultado es fundamental en la teoría de extensiones de cuerpos.

Teorema 1.3.2. *Sea F/K una extensión de cuerpos $u \in F$ un elemento algebraico sobre K. Entonces existe un isomorfismo de cuerpos $\phi : K(u) \to K[x]/(\text{mín}(u,K))$ tal que $\phi(u) = x + \text{mín}(u,K) = \bar{x}$, es decir:*

$$K(u) = K[u] \approx K[x]/(\text{mín}(u,K)).$$

Demostración. Sea φ el homomorfismo de evaluación definido por,

$$\varphi : K[x] \to K[u],$$

$$f(x) \mapsto f(u).$$

Dado que F/K es extensión y $u \in F$ es algebraico sobre K, existe $p(x) = \text{mín}(u,K) = x^n + x^{n-1}a_{n-1} + \cdots + xa_1 + a_0$, tal que $p(u) = 0$. Luego $u^n = -u^{n-1}a_{n-1} + \cdots + ua_1 + a_0$.

Además,

$$\ker(\varphi) = \{f \mid f \in K[x], f(u) = 0\} = (\text{mín}(u,K)).$$

Donde $\text{mín}(u,K)$ es el polinomio mónico irreducible que al evaluarlo en u se anula.

Usando el primer teorema de isomorfismo de anillos se tiene que

$$K[x]/(\ker(\varphi)) = K[x]/(\text{mín}(u,K)) \cong \text{Im}(\varphi) = K[u].$$

Puesto que mín(u,K) es irreducible y $K[x]$ es un anillo de ideales principales, se verifica que $(\text{mín}(u,K))$ es un ideal maximal de $K[x]$. En efecto, suponiendo que $(m(x)) \in K[x]$ es el ideal maximal, es decir, $(\text{mín}(u,K)) \subset (m(x))$ entonces mín$(u,K) \in (m(x))$, lo cual implica que mín$(u,K) = m(x) \cdot n(x)$ donde $n(x) \in K[x]$ es un polinomio de grado menor a mín(u,K), lo que contradice que mín(u,K) es el polinomio mínimo irreducible, en consecuencia $(m(x)) = K[x]$ o $(m(x)) = (\text{mín}(u,K))$.

Así, $K[x]/(\text{mín}(u,K))$ es un cuerpo. En consecuencia, $K[u]$ es un cuerpo y se tiene $K(u) = K[u]$.

Del resultado anterior se tiene la existencia de un isomorfismo de cuerpos $\phi : K(u) \to K[x]/(\text{mín}(u,K))$ tal que $\phi(u) = x + \text{mín}(u,K) = \overline{x}$. ϕ es un homomorfismo inyectivo y sobreyectivo, es decir, un monomorfismo y un epimorfismo. En efecto, sean $u_1, u_2 \in K(u)$, entonces $u_1 = P_1(u)$ y $u_2 = P_2(u)$ y $u_1 \cdot u_2 = P_3(u)$, con grado de P_j menor que el grado del mín(u,K). Así

$$\phi(u_1 + u_2) = \phi(P_1(u) + P_2(u)) = \overline{P_1(x)} + \overline{P_2(x)} = \phi(u_1) + \phi(u_2).$$

Note que, $P_1P_2 - P_3$ se anula en u, por lo tanto es divisible por mín(u,K) y su clase en $K[x]/(\text{mín}(u,K))$ es la clase cero. Por consiguiente

$$\phi(u_1)\phi(u_2) - \phi(u_1u_2) = \overline{P_1(x)P_2(x)} - \overline{P_3(x)} = \overline{0}.$$

Dado que ϕ aplica u en $\overline{x}$, que genera $K[x]/(\text{mín}(u,K))$, es un epimorfismo.

Además, $\phi(u_1) - \phi(u_2) = 0$, entonces $P_1 - P_2 \in \text{mín}(u,K)$ por lo tanto mín$(u,K) \mid P_1 - P_2$ y como

el grado de los P_j son menores que el del $K[x]/(\text{mín}(u,K))$, se tiene entonces que $P_1 = P_2$ y así ϕ es también un monomorfismo. □

Como consecuencia del Teorema 1.3.2 se tiene la relación entre elementos algebraicos y la finitud de la extensión.

Corolario 1.3.1. *Sea F/K una extensión de cuerpos y $u \in F$. Entonces u es algebraico sobre K si y sólo si $K(u)/K$ es una extensión finita.*

Además, si $n = gr(\text{mín}(u,K))$, entonces $\{1,u,\cdots,u^{n-1}\}$ es una K-base de $K(u)$ y $[K(u):K] = n$.

Ejemplo 1.3.3.

1. $\mathbb{Q}(\sqrt[4]{3}) \approx \mathbb{Q}[x]/(x^4-3)$. *En efecto, pues $\sqrt[4]{3}$ es algebraico sobre $\mathbb{Q}$ e* $\text{mín}(\sqrt[4]{3},\mathbb{Q}) = x^4-3$, *además,* $[\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}[x]] = 4$ *y por el Corolario 1.3.1,* $B = \{1,\sqrt[4]{3},\sqrt[4]{3^2},\sqrt[4]{3^3}\}$ *es una $\mathbb{Q}-$base de* $\mathbb{Q}(\sqrt[4]{3}) = \{a,b\sqrt[4]{3},c\sqrt[4]{3^2},d\sqrt[4]{3^3} : a,b,c,d \in \mathbb{Q}\}$.

2. *Sea $p(x) = x^2+x+1 \in \mathbb{Z}_2[x]$, dado que ni 1 ni 0 son raíces de $p(x)$, y $p(x)$ es irreducible en $\mathbb{Z}_2$,entonces existe un $\alpha \in F/\mathbb{Z}_2[x]$ tal que $p(\alpha) = 0$. Luego por el Corolario 1.3.1 se tiene que existe una base para F dada por:* $B = \{0\alpha, 1+0\alpha, 1\alpha, 1+1\alpha\}$.

3. $a = 2^{1/3}$ *es algebraico sobre $\mathbb{Q}$, ya que $p(a) = 0$, donde $p(x) = x^3-2$ es irreducible sobre $\mathbb{Q}$. Luego* $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}[x]] = 3$ *con* $B = \{1,\sqrt[3]{2},\sqrt[3]{2^2}\}$ *una base para* $\mathbb{Q}(\sqrt[3]{2})$ *sobre* $\mathbb{Q}$.

   Observe que $p(x) = x^3-2$ es irreducible sobre $\mathbb{Q}$, en efecto:

Sean $a,b,c,\alpha \in \mathbb{Q}$ *tales que*

$$\begin{aligned} x^3-2 =& (ax^2+bx+c)(x-\alpha), \\ =& ax^3-a\alpha x^2+bx^2-b\alpha x+cx-c\alpha, \\ =& ax^3+(-a\alpha+b)x^2+(-b\alpha+c)x-c\alpha. \end{aligned}$$

Se tiene $a=1$*, entonces* $-a\alpha+b=0$*,* $\alpha=1$ *lo que implica que* $b=\alpha$*. Se sigue que* $-b\alpha+c=0$*, así* $b^2=c$ *que no tiene solución en* $\mathbb{Q}$*.*

Teorema 1.3.3. *Sea* F/K *una extensión de cuerpos y* u *y* v *elementos algebraicos diferentes de cero. Entonces* $u+v$*,* uv*,* u^{-1} *también son elementos algebraicos.*

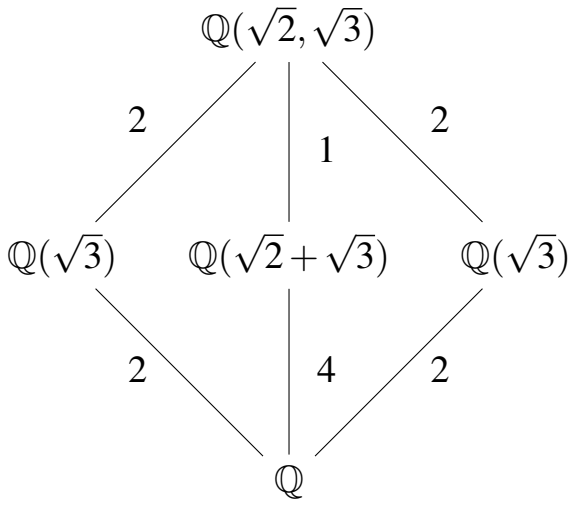
Como consecuencia se tiene la clausura algebraica como cuerpo intermedio.

Corolario 1.3.2. *Sea* F/K *una extensión de cuerpos. Entonces el conjunto* $E=\{u\in F|\quad u\quad$ *es algebraico sobre es un subcuerpo de* F *que contiene a* K*. (*E *se llama la clausura algebraica de* K *en* F*).*

Definición 1.3.2. *Sea* F/K *una extensión de cuerpos. Se dice que* F/K *es una extensión algebraica si todo elemento de* F *es algebraico sobre* K*. En caso contrario, se dice que la extensión es trascendente.*

Teorema 1.3.4. *Una extensión algebraica finitamente generada es finita.*

Ejemplo 1.3.4. *1. Comparando los cuerpos* $\mathbb{Q}(\sqrt{2},\sqrt{3})$*,* $\mathbb{Q}(\sqrt{2}+\sqrt{3})$*,* $(\mathbb{Q}\sqrt{2})$*,* $\mathbb{Q}(\sqrt{3})$ *y* $\mathbb{Q}$*, se puede observar la siguiente relación:*



donde los polinomios mímimos y las dimensiones de $\sqrt{2}$ *y* $\sqrt{3}$ *sobre* $\mathbb{Q}$ *son:*

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2, \quad x^2-2 \quad y \quad [\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2, \quad x^2-3.$$

Por lo tanto, $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2}\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$ *entonces del* ***teorema de transitividad de índices*** *se tiene que*

$$\begin{aligned}[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] &= [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}], \\ &= [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot 2.\end{aligned}$$

Dado que $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$*, donde* $B_1=\{1,\sqrt{3}\}$ *es una base para la extensión,*

entonces

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot 2,$$
$$= 2\cdot 2 = 4,$$

y la base es $B = \{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$*; por lo tanto el grado del polinomio mínimo de* $\sqrt{2}+\sqrt{3}$ *sobre* $\mathbb{Q}$ *es* 4.

Sea

$$P(x) = x^4 + ax^3 + bx^2 + cx + d, \tag{1}$$

tal polinomio mínimo.

Así $(\sqrt{2}+\sqrt{3})^4 + a(\sqrt{2}+\sqrt{3})^3 + b(\sqrt{2}+\sqrt{3})^2 + c(\sqrt{2}+\sqrt{3}) + d = 0.$

Desarrollando la ecuación se tiene que: $(\sqrt{2})^4 + 4(\sqrt{2})^3(\sqrt{3}) + 6(\sqrt{2})^2(\sqrt{3})^2 + 4(\sqrt{2})(\sqrt{3})^3 + (\sqrt{3})^4 + a(\sqrt{2})^3 + 3a(\sqrt{2})^2(\sqrt{3}) + 3a(\sqrt{2})(\sqrt{3})^2 + a(\sqrt{3})^3 + b(\sqrt{2})^2 + 2b(\sqrt{2})(\sqrt{3}) + b(\sqrt{3})^2 + c(\sqrt{2}) + c(\sqrt{3}) + d = 0.$

Así

$$4+8\sqrt{6}+36+12\sqrt{6}+9+2a\sqrt{2}+6a\sqrt{3}+9a\sqrt{2}+3a\sqrt{3}+2b+2b\sqrt{6}+3b+c\sqrt{2}+c\sqrt{3}+d=0.$$

Por lo tanto, se llega a la ecuación:

$2b\sqrt{6}+49+20\sqrt{6}+11a\sqrt{2}+9a\sqrt{3}+5b+c\sqrt{2}+c\sqrt{3}+d=0$, *que se puede ver como:*

$A+B\sqrt{2}+C\sqrt{3}+D\sqrt{6}=0$,

donde,

$$A=49+5b+d=0,$$

$$B=11a+c=0,$$

$$C=9a+c=0,$$

$$D=2b+20=0.$$

Así, de B y C se tiene que $a=c=0$, *y con D se tiene que* $b=-10$*; por lo tanto, de A se deduce que* $d=50-49=1$.

Reemplazando en (1)*, el polinomio mínimo es:*

$$P(x)=x^4-10x^2+1.$$

2. *Para hallar el grado de la extensión* $[\mathbb{Q}(\sqrt{1+\sqrt{3}}):\mathbb{Q}]$ *es necesario calcular el polinomio mínimo. Sea* $\alpha=\sqrt{1+\sqrt{3}}$ *entonces:*

$$\alpha^2=(\sqrt{1+\sqrt{3}})^2=1+\sqrt{3}, \qquad \alpha^2-1=\sqrt{3},$$

por tanto $(\alpha^2-1)^2=3$*, así* $\alpha^4-2\alpha^2-3=0$*. Así el polinomio mínimo es* $p(x)=x^4-2x^2-3$*, que además es irreducible en* $\mathbb{Q}$ *y por tanto el grado de la extensión es* 4.

3. *Dados* $(p_i)_{i=1}^3$*, tres números primos, se define* $K=\mathbb{Q}[\sqrt{p_1},\sqrt{p_2},\sqrt{p_3}]$*, y se tiene que:*

$$\mathbb{Q}\subset\mathbb{Q}[\sqrt{p_1}]\subset\mathbb{Q}[\sqrt{p_1},\sqrt{p_2}]\subset K=\mathbb{Q}[\sqrt{p_1},\sqrt{p_2},\sqrt{p_3}].$$

Denotando a $F_1=\mathbb{Q}[\sqrt{p_1}]$ *y a* $F_2=\mathbb{Q}[\sqrt{p_1},\sqrt{p_2}]$*, se tiene por el teorema de transitividad de índices que:*

$$\begin{aligned}[K:\mathbb{Q}] =& [K:F_2][F_2:F_1][F_1:\mathbb{Q}],\\ =& 2\cdot 2\cdot 2,\\ =& 8,\end{aligned}$$

donde $[F_1:\mathbb{Q}]=2$*,* $x^2-p_1=0$ *y la base es* $B_{F_1}=\{1,\sqrt{p_1}\}$ *y* $[F_2:\mathbb{Q}]=4$ *pues* $(x^2-p_1)(x^2-p_2)=0$*, así la base es* $B_{F_2}=\{1,\sqrt{p_1},\sqrt{p_2},\sqrt{p_1p_2}\}$ *por lo tanto* $[K:\mathbb{Q}]=2\cdot 4=8$ *como se quería mostrar.*

1.4. El cuerpo de descomposición

En la teoría de Galois, a cada extensión F/K se puede asociar el grupo de automorfismos de F que deja fijo el subcuerpo K; por otro lado, a cada grupo G de automorfismos de un cuerpo F se puede asociar el subcuerpo de elementos fijos de K mediante los automorfismos de G, (Belichón, 2008).

Definición 1.4.1. *Sea F/K una extensión de cuerpos y $p(x) \in K[x]$. Se dice que $p(x)$ se descompone sobre F, si $p(x)$ se factoriza como producto de polinomios lineales con coeficientes en F.*

Si $p(x) \in K[x]$ se descompone sobre F, entonces $p(x) = c(x-u_1)\cdots(x-u_n)$ con $0 \neq c \in K$ y $u_1, \ldots, u_n$ raíces de $p(x)$.

Definición 1.4.2. *Sea F/K una extensión de cuerpos y $p(x) \in K[x]$ un polinomio que se descompone sobre F. Se llama el cuerpo de descomposición de $p(x)$ en F sobre K, al menor subcuerpo de F que contiene a K y sobre el cual $p(x)$ se descompone.*

Si $p(x) \in K[x]$ se descompone sobre F y $u_1, \ldots, u_n$ son sus raíces, entonces el cuerpo de descomposición de $p(x)$ es $K(u_1, \ldots, u_n)$.

Ejemplo 1.4.1.

1. *$p(x) = x^2 - 2$. El cuerpo de descomposición de $p(x)$ en $\mathbb{C}$ es $\mathbb{Q}(\sqrt{2})$.*

2. *$p(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[X]$. El polinomio $p(x)$ es irreducible sobre $\mathbb{Q}$, dado que, las raíces de $p(x)$ son $\alpha = \sqrt{2+\sqrt{2}}$, $\beta = \sqrt{2-\sqrt{2}}$, $-\alpha$ y $-\beta$ están en $\mathbb{R}$; por lo tanto, el cuerpo de descomposición de $p(x)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha, \beta)$.*

   Además, dado que $\sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$, entonces $\beta \in \mathbb{Q}(\alpha)$, así $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ y $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

3. *$p(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. El cuerpo de descomposición de $p(x)$ es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, ya que $p(x) = x^4 - 5x^2 + 6 = (x^2 - 3)(x^2 - 2)$.*

Lema 1.4.1. *Sea $p(x) \in K[x]$ irreducible. Entonces existe una extensión F/K tal que $p(x)$ tiene una raíz en F.*

El siguiente resultado garantiza la existencia de cuerpos de descomposición.

Teorema 1.4.1. *Sea K un cuerpo y $p(x) \in K[x]$ no constante, entonces existe un cuerpo de descomposición de $p(x)$ sobre K.*

Demostración. (Bhattacharya, 1994, Teorema 2.3) □

Definición 1.4.3. *Sean E/K y F/K dos extensiones de cuerpos y $\rho : E \to F$ un homomorfismo de cuerpos. $\rho(x)$ es un K-homomorfismo si $\rho(k) = k$ para todo $k \in K$.*

Ahora, se tiene la unicidad del cuerpo de descomposición.

Teorema 1.4.2. *Sea K un cuerpo y sea $p(x) \in K[x]$ no constante. Si E_1 y E_2 son cuerpos de descomposición de $p(x)$ sobre K, entonces existe un $K-$isomorfismo $\tau : E_1 \to E_2$.*

En las siguientes secciones se caracterizan las extensiones de cuerpos, siendo normales y/o separables, éstas permiten comprender las propiedades de los cuerpos y los polinomios en relación con las extensiones. Estos conceptos son fundamentales para el desarrollo de los **siguientes temas**.

1.5. Extensiones normales

Definición 1.5.1. *F/K es una extensión normal, si F es el cuerpo de descomposición de un polinomio sobre K.*

Ejemplo 1.5.1. *1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ es normal.*

Pues $\mathbb{Q}(\sqrt{2},\sqrt{3})$ es el cuerpo de descomposición de

$$\begin{aligned} p(x) =& x^4 - x^2 + 6 \\ =& (x^2-2)\cdot(x^2-3). \end{aligned}$$

2. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *no es normal.*

   Puesto que solo una de las raíces de $(x^3-2) \in \mathbb{Q}(\sqrt[3]{2})$, las otras son imaginarias.

Corolario 1.5.1. *Sea F/K una extensión finita normal. Si E es un subcuerpo intermedio, cualquier $K-$homorfismo $\phi : E \to F$ se extiende a un $K-$automorfismo $\tau : F \to F$.*

Teorema 1.5.1. *Sea F/K una extensión finita. Entonces F/K es normal si y sólo si todo $p(x) \in K[x]$ irreducible que tenga una raíz en F se descompone en $F[x]$.*

Demostración. Sea $F = K(a_1, a_2, \ldots, a_n)$ y sea $P(x) = p_1(x)\cdot p_2(x)\cdot \ldots \cdot p_n(x)$, donde $p_j(x)$ con $j = \{1,2,\ldots,n\}$ es el polinomio mínimo de cada a_j sobre K, es decir, $p_j(x) = \text{mín}(a_j, K)$. Dado que F/K es normal, entonces cada $p_j(x)$ se descompone en factores lineales en $F[x]$ y lo mismo ocurre con $P(x)$, por lo tanto F contiene al cuerpo de descomposición D de $P(x)$ y dado que F está generado por las raíces de $P(x)$, entonces coincide con el cuerpo D.

Recíprocamente sea $P_a(x) \in K[x]$ un polinomio irreducible en K que tiene una raíz a en F, se sabe que $P(x)$ se descompone en $F[x]$ en factores lineales, por consiguiente F es el cuerpo de descomposición de la familia $\{P_a(x)\}_{a\in K}$ de polinomios de $F[x]$, lo que implica que F/K es una extensión normal. □

1.6. Extensiones separables

Suponga que K es un cuerpo. Si $0 \neq p(x) \in K[x]$ y $a \in K$, entonces se puede escribir $p(x) = (x-a)^m g(x)$, donde $g(x) \in K[x]$, $g(a) \neq 0$ y $0 \leq m \leq gr(p(x))$, donde $gr(p(x))$ es el grado del polinomio $p(x)$.

Si $m > 1$, se dice que a es raíz múltiple de $p(x)$ (con multiplicidad m).

Si $m = 1$, se dice que a es raíz simple de $p(x)$.

Teorema 1.6.1. *Sean F un cuerpo, K un subcuerpo de F y $p(x) \in K[x]$ con $p'(x) \neq 0$, entonces,*

1. *Si $a \in F$. Entonces a es raíz múltiple de $p(x)$ si y sólo si $p(a) = p'(a) = 0$.*
2. *Si $(p(x), p'(x)) = 1$, entonces $p(x)$ no tiene raíces múltiples en F.*
3. *Si $p(x)$ es irreducible en $K[x]$, entonces todas sus raíces están en el cuerpo de descomposición de $p(x)$.*

Definición 1.6.1. *Sea K cuerpo y $p(x) \in K[x]$ un polinomio irreducible. Se dice que $p(x)$ es separable si todas las raíces de $p(x)$ en el cuerpo de descomposición de $p(x)$ sobre K son simples.*

Corolario 1.6.1. *Sea K un cuerpo y $p(x) \in K[x]$ un polinomio irreducible. Entonces, $p(x)$ no es separable si y sólo si $p'(x) = 0$. En particular se verifica:*

1. *Si $charK = 0$, todo polinomio irreducible de $K[x]$ es separable.*
2. *Si $charK = p > 0$, un polinomio no es separable si y sólo si es un polinomio en x^p.*

Ejemplo 1.6.1. 1. $p(x) = (x^2+2)^3(x-3)^2(x^5+x^4+x^3++x^2+x+1) \in \mathbb{Q}[x]$ *es separable.*

Definición 1.6.2. *Sea F/K una extensión algebraica. Se dice que F/K es separable si para cualquier $u \in F$,* $\min(u,K)$ *es un polinomio separable.*

El siguiente resultado caracteriza un elemento primitivo de F/K.

Teorema 1.6.2. *Sea F/K una extensión finita de característica cero. Entonces, existe $u \in F$ tal que $F = K(u)$.*

Demostración. Dado que $K \subset F$ y $u \in F$, entonces $K(u) \subset F$. Por otro lado, $K(u)$ contiene a 0 y a u y a todas las potencias de u, por lo tanto $F \subset K(u)$, pues u es el elemento primitivo de F. En consecuencia $F = K(u)$. □

1.7. El grupo de Galois

Definición 1.7.1. *Si F es un cuerpo, un automorfismo de F es un homomorfismo biyectivo de cuerpos de F en F.*

Al cuerpo de los automorfismos de F se denotará por $Aut(F)$. Si F/K es una extensión de cuerpos, un K-automorfismo de F es un automorfismo $\phi : F \to F$ tal que $\phi(u) = u$ para todo $u \in K$. El cuerpo de todos los K-automorfismos de F se denotará $\mathscr{G}al(F/K)$

$$\mathscr{G}al(F/K) = \{\phi \mid \phi \in Aut(F), \phi(u) = u, \quad \forall u \in K\}.$$

Evidentemente, si $\phi, \psi \in \mathscr{G}al(F/K)$, $(\phi \circ \psi) \in \mathscr{G}al(F/K)$. Así $(\mathscr{G}al(F/K), \circ)$ es un grupo. Este grupo se llama **grupo de Galois de la extensión** F/K. En lo que sigue, F/K denotará una extensión de cuerpos finita, (Riquelme, 2007).

Definición 1.7.2. *Una extensión F/K es de Galois si F/K es normal y separable.*

Teorema 1.7.1. *Suponga que F/K es separable, entonces:*

$$|\mathscr{G}al(F/K)| \leq [F:K].$$

Además,

$$|\mathscr{G}al(F/K)| = [F:K]$$

si y sólo si F/K es normal (Galois).

Ejemplo 1.7.1. *1. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Si $\phi \in \mathscr{G}al(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, entonces $\phi(\sqrt[3]{2})$ es una raíz del polinomio x^3-2 y $\phi(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$, por lo que necesariamente $\phi(\mathbb{Q}(\sqrt[3]{2})) = (\sqrt[3]{2})$, así $\phi = Id_{\mathbb{Q}(\sqrt[3]{2})}$ y se tiene que*

$$\mathscr{G}al(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = Id_{\mathbb{Q}(\sqrt[3]{2})}.$$

El siguiente resultado es conocido como Teorema de Dedekind.

Teorema 1.7.2. *Sea K un cuerpo y sean $\tau_1, \cdots, \tau_n$ automorfismos distintos de K. Entonces $\tau_1, \cdots, \tau_n$ son K-linealmente independientes.*

Si E es un cuerpo y S un subgrupo de $Aut(E)$, se define

$$F(S) = \{e \in E \mid \sigma(e) = e, \quad \forall \sigma \in S\},$$

el subcuerpo de E fijado por todos los elementos de S.

Note que, si $S_1 \subseteq S_2 \subseteq Aut(E)$ entonces $F(S_2) \subseteq F(S_1)$.

Teorema 1.7.3 (Artin)**.** *Sean E un cuerpo y S un subgrupo de $Aut(E)$. Si $F = F(S)$, entonces*

$$[E : F] = |\, S \,| \,.$$

Como consecuencia se tiene que:

- Si E/K una extensión de Galois y $G = \mathscr{G}al(E/K)$, $a \in E$ y $\tau(a) = a$, $\forall \tau \in G$, entonces $a \in K$, es decir, $F(G) = K$.
- Si E un cuerpo de característica cero y $S \leq Aut(E)$ un grupo finito, $F = F(S)$ implica que E/F es una extensión de Galois y $\mathscr{G}al(E/F) = S$.

Teorema 1.7.4. *Sea K un cuerpo de característica cero, sea E/K una extensión y sea $K \subseteq L \subseteq E$ un subcuerpo tal que L/K es normal. Entonces $\sigma(L) = L$, para todo $\sigma \in \mathscr{G}al(E/K)$. Si E/K es normal, la aplicación $\rho : \mathscr{G}al(E/K) \to \mathscr{G}al(L/K)$ tal que $\rho(\phi) = \phi_L$ es un automorfismo $\phi_L : L \to L$ tal que $\phi_L(u) = u$ para todo $u \in K$, está bien definida y su núcleo es $\mathscr{G}al(E/L)$ y es sobreyectiva. En particular, $\mathscr{G}al(E/L) \trianglelefteq \mathscr{G}al(E/K)$ y*

$$\mathscr{G}al(E/K)/\mathscr{G}al(E/L) \simeq \mathscr{G}al(L/K).$$

Teorema 1.7.5. *Sea K un cuerpo con característica cero. Suponga que E/K es una extensión de Galois y sea $K \subseteq L \subseteq E$ un subcuerpo. Entonces L/K es normal si y sólo si $\sigma(L) = L$ para todo $\sigma \in \mathscr{G}al(E/K)$.*

Demostración. Se tiene que L/K es normal si $\sigma(L) = L$ para todo $\sigma \in \mathscr{G}al(E/K)$ por el teorema anterior (Teorema 1.7.4) .

Recíprocamente, sea $a \in L$ con polinomio mínimo $p(x) \in K[x]$. Dado que E/K es de Galois, esta extensión es normal por lo tanto $p(x)$ se descompone en E.

Sea $b \in E$ una raíz de $p(x)$ en E, entonces $b = \sigma(a)$ para algún $\sigma \in \mathscr{G}al(E/K)$, ya que $\sigma(L) = L$ y $a \in L$ entonces $\sigma(a) \in \sigma(L)$, por lo tanto $b \in \sigma(L) = L$ implica que $p(x)$ se descompone en L, así L/K es normal. □

El siguiente teorema establece una relación entre las extensiones de Galois, los grupos de Galois y los subcuerpos intermedios. Además permite la caracterización de extensiones normales y su relación con los grupos de Galois.

Teorema 1.7.6 (**Teorema fundamental de Galois**). *Sean E/K una extensión de Galois y $G = \mathscr{G}al(E/K)$. Sean S el conjunto de subconjuntos de G y $\mathscr{K}$ el conjunto de subcuerpos intermedios $K \subseteq L \subseteq E$.*

1. *Las aplicaciones $f : S \to \mathscr{K}$ y $g : \mathscr{K} \to S$ dadas por $f(H) = F(H)$ y $g(L) = \mathscr{G}al(E/L)$ son biyecciones, inversa una de la otra.*

2. *Si $K \subseteq L \subseteq E$, entonces L/K es normal si y sólo si $\mathscr{G}al(E/L) \trianglelefteq \mathscr{G}al(E/K)$. En este caso*

$$\mathscr{G}al(E/K)/\mathscr{G}al(E/L) \simeq \mathscr{G}al(L/K).$$

2. Números P-ádicos

Los números p-ádicos fueron introducidos por Kurt Hensel, quién estaba interesado en la analogía entre el anillo de enteros $\mathbb{Z}$ con su cuerpo de fracciones $\mathbb{Q}$, y, el anillo de polinomios con coeficientes complejos $\mathbb{C}[x]$, con su cuerpo de fracciones $\mathbb{C}(x)$. Un elemento $p(x) \in \mathbb{C}(x)$ es el cociente de dos polinomios, de manera similar, cualquier número racional $x \in \mathbb{Q}$ es un cociente de dos enteros. Asimismo, las propiedades de los anillos son muy similares, pues tanto $\mathbb{Z}$ como $\mathbb{C}[x]$ son anillos de factorización única, es decir, cualquier entero puede expresarse como producto de primos salvo unidades, y cualquier polinomio de $\mathbb{C}[x]$ puede expresarse únicamente como

$$p(x) = \alpha(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

donde α y $\alpha_1, \alpha_2 \ldots \alpha_n$ son números complejos. Este era el motivo principal de Hensel, que los primos $p \in \mathbb{Z}$ son análogos a los polinomios lineales $x-\alpha \in \mathbb{C}[x]$, (López, 2019).

En general los números racionales se escriben en el sistema decimal, es decir, en cifras cuyos números van del 0 al 9. Se conoce la separación de estos números por unidades, decenas, centenas, etc. Por ejemplo el número 561 tiene 1 unidad, 6 decenas y 5 centenas. En otras palabras, el número 561 puede ser representado de la siguiente manera:

$$561 = 5 \cdot 10^2 + 6 \cdot 10^1 + 1 \cdot 10^0$$

Observe que todos los dígitos dependen de la base, y así cada dígito podría tomar valor en

el conjunto de los 10 elementos, $\{0,1,2,3,4,5,6,7,8,9\}$. Si el número tiene decimales, el razonamiento es el mismo. Por ejemplo el número $968,63$ es el resultado de la expansión:

$$968,63 = 9\cdot 10^2 + 6\cdot 10^1 + 8\cdot 10^0 + 6\cdot 10^{-1} + 3\cdot 10^{-2}.$$

Asimismo, esto puede hacerse con cualquier número natural $p \in \mathbb{Z} - \{0\}$. La idea es expresar cualquier número racional q como una expresión polinómica en p, en particular se tomará el caso en el que p es primo. Esta expresión puede involucrar potencias negativas, cuyos coeficientes sea números naturales mayores o iguales a 0 y menores a p. Esto se denomina desarrollo p-ádico de q. Por ejemplo,

$$8534 = 3\cdot 7^4 + 3\cdot 7^3 + 6\cdot 7^2 + 1\cdot 7 + 1;$$

es el desarrollo 7-ádico de 8534. Para encontrar los desarrollos p-ádicos de un número entero m se utiliza el algoritmo de la división de la siguiente manera: primero se divide m por p luego al cociente de dicha división se le divide por p y así sucesivamente hasta llegar a un cociente que sea menor que p. La sucesión (en orden inverso) dada por los restos de las sucesivas divisiones son los coeficientes de la expresión en potencias de p. Por ejemplo,

$$
\begin{array}{cccc|c}
8 & 5 & 3 & 4 & 7 \\
\hline
1 & 5 & & & 1219 \\
\hline
 & 1 & 3 & & 174 \\
\hline
 & & 6 & 4 & 24 \\
\hline
 & & & 1 & 3
\end{array}
$$

Los sucesivos restos, en orden inverso dieron 33611, que son los coeficientes de la expresión dada anteriormente. Usando el algoritmo de división se escribe en cada paso al dividendo como la suma del cociente por el divisor más el residuo.

$$
\begin{aligned}
8534 &= 1219 \cdot 7 + 1, \\
8534 &= (174 \cdot 7 + 1) \cdot 7 + 1, \\
8534 &= 174 \cdot 7^2 + 1 \cdot 7 + 1, \\
8534 &= (24 \cdot 7 + 6) \cdot 7^2 + 1 \cdot 7 + 1, \\
8534 &= 24 \cdot 7^3 + 6 \cdot 7^2 + 1 \cdot 7 + 1, \\
8534 &= (3 \cdot 7 + 3) \cdot 7^3 + 6 \cdot 7^2 + 1 \cdot 7 + 1, \\
8534 &= 3 \cdot 7^4 + 3 \cdot 7^3 + 6 \cdot 7^2 + 1 \cdot 7 + 1.
\end{aligned}
$$

Entonces $8534 = (33611)_7$.

Teorema 2.0.1. *Sea $p \in \mathbb{N}$, $p > 1$. Para todo $n \in \mathbb{N}$ existe una expresión polinomial en p, llamado el desarrollo p-ádico de n, del siguiente tipo*

$$n = \sum_{i=0}^{t} a_i p^i = a_t p^t + \cdots + a_1 p + a_0,$$

donde $a_i \in \mathbb{Z}$, $0 \leq a_i < p$. Dicho desarrollo es único, en el siguiente sentido: si

$$\sum_{i=0}^{t} a_i p^t = \sum_{j=0}^{h} b_j p^j, \qquad 0 \leq i, j < p, a_t \neq 0 \neq b_h,$$

entonces $t = h$ y $a_i = b_i$ para todo $1 \leq i \leq t = h$. En tal caso se dice que $(a_t a_{t-1} \cdots a_1 a_0)_p$ es el desarrollo de n en base p.

2.1. Operaciones con desarrollos p-ádicos

Las operaciones, suma, resta, multiplicación y división, se realizan de manera muy similar a las operaciones en desarrollo decimal o 10-ádico, (Baquero, 2020).

Suma: Para comprender la regla, considere la siguiente suma $(4412)_5 + (301)_5$. Primero se escriben los desarrollos como expresiones polinómicas y se realiza la suma

$$\begin{array}{rcl} (4412)_5 & = & 4\cdot 5^3 + 4\cdot 5^2 + 1\cdot 5 + 2 \\ + \quad (301)_5 & = & \qquad\qquad 3\cdot 5^2 + 0\cdot 5 + 1 \\ \hline & & 4\cdot 5^3 + 7\cdot 5^2 + 1\cdot 5 + 3 \end{array}$$

El resultado obtenido es $4\cdot 5^3+7\cdot 5^2+1\cdot 5+3$, que no es un desarrollo p-ádico pues hay un coeficiente que es mayor que 5. Sin embargo, $7=5+2$, luego $7\cdot 5^2=(5+2)\cdot 5^2=1\cdot 5^3+2\cdot 5^2$ y así

$$\begin{aligned}4\cdot 5^3+7\cdot 5^2+1\cdot 5+3 &= 4\cdot 5^3+1\cdot 5^3+2\cdot 5^2+1\cdot 5+3\\ &= 5\cdot 5^3+2\cdot 5^2+1\cdot 5+3\\ &= 1\cdot 5^4+0\cdot 5^3+2\cdot 5^2+1\cdot 5+3\end{aligned}$$

Luego, $(4412)_5+(301)_5=(10213)_5$. La suma se realiza de forma análoga a la suma usual, se suman las cifras correspondientes y cada que se supera p, en este caso 5, se debe sumar 1 a la cifra siguiente, es decir, utilizando congruencias. Para realizar las operaciones, no se especifica la base en la cual se está trabajando para no complicar la notación.

$$\begin{array}{cccccc} & {}^{+1}4 & 4 & 1 & 2 \\ + & & 3 & 0 & 1 \\ \hline 1 & 0 & 2 & 1 & 3 \end{array}$$

Orden en desarrollos p-ádicos: Sean $a=(a_ta_{t-1}\cdots a_1a_0)_p$ y $b=(b_hb_{h-1}\cdots b_1b_0)_p$ dos números naturales expresados en base p y suponga que $a\neq b$. Luego, $a=a_tp^t+a_{t-1}p^{t-1}+\cdots+a_1p+a_0$, $b=b_hp^h+b_{h-1}p^{h-1}+\cdots+b_1p+b_0$ y por el orden de los naturales tenemos que $a<b$ si y

sólo si

$$a_t p^t + a_{t-1} p^{t-1} + \cdots + a_1 p + a_0 < b_h p^h + b_{h-1} p^{h-1} + \cdots + b_1 p + b_0$$
$$\Leftrightarrow t < h \qquad \text{ó} \qquad t = h \qquad \text{y} \qquad a_m < b_m,$$

donde $m = \text{máx}\{1 \leq i \leq t = h | a_i \neq b_i\}$; tal m existe pues $a \neq b$.

Ejemplo 2.1.1. *1.* $(2020)_3 > (121)_3$.

2. $(201)_3 > (121)_3$.

3. $(210)_3 > (200)_3 > (21)_6$.

Resta: Dado que el conjunto de los números enteros no negativos no es un anillo, primero se describirá la operación de la resta utilizando el orden dado anteriormente, asegurando que el resultado sea un número entero. Considere el siguiente ejemplo:
Tomando $1140 = (3216)_7$ y $216 = (426)_7$, es claro que $1140 - 216 = 924$ y $924 = (2460)_7$. Pues bien,

$$\begin{array}{rcl} (3216)_7 & = & 3\cdot 7^3 + 2\cdot 7^2 + 1\cdot 7 + 6 \\ - \quad (426)_7 & = & \qquad\quad 4\cdot 7^2 + 2\cdot 7 + 6 \\ \hline & & 3\cdot 7^3 - 2\cdot 7^2 - 1\cdot 7 + 0 \end{array}$$

Al igual que para la suma, el resultado obtenido no es un desarrollo 7-ádico. Para lograrlo, se debe operar de la siguiente manera:

$$\begin{aligned} 3\cdot 7^3-2\cdot 7^2-1\cdot 7+0 &= 2\cdot 7^3+1\cdot 7^3-2\cdot 7^2-1\cdot 7+0\\ &= 2\cdot 7^3+7\cdot 7^2-2\cdot 7^2-1\cdot 7+0\\ &= 2\cdot 7^3+5\cdot 7^2-1\cdot 7+0\\ &= 2\cdot 7^3+4\cdot 7^2+1\cdot 7^2-1\cdot 7+0\\ &= 2\cdot 7^3+4\cdot 7^2+7\cdot 7-1\cdot 7+0\\ &= 2\cdot 7^3+4\cdot 7^2+6\cdot 7+0. \end{aligned}$$

Luego, la resta se realiza de forma análoga a la usual restando las cifras correspondientes y cada vez que se deba restar una cifra mayor a una que es menor, se toma prestado de la cifra anterior p unidades, en este caso 7, y se resta 1 a la cifra siguiente, es decir, utilizando congruencias y “sustrayendo unidades":

$$\begin{array}{rcccc} & 3^{-1} & {}^{+7}2^{-1} & {}^{+7}1 & 6\\ - & & 4 & 2 & 6\\ \hline & 2 & 4 & 6 & 0 \end{array}$$

Producto: Del mismo modo que la suma y la resta, en el producto se usarán los desarrollos como expresiones polinómicas y aplicando la ley distributiva. Por ejemplo,

$$\begin{aligned}(142)_5 \times (1303)_5 =& (1\cdot 5^2+4\cdot 5+2)\times(1\cdot 5^3+3\cdot 5^2+0\cdot 5+3),\\ =& 1\cdot 5^5+3\cdot 5^4+3\cdot 5^2+4\cdot 5^4+12\cdot 5^3+12\cdot 5\\ &+2\cdot 5^3+6\cdot 5^2+6,\\ =& 1\cdot 5^5+7\cdot 5^4+14\cdot 5^3+9\cdot 5^2+12\cdot 5+6.\end{aligned}$$

Para escribir el resultado en base 5, se debe reducir la expresión $1\cdot 5^5+7\cdot 5^4+14\cdot 5^3+9\cdot 5^2+12\cdot 5+6$ a un desarrollo 5-ádico. Para ello, se procede como antes

$$\begin{aligned}&1\cdot 5^5+7\cdot 5^4+14\cdot 5^3+9\cdot 5^2+12\cdot 5+6,\\ =&1\cdot 5^5+(5+2)\cdot 5^4+(5\cdot 2+4)\cdot 5^3+(5+4)\cdot 5^2+(5\cdot 2+2)\cdot 5+(5+1),\\ =&1\cdot 5^5+5^5+2\cdot 5^4+2\cdot 5^4+4\cdot 5^3+5^3+4\cdot 5^2+2\cdot 5^2+2\cdot 5+5+1,\\ =&2\cdot 5^5+4\cdot 5^4+5\cdot 5^3+6\cdot 5^2+3\cdot 5+1,\\ =&2\cdot 5^5+4\cdot 5^4+5^4+(5+1)\cdot 5^2+3\cdot 5+1,\\ =&2\cdot 5^5+5\cdot 5^4+5^3+5^2+3\cdot 5+1,\\ =&2\cdot 5^5+5^5+5^3+5^2+3\cdot 5+1,\\ =&3\cdot 5^5+5^3+5^2+3\cdot 5+1.\end{aligned}$$

Así, $(142)_5 \times (1303)_5 = (301131)_5$, y claramente la multiplicación se realiza muy similar a la usual, salvo que luego de multiplicar las cifras, se suma usando congruencia módulo p, que en este caso es 5. Observe:

$$
\begin{array}{cccccc}
 & & 1 & 3 & 0 & 3 \\
 & \times & & 1 & 4 & 2 \\
\hline
 & & {}^{+2}2 & 6 & {}^{+1}0 & 6 \\
 & {}^{+1}6 & 2 & 2 & 2 & \\
{}^{+2}1 & 3 & 0 & 3 & & \\
\hline
3 & 0 & 1 & 1 & 3 & 1
\end{array}
$$

2.2. Anillo de números racionales p-ádicos

Se ha mostrado que todo número entero positivo admite un desarrollo p-ádico, con $p \in \mathbb{N}$, y como tal tiene una escritura en base p que se denota como una sucesión de números a_i donde $0 \leq a_i < p$. Ahora se desea tener un desarrollo p-ádico también para los números negativos, para ello se realiza el desarrollo para -1:

$$\begin{aligned}
-1 =&(p-1)-p,\\
=&(p-1)+[(p-1)-p]\cdot p,\\
=&(p-1)+(p-1)p-p^2,\\
=&(p-1)+(p-1)p+[(p-1)-p]\cdot p^2,\\
=&(p-1)+(p-1)p+(p-1)p^2-p^3,\\
=&(p-1)+(p-1)p+(p-1)p^2+[(p-1)-p]\cdot p^3,\\
=&(p-1)+(p-1)p+(p-1)p^2+(p-1)p^3-p^4.
\end{aligned}$$

Siguiendo el procedimiento anterior se tiene que:

$$-1=(p-1)+(p-1)p+(p-1)p^2+(p-1)p^3+(p-1)p^4+(p-1)p^5+\cdots$$

Entonces $-1=(\ldots(p-1)(p-1)(p-1))_p$ la escritura p-ádica de -1. Análogamente, $-p=(\ldots(p-1)(p-1)(p-1)0)_p$.

Ejemplo 2.2.1. *1. Para escribir* -15 *en base* 7. *Se sabe que* $-15 \equiv 6(mod\ 7)$ *y que*

$$\begin{aligned}
-15 &= -(7\cdot 2+1),\\
&= -1-7\cdot 2,\\
&= 6-7-7\cdot 2,\\
&= 6-7\cdot 3,\\
&= (6)_7+(\ldots 66660)_7\times(3)_7,\\
&= (6)_7+(\ldots 66640)_7,\\
&= (\ldots 666646)_7.
\end{aligned}$$

Así $-15 = (\ldots 666646)_7$

Lema 2.2.1. *Si* $(a_t a_{t-1}\ldots a_1 a_0)_p$ *es el desarrollo en base p de un número entero positivo a, entonces el desarrollo de* $-a$ *esta dado por*

$$(\ldots(p-1)(p-1)[(p-1)-a_t][(p-1)-a_{t-1}]\ldots[(p-1)-a_1](p-a_0))_p.$$

Ejemplo 2.2.2. *1. Considere* -2628*, para escribirlo en base* 7*, note que* $2628 = (10443)_7$ *y por el lema anterior, se tiene entonces que*

$$-2628 = (\ldots 6666(6-1)(6-0)(6-4)(6-4)(7-3))_7 = (\ldots 666656224)_7$$

Una consecuencia de este lema, es que los números enteros negativos están representados por sucesiones infinitas tales que sólo un número finito de cifras es distinta de $p-1$ y están al principio de la sucesión.

Definición 2.2.1. *El anillo de enteros p-ádicos se define como el conjunto de todas las sucesiones cuyos coeficientes son enteros no negativos menores que p:*

$$\mathbb{Z}_p = \{(\ldots a_3 a_2 a_1 a_0) : 0 \leq a_i < p\}.$$

Teorema 2.2.1. *El conjunto $\mathbb{Z}_p$ de los enteros p-ádicos es un anillo conmutativo con las operaciones definidas entre enteros p-ádicos.*

De la construcción se tiene que, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Z}_p$, donde los números naturales están representados en $\mathbb{Z}_p$ como las sucesiones de cifras finitas no nulas.

Lema 2.2.2. $\mathscr{U}(\mathbb{Z}_p) = \{(\ldots a_3 a_2 a_1 a_0) \in \mathbb{Z}_p : (a_0, p) = 1\}$.

Demostración. Las unidades de un anillo son los elementos que tienen inverso con respecto al producto. Sea $a = (\ldots a_2 a_1 a_0)_p$, entonces se busca un $b = (\ldots b_2 b_1 b_0)_p$ tal que $a \cdot b = b \cdot a = 1 = (\ldots 000001)_p$. Entonces

$$
\begin{array}{cccccccc}
 & & \dots & a_3 & a_2 & a_1 & a_0 \\
\times & & \dots & b_3 & b_2 & b_1 & b_0 \\
\hline
 & & \dots & b_0a_3 & b_0a_2 & b_0a_1 & b_0a_0 \\
 & \dots & b_1a_3 & b_1a_2 & b_1a_1 & b_1a_0 & \\
+ & & \vdots & \vdots & \vdots & & \\
\hline
 & & & \dots & (a_0a_2+b_1a_1+b_2a_0) & (b_0a_1+b_1a_0) & b_0a_0
\end{array}
$$

el resultado no está escrito en base p, pues primero se debe reducir la expresión. Para que se cumpla $a \cdot b = 1$, se debe tener que $b_0a_0 \equiv 1(mod\ p)$. Es decir, a_0 debe ser una unidad en $\mathbb{Z}_p$ y esto sucede si y sólo si a_0 es primo relativo con p. Si a_0 cumple esta condición, entonces b_0 queda determinado por el inverso multiplicativo de a_0.

Luego, si $(a_0, p) = 1$ entonces existe $q_0 \in \mathbb{Z}$ tal que $b_0a_0 = q_0 \cdot p + 1$. Por el algoritmo de la adición, para realizar la suma en la segunda cifra se debe sumar q_0 a $b_0a_1 + b_1a_0$ y luego reducir módulo p. Dado que se busca $a \cdot b = (\cdots 00001)$, se debe tener que

$$b_0a_1 + b_1a_0 + q_0 \equiv 0(mod\ p).$$

Por lo tanto, $b_1a_0 \equiv -b_0a_1 - q_0(mod\ p)$ y puesto que a_0 es invertible en $\mathbb{Z}_p$ con inverso b_0, multiplicando a los dos miembros por b_0 se tiene que

$$b_1 \equiv -b_0^2a_1 - q_0b_0(mod\ p).$$

Dado que $0 \leq b_1 < p$, la ecuación anterior determina a b_1. Para hallar a b_2 se procede de la misma forma. Si $b_0a_1 + b_1a_0 + q_0 \equiv 0(mod\ p)$, entonces existe $q_1 \in \mathbb{Z}$ tal que $b_0a_1 + b_1a_0 + q_0 = q_1 \cdot p$. Usando de nuevo el algoritmo de la suma en la tercera cifra, se tiene que

$$b_0a_2 + b_1a_1 + b_2a_0 + q_1 \equiv 0(mod\ p).$$

Así, $b_2a_0 \equiv -b_0a - 2 - b_1a_1 - q_1(\ p)$ y multiplicando a ambos lados por b_0 se tiene

$$b_2 \equiv -b_0^2a_2 - b_0b_1a_1 - b_0q_1(mod\ p).$$

Puesto que $0 \leq b_2 < p$, esta ecuación determina b_2. Siguiendo este método recursivamente se encuentra de manera única el número b que es el inverso multiplicativo de a si y sólo si a_0 es primo relativo de p. □

Ejemplo 2.2.3. *1. Hallar el inverso de* $(\ldots 0004)_5$.

Primero se busca el inverso de $a_0 = 4$ *en* $\mathbb{Z}_5$ *que existe, pues* $(4,5) = 1$, *así* $4 \cdot 4 = 16 \equiv 1(mod\ 5)$, *entonces* $b_0 = 4$. *Además* $16 = 5 \cdot 3 + 1$ *lo que implica que* $q_0 = 3$. *Luego, del procedimiento anterior, se busca un* b_1 *tal que*

$$\begin{aligned} b_1 &\equiv -b_0^2 a_1 - b_0 q_0 (mod\ p), \\ &\equiv -4^2 \cdot 0 - 4 \cdot 3 (mod\ 5), \\ &\equiv -12 (mod\ 5), \\ &\equiv 3 (mod\ 5). \end{aligned}$$

Luego, $b_1 = 3$. *Además,* $b_0 a_1 + b_1 a_0 + q_0 = 4 \cdot 0 + 3 \cdot 4 + 3 = 15 = 3 \cdot 5 = q_1 \cdot 5$, *de donde se sique que* $q_1 = 3$. *Ahora, se busca* b_2 *tal que*

$$\begin{aligned} b_2 &\equiv -b_0^2 a_2 - b_0 b_1 a_1 - b_0 q_1 (mod\ p), \\ &\equiv -4^2 \cdot 0 - 4 \cdot 3 \cdot 0 - 4 \cdot 3 (mod\ 5), \\ &\equiv -12 (mod\ 5), \\ &\equiv 3 (mod\ 5). \end{aligned}$$

Así $b_2 = 3$, *y* $b_0 a_2 + b_1 a_1 + b_2 a_0 + q_1 = 4 \cdot 0 + 3 \cdot 0 + 3 \cdot 4 + 3 = 15 = 3 \cdot 5 = q_2 \cdot 5$, *por lo tanto* $q_2 = 3$. *Ahora se busca un* b_3 *tal que*

$$\begin{aligned} b_3 &\equiv -b_0^2 a_3 - b_0 b_1 a_2 - b_0 b_2 a_1 - b_0 q_2 (mod\ p), \\ &\equiv -4^2 \cdot 0 - 4 \cdot 3 \cdot 0 - 4 \cdot 3 \cdot 0 - 4 \cdot 3 (mod\ 5), \\ &\equiv -12 (mod\ 5), \\ &\equiv 3 (mod\ 5). \end{aligned}$$

Luego $b_3 = 3$, se observa entonces que $b_n = 3$ para todo $n \geq 2$, puesto que $a_j = 0$ para todo $j \geq 1$ y así $q_n = 3$, entonces $(\ldots 0004)_5^{-1} = (\ldots 333334)_5$.

Teorema 2.2.2. *El anillo $\mathbb{Z}_p$ de enteros p-ádicos es un dominio entero.*

Demostración. Sean $a = \sum_{i=0}^{\infty} a_i p^i$ y $b = \sum_{i=0}^{\infty} b_i p^i$ con $a, b \neq 0$. Entonces sea a_k el primer coeficiente distinto de cero de a con $0 < a_k < p$ y del mismo modo b_t el primer coeficiente diferente de cero de b. En particular p no divide a a_k ni a b_t y en consecuencia no divide tampoco a su producto $a_k b_t$. Por definición de la multiplicación, el primer coeficiente distinto de cero del producto ab es el coeficiente c_{k+t} de p^{k+t} donde $0 < c_{k+t} < p$ y este coeficiente se define por $c_{k+t} \equiv a_k b_t (mod\ p)$, así $c_{k+t} \not\equiv 0 (mod\ p)$, por lo tanto $\mathbb{Z}_p$ carece de divisores de cero. □

2.3. Cuerpo de los números p-ádicos

Puesto que no todo elemento de $\mathbb{Z}_p$ tiene inverso, para construir un cuerpo que contenga a $\mathbb{Z}_p$ se deben introducir los inversos de los elementos no nulos, (Gastón, 2008). La extensión de los números racionales se ve reflejada en el desarrollo decimal con la introducción de decimales

$$\frac{1}{50} = 0,02; \qquad \frac{4}{9} = 0,444\ldots$$

Así como el inverso de $p \in \mathbb{Q}$ es $\frac{1}{p} = p^{-1}$, se introducen los inversos de las potencias de p. Para ello se usará la misma notación de decimales, pero sólo admitiendo cifras finitas después de la coma, así:

$$(0,021)_p = 2 \cdot p^{-2} + 1 \cdot p^{-3};$$

$$(321,5642)_7 = 3\cdot 7^2 + 2\cdot 7 + 1 + 5\cdot 7^{-1} + 6\cdot 7^{-2} + 4\cdot 7^{-3} + 2\cdot 7^{-4}.$$

Hasta el momento, el conjunto $\mathbb{Q}_p = \{(\ldots a_2a_1a_0, a_{-1}a_{-2}\ldots a_{-t}) | 0 \leq a_i < p, a_{-t} \neq 0\}$ es un anillo y se denomina el anillo de los números racionales p-ádicos.

Lema 2.3.1. *$\mathbb{Q}_p$ es un cuerpo con las operaciones definidas anteriormente.*

Demostración. Se sabe que $\mathbb{Q}_p$ es un anillo conmutativo con identidad. Además, dado que p es primo entonces todo número a_i con $0 < a_i < p$ es primo relativo con p. Luego, si $a \in \mathbb{Q}_p$ no nulo tiene inverso multiplicativo, esto se tiene por el Lema (2.2.2). Por lo tanto $\mathbb{Q}_p$ es un cuerpo. □

Observe que por la construcción $\mathbb{Z} \subseteq \mathbb{Q}_p$ para todo p primo, luego, dado que $\mathbb{Q}_p$ es un cuerpo, se sigue que $\mathbb{Q} \subset \mathbb{Q}_p$ para todo p. Puesto que $\mathbb{Q}_p$ contiene a $\mathbb{Z}$ y por tanto contiene a $\mathbb{Q}$; dado que todo cuerpo que contiene a $\mathbb{Z}$ contiene una copia de $\mathbb{Q}$.

División: Se mostrará un algoritmo basado en el algoritmo de división de polinomios, que permite escribir a los números racionales en $\mathbb{Q}_p$.

Note que hay racionales que ya se pueden escribir en base p. Por ejemplo $\frac{7}{81}$ en base 3, sería de la forma:

$$\frac{7}{81} = \frac{2\cdot 3+1}{3^4} = \frac{2}{3^3} + \frac{1}{3^4} = 2\cdot 3^{-3} + 1\cdot 3^{-4} = (0,0021)_3.$$

Pero hay racionales que en $\mathbb{Q}_p$ cuyo desarrollo no es tan evidente. Dado que se admiten infinitas cifras a la izquierda , para realizar la división, se pondrá el divisor a la izquierda y el dividendo a la derecha, es decir, con el orden inverso. Así dados $a = (\ldots a_2a_1a_0)_p$ y $b = (\ldots b_2b_1b_0)_p$, se desea

hacer el cociente $\frac{a}{b}$, se expresa:

$$b_0b_1b_2\ldots \;\big|\; a_0a_1a_2\ldots$$

Ahora bien, para escribir a/b en base p, se procede a dividir a por b de acuerdo al algoritmo del siguiente ejemplo.

Ejemplo 2.3.1. *1. Escribir* $\frac{7}{23}$ *en base* 3. *Dado que* $7 = (\ldots 0021)_3$ *y* $23 = (\ldots 000212)_3$ *luego*

$$\begin{array}{rl}
 & 21010\ldots \\
2120000\ldots & \big|\; 12000\ldots \\
 & \underline{-10210\ldots} \\
 & 02112\ldots \\
 & \underline{-2120\ldots} \\
 & 021\ldots \\
 & \underline{-000\ldots} \\
 & 0210\ldots \\
 & \underline{-21\ldots} \\
 & 0\ldots
\end{array}$$

Por lo anterior, $\frac{7}{23} = (\ldots 01012)_3$

2.4. Métricas sobre $\mathbb{Q}$

El objetivo de esta sección es dar una base sólida para la teoría que se ha descrito en el capítulo anterior. La idea principal es introducir una norma diferente en el cuerpo de los números racionales. Una vez se tenga dicha distancia, se procederá a la construcción de los números p-ádicos, (Carrillo, 2008).

2.4.1. Distancias y normas.

Definición 2.4.1. *Sea X un conjunto no vacío. Una métrica o distancia sobre X es una función $d : X \times X \to \mathbb{R}^+$, con $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$, tal que para todo $x, y \in X$ se cumple*

1. $d(x,y) = 0 \Leftrightarrow x = y$.
2. $d(x,y) = d(y,x)$.
3. $d(x,y) \leq d(x,z) + d(z,y)$ *para todo* $z \in X$ *(desigualdad triangular).*

Al par (X,d) se le llamará un espacio métrico, donde X es un conjunto no vacío y d una métrica en X.

Ejemplo 2.4.1. 1. *$(\mathbb{Q}, |\cdot|)$ es un espacio métrico, donde $d(x,y) = |x-y|$ es el valor absoluto usual.*

Definición 2.4.2. *Sea K un cuerpo y $\mathbb{R}^+$ el conjunto de los números reales no negativos. Una norma $|\cdot|$ sobre K es una función $|\cdot| : K \to \mathbb{R}^+$ tal que para todo $x, y \in K$ se tiene*

1. $|x| = 0 \Leftrightarrow x = 0$.

2. $|x \cdot y| = |x| \cdot |y|$.

3. $|x+y| \leq |x| + |y|$ *(desigualdad triangular).*

Una norma se dice no arquimediana si para todo $x, y \in K$ *se tiene que*

$$|x+y| \leq \text{máx}(|x|, |y|).$$

En otro caso, se dice que la norma es arquimediana.

Ejemplo 2.4.2. *Sea* $K = \mathbb{Q}$*, se define sobre* K*:*

1. *La norma*

$$|x| = \begin{cases} x, & si \quad x \geq 0. \\ \\ -x, & si \quad x < 0. \end{cases}$$

donde $|\cdot|$ *es el valor absoluto usual, y se denotará por* $|\cdot|_\infty$*, además es arquimediana, pues si* $x = y = 1$ *se tiene que*

$$|x+y| = 2 > \text{máx}(|x|, |y|) = 1.$$

2. *La norma*

$$|x| = \begin{cases} 0, & si \quad x = 0. \\ \\ 1, & si \quad x \neq 0. \end{cases}$$

se conoce como la norma trivial.

2.4.2. Norma p-ádica. Se sabe que existe una norma sobre el cuerpo $\mathbb{Q}$, el valor absoluto usual $|\cdot|$. Esta norma induce la métrica Arquimediana $d(x,y) = |x-y|$. Se definirá otra norma sobre $\mathbb{Q}$.

Definición 2.4.3. *Sea p un número primo. Se define el orden p-ádico, $ord_p(x)$, de un número racional $x \in \mathbb{Q}$ de la siguiente manera:*

1. $ord_p(x) = \max\{n \in \mathbb{Z} : p^n | x\}$, *si* $x \in \mathbb{Z} - \{0\}$, *es decir, la potencia mayor de p que divide a x.*

2. $ord_p(q) = ord_p(a) - ord_p(b)$, *si* $q = \frac{a}{b} \in \mathbb{Q}$.

3. $ord_p(0) = +\infty$.

El orden p-ádico de x también se denomina ***valuación*** *p-ádica y se denota por $v_p(x)$.*

Observaciones:

- La razón por la que se define $v_p(0) = +\infty$ es que 0 se puede dividir por p^n para cada $n \in \mathbb{N}$.
- Si $(a,p) = 1$ entonces $v_p(a) = 0$.

Ejemplo 2.4.3.

1. $v_5(40) = v_5(2^3 \cdot 5) = 1$.

2. $v_2(40) = v_2(2^3 \cdot 5) = 3$.

3. $v_2(51) = v_2(3 \cdot 17) = 0$, *pues* $(2,51) = 1$.

4. $v_3(51) = v_3(3 \cdot 17) = 1$.

Lema 2.4.1. *Para todo $x, y \in \mathbb{Q} - \{0\}$ se cumple:*

1. $v_p(xy) = v_p(x) + v_p(y)$.

2. $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

Demostración. 1. En efecto, suponga que $x, y \in \mathbb{Z}$ y que $v_p(x) = n$ y $v_p(y) = m$, es decir, $x = a'p^n$, e $y = b'p^m$, para algunos $a'b' \in \mathbb{Z}$, donde $(a', p^n) = 1 = (b', p^m)$. Por lo tanto, $xy = a'b'p^{n+m}$, con $(a'b', p^{n+m}) = 1$, es decir, $v_p(xy) = n + m = v_p(x) + v_p(y)$. Ahora, suponga que $x, y \in \mathbb{Q} - \{0\}$, es decir, son de la forma, $x = \frac{a}{b}$, e $y = \frac{c}{d}$, con $a, b, c, d \in \mathbb{Z}$, por lo tanto el producto $xy = \frac{ac}{bd}$, luego por la definición y lo que se probó se tiene que:

$$\begin{aligned} v_p(xy) =& v_p(ac) - v_p(bd), \\ =& v_p(a) + v_p(c) - (v_p(b) + v_p(d)), \\ =& (v_p(a) - v_p(b)) + (v_p(c) - v_p(d)), \\ =& v_p(x) + v_p(y). \end{aligned}$$

2. Suponga que $x, y \in \mathbb{Q} - \{0\}$, son de la forma, $x = \dfrac{a}{b}$, e $y = \dfrac{c}{d}$, con $a, b, c, d \in \mathbb{Z}$, por lo tanto $x + y = \dfrac{ad + bc}{bd}$, así:

$$v_p(x+y) = v_p(ad+bc) - v_p(bd).$$

Es claro que $v_p(ad + bc) \geq \text{mín}\{v_p(ad), v_p(bc)\}$, pues si se supone que el mínimo del anterior conjunto es n, quiere decir que p^n divide tanto a bc como a ad, así entonces p^n va a

dividir a la suma $ad+bc$. En consecuencia :

$$\begin{aligned} v_p(x+y) &\geq \text{mín}\{v_p(ad), v_p(bc)\} - v_p(bd), \\ &= \text{mín}\{v_p(a)+v_p(d), v_p(b)+v_p(c)\} - (v_p(b)+v_p(d)), \\ &= \text{mín}\{v_p(a)+v_p(d)-(v_p(b)+v_p(d)), v_p(b)+v_p(c)-(v_p(b)+v_p(d))\}, \\ &= \text{mín}\{v_p(a)-v_p(b), v_p(c)-v_p(d)\}. \end{aligned}$$

De donde se concluye que $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

□

Ejemplo 2.4.4. *1.* $v_3(\frac{5}{12}) = v_3(5) - v_3(12) = 0-1 = -1$.

2. $v_{11}(\frac{8}{15}) = v_{11}(8) - v_{11}(15) = 0-0 = 0$.

Definición 2.4.4. *Sea p un número primo, se define en $\mathbb{Q}$ la norma p-ádica por:*

$$|x|_p = p^{-v_p(x)} = \frac{1}{p^{v_p(x)}}, \quad si \quad x \neq 0,$$

y si $x = 0$ se toma $|0|_p = 0$.

El siguiente teorema muestra que en efecto $|\cdot|_p$ es una norma en $\mathbb{Q}$.

Teorema 2.4.1. *Para todo p primo, $|\cdot|_p$ es una norma no arquimediana sobre $\mathbb{Q}$.*

Demostración. Para ver que $|\cdot|_p$ es una norma, se deben verificar las propiedades de la Definición 2.4.2. Sea $x \in \mathbb{Q}$, por definición se tiene que $|x|_p = 0$ si y sólo si $x = 0$.

Sean $x, y \in \mathbb{Q}$. Si $x = 0$ o $y = 0$, entonces $|xy|_p = 0 = |x|_p|y|_p$. Si $x \neq 0 \neq y$, entonces por el Lema 2.4.1 se tiene que

$$|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)} \cdot p^{-v_p(y)} = |x|_p|y|_p,$$

lo que implica que se cumple 2.

3. Si $x = 0$ o $y = 0$ o si $x + y = 0$ ya está. Suponga que x, y, $x+y$ son no nulos, entonces se pueden escribir así: $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$ tales que $(a,b) = 1 = (c,d)$. Entonces $x + y = \dfrac{ad+bc}{bd}$ y $v_p(x+y) = v_p(ad+bc) - v_p(b) - v_p(d)$. Luego, del Lema 2.4.1 se sigue que

$$\begin{aligned} v_p(x+y) &\geq \text{mín}\{v_p(ad), v_p(bc)\} - v_p(b) - v_p(d), \\ &= \text{mín}\{v_p(a) + v_p(d), v_p(b) + v_p(c)\} - v_p(b) - v_p(d), \\ &= \text{mín}\{v_p(a) - v_p(b), v_p(c) - v_p(d)\} = \text{mín}\{v_p(x), v_p(y)\}. \end{aligned}$$

Por lo tanto,

$$\begin{aligned} |x+y|_p &= p^{-v_p(x+y)} \leq p^{-\text{mín}\{v_p(x), v_p(y)\}}, \\ &= \text{máx}\{p^{-v_p(x)}, p^{-v_p(y)}\}, \\ &= \text{máx}\{|x|_p, |y|_p\} \leq |x|_p + |y|_p. \end{aligned}$$

En particular, se ha probado que la norma es no arquimediana. □

Lema 2.4.2. *Sean $|\cdot|_1$ y $|\cdot|_2$ dos normas definidas en un cuerpo K. Las siguientes afirmaciones son equivalentes:*

1. *$|\cdot|_1$ y $|\cdot|_2$ son normas equivalentes.*

2. *Para cada $x \in K$ se tiene que $|x|_1 < 1$ si y sólo si $|x|_2 < 1$.*

3. *Existe $\alpha \in \mathbb{R}$ tal que $\forall x \in K$ se tiene que $|x|_1 = |x|_2^{\alpha}$.*

Teorema 2.4.2. *La norma p-ádica no es equivalente al valor absoluto usual. Además si p y q son primos distintos, las normas p-ádicas y q-ádicas no son equivalentes.*

Demostración. La primera afirmación es clara, ya que para cualquier norma p-ádica se cumple, por ser no arquimediana, que $|n|_p \leq 1$, $\forall n \in \mathbb{Z}$.
Si p y q son primos distintos, se cumple que $|p|_p = p^{-1}$ y $|q|_p = 1$. Por lo tanto, $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes.
Por otro lado, para cualquier primo p, $|p|_p = p^{-1} < 1$ y $|p|_\infty = p > 1$. □

El siguiente teorema destaca la relación entre dos normas en el conjunto de los números racionales ($\mathbb{Q}$).

Teorema 2.4.3 (Ostrowski). *Toda valor absoluto no trivial en $\mathbb{Q}$ es equivalente a la norma $|\cdot|_p$, donde p es un número primo ó $p = \infty$.*

Demostración. Sea $|\cdot|$ una norma sobre $\mathbb{Q}$ y $A = \{n \in \mathbb{N} : |n| > 1\}$ se tienen dos posibilidades mutuamente excluyentes $A \neq \emptyset$ o $A = \emptyset$.

Caso 1: Para $A \neq \emptyset$.

Por el principio del buen orden, existe $n_0 \in A$ tal que $n_0 \leq n$ para todo $n \in A$. Dado que $|n_0| > 1$ existe un número real positivo α tal que $|n_0| = n_0^{\alpha}$. Dado $n \in \mathbb{N}$, su desarrollo en la base n_0 es de la forma

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s,$$

donde $0 \leq a_i < n_0$ y $a_s \neq 0$. Entonces

$$\begin{aligned} |n| \leq & |a_0| + |a_1 n_0| + |a_2 n_0^2| + \cdots + |a_s n_0^s|, \\ = & |a_0| + |a_1| n_0^{\alpha} + |a_2| n_0^{2\alpha} + \cdots + |a_s| n_0^{s\alpha}. \end{aligned}$$

Puesto que todo $a_i < n_0$ para $0 \leq i \leq s$, por la elección de n_0 se tiene que $|a_i| \leq 1$ y como $n \geq n_0^s$, entonces

$$\begin{aligned} |n| \leq & 1 + n_0^{\alpha} + n_0^{2\alpha} + \cdots + n_0^{s\alpha}, \\ = & n_0^{s\alpha}(1 + n_0^{-1} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha}), \\ \leq & n^{s\alpha} \left(\sum_{i=0}^{\infty} \left(\frac{1}{n_0^{\alpha}} \right)^i \right). \end{aligned}$$

Dado que esta serie converge, es una constante finita, nótese esta constante por C. Entonces $|n| \leq Cn^{\alpha}$ para todo $n \in \mathbb{N}$. Sea n arbitrario y N suficientemente grande, reemplazando n por n^N en la desigualdad anterior y tomando la raíz N-ésima resulta $|n| \leq \sqrt[N]{C} n^{\alpha}$ y como $\lim_{N \to \infty} \sqrt[N]{C} = 1$,

por lo que

$$|n| \leq n^{\alpha}, \qquad (1)$$

para todo $n \in \mathbb{N}$.

Por otro lado, si se toma el desarrollo de $n \in \mathbb{N}$ en base n_0, se tiene que $n_0^{s+1} > n \geq n_0^s$,

$$|n| + |n_0^{s+1} - n| \geq |n + n_0^{s+1} - n| = |n_0^{s+1}|,$$

por lo tanto $|n| \geq |n_0^{s+1}| - |n_0^{s+1} - n|$, pero como $|n| \leq n^{\alpha}$ entonces $|n| \geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^{\alpha}$, ya que $|n_0^{s+1}| = |n_0|^{s+1}$, usando la desigualdad $|n| \leq n^{\alpha}$ y el hecho de que $n \geq n_0^s$ se obtiene que

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

para alguna constante C' que depende de n_0 y de α pero no depende de n, de manera análoga a lo hecho anteriormente tomando raíces n-ésimas y haciendo $N \to \infty$ se obtiene

$$|n| \geq n^{\alpha}, \qquad (2)$$

para todo $n \in \mathbb{N}$.

Luego de (1) y (2) se tiene que $|n| = n^{\alpha}$ para todo $n \in \mathbb{N}$ y en consecuencia se concluye que $|x| = |x|^{\alpha}$ para todo $x \in \mathbb{Q}$ donde $|\cdot|$ es la norma usual en $\mathbb{Q}$.

Caso 2: Para $A = \emptyset$.

Suponga que $|n| \leq 1$ para todo $n \in \mathbb{N}$ y sea n_0 el menor entero positivo tal que $n_0 < n$ y $|n_0| < 1$; n_0 existe porque se asumió que $|\cdot|$ es no trivial. Se debe tener que n_0 es primo, en caso contrario si $n_0 = n_1 n_2$ con $n_1, n_2 < n_0$ entonces $|n_1| = |n_2| = 1$ y $|n_0| = |n_1| \cdot |n_2| = 1$ lo que es contradictorio. Nótese ahora a p como el primo n_0, sea q un primo distinto de p, y se probará que $|q| = 1$. Por contradicción, suponga que $|q| < 1$, y para algún N grande tal que $|q^N| = |q|^N < \frac{1}{2}$. También, para algún M grande de modo que $|p^M| < \frac{1}{2}$. Dado que p^M y q^N son primos relativos, por el Lema de Bezout se pueden encontrar enteros m y n tales que $mp^M + nq^N = 1$, entonces

$$1 = |1| = |mp^M + nq^N| \leq |mp^M| + |nq^N| = |m| \cdot |p^M| + |n||q^N|.$$

Pero $|m| \leq 1$ y $|n| \leq 1$, entonces se obtiene

$$1 \leq |p^M| + |q^N| < \frac{1}{2} + \frac{1}{2} = 1.$$

Lo que es contradictorio, por lo tanto $|q| = 1$.

Sea ahora $a \in \mathbb{N}$, su descomposición en factores primos está dada por $a = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, entonces $|a| = |p_1|^{b_1} |p_2|^{b_2} \cdots |p_r|^{b_r}$, pero el único $|p_i|$ que no es igual a 1 podría ser $|p|$, si alguno de los p_i es p, entonces su correspondiente b_i debe ser $v_p(a) = b_i$ y

$$|a| = |p_1|^{b_1} |p_2|^{b_2} \cdots |p_r|^{b_r} = |p|^{v_p(a)}.$$

Sea $s = |p| < 1$, luego $|a| = s^{v_p(a)}$ para todo $n \in \mathbb{N}$, por la propiedad multiplicativa de normas, la igualdad anterior se extiende a cualquier racional no nulo x, de donde $|x| = s^{v_p(x)} = |x|_p$ para todo $x \in \mathbb{Q} - \{0\}$. Se obtiene que $|\cdot|$ es equivalente a $|\cdot|_p$. □

2.5. $\mathbb{Q}_p$ como completación de $\mathbb{Q}$

En esta sección se probará que el cuerpo $\mathbb{Q}$ no es completo respecto a la norma p-ádica y se construirá la completación de $\mathbb{Q}$, llamada cuerpo de los números p-ádicos.

Definición 2.5.1. *Sean K un cuerpo y $|\cdot|$ una norma en K. Una sucesión (x_n) de elementos de K, se llama sucesión de Cauchy si para todo $\varepsilon > 0$ existe un $n_0 \in \mathbb{N}$ (que depende de ε) tal que para todo $n, m \in \mathbb{N}$, con $n \geq n_0$ y $m \geq n_0$, se verifica que*

$$|x_n - x_m| < \varepsilon.$$

Definición 2.5.2. *Sean K un cuerpo y $|\cdot|$ una norma en K. Se dice que K es completo con respecto a $|\cdot|$ si toda sucesión de Cauchy de elementos de K es convergente a un elemento de K.*

Lema 2.5.1. *Una sucesión de números racionales (x_n) es de Cauchy con respecto a una norma no arquimediana $|\cdot|$ si y sólo si*

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0.$$

Demostración. La implicación de derecha a izquierda es trivial, por definición de sucesión de Cauchy.

Para probar la otra implicación, suponga que $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$. Entonces, para $\varepsilon > 0$ existe

n_0 tal que $|x_{n+1}-x_n|<\varepsilon$ para cada $n\geq n_0$.

Si $n,m\geq n_0$ con $m=n+r>n$, se cumple que

$$\begin{aligned}|x_m-x_n| =&|x_{n+r}-x_{n+r-1}+x_{n+r-1}-x_{n+r-2}+\cdots+x_{n+1}-x_n|,\\ \leq&\text{máx}\{|x_{n+r}-x_{n+r-1}|,|x_{n+r-1}-x_{n+r-2}|,\ldots,|x_{n+1}-x_n|\},\\ <&\varepsilon.\end{aligned}$$

y así (x_n) es de Cauchy. □

Definición 2.5.3. *Si $|\cdot|_p$ es una norma p-ádica en $\mathbb{Q}$, se denota por $\mathscr{C}$ o por $\mathscr{C}_p(\mathbb{Q})$, el conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$ con respecto a $|\cdot|_p$, es decir,*

$$\mathscr{C}=\mathscr{C}_p(\mathbb{Q})=\{(x_n):(x_n)\quad \textit{es una sucesión de Cauchy con respecto a}\quad |\cdot|_p\}.$$

Proposición 1. *$\mathscr{C}_p(\mathbb{Q})$ es un anillo conmutativo unitario, con las operaciones dadas por:*

$$\begin{aligned}(x_n)+(y_n)=&(x_n+y_n),\\ (x_n)\cdot(y_n)=&(x_n\cdot y_n),\end{aligned}$$

donde el cero en $\mathscr{C}_p(\mathbb{Q})$ es (0) y el elemento unitario es (1).

Lema 2.5.2. *La función $f:\mathbb{Q}\to\mathscr{C}$ definida por $f(x)=(x)$ es una inclusión de $\mathbb{Q}$ en $\mathscr{C}$.*

Definición 2.5.4. *Sea $\mathscr{N} \subset \mathscr{C}$ el conjunto*

$$\mathscr{N} = \{(x_n) \in \mathscr{C} : x_n \to 0\} = \{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\},$$

es decir, el conjunto de sucesiones de Cauchy de elementos de $\mathbb{Q}$ que convergen a cero con respecto al valor absoluto $|\cdot|_p$.

Lema 2.5.3. *Si (x_n) es una sucesión de Cauchy tal que $\lim_{n\to\infty} x_n \neq 0$ entonces existen $c > 0$ y $N \in \mathbb{N}$ tal que $|x_n|_p > c$, para $n \geq N$.*

Proposición 2. *$\mathscr{N}$ es un ideal maximal de $\mathscr{C}$.*

Demostración. Para probar que $\mathscr{N}$ es un ideal, se tiene que

1. $(0) \in \mathscr{N}$ pues $\lim_{n\to\infty} |0|_p = 0$.

2. Si $(x_n), (y_m) \in \mathscr{N}$ para $\varepsilon > 0$ existen N_1, N_2 tal que si $n \geq N_1$ y $m \geq N_2$ entonces

$$|x_{n+1} - x_n|_p < \varepsilon \quad \text{y} \quad |y_{m+1} - y_m|_p < \varepsilon.$$

Sea $N = \max\{N_1, N_2\}$. Para $n \geq N$ se tiene

$$\begin{aligned} |x_n - y_n|_p &= |x_n - x_{n-1} + x_{n-1} - \cdots + y_{n+1} - y_n|_p, \\ &\leq \max\{|x_n - x_{n-1}|_p, \cdots |y_{n-1} - y_n|_p\}, \\ &< \varepsilon, \end{aligned}$$

entonces $\lim_{n\to\infty} x_n - y_n = 0$. Así, $((x_n) - (y_n)) \in \mathscr{N}$.

3. Sean $(y_n) \in \mathscr{C}$ y $(x_n) \in \mathscr{N}$, se tiene $(x_n)(y_n) = (x_n y_n)$, luego $|x_n y_n|_p = |x_n|_p |y_n|_p$, dado que $(y_n) \in \mathscr{C}$, entonces existe $k \in \mathbb{R}$ tal que $|y_n|_p \leq k$ para todo $n \in \mathbb{N}$.

   Luego,

$$\lim_{n\to\infty} |x_n|_p |y_n|_p \leq \lim_{n\to\infty} k|x_n|_p = 0 \Rightarrow \lim_{n\to\infty} |x_n y_n|_p = 0.$$

   Así, $(x_n)(y_n) \in \mathscr{N}$.

Para ver que $\mathscr{N}$ es maximal, sea I un ideal de $\mathscr{C}$ tal que $\mathscr{N} \subsetneq I$, se probará que $I = \mathscr{C}$.

Dado que $\mathscr{N} \neq I$ existe $(x_n) \in I$ tal que $\lim_{n\to\infty} x_n \neq$, usando además que (x_n) es una sucesión de Cauchy, por el Lema 2.5.3 existen $c > 0$ y $N \in \mathbb{N}$ tal que si $n \geq N$ entonces $|x_n|_p > c$. Se define (y_n) como

$$y_n = \begin{cases} 0, & \text{si} \quad n < N, \\ \dfrac{1}{x_n}, & \text{si} \quad n \geq N. \end{cases}$$

Se tiene

$$|y_{n+1} - y_n|_p = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right|_p = \frac{|x_n - x_{n+1}|_p}{|x_{n+1}|_p |x_n|_p} < \frac{|x_n - x_{n+1}|_p}{c^2} \quad \text{para} \quad n \geq N.$$

La sucesión (x_n) es de Cauchy y por el Lema 2.5.1 se tiene $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$, por consiguiente

$$\lim_{n\to\infty} |y_{n+1} - y_n|_p \leq \lim_{n\to\infty} \frac{|x_n - x_{n+1}|_p}{c^2} = 0 \Rightarrow \lim_{n\to\infty} |y_{n+1} - y_n|_p = 0.$$

Así, por el Lema 2.5.1 se tiene que (y_n) es una sucesión de Cauchy.

Así, $(x_n)(y_n) \in I$ por ser I un ideal de $\mathscr{C}$. Por otro lado,

$$(x_n y_n) = \begin{cases} 0 & \text{si} \quad n < N, \\ \\ 1 & \text{si} \quad n \geq N. \end{cases}$$

En consecuencia $(1-(x_n y_n)) \in \mathscr{N}$, sea $(z_n) = 1-(x_n y_n)$. Luego $1 = (x_n y_n) + (z_n) \in I$ pues $(z_n), (x_n y_n) \in I$. Así, $I = \mathscr{C}$ y por tanto $\mathscr{N}$ es maximal en $\mathscr{C}$. □

Dado que $\mathscr{N}$ es un ideal maximal del anillo conmutativo con unidad, se tiene que $\mathscr{C}/\mathscr{N}$ es un cuerpo.

Definición 2.5.5. *El cuerpo de los números p-ádicos denotado por $\mathbb{Q}_p$, se define como el cuerpo cociente,*

$$\mathbb{Q}_p = \frac{\mathscr{C}}{\mathscr{N}}.$$

Lema 2.5.4. *Sea $(x_n) \in \mathscr{C}, (x_n) \notin \mathscr{N}$, la sucesión de números reales es eventualmente estacionaria, si, existe $N \in \mathbb{Z}$ tal que para cada $n, m \in \mathbb{N}$ con $m, n \geq N$, entonces*

$$|x_n|_p = |x_m|_p.$$

Demostración. Dado que (x_n) es una sucesión de Cauchy que no converge a cero, por el Lema 2.5.3 existen $c > 0$ y $N_1 \in \mathbb{Z}$ tales que $|x_n|_p \geq c$, $\forall n \geq N_1$. Por otro lado, también existe $N_2 \in \mathbb{Z}$ tal que $|x_n - x_m|_p < c$, $\forall n, m \geq N_2$.

Considere $N = \max\{N_1, N_2\}$ si $n, m \geq N$, entonces:

$$|x_n - x_m|_p < c \leq |x_n|_p \quad \text{y} \quad |x_n - x_m|_p < c \leq |x_m|_p.$$

Luego, si $n, m \geq N$ entonces $|x_n - x_m|_p \leq \max\{|x_n|_p, |x_m|_p\}$. Así, por la propiedad no arquimediana, se tiene que $|x_n|_p = |x_m|_p$ si $n, m \geq N$. □

Definición 2.5.6. *Si $x \in \mathbb{Q}_p$ y (x_n) es cualquier sucesión de Cauchy representante de x, se define*

$$|x|_p = \lim_{n\to\infty} |x_n|_p. \tag{2}$$

Observaciones:

- Dado que el límite (2) existe y no depende de la elección de la sucesión de Cauchy (x_n) en $\mathbb{Q}_p$, es decir, si $(x_n) \sim (\overline{x_n})$ entonces $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |\overline{x_n}|_p$, en efecto, se tiene que:

$$||x_n|_p - |\overline{x_n}|_p|_p \leq |x_n - \overline{x_n}|_p,$$

entonces

$$0 \leq \lim_{n\to\infty} ||x_n|_p - |\overline{x_n}|_p|_p \leq \lim_{n\to\infty} |x_n - \overline{x_n}|_p,$$

y dado que$(x_n) = \overline{x_n} + N$ entonces $(x_n) - (\overline{x_n}) \to 0$ ya que son sucesiones de Cauchy. Así, $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |\overline{x_n}|_p$.

- $|\cdot|_p$ es una norma de $\mathbb{Q}_p$. En efecto, sean $(x_n), (y_n)$ sucesiones representantes de $x, y \in \mathbb{Q}_p$

respectivamente. Entonces $|x|_p = 0$ si y sólo si $\lim_{n\to\infty} |x_n|_p = 0$, que sucede si (x_n) es una sucesión nula, es decir, si $(x_n) = 0$. Por otro lado,

$$\begin{aligned} |x \cdot y|_p &= \lim_{n\to\infty} |x_n \cdot y_n|_p, \\ &= \lim_{n\to\infty} |x_n|_p \cdot |y_n|_p, \\ &= \lim_{n\to\infty} |x_n|_p \cdot \lim_{n\to\infty} |y_n|_p, \\ &= |x|_p \cdot |y|_p. \end{aligned}$$

Finalmente,

$$\begin{aligned} |x+y|_p &= \lim_{n\to\infty} |x_n + y_n|_p, \\ &\leq \lim_{n\to\infty} |x_n|_p + \lim_{n\to\infty} |y_n|_p, \\ &= |x|_p + |y|_p. \end{aligned}$$

Teorema 2.5.1. *Para cada primo p, $|\cdot|_p$ es una norma en $\mathbb{Q}_p$ que extiende a la norma p-ádica de $\mathbb{Q}$. Además,*

1. *Cada elemento de $\mathbb{Q}_p$ es el límite de alguna sucesión de Cauchy de elementos de $\mathbb{Q}$. Por tanto, la imagen de $\mathbb{Q}$ en $\mathbb{Q}_p$ es densa en $\mathbb{Q}_p$ respecto a la no$|\cdot|_p$.*

2. *$\mathbb{Q}_p$ es completo con respecto a la norma $|\cdot|_p$.*

Demostración. 1. Por la Definición 2.5.6 se deduce que cada elemento $x = (x_n) + \mathscr{N} \in \mathbb{Q}_p$ es

el límite de una sucesión de Cauchy (x_n) de elementos de $\mathbb{Q}$ ya que

$$|(x_n)+\mathscr{N}|_p = \lim_{n\to\infty}|x_n|_p \Rightarrow (x_n)+\mathscr{N} = \lim_{n\to\infty}(x_n).$$

2. Sea (x_n) una sucesión de Cauchy de elementos en $\mathbb{Q}_p$. Dado que $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, para cada x_n existe $y^{(n)} \in \mathbb{Q}$ tal que $\lim_{n\to\infty}|x_n-(y^{(n)})|_p = 0$. La sucesión $(y^{(k)})$ es de Cauchy de elementos de $\mathbb{Q}$. Si $\lambda = (y^{(k)})+\mathscr{N}$, se cumple que $\lim_{n\to\infty} x_n = \lambda$.

□

A continuación se enuncia otra forma de identificar los elementos de $\mathbb{Z}_p$ que son llamados enteros p-ádicos.

Definición 2.5.7. *El conjunto de los enteros p-ádicos esta dado por:*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Teorema 2.5.2. *Si $|\cdot|$ es una norma no arquimediana en un cuerpo K entonces se cumple que $|K| = |\tilde{K}|$, donde $\tilde{K}$ es la completación de K.*

Demostración. Sea $x \in \tilde{K}$. Si $x = 0$, $|x| = 0$. Suponga que $x \neq 0$, ya que K es denso en $\tilde{K}$, existe una sucesión de Cauchy (a_n) de elementos de K tal que $\lim_{n\to\infty} a_n = x$. Sin embargo, como $|\cdot|$ es una norma no arquimediana en K entonces

$$|a_n| = |x+(a_n-x)| \leq \text{máx}\{|x|,|a_n-x|\}.$$

Como $|x| \neq 0$ y $|a_n - x|$ se puede hacer arbitrariamente pequeño tomando n suficientemente grande, se tiene que

$$\lim_{n\to\infty} |a_n| = \lim_{n\to\infty} |x|,$$

lo que concluye la prueba. □

Lema 2.5.5. *Si $x \in \mathbb{Q}$ y $|x|_p \leq 1$ entonces para cualquier $i \in \mathbb{N}$ existe un número entero $\alpha \in \mathbb{Z}$ tal que*

$$|\alpha - x|_p \leq \frac{1}{p^i},$$

donde el entero α puede ser elegido del conjunto $\{0, 1, 2, \ldots, p^i - 1\}$.

Demostración. Sea $x = \dfrac{a}{b}$ donde a y b son primos relativos. Puesto que $|x|_p \leq 1$, se sigue que p no divide a b y por lo tanto b y p^i son primos relativos. Así que se pueden encontrar enteros m y n tales que $mb + np^i = 1$. Sea $\alpha = am$. Entonces

$$|\alpha - x|_p = \left|am - \frac{a}{b}\right|_p = \left|\frac{amb - a}{b}\right|_p = \left|\frac{a}{b}(mb - 1)\right|_p = \left|\frac{a}{b}\right|_p |mb - 1|_p,$$

como $|\frac{a}{b}|_p \leq 1$, entonces

$$\left|\frac{a}{b}\right|_p |mb - 1|_p \leq |mb - 1|_p = |np^i|_p = |n|_p |p^i|_p = |n|_p \frac{1}{p^i} \leq \frac{1}{p^i},$$

ya que $n \in \mathbb{Z}$ se tiene que $|n|_p \leq 1$. Por último usando la desigualdad triangular, se puede añadir un múltiplo de p^i al entero α para obtener un entero entre 0 y p^i para que $|\alpha - x|_p \leq p^{-i}$. □

Teorema 2.5.3. *Toda clase de equivalencia a en $\mathbb{Q}_p$ que satisface $|a|_p \leq 1$ tiene exactamente una representación (a_i) de la sucesión de Cauchy tal que:*

1. $a_i \in \mathbb{Z}$, $0 \leq a_i < p^i$ *para* $i = 1, 2, \ldots$.

2. $a_i \equiv a_{i+1} (mod\ p^i)$ *para* $i = 1, 2, \ldots$.

Demostración. Ver la prueba en (López, 2019, Teorema 45) □

Estas propiedades permiten la representación y operación de los números p-ádicos. La sucesión de Cauchy proporciona una forma única de representar los números p-ádicos que cumple con estas propiedades.

Definición 2.5.8. *Cualquier número p-ádico x puede ser escrito en la forma*

$$x = a_{-n_0} p^{-n_0} + a_{-n_0+1} p^{-n_0+1} + \cdots + a_0 + a_1 p + \cdots + a_n p^n + \cdots = \sum_{n \geq -n_0} a_n p^n,$$

donde $a_n \in \mathbb{Z}$ con $0 \leq a_n \leq p-1$, y $a_{-n_0} \neq 0$. Esta representación es única y además $v_p(x) = -n_0$.

Teorema 2.5.4. *El conjunto de los enteros p-ádicos es no contable.*

Demostración. En efecto, tomando cualquier sucesión de números p-ádicos enteros

$$a = \sum_{i=0}^{\infty} a_i p^i; \quad b = \sum_{i=0}^{\infty} b_i p^i; \quad c = \sum_{i=0}^{\infty} c_i p^i; \quad \cdots,$$

Se puede definir un entero p-ádico

$$x = \sum_{i=0}^{\infty} x_i p^i,$$

escogiendo $x_0 \neq a_0$, $x_1 \neq b_1$, $x_2 \neq c_2, \cdots$ construyendo un entero p-ádico distinto de a, b, c, $\cdots$. Esto muestra que la sucesión $a, b, c, \cdots$ no acota el conjunto de números enteros p-ádicos. Por tanto una función de conjunto de números naturales $\mathbb{N}$ en el conjunto de números enteros p-ádicos nunca es sobreyectiva. □

2.5.1. Algunas propiedades de $\mathbb{Q}_p$. En cierta medida, los cuerpos $\mathbb{R}$ y $\mathbb{Q}_p$ se relacionan ya que son la completación de $\mathbb{Q}$, pero con diferentes normas. Se puede verificar que $\mathbb{Q}_p$ no es algebraicamente cerrado, por ejemplo, $x^2 - p = 0$ no tiene solución en $\mathbb{Q}_p$. Considerando que en el caso de que exista $\sqrt{p} \in \mathbb{Q}_p$ será de la forma:

$$\sqrt{p} = a_0 + a_1 p + a_2 p^2 + \cdots,$$

que es equivalente a

$$(a_0 + a_1 p + a_2 p^2 + \cdots)^2 = 0 + 1p,$$

de donde $a_0^2 \equiv 0 (mod\ p)$ y por consiguiente $a_0 = 0$. Luego, $2a_1 a_0 \equiv 1 (mod\ p)$ lo cual es imposible. Cabe aclarar que $\mathbb{Q}_p$ no es comparable con $\mathbb{R}$, pues por ejemplo, $\sqrt{7} \notin \mathbb{Q}_5$ mientras que $i = \sqrt{-1} \in \mathbb{Q}_5$.

En el caso de que exista $\sqrt{7}$ será de la forma

$$\sqrt{7} = a_0 + a_1 5 + a_2 5^2 + \cdots,$$

y se debe tener que

$$(a_0 + a_1 5 + a_2 5^2 + \cdots)^2 = 7 = 2 + 1 \cdot 5,$$

donde $a_0^2 \equiv 2(mod\ 5)$ como esta ecuación no tiene solución se puede afirmar que $\sqrt{7}$ no existe en $\mathbb{Q}_5$. Así mismo como $-1 = (5-1) + (5-1)\cdot 5 + (5-1)\cdot 5^2 + \cdots$ de ahí que $a_0^2 \equiv 4(mod\ 5)$ de donde $a_0 = 2, 3$ por lo tanto $\sqrt{-1} \in \mathbb{Q}_5$.

Teorema 2.5.5. *Toda sucesión infinita de enteros p-ádicos tiene una subsucesión convergente.*

Demostración. (Maldonado, 2015, Teorema 50) □

2.5.2. Orden en $\mathbb{Q}_p$. El cuerpo de los reales $\mathbb{R}$ con la norma usual $|\cdot|$, tiene la propiedad de ser ordenado. Un anillo K se dice ordenado si para sus elementos x la relación $>$ puede ser definida y cumple las siguientes propiedades:

1. Todo entero $x \in K$ satisface una y sólo una de las siguientes relaciones

$$x = 0 \text{ ó } x > 0 \text{ ó } x < 0.$$

2. Si x e y son dos elementos de K que satisfacen $x > 0$ y $y > 0$ entonces $x + y > 0$ y $xy > 0$.

3. Si $x \in K$, $x \neq 0$ entonces $x^2 > 0$.

Un anillo K no puede ser ordenado si contiene un número finito de elementos $x_1, x_2, \ldots, x_n$ distintos de cero que satisfacen $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$. Por ejemplo, el cuerpo de los números complejos, dado que $1^2 + i^2 = 0$.

En particular el anillo $\mathbb{Q}_p$ no es ordenado, por ejemplo para $p = 2$ existe$x \in \mathbb{Q}_p$ con $x \neq 0$ tal que $-7 = 1 - 8 = x^2$ y

$$A_1 = (00\ldots0x),\ A_2 = A_3 = \ldots = A_8 = (00\ldots01),$$

y además

$$A_1^2 + A_2^2 + \cdots + A_8^2 = 0.$$

Si $p \geq 3$ es primo, y denotando por y el número p-ádico para el cual $1 - p = y^2$ y tomando

$$A_1 = (00\ldots0y),\ A_2 = A_3 = \ldots = A_p = (00\ldots01),$$

se tiene que estos números $p$ádicos son todos distintos de cero, pero es evidente que

$$A_1^2 + A_2^2 + \cdots + A_p^2 = 0.$$

Para cada número natural k, se define el conjunto de los enteros p-ádicos divisibles por p^k como :

$$\mathscr{O}_{p^k} = \{z \in \mathbb{Z}_p : |z|_p \leq p^{-k}\}.$$

Este conjunto es un ideal de $\mathbb{Z}_p$.

Puesto que $\mathbb{Q}_p$ no es algebraicamente cerrado; es decir, no todo polinomio con coeficientes en $\mathbb{Q}_p$ tiene sus raíces en $\mathbb{Q}_p$, por lo cual surge el Lema de Hensel como una herramienta importante

para el estudio de las ecuaciones polinómicas sobre los números p-ádicos. Esto nos proporciona una forma de encontrar raíces aproximadas de estos polinomios.

Teorema 2.5.6 (**Lema de Hensel**). *Sea* $F(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ *un polinomio cuyos coeficientes son enteros p-ádicos. Sea*

$$F'(x) = b_1 + 2b_2x + 3b_3x^2 + \cdots + nb_nx^{n-1},$$

la derivada de $F(x)$. *Suponga que* $\tilde{a_0}$ *es un entero p-ádico que satisface que*

$$F(\tilde{a_0}) \equiv 0(mod\ p) \quad y \quad F'(\tilde{a_0}) \not\equiv 0(mod\ p).$$

Entonces existe un único entero p-ádico a tal que $F(a) = 0$ *y* $a \equiv \tilde{a_0}(mod\ p)$.

Demostración. Para verificar la existencia de a construyendo su expansión p-ádica, se toma $a = b_0 + b_1p + b_2p^2 + \cdots$ inductivamente sobre k. En el paso k-ésimo de inducción, se encuentra $a_k = b_0 + b_1p + \cdots + b_kp^k$ la k-ésima aproximación de a. Cada a_k no será una verdadera raíz de $F(x)$ pero será solo una raíz módulo p^{k+1}, es decir, $F(a_k) \equiv 0(mod\ p^{k+1})$ para todo k. Cuando $k \to \infty$ se obtendrá a, la verdadera raíz para F.

Es decir, se probará por inducción sobre k que:

Para algún $n \geq 0$ existe un entero p-ádico de la forma $a_k = b_0 + \cdots + b_kp^k$ con $b_i \in \{0, \cdots, p-1\}$ tal que

$$F(a_k) \equiv 0(mod\ p^{k+1}) \quad \text{y} \quad a_k \equiv \tilde{a_0}(mod\ p).$$

Sea b_0 el primer dígito p-ádico de $\tilde{a_0}$, se tiene que $a_0 \equiv \tilde{a_0}(mod\ p)$ y $F(a_0) \equiv 0(mod\ p)$.

Ahora, sea $a_k = a_{k-1} + b_k p^k$ para algún b_k que satisface $0 \leq b_k < p$ y expande a $F(a_k)$, ignorando términos divisibles por p^{k+1}

$$\begin{aligned} F(a_k) =& F(a_{k-1} + b_k p^k) = \sum_{i=0}^{n} c_i (a_{k-1} + b_k p^k)^i, \\ =& \sum_{i=0}^{n} c_i (a_{k-1}^i + i a_{k-1}^{k-1} b_k p^k + \text{términos divisibles por } p^{k+1}), \\ \equiv& F(a_{k-1}) + b_k p^k F'(a_{k-1})(mod\ p). \end{aligned}$$

Dado que $F(a_{k-1}) \equiv 0(mod\ p^k)$ por hipótesis de inducción

$$F(a_k) \equiv \alpha_k p^k + b_k p^k F'(a_{k-1})(mod\ p),$$

para algún entero $\alpha_k \in \{0, 1, \cdots, p-1\}$. Así que la ecuación para el b_k desconocido es

$$\alpha_K + b_k F'(a_{k-1})(mod\ p).$$

Que se resuelve siempre que $F'(a_{k-1}) \not\equiv 0(mod\ p)$ que se cumple, pues $a_{k-1} \equiv \tilde{a_0}(mod\ p)$, de modo que

$$F'(a_{k-1}) \equiv F'(\tilde{a_0}) \not\equiv 0(mod\ p).$$

Dividiendo por $F'(a_{k-1})$ se puede encontrar el b_k

$$b_k = \frac{-\alpha_k}{F'(a_{k-1})}(mod\ p),$$

y puesto que $F(a_k) \equiv \alpha_k p^k + b_k p^k F'(a_{k-1})(mod\ p)$. Por lo tanto $F(a_k) \equiv 0(mod\ p^{k+1})$ lo que completa la inducción.

Ahora, sea $a = \tilde{a_0} + b_1 p + b_2 p^2 + \cdots$ se da, ya que $F(a) = 0$ ya que para todo k se tiene

$$F(a) \equiv F(a_k) \equiv 0(mod\ p^{k+1}).$$

La unicidad de a se sigue de la unicidad de las sucesiones $\{a_k\}$. □

Ejemplo 2.5.1. *1. Sea $f(x) = x^3 - 2 \in \mathbb{Z}_5[x]$, y tomando $a_0 = 3$. Se tiene que $f'(x) = 3x^2$, por lo tanto*

$$f(3) = 3^2 - 2 = 27 - 2 = 25 \equiv 0(mod\ 5),$$

y

$$f'(3) = 3(3)^2 = 3(9) = 27 \not\equiv 0(mod\ 5).$$

Entonces, por el Lema de Hensel, existe un entero 5-ádico a tal que $a^3 = 2$, es decir, $a = \sqrt[3]{2}$. Si $a \equiv 3(mod\ 5)$, entonces $a = 3 + b_1 \cdot 5 + b_2 \cdot 5^2 + \cdots$ con $b_i \in \{0,1,2,3,4\}$.

2. Sea $f(x) = x^2 + 2 \in \mathbb{Q}_3[x]$, tomando $a_0 = 1$, $f'(x) = 2x$. Así, $f(1) = 3 \equiv 0(mod\ 3)$ y $f'(1) = 2 \not\equiv (mod\ 3)$; luego por el Lema de Hensel, $f(x)$ tiene una raíz en $\mathbb{Q}_3$, es decir $\sqrt{-2} \in \mathbb{Q}_3$.

3. *Sea* $f(x) = x^2 - 2 \in \mathbb{Q}_3[x]$. *Dado que* $f(1) \equiv 2(mod\ 3)$ *y* $f(2) \equiv 2(mod\ 3)$ *entonces no existe un entero* 3*-ádico a tal que* $f(a) = 0$, *por lo tanto* $\sqrt{2} \notin \mathbb{Q}_3$.

4. *Sea* $f(x) = x^2 - 6 \in \mathbb{Q}_5[x]$. *Tomando* $a_0 = 1$ *se cumple que* $f(1) = 1 - 6 = -5 \equiv 0(mod\ 5)$ *y* $f'(1) = 2 \not\equiv 0(mod\ 5)$, *de este modo, por el Lema de Hensel existe un entero* 5*-ádico a tal que* $a^2 = 6$. *Así* $\sqrt{6}$ *pertenece a* $\mathbb{Z}_5$.

5. *Sea* $f(x) = x^3 + 1 \in \mathbb{Q}_3[x]$, *dado que* $f'(x) = 3x \equiv 0(mod\ 3)$, *entonces no existen raíces cúbicas de la unidad en* $\mathbb{Q}_3$.

6. *Sea* $f(x) = x^2 + 1 \in \mathbb{Q}_5[x]$, *entonces* $f'(x) = 2x$. *Tomando* $a_0 = 2$, *se tiene que:*

$$f(2) = 5 \equiv 0(mod\ 5),$$

y

$$f'(2) = 4 \not\equiv 0(mod\ 5).$$

Aplicando entonces el Lema de Hensel, existe un entero 5*-ádico a tal que* $a^2 = -1$.

Teniendo en cuenta que $a \equiv 2(mod\ 5)$ *entonces a tendrá una expansión de la forma:*

$$a = 2 + b_1 \cdot 5 + b_2 \cdot 5^2 + \cdots,$$

con enteros $b_i \in \{0, 1, \ldots, 4\}$. *Una de las formas de calcular los* b_i*'s es la siguiente:*

- *Sea* $a_1 = 2 + b_1 \cdot 5$, *dado que* $b_0 = 2$, *para u entero, se resuelve* $f(b_0) = u \cdot 5(mod\ 5^2)$,

es decir, $5 \equiv u \cdot 5 (mod\ 5^2)$*, de ahí se tiene que* $1 \equiv u (mod\ 5)$ *así* $u = 1$*. Se desea que se satisfaga* $f(a_1) \equiv 0 (mod\ 5^2)$*, lo cual ocurre si*

$$\begin{aligned} u \cdot 5 + f'(b_0) \cdot b_1 \cdot 5 &\equiv 0 (mod\ 5^2), \\ u + f'(b_0) b_1 &\equiv 0 (mod\ 5), \\ 1 + 4 \cdot b_1 &\equiv 0 (mod\ 5). \end{aligned}$$

Por lo tanto, $b_1 = 1$ *así* $a_1 = 2 + 1 \cdot 5 = 7$ *y se tiene que* $f(7) = 7^2 + 1 = 50 \equiv 0 (mod\ 5)$ *y* $f'(7) = 7 \cdot 2 = 14 \equiv 4 (mod\ 5)$.

- *Ahora, tomando* $a_2 = 2 + 1 \cdot 5 + b_2 \cdot 5^2$ *y haciendo el proceso anterior, se tiene que* $f(a_1) \equiv u \cdot 5^2 (mod\ 5^3)$, $50 \equiv u \cdot 5^2 (mod\ 5^3)$*, de donde se tiene que* $2 \equiv u \cdot (mod\ 5)$ *así* $u = 2$*. Luego,* $f(a_2) \equiv 0 (mod\ 5^3)$ *lo que sucederá si*

$$\begin{aligned} u \cdot 5^2 + f'(a_1) b_2 \cdot 5^2 &\equiv 0 (mod\ 5^3), \\ 2 + 14 \cdot b_2 &\equiv 0 (mod\ 5), \end{aligned}$$

de donde se obtiene que $b_2 = 2$*, de esta forma,* $a_2 = 2 + 1 \cdot 5 + 2 \cdot 5^2$ *y* $f(a_2) = 3250 \equiv 0 (mod\ 5)$ *y* $f'(a_2) = 114 \equiv 4 (mod\ 5)$.

Este proceso se repite hasta hallar la raíz.

7. *Considere* $f(x) = x^2 + 7 \in \mathbb{Q}_{11}[x]$*. Se desea encontrar a tal que* $a^2 = -7$*. La expansión*

11-*ádica de a es de la forma*

$$a = a_0 + a_1 \cdot 11 + a_2 \cdot 11^2 + a_3 \cdot 11^3 + \cdots$$

y la expresión 11-*ádica de* -7 *es:*

$$-7 = 4 + 10 \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + \cdots \tag{3}$$

Sumando 7 *a (3) se obtiene*

$$\begin{aligned} 7 + (-7) =& 7 + (4 + 10 \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + \cdots) \\ =& 11 + 10 \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + \cdots \\ =& (1 + 10) \cdot 11 + 10 \cdot 11^2 + \cdots \\ =& 11 \cdot 11 + 10 \cdot 11^2 + \cdots \\ & \vdots \\ =& 0. \end{aligned}$$

Entonces, se quiere resolver la siguiente ecuación:

$$(a_0 + a_1 \cdot 11 + a_2 \cdot 11^2 + a_3 \cdot 11^3 + \cdots)^2 = 4 + 10 \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + \cdots .$$

Así, mirando las congruencias módulo 11*, se tiene* $a_0^2 \equiv 4 (mod\ 11)$ *entonces* $a_0 = 2$ *o* 9*,*

tomando $a_0 = 2$ *y se resuelve como una congruencia módulo* 11^2*:*

$$\begin{aligned}(a_0 + a_1 \cdot 11)^2 &\equiv 4 + 10 \cdot 11 (mod\ 11^2),\\ a_0^2 + 2a_0a_1 \cdot 11 &\equiv 4 + 10 \cdot 11 (mod\ 11^2),\\ 4 + 4a_1 \cdot 11 &\equiv 4 + 10 \cdot 11 (mod\ 11^2),\\ 4a_1 \cdot 11 &\equiv 10 \cdot 11 (mod\ 11^2),\\ 4a_1 &\equiv 10 (mod\ 11).\end{aligned}$$

Multiplicando ambas partes por 3 *se tiene que* $a_1 \equiv 8(mod\ 11)$*, así* $a_1 = 8$*. Continuando módulo* 11^3 *se tiene que:*

$$\begin{aligned}(a_0 + a_1 \cdot 11 + a_2 \cdot 11^2)^2 &\equiv 4 + 10 \cdot 11 + 10 \cdot 11^2 (mod\ 11^3),\\ a_0^2 + 2a_0a_1 \cdot 11 + (2a_0a_2 + a_1^2) \cdot 11^2 &\equiv 4 + 10 \cdot 11 + 10 \cdot 11^2 (mod\ 11^3),\\ 4 + 32 \cdot 11 + (4a_2 + 64) \cdot 11^2 &\equiv 4 + 10 \cdot 11 + 10 \cdot 11^2 (mod\ 11^3),\\ 22 \cdot 11 + (4a_2 + 64) \cdot 11^2 &\equiv 10 \cdot 11^2 (mod\ 11^3),\\ 2 \cdot 11^2 + 4a_2 \cdot 11^2 + 64 \cdot 11^2 &\equiv 10 \cdot 11^2 (mod\ 11^3),\\ 4a_2 \cdot 11^2 &\equiv -56 \cdot 11^2 (mod\ 11^3),\\ 4a_2 &\equiv -56 \equiv 10 (mod\ 11).\end{aligned}$$

Multiplicando por 3 *se tiene que* $a_2 \equiv 30 \equiv 8 (mod\ 11)$*, entonces* $a_2 = 8$.

De esta manera, se encuentra cada coeficiente de la expresión 11*-ádica de* $a = 2 + 8 \cdot 11 + 8 \cdot 11^2 + \cdots$.

A continuación se presenta otro método iterativo, llamado *método de Newton*. Este refina el Lema de Hensel, dado que partiendo de un entero p-ádico con ciertas características, es posible construir una sucesión que converge a una raíz p-ádica de un polinomio.

Teorema 2.5.7 (Método de Newton). *Sea* $f(x) \in \mathbb{Z}_p[x]$*. Suponga que* a_0 *es un entero p-ádico que satisface:*

$$\left| \frac{f(a_0)}{f'(a_0)^2} \right|_p < r < 1, \quad r \neq 0.$$

Entonces a_0 *puede refinarse a una raíz de* $f(x)$*. Para ser más preciso, la sucesión*

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)},$$

converge a una raíz entera p-ádica a de $f(x)$*. Además, se cumple que:*

$$|a - a_0|_p \leq \left| \frac{f(a_0)}{f'(a_0)} \right|_p < r < 1.$$

Ejemplo 2.5.2. *1. Sea* $f(x) = x^3 + 2x^2 - 5x - 6$*, se tiene que* $f'(x) = 3x^2 + 4x - 5$*. Analizando sobre* $\mathbb{Q}_2$ *se toma a* $a_0 = 1$*, entonces* $f(1) = -8$ *y* $f'(1) = 2$*, entonces*

$$\left| \frac{f(a_0)}{f'(a_0)^2} \right|_2 = \left| \frac{-8}{4} \right|_2 = \frac{1}{2} < 1.$$

Por lo tanto, se puede aplicar el método de Newton:

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = 1 - \frac{-8}{2} = 5.$$

Así, $f(5) = 144$ *y* $f'(5) = 90$.

$$a_2 = a_1 - \frac{f(a_1)}{f'(a_1)} = 5 - \frac{144}{90} = \frac{17}{5}.$$

De aquí, $f(\frac{17}{5}) = \frac{4928}{125}$. *Se sigue el procedimiento sucesivamente.*

2. *Sea* $f(x) = x^3 - 2$, *tomando* $a_0 = 3$ *en* $\mathbb{Q}_5$. *Se sabe que* $f'(x) = 3x^2$, *entonces* $f(3) = 25$ *y* $f'(3) = 27$. *Por lo cual se tiene que :*

$$\left|\frac{25}{27^2}\right|_5 = \frac{\frac{1}{5^2}}{\frac{1}{5^0}} = \frac{1}{25} < 1,$$

y se puede aplicar el método de Newton, así:

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = 3 - \frac{25}{27} = \frac{56}{27},$$

Así, $f\left(\frac{56}{27}\right) = \frac{136250}{19683}$ *y* $f'\left(\frac{56}{27}\right) = \frac{3136}{243}$.

$$a_2 = a_1 - \frac{f(a_1)}{f'(a_1)} = \frac{56}{27} - \frac{\frac{136250}{19683}}{\frac{3136}{243}} = \frac{195299}{127008}.$$

De aquí, $f\left(\frac{195299}{127008}\right) = 1.635857277.$

Es claro que el Lema de Hensel proporciona un método para hallar las raíces *p*-ádicas de polinomios con coeficientes enteros *p*-ádicos. Para utilizar este método es necesario iniciar el proceso ya que el resto es resolver congruencias lineales. Al saber como hallar las raíces de un polinomio *p*-ádico, se pueden definir las extensiones *p*-ádicas, (Mas Huamán, 2015), (Wiswell, 2011), (Jena, 2016), (Turner, 2011).

3. Extensiones p-ádicas

Dado un cuerpo $K \supset \mathbb{Q}_p$, con métrica no arquimediana $|\cdot|_K$, se dice que K es una extensión p-ádica si cumple que $|x|_K = |x|_p$ para todo $x \in \mathbb{Q}_p$. Dado que la única norma que se usará es la p-ádica o sus extensiones, a partir de ahora se usará $|x|$ en vez de $|x|_p$.

Sea K una extensión finita de grado n de $\mathbb{Q}_p$. La norma de u, denotada por $N_{K/\mathbb{Q}_p}(u)$, es el número p-ádico

$$N_{K/\mathbb{Q}_p}(u) = \prod_{i=1}^{n} \sigma_i(u),$$

donde σ_i son distintos $\mathbb{Q}_p$-monomorfismo de K en una clausura algebraica de $\mathbb{Q}_p$.

En este trabajo, se mostrará el caso en que u es raíz del polinomio irreducible

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}_[x],$$

la norma de u está dada por

$$N_{K/\mathbb{Q}_p}(u) = \prod_{i=1}^{n} u_i,$$

donde u_i son los conjugados de $u = u_1$ sobre $\mathbb{Q}_p$.

La norma algebraica $N_{K/\mathbb{Q}_p}$ cumple las siguientes propiedades, para $u, v \in K$:

- $N_{K/\mathbb{Q}_p}(u \cdot v) = N_{K/\mathbb{Q}_p}(u) \cdot N_{K/\mathbb{Q}_p}(v)$ llamada la propiedad multiplicativa.
- Para un cuerpo intermedio E, se tiene $N_{E/\mathbb{Q}_p}(N_{K/E}(u)) = N_{K/\mathbb{Q}_p}(u)$.

- $N_{K/\mathbb{Q}_p}(a) = a^n$, para $a \in \mathbb{Q}_p$ y n es el grado de la extensión.

Teorema 3.0.1. *Sea K una extensión finita de grado n sobre $\mathbb{Q}_p$, entonces:*

$$|x|_K = |N_{K/\mathbb{Q}_p}(x)|_p^{\frac{1}{n}},$$

define una norma sobre K que extiende a la norma definida en $\mathbb{Q}_p$.

Demostración. Sean $x, y \in K$, se tiene que:

1. $|x| = 0$ si $N_{K/\mathbb{Q}_p}(x) = 0$; lo que sucederá si la multiplicación por x no es invertible, y dado que K es campo, esto pasa solo si $x = 0$.

2. Puesto que $N_{K/\mathbb{Q}_p}(x \cdot y) = N_{K/\mathbb{Q}_p}(x) \cdot N_{K/\mathbb{Q}_p}(y)$ entonces $|x \cdot y| = |x| \cdot |y|$.

3. Si $x \in \mathbb{Q}_p$ entonces $N_{K/\mathbb{Q}_p}(x) = x^n$, luego $|x| = |x^n|_p^{\frac{1}{n}} = |x|_p$.

4. Además la norma es no arquimediana, ver (Q. Gouv$\widehat{e}$a, 2003, Teorema 5.3.5).

□

Esta norma cumple que el conjunto de valores no nulos de $|\cdot|_K$ en K es subconjunto de $\{p^{\frac{m}{n}} : m \in \mathbb{Z}\}$, donde $n = [K : \mathbb{Q}_p]$.

Ejemplo 3.0.1. *1. La completación $\mathbb{R}$ de $\mathbb{Q}$ con el valor absoluto usual tiene una extensión algebraica, llamada $\mathbb{C}$. Así el valor absoluto usual $|\cdot|$ en $\mathbb{R}$ tiene una única extensión sobre $\mathbb{C}$, dada por*

$$|\alpha|_{\mathbb{C}} = |N_{\mathbb{C}/\mathbb{R}}(\alpha)|^{\frac{1}{2}} = |\alpha \cdot \overline{\alpha}|^{\frac{1}{2}}.$$

Dada la extensión $[K:\mathbb{Q}_p]=n$ se pueden definir los conjuntos:

$$\mathbb{Z}_K=\{x\in K:|x|_K\leq 1\},$$

y

$$\mathscr{O}_K=\{x\in K:|x|_K<1\}.$$

Entonces $\mathbb{Z}_K$ es el anillo de enteros de K y $\mathscr{O}_K$ un ideal maximal de éste. En efecto, sea $a\in\mathbb{Z}_K$ y $b\in\mathscr{O}_K$, entonces $|a\cdot b|_p=|a|_p\cdot|b|_p<1$, así $a\cdot b\in\mathscr{O}_K$, por lo tanto $\mathscr{O}_K$ es un grupo aditivo de $\mathbb{Z}_K$, lo cual implica que $\mathscr{O}_K$ es un ideal.

Suponga ahora que M es un ideal maximal tal que $\mathscr{O}_K\subset M\subset\mathbb{Z}_K$. Luego, existe $a\in\mathbb{Z}_K$ tal que $a\in M$ pero $a\notin\mathscr{O}_K$. Por lo tanto, $|a|_p=1$ así $|\frac{1}{a}|_p=1$, es decir $\frac{1}{a}\in\mathbb{Z}_K$, por consiguiente $a\cdot\frac{1}{a}\in M$, que es una contradicción puesto que $M\neq\mathbb{Z}_K$, entonces $\mathscr{O}_K$ es el único ideal maximal en $\mathbb{Z}_K$. Así el anillo cociente $\mathbb{Z}_K/\mathscr{O}_K$ es un cuerpo, llamado el cuerpo de las clases residuales de K.

El grado de $\mathbb{Z}_K/\mathscr{O}_K$ sobre $\mathbb{Z}_p/p\mathbb{Z}_p=\mathbb{F}_p$ es llamado el *grado de las clases residuales* de K y se denota por f, es decir:

$$f=[\mathbb{Z}_K/\mathscr{O}_K:\mathbb{Z}_p/p\mathbb{Z}_p].$$

Sea $n=[K:\mathbb{Q}_p]$ entonces $|K^*|_K=\{|x|_K:x\in K^*\}$ es un subgrupo cíclico del grupo multiplicativo generado por $p^{-1/n}$. Así $|K^*|_K$ es generado por p^{-1/e_k} para algún divisor positivo e_k de n.

A e_K se le conoce como el *índice de ramificación* de la extensión, este índice también queda definido por el índice de grupos $[|K^*| : |\mathbb{Q}_p^*|]$.

Se dice que $\pi \in \mathbb{Z}_K$ es un *uniformizador* si se tiene $\pi \in \mathscr{O}_K$ y $\pi \notin \mathscr{O}_K^2$, es decir, es el elemento generador de $\mathscr{O}_K$.

Ejemplo 3.0.2. *1. En $\mathbb{Z}_p$, el elemento $\pi = p$ es un uniformizador. Al igual que en los p-ádicos, cada $x \in \mathbb{Z}_K$ se puede escribir como:*

$$x = a_0 + a_1\pi + a_2\pi^2 + \cdots,$$

con $a_i \in \mathbb{Z}_K/\mathscr{O}_K$.

Lema 3.0.1. *Sean $a_1, a_2, \ldots, a_n \in K$. Si $|a_1| > |a_i|$ para $i = 2, \ldots, n$, entonces se cumple*

$$|a_1| = |a_1 + \cdots + a_r|.$$

Demostración. Dado que todo triángulo con norma p-ádica es isósceles y $|a_1| > |a_2|$ obliga a tener que $|a_1 + a_2| = |a_1| > |a_3|$, de la misma manera se tiene que $|a_1 + a_2 + a_3| = |a_1| > |a_4|$, luego de un número finito de iteraciones se llega a $|a_1| = |a_1 + \cdots + a_r|$. □

Lema 3.0.2. *Sean $x_1, \ldots, x_f \in \mathbb{Z}_K$ tales que $x_1 + \mathscr{O}_K, \ldots, x_f + \mathscr{O}_K$ son linealemente independientes sobre $\mathbb{F}_p$, y sean $a_1, a_2, \ldots, a_f \in \mathbb{Q}_p$. Entonces*

$$|a_1x_1 + \cdots + a_fx_f| = \max_r |a_r|_p.$$

Demostración. Si $a_r = 0$ para todo $r \in \{1,\dots,f\}$, ya está.

Si $|a_1| = \max_r |a_r|_p$ y definiendo $b_r = \dfrac{a_r}{a_1}$ para $r \in \{1,\dots,f\}$, entonces $|b_r| \leq 1$ y $b_1 = 1$, $|x_1 + b_2x_2 \cdots + b_fx_f| = 1$.

En efecto, dado que $x_1 + b_2x_2 \cdots + b_fx_f \in \mathbb{Z}_K$ se tiene que $|x_1 + b_2x_2 \cdots + b_fx_f| \leq 1$, si la desigualdad fuera estricta, entonces $x_1 + b_2x_2 \cdots + b_fx_f \in \mathscr{O}_K$ así

$$(x_1 + \mathscr{O}_K) + (b_2 + \mathscr{O}_K)(x_2 + \mathscr{O}_K) + \cdots + (b_f + \mathscr{O}_K)(x_f + \mathscr{O}_K) = \mathscr{O}_K,$$

lo que implica que $\mathscr{O}_K$ es combinación lineal de los $x_i + \mathscr{O}_K$ que es una contradicción. □

Lema 3.0.3. *Sea π un uniformizador de $\mathbb{Z}_K$ con $|\pi| = p^{-1/e}$ y sean $x_1,\dots,x_f$ elementos de $\mathbb{Z}_K$ tales que $\overline{x_1},\dots,\overline{x_f}$ forman una base de $\mathbb{Z}_K/\mathscr{O}_K$ sobre $\mathbb{F}_p$. Entonces $\mathbb{Z}_K$ es un $\mathbb{Z}_p$-módulo libre con base*

$$\{x_i\pi^j : i = 1,\dots,f;\ j = 0,\dots,e-1\}.$$

Por definición, lo anterior significa que todo $x \in \mathbb{Z}_K$ puede ser expresado de manera única como

$$x = \sum_{j=0}^{e-1}\sum_{i=0}^{f} a_{ij}x_i\pi^j, \qquad con \qquad a_{ij} \in \mathbb{Z}_p.$$

Demostración. Sea $x \in \mathbb{Z}_K$ distinto de cero, dado que $|p^r\pi^j| = |\pi^{er+j}|$, entonces $er + j$ recorre todos los enteros no negativos mientras $r \geq 0$ y $j \in \{0,\dots,e-1\}$.

Por lo tanto $|p^r\pi^j|$ asume todos los valores posibles de la norma $|\cdot|_K$ menores o iguales a 1. Así para algún r y j se cumple $|x| = |p^r\pi^j|$.

En particular, para $y = \dfrac{x}{p^r \pi^j}$ se tiene $|y| = 1$. Luego, en el espacio vectorial $\mathbb{Z}_K/\mathscr{O}_K$ sobre $\mathbb{F}_p$ existen $a_r \in \mathbb{Z}_p$, no todos en $\mathscr{O}_K$ tales que:

$$\begin{aligned} y + \mathscr{O}_K =& (a_1 + \mathscr{O}_K)(x_1 + \mathscr{O}_K) + \cdots + (a_f + \mathscr{O}_K)(x_f + \mathscr{O}_K), \\ =& (a_1 x_1 + \cdots + a_f x_f) + \mathscr{O}_K, \end{aligned}$$

es decir,

$$|y - (a_1 x_1 + \cdots + a_f x_f)| < 1,$$

por lo tanto,

$$|x - (a_1 x_1 + \cdots + a_f x_f) p^r \pi^j| < |p^r \pi^j|.$$

Si $z = x - (a_1 x_1 + \cdots + a_f x_f) p^r \pi^j$, se tiene, $x = (a_1 x_1 + \cdots + a_f x_f) p^r \pi^j + z$ de donde se cumple $|z| < |p^r \pi^j|$.

Este resultado, se usará reiteradamente para construir una serie convergente.

Sea $w \in \mathbb{Z}_K$ no nulo tal que $|w| \leq 1$. Por lo ya visto, w se puede escribir como:

$$w = a_{001} x_1 + \cdots + a_{00f} x_f + w_1,$$

donde $a_{001} \in \mathbb{Z}_p$ y $|w_1| < 1$. Así $|w_1| \leq |\pi|$ y se continua con:

$$w_1 = (a_{011} x_1 + \cdots + a_{01f} x_f)\pi + w_2,$$

donde $|w_2| \leq |\pi|$ y así $|w_2| < |\pi^2|$. Al repetir $e-1$ veces se obtiene:

$$w_{e-1} = (a_{0e-1,1}x_1 + \cdots + a_{0e-1,f}x_f)\pi^{e-1} + w_e,$$

donde $|w_e| \leq |\pi^e| = |p|$. Luego

$$w_e = (a_{101}x_1 + \cdots + a_{10f}x_f)p + w_{e+1},$$

donde $|w_{e+1}| \leq |p\pi|$.

En general, w se puede escribir como

$$w = \sum_{r,j}^{m} (a_{rj1}x_1 + \cdots + a_{rjf}x_f)p^r\pi^j + z_m.$$

Al tomar el límite cuando $m \to \infty$ se tiene

$$w = \sum_{r,j} (a_{rj1}x_1 + \cdots + a_{rjf}x_f)p^r\pi^j,$$

donde, $r = 0, 1, \ldots$ y $j = 0, 1, \ldots, e-1$, por lo tanto,

$$w = \sum_{j=0}^{e-1} \left((\sum_r a_{rj1}p^r)x_1 + \cdots + (\sum_r a_{rjf}p^r)x_f \right) \pi^j.$$

Las series $a_{rjf}p^r$ convergen puesto que $a_{rjf} \in \mathbb{Z}_p$ y $|a_{rjf}| \to 0$. □

Teorema 3.0.2. *Sea K una extensión finita de $\mathbb{Q}_p$ con índice de ramificación $e = e_K$ y clase residual $f = f_K$. Entonces se satisface $[K : \mathbb{Q}_p] = e \cdot f$.*

Demostración. Sean $x_1, \ldots, x_f \in \mathbb{Z}_K$ tales que $x_1 + \mathcal{O}_K, \ldots, x_f + \mathcal{O}_K$ son linealmente independientes sobre $\mathbb{F}_p$ y $y_1, \ldots, y_e \in K^*$ elementos distintos de modo que:

$$|y_1||\mathbb{Q}_p^*|, \ldots, |y_e||\mathbb{Q}_p^*|,$$

sean las clases laterales multiplicativas distintas.

Se quiere probar que los $x_r y_s$ con $r = 1, \ldots, f$ y $s = 1, \ldots, e$, son linealmente independientes sobre $\mathbb{Q}_p$. Así, $e \cdot f \leq n = dim_{\mathbb{Q}_p} K$.

Suponiendo,

$$\sum_{rs} c_{rs} x_r y_s = 0,$$

para $c_{rs} \in \mathbb{Q}_p$. Al agrupar, $\sum_s \left(\sum_r c_{rs} x_r\right) y_s = 0$. Por el Lema 3.0.2 para cada s fijo

$$\left|\left(\sum_r c_{rs} x_r\right) y_s\right| = \left|\sum_r c_{rs} x_r\right| |y_s| = \max_r |c_{rs}||y_s|.$$

Como las clases laterales $|y_1||\mathbb{Q}_p^*|, \ldots, |y_e||\mathbb{Q}_p^*|$ toman valores disjuntos, las valuaciones $\max_r |c_{rs} y_s|$ serán distintas y por el Lema 3.0.1 se tiene

$$0 = \left|\sum_s \sum_r c_{rs} x_r y_s\right| = \max_s \max_r |c_{rs}| \cdot |y_s|.$$

La única posibilidad es $c_{rs} = 0$, para todo r, s. Por consiguiente $e \cdot f \leq n$, y $e \cdot f \geq n$ se obtiene del Lema 3.0.3. □

Para una extensión finita K de $\mathbb{Q}_p$:

- Si $e = 1$, se dice que la extensión K no ramifica.
- Si $e = n$, se dice que la extensión K ramifica totalmente.
- Si p no divide a e, se dice que la extensión K ramifica débilmente.
- Si $e = p^k$ para algún entero k entero positivo, se dice que la extensión K ramifica salvajemente.

Ejemplo 3.0.3. *1. Sea $K = \mathbb{Q}_3(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}_3\}$. Se tiene que $\sqrt{3}$ es una de las raíces de $f(x) = x^2 - 3$, donde $f(x)$ es irreducible y $\sqrt{3} \notin \mathbb{Q}_3$.*

Luego la norma de $\sqrt{3}$ esta dada por:

$$|\sqrt{3}|_{\mathbb{Q}_3(\sqrt{3})} = |N_{\mathbb{Q}_3(\sqrt{3})/\mathbb{Q}_3}(\sqrt{3})|_3^{\frac{1}{2}} = |3|_3^{\frac{1}{2}} = 3^{-\frac{1}{2}}.$$

En general, para $a, b \in \mathbb{Q}_3$ se tiene que:

$$\begin{aligned} |a + b\sqrt{3}|_3 &= |N_{\mathbb{Q}_3(\sqrt{3})/\mathbb{Q}_3}(a + b\sqrt{3})|_3^{\frac{1}{2}}, \\ &= |a^2 - 3b^2|_3^{\frac{1}{2}}, \\ &= \text{máx}(|a|_3, 3^{-\frac{1}{2}}|b|_3). \end{aligned}$$

Así,

$$\mathbb{Z}_K = \{a + b\sqrt{3} : a, b \in \mathbb{Z}_3\},$$
$$\mathscr{O}_K = \{a + b\sqrt{3} : a \in 3\mathbb{Z}_3, b \in \mathbb{Z}_3\} = \sqrt{3}\mathbb{Z}_K,$$
$$\mathbb{Z}_K/\mathscr{O}_K \cong \mathbb{Z}_3/3\mathbb{Z}_3 = \mathbb{F}_3.$$

Por lo tanto, para este caso particular se tiene que $e_K = 2$ *y* $f_K = 1$*, esto implica que K es total y mansamente ramificada.*

Lema 3.0.4. *Sea* $f(x) \in \mathbb{Z}_p[x]$ *un polinomio mónico cuyo módulo p es irreducible en* $\mathbb{F}_p$*. Entonces* $f(x)$ *es irreducible sobre* $\mathbb{Q}_p$*.*

Demostración. Si $f(x)$ se factoriza sobre $\mathbb{Q}_p$ entonces $f(x)$ se factoriza sobre $\mathbb{Z}_p$. Luego haciendo reducción módulo p a la factorización, ésta da una factorización sobre $\mathbb{F}_p$, lo que contradice la hipótesis. □

3.1. Propiedades de las extensiones finitas de $\mathbb{Q}_p$

Sea K una extensión finita de $\mathbb{Q}_p$ de grado n. Se denota por $|\cdot|_p$ el valor absoluto p-ádico y la única extensión de valor absoluto en K dada por:

$$|x|_p = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}.$$

Recordando que el valor absoluto p-ádico de un elemento diferente de cero de $\mathbb{Q}_p$ es de la forma p^k para algún $k \in \mathbb{Z}$. Entonces para un elemento diferente de cero de K es de la forma $p^{k/n}$

para algún $k \in \mathbb{Z}$.

Si $x \in \mathbb{Q}$ y $|x|_p = p^{-k}$ entonces k es el orden p-ádico de x.

Definición 3.1.1. *Sea K una extensión finita de $\mathbb{Q}_p$. Para algún $0 \neq x \in K$, se define el orden p-ádico de x, denotado por $ord_p(x)$, el único racional que satisface:*

$$|x|_p = p^{-ord_p(x)}.$$

Se define:

- $ord_p(0) = \infty$,
- $ord_p(x) = \frac{1}{n} ord_p(N_{K/\mathbb{Q}_p}(x))$, *donde* $n = [K : \mathbb{Q}_p]$,
- $ord_p(x) = -\log_p |x|_p = -\log_p |N_{K/\mathbb{Q}_p}(x)|_p^{\frac{1}{n}} = -\frac{1}{n} \log_p |N_{K/\mathbb{Q}_p}(x)|_p$.

Ejemplo 3.1.1. *1. Calcular $ord_5(1+4\sqrt{2})$ en $\mathbb{Q}_5(\sqrt{2})$.*

Se sabe que $[\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5] = 2$ y la norma de $a+b\sqrt{2} \in \mathbb{Q}_5(\sqrt{2})$ es :

$$N_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(a+b\sqrt{2}) = a^2 - 2b^2,$$

entonces

$$N_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(1+4\sqrt{2}) = 1^2 - 2 \cdot 4^2 = -31,$$

por lo tanto, $ord_5(-31) = 0$ y $ord_5(1+4\sqrt{2}) = \frac{1}{2} ord_5(-31) = 0$.

Proposición 3. *Sea K una extensión finita de $\mathbb{Q}_p$ de grado n. La imagen de K^* bajo la valuación p-ádica es de la forma $\frac{1}{e}\mathbb{Z}$, donde e es un entero, el cual divide a n.*

Demostración. Se tiene que para $x, y \in K$, el $ord_p(x \cdot y) = ord_p(x) + ord_p(y)$; por lo tanto, ord_p es un homomorfismo de grupos, del grupo multiplicativo K^* al grupo aditivo $\frac{1}{n}\mathbb{Z}$. La imagen contiene todos los enteros, ya que es la imagen de $\mathbb{Q}_p^*$ y es un subgrupo de $\frac{1}{n}\mathbb{Z}$. Los subgrupos no triviales de $\frac{1}{n}\mathbb{Z}$ son de la forma $\frac{1}{e}\mathbb{Z}$, donde e divide a n, se sigue inmediatamente que la imagen de K^* es de esta forma. □

Definición 3.1.2. *Sea K una extensión finita de $\mathbb{Q}_p$ de grado n, se define e el único entero que satisface que:*

$$ord_p(K^*) = \frac{1}{e}\mathbb{Z}.$$

Ejemplo 3.1.2. *1. Para calcular el índice de ramificación de $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$, se sabe que el grado de la extensión es 2, por lo tanto se necesita saber que valores puede tomar $ord_5(a+b\sqrt{2})$ para $a+b\sqrt{2} \in \mathbb{Q}_5(\sqrt{2})$.*

$$ord_5(a+b\sqrt{2}) = \frac{1}{2}\left(N_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(a+b\sqrt{2})\right) = \frac{1}{2}\left(a^2-2b^2\right).$$

Debido a los términos cuadrados, la mayor potencia de 5 que divide a (a^2-2b^2) es par. Entonces $ord_5(a+b\sqrt{2})$ es un entero, así el índice de ramificación es $e=1$, es decir, la extensión no ramifica.

Definición 3.1.3. *Sea $K/\mathbb{Q}_p$ un extensión finita con índice de ramificación e. Se dice que $\pi \in K$ es*

un uniformizador si $ord_p(\pi) = \frac{1}{e}$.

Definición 3.1.4. *Sea* $f(x) = x^n + a_{n-1}x^{n+1} + \cdots + a_1x + a_0$ *un polinomio con coeficientes en* $\mathbb{Z}_p$. *Si* $ord_p(a_k) \geq 1$ *para* $k \geq 0$ *y* $ord_p(a_0) = 1$. *Entonces* $f(x)$ *es un polinomio de Eisenstein.*

El siguiente resultado caracteriza las extensiones totalmente ramificadas de $\mathbb{Q}_p$.

Teorema 3.1.1. *Si* $K/\mathbb{Q}_p$ *es una extensión finita totalmente ramificada de grado* n *y* $\pi \in K$ *es un uniformizador, entonces* $K = \mathbb{Q}_p(\pi)$.

Además, π *es una raíz de un polinomio de Eisenstein, es decir, una extensión finita totalmente ramificada de* $\mathbb{Q}_p$ *es generada por un polinomio de Eisenstein.*

Demostración. Sea π un uniformizador, tal que $ord_p(\pi) = \dfrac{1}{n} = \dfrac{1}{e}$, es decir, $|\pi|_p = p^{-\frac{1}{n}}$. Sea $f(x)$ el polinomio mínimo de π sobre $\mathbb{Q}_p$ y suponiendo que $f(x)$ tiene grado m.

$$N_{K/\mathbb{Q}_p}(\pi) = ((-1)^m a_0)^r,$$

donde $r = [K : \mathbb{Q}_p(\pi)]$ y

$$p^{-\frac{1}{n}} = |\pi|_p = \sqrt[n]{|N_{K/\mathbb{Q}_p}(\pi)|_p} = |a_0|_p^{\frac{r}{n}}.$$

Dado que a_0 es un número p-ádico, el valor absoluto es un entero que es potencia de p. Luego, por la ecuación anterior, se debe tener que $r = 1$ y $|a_0|_p = p^{-1}$. Además,

$$n = [K : \mathbb{Q}_p] = [K : \mathbb{Q}_p(\pi)][\mathbb{Q}_p(\pi) : \mathbb{Q}_p] = r \cdot m,$$

se deduce que el grado de $f(x)$ es n, y el hecho de que $[K:\mathbb{Q}_p] = [\mathbb{Q}_p(\pi):\mathbb{Q}_p]$ prueba que $K = \mathbb{Q}_p(\pi)$.

Para ver que $f(x)$ es un polinomio de Eisenstein , se debe ver que $ord_p(a_i) \geq 1$ para todo $i \geq 1$ y $ord_p(a_0) = 1$. Dado que $|a_0|_p = p^{-1}$, entonces $ord_p(a_0) = 1$, así cada conjugado $\sigma(\pi)$ de π es una raíz de $f(x)$, y tiene el mismo valor absoluto de π.

En particular, $|\sigma(\pi)|_p = p^{-\frac{1}{n}} < 1$. Luego cada coeficiente de $f(x)$ está dado por la suma y el producto de sus raíces, así $|a_i|_p < 1$ para $i \geq 1$, por lo tanto el $ord_p(a_i) \geq 1$ para $i \geq 0$. □

Si π es la raíz de un polinomio de Eisenstein de grado n entonces $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ es una extensión de grado n y aplicando la definición de valor absoluto usando $N_{K/\mathbb{Q}_p}(\pi)$ se tiene que $|\pi|_p = p^{-\frac{1}{n}}$.

Teorema 3.1.2. *Para cada entero positivo n, existe exactamente una extensión ramificada K de $\mathbb{Q}_p$ de grado n. Si $\overline{f}(x)$ es un polinomio irreducible de grado n sobre $\mathbb{Z}/p\mathbb{Z}$ el cuerpo residual de $\mathbb{Q}_p$ y si $f(x)$ es un polinomio de grado n sobre $\mathbb{Q}_p$ que asigna canónicamente a $\overline{f}(x)$, entonces $f(x)$ genera a K.*

3.2. Ejemplos

1. La extensión $K = \mathbb{Q}_5(\sqrt{5})/\mathbb{Q}_5$ es una extensión totalmente ramificada, con $\pi = \sqrt{5}$ el uniformizador. El polinomio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}_5$ es $p(x) = x^2 - 5$ que es de Eisenstein.

2. Sea $f(x) = x^2 - 2 \in \mathbb{Q}_2[x]$. Se sabe que $\sqrt{2}$ es una raíz de alguna extensión, entonces:

$$|\sqrt{2}|_{\mathbb{Q}_2(\sqrt{2})} = |N_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\sqrt{2})|_2^{\frac{1}{2}} = |2|_2^{\frac{1}{2}} = 2^{-\frac{1}{2}}.$$

La norma $|\sqrt{2}|_p$ no pertenece al conjunto de valores de $|\cdot|_2$ en $\mathbb{Q}_2$.

Por lo tanto, para $a,b \in \mathbb{Q}_2$ en cualquier extensión, se tiene que:

$$\begin{aligned} |a+b\sqrt{2}|_{\mathbb{Q}_2(\sqrt{2})} &= |N_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(a+b\sqrt{2})|_2^{\frac{1}{2}}, \\ &= |a^2-2b^2|_2^{\frac{1}{2}}, \\ &= \text{máx}(|a|_2, 2^{-\frac{1}{2}}|b|_2). \end{aligned}$$

Para determinar el anillo Z_K y su ideal $\mathscr{O}_K$ se deben encontrar los valores de a y $b \in \mathbb{Q}_2$, tales que la norma $|a+b\sqrt{2}|_K \leq 1$.

De la Definición 2.5.8, a y $b \in \mathbb{Q}_2$ se pueden expresar de la siguiente manera:

$a = \sum_{n \geq -n_0} a_n 2^n$ y $b = \sum_{n \geq -n_0} b_n 2^n$ donde $a_n, b_n \in \mathbb{Z}$ con $0 \leq a_n, b_n \leq 1$ y $a_{-n_0} \neq 0 \neq b_{-n_0}$.

Entonces $|a|_2 = 2^{-v_2(a)} = 2^{n_0} > 1$ y $2^{-\frac{1}{2}}|b|_2 = 2^{-\frac{1}{2}}2^{n_0} > 1$, por consiguiente a,b deben estar en $\mathbb{Z}_2$ para el caso de $|a|_2 \leq 1$ y $2^{-\frac{1}{2}}|b|_2 \leq 1$, así:

$$\mathbb{Z}_K = \{a+b\sqrt{2} : a,b \in \mathbb{Z}_2\}.$$

Ahora, para el caso en que la norma sea estricta menor que 1, es necesario que $a \in 2\mathbb{Z}_2$ y $b \in \mathbb{Z}_2$. En efecto, pues si $a = a_0 + a_1 2 + a_2 2^2 + \cdots$ y $b = b_0 + b_1 2 + b_2 2^2 + \cdots$ se tiene que $2^{-\frac{1}{2}}|b|_2 < 1$ dado que $|b|_2 \leq 1$, y al multiplicarse por un número menor, este me será menor que 1 como se espera. Ahora, $|a|_2 = 2^0 = 1$ si $a_0 \neq 0$ entonces para garantizar la desigualdad

estricta, $a_0 = 0$ lo que sucede si $a \in 2\mathbb{Z}_2$. Por lo tanto,

$$\mathscr{O}_K = \{a + b\sqrt{2} : a \in 2\mathbb{Z}_2, b \in \mathbb{Z}_2\},$$

además, $\mathscr{O}_K = \sqrt{2}\mathbb{Z}_K$ ya que para $a+b\sqrt{2} \in \mathbb{Z}_K$ se tiene que $\sqrt{2}(a+b\sqrt{2}) = a\sqrt{2}+2b \in \mathscr{O}_K$, así el cuerpo de las clases residuales es:

$$\mathbb{Z}_K/\mathscr{O}_K \cong \mathbb{Z}_2/2\mathbb{Z}_2 = \mathbb{F}_2.$$

Por lo tanto, $e_K = 2$ y $f_K = 1$, esto implica que K es total y salvajemente ramificada.

3. El polinomio $p(x) = x^2 - 2x + 2 \in \mathbb{Q}_2[x]$, con $1+i$ una raíz de $p(x)$. Para mostrar que $\mathbb{Q}_2(i+1)$ es una extensión de grado 2, basta ver que $i \notin \mathbb{Q}_2$.

   Suponga que $i \in \mathbb{Q}_2$, entonces i anula a $x^2+1 \in \mathbb{Q}_2[x]$, además $|i|_2 = 1$ e i debe ser un entero 2-ádico.

   Entonces,

$$i = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots \quad \text{con} \quad a_i \in \{0,1\},$$

$$i^2 = a_0^2 + (2a_0a_1) \cdot 2 + (a_1^2 + 2a_0a_2) \cdot 2^2 + \cdots = -1.$$

   Luego, por congruencias módulo 2, $a_0^2 \equiv -1 (mod\ 2)$, en consecuencia $a_0 = 1$. Siguiendo

con este valor y tomando congruencias módulo 2^3 se tiene:

$$1+(a_1+a_1^2)\cdot 2^2 \equiv -1 (mod\ 2^3),$$

$$1+(a_1+a_1^2)\cdot 2 \equiv 0 (mod\ 2^2),$$

sin solución para $a_1 \in \{0,1\}$, por lo tanto $i \notin \mathbb{Q}_2$.

Dado que i y $-i$ son conjugados:

$$\begin{aligned} |1+i|_{\mathbb{Q}_2(i} &= |N_{\mathbb{Q}_2(i)/\mathbb{Q}_2}(1+i)|_2^{\frac{1}{2}}, \\ &= |(1+i)(1-i)|_2^{\frac{1}{2}}, \\ &= |2|_2^{\frac{1}{2}} = 2^{-\frac{1}{2}}. \end{aligned}$$

Para $a, b \in \mathbb{Q}_2$,

$$\begin{aligned} |a+bi|_{\mathbb{Q}_2(i)} &= |N_{\mathbb{Q}_2(i)/\mathbb{Q}_2}(a+bi)|_2^{\frac{1}{2}}, \\ &= |a^2-b^2|_2^{\frac{1}{2}}, \\ &= \text{máx}(|a|_2, |b|_2). \end{aligned}$$

Así, para $K = \mathbb{Q}_2(1+i)$

$$\mathbb{Z}_K = \{a+bi : a,b \in \mathbb{Z}_2\},$$

$$\mathscr{O}_K = (1+i)\mathbb{Z}_K$$

$$\mathbb{Z}_K/\mathscr{O}_K \cong \mathbb{F}_2.$$

Por lo tanto, $e_K = 2$ y $f_K = 1$, esto implica que K es total y salvajemente ramificada.

Referencias Bibliográficas

Albarracín, A. A. (2022). Introducción números *p*-ádicos. Semillero de Investigación, Universidad Industrial de Santander.

Baquero, A. y Steven, E. (2020). Una introducción a los números *p*-ádicos, su aritmética y algunas simulaciones en python. Trabajo de grado (matemático), Pontificia Universidad Javeriana, Bogotá - Colombia.

Belichón, J. A. (2008). Teoría de galois. Notas del curso de Álgebra.

Bhattacharya, P.B., J. S. y. N. S. (1994). *Basic abstract algebra*. Cambridge University Press.

Carrillo, T. S. y Hurtado, A. C. (2008). Una introducción a los números *p*-ádicos. In *Memorias XVIII Encuentro de Geometría y VI de Aritmética*, pages 359–369.

Echevarría, G. P. (2016). Introducción a los cuerpos *p*-ádicos. Trabajo de grado (matemática), Universidad de Cantabria, Santander - España.

Gastón, G. A. (2008). Números *p*-ádicos. Notas de curso, IV Encuentro Nacional de Álgebra.

Huguet, R. L., R. C. J. y. T. A. J. G. (2013). *Criptografía avanzada*. Eureca Media.

Jara, M. P. (2018). Extensiones de cuerpos. Notas de trabajo, 16 Universidad de Granada.

Jena, A. (2016). Semester project on ramification of finite extensions of $\mathbb{Q}_p$. National Institute of Science.

Leinster, T. (2022). *Galois Theory*. University of Edinburgh.

Lezama, O. (2017). Cuerpos. Cuadernos de Álgebra.

López, S. P. (2019). Números *p*-ádicos. Trabajo de grado (matemático), Universidad de Santiago de Compostela, Santiago de Compostela - España.

Maldonado, G. D. (2015). Introducción a los números *p*-ádicos y análisis *p*-ádicos. Trabajo de grado (matemática), Universidad Industrial de Santander, Bucaramanga - Colombia.

Mas Huamán, R. (2015). Raíces *p*-ádicas de la unidad. Tesis de maestría (magister en matemáticas, Pontificia Universidad Católica del Perú, Perú.

Monsalve, L. M. (2018). Una aplicación del análisis *p*-ádico. In *La Gaceta de la RSME*, pages 147–168.

Q. Gouv$\hat{e}$a, F. (2003). *p-adic numbers an introduction*. Springer.

Riquelme, F. E. A. (2007). Teoría de galois y ecuaciones algebraicas. Trabajo de grado (educació matemática), Universidad del BÍO-BÍO, Chillán - Chile.

Turner, E. (2011). The *p*-adic numbers and finite field extensions of $\mathbb{Q}_p$.

Wiswell, A. (2011). Finite field extensions of the *p*-adic numbers. Tesis de maestría (magister en matemáticas, Universidad de Nevada, Reno.