PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Escuela de Postgrado

Magister en Matemáticas

Tesis de Maestría

título

Raíces p-ádicas de la unidad

por

Ronald Mas Huamán

asesor

Dr. Alfredo Poirier

Lima, Perú

2015

Introducción

El tema de la presente tesis es el estudio de la ecuación $x^n - 1 = 0$ en los números p-ádicos. Para ello la primera tarea es factorizar $f(x) = x^n - 1$ a como de lugar en producto de irreducibles. Llegado a esa instancia, la idea es conseguir una extensión que nos permita descomponer completamente el polinomio $f(x)$ y mostrar el comportamiento algebraico de las raíces. En los p-ádicos, ello se logra una vez introducidos los conceptos de índice de ramificación y grado de clases residuales.

Empezamos esta tesis con un repaso de las extensiones ciclótomicas sobre $\mathbb{Q}$ en el Capítulo 1. Éstas resultan de adjuntar una raíz primitiva de la unidad a $\mathbb{Q}$, generando así una extensión que resulta ser de Galois. Además, dado que los enteros p-ádicos también poseen una buena reducción módulo el primo p de preferencia, es preciso recordar algunas propiedades de los cuerpos finitos. Este repaso nos permitirá realizar un correcto manejo del grado de clases residuales y índice de ramificación, conceptos estrechamente relacionadas con el grado de la extensión.

A partir de allí, en el Capítulo 3 concentramos nuestra atención en los números p-ádicos. Nos valdremos de algunos resultados expuestos en la tesis de maestría de José Condori [2], sobre todo en lo referente a las propiedades elementales de los números p-ádicos. Como caso especial estudiaremos las raíces p-ádicas de la unidad en $\mathbb{Q}_p$ y también mostraremos las extensiones cuádraticas que se pueden construir. Es bien sabido que hallar una extensión cuadrática equivale a resolver la ecuación $x^2 - a = 0$ con $a \in \mathbb{Q}_p$.

En el Capítulo 4 completamos el estudio de las propiedades algebraicas de las

raíces p-ádicas de la unidad y las separamos en dos subgrupos $\mu_{(p)}(K)$ y $\mu_{(p^\infty)}(K)$, los mismos que son las raíces de orden coprimo con p y raíces de orden una potencia de un primo. Por muy simple que parezca, esta agrupación de las raíces nos permitirá una clasificación de ciertas extensiones p-ádicas.

Finalmente, es grato resaltar al Doctor Alfredo Poirier por su paciencia en la asesoría brindada para la elaboración de esta tesis.

Índice general

Capítulo 1

Extensiones ciclotómicas

En este primer capítulo recordamos cómo la teoría de Galois nos brinda información sobre la naturaleza de los posibles factores de un polinomio. Como sabemos, en un cuerpo todo polinomio se puede descomponer como producto de sus factores irreducibles. Para nuestro interés el polinomio $x^n - 1$ no será la excepción. Como es sabido, los valores que anulan dicho polinomio son las raíces n-ésimas de la unidad.

1.1. Raíces de la unidad

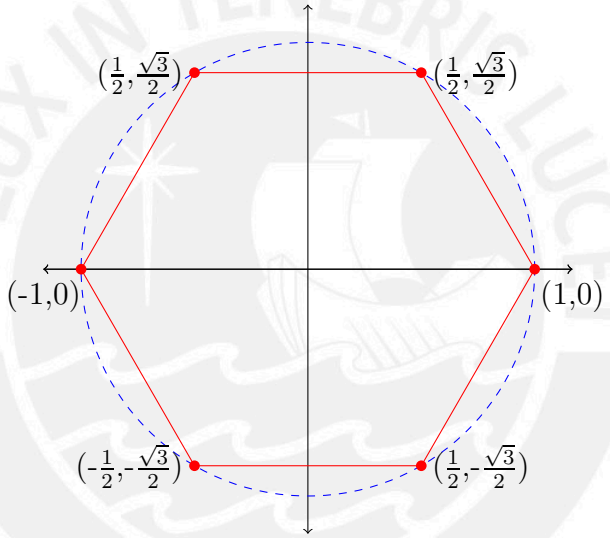
La ecuación polinomial $x^n - 1 = 0$ con coeficientes racionales al ser resuelta sobre $\mathbb{Q}$ arroja como únicas posibles raíces 1 y -1. La razón es sencilla: si $\mid x \mid < 1$ entonces $\mid x^n \mid < \mid x \mid < 1$ para todo n entero positivo, mientras que si $\mid x \mid > 1$ entonces $\mid x^n \mid > \mid x \mid > 1$. Desde el punto de vista algebraico ello no es sorpresa, pues gracias al lema de Gauss sabemos que una factorización del polinomio $x^n - 1$ en $\mathbb{Q}$ automáticamente proporciona una factorización en $\mathbb{Z}$. En general, para cualquier n entero positivo tenemos $x^n - 1 = (x-1)(x^{n-1} + \ldots + x + 1)$. Mejor aún, si n es par tenemos $x^{2k} - 1 = (x^2 - 1)(x^{2k-2} + \ldots + 1)$, donde $n = 2k$.

Por otro lado, por un argumento similar al anterior, factorizar $x^n - 1$ en $\mathbb{R}$ no reporta nada novedoso. Esto significa que perdemos muchas soluciones si nos circunscribimos a tales cuerpos numéricos. Para hacer el trabajo redondo es preciso movilizarnos a un cuerpo donde se pueda encontrar al menos una raíz de este polinomio. Por ejemplo, en última instancia siempre podemos recurrir a los complejos

$\mathbb{C}$.

El polinomio $x^n - 1$ puede ser factorizado totalmente en $\mathbb{C}$, pues este cuerpo es algebraicamente cerrado. Es decir, sus factores son lineales. Es más, sus raíces $e^{2\pi ik/n}$, con $k = 0, 1, 2, \ldots, n-1$, están ubicadas de manera simétrica sobre el círculo unitario. De quererlas dibujar sobre el plano complejo, al ser unidas generarán un polígono regular de n lados. Obsérvese además que si ζ es una raíz n-ésima de la unidad, entonces ζ^k y $\overline{\zeta}$ también lo son.

Ejemplo 1.1. Las raíces del polinomio $x^6 - 1$ están dadas por $e^{2\pi ik/6}$, con $k = 0, 1, 2, 3, 4, 5$. La figura indica cómo se esparcen sobre el círculo unitario; al unir los puntos forman un hexágono regular.



El conjunto formado por todas las raíces n-ésimas de la unidad es un subgrupo multiplicativo de $\mathbb{C}^*$ que resulta ser cíclico. Además, puesto que hemos encontrado un total de n raíces distintas, dicho polinomio no posee raíces múltiples en $\mathbb{C}$.

A las raíces n-ésimas de la unidad cuyo orden es precisamente n (es decir, a los generadores del grupo cíclico) se les llama **raíces n-ésimas primitivas** de la unidad. Así, si ζ es una raíz n-ésima primitiva de la unidad entonces el conjunto de raíces n-ésimas de la unidad está formado por $\{1, \zeta, \zeta^2 \ldots \zeta^{n-1}\}$. Recordemos que la **función de Euler** de n, denotada por $\phi(n)$, indica la cantidad de números entre 1 y n inclusive que son relativamente primos con n. Además, por teoría de

grupos sabemos que $\phi(n)$ cuenta el número de elementos de orden multiplicativo igual a n. En otras palabras, existen $\phi(n)$ raíces n-ésimas primitivas de la unidad. Por convención $\phi(1)$ valdrá 1.

1.2. Polinomios ciclotómicos

La discusión de la sección anterior muestra que el menor subcuerpo de $\mathbb{C}$ donde $x^n - 1$ se descompone en factores lineales es $\mathbb{Q}(\zeta)$, donde ζ es cualquier raíz primitiva n-ésima de la unidad. Este cuerpo recibe el nombre de **extensión ciclotómica n-ésima de** $\mathbb{Q}$, y el hecho de que lo hayamos materializado como subconjunto de $\mathbb{C}$ es intrascendente como veremos en el Teorema 1.5. Asimismo, por lo argumentado anteriormente, es claro que si η es otra raíz primitiva n-ésima de la unidad, tenemos $\mathbb{Q}(\zeta) = \mathbb{Q}(\eta)$.

Definamos el polinomio $\Phi_n(x) = \Pi_{i=1}^{m}(x - \zeta_i)$, donde $\{\zeta_i\}_{i=1}^{m}$ son las raíces n-ésimas primitivas de la unidad. Este polinomio es llamado **polinomio ciclotómico** n-ésimo. Es más, por la definición de la función de Euler, este polinomio tiene grado $\phi(n)$. Como caso particular tenemos $\Phi_1(x) = x - 1$, de grado 1.

Teorema 1.2. *El polinomio $x^n - 1$ se factoriza en $\mathbb{C}[x]$ como*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Demostración. Para cada divisor d de n sea R_d el conjunto de las raíces de la unidad de orden exactamente d. Entonces $\{R_d\}_{d|n}$ es una partición del conjunto de las raíces n-ésimas de la unidad, es decir, una partición del conjunto de raíces de $x^n - 1$. Los elementos de cada R_d son las raíces d-ésimas primitivas de la unidad en $\mathbb{C}$, de ahí que $\Phi_d(x)$ posea como raíces los elementos de R_n. □

Teorema 1.3. *Los polinomios ciclotómicos tienen coeficientes enteros. En símbolos tendremos $\Phi_n(x) \in \mathbb{Z}[x]$.*

Demostración. La prueba la hacemos por inducción sobre n. Para $n = 1$ tenemos $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Supongamos que el resultado sea válido para $1 \leq d < n$. Entonces se tiene $\Phi_d(x) \in \mathbb{Z}[x]$ para todo $d < n$, y en particular esto vale para los divisores no triviales de n. Sea

$$f(x) = \prod_{d|n, d<n} \Phi_d(x);$$

polinomio que por hipótesis de inducción pertenece al anillo $\mathbb{Z}[x]$. Por el teorema anterior se tiene $x^n - 1 = f(x)\Phi_n(x)$, de donde por el lema de Gauss se concluye que $\Phi_n(x)$ también tiene coeficientes enteros. □

Ejemplo 1.4. Consideremos el polinomio $x^{12} - 1$. Una raíz primitiva es $\zeta = e^{2\pi i/12}$, las otras son ζ^n donde $mcd(n, 12) = 1$ y $n < 12$. El polinomio ciclotómico está dado explícitamente por

$$\Phi_{12}(x) = \prod_{i=1}^{4}(x - \zeta_i) = (x - \zeta)(x - \zeta^5)(x - \zeta^7)(x - \zeta^{11}).$$

Al efectuar las operaciones obtenemos

$$\begin{aligned}
\Phi_{12}(x) &= (x - \zeta)(x - \zeta^{11})(x - \zeta^5)(x - \zeta^7) \\
&= (x^2 - 2\cos\tfrac{\pi}{6}x + 1)(x^2 - 2\cos\tfrac{5\pi}{6}x + 1) \\
&= (x^2 - \sqrt{3}x + 1)(x^2 + \sqrt{3}x + 1) \\
&= x^4 - x^2 + 1.
\end{aligned}$$

De igual manera podemos hallar los polinomios ciclotómicos asociados a cada divisor positivo propio de 12. Estos están dados por

$$\begin{aligned}
\Phi_6(x) &= x^2 - x + 1, \\
\Phi_4(x) &= x^2 + 1, \\
\Phi_3(x) &= x^2 + x + 1, \\
\Phi_2(x) &= x + 1, \\
\Phi_1(x) &= x - 1.
\end{aligned}$$

Por supuesto, el Teorema 1.2 obliga a que se cumpla

$$x^{12} - 1 = \prod_{d|12} \Phi_{12}(x) = (x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)(x^4 - x^2 + 1).$$

La importancia de hallar explícitamente los polinomios ciclotómicos radica en que así se obtiene la factorización definitiva en $\mathbb{Z}[x]$. En efecto, estos polinomios ciclótomicos son ya irreducibles.

Teorema 1.5. *Cada polinomio ciclotómico $\Phi_n(x)$ es irreducible en $\mathbb{Q}[x]$.*

Demostración. Gracias al lema de Gauss es suficiente probar que $\Phi_n(x)$ es irreducible en $\mathbb{Z}[x]$. Para ello supongamos que se tenga una factorización $\Phi_n = fg$ con $f, g \in \mathbb{Z}[x]$ mónicos y f irreducible y no trivial. Sea ζ una raíz n-ésima primitiva de la unidad que sea raíz de f. Fijemos un primo p que no divida a n. Entonces ζ^p es una raíz n-ésima primitiva de la unidad, motivo por el cual será raíz de Φ_n; en otras palabras ζ^p es raíz de f ó g.

Si ζ^p es raíz de g, entonces ζ es raíz de $g(x^p)$ y se tiene $f(x) \mid g(x^p)$ en $\mathbb{Z}[x]$, pues f es el polinomio minimal de ζ. De esta manera existe $h \in \mathbb{Z}[x]$ tal que $g(x^p) = f(x)h(x)$. Al reducir módulo p tenemos $\overline{g}(t^p) = \overline{f}(t)\overline{h}(t)$ en $\mathbb{F}_p[t]$. Como en $\mathbb{F}_p[t]$ se cumple $\overline{f}(t)\overline{h}(t) = \overline{g}(t^p) = \overline{g}(t)^p$ y por ser además $\mathbb{F}_p[t]$ un dominio de factorización única tenemos que $\overline{f}$ y $\overline{g}$ poseen un factor en común en $\mathbb{F}_p[t]$. Pero $\Phi_n = fg$ implica entonces que $\overline{\Phi}_n = \overline{f}\overline{g}$ en $\mathbb{F}_p[t]$ posee una raíz múltiple en alguna extensión de $\mathbb{F}_p$. En resumen $t^n - 1 \in \mathbb{F}_p[t]$ tiene una raíz múltiple, pues acepta a $\overline{\Phi}_n$ como factor. Esto es una contradicción ya que todas las raíces de $t^n - 1$ son diferentes entre sí en cualquier cuerpo de característica que no divide a n. Detalles adicionales sobre reducción módulo p se tratarán en el Capítulo 2.

La alternativa es que ζ^p sea raíz de f, para toda raíz ζ de f. Luego ζ^a es raíz de f para todo a tal que $(a, n) = 1$, pues si $a = p_1 \dots p_k$ es producto de primos que no dividen a n entonces $\zeta^{p_1}, (\zeta^{p_1})^{p_2}, \dots \zeta^{p_1 p_2 \cdots p_k}$ son también raíces de f. Si revisamos esto, estamos confirmando que toda raíz n-ésima primitiva de la unidad es raíz de f. Por lo tanto se tiene $f = \Phi_n$; esto prueba el teorema. □

Teorema 1.6. *Sea ζ una raíz n-ésima primitiva de la unidad. Entonces $\Phi_n(x)$ es el polinomio minimal de ζ. Además el grupo de Galois $Gal_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}$ es isomorfo al grupo multiplicativo $(\mathbb{Z}/\langle n \rangle)^*$ conformado por todas las clases relativamente primas a n.*

Demostración. La primera afirmación es inmediata puesto que se satisface $\Phi_n(\zeta) = 0$ y $\Phi_n(x)$ es irreducible. La siguiente afirmación se debe a que como ζ es una raíz n-ésima primitiva de unidad, entonces ζ^k es también una raíz n-ésima primitiva de unidad para todo k con $(k, n) = 1$.

Definimos

$$\begin{array}{rccc} \varphi: & (\mathbb{Z}/\langle n\rangle)^* & \to & Gal_{\mathbb{Q}}^{\mathbb{Q}(\zeta)} \\ & k & \mapsto & \sigma_k \end{array}$$

donde σ_k se caracteriza por $\sigma_k \mid_{\mathbb{Q}} = id$ y $\sigma_k(\zeta) = \zeta^k$, la cuál está bien definida.

Esta φ es un homomorfismo, pues $\sigma_k\sigma_l(\zeta) = \sigma_k(\zeta^l) = (\zeta^l)^k = \zeta^{lk} = \sigma_{kl}(\zeta)$ significa $\sigma_k\sigma_l = \sigma_{kl}$, para todo $k, l \in (\mathbb{Z}/\langle n\rangle)^*$. Claramente se puede ver además que φ es biyectiva. □

Ejemplo 1.7. Si ζ es una raíz quinta de la unidad, entonces $\mathbb{Q}(\zeta)$ es Galois y $Gal_{\mathbb{Q}}^{\mathbb{Q}(\zeta)} = (\mathbb{Z}/\langle 5\rangle)^*$, posee cuatro elementos.

Por otro lado, podemos notar que cualquier factor de $x^n - 1$ en $\mathbb{Z}[x]$ provee gratis un factor de $x^n - 1$ en $R[x]$ donde R es cualquier anillo conmutativo con unidad. La recíproca no es válida.

Ejemplo 1.8. Al factorizar $t^4 - 1$ en $\mathbb{Z}/\langle 2\rangle[t]$ tenemos que $t^4 - 1 = (t - 1)^4$ posee una única raíz de multiplicidad 4.

Ejemplo 1.9. Al factorizar $t^6 - 1$ en $\mathbb{Z}/\langle 7\rangle[t]$ tenemos que

$$t^6 - 1 = (t - 1)(t - 2)(t - 3)(t - 4)(t - 5)(t - 6)$$

posee raíces diferentes, las cuales coinciden con los elementos de $(\mathbb{Z}/\langle 7\rangle)^*$.

Capítulo 2

Cuerpos finitos

Los cuerpos finitos juegan un papel importante cuando se estudia extensiones algebraicas de cuerpos númericos. Por ejemplo, ellos hicieron sentir su presencia en la demostración del Teorema 1.5. Probaremos en primer lugar que todo cuerpo finito tiene p^n elementos, donde p es la característica del cuerpo y n es un número natural. Luego veremos que para cada número natural n y cada primo p existe un único cuerpo (salvo isomorfismos) de p^n elementos. Nuestro interés en estudiar las raíces n-ésimas de la unidad en un cuerpo arbitrario nos lleva a plantearnos diversas posibilidades.

Si la característica de K es 0 ó un número primo p que no divide a n, entonces la derivada formal del polinomio $x^n - 1$ es nx^{n-1}, el cuál no es nulo sobre $K[x]$. Además, como la única raíz de este polinomio es 0, el cuál no es raíz de $x^n - 1$, se concluye que todas las raíces de $x^n - 1 = 0$ son diferentes.

Si la característica de K es un número primo p y se tiene $n = p^k m$, entonces se cumple $x^n - 1 = (x^m - 1)^{p^k}$. Esto quiere decir que el cuerpo donde $x^n - 1$ se descompone es el mismo cuerpo de descomposición de $x^m - 1$ siempre que m sea primo relativo con p . Esto reduce el estudio al caso donde la característica de K es 0 ó un número primo p que no divide a n.

2.1. Cuerpos finitos

Denotemos por $\mathbb{F}_p$, donde p es un número primo, al **cuerpo finito con p elementos**. Ellos aparecen como el cociente de los enteros sobre sus ideales maximales. Concretamente se tiene que $\mathbb{F}_p = \mathbb{Z}/\langle p\rangle$ es un cuerpo finito, si p es primo.

Lema 2.1. *Todos los cuerpos con p elementos son isomorfos a $\mathbb{F}_p$.*

Demostración. Sea K un cuerpo con p elementos. Definamos la función

$$\begin{array}{rccl} \varphi: & \mathbb{Z} & \to & K \\ & n & \mapsto & \overline{1}_K + \overline{1}_K + \cdots \overline{1}_K \quad (n\, veces), \end{array}$$

la cual claramente está bien definida y es un homomorfismo. Es más, se cumple $Ker(\varphi) = p\mathbb{Z}$ y por consiguiente tenemos

$$\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}} \simeq K.$$

□

Veremos pronto que dos cuerpos finitos con el mismo número de elementos son isomorfos; esto será una consecuencia de la unicidad de cuerpos de descomposición, tema a tratarse luego.

Recordemos que la **característica de un anillo** es el menor n entero positivo que satisface

$$\underbrace{1_R + 1_R + \cdots 1_R}_{n\ veces} = 0$$

Lema 2.2. *La característica de todo cuerpo finito es un número primo.*

Demostración. Si $car(K) = q$ entonces $q = q \cdot 1 = 0$, pues el orden aditivo de todo elemento divide a q. Cualquier valor con una propiedad similar ha de ser un primo, pues de lo contrario aparecerían divisores de cero. □

Lema 2.3. *Sea K con q elementos. Entonces se cumple $x^q = x$ para todo $x \in K$.*

Demostración. Si $x \neq 0$, la función multiplicación por x de K^* en K^* es biyectiva. Por ello se tiene

$$\prod_{a \in K^*} a = \prod_{a \in K^*} xa = x^{q-1} \prod_{a \in K^*} a.$$

Como $\prod_{a \in K*} a$ es no nulo, concluimos que se debe tener $x^{q-1} = 1$; lo cual implica $x^q = x$. Para $x = 0$ obviamente se cumple $x^q = x$. □

Todo cuerpo K de característica p contiene una copia de $\{m1_K : m \in \mathbb{Z}\}$. Gracias a ello podemos identificar $\mathbb{F}_p$ con este subcuerpo de K.

Lema 2.4. *Sea K una extensión finita de grado n sobre un cuerpo finito F. Si F tiene q elementos, entonces E tiene q^n elementos.*

Demostración. Sea $\{u_1, u_2, ..., u_n\}$ una base para K como espacio vectorial sobre F. Entonces, todo $v \in K$ puede escribirse de manera única en la forma

$$\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n,$$

donde $\alpha_i \in F$. Como cada α_i puede ser alguno de los q elementos de F, el número total de dichas combinaciones lineales distintas es q^n. □

Corolario 2.5. *Sea F un cuerpo finito. Entonces existe un primo p y un $n \in \mathbb{N}$, ambos únicos, tales que F tiene p^n elementos.*

Demostración. Como F tiene un número finito de elementos, su característica debe ser un primo p. Por el lema anterior F tiene p^n elementos, para cierto n. □

Decimos que E es un **cuerpo de descomposición** de un polinomio $f(x) \in F[x]$ si éste es el menor cuerpo donde f se descompone como producto de factores lineales en $E[x]$.

Corolario 2.6. *Para todo p primo y todo entero $n \geq 1$ existe un cuerpo con p^n elementos.*

Demostración. Sea E un cuerpo de descomposición de $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Como la derivada formal $f' = p^n x^{p^n - 1} - 1 = -1$ y f son primos entre sí, tenemos que f posee p^n raíces distintas en E. Sea K el conjunto formado por dichas raíces.

Veamos que K es un subcuerpo de E. Claramente los elementos 0 y 1 están en K. Supongamos se tenga $a, b \in K$. Entonces se tiene

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b,$$

y así también $a - b \in K$. Por otro lado, si $b \neq 0$, entonces se cumple

$$(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1},$$

con lo que obtenemos $ab^{-1} \in K$. Por lo tanto K es un cuerpo. □

Teorema 2.7. *En todo cuerpo finito $\mathbb{F}_q$ la parte multiplicativa $\mathbb{F}_q^*$ es un grupo cíclico.*

Demostración. Es claro que podemos asumir $q \geq 3$. Descompongamos $q - 1 = p_1^{r_1} p_2^{r_2} ... p_m^{r_m}$ con $p_1, p_2..., p_m$ primos y $r_1, r_2..., r_m$ positivos. Para todo $1 \leq i \leq m$ el polinomio $f_i(t) = t^{(q-1)/p_i} - 1$ tiene a lo más $(q-1)/p_i$ raíces en $\mathbb{F}_q$. Como además se tiene $(q-1)/p_i < (q-1)$, existen elementos no nulos en $\mathbb{F}_q$ que no son raíces de f_i. Para cada $1 \leq i \leq m$ fijemos un elemento a_i que no sea raíz de f_i y pongamos $b_i = a_i^{(q-1)/p_i^{r_i}}$. Observamos que se cumple $b_i^{p_i^{r_i}} = a_i^{q-1} = 1$, de ahí que el orden de b_i sea un divisor de $p_i^{r_i}$ y por lo mismo será de la forma $p_i^{s_i}$ con $0 \leq s_i \leq r_i$. Por otro lado se tiene $b_i^{p_i^{r_i-1}} = a_i^{(q-1)/p_i} \neq 1$ ya que b_i no es un cero de f_i, y de este modo el orden de b_i es exactamente $p_i^{r_i}$. Veamos que el orden de $b = b_1 b_2 ... b_m$ debe ser $q - 1$. Por contradicción supongamos que el orden de b sea un divisor propio de $h = q - 1$. Entonces, como cierto orden de b es $q-1$ dividido entre algún primo p_i, supongamos que éste sea p_1. Así tenemos

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} ... b_m^{h/p_1}.$$

Ahora, para $2 \leq i \leq m$ tenemos que $p_i^{r_i}$ divide a h/p_1, así que se cumple $b_i^{h/p_i} = 1$ para estos índices, y de ello se deriva $b_1^{h/p_1} = 1$. Esto implica que h/p_1 es múltiplo del orden de b_1, en particular de $p_1^{r_1}$, lo cual es una contradicción. En consecuencia $\mathbb{F}_q^*$ es un grupo cíclico con generador b. □

Los elementos que generan el grupo cíclico $\mathbb{F}_q^*$ son también llamados **elementos primitivos** de $\mathbb{F}_q$. Como sabemos, $\mathbb{F}_q$ tiene $\phi(q-1)$ generadores, y así posee $\phi(q-1)$ elementos primitivos. La existencia de elementos primitivos se usa en particular para establecer que todo cuerpo finito puede ser interpretado como una extensión algebraica simple de su subcuerpo primo base.

2.2. Extensiones finitas de cuerpos finitos

Resulta que E es extensión finita de F si E puede ser visto como un F espacio vectorial finito. Además, llamaremos **grado de la extensión de E sobre F** a la dimensión del espacio vectorial E sobre F, denotado por $n = [E : F]$.

Sea E cuerpo de descomposición del polinomio $f(x) = x^q - x \in K[x]$ con $q = p^n$. Como la derivada formal $f'(x) = -1$ es relativamente prima con $f(x)$, se sigue que $f(x)$ tiene q raíces distintas en E. Entonces E coincide con el conjunto formado por K y la adjunción de las raíces de dicho polinomio.

En lo que sigue K será un cuerpo arbitrario.

Teorema 2.8. *Dado $f(x) \in K[x]$ existe un cuerpo donde f se factoriza en factores lineales.*

Demostración. La existencia se prueba adjuntando una a una sus raíces. □

Teorema 2.9. *Dos cuerpos de descomposición de un mismo polinomio son isomorfos.*

Demostración. Por inducción en el grado $n = [E : K]$, mostraremos que si E es cuerpo de descomposición de un polinomio $f \in K[x]$ entonces cualquier cuerpo de descomposición de f es isomorfo a E sobre K.

Si $n = 1$ entonces $E = K$ y f se factoriza completamente en K. Así dado otro cuerpo de descomposición de f que contiene a K, éste debe ser K, pero K es isomorfo a K sobre K.

En general sean E y E' cuerpos de descomposición de $f \in K[x]$ y sea $g \in K[x]$ un factor irreducible de p. Tomemos una raíz $\alpha \in E$ de g y otra $\alpha' \in E'$ de g. Con ello $K(\alpha) \subset E$ y $K(\alpha') \subset E'$ son isomorfos a $K[x]/\langle q \rangle$ y por lo tanto son isomorfos entre sí. De esta forma se puede asumir $\alpha = \alpha'$. Así tenemos que $f \in K(\alpha)[x]$ tiene como cuerpos de descomposición a E y E'. Luego, al tenerse $[E : K(\alpha)] < [E : K]$, se cumple que E y E' son isomorfos por la hipótesis inductiva. □

Proposición 2.10. *Toda extensión finita de un cuerpo finito es simple.*

Demostración. Sea E una extensión finita del cuerpo finito F. Como la parte multiplicativa E^* del cuerpo E es cíclico, tenemos que si ζ genera E^* como un grupo multiplicativo, entonces se cumple $E = F(\zeta)$. □

Teorema 2.11. *Sea f un polinomio irreducible en $\mathbb{F}_q[t]$ de grado m. Entonces f admite una raíz α en la extensión $\mathbb{F}_{q^m}$. Todas las raíces de f son simples y están dadas por los m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demostración. Sea α una raíz de f en alguna extensión algebraica de $\mathbb{F}_q$. Entonces de $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ se pasa a $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ y en particular a $\alpha \in \mathbb{F}_{q^m}$. Ahora, cuando $\alpha \in \mathbb{F}_{q^m}$ sea una raíz de f, veamos que α^q es también una raíz de f. Sea $f(t) = a_m t^m + ... + a_1 t + a_0$ con $a_i \in \mathbb{F}_q$ para $0 \leq i \leq m$. Como $a_i \in \mathbb{F}_q$ implica $a_i^q = a_i$, obtenemos

$$\begin{aligned} f(\alpha^q) &= a_m\alpha^{qm} + ... + a_1\alpha^q + a_0 &= a_m^q\alpha^{qm} + ... + a_1^q\alpha^q + a_0^q \\ &= (a_m\alpha^m + ... + a_1\alpha + a_0)^q &= f(\alpha)^q = 0. \end{aligned}$$

Continuando inductivamente con el procedimiento concluimos que los elementos $\alpha^{q^2}, ..., \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$ son también raíces de f. Supongamos por un instante que dos de estas raíces sean iguales, es decir $\alpha^{q^j} = \alpha^{q^k}$ para algunos enteros j y k con $0 \leq j < k \leq m-1$. Al elevar ambos miembros a la potencia q^{m-k} obtenemos

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

Entonces $\alpha \in \mathbb{F}_{q^m}$ es raíz de $t^{q^{m-k+j}} - t$. Acto seguido, si $\beta \in \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ tendremos $\beta = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$, donde $a_i \in \mathbb{F}_q$, y así

$$\begin{aligned} \beta^{q^{m-k+j}} &= (a_0 + a_1\alpha + \cdots + a_{m-1}\alpha_{m-1})^{q^{m-k+j}} \\ &= a_0^{q^{m-k+j}} + a_1^{q^{m-k+j}}\alpha^{q^{m-k+j}} + \cdots + a_{m-1}^{q^{m-k+j}}\alpha_{m-1}^{q^{m-k+j}} \\ &= a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \\ &= \beta. \end{aligned}$$

Esto significa que todo elemento de $\mathbb{F}_{q^m}$ es una solución de la ecuación $t^{q^{m-k+j}} - t$. Ello nos conduce a $m-k+j \geq m$, lo cual es una contradicción a $m-k+j < m$. □

Veamos una consecuencia del teorema anterior. Sea $\mathbb{F}_{q^m}$ es una extensión de $\mathbb{F}_q$ y $\alpha \in \mathbb{F}_{q^m}$. Los elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ son llamados **conjugados de** α con respecto a $\mathbb{F}_q$. Los elementos conjugados son obtenidos por el automorfismo

$$\begin{aligned} f : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ t &\mapsto t^q, \end{aligned}$$

conocido como el **automorfismo de Frobenius**.

Los conjugados de $\alpha \in \mathbb{F}_{q^m}$ con respecto a $\mathbb{F}_q$ son distintos si y sólo si el polinomio minimal de α sobre $\mathbb{F}_q$ tiene grado m. Caso contrario, el grado d de este polinomio minimal es un divisor propio de m, y además los conjugados de α con respecto a $\mathbb{F}_q$ son los elementos distintos $\alpha, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$ (repetidos cada m/d veces).

Ejemplo 2.12. Sea $\alpha \in \mathbb{F}_{16}$ una raíz de $f(t) = t^4 + t + 1 \in \mathbb{F}_2[t]$. Entonces los conjugados de α con respecto a $\mathbb{F}_2$ son $\alpha, \alpha^2, \alpha^4 = \alpha + 1$ y $\alpha^8 = \alpha^2 + 1$; cada uno de ellos es un elemento primitivo de $\mathbb{F}_{16}$. Por otro lado, los conjugados de α con respecto de $\mathbb{F}_4$ son α y $\alpha^4 = \alpha + 1$.

Corolario 2.13. *Sea E un cuerpo con p^n elementos. Para cada divisor positivo m de n, el cuerpo E contiene exactamente un cuerpo con p^m elementos.*

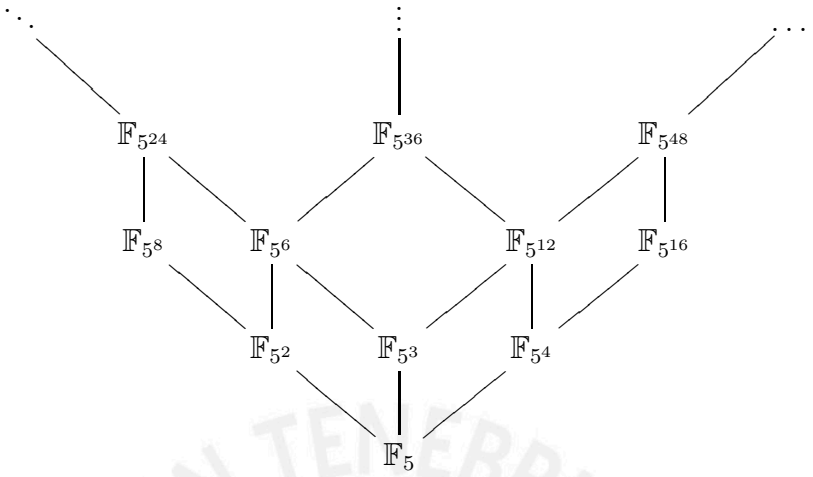
Demostración. Como todo cuerpo finito es simple, sean β y β' tales que $\mathbb{F}_p(\beta) \subset E$ y $\mathbb{F}_p(\beta') \subset E$ tengan cardinalidad p^m. Como ambos son cuerpos de descomposición de $t^{p^m} - t$, ellos deben coincidir. □

Proposición 2.14. *Cuando m, n son enteros positivos, entonces $\mathbb{F}_{p^m}$ es un subcuerpo de $\mathbb{F}_{p^n}$ si y sólo si m divide a n.*

Demostración. Veamos la ida. Dado $a \in \mathbb{F}_{p^m}$, se tiene que a es una raíz del polinomio $f(t) = t^{p^m} - t$. De ahí que como se cumple $(t^{p^m} - t) \mid (t^{p^n} - t)$, se concluye que m divide a n. La vuelta es similar. □

Ejemplo 2.15. Como consecuencia de la propiedad anterior, observemos la construcción de los cuerpos finitos bajo estas condiciones para el primo $p = 5$. Recorde-

mos que para cada potencia de 5 tendremos en $\mathbb{F}_{5^m}$ una extensión finita de $\mathbb{F}_5$.



En general, definamos la inyección $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ con m divisor de n. Resulta que $K = \bigcup \mathbb{F}_{p^m}$ es un cuerpo.

En efecto, esto se debe a que para $a, b \in K$ existen i, j tales que $a \in \mathbb{F}_{p^i}$ y $b \in \mathbb{F}_{p^j}$. Sin embargo, de $\mathbb{F}_{p^i}, \mathbb{F}_{p^j} \subset \mathbb{F}_{p^{ij}}$, se tiene $a + b, ab \in \mathbb{F}_{p^{ij}} \subset K$. Es más, dado $a \in K$ existe m_i con el cual se cumple $a \in \mathbb{F}_{p^{m_i}}$ por lo tanto, la inversa a^{-1} ya se encuentra en $\mathbb{F}_{p^{m_i}} \subset K$.

Este cuerpo terminal nos permite representar de manera económica la clausura algebraica de $\mathbb{F}_p$.

Teorema 2.16. *La clausura algebraica de $\mathbb{F}_p$ coincide con $\bigcup \mathbb{F}_{p^n}$.*

Demostración. Sea un polinomio $p(t) \in \bigcup \mathbb{F}_{p^n}[t]$. Como este cuerpo es un retículo y la cantidad de coeficientes es finita, existe un $n_0 \in \mathbb{Z}^+$ con el que se tiene $p(t) \in \mathbb{F}_{p^{n_0}}[t]$. Todas las raíces de este polinomio se encuentran en una extensión finita de $\mathbb{F}_{p^{n_0}}$, es decir en algún $\mathbb{F}_{p^m} \subset \cup \mathbb{F}_{p^n}$ con $m \in \mathbb{Z}^+$ y $n_0 \mid m$. □

Capítulo 3

Raíces de la unidad en los enteros p-ádicos

La obtención de raíces n-ésimas de la unidad sobre el cuerpo de los números p-ádicos nos remite al lema de Hensel y al método de Newton. Una introducción a estos conceptos y técnicas elementales, así como las correspondientes pruebas, pueden encontrarse en la tesis de Condori [2] o de Gayta [3]. En adelante asumiremos que los polinomios mencionados son mónicos; esto por una sencilla razón: al multiplicar $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$ por el entero p-ádico a_n^{n-1} resulta

$$g(a_n x) = a_n^{n-1} f(x) = (a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_1 a_n^{n-2}(a_n x) + a_n^{n-1} a_0,$$

y resolver $g(x) = 0$ es técnicamente lo mismo que resolver $f(x) = 0$.

3.1. Un repaso de los números p-ádicos

Fijemos un primo arbitrario $p \in \mathbb{Z}^+$. La **norma p-ádica** de un número racional, denotada por $|\ .\ |_p$, está definida como

$$\left| p^n \frac{x}{y} \right|_p = p^{-n},$$

siempre que x e y sean relativamente primos con p. Para 0 ponemos $|\ 0\ |_p = 0$. Es conocido que la norma p-ádica verifica las siguientes propiedades:

i) $\mid x \mid_p \geq 0$, con igualdad si y sólo si $x = 0$,

ii) $\mid xy \mid_p = \mid x \mid_p \mid y \mid_p$,

iii) $\mid x+y \mid_p \leq máx\{\mid x \mid_p, \mid y \mid_p\}$ (llamada **desigualdad triangular ultramétrica o no arquimediana**).

Al considerar $\mathbb{Q}$ con la norma p-ádica $\mid . \mid_p$, resulta que $\mathbb{Q}$ no es completo. Será su compleción $\mathbb{Q}_p$ la que dará origen al cuerpo de los números p-ádicos. Resulta, al igual que $\mathbb{R}$, que $\mathbb{Q}_p$ hereda una estructura algebraica compatible con la estructura métrica. Claramente de la definición se aprecia que el conjunto de valores para $\mid . \mid_p$ en $\mathbb{Q}_p$ es $\{0\} \cup \{p^m : m \in \mathbb{Z}\}$.

Los elementos del anillo $\mathbb{Z}_p = \{z \in \mathbb{Q}_p :\mid z \mid_p \leq 1\}$ serán llamados **enteros p-ádicos**. Notemos que sus expansiones p-ádicas tienen la forma siguiente: $b_0 + b_1 p + b_2 p^2 + \cdots$, con $b_i \in \{0, 1, 2, \ldots, p-1\}$. Acá no hay que dejarse engañar por la notación: este conjunto no es el anillo cociente $\mathbb{Z}/(p)$.

Fijado un primo p, por el teorema fundamental de la aritmética, para cada $a \in \mathbb{Z}$ existe un único n natural tal que $a = p^n r$, con $(r, p) = 1$. Basándonos en ello definimos la **valuación p-ádica** de un número racional como la función

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

dada por

$$v_p(x) = \begin{cases} máx\{n \in \mathbb{Z} : p^n \mid x\} & si \quad x \in \mathbb{Z}^*, \\ v_p(a) - v_p(b) & si \quad x = \frac{a}{b} \in \mathbb{Q}, \\ \infty & si \quad x = 0. \end{cases}$$

De la definición podemos deducir algunas propiedades.

i) Se cumple $v(x) = \infty$ si y sólo si $x = 0$;

ii) se cumple $v(xy) = v(x) + v(y)$;

iii) se cumple $v(x + y) \geq \text{mín}\{v(x), v(y)\}$, para todo $x, y \in \mathbb{Q}_p$.

Para cada número natural k, el conjunto $\mathcal{O}_{p^k} = \{z \in \mathbb{Z}_p :| z |_p \leq p^{-k}\}$ es un ideal de $\mathbb{Z}_p$. En términos prácticos $\mathcal{O}_{p^k}$ es el conjunto de los enteros p-ádicos divisibles por p^k. Denotamos por $E_{p^k} = \mathbb{Z}_p/\mathcal{O}_{p^k}$ el respectivo anillo cociente.

Es claro que para $k = 1$ el ideal $\mathcal{O}_p$ es máximal, y por ello $\mathbb{Z}_p/\mathcal{O}_p$ es un cuerpo. Es más, es el único ideal maximal de $\mathbb{Z}_p$. Como $\{0, 1, \ldots, p-1\}$ son representantes de este cociente, el cuerpo resulta finito e identificable con $\mathbb{F}_p$. Es más, la función

$$\begin{array}{rccc} \varepsilon : & \mathbb{Z}_p & \to & \mathbb{F}_p \\ & a = \sum_{i\geq 0} a_i p^i & \mapsto & a_0 \, mód \, p \end{array}$$

define un homomorfismo llamado **reducción módulo p**. Este homomorfismo es sobreyectivo con núcleo

$$\{a \in \mathbb{Z}_p : a_0 = 0\} = \left\{ \sum_{i\geq 1} a_i p^i = p \sum_{j\geq 0} a_j p^j = p\mathbb{Z}_p \right\} = \mathcal{O}_p.$$

Proposición 3.1. *El grupo multiplicativo $\mathbb{Z}_p^\times$ de elementos invertibles en el anillo $\mathbb{Z}_p$ consiste de los enteros p-ádicos de valuación cero; esto es, se tiene*

$$\mathbb{Z}_p^\times = \left\{ \sum_{i\geq 0} a_i p^i : a_0 \neq 0 \right\}.$$

Demostración. Si un entero p-ádico es invertible, también lo es su proyección en $\mathbb{F}_p$. Así se tiene $\varepsilon(a) \neq 0$ y por lo tanto se cumple $a \notin \mathcal{O}_p$. Para la recíproca tenemos que mostrar que todo entero p-ádico a con $\upsilon(a) = 0$ es invertible. En este caso la reducción $\varepsilon(a) = a_0 \in \mathbb{F}_p$ no es cero, y por lo consiguiente es invertible en este cuerpo. De este modo existe un $b_0 \in \{1, \ldots, p-1\}$ tal que $a_0 b_0 \equiv 1 \, mód \, p$. Escribamos $a_0 b_0 = 1 + kp$. Si desarrollamos $a = a_0 + p\alpha$ con $\alpha \in \mathbb{Z}_p$, se ha de tener

$$a \cdot b_0 = 1 + kp + p\alpha b_0 = 1 + k'p$$

donde $k' = k + \alpha b_0$ es un entero pádico. Esto significa que es suficiente mostrar que todo entero p-ádico de la forma $1 + kp$ es invertible debido a que podemos escribir

$$a \cdot b_0(1 + kp)^{-1} = 1\,, \quad a^{-1} = b_0(1 + kp)^{-1}.$$

En resumen, es suficiente tratar el caso $a_0 = 1, a = 1 + kp$. Pero como se cumple

$$(1 + kp)^{-1} = 1 - kp + (kp)^2 - \ldots,$$

expansión que converge pues $| \, kp \, |_p \leq p^{-n}$, obtenemos la prueba deseada. □

Fácilmente se puede deducir la igualdad

$$\mathbb{Z}_p^{\times} = \{x \in \mathbb{Q}_p :| \, x \, |_p = 1\},$$

propiedad que dejamos como ejercicio para el lector.

El concepto de congruencia en $\mathbb{Z}$ nos permite estudiar a los números enteros clasificándolos en distintas clases de equivalencia. La idea en nuestro contexto es imitar lo anterior. Definamos la relación $a \equiv b \, (mód \, p)$ siempre que se tenga $| \, a-b \, |_p < 1$, caso contrario escribiremos $a \not\equiv b \, (mód \, p)$. En general ponemos $a \equiv b \, (mód \, p^n)$ si $a - b \in \mathcal{O}_{p^n}$, para $n \geq 1$ dado. Esta relación de congruencia coincide con la de los enteros para $a, b \in \mathbb{Z}$.

Un fácil ejercicio basado en este concepto es el siguiente hecho. De $\alpha \in \mathbb{Z}^{\times}$, se sigue $\alpha^{p-1} \equiv 1 \, (mód \, \mathcal{O}_p)$, pues esta propiedad es ya válida en $\mathbb{Z}_p/\mathbb{O}_p \simeq \mathbb{F}_p$.

Presentamos a continuación el lema de Hensel, el mismo que nos garantiza existencia de raíces p-ádicas de ciertas ecuaciones.

Lema 3.2. *(Lema de Hensel) Sea $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ un polinomio con coeficientes enteros p-ádicos y sea $f'(x) = c_1 + 2c_2 x + \cdots + n c_n x^{n-1}$ su derivada formal. Si a_0 es un entero p-ádico tal que $f(a_0) \equiv 0 \, (mód \, p)$ y $f'(a_0) \not\equiv 0 \, (mód \, p)$, entonces existe un único entero p-ádico x_0 sujeto a $x_0 \equiv a_0 (mód \, p)$ que satisface $f(x_0) = 0$.*

Demostración. El lector interesado en la prueba puede consultar [2]. □

Queda claro que el lema de Hensel nos 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. Veamos un caso de cerca a modo de ilustración.

Ejemplo 3.3. Utilizemos el lema de Hensel para resolver $x^2 + 1 = 0$ en $\mathbb{Q}_5$.

Para $f(x) = x^2 + 1$ en $\mathbb{Q}_5[x]$, tentamos con $a_0 = 2$. Al realizar los cálculos respectivos tenemos $f(a_0) = 5$, $f'(a_0) = 4$. Como se ve, ellos satisfacen las hipótesis

y garantizan la existencia de un entero 5-ádico x_0 que cumple $x_0^2 = -1$; realmente hay dos soluciones pues también $a_0 \equiv 3\,(mód\,5)$ da cabida a otra solución.

Desarrollemos al detalle la primera opción $x_0 \equiv 2\,(mód\,5)$. El valor x_0 tendrá una expansión $x_0 = 2 + b_1 5 + b_2 5^2 + \cdots$, con enteros $b_i \in \{0, 1, \ldots, 4\}$.

Veamos cómo calcular los valores $b_1, b_2, b_3, \ldots$.

Paso 1. Sea $a_1 = 2 + b_1 5$ con b_1 por determinar. Como ya tenemos $b_0 = 2$, para u entero resolvemos $f(b_0) \equiv u5\,(mód\,5^2)$, es decir $5 \equiv u5\,(mód\,5^2)$, y hallamos $u = 1$. Deseamos que se satisfaga $f(a_1) \equiv 0\,(mód\,5^2)$ y ello sucederá si $u \cdot 5 + f'(b_0)b_1 \cdot 5 \equiv 0\,(mód\,5^2)$, es decir si se cumple $u + f'(b_0)b_1 \equiv 0\,(mód\,5)$; esto es $1 + 4b_1 \equiv 0\,(mód\,5)$ y hallamos el valor $b_1 = 1$. Entonces tenemos $a_1 = 2 + 1 \cdot 5$, $f(a_1) = 50$ y $f'(a_1) = 14$, éste último número congruente a $f'(a_0) = 4$ módulo 5.

Paso 2. De este modo se ha de tener $a_2 = 2 + 1 \cdot 5 + b_2 \cdot 5^2$. Sigamos el mismo proceso anterior. De $50 \equiv u5^2\,(mód\,5^3)$ hallamos $u = 2$; de $2 + 14b_2 \equiv 0\,(mód\,5)$, $b_2 = 2$, y concluimos la igualdad $a_2 = 2+1\cdot 5+2\cdot 5^2$; con ellos tenemos $f(a_2) = 3250$, junto con $f'(a_2) = 114$, valor también congruente a $f'(a_0) = 4$ módulo 5.

Paso 3. Sea $a_3 = 2 + 1 \cdot 5 + 2 \cdot 5^2 + b_3 5^3$. De $3250 \equiv u5^3\,(mód\,5^4)$, es decir $u = 1$, obtenemos $1 + 14b_3 \equiv 0\,(mód\,5)$, satisfecho por $b_3 = 1$. Entonces tendremos $a_3 = 2+1\cdot 5+2\cdot 5^2+1\cdot 5^3$. Con la misma tónica podemos encontrar sucesivamente los restantes valores para a_i. Por lo expuesto, la raíz 5-ádica será $x_0 = 2, 131\ldots_{(5)}$. La otra raíz 5-ádica será, por supuesto, $-x_0$.

A continuación presentamos otro método iterativo, llamado el **método de Newton**. Éste, que refina un tanto el lema de Hensel, nos permite, partiendo de un entero p-ádico con ciertas características, construir una sucesión que converge a una raíz p-ádica de un polinomio.

Teorema 3.4. *(Método de Newton) Sea $f(x) \in \mathbb{Z}_p[x]$. Supongamos que a_0 sea un entero p-ádico que satisface la relación*

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

Entonces a_0 puede refinarse a un 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

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

Demostración. El lector interesado en la prueba puede consultar [2]. □

Ejemplo 3.5. Consideremos el polinomio $f(x) = x^3+2x^2-5x-6$ sobre $\mathbb{Q}$. Al evaluar en todos los factores de 6, es decir en $\pm1, \pm2, \pm3, \pm6$, se deduce que $f(x)$ no acepta factores lineales y por ende resulta irreducible. Analicemos este polinomio sobre $\mathbb{Q}_2$, específicamente determinemos si preserva la propiedad de ser irreducible. Para $a_0 = 0$ se tiene $f(0) = -6$ y $f'(0) = -5$; por consiguiente se cumple $r = \left| \frac{f(0)}{f'(0)^2} \right|_2 = 2^{-1} < 1$, y el método de Newton es aplicable.

Si a es la raíz prometida por el teorema, se tiene $v(a-a_0) = v(a-0) \geq v(\frac{f(0)}{f'(0)}) = 2$. Siguiendo la secuencia obtenemos

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = -\frac{6}{5}, \qquad v(a + \frac{6}{5}) \geq v(\frac{f(a_1)}{f'(a_1)}) = \frac{1}{16} \quad \text{en una primera iteración;}$$

$$a_2 = a_1 - \frac{f(a_1)}{f'(a_1)} = -\frac{966}{685}, \quad \text{etcétera.}$$

Como se cumple $-\frac{966}{685} = -1,00110011\ldots$ tenemos que la raíz 2-ádica a tendrá la forma aproximada $a = -1,00110011\ldots$.

3.2. Factorización p-ádica

Veamos un resultado que generaliza el lema de Hensel presentado al inicio, el mismo que nos permite factorizar polinomios en $\mathbb{Z}_p$ en vez de hallar raíces, denominado a veces **lema de Hensel versión 2**.

Empecemos con dos definiciones. Decimos que un polinomio $f \in \mathbb{Z}_p[x]$ es **primitivo** si $\overline{f} \neq \overline{0}$ donde $\overline{f}$ es la proyección a $\mathbb{F}_p[t]$. Por otro lado, sea $g = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{Q}_p[x]$ cualquiera y pongamos $\overline{v}(g) = \text{mín}\{v(b_0), \ldots, v(b_m)\}$. Por ejemplo, cuando g es primitivo tendremos $\overline{v}(g) = 0$.

Teorema 3.6. *(Lema de Hensel versión 2) Sea $f \in \mathbb{Z}_p[x]$ primitivo. Supongamos que G y H sean polinomios sobre $\mathbb{F}_p$, relativamente primos y tales que cumplen*

$$\overline{f} = G \cdot H.$$

Entonces existen $g, h \in \mathbb{Z}_p[x]$ que satisfacen

1. *$f = g \cdot h$;*
2. *$\overline{g} = G, \overline{h} = H$;*
3. *grad g= grad G.*

Demostración. Consultar [2]. □

Ejemplo 3.7. Consideremos el polinomio primitivo

$$f(x) = x^4 + 6x^3 + 4x^2 + 3x - 2 \text{ en } \mathbb{Z}_5[x].$$

Al aplicar reducción módulo 5 tenemos $\overline{f}(t) = (t^2 + t + 1)(t^2 + 3) \neq \overline{0}$. Para aplicar el lema de Hensel versión 2 identificamos

$$\begin{aligned} G(t) &= t^2 + t + \overline{1}, \quad & H(t) &= t^2 + \overline{3}, \quad & \text{en } \mathbb{F}_5[t]; \\ g_1(x) &= x^2 + x + 1, \quad & h_1(x) &= x^2 + 3, \quad & \text{en } \mathbb{Z}_5[x]. \end{aligned}$$

Como los polinomios G y H son relativamente primos en $\mathbb{F}_5[x]$, no es sorpresa que existen $a = -3x - 6, b = 3x + 9$ sobre $\mathbb{Z}_5[x]$ tales que

$$\overline{a}G + \overline{b}H = \overline{1} \quad \text{en } \mathbb{F}_5[t].$$

Al tomar valuaciones respectivas, conseguimos $\overline{v}(f - g_1h_1) = \overline{v}(5x^3 + 5x^2 + 5x) = 1$, $\overline{v}(ag_1 + bh_1 - 1) = 1$. Como mín$\{f - g_1h_1, ag_1 + bh_1 - 1\} = 1$, tenemos ya una solución módulo el ideal $\mathcal{O}_5[x]$.

Para la segunda iteración del procedimiento tentamos con polinomios g_2, h_2 de la forma

$$g_2 = g_1 + 5u, \ h_2 = h_1 + 5v,$$

donde $u, v \in \mathbb{Z}_5[x]$.

De este modo u es el resto y q el cociente de la división $\frac{(f-g_1h_1)}{5}b$ por g_1, que resulta ser $u=0$ y $q=3x^2+9x$. Para hallar v, calculamos $\frac{(f-g_1h_1)}{5}a+qh_1 = 5x^4+10x^2+x\,(mód\,5)$, de ahí obtenemos $v=x$ y deducimos las igualdades

$$\begin{aligned} g_2(x) &= x^2+x+1 \quad = x^2+x+1,00\ldots \\ h_2(x) &= x^2+5x+3 \quad = x^2+10,00\ldots x+3,00\ldots \end{aligned}$$

donde $5=10,00\ldots$, $3=3,00\ldots$ y $1=1,00\ldots$ módulo 5. Todo esto desemboca en una eficaz aproximación módulo $\mathcal{O}_5^2[x]$.

Veamos algunas consecuencias que se derivan de esta versión del lema de Hensel.

Corolario 3.8. *Sea $f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in\mathbb{Q}_p[x]$ irreducible. Si se tiene $a_n\in\mathbb{Z}_p$, entonces todos los a_i pertenecen a $\mathbb{Z}_p$.*

Demostración. Procedamos por contradicción. Supongamos que se tenga $\mid a_i \mid > 1$ para algún $i=1,\ldots,n-1$. Al multiplicar f por una potencia positiva adecuada del primo p obtenemos un nuevo polinomio g con coeficientes enteros p-ádicos: este g es primitivo, no constante y su coeficiente principal es una potencia positiva de p. Se sigue que

$$\overline{g}=\overline{g}\cdot\overline{1}$$

es una factorización de $\overline{g}$ que satisface

$$0<grad\,\overline{g}<\overline{f}=n.$$

Por el lema de Hensel-versión 2 existen polinomios G y H sobre $\mathbb{Z}_p$ con los cuales se tiene $grad\,G=grad\,\overline{g}$ y $g=GH$. De esto deducimos inmediatamente la existencia de una factorización propia de f, lo cual contradice la irreducibilidad de f. □

Un polinomio $f(x)\in\mathbb{Z}_p[x]$ de grado $n\geq 1$ que satisface las siguientes propiedades

$$f(x)\equiv x^n\,(mód\,p),\ \ f(0)\not\equiv 0\,(mód\,p^2)$$

es llamado un **polinomio de Eisenstein**. Es claro que un polinomio de Eisenstein es irreducible en los enteros p-ádicos.

Si f resulta un polinomio irreducible sobre $\mathbb{Z}_p$, no necesariamente ello implica que $\overline{f}$ también lo sea sobre $\mathbb{F}_p$. Por ejemplo x^2+px+p es un polinomio de Eisenstein, pero su reducción $\overline{f}=t^2$ es potencia de t en $\mathbb{F}_p[t]$.

Corolario 3.9. *Si $f \in \mathbb{Z}_p[x]$ es mónico e irreducible sobre $\mathbb{Q}_p$, entonces $\overline{f}$ es una potencia de un polinomio irreducible sobre $\mathbb{F}_p$.*

Demostración. Esto es otra consecuencia del lema de Hensel versión 2. □

3.3. Extensiones p-ádicas

Dado un cuerpo $K \supset \mathbb{Q}_p$, con métrica no arquimediana $|\,|_K$, decimos que K es una **extensión p-ádica** si cumple $\mid x \mid_K = \mid x \mid_p$ para todo $x \in \mathbb{Q}_p$.

Como la única norma que usaremos es la p-ádica o sus extensiones, a partir de ahora, si en el contexto es claro, utilizaremos $\mid x \mid$ en vez de $\mid x \mid_p$.

Repasemos un concepto básico en extensiones de cuerpos como es la norma algebraica de un elemento. El uso de la palabra norma no debe ser confundido con el uso que se le presta en el análisis funcional.

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 los distintos $\mathbb{Q}_p$-monomorfismos de K en una clausura algebraica de $\mathbb{Q}_p$.

Como un caso especial, si u es raíz del polinomio irreducible

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

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 $\mathbb{Q}_p$.

Como consecuencia de esta observación se tiene $N_{K/\mathbb{Q}_p}(u) = (-1)^n a_0$ como caso particular.

La norma algebraica $N_{K/\mathbb{Q}_p}$ cumple con las siguientes propiedades:

- $N_{K/\mathbb{Q}_p}(uv) = N_{K/\mathbb{Q}_p}(u)N_{K/\mathbb{Q}_p}(v)$, llamada 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 $a \in \mathbb{Q}_p$.

Teorema 3.10. *Sea K una extensión finita de grado n sobre $\mathbb{Q}_p$. Entonces*

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

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

Demostración. Esto es una consecuencia casi inmediata de las tres propiedades enumeradas arriba. Consultar [2]. □

Notemos que este nuevo valor absoluto $|\cdot|_K$ cumple con varias propiedades más o menos obvias dada su definición.

1. *El conjunto de valores no nulos de $|\cdot|_K$ en K es subconjunto de $\{p^{\frac{m}{n}} : m \in \mathbb{Z}\}$, donde $n = [K : \mathbb{Q}_p]$.*
2. *Cualquier norma sobre K equivalente a $|\cdot|_K$ es de la forma $|\cdot|_K^s$, para algún $s > 0$. De todas ellas, solamente $|\cdot|_K$ es la extensión p-ádica.*

Ejemplo 3.11. La compleción $\mathbb{R}$ de $\mathbb{Q}$ con respecto al valor absoluto usual posee solamente una extensión algebraica, llamada $\mathbb{C}$. Por lo tanto el valor absoluto usual $|\,.\,|$ en $\mathbb{R}$ posee una única extensión sobre $\mathbb{C}$, dada por

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

Dada una extensión K de $\mathbb{Q}_p$, consideramos los conjuntos

$$\mathbb{Z}_K = \{x \in K :| x |_K \leq 1\} \text{ y } \mathcal{O}_K = \{x \in K :| x |_K < 1\}.$$

Entonces $\mathbb{Z}_K$ resulta **el anillo de enteros de** K y $\mathcal{O}_K$ un ideal maximal en éste. Por lo tanto, el anillo cociente $\mathbb{Z}_K/\mathcal{O}_K$ es un cuerpo, llamado **cuerpo de clases residuales** de K.

El grado de $\mathbb{Z}_K/\mathcal{O}_K$ sobre $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ es llamado el **grado de clases residuales** de K y lo denotamos por f, valor que por definición coincide con $[\mathbb{Z}_K/\mathcal{O}_K : \mathbb{Z}_p/p\mathbb{Z}_p]$.

Sea $n = [K : \mathbb{Q}_p]$. Entonces $\mid K^\times \mid_K = \{\mid x \mid_K : x \in K^\times\}$ es un subgrupo del grupo cíclico multiplicativo generado por $p^{-1/n}$. Así $\mid K^\times \mid_K$ es generado por p^{-1/e_K} para algún divisor positivo e_K de n. Llamemos a e_K **índice de ramificación** de la extensión. Notemos que éste queda definido también por el índice de grupos $[\mid K^\times \mid : \mid \mathbb{Q}_p^\times \mid]$.

Decimos que $\pi \in \mathbb{Z}_K$ es un **uniformizador** si se tiene $\pi \in \mathcal{O}_K$ mas no así $\pi \notin \mathcal{O}_K^2$. Por ejemplo en $\mathbb{Z}_p$, el elemento $\pi = p$ es un uniformizador. Al igual que en los enteros p-ádicos, cada $x \in \mathbb{Z}_K$ puede ser escrito como

$$x = a_0 + a_1\pi + a_2\pi^2 + \ldots, \text{ con } a_i \in \mathbb{Z}_K/\mathcal{O}_K.$$

A continuación veamos tres lemas técnicos que nos conducirán a una fórmula que relaciona e, f y n.

Lema 3.12. *Sean* $a_1, \ldots a_n \in K$. *Si* $\mid a_1 \mid > \mid a_i \mid$ *para* $i = 2, \ldots, n$, *entonces se cumple*

$$\mid a_1 \mid = \mid a_1 + \ldots + a_r \mid .$$

Demostración. Sabemos que todo triángulo con una norma p-ádica resulta isósceles y $\mid a_1 \mid > \mid a_2 \mid$ obliga a tener $\mid a_1 + a_2 \mid = \mid a_1 \mid > \mid a_3 \mid$. Con el mismo proceso se obtiene $\mid a_1 + a_2 + a_3 \mid = \mid a_1 + a_2 \mid = \mid a_1 \mid > \mid a_4 \mid$. Luego de un número finito de iteraciones llegamos a $\mid a_1 \mid = \mid a_1 + \ldots + a_r \mid$. □

Lema 3.13. *Sean* $x_1, \ldots, x_f$ *elementos en* $\mathbb{Z}_K$ *tales que* $x_1 + \mathcal{O}_K, \ldots, x_f + \mathcal{O}_K$ *son linealmente independientes sobre* $\mathbb{F}_p$, *y sean* $a_1, \ldots, a_f \in \mathbb{Q}_p$. *Entonces se cumple*

$$\mid a_1x_1 + \cdots + a_fx_f \mid = \max_r \mid a_r \mid_p .$$

Demostración. Si $a_r = 0$ para todo $r \in \{1, ..., f\}$ el resultado es obvio. Caso contrario, supongamos se tenga $\mid a_1 \mid = \text{máx}_r \mid a_r \mid_p$ y definamos $b_r = a_r/a_1$ $(r = 1, ..., f)$. Entonces se tiene $\mid b_r \mid \leq 1$ y $b_1 = 1$. Para concluir la demostración falta ver que se cumple

$$\mid x_1 + b_2x_2 + \cdots + b_fx_f \mid = 1.$$

En primer lugar es claro que se tiene $\mid x_1 + b_2x_2 + \cdots + b_fx_f \mid \leq 1$, ya que se cumple $x_1 + b_2x_2 + \cdots + b_fx_f \in \mathbb{Z}_K$. Si la desigualdad fuese estricta, se tendría

$$x_1 + b_2x_2 + \cdots + b_fx_f \in \mathcal{O}_K,$$

lo cual a su vez implicaría

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

Esto quiere decir que $\mathcal{O}_K$ sería una combinación lineal de los $x_i + \mathcal{O}_K$ con coeficientes en $\mathbb{F}_p$, lo cual contradiría la independencia lineal de los $x_i + \mathcal{O}_K$. □

Lema 3.14. *Sea π un uniformizador de $\mathbb{Z}_K$ con $\mid \pi \mid = p^{-1/e}$, y sean $x_1, \ldots, x_f$ elementos de $\mathbb{Z}_K$ tales que $\overline{x_1}, \ldots, \overline{x_f}$ forman una base de $\mathbb{Z}_K/\mathcal{O}_K$ sobre $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$. Entonces $\mathbb{Z}_K$ es un $\mathbb{Z}_p$- módulo libre con base*

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

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

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

Demostración. Sea $x \in \mathbb{Z}_K$ distinto de cero. Como se tiene $\mid p^r\pi^j \mid = \mid \pi^{er+j} \mid$, se puede observar que $er + j$ recorre todos los enteros no negativos mientras $r \geq 0$ y $j \in \{0, \ldots, e-1\}$. Por lo tanto $\mid p^r\pi^j \mid$ asume todos los valores posibles de la norma $\mid \cdot \mid_K$ menores o iguales a 1. De este modo para algún r y j se cumple $\mid x \mid = \mid p^r\pi^j \mid$. En particular para $y = x/p^r\pi^j$ se tiene $\mid y \mid = 1$. Luego, en el espacio vectorial $\mathbb{Z}_K/\mathcal{O}_K$ sobre $\mathbb{F}_p$, existen $a_r \in \mathbb{Z}_p$, no todos en $\mathcal{O}_K$, tales que se cumple

$$y + \mathcal{O}_K = (a_1 + \mathcal{O}_p)(x_1 + \mathcal{O}_K) + \cdots + (a_f + \mathcal{O}_p)(x_f + \mathcal{O}_K).$$

Al operar se tiene

$$y + \mathcal{O}_K = (a_1x_1 + \cdots + a_fx_f) + \mathcal{O}_K;$$

lo que significa la desigualdad

$$| \, y - (a_1x_1 + \cdots + a_fx_f) \, | < 1.$$

Al regresar a las coordenadas originales logramos

$$| \, x - (a_1x_1 + \cdots + a_fx_f)p^r\pi^j \, | < | \, p^r\pi^j \, | \, .$$

Al escribir $z = x - (a_1x_1 + \cdots + a_fx_f)p^r\pi^j$, se tiene

$$x = (a_1x_1 + \cdots + a_fx_f)p^r\pi^j + z,$$

donde se cumple $| \, z \, | < | \, p^r\pi^j \, |$.

Usaremos el resultado anterior reiteradamente para construir una serie convergente. Sea $w \in \mathbb{Z}_K$ no nulo y que satisface $| \, w \, | \leq 1$. Por lo ya trabajado se puede escribir

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

donde $a_{00i} \in \mathbb{Z}_p$ y $| \, w_1 \, | < 1$. De este modo se tiene $| \, w_1 \, | \leq | \, \pi \, |$ y continuamos con

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

donde $| \, w_2 \, | < | \, \pi \, |$ y así $| \, w_2 \, | < | \, \pi^2 \, |$. Al repetir la iteración $e - 1$ 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 $| \, w_e \, | \leq | \, \pi^e \, | = | \, p \, |$. De aquí pasamos a

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

donde $| \, w_{e+1} \, | \leq | \, p\pi \, |$. Un paso adicional da

$$w_{e+1} = (a_{111}x_1 + \cdots + a_{11f}x_f)p\pi + w_{e+2},$$

con $| \, w_{e+2} \, | \leq | \, p\pi^2 \, |$.

En general w puede ser escrito como

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

Al tomar límite cuando $m \to \infty$ conseguimos

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

donde $r = 0, 1, \ldots$ y $j = 0, 1 \ldots, e-1$. Por lo tanto se tiene

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

Las series $\sum_r a_{rjk}p^r$ convergen puesto que se cumple $a_{rjk} \in \mathbb{Z}_p$ y $\mid a_{rjk}p^r \mid \to 0$. Es más, si $s_n = \sum_r^n a_{ijk}p^r$ denota la n-ésima suma parcial entonces se satisface $\mid s_n \mid \leq 1$ para todo $n \in \mathbb{N}$. □

Teorema 3.15. *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. Empecemos probando la desigualdad $ef \leq n$. Sean $x_1, ..., x_f$ elementos en $\mathbb{Z}_K$ tales que $x_1 + \mathcal{O}_K, ..., x_f + \mathcal{O}_K$ sean linealmente independientes sobre $\mathbb{F}_p$; esto es posible debido a que f es la dimensión del $\mathbb{F}_p$-espacio vectorial $\mathbb{Z}_K$. También, sean $y_1, ..., y_e$ distintos elementos de $\mathbb{K}^\times$ elegidos de modo que $\mid y_1 \mid\mid \mathbb{Q}_p^\times \mid, ..., \mid y_e \mid\mid \mathbb{Q}_p^\times \mid$ sean las distintas clases laterales multiplicativas; esto es posible por la definición del índice e.

Deseamos probar que los $x_r y_s$ $(r = 1, \ldots, f;\ s = 1, \ldots, e)$ son linealmente independientes sobre $\mathbb{Q}_p$; con ello concluiremos la desigualdad deseada $ef \leq n = dim_{\mathbb{Q}_p} K$. Supongamos que se tenga

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

donde $c_{rs} \in \mathbb{Q}_p$. Al agrupar coeficientes podemos reescribir

$$\sum_s (\sum_r c_{rs}x_r)y_s = 0.$$

Por el Lema 3.13, para cada s fijo se tiene

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

Como las clases laterales $| y_1 \,||\, \mathbb{Q}_p^* |, ..., | y_e \,||\, \mathbb{Q}_p^* |$ asumen valores disjuntos, las valuaciones $\max_r | c_{rs}y_s |$ serán distintas (salvo que todos valgan 0), y en uso del Lema 3.12 se tiene la igualdad.

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

Por supuesto la única posibilidad de tener $\max_s \max_r | c_{rs} \,||\, y_s | = 0$ pasa por $c_{rs} = 0$ para todo r, s. Esto confirma la desigualdad $ef \leq n$. La desigualdad opuesta es consecuencia inmediata del Lema 3.14. □

De aquí en adelante para una extensión finita K de $\mathbb{Q}_p$ usaremos la siguiente terminología.

- Si $e = 1$, decimos que la **extensión K no ramifica**,
- si $e = n$, decimos que la **extensión K ramifica totalmente**,
- si p no divide a e, decimos que la **extensión K ramifica mansamente**,
- si $e = p^k$ para algún k entero positivo, decimos que la **extensión K ramifica salvajemente**.

Ejemplo 3.16. Sea $K = \mathbb{Q}_3(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}_3\}$, donde $\sqrt{3}$ es una de las raíces de $f(x) = x^2 - 3$. Como $f(x)$ es un polinomio de Eisenstein, $f(x)$ es irreducible: en términos prácticos se tiene $\sqrt{3} \notin \mathbb{Q}_3$. Sin embargo la norma de $\sqrt{3}$ puede ser fácilmente calculada en cualquier extensión que lo contenga vía

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

y así $| \sqrt{3} |_3$ no pertenece al conjunto de valores que asume $| \cdot |_3$ en $\mathbb{Q}_3$. En general, para $a, b \in \mathbb{Q}_3$ tenemos

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

De este modo obtenemos

$$\begin{aligned}
&\mathbb{Z}_K = \{a + b\sqrt{3} : a, b \in \mathbb{Z}_3\},\\
&\mathcal{O}_K = \{a + b\sqrt{3} : a \in 3\mathbb{Z}_3, b \in \mathbb{Z}_3\} = \sqrt{3}\mathbb{Z}_K,\\
&\mathbb{Z}_K/\mathcal{O}_K \cong \mathbb{Z}_3/3\mathbb{Z}_3 = \mathbb{F}_3.
\end{aligned}$$

Por lo tanto, en este caso particular se tiene $e_K = 2, f_K = 1$, y la extensión K es total y mansamente ramificada.

Mostremos algunos ejemplos de extensiones cuadráticas de $\mathbb{Q}_2$.

Ejemplo 3.17. Consideremos el polinomio $f(x) = x^2 - 2 \in \mathbb{Q}_2[x]$, de Eisenstein. Sea $\sqrt{2}$ raíz en alguna extensión. Por supuesto, como se tiene

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

la norma $| \sqrt{2} |_2$ no pertenece al conjunto de valores de $| \cdot |_2$ en $\mathbb{Q}_2$. En general, para $a, b \in \mathbb{Q}_2$ en cualquier extensión obtendremos

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

Esto quiere decir que para $K = \mathbb{Q}_2(\sqrt{2})$ se tiene

$$\begin{aligned}
&\mathbb{Z}_K = \{a + b\sqrt{2} : a, b \in \mathbb{Z}_2\},\\
&\mathcal{O}_K = \{a + b\sqrt{2} : a \in 2\mathbb{Z}_2, b \in \mathbb{Z}_2\} = \sqrt{2}\mathbb{Z}_K,\\
&\mathbb{Z}_K/\mathcal{O}_K \cong \mathbb{F}_2.
\end{aligned}$$

Por lo tanto $e_K = 2, f_K = 1$, y la extensión K es total y salvajemente ramificada.

Ejemplo 3.18. Consideremos el polinomio $p(x) = x^2 - 2x + 2 \in \mathbb{Q}_2[x]$, de Eisenstein, con $1+i$ ($i = \sqrt{-1}$) una raíz del polinomio. Para probar que $\mathbb{Q}_2(1+i)$ es una extensión de grado 2, basta comprobar que se tiene $i \notin \mathbb{Q}_2$. Por el absurdo, supongamos que se tenga $i \in \mathbb{Q}_2$. Entonces éste i anula al polinomio $x^2 + 1 \in \mathbb{Q}_2[x]$. Obligado se tiene $| i |_2 = 1$ e i ha de ser un entero 2-ádico. Al expandir se tendrá $i = a_0 + a_1 2 + a_2 2^2 + a_3 2^3 + \cdots$ con $a_i \in \{0, 1\}$, y de esta manera obtenemos

$$i^2 = a_0^2 + (2a_0a_1)2 + (a_1^2 + 2a_0a_2)2^2 + (2a_0a_3 + 2a_1a_2)2^3 + \cdots = -1.$$

Vía congruencias módulo 2 resulta $a_0^2 \equiv -1$; con solución $a_0 = 1$. Al trabajar con dicho valor y tomar congruencias módulo 2^3 tenemos $1 + (a_1 + a_1^2)2^2 \equiv -1\,(mód\,2^3)$; de ello resulta $1 + (a_1 + a_1^2)2 \equiv 0\,(mód\,2^2)$, congruencia sin solución con a_1 en $\{0, 1\}$; de este modo queda confirmado que i no pertenece a $\mathbb{Q}_2$. Por otro lado, en cualquier extensión resulta obvio que i e $-i$ son conjugados. Concluimos que se cumple

$$| \, i+1 \, |_{\mathbb{Q}_2(i)} = | \, N_{\mathbb{Q}_2(i)/\mathbb{Q}}(i+1) \, |_2^{1/2} = | \, (1+i)(1-i) \, |_2^{1/2} = | \, 2 \, |_2^{1/2} | = 2^{-1/2},$$

es decir $| \, i+1 \, |_{\mathbb{Q}_2(i)}$ no pertenece al conjunto de valores de $| \cdot |_2$ en $\mathbb{Q}_2$.

En general, para $a, b \in \mathbb{Q}_2$ tendremos

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

En resumen, para $K = \mathbb{Q}_2(1+i)$ se tiene

$$\begin{aligned} &\mathbb{Z}_K = \{a + bi : a, b \in \mathbb{Z}_2\}, \\ &\mathcal{O}_K = (1+i)\mathbb{Z}_K, \\ &\mathbb{Z}_K / \mathcal{O}_K \cong \mathbb{F}_2. \end{aligned}$$

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

3.4. Raíces de la unidad en $\mathbb{Z}_p$

Una raíz de la unidad en $\mathbb{Q}_p$ es, por supuesto, un valor $\zeta \in \mathbb{Q}_p$ que satisface $\zeta^n = 1$ para cierto n. Como se cumple $nv(\zeta) = v(1) = 0$, se tiene $v(\zeta) = 0$ y necesariamente ζ es un valor en $\mathbb{Z}_p$ invertible, es decir pertenece a $\mathbb{Z}_p^\times$. En particular cada raíz n-ésima de la unidad tiene una buena reducción módulo p: así tenemos $\overline{\zeta} \in \mathbb{F}_p$, donde $\mathbb{F}_p = \mathbb{Z}/\mathcal{O}_p$. Pondremos $\mu(K)$ para referirnos al conjunto de las raíces de la unidad en un cuerpo K.

El polinomio $t^{p-1} - 1$ tiene $p-1$ raíces distintas en el cuerpo $\mathbb{F}_p$: el lema de Hensel implica entonces que $x^{p-1} - 1$ posee $p-1$ raíces distintas en $\mathbb{Z}_p^\times$. Esto prueba que el cuerpo $\mathbb{Q}_p$ de números p-ádicos siempre contiene un subgrupo cíclico de orden $p-1$ bajo la secuencia de inclusiones

$$\mu_{p-1} \subset \mathbb{Z}_p^\times \subset \mathbb{Q}_p^*,$$

donde μ_{p-1} denota el conjunto de raíces $p-1$-ésimas de la unidad.

En un contexto más amplio puede darse como excepción que dos raíces n-ésimas de la unidad pertenezcan a la misma clase, fenómeno que será tratado más adelante.

Proposición 3.19. *Si p es un número primo impar, el grupo de raíces de la unidad que pertenecen al cuerpo $\mathbb{Q}_p$ es precisamente μ_{p-1}.*

Demostración. Como existe un homomorfismo biyectivo entre $\mathbb{F}_p^*$ y μ_{p-1}, vamos a probar que también existe un homomorfismo biyectivo entre $\mu(\mathbb{Q}_p)$ y $\mathbb{F}_p^*$; de ese modo habrá un homomorfismo biyectivo entre μ_{p-1} y $\mu(\mathbb{Q}_p)$, lo que concluirá la prueba.

Consideremos el homomorfismo canónico

$$\begin{array}{rccc} \varphi: & \mu(\mathbb{Q}_p) & \to & \mathbb{F}_p^* \\ & \zeta & \mapsto & \overline{\zeta}. \end{array}$$

Veamos que es biyectivo. Por el lema de Hensel sabemos que φ es sobreyectivo. Por otro lado, tomemos $\zeta \in \mu(\mathbb{Q}_p)$ una raíz de la unidad de orden n. Entonces se tiene $\zeta \in \mathbb{Z}_p^\times$ y podemos asumir así que se cumple $\zeta = 1 + pt \in Ker(\varphi)$ con $t \in \mathbb{Z}_p$. De este modo se tendrá

$$\zeta^n = (1+pt)^n = 1,$$

y por lo tanto $npt + \binom{n}{2}p^2t^2 + \ldots + p^nt^n = 0$. Al factorizar t y simplificar p se logra

$$t(n + \binom{n}{2}pt + \ldots + p^{n-1}t^{n-1}) = 0.$$

Esto muestra que se deberá tener $t = 0$ (cuando $p \nmid n$) ó $p \mid n$. Para el segundo caso, reemplazamos ζ por ζ^p y n por $\frac{n}{p}$, y efectuamos el mismo cálculo. Si $t \neq 0$, hay dos posibilidades: o podemos proceder indefinidamente (lo cual es irreal) o bien podemos limitarnos a tratar el caso $n = p$. Así tenemos

$$t(p + \binom{p}{2}pt + \ldots + p^{p-1}t^{p-1}) = 0,$$

y como se tiene $p \geq 3$, obtenemos

$$p + \binom{p}{2}pt + \ldots + p^{p-1}t^{p-1} = p + p^2(\ldots) \neq 0,$$

lo cual es imposible. Esto prueba que obligatoriamente se cumple $t = 0$ en todos los casos y $\zeta = 1$ es la única raíz en el núcleo. Luego φ es también inyectiva. □

Cuando p es impar, $p-1$ es par y de este modo -1 pertenece a μ_{p-1}. El número -1 tiene una raíz cuadrada en $\mathbb{Q}_p$ precisamente cuando $(p-1)/2$ es aún par, específicamente cuando cumple $p \equiv 1 \, mód \, 4$, ello debido a que en tal caso tenemos

$$t^{p-1} - 1 = (t^{\frac{p-1}{4}} - 1)(t^{\frac{p-1}{4}} + 1)(t^{\frac{p-1}{2}} + 1)$$

en $\mathbb{F}_p[t]$; esto es parte de la conocida reciprocidad cuadrática. Tenemos así que se cumple

$$\sqrt{-1} \in \mathbb{Q}_p \text{ si y sólo si } p \equiv 1 \,\text{mód}\, 4.$$

Por ejemplo $i = \sqrt{-1}$ puede ser encontrado en $\mathbb{Q}_5, \mathbb{Q}_{13}, \ldots$, más no así en $\mathbb{Q}_7, \mathbb{Q}_{11}$, entre otros cuerpos.

Proposición 3.20. *El grupo de raíces de la unidad en el cuerpo $\mathbb{Q}_2$ es $\mu_2 = \{\pm 1\}$.*

Demostración. Con la notación

$$R = \{x \in \mathbb{Q}_2 : x^n = 1 \,, \text{para algún} \, n \in \mathbb{N}\},$$

debemos demostrar que se cumple $R = \mu_2$. Claramente se tiene $\mu_2 = \{\pm 1\} \subset R$. Recíprocamente, sea $\zeta \in R$. Entonces $\zeta = 1 + 2t \in \mathbb{Z}_2^*$ con $t \in \mathbb{Z}_2$ implica

$$\zeta^n = (1+2t)^n = 1,$$

y por lo tanto también $n2t + \binom{n}{2} 2^2 t^2 + \ldots + 2^n t^n = 0$. Al factorizar t y dividir entre 2 se logra

$$t(n + \binom{n}{2} 2t + \ldots + 2^{n-1} t^{n-1}) = 0.$$

Esto muestra que se deberá tener $t = 0$ (cuando $2 \nmid n$) ó $2 \mid n$. Para el segundo caso, reemplazamos ζ por ζ^2 y n por $\dfrac{n}{2}$, realizamos el mismo cálculo y concluimos que se cumple $t = 0$ ó $2^2 \mid n$. Notamos que o bien se procede indefinidamente o bien caemos en $t = 0$. Finalmente nos concentramos en el caso $n = 2$. Así tenemos

$$(1+2t)^2 = 1,$$

lo cual deriva en $t = 0$ ó $t = -1$; casos que conducen a $\zeta = 1$, $\zeta = -1$, respectivamente. Por consiguiente tenemos $R \subset \mu_2$, lo cual concluye la prueba. □

Lema 3.21. *Para $\eta \in \mathbb{Q}_p^*$, las siguientes propiedades son equivalentes:*

i) η es una unidad ($\eta \in \mathbb{Z}_p^\times$),

ii) η^{p-1} posee raíces n-ésimas para infinitos valores de n.

Demostración. Si η es una unidad, entonces se tiene $\eta \not\equiv 0 \,(mód\, p\mathbb{Z}_p)$ y con ello $\eta^{p-1} \equiv 1 \,(mód\, p\mathbb{Z}_p)$. Al hacer el cambio $a = \eta^{p-1}$ y considerar $x^n - a = 0$ vemos que esta ecuación admite una raíz congruente a 1 módulo p; además, cuando n es coprimo con p se cumple $p'(1) = n \not\equiv 0 \,(mód\, p)$, y el lema de Hensel es aplicable: la ecuación posee solución, y esto quiere decir que existe $\xi \in \mathbb{Z}_p$ tal que $\xi^n = a = \eta^{p-1}$.

Recíprocamente, si $\eta^{p-1} = y_n^n$, tenemos

$$(p-1)v(\eta) = n \cdot v(y_n),$$

y n divide a $(p-1)v(\eta)$. Si ello ocurre para infinitos valores de n, se tiene $v(\eta) = 0$ y por lo tanto ζ es unidad. □

3.5. Extensiones cuadráticas de $\mathbb{Q}_p$

Conseguir raíces cuadradas en $\mathbb{Q}_p$ se convierte en el problema de buscar raíces al polinomio $f(x) = x^2 - a$, donde $a \in \mathbb{Q}_p$. Es más, si $r \in \mathbb{Z}_p$ fuese la raíz cuadrada de alguién, entonces el valor $v(a) = v(r^2) = 2v(r)$ será par. Si dividimos a por una potencia par adecuada de p, podemos conseguir $v(a) = 0$, lo que permite asumir $a \in \mathbb{Z}_p^\times$. Como se tiene $p'(r) = 2r \not\equiv 0 \,(mód\, p)$ para p primo impar, el lema de Hensel es aplicable; el caso $p = 2$ debe ser tratado con cautela.

Recordemos que el **símbolo de residuos cuadráticos de Legendre** se define como

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } a \text{ es un cuadrado módulo } p, \\ -1 & \text{si } a \text{ no es un cuadrado módulo } p. \end{cases}$$

Lema 3.22. *Sea p un primo impar. Consideremos el polinomio $f(x) = x^2 - a \in \mathbb{Z}_p[x]$. Entonces*

1. $f(x)$ no posee ninguna solución si $a \equiv 0 \,(mód\, p)$ y $a \not\equiv 0 \,(mód\, p^2)$, mientras

2. *$f(x)$ posee $\left(\frac{a}{p}\right)+1$ soluciones para $a \not\equiv 0\,(mód\,p)$; es decir, dos soluciones si a es cuadrado módulo p y ninguna si no lo es.*

Demostración. Para la primera parte supongamos que $f(x)=x^2-a$ posea solución en $\mathbb{Q}_p$: sea $\sqrt{a}$ dicha solución. Como se cumple $a \equiv 0\,(mód\,p)$ además de $a \not\equiv 0\,(mód\,p^2)$, tenemos

$$p^{-1} =\mid a \mid_p =\mid \sqrt{a}\sqrt{a} \mid_p =\mid \sqrt{a} \mid_p \mid \sqrt{a} \mid_p =\mid \sqrt{a} \mid_p^2 .$$

De ello obtenemos $\mid \sqrt{a} \mid_p = p^{-\frac{1}{2}}$, lo cual es impensable.

Para la segunda parte trabajemos de acuerdo con el valor $\left(\frac{a}{p}\right)$.

Si $\left(\frac{a}{p}\right)=1$, entonces existe un entero m sujeto a $a \equiv m^2\,(mód\,p)$, y como además se tiene $a \not\equiv 0\,(mód\,p)$, necesariamente $m^2 \not\equiv 0\,(mód\,p)$ implica $m \not\equiv 0\,(mód\,p)$. Al multiplicar por 2 esta última congruencia, como p es un primo impar, obtenemos $f'(m)=2m \not\equiv 0\,(mód\,p)$, y el lema de Hensel es aplicable. Por lo tanto existen dos soluciones ($\pm\sqrt{a} \in \mathbb{Q}_p$).

Si $\left(\frac{a}{p}\right)=-1$, supongamos que $x^2-a=0$ posea solución, digamos $m \in \mathbb{Q}_p$. Así tenemos

$$a \equiv m^2 \equiv b^2\,(mód\,p),$$

para algún b entero con $0<b<p$, lo cual no es compatible con la definición del símbolo. □

Ahora toca decir algo acerca del grupo cociente $\mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$. Al poner $\overline{x}=\{xu^2 : u \in \mathbb{Q}_p^*\}$, dos elementos x_1 y x_2 son acá equivalentes si y sólo si x_1/x_2 es el cuadrado de un número p-ádico.

Este grupo, por inocente que pretenda parecer, permite clasificar las extensiones cuadráticas en cuerpos de característica cero.

Lema 3.23. *Se tiene $\mathbb{Q}_p(\sqrt{d_1})=\mathbb{Q}_p(\sqrt{d_2})$ si y sólo si $\overline{d_1}=\overline{d_2}$ en $\dfrac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*^2}}$.*

Demostración. Empecemos con la ida. Como $\sqrt{d_1} \in \mathbb{Q}_p(\sqrt{d_1}) = \mathbb{Q}_p(\sqrt{d_2})$, se tiene $\sqrt{d_1} = a + b\sqrt{d_2}$ con $a, b \in \mathbb{Q}_p$. Al elevar al cuadrado se logra $d_1 = a^2 + 2ab\sqrt{d_2} + b^2 d_2$. Luego se tiene

$$2ab\sqrt{d_2} = d_1 - a^2 - b^2 d_2.$$

De $d_1 - a^2 - b^2 d_2 \in \mathbb{Q}_p$ se pasa a $2ab\sqrt{d_2} \in \mathbb{Q}_p$, y como la característica de $\mathbb{Q}_p$ es distinta de 2, tenemos $a \cdot b = 0$, lo que conduce a $a = 0$ ó $b = 0$. Si $b = 0$, tenemos $\sqrt{d_1} = a \in \mathbb{Q}_p$, lo cual es una contradicción ya que d_1 no posee raíz cuadrada. En resumen, se debe tener $a = 0$, y con ello $\overline{d_1} = \overline{d_2}$, pues $d_1 = b^2 d_2$.

Recíprocamente, como se satisface $\sqrt{d_1} = k\sqrt{d_2} \in \mathbb{Q}_p(\sqrt{d_1})$ con $k \in \mathbb{Q}_p^*$, obtenemos $\sqrt{d_2} = \dfrac{\sqrt{d_1}}{k} \in \mathbb{Q}_p(\sqrt{d_1})$ y por lo tanto $\mathbb{Q}_p(\sqrt{d_2}) \subset \mathbb{Q}_p(\sqrt{d_1})$. Del mismo modo se consigue $\mathbb{Q}_p(\sqrt{d_1}) \subset \mathbb{Q}_p(\sqrt{d_2})$, y con ello también la igualdad $\mathbb{Q}_p(\sqrt{d_1}) = \mathbb{Q}_p(\sqrt{d_2})$. □

Sea a un entero tal que $1 < a < p$ y que no sea un cuadrado módulo p. Entonces los números a, p y ap no tienen raíz cuadrada en $\mathbb{Q}_p$, lo que conduce fácilmente a $\{\overline{1}, \overline{p}, \overline{a}, \overline{ap}\} \subset \mathbb{Q}_p^{*^2}$. Es más, este conjunto forma una lista completa de representantes como veremos en el siguiente corolario.

Corolario 3.24. *Sean p primo impar y $a \in \{1, \ldots, p-1\}$ sujeto a $\left(\dfrac{a}{p}\right) = -1$ con $1 < a < p$. Entonces $\{\overline{1}, \overline{p}, \overline{a}, \overline{ap}\}$ forma un conjunto completo de representantes de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$. En otras palabras, existen apenas tres extensiones cuadráticas de $\mathbb{Q}_p$. Dos de ellas son totalmente ramificadas.*

Demostración. Sea $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$ cualquiera. Entonces existen $a \in \mathbb{Z}_p^*$ y $n \in \mathbb{Z}^+ \cup \{0\}$ relacionados vía $x = p^n a$, número que resulta cuadrado perfecto si n es par y a es un cuadrado en $\mathbb{Z}_p^\times$. De tenerse $\left(\dfrac{a}{p}\right) = -1$, los elementos $\overline{1}, \overline{p}, \overline{a}, \overline{ap}$ aparecen como los únicos representantes del cociente, es decir, se tiene

$$\frac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*^2}} = \{\overline{1}, \overline{p}, \overline{a}, \overline{ap}\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Como toda extensión cuadrática de $\mathbb{Q}_p$ es generada por la raíz cuadrada de un elemento (toda extensión cuadrática de un cuerpo de característica cero es generado

por una raíz cuadrada), todas la extensiones cuadráticas del cuerpo $\mathbb{Q}_p$ con $p \geq 3$ están dadas por

$$\mathbb{Q}_p(\sqrt{a}),\ \mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{ap}).$$

En virtud del lema anterior vemos que estas extensiones son distintas. Sin embargo, dos de ellas son totalmente ramificadas: $\mathbb{Q}_p(\sqrt{p})$ y $\mathbb{Q}_p(\sqrt{ap})$. Concretamente, para el caso $K = \mathbb{Q}_p(\sqrt{p})$ tenemos

$$\begin{aligned} \mathbb{Z}_K &= \{a + b\sqrt{p} : a, b \in \mathbb{Z}_p\} \\ \mathcal{O}_K &= \{a + b\sqrt{p} : a \in p\mathbb{Z}_p, b \in \mathbb{Z}_p\}. \end{aligned}$$

Se tiene $\mathbb{Z}_K/\mathcal{O}_K \cong \mathbb{F}_p$, y así $f = 1$ y $e = 2$. Para $K = \mathbb{Q}_p(\sqrt{ap})$ se procede de modo idéntico. □

Es necesario resaltar que las extensiones $\mathbb{Q}_p(\sqrt{p})$ y $\mathbb{Q}_p(\sqrt{ap})$, aunque resulten totalmente ramificadas, no son isomorfas. Ello no ocurre en el caso de no ramificación como veremos más adelante.

Lema 3.25. *Consideraremos $f(x) = x^2 - a \in \mathbb{Q}_2[x]$ con $a \not\equiv 0\,(mód\,4)$. Entonces en $\mathbb{Q}_2$ el polinomio f tiene*

1. *ninguna solución si $a \equiv 0\,(mód\,2)$; caso contrario*
2. *dos soluciones cuando a es congruente a 1 módulo 8 y ninguna si no lo es.*

Demostración. Para el primer caso la demostración es similar al caso p impar. Veamos el segundo. Sea $a \not\equiv 0\,(mód\,2)$. Primero analicemos $a \equiv 1\,(mód\,8)$ como posibilidad. Acá deseamos probar que $f(x) = x^2 - a$ posee dos raíces. Para aplicar el método de Newton, requerimos de un entero 2-ádico m sujeto a

$$\left|\frac{m^2 - a}{4m^2}\right|_2 < 1.$$

Y en efecto, con $m = 1$, tenemos

$$\left|\frac{1^2 - a}{4 \cdot 1^2}\right|_2 = \frac{|1 - a|_2}{|4|_2} \leq \frac{2^{-3}}{2^{-2}} < 1,$$

y es posible aplicar el método de Newton. Para el resto de casos, supongamos que $a \not\equiv 1\,(mód\,8)$ sea un cuadrado perfecto. Entonces se tiene $a = b^2 \in \mathbb{Z}_2^*$ para algún

$b = 1 + b_1 2 + b_2 2^2 + \cdots = 1 + 2c$, lo que obligadamente lleva a $b^2 = 1 + 4(c + c^2)$. Como se tiene $c \equiv c^2 \,(mód\, 2\mathbb{Z}_2)$, obtenemos $a = b^2 \in 1 + 8\mathbb{Z}_2$, lo cual es una contradicción. □

Es preciso notar que cuando se cumple $\overline{x} \in \mathbb{Q}_2^*/\mathbb{Q}_2^{*^2}$, los elementos x y x^{-1} resultan equivalentes; es decir para $x = a/b \cdot u^2$, con $a, b \in \mathbb{Z}_2^*$ primos relativos y $u \in \mathbb{Q}_2^*$, se tiene que b y b^{-1} son equivalentes y con ello a/b resulta equivalente a $a \cdot b$. Por lo tanto, todos los representantes de $\mathbb{Q}_2^*/\mathbb{Q}_2^{*^2}$ pueden elegirse con $x \in \mathbb{Z}_2^*$.

Para obtener los elementos que conforman este grupo cociente, fijamos $a \in \mathbb{Q}_2^*$. Entonces para $a = u \cdot 2^n$ se presentan varias alternativas.

Si u es un cuadrado y n es par, entonces se tiene $a \in \mathbb{Q}_2^{*^2}$. Si u es un cuadrado y n es impar, obtenemos $a \in 2\mathbb{Q}_2^{*^2}$. Caso contrario, si u no es un cuadrado, en uso del Lema 3.25 se presentan algunas alternativas. Si se tiene $u = 1 + 1 \cdot 2 + 0 \cdot 2^2 + \ldots$ y n es par, tenemos $a \in 3\mathbb{Q}_2^{*^2}$; por lo contrario, si n es impar, obtenemos $a \in 3 \cdot 2\mathbb{Q}_2^{*^2}$. Si $u = 1 + 0 \cdot 2 + 1 \cdot 2^2 + \ldots$ y n es par tenemos $a \in 5\mathbb{Q}_2^{*^2}$; por lo contrario, si n es impar se logra $a \in 5 \cdot 2\mathbb{Q}_2^{*^2}$. Finalmente, si $u = 1 + 1 \cdot 2 + 1 \cdot 2^2 + \ldots$ y n es par tenemos $a \in 7\mathbb{Q}_2^{*^2}$; a su vez, si n es impar obtenemos $a \in 7 \cdot 2\mathbb{Q}_2^{*^2}$.

Gracias a lo anterior concluimos la identificación

$$\frac{\mathbb{Q}_2^*}{\mathbb{Q}_2^{*^2}} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{1 \cdot 2}, \overline{3 \cdot 2}, \overline{5 \cdot 2}, \overline{7 \cdot 2}\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Ejemplo 3.26. Sea el polinomio $f(x) = x^2 + 7 \in \mathbb{Q}_2[x]$. Como se tiene $f'(x) = 2x$, el lema de Hensel no es aplicable. Sin embargo, al cumplirse $-7 \equiv 1 \,(mód\, 8)$, esta ecuación posee solución de acuerdo con el análisis efectuado hace unos instantes. Veamos cuál o cuales son las raíces de dicho polinomio. Para $x \in \mathbb{Z}_2^*$ tenemos $x = 1 + a_1 2 + a_2 2^2 + a_3 2^3 + \ldots$, y con ello logramos

$$x^2 = a_0^2 + (a_0 a_1 + a_1^2)2^2 + (a_0 a_2)2^3 + \ldots.$$

Al aplicar las congruencias sobre las potencias convenientes de 2 logramos cierta solución $x = 1 + 2 + 2^2 + \ldots$, la otra solución está dada por $-x$.

Gracias a lo visto anteriormente, tenemos el siguiente cuadro resumen. Acá $p \neq 2$.

Cuerpo	Unidades	Cuadrados perfectos	Raíces de la unidad	Número de extensiones cuadráticas
$\mathbb{Q}_2$	$\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$	$1 + 8\mathbb{Z}_2$	$\mu_2 = \{\pm 1\}$	7
$\mathbb{Q}_p$	$\mathbb{Z}_p^\times \supset 1 + p\mathbb{Z}_p$	$1 + p\mathbb{Z}_p$	μ_{p-1}	3

Queda la duda de cuáles de las siete extensiones cuadráticas de $\mathbb{Q}_2$ son no ramificadas. Entre ellas, es claro que debemos centrar nuestra atención exclusivamente en $\mathbb{Q}_2(\sqrt{3}), \mathbb{Q}_2(\sqrt{5}), \mathbb{Q}_2(\sqrt{7})$ pues $\mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{6}), \mathbb{Q}_2(\sqrt{10}), \mathbb{Q}_2(\sqrt{14})$ obviamente ramifican. Además, notemos que es relativamente sencillo demostrar que si se tiene $|a-1|_2 < 1$ (por ejemplo para $a = 3, 5, 7$) entonces, en cualquier extensión donde tenga sentido, se cumplirá $|\sqrt{a}-1|_2 < 1$.

De no haber ramificación se tendrá $e = 1$ y ello fuerza a $f(K, \mathbb{Q}_2) = 2$; es decir, debemos tener una extensión de grado 2 del cuerpo residual $\mathbb{F}_2$. Por supuesto, de acuerdo con lo desarrollado arriba, esto significa que seremos capaces de resolver la ecuación $t^2 + t + 1 = 0$ en $\mathbb{F}_{p^2}$. En particular, si partimos desde cero y planteamos la ecuación

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

en $\mathbb{Q}_2$, veremos que ella no admite solución. Si α es una raíz abstracta de esta ecuación, tendremos $K = \mathbb{Q}_2(\alpha)$. Claramente, por tratarse de un polinomio minimal mónico, tendremos $|\alpha|_K = |f(0)|_2 = |1| = 1$. Acá es importante insistir en que α no puede ser congruente a 1, pues de lo contrario $t = 1$ sería solución de $\bar{f}(t) = t^2 + t + 1 = 0$, lo que no es cierto.

Pero a diferencia de $\mathbb{F}_2$, el cuerpo $\mathbb{Q}_2$ es de característica cero; motivo por cual toda ecuación de grado dos se resuelve completando cuadrados. En otras palabras, resolver $x^2 + x + 1 = 0$ es lo mismo que despejar

$$\left(x + \frac{1}{2}\right)^2 = -\frac{3}{4}.$$

Esto prueba que la solución, digamos α, pertenece al cuerpo $\mathbb{Q}_2(\sqrt{-3})$. Sin embargo, según nuestro trabajo preliminar, al ser -3 congruente a 5 módulo 8, se ha de tener

$\mathbb{Q}_2(\sqrt{-3}) = \mathbb{Q}_2(\sqrt{5})$. En resumen obtenemos

$$\alpha \in \mathbb{Q}_2(\sqrt{-3}) = \mathbb{Q}_2(\sqrt{5}).$$

Como la extensión no ramificada $\mathbb{Q}_2(\alpha)$ es una extensión de grado 2 contenida en la extensión $\mathbb{Q}_2(\sqrt{5})$, también de grado dos, hemos probado la igualdad

$$\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\sqrt{5}).$$

Con este argumento hemos probado el siguiente análogo del Corolario 3.24.

Proposición 3.27. *Entre las siete extensiones cuadráticas de $\mathbb{Q}_2$, exclusivamente $\mathbb{Q}_2(\sqrt{5})$ es no ramificada.* □

Hay un hecho adicional que es imperativo resaltar. Si bien las extensiones $\mathbb{Q}_2(\sqrt{3})$ y $\mathbb{Q}_2(\sqrt{7})$ son por derecho propio totalmente ramificadas, ello no ocurre con $K = \mathbb{Q}_2(\sqrt{3}, \sqrt{7}) = \mathbb{Q}_2(\sqrt{3} + \sqrt{7})$, extensión de grado 4. En efecto, de $\sqrt{3}, \sqrt{7} \in K$ obtenemos $\sqrt{21} \in K$, lo cual a su vez implica $\mathbb{Q}_2(\sqrt{21}) \subset K$. Pero como 21 es congruente a 5 mólulo 8, obtenemos

$$\mathbb{Q}_2(\sqrt{5}) = \mathbb{Q}_2(\sqrt{21}) \subset K.$$

Esto muestra en particular que el cuerpo residual crece, es decir tenemos $f = f(K, \mathbb{Q}_2) > 1$. Por otro lado, un cálculo directo conduce a

$$|1 + \sqrt{3}| = |(1 + \sqrt{3})(1 - \sqrt{3})|^{1/2} = |1 - 3|^{1/2} = 2^{-1/2},$$

con lo cual aparece ramificación en K; es decir, tenemos $e = e(K, \mathbb{Q}_2) > 1$. Como se debe tener $[K : Q_2] = 4 = ef$, concluimos la igualdad $e = f = 2$.

Es importante añadir que $\mathbb{Q}_2(\sqrt{3}, \sqrt{7})$ no contiene a ninguna de las raíces $\sqrt{2}$, $\sqrt{6}$, $\sqrt{10}$, $\sqrt{14}$. Esta vez el argumento puede hacerse de modo indirecto. Como $\mathbb{Q}_2(\sqrt{3}, \sqrt{7})$ es el aglomerado de dos extensiones cuadráticas, debe ser Galois. Pero como entonces el grupo de Galois es de orden 4, y tiene al menos 3 subgrupos no triviales (a saber $(\mathbb{Q}_2(\sqrt{n})$, con $n = 3, 5, 7$), éste debe ser isomorfo al grupo de Klein y no puede contener subcuerpos intermedios adicionales.

¿Qué ocurre entonces si consideramos otras combinaciones, como por ejemplo $K = \mathbb{Q}_2(\sqrt{2}, \sqrt{6})$? Pues en este caso aparecerá una tercera raíz cuadrada no equivalente en K al multiplicar:

$$2\sqrt{3} = \sqrt{2}\sqrt{6} \in K,$$

relación que a la larga implica

$$K = \mathbb{Q}_2(\sqrt{2}, \sqrt{6}) = \mathbb{Q}_2(\sqrt{2}, \sqrt{3}) = \mathbb{Q}_2(\sqrt{3}, \sqrt{6}).$$

El mismo argumento del párrafo anterior (vía teoría de Galois), impide a $\sqrt{5}$ pertenecer a este cuerpo, motivo por el cual $f = f(K, \mathbb{Q}_2)$ no puede ser exactamente igual a 2. Como la presencia de $\sqrt{2}$ en K es síntoma de ramificación, se concluye que $e = e(K, \mathbb{Q}_2)$ es no trivial. Por supuesto, la única posibilidad es tener $e = 4$ y $f = 1$, es decir, una extensión totalmente ramificada. Obsérvese que por definición se tiene

$$|1+\sqrt{2}+\sqrt{3}|^4 = |(1+\sqrt{2}+\sqrt{3})(1-\sqrt{2}+\sqrt{3})(1+\sqrt{2}-\sqrt{3})(1-\sqrt{2}-\sqrt{3})| = |-8|.$$

Esto, a su vez, implica

$$\left|\frac{1+\sqrt{2}+\sqrt{3}}{\sqrt{2}}\right|_2 = 2^{-1/4};$$

con lo que hemos exhibido explícitamente el uniformizador de K.

Finalmente, dejamos para el lector la tarea de verificar que $K = \mathbb{Q}_2(\sqrt{2}, \sqrt{3}, \sqrt{5})$ es una extensión Galois de grado 8 en donde todo elemento de $\mathbb{Q}_2$ admite raíz cuadrada. Para esta extensión se tiene $e = 4$ y $f = 2$. Es más, puesto que K contiene como extensiones intermedias las 7 extensiones cuadráticas de $\mathbb{Q}_2$, necesariamente su grupo de Galois ha de ser isomorfo a $(\mathbb{Z}/2\mathbb{Z})^3$.

Capítulo 4

Ramificación y raíces p-ádicas de la unidad

En este capítulo analizaremos la estrecha relación que existe entre el tipo de raíz de la unidad y la facultad de dar cabida a una extensión ramificada o no. En particular veremos que la no ramificación está vinculada a la adjunción de raíces de la unidad de cierto tipo.

4.1. Extensiones totalmente ramificadas

Los polinomios de Eisenstein juegan un rol importante en el estudio de las extensiones totalmente ramificadas. Realmente, éstas pueden ser caracterizadas en términos de los polinomios de Eisenstein, puesto que para toda extensión K finita totalmente ramificada de $\mathbb{Q}_p$ existe un polinomio de Eisenstein que determina K. Por otro lado, las extensiones no ramificadas requieren de un estudio separado. Específicamente, es preciso estudiar las raíces n-ésimas de la unidad en una extensión finita K de $\mathbb{Q}_p$ para por fin poderlas caracterizar.

Teorema 4.1. *Si f es un polinomio de Eisenstein, entonces $\dfrac{\mathbb{Q}_p[x]}{\langle f(x)\rangle}$ es una extensión de $\mathbb{Q}_p$ totalmente ramificada.*

Demostración. Pongamos $K = \dfrac{\mathbb{Q}_p[x]}{\langle f(x)\rangle}$, con

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}_p[x],$$

polinomio de Eisenstein irreducible. Para π raíz de f, se cumple

$$\pi^n + a_{n-1}\pi^{n-1} + \ldots + a_1\pi + a_0 = 0.$$

Como π debe ser un entero, tenemos

$$|\pi^n| = |a_{n-1}\pi^{n-1} + \cdots + a_0| \leq \text{máx}\{|a_i\pi^i|\}.$$

Pero como f es un polinomio de Eisenstein, por definición se tiene $|a_i| \leq 1/p$ y con ello se satisface

$$|\pi^n| \leq \text{máx}\,|a_{n-1}|, \ldots, |a_0| \leq 1/p.$$

En particular conseguimos $|\pi| \leq (1/p)^{1/n}$.

Por su parte, si se tuviese la desigualdad estricta $|\pi| < (1/p)^{1/n}$, tendríamos también

$$|a_0| = |\pi^n + \pi(a_{n-1}\pi^{n-2} + \cdots + a_1)| \leq \text{máx}\,|\pi^n|, |\pi||a_{n-1}\pi^{n-2} + \cdots + a_1|.$$

Esto, junto con $|a_{n-1}\pi^{n-2} + \cdots + a_1| \leq 1/p$ y $|\pi^n| < 1/p$ inevitablemente conduce a $|a_0| < 1/p$, lo cual contradice el hecho de que f sea un polinomio de Eisenstein.

Finalmente, la condición $|\pi| = (1/p)^{1/n}$ implica que e es un múltiplo de n. Como e debe dividir a n, ha de haber igualdad. □

Ejemplo 4.2. Para $n \geq 2$ el polinomio $x^n - p$ es de Eisenstein. De acuerdo con el teorema anterior la extensión $\mathbb{Q}_p(\sqrt[n]{p}) \cong \dfrac{\mathbb{Q}_p[x]}{\langle x^n - p\rangle}$ es totalmente ramificada.

Teorema 4.3. *Sea K una extensión finita totalmente ramificada de $\mathbb{Q}_p$. Entonces alguna raíz de cierto polinomio de Eisenstein determina K.*

Demostración. El ideal máximal $\mathcal{O}_K$ del anillo $\mathbb{Z}_K$ de K es principal y generado por un elemento π con $\mid \pi \mid^e = \mid p \mid$. Como se tiene $n = [K : \mathbb{Q}_p] = e$, las potencias linealmente independientes $(\pi^i)_{0 \leq i < e}$ generan $K = \mathbb{Q}_p(\pi)$ como espacio vectorial. El polinomio irreducible de este elemento puede ser factorizado en una extensión de Galois de $\mathbb{Q}_p$ que contiene a K cual

$$f(x) = \prod_{\sigma}(x - \pi^\sigma) = x^e + \sum_{0<i<e} a_i x^i \pm \prod_{\sigma} \pi^\sigma.$$

El término constante tiene valor absoluto $\mid \prod_\sigma \pi^\sigma \mid = \mid \pi \mid^e = \mid p \mid$. También se debe tener $\mid a_i \mid < 1$ pues cada $a_i \in \mathbb{Z}_p$ es una combinación algebraica elemental de los conjugados π^σ. Por lo tanto, estos coeficientes intermedios pertenecen a $p\mathbb{Z}_p$, como deseamos. □

Ejemplo 4.4. Para $p = 2$, sabemos que -1 no tiene raíz cuadrada en $\mathbb{Q}_2$, motivo por el cual construimos la extensión cuadrática $K = \mathbb{Q}_2(i) \cong \mathbb{Q}_2[x]/(x^2 + 1)$. Como se tiene

$$(1 + i)^2 = 2i,$$

el elemento $i + 1$ es una raíz cuadrada de $2i$. Por ello se satisface

$$\mid i + 1 \mid^2_{\mathbb{Q}_2(i)} = \mid 2i \mid_{\mathbb{Q}_2(i)} = \mid 2 \mid_2 = 2^{-1}, \text{ es decir } \mid i + 1 \mid_{\mathbb{Q}_2(i)} = 2^{-1/2}.$$

Así $1 + i$ es un generador del ideal máximal $\mathcal{O}_K$, lo que implica $\mathcal{O}_K = (1 + i)\mathbb{Z}_K$. Se sigue fácilmente que la extensión K es totalmente ramificada con índice $e = 2$. De esta forma ramifica salvajemente según la definición. Escribamos $x = 1 + i$, para tener $x - 1 = i$ y $(x - 1)^2 = -1$, es decir x es una raíz del polinomio

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

Éste es un polinomio de Eisenstein y concluimos que $K = \mathbb{Q}_2(i)$ puede también ser obtenido como un cuerpo de descomposición de este polinomio.

Ejemplo 4.5. Para $p \neq 2$ sea ξ una raíz p-ésima primitiva de la unidad en $\mathbb{Q}_p$. De este modo ξ es una raíz del polinomio ciclótomico

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1.$$

Este polinomio es irreducible, puesto que el cambio de variable $x-1=y$ produce

$$\Phi_p(x)=\frac{(y+1)^p-1}{y}=y^{p-1}+p(\cdots)+p,$$

un polinomio de Eisenstein. Por lo tanto obtenemos una extensión de grado $p-1$, valor coprimo con p. El Teorema 4.1 garantiza que K es una extensión totalmente ramificada.

Si queremos constatar este hecho de manera directa notamos que como los ξ^j son también raíces de la misma ecuación, cada vez que j no sea múltiplo de p las potencias ξ^j, con $1\leq j\leq p-1$, formarán un conjunto completo de conjugados de ξ, y de este modo se tiene

$$\Phi_p(x)=\prod_{1\leq j\leq p-1}(x-\xi^j).$$

Al reemplazar $x=1$ se logra

$$p=\Phi_p(1)=\prod_{1\leq j\leq p-1}(1-\xi^j).$$

Pero al ser todos los valores absolutos $\mid 1-\xi^j \mid$ iguales entre sí, tras multiplicar estos elementos conjugados se obtiene

$$\mid p \mid=\prod_{1\leq j\leq p-1}\mid 1-\xi^j \mid=\mid 1-\xi \mid^{p-1}.$$

Lo anterior prueba que $\pi=1-\xi$ es un uniformizador de $\mathcal{O}_K$ en $\mathbb{Z}_K$. La extensión $K=\mathbb{Q}_p(\xi)$ es ramificada con grado $n=e=p-1$ y por lo tanto total y mansamente ramificada.

Por su parte, la factorización

$$1-\xi^j=(1-\xi)(1+\cdots+\xi^{j-1})$$

implica

$$\mid 1+\xi+\cdots+\xi^{j-1} \mid=\mid \frac{1-\xi^j}{1-\xi} \mid=1,$$

y de esta manera $1+\xi+\cdots+\xi^{j-1}$ es unidad del anillo máximal $\mathbb{Z}_K\subset K=\mathbb{Q}_p(\xi)$. Éste elemento es llamado comúnmente **unidad ciclótomica** de K. Como se cumple $\xi\equiv 1(mód\,\mathcal{O})$, inevitablemente se tiene $1+\xi+\cdots+\xi^{j-1}\equiv j\,(mód\,\mathcal{O})$.

4.2. Raíces de la unidad y extensiones no ramificadas

Sea K un cuerpo conmutativo de característica 0 y sea $\mu(K)$ el grupo mutiplicativo formado por todas la raíces de la unidad en K. Como todos los elementos de este grupo poseen orden finito, es posible aplicar el teorema chino del resto y escribir

$$\mu(K) = \mu_{p^\infty}(K) \cdot \mu_{(p)}(K),$$

donde los elementos en $\mu_{p^\infty}(K)$ poseen como orden potencias de p y los elementos en $\mu_{(p)}(K)$ poseen orden coprimo con p. Vamos a probar que cuando K es una extensión finita de $\mathbb{Q}_p$, ambos grupos $\mu_{(p)}(K)$ y μ_{p^∞} son finitos.

En un cuerpo valuado, todas las raíces de la unidad se encuentran en la esfera unitaria. Obsérvese que para una extensión ultramétrica de $\mathbb{Q}_p$ se cumple

$$K \supset A = \{x \in K :| x |\leq 1\} \supset M = \{x \in K :| x |< 1\}.$$

De este modo se tendrá $\mu = \mu(K) \subset A^\times \subset K^*$. Por tal motivo vía reducción módulo M mediante la proyección

$$\varepsilon : \quad A \quad \to \quad A/M = k$$

se obtiene $\varepsilon(\mu) \subset k^*$. Veamos las consecuencias que se pueden extraer de la reducción módulo M de las raíces de la unidad.

Empecemos con un teorema similar al método de Newton, al que llamaremos **forma general del método de Newton**, resultado que tiene una utilidad ánaloga al del caso estándar.

Teorema 4.6. *(Forma general del método de Newton) Sea K un cuerpo ultramétrico completo con anillo de enteros $A = \{x \in K :| x |\leq 1\}$. Consideremos un polinomio $f(x) \in A[x]$. Si $x_0 \in A$ satisface $| f(x_0) |<| f'(x_0) |^2$, entonces existe una raíz $\xi \in A$ de f que cumple $| \xi - x_0 |=| f(x_0)/f'(x_0) |<| f'(x_0) |\leq 1$.*

Demostración. La prueba del teorema es imitar la prueba del método de Newton ya válida en los números p-ádicos. Consultar [2]. □

Observamos que el valor absoluto trivial toma apenas los valores 0 y 1. Así de tenerse en tal caso $\mid f(x_0) \mid < \mid f'(x_0) \mid^2 = 1$, el teorema es aplicable, pero brinda información prácticamente trivial, pues x_0 es ya una raíz de la ecuación en estudio.

Proposición 4.7. *Sea K una extensión ultramétrica de $\mathbb{Q}_p$. Entonces se cumple*

$$\mu_{p^\infty}(K) = \mu(K) \cap (1 + M).$$

Demostración. Si $\zeta \in \mu(K)$ tiene orden una potencia de p, denotamos por $\overline{\zeta} = \varepsilon(\zeta) \in k$ su reducción. Entonces se cumple $\zeta^{p^j} = 1$ y al aplicar la reducción módulo M se tiene $\overline{\zeta}^{p^j} = \overline{1}$. Por otro lado, se satisface $\overline{\zeta}^{p^k-1} = \overline{1}$ para $\kappa = [\mathbb{F}_p(\overline{\zeta}) : \mathbb{F}_p]$. Como p^j y $p^k - 1$ son relativamente primos, existen $a, b \in \mathbb{Z}$ tales que $ap^j + bp^{k-1} = 1$. Ello lleva a

$$\overline{\zeta} = (\overline{\zeta}^{p^j})^a (\overline{\zeta}^{p^k-1})^b = 1^a 1^b = 1.$$

Ello significa en pocas palabras que ζ pertenece a $1 + M$.

Recíprocamente, si $\zeta \in 1 + M$ tiene orden $n > 1$, escribimos $\zeta = 1 + \xi$ con $0 \neq \mid \xi \mid < 1$. Entonces se cumple

$$1 = (1 + \xi)^n = 1 + n\xi + \cdots + \xi^n = 1 + \xi(n + \xi\alpha).$$

De aquí deducimos la igualdad $n + \xi\alpha = 0$, y al tomar norma obtendremos

$$\mid n \mid = \mid \xi\alpha \mid \leq \mid \xi \mid < 1;$$

concluimos que p debe dividir a n. Si $n \neq p$, podemos reemplazar ζ por ζ^p, que tiene orden $n/p > 1$, y repetir el proceso. Un proceso inductivo ya familiar permite concluir que n es potencia de p. □

Proposición 4.8. *Si K es una extensión de $\mathbb{Q}_p$ topológicamente completa y con cuerpo residual k algebraico sobre $\mathbb{F}_p$, entonces existe una descomposición como sucesión exacta corta*

$$(1) \longrightarrow \mu_{p^\infty}(K) \longrightarrow \mu(K) \longrightarrow k^\times \longrightarrow (1)\ .$$

Es más, si el cuerpo residual k es finito, digamos con $f = [k : \mathbb{F}_p] < \infty$, entonces el grupo cíclico $\mu_{(p)}(K)$ tiene orden $p^f - 1$.

Demostración. Al tenerse $\mu_{p^\infty}(K) \subset \mu(K)$, existe gratis un homomorfismo inyectivo

$$\begin{array}{rccc} i: & \mu_{p^\infty}(K) & \to & \mu(K) \\ & x & \mapsto & x. \end{array}$$

Del mismo modo, al restringir el homomorfismo $\varepsilon : A \to k$ obtenemos el homomorfismo inducido $\overline{\varepsilon} : \mu(K) \to k^\times$. Veamos que éste es sobreyectivo. Tomemos $\alpha \in k^\times$ y reemplacemos k por la extensión $\mathbb{F}_p(\alpha) \cong \mathbb{F}_q$, digamos de grado n, de modo que m, el orden multiplicativo de α, divida a $p^n - 1 = q - 1$. Sea $a \in A$ con $\varepsilon(a) = \alpha$ y consideremos el problema

$$x^m - 1 = 0, \text{ con } x \equiv a \,(mód\, M).$$

Como m es primo relativo con p y K es completo, según el Teorema 4.6 existe un elemento $x \in K^\times$ congruente con a que cumple $x^m = 1$. Por lo tanto se tiene $x \in \mu_{(p)}(K)$ y $\varepsilon(x) = \varepsilon(a) = \alpha$. Esto prueba que cuando el cuerpo residual k es algebraico, la restricción de la reducción módulo M determina un isomorfismo $\mu_{(p)}(K) \cong k^\times$.

En resumen tenemos el diagrama de homomorfismos

$$(1) \longrightarrow \mu_{p^\infty}(K) \xrightarrow{\ i\ } \mu(K) \xrightarrow{\ \overline{\varepsilon}\ } k^\times \longrightarrow (1)\ .$$

Para que esta secuencia sea exacta nos falta comprobar la igualdad $Ker(\overline{\varepsilon}) = Im(i)$. La Proposición 4.7 implica $\overline{\varepsilon}(\mu_{p^\infty}) = 1$; es decir $Im(i) \subset Ker(\overline{\varepsilon})$. Recíprocamente, si $a \in \mu(K)$ proyecta a 1, entonces la Proposición 4.7 también afirma que se cumple $a \in \mu(K) \cap (1 + M) = \mu_{p^\infty}(K) = Im(i)$. □

Lema 4.9. *Si K es una extensión finita de $\mathbb{Q}_p$ con grado de clases residuales f, entonces la ecuación*

$$x^{p^f - 1} = 1$$

tiene todas sus raíces en K. En particular, el cuerpo K contiene una raíz primitiva $p^f - 1$-ésima de la unidad.

Demostración. Este resultado se desprende directamente del Teorema 4.6. □

Las extensiones no ramificadas de $\mathbb{Q}_p$ ya pueden clasificarse con la información a mano.

Teorema 4.10. *Para cada f existe apenas una extensión no ramificada de grado f de $\mathbb{Q}_p$. Ésta se obtiene adjuntando a $\mathbb{Q}_p$ una raíz (p^f-1)-ésima primitiva de la unidad.*

Demostración. Primero veamos la existencia de tal extensión. Sea $\mathbb{F}_{p^f} = \mathbb{F}_p(\overline{\alpha})$ la extensión de $\mathbb{F}_p$ de grado f, y sea

$$\overline{g}(t) = t^f + \overline{a}_{f-1}t^{f-1} + \ldots + \overline{a}_1 t + \overline{a}_0 \in \mathbb{F}_p[t]$$

el polinomio mínimo de $\overline{\alpha}$ sobre $\mathbb{F}_p$. Como $\overline{g}(t)$ es irreducible en $\mathbb{F}_p$, resulta que proviene de un $g(x)$ irreducible en $\mathbb{Q}_p$. Si α es raíz de $g(x)$, entonces $\mathbb{Q}_p(\alpha)$ es una extensión de grado f pues g y $\overline{g}$ tienen el mismo grado. Veamos que $\mathbb{Q}_p(\alpha)$ es una extensión no ramificada. Como $\mathbb{F}_p(\overline{\alpha})$ es el cuerpo de clases residuales que contiene una raíz de g módulo p, se tiene $[\mathbb{F}_p(\overline{\alpha}) : \mathbb{F}_p] \geq f$. Por otro lado, se tiene también $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \leq [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$, lo que permite concluir la igualdad $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = f$.

Ahora veamos la unicidad. Para K extensión no ramificada de $\mathbb{Q}_p$, veremos que ésta resulta ser la misma extensión que se obtiene adjuntando una raíz (p^f-1)-ésima primitiva de la unidad. Primero que nada, notemos que por el Lema 4.9 el cuerpo K contiene todas las raíces (p^f-1)-ésimas de la unidad, por ello es suficiente probar que éste resulta ser el menor cuerpo con dicha propiedad. Para β una raíz (p^f-1)-ésima de la unidad obtenemos

$$\mathbb{Q}_p \subset \mathbb{Q}_p(\beta) \subset K.$$

Pero el cuerpo de clases residuales de $\mathbb{Q}_p(\beta)$ también contiene todas las raíces (p^f-1)-ésimas de la unidad, es decir, éste contiene a $\mathbb{F}_{p^f}$, lo cual implica $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \leq f$ y con ello se logra $K = \mathbb{Q}_p(\beta)$. □

Las definiciones de índice de ramificación y grado residual de una extensión se pueden aprovechar cuando se busca relacionar dos extensiones finitas de un mismo cuerpo; por ejemplo si K y L son extensiones finitas de $\mathbb{Q}_p$ con $K \subset L$. Escribamos como antes A_K para referirnos al anillo de enteros algebraicos de K y M_K a su ideal máximal, con ello se tiene un cuerpo residual $k_K = A_K/M_K$; de igual modo A_L y M_L denotarán el anillo de enteros algebraicos de L y su ideal máximal, respectivamente,

y $k_L = A_L/M_L$ será el cuerpo residual de L. Definamos

$$\begin{aligned} e &= e(L/K) = [\mid L^\times \mid : \mid K^\times \mid], \\ f &= f(L/K) = [k_L : k] = dim_k k_L, \\ n &= [L : K] = dim_K(L). \end{aligned}$$

Si escribimos

$$\begin{aligned} n' &= e'f' \quad \text{con } n' = [L : \mathbb{Q}_p], \\ n'' &= e''f'' \quad \text{con } n'' = [K : \mathbb{Q}_p], \end{aligned}$$

la relación $n' = n \cdot n''$, fuerza a que se cumpla

$$n = \frac{n'}{n''} = \frac{e'}{e''} \cdot \frac{f'}{f''}.$$

Teorema 4.11. *Sean K y L dos extensiones finitas de $\mathbb{Q}_p$ con $K \subset L$. Entonces existe una única extensión intermedia maximal $K \subset K_{nr} \subset L$ que resulta no ramificada sobre K.*

Demostración. Si el cuerpo residual k_L de L posee orden q_L, se tiene que $L^\times$ contiene un subgrupo cíclico de raíces de la unidad $\mu_{(p)}(L)$ de orden $q_L - 1$. Para ser más preciso, si se tiene $q = \mid k \mid$ y $f = f(L/K) = [k_L : k]$ es el grado residual, entonces se satisface $q_L = q^f$. Las extensiones no ramificadas de K contenidas en L se corresponden uno a uno con las extensiones de $k = \mathbb{F}_q$ en k_L. Como esta correspondencia preserva el orden, de ahí se desprende la unicidad de la extensión no ramificada. Explícitamente se tiene $K_{nr} = K(\mu_{(p)(L)}) = K(\mu_{q_L - 1}) \subset L$. □

Teorema 4.12. *Todas las extensiones no ramificadas de $\mathbb{Q}_p$ de grado f son isomorfas entre sí.*

Demostración. Sea E una extensión p-ádica de grado f que incluya una raíz no trivial del polinomio $g(x) = x^{p^f} - x$. Como se cumple $g'(x) = p^f x^{p^f - 1} - 1 \equiv -1 \,(mód\, p)$, se observa que todas las raíces son simples. Como todo elemento de $\mathbb{F}_{p^f}$ es una raíz, concluimos que $\mathbb{Q}_p(\zeta)$ es una extensión de grado f.

Sea $q(x)$ un polinomio mónico irredudible de grado f que genere una extensión no ramificada. Por el lema de Hensel versión 2, $q(x)$ proyecta sobre un polinomio irreducible de grado f a la potencia e: como la extensión no ramifica, se tiene $e = 1$. Por definición, como el polinomio es irreducible, la proyección de $q(x)$ se rompe en $\mathbb{F}_{p^f}$ en factores lineales distintos. Aplicando el lema Hensel a cualquier raíz obtenemos que el polinomio admite una raíz en $\mathbb{Q}_p(\zeta)$. Como esta extensión es Galois, todas las raíces están en $\mathbb{Q}_p(\zeta)$. □

Corolario 4.13. *Todas las extensiones no ramificadas de $\mathbb{Q}_p$ son extensiones de Galois.*

Demostración. Con la notación del teorema anterior estamos hablando del cuerpo de ruptura del polinomio $x^{p^f} - x = 0$. □

4.3. Extensiones mansamente ramificadas

Queda claro que toda extensión no ramificada resulta mansa. Por el Teorema 4.11 toda extensión finita K de $\mathbb{Q}_p$ contiene una subextensión maximal no ramificada. Es más, si K es completo, el grupo $\mu_{(p)}(K)$ es isomorfo al grupo cíclico k^* de orden $q - 1 = p^f - 1$. Es decir, se tiene

$$K_{nr} = \mathbb{Q}_p(\zeta_{q-1}) = \mathbb{Q}_p(\mu_{q-1}) \subset K.$$

Por supuesto, cada raíz primitiva de la unidad que satisface $\zeta \in \mu_{q-1}$ determina una extensión finita $\mathbb{Q}_p(\zeta)$ mansa sobre $\mathbb{Q}_p$.

Teorema 4.14. *Sean $K \subset L$ extensiones finitas de $\mathbb{Q}_p$. Si L/K es total y mansamente ramificada de grado e, entonces existe un generador canónico π del anillo maximal $A_K \subset K$ tal que L es generado por una raíz e-ésima de π.*

Demostración. Sean los generadores π_K de $M_K \subset A_K \subset K$ y π_L de $M_L \subset A_L \subset L$. Como L/K es totalmente ramificada de grado e se tiene $|\ \pi_L\ |^e = |\ \pi_K\ |$, y además $\pi_L^e/\pi_K = u$ es una unidad en A_L. Por otro lado, como se tiene $f = 1$, existe una unidad $\eta \in A_K$ sujeta a $\eta \equiv u\,(\mathit{mód}\, M_L)$. Escribamos

$$\pi_L^e = \pi_K \cdot u, \quad u = \eta + \pi_L v \text{ con } \ v \in A_L,$$

es decir $\pi_L^e = \pi_K \cdot (\eta + \pi_L v) = \eta\pi_K + \pi_K\pi_L v$.

El elemento $\eta\pi_K$ es también generador del ideal M_K pues tiene la misma norma que π_K. Afirmamos que L es generado por una raíz del polinomio $x^e - \eta\pi_K$. A fin de simplificar notación notemos que al reemplazar el generador π_K por $\pi'_K = \eta\pi_K$ y simplemente volver a denotar éste elemento por π_K, se puede asumir que los generadores π_K y π_L ya están relacionados vía

$$\pi_L^e = \pi_K + \pi_K\pi_L v \ \text{ con } v \in A_L,$$

y que la ecuación a estudiar es $x^e - \pi_K = 0$.

El polinomio $f(x) = x^e - \pi_K \in A_K[x]$ es un polinomio de Eisenstein, por lo tanto irreducible en $K[x]$. Así tenemos $f(\pi_L) = \pi_L^e - \pi_K = \pi_K\pi_L v$, lo cual implica $\mid f(\pi_L) \mid = \mid \pi_K\pi_L v \mid < \mid \pi_K \mid$. Luego, en alguna extensión algebraica f se rompe como

$$f(x) = x^e - \pi_K = \prod_{1\leq i\leq e} (x - \alpha_i),$$

donde $\prod \alpha_i = \pm\pi_K$. Las raíces α_i son conjugadas y tienen la misma norma igual, digamos, a c. La meta es probar que alguna de ellas pertenece a L.

De no ser así, $f(x)$ podrá factorizarse en $L[x]$ en polinomios irreducibles de grado no menor que 2. Esto significa que para cada una de las raíces α_i existirá un automorfismo σ_i que fija L con el cual se tendrá que $\sigma_i(\alpha_i)$ es una raíz de f distinta de α_i.

Ahora, puesto que los α_i son conjugados sobre K tenemos

$$c^e = \prod_{1\leq i\leq e} \mid \alpha_i \mid = \mid \pi_K \mid = \mid \pi_L \mid^e,$$

lo cual lleva a $\mid \pi_L \mid = c$. Gracias a ello, se tiene para todo i la relación

$$\mid \pi_L - \alpha_i \mid \leq \text{máx}\{\mid \pi_L \mid, \mid \alpha_i \mid\} = c.$$

Sin embargo, al reemplazar en el polinomio original obtenemos

$$\prod_{1\leq i\leq e} \mid \pi_L - \alpha_i \mid = \mid f(\pi_L) \mid < \mid \pi_K \mid = \mid \pi_L \mid^e = c^e$$

con lo cual se ha de cumplir $\mid \pi_L - \alpha_i \mid < c$ al menos para un α_i, digamos α_1. Por definición de norma se tendrá también $\mid \pi_L - \alpha_1 \mid = \mid \sigma_1(\pi_L - \alpha_1) \mid = \mid \pi_L - \sigma_1(\alpha_1) \mid < c$.

Pero obviamente las raíces de f son todas de la forma $\alpha_i = \zeta_i \alpha_1$, donde $\zeta_i^e = 1$. Como la extensión es mansa, el índice e es valor coprimo con p. Por tanto se cumple $\mid \zeta_i - 1 \mid = 1$ siempre que ζ_i no sea 1. En particular se tendrá $\sigma_1(\alpha_1) = \zeta_j \alpha_1$ para cierto $j \neq 1$.

Al poner todo junto conseguimos por un lado

$$\mid \sigma_1(\alpha_1) - \alpha_1 \mid = \mid \alpha_1 \mid\mid \zeta_j - 1 \mid = \mid \alpha_1 \mid = c,$$

mientras por otro

$$\mid \sigma_1(\alpha_1) - \alpha_1 \mid \leq \text{máx}\{\mid \sigma_1(\alpha_1) - \pi_L \mid, \mid \alpha_1 - \pi_L \mid\} < c.$$

Esta contradicción muestra entonces que alguna raíz pertenece a $L = K(\pi_L)$, y como α tiene grado e, queda establecido el resultado. □

El argumento utilizado para rematar la prueba del Teorema 4.14 está inspirado en el llamado lema de Krasner (Ver [1], Teorema 1 en Sección 3.1.5).

Acabamos de ver que toda extensión mansamente ramificada es de modo directo soluble por radicales, en el sentido que se tiene $L = K(\pi_L)$, donde $\pi_L^e \in K$ es un uniformizador de K. A la larga, los conjugados algebraicos de π_L serán los productos $\zeta^i \pi_L$, donde ζ representa una raíz e-ésima primitiva de la unidad. Por otro lado, acabamos de ver en la Sección 4.2 que al ser e y p relativamente primos, la presencia de un ζ con tales características no tiene que ver con ramificación, sino con el crecimiento del grado residual. En resumen, si bien $K(\pi_L)$, donde $\pi_L^e \in K$ es uniformizador de K, no tiene por que ser Galois, basta adjuntarle una raíz e-ésima primitiva de la unidad para que obligatoriamente lo sea. El grado f de esta extensión no ramificada será un divisor de $\phi(e(L, K))$.

Por otro lado, queda aún la duda de qué parejas π_1, π_2 de uniformizadores de L generan la misma extensión (siempre, claro está, que π_1^e, π_2^e sean uniformizadores de K.) Este problema, en principio, puede no ser trivial aun en el caso cuando se cumple $\pi_1^e = \pi_2^e$, pues esto apenas significa que los generadores difieren multiplicativamente por una raíz de la unidad de orden e. Vemos entonces que de ser así, los cuerpos generados por ellos serán el mismo única y exclusivamente cuando K contenga a la aludida raíz e-ésima de la unidad.

Precisamente por ello, para atacar acertadamente el problema de catalogar las extensiones mansas de grado e, es saludable asumir que K, el cuerpo base, ya contiene todas las raíces de orden e. Por ejemplo, en el caso cuadrático esta condición pasa desapercibida puesto que las raíces cuadradas de la unidad son simplemente ± 1.

Bajo los supuestos anteriores, estamos listos para clasificar las extensiones totalmente ramificadas y mansas de un grado dado.

Teorema 4.15. *Sea e relativamente primo con p. Supongamos que el cuerpo K contenga todas las raíces de la unidad de orden e. Sean L_1, L_2 extensiones mansas de K, ambas de grado e, con generadores canónicos π_1, π_2 respectivamente (ver Teorema 4.14). Entonces se tiene $L_1 = L_2$ si y sólo si la clase de $(\pi_1/\pi_2)^e$ en el cuerpo residual de K es la raíz e-ésima de un elemento residual.*

Demostración. Si se tiene $L_1 = L_2$, entonces un argumento similar al presentado en el Lema 3.14 muestra que se debe tener

$$\pi_1 = a_1\pi_2 + a_2\pi_2^2 + \cdots + a_e\pi_2^e,$$

con $a_1, \cdots, a_e \in \mathbb{Z}_K$, pues π_2 es tan buen generador de L como lo es π_1. De este modo se logra $\pi_1/\pi_2 \equiv a_1$ módulo $\mathcal{O}_L$ y con ello de paso $(\pi_1/\pi_2)^e \equiv a_1^e$ módulo $\mathcal{O}_L$.

Recíprocamente, si $(\pi_1/\pi_2)^e \equiv \alpha^e$ módulo $\mathcal{O}_L$ para algún $\alpha \in \mathbb{Z}_K$, entonces la ecuación $x^e - (\pi_1/\pi_2)^e \in K[x]$ proyecta módulo $\mathcal{O}_K$ a

$$t^e - (\pi_1/\pi_2)^e = t^e - \alpha^e,$$

la cual se factoriza totalmente en el cuerpo residual pues éste contiene todas las raíces e-ésimas de la unidad. Por el lema de Hensel $x^e - (\pi_1/\pi_2)^e$ se factoriza totalmente en $K[x]$. En particular se tiene $\pi_1/\pi_2 \in K$. Esto implica $\pi_1 \in K(\pi_2)$ lo que conduce a $K(\pi_1) \subset K(\pi_2)$. Como $K(\pi_1), K(\pi_2)$ son extensiones de K del mismo grado, concluimos la igualdad $K(\pi_1) = K(\pi_2)$ buscada.

4.4. Extensiones salvajemente ramificadas

Una extensión K de $\mathbb{Q}_p$ con $n = [K : \mathbb{Q}_p]$ ramifica salvajemente si se tiene $e = p^k$ para algún k entero positivo. Esto significa que no existe una extensión

salvaje y mansamente ramificada al mismo tiempo. Empecemos con un resultado que relaciona k^* con el grupo μ_{p^∞}.

Proposición 4.16. *La restricción a $\mu(K)$ de la proyección módulo p tiene núcleo $\mu_{p^\infty}(K)$. Esta proyección resulta inyectiva en $\mu_{(p)}(K)$.*

Demostración. Consideremos la proyección

$$\begin{array}{rccc} \varepsilon: & \mu(K) & \longrightarrow & K^* \\ & \zeta & \longmapsto & \overline{\zeta}. \end{array}$$

Para $\zeta \in ker(\varepsilon)$ se tiene $\varepsilon(\zeta) = \overline{\zeta} = \overline{1}$, y por consiguiente $\zeta \in 1 + M$. De la Proposición 4.7 concluimos que se cumple $\zeta \in \mu_{p^\infty}(K)$.

Recíprocamente, con $\zeta \in \mu_{p^\infty}(K)$ se tiene $\overline{\zeta} = \overline{1} = \varepsilon(\zeta)$ y así $\zeta \in ker(\varepsilon)$.

Por otro lado, si consideramos la restricción

$$\begin{array}{rccc} \varepsilon: & \mu_{(p)}(K) & \longrightarrow & K^* \\ & \zeta & \longmapsto & \overline{\zeta}, \end{array}$$

ésta sí resulta inyectiva. En efecto $\varepsilon(\zeta) = \overline{1} = \overline{\zeta}$ implica $\zeta \in 1+M$, lo que nos obliga a tener $\zeta \in \mu_{p^\infty}(K) \cap \mu_{(p)}(K)$ por la Proposición 4.7. Por lo tanto se tiene $\zeta = 1$. □

Teorema 4.17. *Para toda raíz de la unidad ζ cuyo orden es exactamente p^{n_0}, donde $n_0 \geq 1$, se satisface $\mid \zeta - 1 \mid = p^{-1/\phi(p^{n_0})} < 1$; acá ϕ es la función de Euler.*

Demostración. Para el caso especial $n_0 = 1$, la raíz ζ tiene orden p. Acá se cumple $\zeta^p = 1$, y $\zeta = 1+\xi$, con $\mid \xi \mid < 1$, es una raíz del polinomio $(x^p-1)/(x-1)$; es decir, se satisface

$$0 = \frac{(1+\xi)^p - 1}{\xi} = \frac{1}{\xi}(p\xi + p\xi^2 t + \xi^p), \text{ con } \mid t \mid \leq 1.$$

Debido a ello tenemos

$$p(1+\xi t) + \xi^{p-1} = 0,$$

y como se cumple $\mid \xi \mid < 1$ y $\mid t \mid \leq 1$, obtenemos $\mid 1+\xi t \mid = 1$ y por lo tanto, también $\mid \xi^{p-1} \mid = \mid -p(1+\xi t) \mid = \mid p \mid$. Gracias a ello obtenemos $\mid \zeta - 1 \mid = \mid \xi \mid = \mid p \mid^{1/(p-1)} < 1$. Como se satisface $\phi(p) = p - 1$, se sigue la validez de este caso particular.

En adelante escribiremos $r_p = \mid p \mid^{\frac{1}{p-1}}$. Vemos que se satisface

$$\frac{1}{p} = \mid p \mid \leq r_p < 1.$$

Por ejemplo tenemos $r_2 = \frac{1}{2}$ y se cumple $r_p > \frac{1}{p}$ para p primo impar.

Ahora tratemos el caso general. Supongamos que el orden de ζ sea p^{n_0+1}. Entonces $\zeta^{p^{n_0}}$ tiene orden p, y por el caso especial tratado arriba obtenemos

$$\mid \zeta^{p^{n_0}} - 1 \mid = r_p < 1.$$

Hacemos ahora $\zeta = 1 + \eta$ con $\mid \eta \mid < 1$ para obtener

$$\zeta^{p^{n_0}} - 1 = (1+\eta)^{p^{n_0}} - 1 = \eta^{p^{n_0}} + p\eta y$$

con $\mid y \mid \leq 1$. Luego se tiene

$$\mid p\eta y \mid < \mid p \mid \leq r_p = \mid \zeta^{p^{n_0}} - 1 \mid = \mid \eta^{p^{n_0}} + p\eta y \mid,$$

lo cual, por el principio de los triángulos isósceles, implica $\mid \eta^{p^{n_0}} + p\eta y \mid = \mid \eta^{p^{n_0}} \mid$.

Por lo tanto tenemos $\mid \zeta^{p^{n_0}} - 1 \mid = \mid \eta^{p^{n_0}} \mid = r_p$, lo que directamente conduce a $\mid \eta \mid = r_p^{1/p^{n_0}}$, como esperabamos, ya que para $n_0 > 1$ se tiene $\phi(p^{n_0}) = p^{n_0} - p^{n_0-1}$. □

Recordemos que el polinomio

$$\phi_p(x) = \frac{x^p - 1}{x - 1}$$

denota el p-ésimo polinomio ciclótomico (el cual por ser p primo es de grado $p-1$).

Para $i > 1$ el p^i-ésimo polinomio ciclótomico debe tener grado $\phi(p^i) = p^{i-1}(p-1)$. Pero notemos que $\phi_p(x^{p^{i-1}})$ tiene el grado y las raíces correctas, y por lo tanto es igual a $\phi_{p^i}(x)$. Lo importante acá es que al ser la composición de un polinomio de Eisenstein con el monomio $x^{p^{i-1}}$ resulta también un polinomio de Eisenstein.

Si combinamos este análisis con el Teorema 4.1 concluimos que la adjunción de raíces de la unidad de orden una potencia de p induce exclusivamente ramificación.

Corolario 4.18. *Si el índice de ramificación $e = e(K)$ es finito, entonces el grupo $\mu_{p^\infty}(K)$ de raíces de la unidad en K posee orden una potencia de p. Es más, este orden es menor que $e/(1-1/p)$.*

Demostración. En general, si el cuerpo K tiene una raíz de orden p^t, el Teorema 4.17 muestra que el índice de ramificación es un múltiplo de $\varphi(p^t) = p^t - p^{t-1}$. Por lo tanto se tiene

$$p^t(1 - 1/p) \leq e.$$

Así tenemos en $p^t \leq \dfrac{ep}{p-1}$ una cota para el orden, y por consiguiente se cumple

$$\#(\mu_{p^\infty}(K)) \leq \frac{ep}{p-1},$$

pues los subgrupos finitos de las raíces de la unidad son cíclicos. □

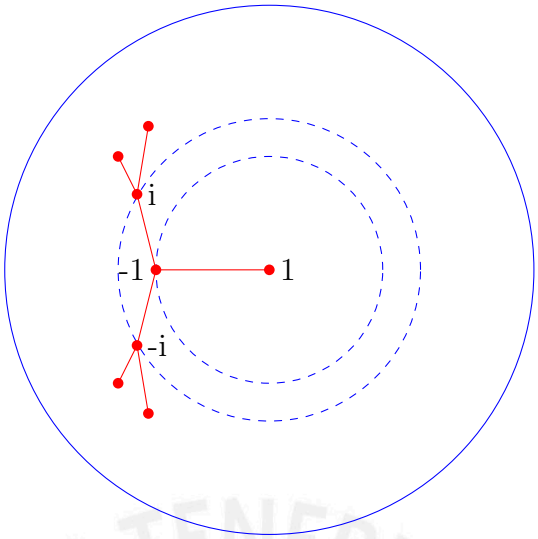
Notemos que el resultado de este corolario es válido para todos los cuerpos valuados K de característica 0 provistos de un valor absoluto que extiende el p-ádico. En particular si $e = 1$, tenemos $\#(\mu_{p^\infty}(K)) \leq p/(p-1)$. En particular para $p \geq 3$ tendremos $\#(\mu_{p^\infty}(K)) = 1$; mientras para $p = 2$ se consigue $\#(\mu_{2^\infty}(K)) \leq 2$. Pero ambos resultados ya eran conocidos desde el Capítulo 3.

Ejemplo 4.19. Sea el polinomio $p(x) = x^{2^n} - 1 \in \mathbb{Q}_2[x]$ con raíz ξ en alguna extensión finita K. Por la definición de norma se tiene $| \xi |_K = 1$; esto quiere decir que sus raíces estan ubicadas sobre la esfera unitaria. Es más, como ξ tiene orden una potencia de 2, digamos 2^{n_0}, se tiene gracias al Teorema 4.16 la desigualdad dada por $| \xi - 1 | = | 2 |^{1/\varphi(p^{n_0})} < 1$.

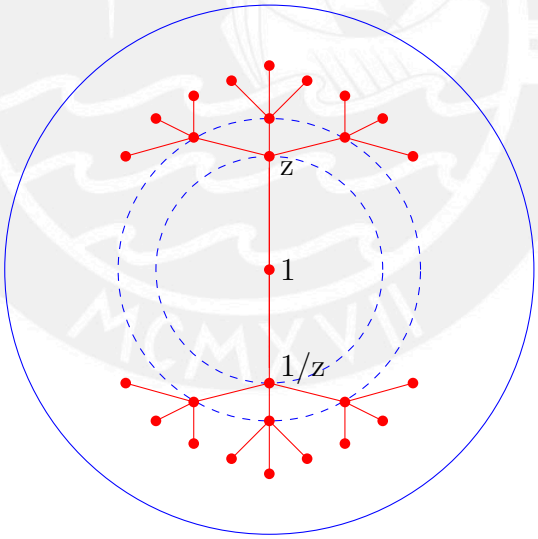
Por ejemplo, el cuarteto $\{-1, 1, -i, i\}$ cumple

$$| 1 - (-1) | = 2^{-1} \text{ y } | 1 - (-i) | = | 1 - (i) | = 2^{-1/2}.$$

Siguiendo de cerca a Robert[1], la siguiente figura muestra en forma esquemática la localización de las 2^n-ésimas raíces de la unidad.



Ejemplo 4.20. Realizando un estudio similar al ejemplo anterior, se puede localizar las 3^n-ésimas raíces de la unidad en la esfera unitaria de la clausura algebraica de $\mathbb{Q}_3$. Por ejemplo, si z fuese una raíz de la unidad en alguna extensión finita K se tiene $\mid z-1 \mid = \mid 1/z-1 \mid$. El esquema muestra la disposición de dichas raíces.



Ejemplo 4.21. Sea K una extensión generada sobre $\mathbb{Q}_p$ por una raíz p-ésima primitiva de la unidad y K' generada por una raíz primitiva de la unidad de orden

p^2. Ambas extensiones son totalmente ramificadas. Los grados de estas extensiones ciclotómicas están determinados por la teoría previa. El diagrama

$$\begin{array}{lcl} & K' = \mathbb{Q}_p(\zeta_{p^2}) & \\ \text{grado } p & | & \text{salvaje} \\ & K = \mathbb{Q}_p(\zeta_p) & \\ \text{grado } p-1 & | & \text{mansa} \\ & \mathbb{Q}_p & \end{array}$$

resume la situación. El elemento $\pi = \zeta_p - 1$ tiene valor absoluto $\mid \pi \mid = \mid p \mid^{1/(p-1)}$ y genera el grupo de valores $\mid K^* \mid$. Del mismo modo $\pi' = \zeta_{p^2} - 1$ tiene valor absoluto $\pi' = \mid p \mid^{1/p(p-1)}$ y genera el grupo de valores K'^*.

En resumen, si ζ es raíz primitiva de la unidad en alguna extensión finita K con $\zeta \in \mu_{p^\infty}(K)$, se tiene que $\mathbb{Q}_p(\zeta)$ resulta ser una extensión mansa debido a que se cumple $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p)] = p - 1$. Sin embargo si ζ es una raíz de orden p^k, con $k \geq 2$; ésta genera una extensión salvaje de $\mathbb{Q}_p(\zeta)$; es decir, somos capaces de generar extensiones salvajes a partir del estudio del grupo $\mu_{p^\infty}(K)$, motivo por el cuál nos preguntamos si toda extensión salvaje es generada por una raíz de la unidad de orden p^k. La respuesta es no. Ello se puede apreciar en el Ejemplo 3.18 en donde se obtuvo la extensión salvaje $\mathbb{Q}_2(\eta)$ con η raíz del polinomio $f(x) = x^2 - 2x + 2$ sin que la extensión fuese equivalente a la generada por una raíz de la unidad.

Bibliografía

[1] Atiyah, McDonald. *Introducción al algebra conmutativa*. Addison-Wesley, 1978.

[2] Condori. *Factorización de los polinomios sobre los números p-ádicos*. Tesis de maestría en Matemáticas, PUCP, 2001.

[3] Gaita. *Introducción a los números p-ádicos y comportamiento dinámico de polinomios en* $\mathbb{Q}_p$. Tesis de maestría en Matemáticas, PUCP, 1997.

[4] Lang. *Teoría de números algebraicos*. Addison-Wesley, 1970.

[5] Milne. *Cuerpos y teoría de Galois*. Notes, 2003

[6] Robert. *Un curso en análisis p-ádico*. Springer-Verlag, New York, 2000.

[7] Stewart and Tall. *Teoría algebraica de números y el último teorema de Fermat*. A. K. Peters, 2002.

[8] Weintraub. *Teoría de Galois*. Lehigh University Press, 2006.