Facultad
de
Ciencias

INTRODUCCIÓN A LOS CUERPOS P-ÁDICOS
(INTRODUCTION TO P-ADIC FIELDS)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Paula Echevarría González

Director: Maria Pilar Fernández-Ferreirós Erviti

Febrero-2016

1. Resumen

Es conocido que el cuerpo de los números reales surgió por la necesidad de completar el cuerpo de los números racionales y su completación se construyó gracias al valor absoluto usual. Pues bien, los cuerpos p-ádicos se obtienen al completar el cuerpo de los números racionales con respecto a los valores absolutos p-ádicos.

El objetivo del presente trabajo es estudiar la construcción y propiedades básicas de los cuerpos p-ádicos, prestando especial atención al Lema de Hensel y mostrando algunas de sus aplicaciones a la obtención de propiedades algebraicas de dichos cuerpos.

Los números p-ádicos tienen gran interés teórico pero además han servido como herramienta base en la obtención de importantes resultados en Álgebra, Análisis, Aritmética y posteriormente, también en Física.

Palabras Clave: p-ádico, valor absoluto, completación, números racionales, lema de Hensel, raíces de la unidad.

2. Abstract

It is known that the real number field appear from the need to complete the rational number field and its completion was built from the usual absolute value. In the same way, the p-adic fields arise when the rational number field is completed from the p-adic absolute values.

The aim of this work is to study the construction and basic properties of the p-adic numbers, paying special attention to Hensel's lemma and showing some of their applications to obtain algebraic properties of that fields.

The p-adic numbers have not only theoretical interest but they have been a useful tool to obtain important results in Algebra, Analysis, Arithmetic and later, also in Physics.

Key Words: p-adic, absolute value , completion, rational numbers, Hensel's lemma, roots of unity.

Índice general

1. Historia **5**
1.1. Los números p-ádicos 5
1.2. Biografía de Kurt Hensel 6

2. Introducción a los números p-ádicos **9**
2.1. Valor absoluto p-ádico 9
2.2. Compleción de $\mathbb{Q}$ 14
2.3. Los enteros p-ádicos 22
2.4. El lema de Hensel 32
2.5. Aplicaciones del lema de Hensel 38
2.5.1. Determinación y Cálculo de las Unidades de $\mathbb{Z}_p$ 38
2.5.2. Raíces cuadradas en $\mathbb{Q}_p$ 38
2.5.3. Raíces de la unidad en $\mathbb{Q}_p$ 42

Capítulo 1

Historia

1.1. Los números p-ádicos

Los números p-ádicos fueron descritos por primera vez por Kurt Hensel en torno al 1897. Estos números surgieron del interés por calcular la potencia exacta con la que un primo divide al discriminante de un cuerpo de números. El ejemplo 2 que exponemos en la sección 3 de Capítulo 2 muestra cómo la construcción de los números p-ádicos está estrechamente relacionada con la resolución de ecuaciones en congruencias módulo p^n.

Para abordar este tema, Hensel comenzó observando las muchas propiedades semejantes que tienen el cuerpo de los números racionales $\mathbb{Q}$ y el anillo de los polinomios con coeficientes complejos $\mathbb{C}(X)$.

Por una parte consideramos $\mathbb{Z}$ junto con su cuerpo de fracciones $\mathbb{Q}$ y por otra $\mathbb{C}[X]$ junto con su cuerpo de fracciones $\mathbb{C}(X)$. Sean $f(X) \in \mathbb{C}(X)$ y $x \in \mathbb{Q}$, podemos ver que ambos son muy similares:

$$f(X) = \frac{P(X)}{Q(X)} \qquad\qquad x = \frac{p}{q}$$

donde $P(X), Q(X) \in \mathbb{C}[X]$ con $Q(X) \neq 0$ y $p, q \in \mathbb{Z}$ con $q \neq 0$.

Además Hensel notó que tanto $\mathbb{C}(X)$ como $\mathbb{Q}$ son cuerpos de fracciones de un dominio de ideales principales en el cual todos los ideales primos no nulos son maximales. Así, observó que los anillos $\mathbb{Z}$ y $\mathbb{C}[X]$ admiten factorización única. Si nos fijamos, todo número entero puede expresarse de forma única como producto de primos y, al mismo tiempo, cualquier polinomio puede expresarse de forma única del modo siguiente:

$$P(X) = a(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$$

Es decir, según Hensel, los números primos $p \in \mathbb{Z}$ son semejantes a los polinomios lineales $(x - \alpha) \in \mathbb{C}[X]$.

Sea $P(X) \in \mathbb{C}[X]$ y $\alpha \in \mathbb{C}$, es posible escribir su desarrollo en serie de potencias de $(x - \alpha)$ (por ejemplo con el desarrollo en serie de potencias de Taylor)

$$P(X) = \sum_{i=0}^{n} a_i (x - \alpha)^i$$

con $a_i \in \mathbb{C}$. De esta forma, tenemos que el análogo a este desarrollo es el desarrollo de un entero positivo m en potencias de p con p primo, es decir,

$$m = \sum_{i=0}^{n} a_i p^i$$

con $a_i \in \mathbb{Z}$ y $0 \leq a_i < p$. Esta expresión es la que se denomina desarrollo p-ádico de m.

Finalmente, dado $f(X) \in \mathbb{C}(X)$ y $\alpha \in \mathbb{C}$, es posible expandir f(X) como una serie de Laurent en torno a α_i

$$f(X) = \sum_{i \geq n_0} a_i (X - \alpha)^i$$

Y dado $x \in \mathbb{Q}$ se puede operar análogamente y obtener una serie de Laurent en potencias de p:

$$x = \sum_{i \geq n_0} a_i p^i$$

De este modo fue como Hensel vio que el conjunto de todas las series formales de Laurent en p forman un cuerpo, al que denominaremos cuerpo de los números p-ádicos y denotaremos por $\mathbb{Q}_p$. Este cuerpo contiene al cuerpo de los números racionales pero es estrictamente mayor que él.

1.2. Biografía de Kurt Hensel

Kurt Hensel nació el 29 de diciembre de 1861 en Prusia Oriental donde vivió 9 años, edad a la que se trasladó a Berlín. Su padre era terrateniente en Prusia pero al mudarse a Berlín se convirtió en director de una empresa de construcción.

Durante el tiempo que vivió en Prusia no fue a la escuela, sino que fue educado por sus padres en casa. A los 9 años pisó por primera vez un colegio, Friedrich-Wilhelm Gymnasium, donde descubrió su pasión por las matemáticas gracias a su profesor, K. H. Schellbach. Schellbach no tardó en darse cuenta de que Hensel no era un alumno cualquiera, sino que era

un alumno muy aventajado en lo que a matemáticas se refería. Por ello, Schellbach le proporcionaba material más técnico y avanzado. Cuando llegó la hora de pasar a la universidad Hensel no tenía ninguna duda de qué carrera estudiaría, matemáticas. En esta época los estudiantes alemanes no elegían una sola universidad en la que cursar sus estudios, sino que escogían varias y se iban moviendo por las diferentes clases. Hensel escogió las universidades de Berlín y Bonn. Entre otros muchos profesores, tuvo la suerte de coincidir con Lipschitz, Weierstrass, Borchardt, Kirchhoff, Helmholtz y Kronecker. Pero sin duda fue Kronecker quien más influencia tuvo sobre él, por eso fue quien dirigió su tesis doctoral en 1884 en la universidad de Berlín, donde continuó trabajando.

Entre 1895 y 1930 publicó 5 volúmenes en los que recopiló la obra de Kronecker. El trabajo que hizo Weierstrass en 1897 del desarrollo en series de potencias de las funciones algebraicas, le llevó a definir los números p-ádicos debido a su interés por calcular la potencia exacta con la que un primo divide al discriminante de un cuerpo de números. Con esta técnica pudo probar muchos resultados sobre formas cuadráticas y teoría de números. La enorme potencia de su técnica no fue valorada hasta 1921 cuando Hasse probó el llamado principio local-global: demostró que una forma cuadrática tiene una solución racional si y sólo si la tiene en los números reales y en los p-ádicos para todo primo p.

En su obra "Theorie der algebraischen Zahlen" publicada en 1908 desarrolla toda su teoría sobre los números p-ádicos. En esta obra y en la siguiente "Zahlentheorie" publicada en 1917 muestra toda la fuerza de esta técnica para abordar problemas de divisibilidad en un cuerpo de números.

Hensel murió el 1 de junio del 1941 a los 79 años.

Capítulo 2

Introducción a los números p-ádicos

2.1. Valor absoluto p-ádico

Definición 2.1.1 *Sea K un cuerpo, se denomina valor absoluto sobre K a una función*

$$|\ |: K \ \to \mathbb{R}^+$$

que $\forall x, y \in K$ verifica las siguientes propiedades:

1. $|x| \geq 0$; $|x| = 0$ *si y sólo si* $x = 0$
2. $|x + y| \leq |x| + |y|$ *(Desigualdad triangular)*
3. $|xy| = |x||y|$

Definición 2.1.2 *Un valor absoluto $|\ |$ en un cuerpo K es no arquimediano si para $x \in K$ se cumple*

$$|x| \leq 1 \Rightarrow |1 + x| \leq 1$$

Lema 2.1.1 *El valor absoluto $|\ |$ en un cuerpo K es no arquimediano si y sólo si cumple la desigualdad triangular fuerte, es decir, si $\forall x, y \in K$*

$$|x + y| \leq max\{|x|, |y|\}$$

Dem: Queremos demostrar que

$$|x| \leq 1 \Rightarrow |x+1| \leq 1 \text{ si y sólo si } |x+y| \leq max\{|x|, |y|\}$$

La implicación de derecha a izquierda es trivial tomando $y = 1$, por tanto vamos a probar la otra implicación.

Vamos a suponer que $xy \neq 0$ (si $xy = 0$ es trivial). También vamos a suponer, sin pérdida de generalidad, que $|x| \leq |y|$.

$$|x+y||y|^{-1} = |\tfrac{x+y}{y}| = |\tfrac{x}{y} + 1|$$

Como $|x| \leq |y|$ entonces $\frac{|x|}{|y|} \leq 1$ y por tanto $\left|\frac{x}{y}\right| \leq 1$.

Así, como $\left|\frac{x}{y}\right| \leq 1$ entonces $|\frac{x}{y} + 1| \leq 1$, es decir, $|x+y||y|^{-1} \leq 1$. Por tanto,

$$|x+y| \leq |y| = max\{|x|, |y|\}$$

Además se cumple que, si $|x| \neq |y|$ entonces $|x+y| = max\{|x|, |y|\}$.

Ahora vamos a introducir la definición de valor absoluto p-ádico en $\mathbb{Q}$. Para ello vamos a comenzar dando la definición de valoración y cuerpo valuado, luego introduciremos la definición de valoración p-ádica en $\mathbb{Z}$ y veremos cómo extenderla a $\mathbb{Q}$.

Definición 2.1.3 *Si K es un cuerpo, se denomina valoración sobre K a una función*

$$v : K \to \mathbb{R} \cup \{\infty\}$$

que verifica las siguientes propiedades: si $x, y \in K$

1. $v(x) = \infty \Leftrightarrow x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x+y) \geq min\{v(x), v(y)\}$

En este caso diremos que el par (K, v) es un cuerpo valuado.

Definición 2.1.4 *Dado un número primo $p \in \mathbb{Z}$, cualquier entero no nulo a se expresa de una única manera en la forma $a = p^r a'$ con r entero no negativo y a' no divisible por p. De acuerdo con esta propiedad, se denomina valoración p-ádica en $\mathbb{Z}$ a la función*

$$v_p : \mathbb{Z}\setminus\{0\} \ \to \mathbb{R}$$

que asocia, a cada entero no nulo $a \in \mathbb{Z}$, el único entero no negativo $v_p(a)$ tal que $a = p^{v_p(a)}a'$ donde $(p, a') = 1$.

Veamos ahora cómo se puede extender v_p al cuerpo de los números racionales.

Si $x \in \mathbb{Q}, x = \frac{a}{b}$ con $a, b \in \mathbb{Z}$. Entonces, se tiene

$$a = p^{v_p(a)}a' \qquad\qquad b = p^{v_p(b)}b'$$

Por tanto, se puede escribir $x = p^{v_p(a)-v_p(b)}\frac{a'}{b'}$ y con a' y b' primos con p.

Veamos ahora que esta expresión es única. Suponemos que hay dos expresiones distintas,

$$x = p^r\frac{a'}{b'} = p^s\frac{a''}{b''}$$

con a', a'', b' y b'' primos con p. Así tenemos, $p^r a'b'' = p^s a''b'$ de donde $r = s$ y nos queda $a'b'' = b'a''$. Por tanto $\frac{a'}{b'} = \frac{a''}{b''}$. Así que la expresión es única y no depende de la representación de x como cociente de dos enteros.

Definición 2.1.5 *Sea $x = \frac{a}{b} \in \mathbb{Q}^*$, la valoración p-ádica de $\mathbb{Q}$ viene determinada por la formula*

$$x = \frac{a}{b} = p^{v_p(x)}\frac{a'}{b'}$$

donde $(p, a') = 1$ y $(p, b') = 1$.

Lema 2.1.2 *Para todo $x, y \in \mathbb{Q}^*$ se tiene*

1. *$v_p(xy) = v_p(x) + v_p(y)$*
2. *$v_p(x + y) \geq min\{v_p(x), v_p(y)\}$.*

Si además $v_p(x) \neq v_p(y)$, se cumple que $v_p(x + y) = min\{v_p(x), v_p(y)\}$.

Dem: Consideramos $x, y \in \mathbb{Q}$. Por comodidad vamos a llamar $r = v_p(x)$ y $s = v_p(y)$.

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

   Escribimos

$$x = p^r x' \qquad\qquad y = p^s y'$$

Así, por una parte tenemos

$$xy = p^{v_p(xy)}(xy)'$$

Y por otra

$$xy = p^r p^s x'y' = p^{r+s}x'y'$$

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

   Sean

   $$x = \frac{a}{b} = p^r \frac{a'}{b'} \qquad\qquad y = \frac{c}{d} = p^s \frac{c'}{d'}.$$

   con $(a'b', p) = 1 = (c'd', p)$ y $r, s \in \mathbb{Z}$.

   Primero vamos a suponer que $r < s$,

   $$x + y = p^r \frac{a'}{b'} + p^s \frac{c'}{d'} = \frac{p^r a'd' + p^s b'c'}{b'd'} = \frac{p^r(a'd' + p^{s-r}b'c')}{b'd'} = p^r \frac{a'd' + p^{s-r}b'c'}{b'd'}$$

   donde tanto el numerador como el denominador son primos con p. Por tanto, $v_p(x+y) = r = min\{r, s\}$.

   Veamos ahora que ocurre cuando $r = s$.

   $$x + y = p^r \frac{a'}{b'} + p^s \frac{c'}{d'} = \frac{p^r a'd' + p^s b'c'}{b'd'} = p^r \frac{(a'd' + b'c')}{b'd'}$$

   donde sabemos que $b'd'$ es primo con p pero $a'd' + b'c'$ no tiene por que serlo. Por tanto, vamos a escribir $a'd' + b'c' = p^t e$ con $t \geq 0$ y $(e, p) = 1$. Entonces,

   $$p^r \frac{(a'd' + b'c')}{b'd'} = p^{r+t} \frac{e}{b'd'}$$

   Así, en este caso $v_p(x+y) = r + t \geq r = min\{r, s\}$

Definición 2.1.6 *Para cada $x \in \mathbb{Q}$ con $x \neq 0$, definimos valor absoluto p-ádico en $\mathbb{Q}$ como*

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

Si $x = 0$ definimos $|x| = 0$, es decir $v_p(0) = \infty$

Ahora nos falta comprobar que lo que acabamos de definir es de verdad un valor absoluto.

Proposición 2.1.1 *La función $|\ |_p$ es un valor absoluto no arquimediano.*

Dem: Vamos a comprobar las 3 propiedades que tiene que cumplir para ser un valor absoluto. Sean $x, y \in \mathbb{Q}$

1. $|x|_p \geq 0; |x|_p = 0 \Leftrightarrow x = 0$

   Como p es un número primo $p > 1$, por tanto $|x|_p = p^{-v_p(x)} \geq 0$. Por definición está claro que $|x|_p = 0 \Leftrightarrow x = 0$

2. $|x + y|_p \leq |x|_p + |y|_p$

   Por el lema 2.1.2 sabemos que $v_p(x+y) \geq min\{v_p(x), v_p(y)\}$; además vamos a suponer, sin pérdida de generalidad, que $v_p(x) \leq v_p(y)$

$$\begin{aligned} |x+y|_p &= p^{-v_p(xy)} \leq p^{-min\{v_p(x),v_p(y)\}} = p^{-v_p(x)} \leq \\ &\leq p^{-v_p(x)} + p^{-v_p(y)} = |x|_p + |y|_p \end{aligned}$$

3. $|xy|_p = |x|_p|y|_p$

   Por el lema 2.1.2 sabemos que $v_p(xy) = v_p(x) + v_p(y)$ por tanto tenemos,

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

Para comprobar que es no arquimediano basta ver que se cumple la condición siguiente

$$|x + y|_p \leq max\{|x|_p, |y|_p\}$$

Para demostrarlo, utilizamos la desigualdad ya probada en 2:

$$|x + y|_p \leq p^{-min\{v_p(x),v_p(y)\}}$$

Entonces

$$|x + y|_p \leq p^{-min\{v_p(x),v_p(y)\}} = max\left\{p^{-v_p(x)}, p^{-v_p(y)}\right\} = max\{|x|_p, |y|_p\}$$

Por tanto, hasta ahora conocemos los siguientes valores absolutos definidos sobre $\mathbb{Q}$:

- El valor absoluto trivial.
- El valor absoluto usual, que representaremos por $|\ |_\infty$.

- Para cada primo p, el valor absoluto p-ádico, $|\ |_p$.

Para compararlos y estudiar la posible existencia de otros, se introduce el concepto de valores absolutos equivalentes, es decir, aquellos que definen la misma topología.

Lema 2.1.3 *Sean $|\ |_1$ y $|\ |_2$ dos valores absolutos en un cuerpo K. Las condiciones siguientes son equivalentes:*

- *$|\ |_1$ y $|\ |_2$ son valores absolutos equivalentes.*
- *Para cada $x \in K$ tenemos $|x|_1 < 1$ si y sólo si $|x|_2 < 1$.*
- *Existe $\alpha \in \mathbb{R}$ tal que $\forall x \in K$ se tenga que*

$$|x|_1 = |x|_2^{\alpha}$$

Proposición 2.1.2 *Un valor absoluto p-ádico no es equivalente al valor absoluto usual. Además, si p, q son primos distintos, los valores absolutos p-ádico y q-ádico no son equivalentes.*

Dem: La primera afirmación es obvia ya que para cualquier valor absoluto p-ádico se cumple, por ser no-arquimediano, que $|n| \leq 1\ \forall n \in \mathbb{Z}$.

Si p, q son primos distintos, se cumple que $|p|_p = p^{-1} < 1$ y $|p|_q = 1$. Por tanto $|\ |_p$ y $|\ |_q$ no son equivalentes.

Por otro lado, para cualquier primo p, es $|p|_p = p^{-1} < 1$ y $|p|_\infty = p > 1$

Teorema 2.1.1 *(Ostrowski) Todo valor absoluto no trivial en $\mathbb{Q}$ es equivalente a un valor absoluto $|\ |_p$ donde p es un número primo o $p = \infty$*

2.2. Compleción de $\mathbb{Q}$

Definición 2.2.1 *Sea K un cuerpo y sea $|\ |$ un valor absoluto en K. Una sucesión (x_n) se llama sucesión de Cauchy si $\forall \epsilon > 0$ existe un índice n_0 (que depende de ϵ) tal que $\forall n, m$ con $n \geq n_0$ y $m \geq n_0$ se verifica*

$$|x_n - x_m| < \epsilon$$

Definición 2.2.2 *Sea K un cuerpo y sea $|\ |$ un valor absoluto en K. Se dice que K es completo con respecto a $|\ |$ si toda sucesión de Cauchy de elementos de K es convergente.*

Es conocido por todos que el cuerpo de los números racionales $\mathbb{Q}$ no es completo con respecto al valor absoluto usual y que el cuerpo de los números reales $\mathbb{R}$ es su completado respecto a este valor absoluto.

Probaremos en esta sección que el cuerpo $\mathbb{Q}$ tampoco es completo respecto de ningún valor absoluto p-ádico y construiremos su completado, el llamado cuerpo de los números p-ádicos .

Lema 2.2.1 *Una sucesión de números racionales (x_n) es de Cauchy con respecto a un valor absoluto no arquimediano $|\ |$ si y sólo si*

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

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

Para probar la otra implicación suponemos que $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$. Entonces, para $\epsilon > 0$, existe n_0 tal que $|x_{n+1} - x_n| < \epsilon$ para cada $n \geq n_0$.

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

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + ... + x_{n+1} - x_n| \leq \\ &\leq max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, ..., |x_{n+1} - x_n|\} < \epsilon \end{aligned}$$

y (x_n) es de Cauchy.

Lema 2.2.2 *El cuerpo $\mathbb{Q}$ no es completo respecto de ningún valor absoluto p-ádico.*

Dem: Consideramos $|\ |_p$ para algún primo p y construiremos una sucesión de Cauchy en $\mathbb{Q}$ cuyo límite no esté en $\mathbb{Q}$. Para ello vamos a buscar una sucesión de soluciones módulo p^n de una ecuación que no tenga solución en $\mathbb{Q}$.

Lo probamos en primer lugar cuando p es un primo impar y luego lo veremos para $p = 2$:

Sea $a \in \mathbb{Z}$ cumpliendo las condiciones siguientes:

- a no es cuadrado en $\mathbb{Q}$.
- a primo con p.
- a residuo cuadrático módulo p, es decir, existe solución de la ecuación $x^2 \equiv a$ mód p.

Para elegir dicho entero a, basta escoger el cuadrado de cualquier entero b que sea primo con p y elegir un entero t de forma que $a = b^2 + tp$ no sea cuadrado en $\mathbb{Q}$.

Construimos ahora la sucesión de Cauchy del modo siguiente:

- escogemos $x_1 = b$ que es solución de $x_1^2 \equiv a \text{ mód } p$
- escogemos x_2 tal que

$$x_2 \equiv x_1 \text{ mód } p \text{ y } x_2^2 \equiv a \text{ mód } p^2$$

- en general, escogemos x_{n+1} tal que

$$x_{n+1} \equiv x_n \text{ mód } p^n \text{ y } x_{n+1}^2 \equiv a \text{ mód } p^{n+1}.$$

La existencia de los x_n elegidos anteriormente la vamos a probar por inducción.

Para $n = 1$ es $x_1 = b$ y $x_1^2 = a + pc$ con $c \in \mathbb{Z}$. Para encontrar x_2 tal que $x_2 \equiv x_1$ mód p, vale cualquiera de la forma $x_2 = x_1 + tp$ con $t \in \mathbb{Z}$. Así que vamos a tratar de calcular dicho t para que se cumpla $x_2 \equiv a$ mód p^2.

$$x_2^2 = (x_1 + tp)^2 \equiv x_1^2 + 2x_1tp = a + pc + 2x_1tp \text{ mód } p^2$$

y entonces

$$x_2^2 \equiv a \text{ mód } p^2 \Leftrightarrow pc + 2tx_1p = p(c + 2tx_1) \equiv 0 \text{ mód } p^2 \Leftrightarrow c + 2tx_1 \equiv 0 \text{ mód } p$$

Como $2x_1$ es primo con p entonces existe $(2x_1)^{-1}$ mód p y por tanto ya tenemos que $t = -c(2x_1)^{-1}$ existe y es único.

Ahora vamos a suponer que existe x_n tal que

$$x_n \equiv x_{n-1} \text{ mód } p^n \qquad \text{y} \qquad x_n^2 \equiv a \text{ mód } p^{n+1}$$

Vamos a trabajar de forma análoga al caso $n = 1$. Como sabemos que $x_n^2 \equiv a$ mód p^{n+1} entonces $x_n^2 = a + cp^{n+1}$ con $c \in \mathbb{Z}$.

Para que $x_{n+1} \equiv x_n$ mód p^{n+1}, debe ser $x_{n+1} = x_n + tp^{n+1}$ para algún $t \in \mathbb{Z}$. Así que vamos a calcular t para que se cumpla $x_{n+1}^2 \equiv a$ mód p^{n+2}.

$$\begin{aligned} x_{n+1}^2 &= (x_n + tp^{n+1})^2 = x_n^2 + t^2p^{2n+2} + 2x_ntp^{n+1} = x_n^2 + t^2p^{n+2}p^n + 2x_ntp^{n+1} \\ &\equiv x_n^2 + 2x_ntp^{n+1} = a + bp^{n+1} + 2x_ntp^{n+1} \text{ mód } p^{n+2} \end{aligned}$$

y entonces

$$x_{n+1}^2 \equiv a \text{ mód } p^{n+2} \Leftrightarrow p^{n+1}(b + 2tx_n) \equiv 0 \text{ mód } p^{n+2} \Leftrightarrow b + 2tx_n \equiv 0 \text{ mód } p$$

Continuando de la misma forma que en el caso anterior tenemos que

$$t = -b(2x_n^{-1})$$

existe y además es único. Así queda demostrado que la sucesión existe siempre que exista el elemento x_1 inicial. Pero falta comprobar que la sucesión es de Cauchy.

Gracias al lema 2.2.1, basta comprobar que

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

Como para cada n, es $x_{n+1} \equiv x_n$ mód p^{n+1} se cumple que

$$|x_{n+1} - x_n| = |tp^{n+1}| \leq p^{-(n+1)}$$

entonces $lim_{n\to\infty}|x_{n+1} - x_n| = 0$ y (x_n) es una sucesión de Cauchy.

Además, como, para cada n, es $x_n^2 \equiv a$ mód p^{n+1}, se cumple que

$$|x_n^2 - a| = |cp^{n+1}| \leq p^{-(n+1)}$$

Por tanto, $lim_{n\to\infty}|x_n^2 - a| = 0$, es decir, el límite de (x_n), en caso de existir, tiene que ser la raíz cuadrada de a. Como habíamos escogido a de forma que no fuese raíz cuadrada en $\mathbb{Q}$, entonces la sucesión no tiene límite en $\mathbb{Q}$.

Probamos ahora que $\mathbb{Q}$ no es completo respecto del valor absoluto $|\ |_2$ construyendo una sucesión de Cauchy (x_n) de forma que $(x_n^2 + 7) \to 0$.

Para $x_1 = 1$ se cumple que $x_1^2 + 7 \equiv 0$ mód 2^3 y $x_1^2 + 7 = 2^3 b_1$ con $b_1 = 1$.

Buscamos x_2 tal que $x_2 \equiv x_1$ mód 4 y $x_2^2 + 7 \equiv 0$ mód 2^4. Entonces $x_2 = x_1 + 4t$ y

$$x_2^2 + 7 = (x_1 + 4t)^2 + 7 = x_1^2 + 7 + 16t^2 + 8tx_1 = 2^3 b_1 + 16t^2 + 8tx_1$$

Se cumple que

$$x_2^2 + 7 = 2^3 + 16t^2 + 8t \equiv 0 \text{ mód } 2^4 \Leftrightarrow 1 + t \equiv 0 \text{ mód } 2$$

Para $t = 1$, se obtiene $x_2 = 5$ con $x_2^2 + 7 \equiv 0$ mód 2^5.

En general, si $n > 1$ y existe x_n de forma que $x_n \equiv x_{n-1}$ mód 2^n y $x_n^2 + 7 \equiv 0$ mód 2^{n+2} con $x_n^2 + 7 = 2^{n+2}b_n$, x_n es impar y para el elemento $x_{n+1} = x_n + 2^{n+1}b_n$ se cumple que $x_{n+1} \equiv x_n$ mód 2^{n+1} y

$$\begin{aligned} x_{n+1}^2 + 7 &= x_n^2 + 7 + 2^{2n+2}b_n^2 + 2^{n+2}b_n x_n = 2^{n+2}b_n + 2^{2n+2}b_n^2 + 2^{n+2}b_n x_n = \\ &= 2^{2n+2}b_n^2 + 2^{n+2}b_n(1 + x_n) \equiv 0 \text{ mód } 2^{n+3} \end{aligned}$$

Se obtiene así una sucesión de enteros (x_n) que es de Cauchy y cumple que $|x_n^2 + 7|_2 < 2^{-(n+2)}$ para cada n. Además no tiene límite en $\mathbb{Q}$ puesto que no existe $a \in \mathbb{Q}$ tal que $a^2 = -7$.

Así queda demostrado que $\mathbb{Q}$ no es completo con respecto a ningún valor absoluto p-ádico.

Para construir su completado nos basaremos en la construcción de $\mathbb{R}$ a partir de $\mathbb{Q}$. Es decir, vamos a tratar de "añadir" a $\mathbb{Q}$ los límites de todas las sucesiones de Cauchy.

Definición 2.2.3 *Si $|\ |_p$ es un valor absoluto p-ádico en $\mathbb{Q}$, denotamos por $\mathcal{C}$ al conjunto de todas las sucesiones de Cauchy de elementos de $\mathbb{Q}$*

$$\mathcal{C} = \{(x_n) : (x_n) \text{ es una sucesión de Cauchy con respecto a } |\ |_p\}$$

Proposición 2.2.1 *Si definimos la suma y el producto de sucesiones del modo siguiente*

$$(x_n) + (y_n) = (x_n + y_n)$$

$$(x_n)(y_n) = (x_n y_n)$$

entonces $\mathcal{C}$ es un anillo conmutativo con unidad.

Dem: Es fácil ver que tanto para la suma como para el producto se cumplen la propiedad asociativa y conmutativa, al igual que la distributiva. Además está claro que para la suma existe elemento neutro (la sucesión constante cero) y elemento opuesto y que el elemento neutro para el producto es la sucesión constante 1.

Por tanto, lo único que tenemos que probar es que la suma y producto de sucesiones de Cauchy es de Cauchy. Aplicando el lema 2.2.1 basta probar para dos sucesiones de Cauchy (x_n), (y_n) las dos propiedades siguientes:

- $lim_{n\to\infty}|(x_{n+1} + y_{n+1}) - (x_n + y_n)|_p = 0$

$$\begin{aligned} 0 &\leq |(x_{n+1} + y_{n+1}) - (x_n + y_n)|_p = |(x_{n+1} - x_n) + (y_{n+1} - y_n)|_p \leq \\ &\leq (|x_{n+1} - x_n|_p + |y_{n+1} - y_n|_p) = |x_{n+1} - x_n|_p + |y_{n+1} - y_n|_p = 0 \end{aligned}$$

- $lim|x_{n+1}y_{n+1} - x_n y_n|_p = 0$

$$\begin{aligned}
& |x_{n+1}y_{n+1} - x_n y_n|_p = \\
= \; & |x_{n+1}(y_{n+1} - y_n) + x_{n+1}y_n - x_n y_n|_p = \\
= \; & |x_{n+1}(y_{n+1} - y_n) + y_n(x_{n+1} - x_n)|_p \leq \\
\leq \; & [|x_{n+1}(y_{n+1} - y_n)|_p + |y_n(x_{n+1} - x_n)|_p] = \\
= \; & |x_{n+1}(y_{n+1} - y_n)|_p + |y_n(x_{n+1} - x_n)|_p] = \\
= \; & [|x_{n+1}|_p|y_{n+1} - y_n|_p] + [|y_n|_p|x_{n+1} - x_n|_p] = \\
= \; & |x_{n+1}|_p lim|y_{n+1} - y_n|_p + |y_n|_p lim|x_{n+1} - x_n|_p = 0
\end{aligned}$$

El propósito final de este capítulo es llegar a construir la completación de $\mathbb{Q}$ y por tanto no debemos olvidar que dicha construcción debe extender a $\mathbb{Q}$. Así que ahora vamos ver que existe una inclusión de $\mathbb{Q}$ en $\mathcal{C}$. Para ello basta considerar, para cada $x \in \mathbb{Q}$, la sucesión de Cauchy $x, x, x, x, x...$ a la que denominaremos sucesión constante asociada a x y denotaremos por (x). Así tenemos que la función $x \longrightarrow (x)$ es claramente una inclusión de $\mathbb{Q}$ en $\mathcal{C}$.

En un principio dijimos que íbamos a tratar de "añadir" a $\mathbb{Q}$ los límites de todas las sucesiones de Cauchy. Para ello hemos construido el anillo $\mathcal{C}$. El problema que ahora surge con este anillo es que, diferentes sucesiones de Cauchy cuyos términos se van acercando, deberían de tener el mismo límite, pero en nuestro anillo son objetos diferentes. Es decir, podemos encontrar dos sucesiones distintas convergiendo al mismo valor en $\mathcal{C}$.

Sabemos que dos sucesiones tienen el mismo límite cuando sus términos están cada vez más cerca, es decir, cuando su diferencia tiende a cero. Así vamos a analizar las sucesiones que tienden a cero.

Definición 2.2.4 *Sea $\mathcal{N} \subset \mathcal{C}$ el ideal que contiene a las sucesiones que tienden a cero con respecto al valor absoluto $|\ |_p$*

$$\mathcal{N} = \{(x_n) : x_n \to 0\} = \{(x_n) : lim_{n\to\infty}|x_n|_p = 0\}$$

Lema 2.2.3 *$\mathcal{N}$ es un ideal maximal de $\mathcal{C}$*

Dem: Es fácil comprobar que $\mathcal{N}$ cumple las condiciones para ser un ideal de $\mathcal{C}$. Veamos ahora que efectivamente es maximal.

Sea $(x_n) \in \mathcal{C}\backslash\mathcal{N}$, es decir, (x_n) es una sucesión de Cauchy cuyo límite es distinto de cero. Probaremos que el ideal I generado por (x_n) y $\mathcal{N}$, coincide con $\mathcal{C}$. Para ello, basta probar que $(1) \in I$.

Como (x_n) es de Cauchy pero no converge a cero, entonces tienen que existir $c > 0$ y $N \in \mathbb{N}$ tales que $|x_n| \geq c > 0$, $\forall n \geq N$. En particular, si $n \geq N$ entonces $x_n \neq 0$. Así que vamos a definir una nueva sucesión (y_n) como

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

Vamos a probar ahora que (y_n) es de Cauchy. Al igual que en ocasiones anteriores, como $|\ |_p$ es no arquimediano, apoyandonos en el lema 2.2.1, basta probar que

$$|y_{n+1} - y_n| \longrightarrow 0$$

Por como hemos definido y_n, es suficiente con probarlo cuando $n > N$.

$$|y_{n+1} - y_n| = |\tfrac{1}{x_{n+1}} - \tfrac{1}{x_n}| = |\tfrac{x_{n+1}-x_n}{x_{n+1}x_n}| = \tfrac{|x_{n+1}-x_n|}{|x_{n+1}x_n|} \leq \tfrac{|x_{n+1}-x_n|}{c^2} \longrightarrow 0$$

Por tanto, (y_n) es una sucesión de Cauchy. Así,

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

Por tanto, si a la sucesión (1) le restamos el producto de (x_n) e (y_n), obtenemos una sucesión que tiende a cero. Es decir,

$$(1) - (x_n)(y_n) \in \mathcal{N}$$

Esto quiere decir que la sucesión constante 1 se puede escribir como múltiplo de (x_n) más un elemento de $\mathcal{N}$ y por tanto $(1) \in I$.

Como lo que queremos conseguir es identificar las sucesiones que tienen el mismo límite, es decir, aquellas que difieren en elementos de $\mathcal{N}$, lo que haremos será utilizar la herramienta algebraica de pasar al cociente. Vamos a hacer el cociente del anillo $\mathcal{C}$ por el ideal $\mathcal{N}$. Como hemos probado que el ideal es maximal, entonces dicho cociente es un cuerpo.

Definición 2.2.5 *Definimos el cuerpo de los números p-ádicos como el cociente del anillo $\mathcal{C}$ y su ideal maximal $\mathcal{N}$:*

$$\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$$

Notemos que dos sucesiones constantes distintas nunca difieren en un elemento de $\mathcal{N}$ y por tanto continuamos teniendo la inclusión

$$\mathbb{Q} \longrightarrow \mathbb{Q}_p$$

simplemente enviando a cada $x \in \mathbb{Q}$ a la clase de equivalencia de (x).

Así ya tenemos un cuerpo y una inclusión de $\mathbb{Q}$ en dicho cuerpo. Ahora tenemos que comprobar que se cumplen las propiedades de la completación y para ello lo primero que vamos a ver es que el valor absoluto $|\ |_p$ se extiende a $\mathbb{Q}_p$

Lema 2.2.4 *Sea $(x_n) \in \mathcal{C}\backslash\mathcal{N}$, la sucesión $|x_n|_p$ de números reales es estacionaria, es decir, existe $N \in \mathbb{Z}$ tal que, si $n, m \geq N$ entonces*

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

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

Si consideramos $N = max\{N_1, N_2\}$, ambas condiciones se cumplen y tenemos que $\forall n, m \geq N$,

$$|x_n - x_m| < max\{|x_n|, |x_m|\}$$

Así, por la propiedad no arquimediana vista en el Lema 2.1.1, se tiene que $|x_n| = |x_m|$

Del resultado anterior se deduce que si $(x_n) \in \mathcal{C}\backslash\mathcal{N}$, la sucesión $|x_n|_p$ es convergente en $\mathbb{R}$, lo que nos permite dar la siguiente definición

Definición 2.2.6 *Si $x \in \mathbb{Q}_p$ y (x_n) es una sucesión de Cauchy representando a x, definimos*

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

Es inmediato comprobar que, con esta definición, el valor de $|\ |_p$ no depende del representante (x_n) elegido y que $|\ |_p$ es un valor absoluto de $\mathbb{Q}_p$.

Teorema 2.2.1 *Para cada primo p, $|\ |_p$ es un valor absoluto en $\mathbb{Q}_p$ que extiende al valor absoluto p-ádico de $\mathbb{Q}$. Además*

1. *Cada elemento de $\mathbb{Q}_p$ es el límite de alguna sucesión de Cauchy de elementos de $\mathbb{Q}$. Por tanto, la imagen de $\mathbb{Q}$ en $\mathbb{Q}_p$ es densa en $\mathbb{Q}_p$.*

2. *$\mathbb{Q}_p$ es completo con respecto al valor absoluto $|\ |_p$.*

Dem:

1. De la definición 2.2.6 se deduce que cada elemento $x = (x_n) + \mathcal{N} \in \mathbb{Q}_p$ es el límite de una sucesión de Cauchy (x_n) de elementos de $\mathbb{Q}$ ya que

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

2. Sea (x_n) una sucesión de Cauchy de elementos en $\mathbb{Q}_p$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, para cada x_n existe $y^{(n)} \in \mathbb{Q}$ tal que $\lim_{n\to\infty} |x_n - (y^{(n)})|_p = 0$.

   Se comprueba ahora que la sucesión $(y^{(k)})_k$ es una sucesión de Cauchy de elementos de $\mathbb{Q}$. Si $\lambda = (y^{(k)}) + \mathcal{N}$, se cumple que $\lim_{n\to\infty}(x_n) = \lambda$.

Definición 2.2.7 *Si K es un cuerpo valuado con un valor absoluto $|\ |$, el conjunto $V_K = \{|a| : a \in K^*\}$ es un subgrupo del grupo multiplicativo de los reales positivos y se llama grupo de valores de K.*

Corolario 2.2.1 *El grupo de valores de $|\ |_p$ en $\mathbb{Q}_p$ coincide con el de $|\ |_p$ en $\mathbb{Q}$.*

Dem: Sean V_1, V_2, respectivamente, los grupos de valores de $\mathbb{Q}$ y $\mathbb{Q}_p$ respecto del valor absoluto p-ádico. Es obvio que $V_1 \subseteq V_2$.

Por otro lado, si $0 \neq \lambda \in \mathbb{Q}_p$, $\lambda = lim_n(x_n)$ siendo (x_n) una sucesión de Cauchy de elementos de $\mathbb{Q}$.

Para cada $\epsilon > 0$ existe entonces un entero N tal que $|\lambda - x_n| < \epsilon\ \forall n > N$. Eligiendo ϵ tal que $0 < \epsilon < |\lambda|_p$, resulta que, para cada $n > N$,

$$|x_n|_p = |x_n - \lambda + \lambda|_p = \text{máx}\{|x_n - \lambda|_p, |\lambda|_p\} = |\lambda|_p$$

Por tanto, $V_2 \subseteq V_1$ y $V_1 = V_2$.

Ahora vamos a analizar la estructura de $\mathbb{Q}_p$.

2.3. Los enteros p-ádicos

Proposición 2.3.1 a) *El subconjunto de $\mathbb{Q}_p$, $\mathbb{Z}_p = \{\lambda \in \mathbb{Q}_p / |\lambda|_p \leq 1\}$ es un subanillo de $\mathbb{Q}_p$ llamado anillo de los enteros p-ádicos. Además, $P_p = \{\lambda \in \mathbb{Q}_p / |\lambda|_p < 1\}$ es el único ideal maximal de $\mathbb{Z}_p$.*

b) $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} : p \text{ no divide a } b\}$ *es un subanillo de* $\mathbb{Q}$ *y*

$$P_{(p)} = P_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} : p/a \text{ y } p \text{ no divide a } b\}$$

es su único ideal maximal.

c) *Los cuerpos* $\mathbb{Z}_p/P_p$ *y* $\mathbb{Z}_{(p)}/P_{(p)}$*, que reciben el nombre de cuerpo residual de* $\mathbb{Q}_p$ *y* $\mathbb{Q}$ *respectivamente, son ambos isomorfos a* $\mathbb{Z}/p\mathbb{Z}$*.*

Dem:

a) Es claro que $\mathbb{Z}_p$ es un subanillo de $\mathbb{Q}_p$ y que P_p es un ideal de $\mathbb{Z}_p$. Para probar que P_p es maximal basta observar que para cada $\lambda \in \mathbb{Q}_p \backslash P_p$, se cumple que $|\lambda|_p = 1$. Por tanto, $\lambda^{-1} \in \mathbb{Z}_p$ y λ es unidad en $\mathbb{Z}_p$. Esto prueba también que P_p es el único ideal maximal de $\mathbb{Z}_p$.

b) Es claro que $\mathbb{Z}_{(p)}$ es subanillo de $\mathbb{Q}$ y que $P_{(p)}$ es un ideal de $\mathbb{Z}_{(p)}$.

Se comprueba, como en a), que cada elemento de $\mathbb{Z}_{(p)} \backslash P_{(p)}$ es unidad en $\mathbb{Z}_{(p)}$ por lo que $P_{(p)}$ es el único ideal maximal de $\mathbb{Z}_{(p)}$.

c) En primer lugar se observa que la inclusión $\sigma : \mathbb{Z}_{(p)} \to \mathbb{Z}_p$ es un homomorfismo de anillos tal que $\sigma(P_{(p)}) \subseteq P_p$. Induce por tanto, un homomorfismo

$$\begin{array}{rcl} \sigma_1 : \mathbb{Z}_{(p)}/P_{(p)} & \to & \mathbb{Z}_p/P_p \\ \frac{a}{b} + P_{(p)} & \mapsto & \frac{a}{b} + P_p \end{array}$$

que es además monomorfismo. Por tanto, $\mathbb{Z}_{(p)}/P_{(p)}$ es isomorfo a un subcuerpo de $\mathbb{Z}_p/P_p$.

Por otro lado, si $\lambda \in \mathbb{Z}_p$, $\lambda = \lim_n(a_n)$ donde (a_n) es una sucesión de Cauchy de elementos de $\mathbb{Q}$ y existe un entero N tal que $\forall n > N$ se tiene que $|\lambda - a_n|_p < 1$. Para cualquiera de estos n se cumple que

$$|a_n|_p = |a_n - \lambda + \lambda|_p \leq \text{máx}\{|a_n - \lambda|_p, |\lambda|_p\} \leq 1$$

Por tanto $a_n \in \mathbb{Z}_{(p)}$ y $a_n - \lambda \in P_p$. Entonces $\lambda + P_p = a_n + P_p = \sigma(a_n + P_{(p)})$, σ_1 es también suprayectivo y es un isomorfismo.

Basta probar ahora que $\mathbb{Z}_{(p)}/P_{(p)}$ es isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Se considera para ello la aplicación

$$\begin{array}{rcl} \varphi : \mathbb{Z}_{(p)} & \to & \mathbb{Z}/p\mathbb{Z} \\ \frac{a}{b} & \mapsto & [a][b]^{-1} \end{array}$$

donde $[a]$ representa la clase del entero a en $\mathbb{Z}/p\mathbb{Z}$.

Se comprueba directamente que φ está bien definida y es homomorfismo. Es también suprayectivo ya que $[a] = \varphi(\frac{a}{1})$. Además

$$Ker\ \varphi = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} / a \equiv 0 \text{ mód } p \right\} = P_{(p)}$$

Por tanto, $\mathbb{Z}_{(p)}/P_{(p)} \approx \mathbb{Z}/p\mathbb{Z}$.

Proposición 2.3.2 *Para cada entero p-ádico $x \in \mathbb{Z}_p$ y cada entero positivo n existe un único número entero x_n tal que $0 \leq x_n \leq p^n - 1$ y $|x - x_n|_p \leq p^{-n}$.*

La sucesión de enteros (x_n) es una sucesión de elementos de $\mathbb{Z}$ tales que

- $x_n \in \mathbb{Z}$ *con* $0 \leq x_n \leq p^n - 1$
- $x_n \equiv x_{n-1} \text{ mód } p^{n-1}$

que es de Cauchy y converge a x.

Dem: Veamos primero que dado $x \in \mathbb{Z}_p$ y $n \geq 1$ existe un único entero $x_n \in \mathbb{Z}$ con $0 \leq x_n \leq p^n - 1$ y tal que $|x - x_n|_p \leq p^{n-1}$.

Sea $x \in \mathbb{Z}_p$ y $n \geq 1$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, se puede encontrar $\frac{a}{b} \in \mathbb{Q}$ suficientemente cerca de x tal que

$$|x - \frac{a}{b}|_p \leq p^{-n} < 1$$

Como tenemos que

$$|\frac{a}{b}|_p \leq max \left\{ |x|_p, |x - \frac{a}{b}|_p \right\} \leq 1$$

se cumple que $\frac{a}{b} \in \mathbb{Z}_{(p)}$, es decir que p no divide b. Entonces, $m.c.d(b, p^n) = 1$ y existen $b', c \in \mathbb{Z}$ tales que $1 = bb' + p^n c$.

Por tanto, $\frac{a}{b} = ab' + \frac{ac}{b}p^n$ y

$$\left| \frac{a}{b} - ab' \right|_p \leq p^{-n}$$

con $ab' \in \mathbb{Z}$. Tomando ahora x_n como el único entero tal que $0 \leq x_n \leq p^{n-1}$ y $x_n \equiv ab' \text{ mód } p^n$, se cumple que

$$\left| \frac{a}{b} - x_n \right|_p \leq p^{-n}$$

y entonces

$$|x - x_n|_p \leq \text{máx}\{\Big|x - \frac{a}{b}\Big|_p, \Big|\frac{a}{b} - x_n\Big|_p\} \leq p^{-n}$$

Probamos ahora la unicidad de x_n: si z es un entero tal que $0 \leq z \leq p^n - 1$ y $|x - x_n|_p \leq p^{-n}$, se cumple que

$$|x_n - z|_p \leq \text{máx}\{|x - x_n|_p, |x_n - z|_p\} \leq p^{-n}$$

Por tanto $x_n \equiv z$ mód p^n y como $0 \leq x_n, z \leq p^n - 1$, debe ser $x_n = z$.

Para probar la última afirmación sólo queda por comprobar que, para cada $n \geq 1$ se cumple que $x_n \equiv x_{n-1}$ mód p^{n-1}.

Sean x_n, x_{n-1} los enteros tales que

- $0 \leq x_{n-1} \leq p^{n-1} - 1$
- $0 \leq x_n \leq p^n - 1$
- $|x - x_{n-1}|_p \leq p^{-(n-1)}$
- $x - x_n|_p \leq p^{-n}$

Entonces

$$|x_n - x_{n-1}|_p \leq \text{máx}\{|x_n - x|_p, |x - x_{n-1}|\} \leq p^{-(n-1)}$$

y $x_n \equiv x_{n-1}$ mód p^{n-1}.

Probaremos ahora que cada número p-ádico se puede representar como "serie de potencias en p". Comenzamos probándolo para un entero p-ádico.

Proposición 2.3.3 *Dado cualquier $x \in \mathbb{Z}_p$, existe una serie de la forma*

$$b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots + b_n p^n + \cdots$$

con $0 \leq b_i \leq p - 1$ para cada i, que converge a x.

Dem: La Proposición 2.3.2 asegura que existe una sucesión de enteros x_n que converge a x y tal que

- $x_n \equiv x$ mód p^n
- $x_{n+1} \equiv x_n$ mód p^n
- $0 \leq x_n \leq p^n - 1$

Si se utiliza la expresión de cada entero x_n en base p:

$$x_n = b_0 + b_1 p + b_2 p^2 + \cdots + b_{r_n} p^{r_n}$$

la reducción de x_n módulo p^n es sencilla: basta suprimir los sumandos que son multiplo de p^n. De esta forma, la condición

$$x_{n+1} \equiv x_n \text{ mód } p^n$$

simplemente nos indica que los $n-1$ primeros sumandos de ambos números son iguales. Escribiendo de esta forma los elementos de la sucesión se obtiene:

$$\begin{aligned} x_0 &= b_0 && 0 \leq b_0 \leq p-1 \\ x_1 &= b_0 + b_1 p && 0 \leq b_1 \leq p-1 \\ x_2 &= b_0 + b_1 p + b_2 p^2 && 0 \leq b_2 \leq p-1 \end{aligned}$$

En general, para un n cualquiera, $x_n = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n$ con $0 \leq b_i \leq p-1$ para cada $i = 0, \ldots, n$.

Es claro que la serie $b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots$ converge a x ya que sus sumas parciales, que son los x_n, convergen a x. Queda así justificada la expresión

$$x = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots + b_n p^n + \cdots$$

Corolario 2.3.1 *Todo $x \in \mathbb{Z}_p$ puede ser escrito de la forma siguiente:*

$$x = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots + b_n p^n + \cdots$$

con $0 \leq b_i \leq p-1$. Además su representación es única.

Dem: Sabemos por Proposición 2.3.2 que los x_n son únicos y por tanto los b_n también lo son por ser los dígitos de cada x_n en base p.

Ejemplo 2.3.1

- *Para $2804 \in \mathbb{Z}_5$ se tiene que*

$$2804 = 4 + 2 * 5^2 + 2 * 5^3 + 4 * 5^4$$

- *Para $-1 \in \mathbb{Z}_p$, se tiene que*

$$-1 = \textstyle\sum_{i=0}^{\infty} b_i p^i \text{ con } b_i = p-1 \forall i$$

es decir,

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + ... + (p-1)p^n + ...$$

Para demostrarlo vamos a probar que

$$1 + [(p-1) + (p-1)p + (p-1)p^2 + ... + (p-1)p^n + ...] \to 0$$

En efecto,

$$\boxed{1 + (p-1)} + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^n + \cdots$$

$$= \boxed{p + (p-1)p} + (p-1)p^2 + \cdots + (p-1)p^n + \cdots$$

$$= \boxed{p^2 + (p-1)p^2} + \cdots + (p-1)p^n + \cdots$$

$$= p^3 + \cdots + (p-1)p^n + \cdots \to 0$$

- *Para* $-7 \in \mathbb{Z}_5$

$$\begin{aligned} -7 &= -2 - 5 = 3 + 5(-2) = 3 + 3 \cdot 5 - 5^2 = 3 + 3 \cdot 5 + 4 \cdot 5^2 - 5^3 = \\ &= 3 + 3 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 - 5^4 = \cdots = \\ &= 3 + 3 \cdot 5 + 4(5^2 + 5^3 + 5^4 + \cdots) = \\ &= 18 + 4 \cdot 25(1 + 5 + 5^2 + \cdots) = 18 + 4 \cdot 25 \frac{1}{1-5} \end{aligned}$$

- $\frac{1}{21} \in \mathbb{Z}_5$

  En primer lugar $21 = 4 \cdot 5 + 1 \Rightarrow 1 = 21 - 4 \cdot 5$ *y* $\frac{1}{21} = 1 - \frac{4}{21}5$

$$\begin{aligned} \frac{1}{21} &= 1 - \frac{4}{21}5 = 1 - 4(1 - 4 \cdot 5\frac{1}{21})5 = 1 - 4 \cdot 5 + \frac{16}{21}5^2 = \\ &= 1 + 5 + (\frac{16}{21} - 1) \cdot 5^2 = \boxed{1 + 5 - \frac{1}{21}5^3} = \\ &= 1 + 5 - 5^3(1 - 4 \cdot 5\frac{1}{21}) = 1 + 5 - 5^3 + 5^4\frac{4}{21} = \\ &= 1 + 5 + 4 \cdot 5^3 + 5^4(\frac{4}{21} - 1) = \boxed{1 + 5 + 4 \cdot 5^3 - \frac{17}{21}5^4} = \end{aligned}$$

$$
\begin{aligned}
&= 1+5+4\cdot 5^3-\frac{3\cdot 5+2}{21}5^4 = 1+5+4\cdot 5^3-\frac{2}{21}5^4-\frac{3}{21}5^5 = \\
&= 1+5+4\cdot 5^3-2(1-4\cdot 5\frac{1}{21})5^4-\frac{3}{21}5^5 = \\
&= 1+5+4\cdot 5^3+3\cdot 5^4+(\frac{8}{21}-1)5^5-\frac{3}{21}5^5 = \\
&= \boxed{1+5+4\cdot 5^3+3\cdot 5^4-\frac{16}{21}5^5} = 1+5+4\cdot 5^3+3\cdot 5^4-\frac{3\cdot 5+1}{21}5^5 = \\
&= 1+5+4\cdot 5^3+3\cdot 5^4-5^5(1-\frac{4\cdot 5}{21})-\frac{3}{21}5^6 = \\
&= \boxed{1+5+4\cdot 5^3+3\cdot 5^4+4\cdot 5^5-\frac{4}{21}5^7} = \\
&= 1+5+4\cdot 5^3+3\cdot 5^4+4\cdot 5^5-4(1-\frac{4}{21}5)5^7 = \\
&= 1+5+4\cdot 5^3+3\cdot 5^4+4\cdot 5^5+5^7+(\frac{16}{21}-1)5^8 = \\
&= \boxed{1+5+4\cdot 5^3+3\cdot 5^4+4\cdot 5^5+5^7-\frac{1}{21}5^9} = \cdots
\end{aligned}
$$

y comienza un nuevo ciclo: $(1,[1,0,4,3,4,0],[1,0,4,3,4,0],\ldots)$

Para extender esta representación a todo $\mathbb{Q}_p$, observemos que para cada $x\in\mathbb{Q}_p$, existe un entero m tal que $|p^m x|\leq 1$. Por tanto, x se puede escribir como $\frac{y}{p^m}$ con $y\in\mathbb{Z}_p$. Si expresamos y como serie de potencias en p y dividimos entre p^m, obtendremos una serie de potencias en p que podría comenzar con una potencia negativa de p y converge a x.

Corolario 2.3.2 *Si $x\in\mathbb{Q}_p\backslash\mathbb{Z}_p$, $|x|_p=p^{n_0}$ con $n_0>0$ y x puede ser escrito del modo siguiente:*

$$x=\sum_{n=-n_0}^{\infty}b_n p^n$$

con $0\leq b_n\leq p-1$. Además esta representación es única.

Dem: Basta observar que $|p^{n_0}x|=1$ y por Proposición 2.3.3, es

$$p^{n_0}x=b_0+b_1x+\cdots+b_np^n+\cdots$$

con lo cual $x=\sum_{-n_0}^{\infty}b_np^{n-n_0}$.

Una vez probado que cada número p-ádico se expresa de forma única como serie de potencias de p, el siguiente resultado permite reconocer a los números racionales entre los p-ádicos a partir de estas expansiones. El resultado es similar a la caracterización de los racionales entre los reales a partir de su expresión decimal.

Proposición 2.3.4 *Sea $x = \sum_n a_n p^n \in \mathbb{Q}_p$ ($n \geq v(x)$, $0 \leq a_n \leq p-1$). Entonces, x es un racional si y sólo si la sucesión $\{a_n\}$ es periódica a partir de algún n (eventualmente periódica).*

Dem: Multiplicando x por una potencia adecuada de p, se obtiene $x \in \mathbb{Z}_p$ y, probado para este caso, es inmediato el caso general.

Veamos primero que si (a_n) es eventualmente periódica entonces x es racional. Sea $x = \sum_{n\geq 0} a_n p^n$. Si la suma es finita, x es un entero positivo. Si (a_n) es eventualmente periódica, existen enteros positivos r, t tales que

$$x = a_0 + \cdots + a_r p^r + (a_{r+1}p^{r+1} + \cdots + a_{r+t}p^{r+t}) + (a_r p^{r+t+1} + \cdots + a_{r+t}p^{r+2t}) + \cdots = n + y$$

donde $n = a_0 + \cdots + a_r p^r$ es un entero positivo y

$$\begin{aligned} y &= \sum_{k=0}^{\infty} (a_r p^{r+kt+1} + \cdots + a_{r+t} p^{r+(k+1)t}) = \\ &= a_r \sum_{k=0}^{\infty} p^{r+kt+1} + a_{r+1} \sum_{k=0}^{\infty} p^{r+kt+2} + \cdots + a_{r+t} \sum_{k=0}^{\infty} a_{r+t} p^{r+(k+1)t} = \\ &= a_r p^{r+1} \frac{1}{1-p^t} + a_{r+1} p^{r+2} \frac{1}{1-p^t} + \cdots + a_{r+t} p^{r+t} \frac{1}{1-p^t} \end{aligned}$$

Por tanto, $x = n + y \in \mathbb{Q}$.

Vamos a probar ahora la otra implicación, es decir que si x es racional entonces (a_n) es eventualmente periódica Sea $x \in \mathbb{Z}_p$ y $x = \frac{a}{b} \in \mathbb{Q}$ con $a, b \in \mathbb{Z}$ y $(a, b) = 1$. Existe un entero positivo m tal que $x + m$ es positivo. Como el desarrollo de m en serie de potencias de p es una suma finita, bastará probar que el desarrollo de $x + m$ en serie de potencia es eventualmente periódica.

Suponemos por tanto que $x \in \mathbb{Z}_p$ y $x = \frac{a}{b} \in \mathbb{Q}$ con a, b enteros positivos y $(a, b) = 1$. Entonces será $(b, p) = 1$ y la expansión de x es de la forma $x = \sum_{i\geq 0} c_i p^i$.

Las expansiones p-ádicas de a y b serán de la forma $a = \sum_{j=0}^{n} a_j p^j$, $b = \sum_{k=0}^{m} b_k p^k$ con $b_0 \neq 0$ y se cumple que

$$bx = a \Rightarrow \left(\sum_{k=0}^{m} b_k p^k\right)\left(\sum_{i\geq 0} c_i p^i\right) = a = \sum_{j=0}^{n} a_j p^j$$

Para cada $l \geq 0$, el coeficiente de p^l en la parte izquierda es

$$t_l = b_0 c_l + b_1 c_{l-1} + \cdots + b_m c_{l-m} + r_l$$

donde r_l es la llevada acumulada de la suma que le precede, y se debe cumplir que $t_l = a_l + r_{l+1}p$. Cuando $l > n$, se obtiene

$$t_l = b_0 c_l + b_1 c_{l-1} + \cdots + b_m c_{l-m} + r_l = r_{l+1}p$$

Estas ecuaciones permiten ir calculando los c_i como sigue:

De la ecuación $t_0 = b_0 c_0 = a_0 + r_0 p$ se calcula c_0 a partir de a_0, b_0 resolviendo primero la ecuación $b_0 c_0 \equiv a_0$ mód p, obteniendo así t_0 y $r_0 = \frac{t_0}{p}$. A continuación se considera la ecuación $t_1 = b_1 c_0 + b_0 c_1 = a_1 + r_1 p$ donde se conocen b_0, b_1, a_1, c_0 y se calcula c_1 a partir de $b_0 c_1 \equiv a_1 - b_1 c_0$ mód p. Luego se calcula t_1 y $r_1 = \frac{t_1}{p}$.

Así, para un $l > n$,

$$\begin{aligned} t_l &= b_0 c_l + b_1 c_{l-1} + \cdots + b_m c_{l-m} + r_l = r_{l+1}p \\ t_{l+1} &= b_0 c_{l+1} + b_1 c_l + \cdots + b_m c_{l+1-m} + r_{l+1} = r_{l+2}p \\ \cdots &\quad \cdots \end{aligned}$$

En la primera ecuación son conocidos $c_0, \ldots, c_{l-1}, r_l$ y se calcula c_l módulo p a partir de la ecuación $b_0 c_l \equiv -(b_1 c_{l-1} + \cdots + b_m c_{l-m} + r_l)$. Después se calcula t_l y $r_{l+1} = \frac{t_l}{p}$.

Es decir, se obtiene c_l mód p a partir $c_{l-1}, \ldots c_{l-m}, r_l$, se calcula luego t_l y al dividir éste por p, se obtiene la "llevada" r_{l+1}.

En la siguiente ecuación se calculará c_{l+1} mód p a partir de $c_l, \ldots, c_{l+1-m}, r_{l+1}$ y, a partir de éste se obtendrá t_{l+1} y $r_{l+2} = \frac{t_{l+1}}{p}$.

En otras palabras, para cada $l > n$, hay un algoritmo que, a partir de los datos $(c_{l-1}, \ldots, c_{l-m}, r_l) \in (\mathbb{Z}/p\mathbb{Z})^{m+1}$ y los valores fijos $b_0, \ldots, b_m$, permite obtener $(c_l, c_{l-1}, \ldots, c_{l-m+1}, r_{l+1}) \in (\mathbb{Z}/p\mathbb{Z})^{m+1}$. Como $(\mathbb{Z}/p\mathbb{Z})^{m+1}$ es finito, en algún momento aparece una lista $(c_{l-1}, \ldots, c_{l-m}, r_l)$ repetida (ver el desarrollo de 1/21 en el Ejemplo 2.3.1)

Corolario 2.3.3 *Los enteros p-ádicos* $\sum p^{n^2}$ *y* $\sum p^{n!}$ *no son racionales.*

Dem: Para $n > 0$, $(n+1)^2 - n^2 = 2n + 1$. Por tanto, esta expansión tiene entre cada dos unos un número distinto de ceros cada vez:

$$1 + p + p^4 + p^9 + p^{16} + \cdots = 11001000010000001$$

y no es periódica.

Para la otra expansión, se cumple que $(n+1)! - n! = n!n$ lo que significa que entre el 1 correspondiente a $p^{n!}$ y el de $p^{(n+1)!}$ hay $n!n - 1$ ceros, luego la expansión no es periódica.

$$1 + p + p^2 + p^6 + p^{24} + p^{120} + \ldots = 111000100\ldots$$

Las expresiones obtenidas para los números p-ádicos nos permiten manejar fácilmente situaciones como la que muestra el ejemplo siguiente.

Ejemplo 2.3.2 *Resolver las congruencias* $x^2 \equiv 2 \pmod{7^n}$ *con* $n = 1, 2, \ldots$.

Entonces $x^2 \equiv 2 \pmod 7$ *y debe ser* $x \equiv 3, 4 \pmod 7$.

Para $n = 1$, *las soluciones son* $x = 3$ *y* $x = 4$.

Para $n = 2$, *consideramos los* x *de la forma* $x = 3 + 7k$ *y* $x = 4 + 7k$ *ya que, para cada* n, *una solución módulo* 7^n *debe ser siempre una solución módulo* 7^{n-1}.

De $(3 + 7k)^2 \equiv 2 \pmod{7^2}$ *resulta que*

$$9 + 42k \equiv 2 \pmod{7^2} \qquad y \qquad 7 + 42k \equiv 0 \pmod{7^2}$$

Por tanto tenemos que $1+6k \equiv 0 \pmod 7$ *y* $k \equiv 1 \pmod 7$. *Luego las soluciones de* $x^2 \equiv 2 \pmod{7^2}$ *tales que* $x \equiv 3 \pmod 7$ *son las de la forma*

$$x = 3 + 7(7r + 1) = 10 + 7^2 r$$

es decir los enteros positivos x *tales que* $x \equiv 10 \pmod{7^2}$.

De igual forma, las soluciones de $x^2 \equiv 2 \pmod{7^2}$ *tales que* $x \equiv 4 \pmod 7$ *son las de la forma*

$$x = 4 + 7(7r + 5) = 39 + 7^2 r$$

es decir los enteros positivos x *tales que* $x \equiv 39 \equiv -10 \pmod{7^2}$.

Una vez encontrada una solución de la ecuación $x^2 \equiv 2 \pmod{7^n}$ *siempre existe una única solución de la ecuación* $x^2 \equiv 2 \pmod{7^{n+1}}$ *y, por tanto, el proceso continua indefinidamente: en efecto, si* $a_n^2 \equiv 2 \pmod{7^n}$ *se cumple que*

$7^n/(a_n^2-2)$. *Escribiendo* $a_n^2-2=7^n r$ *y tomando* $a_{n+1}=a_n+7^n k$ *resulta que*

$$\begin{aligned} a_{n+1}^2-2 &= (a_n+7^n k)^2-2=(a_n^2-2)+2\cdot 7^n a_n k+7^{2n}k^2= \\ &= 7^n r+2\cdot 7^n a_n k+7^{2n}k^2\equiv 7^n(r+2a_n k) \text{ mód } 7^{2n} \end{aligned}$$

Basta por tanto, que exista k *tal que* $r+2a_n k\equiv 0 \text{ mód } 7$ *pero esto es cierto porque al ser* $a_n\neq 0$ *es* $(a_n,7)=1$ *y entonces la ecuación anterior tiene solución única en* $\mathbb{Z}_7$.

Observemos que la expansión 7-ádica de las soluciones que se van obteniendo para el caso $x\equiv 3 \text{ mód } 7$*:* $x=(3,10,108,2166,\ldots)$ *es*

$$3,\ 3+7,\ 3+7+2\cdot 7^2,\ 3+7+2\cdot 7^2+6\cdot 7^3,\ldots$$

y la de las obtenidas para el caso $x\equiv 4 \text{ mód } 7$*:* $x=(4,39,235,235,)=(-3,-10,-108,-2166,\ldots)$ *es*

$$4,\ 4+5\cdot 7,\ 4+5\cdot 7+4\cdot 7^2,\ 4+5\cdot 7+4\cdot 7^2+0\cdot 7^3,\ldots$$

Se observa que corresponden, respectivamente a los dos números p-ádicos siguientes

$$x_1=3+7+2\cdot 7^2+6\cdot 7^3+\cdots$$

$$x_2=4+5\cdot 7+4\cdot 7^2+0\cdot 7^3+\cdots=-x_1$$

Hemos encontrado así las dos soluciones de la ecuación $x^2=2$ *en el cuerpo* $\mathbb{Q}_7$ *de los números 7-ádicos.*

2.4. El lema de Hensel

Gracias a toda la teoría vista hasta aquí, tenemos suficientes herramientas matemáticas para poder abordar el lema de Hensel. Este lema es probablemente la propiedad algebraica más importante de los números p-ádicos. En él se relacionan las raíces de un polinomio con su solución módulo un primo p.

Tanto el lema como su demostración se basan en procedimientos iterativos que devuelven una solución aceptable si se escoge un punto inicial adecuado.

De hecho, el lema de Hensel es similar al método de Newton. Recordemos que el método de Newton permite encontrar raíces reales de un polinomio a partir de un punto inicial, haciendo aproximaciones basadas en la derivada

del polinomio en dicho punto. Para ello, es necesario que la derivada en este punto sea distinta de cero.

El Lema de Hensel se basa en aplicar a un polinomio $f(x) \in \mathbb{Z}_p[x]$ que posea una raíz $a_0 \in \mathbb{Z}/p\mathbb{Z}$, una iteración que va calculando raíces de dicho polinomio módulo $p, p^2, p^3...$ hasta probar la existencia de una raíz de $f(x)$ en $\mathbb{Z}_p$. Para esta iteración, es condición necesaria que $f'(a_0) \not\equiv 0$ mód p.

El siguiente resultado sirve de base para esta iteración:

Lema 2.4.1 *Si A es un anillo y $f(x) \in A[x]$ un polinomio, existen polinomios $f_1(x,y), f_2(x,y) \in A[x,y]$ tales que*

$$f(x+h) = f(x) + hf_1(x,h) = f(x) + hf'(x) + h^2 f_2(x,h)$$

Dem: Sea $f(x) = \sum_{i=0}^{n} a_i x^i$. Entonces

$$\begin{aligned} f(x+h) &= \sum_i a_i (x+h)^i = \sum_i a_i (x^i + i x^{i-1} h + h^2(\ldots)) = \\ &= \sum_i a_i x^i + h \sum_i i a_i x^{i-1} + h^2 f_2(x,h) \end{aligned}$$

Proposición 2.4.1 *(Lema de Hensel (forma fuerte)) Sea p un primo y $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ un polinomio en $\mathbb{Z}_p[x]$. Si existe un entero p-ádico $\alpha_1 \in \mathbb{Z}_p$ tal que*

$$f(\alpha_1) \equiv 0 \text{ mód } p\mathbb{Z}_p \quad y \quad f'(\alpha_1) \neq 0 \text{ mód } p\mathbb{Z}_p$$

existe un único entero p-ádico $\alpha \in \mathbb{Z}_p$ tal que $\alpha \equiv \alpha_1$ mód $p\mathbb{Z}_p$, $|f'(\alpha)|_p = 1$ y $f(\alpha) = 0$.

Dem: Sea $f(x) \in \mathbb{Z}_p[x]$ y $\alpha_1 \in \mathbb{Z}_p$ tal que $f(\alpha_1) \equiv 0$ mód p. Para demostrar que la raíz α existe, construiremos una sucesión de Cauchy de enteros p-ádicos (α_n) tales que, para cada n, es $\alpha_n \equiv \alpha_{n-1}$ mód p^{n-1}, $|f(\alpha_n)| \leq p^{-n}$ y $\lim_n(\alpha_n) = \alpha$.

En primer lugar, buscamos $\alpha_2 \in \mathbb{Z}_p$ tal que $\alpha_2 \equiv \alpha_1$ mód p y $f(\alpha_2) \equiv 0$ mód p^2, para lo cual se escribe $\alpha_2 = \alpha_1 + pt_1$ con t_1 a determinar.

Por el Lema 2.4.1 es

$$f(\alpha_2) = f(\alpha_1 + pt_1) = f(\alpha_1) + pt_1 f'(\alpha_1) + (pt_1)^2 f_2(\alpha_1, h)$$

y entonces

$$f(\alpha_2) \equiv 0 \text{ mód } p^2 \Leftrightarrow f(\alpha_1) + pt_1 f'(\alpha_1) \equiv 0 \text{ mód } p^2$$

Como $f(\alpha_1) \equiv 0$ mód p, existe $r_0 \in \mathbb{Z}_p$ tal que $f(\alpha_1) = pr_1$ y

$$f(\alpha_1) + pt_1 f'(\alpha_1) = pr_1 + pt_1 f'(\alpha_1) \equiv 0 \text{ mód } p^2 \Leftrightarrow r_1 + t_1 f'(\alpha_1) \equiv 0 \text{ mód } p$$

Si $f'(\alpha_1) \not\equiv 0$ mód p, basta tomar ahora $t_1 \equiv \frac{-r_1}{f'(\alpha_1)}$ mód p y este valor t_1 es único si se elige de forma que $0 \leq t_1 < p$.

Resulta entonces que

$$\alpha_2 = \alpha_1 + pt_1 = \alpha_1 - \frac{r_1 p}{f'(\alpha_1)} = \alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)}$$

expresión idéntica a la utilizada en el método de Newton.

Además, $f'(\alpha_2) \not\equiv 0$ mód p ya que

$$f'(\alpha_2) = f'(\alpha_1 + (\alpha_2 - \alpha_1)) = f'(\alpha_1) + (\alpha_2 - \alpha_1)d \text{ con } d \in \mathbb{Z}_p$$

De igual forma, para cualquier $n \geq 1$, se puede obtener α_n a partir de un α_{n-1} tal que $f(\alpha_{n-1}) \equiv 0$ mód p^{n-1} y $f'(\alpha_{n-1}) \not\equiv 0$ mód p. Para ello se supone $\alpha_n = \alpha_{n-1} + p^{n-1}t_{n-1}$ con t_{n-1} a determinar. Entonces

$$\begin{aligned} f(\alpha_n) &= f(\alpha_{n-1} + p^{n-1}t_{n-1}) = f(\alpha_{n-1}) + p^{n-1}t_{n-1}f'(\alpha_{n-1}) + \\ &\quad + (p^{n-1}t_{n-1})^2 f_2(\alpha_{n-1}, h) \end{aligned}$$

y

$$f(\alpha_n) \equiv 0 \text{ mód } p^n \Leftrightarrow f(\alpha_{n-1}) + p^{n-1}t_{n-1}f'(\alpha_{n-1}) \equiv 0 \text{ mód } p^n$$

Como $f(\alpha_{n-1}) \equiv 0$ mód p^{n-1}, existe $r_{n-1} \in \mathbb{Z}_p$ tal que $f(\alpha_{n-1}) = p^{n-1}r_{n-1}$ y

$$f(\alpha_{n-1}) + p^{n-1}t_{n-1}f'(\alpha_{n-1}) = p^{n-1}r_{n-1} + p^{n-1}t_{n-1}f'(\alpha_{n-1})$$

de donde

$$f(\alpha_{n-1}) + p^{n-1}t_{n-1}f'(\alpha_{n-1}) \equiv 0 \text{ mód } p^n \Leftrightarrow r_{n-1} + t_{n-1}f'(\alpha_{n-1}) \equiv 0 \text{ mód } p$$

Puesto que $f'(\alpha_{n-1}) \not\equiv 0$ mód p, basta tomar ahora $t_{n-1} \equiv \frac{-r_{n-1}}{f'(\alpha_{n-1})}$ mód p y este valor t_{n-1} es único si se elige de forma que $0 \leq t_{n-1} < p$.

Es obvio además que

$$|f'(\alpha_n)|_p = |f'(\alpha_{n-1} + p^{n-1}t_{n-1})|_p = |f'(\alpha_{n-1})|_p = 1$$

De este modo se obtiene una sucesión de Cauchy (α_n) de tal forma que, para cada n, $|f(\alpha_n)|_p \leq p^{-n}$ y $|f'(\alpha_n)|_p = 1$. Si $\alpha \in \mathbb{Z}_p$ es el límite de dicha sucesión, por ser $f(x)$ una función continua, se cumple que $f(\alpha) = 0$.

Para probar la unicidad, supongamos ahora la existencia de raíces α, β de $f(x)$ en $\mathbb{Z}_p$ tales que $\alpha \equiv \beta$ mód p y $|f'(\alpha)|_p = |f'(\beta)|_p = 1$. Entonces, $\alpha = \beta + pr$ para algún $r \in \mathbb{Z}_p$ y

$$f(\alpha) = f(\beta + pr) = f(\beta) + prf'(\beta) + (pr)^2 f_2(\beta, pr)$$

Entonces $0 = pr(f'(\beta) + prf_2(\alpha, \beta))$. Como $|f'(\beta)| = 1$ y $|prf_2(\alpha, \beta)| < 1$, resulta que $|f'(\beta) + prf_2(\alpha, \beta)| = 1$. Por tanto, $f'(\beta) + prf_2(\alpha, \beta) \neq 0$, $r = 0$ y $\alpha = \beta$.

Ejemplo 2.4.1 *Se considera el polinomio $f(x) = x^3 - 2$ y el entero $\alpha_1 = 3$. Tenemos que*

$$f(3) = 25 \equiv 0 \text{ mód } 5$$

y además como $f'(x) = 3x^2$, $f'(3) = 27 \equiv 2$ mód 5. Así, por el lema de Hensel sabemos que existe una única raíz cúbica de 2 en $\mathbb{Z}_5$ que es congruente con 3 módulo 5. Esta raíz es $\alpha = 3 + 2 \cdot 5^2 + 2 \cdot 5^3 + 3 \cdot 5^4 + ...$

El resultado siguiente prueba que, también en el caso en que $f'(a_1) \equiv 0$ mód p, se puede obtener una aproximación a_n módulo p^n de la raíz a_1 módulo p y una raíz $\alpha \in \mathbb{Z}_p$ de $f(x)$. Es la conocida como forma débil del Lema de Hensel.

Teorema 2.4.1 *(Lema de Hensel (forma débil)) Sea $f(x) \in \mathbb{Z}_p[x]$ y $\alpha_1 \in \mathbb{Z}_p$ con*

$$|f(\alpha_1)| < |f'(\alpha_1)|^2$$

entonces existe un $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$.

Además, se cumple que

$$|\alpha - \alpha_1| \leq \frac{|f(\alpha_1)|}{|f'(\alpha_1)|}$$

y α es la única raíz de $f(x)$ que satisface la condición anterior.

Como $f'(\alpha_1) \in \mathbb{Z}_p$ entonces $|f'(\alpha_1)|_p \leq 1$ y por tanto, para $|f'(\alpha_1)| = 1$ tenemos las condiciones impuestas en la primera versión del lema de Hensel (Proposición 2.4.1).

Dem: Como $|f(\alpha_1)| < |f'(\alpha_1)|^2$, es $\left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right| < 1$ y entonces existe $\beta_1 \in \mathbb{Z}_p$ tal que $|\beta_1| < 1$ y

$$f(\alpha_1) + \beta_1 f'(\alpha_1) = 0$$

Entonces, por Lema 2.4.1 tenemos que

$$f(\alpha_1 + \beta_1) = f(\alpha_1) + \beta_1 f'(\alpha_1) + \beta_1^2 f_2(\alpha_1, \beta_1) = \beta_1^2 f_2(\alpha_1, \beta_1)$$

y

$$|f(\alpha_1 + \beta_1)| \leq |\beta_1|^2$$

ya que $f_2(\alpha_1, \beta_1) \in \mathbb{Z}_p$. Por tanto,

$$|f(\alpha_1 + \beta_1)| \leq |\beta_1|^2 = \frac{|f(\alpha_1)|^2}{|f'(\alpha_1)|^2} < |f(\alpha_1)|$$

Análogamente, expresando

$$f'(\alpha_1 + \beta_1) = f'(\alpha_1) + \sum_{i \geq 1} \beta_1^i g_i(\alpha_1)$$

resulta que

$$|f'(\alpha_1 + \beta_1) - f'(\alpha_1)| \leq |\beta_1| = \frac{|f(\alpha_1)|}{|f'(\alpha_1)|} < |f'(\alpha_1)|$$

y entonces

$$|f'(\alpha_1 + \beta_1)| = |(f'(\alpha_1 + \beta_1) - f(\alpha_1)) + f(\alpha_1)| = |f'(\alpha_1)|$$

Considerando ahora $\alpha_2 = \alpha_1 + \beta_1$, se cumple $\alpha_2 \in \mathbb{Z}_p$, $|f(\alpha_2)| < |f(\alpha_1)|$ y $|f'(\alpha_2)| = |f'(\alpha_1)|$ con lo que puede repetirse el proceso. De esta manera se obtiene una sucesión

$$\alpha_n = \alpha_{n-1} + \beta_{n-1}$$

tal que $|f'(\alpha_n)| = |f'(\alpha_1)|$ $\forall n$ y

$$|f(\alpha_n)| \leq |\beta_{n-1}|^2 = \frac{|f(\alpha_{n-1})|^2}{|f'(\alpha_{n-1})|^2} < |f(\alpha_{n-1})|$$

Por tanto $f(\alpha_n) \longrightarrow 0$. Además, la sucesión es de Cauchy ya que

$$|\alpha_{n+1} - \alpha_n| = |\beta_n| = \frac{|f(\alpha_n)|}{|f'(\alpha_n)|} = \frac{|f(\alpha_n)|}{|f'(\alpha_1)|} \longrightarrow 0$$

Por tanto, la sucesión α_n tiene límite $\alpha \in \mathbb{Z}_p$ y como $f(x)$ es continua, se cumple que $f(\alpha) = 0$.

Comprobamos ahora que $|\alpha - \alpha_1| \leq \frac{|f(\alpha_1)|}{|f'(\alpha_1)|}$:

Por la contrucción hecha antes es claro que $\alpha - \alpha_1 = \sum_{n\geq 1} \beta_n$, de donde resulta que $|\alpha - \alpha_1| \leq |\beta_1|$ con $\beta_1 = \frac{-f(\alpha_1)}{f'(\alpha_1)}$. Por tanto, $|\alpha - \alpha_1| \leq \frac{|f(\alpha_1)|}{|f'(\alpha_1)|}$.

Supongamos ahora que existe $\alpha^* \neq \alpha$ tal que

$$f(\alpha^*) = 0 \qquad \text{y} \qquad |\alpha^* - \alpha_1| \leq \frac{|f(\alpha_1)|}{|f'(\alpha_1)|}$$

Escribimos $\alpha^* = \alpha + \beta^*$ y entonces

$$|\beta^*| = |\alpha^* - \alpha| \leq \text{máx}\{|\alpha^* - \alpha_1|, |\alpha_1 - \alpha|\} \leq \frac{|f(\alpha_1)|}{|f'(\alpha_1)|} < |f'(\alpha_1)| = |f'(\alpha)| \neq 0$$

Por otro lado,

$$0 = f(\alpha + \beta^*) - f(\alpha) = \beta^* f'(\alpha) + \beta^{*2} f_2(\alpha, \beta^*) = \beta^*(f'(\alpha) + \beta^* f_2(\alpha, \beta^*))$$

Si $\beta^* \neq 0$, debe ser $f'(\alpha) + \beta^* f_2(\alpha, \beta^*) = 0$ pero esto es imposible ya que $|\beta^*| < |f'(\alpha)| \Rightarrow |f'(\alpha) + \beta^* f_2(\alpha, \beta^*)| = |f'(\alpha)|$

El siguiente resultado prueba un recíproco parcial a la Proposición 2.4.1.

Proposición 2.4.2 *Si $f(x) \in \mathbb{Z}_p[x]$ tiene una raíz simple $\alpha \in \mathbb{Z}_p$, existe $r \in \mathbb{N}$ tal que, para cada $n \geq r$ se cumple*

$$\alpha \equiv a \text{ mód } p^n \Rightarrow |f(a)| < |f'(a)|^2$$

Además, α es la única raíz de $f(x)$ en $\mathbb{Q}_p$ tal que $|\alpha - a| \leq \frac{|f(a)|}{|f'(a)|}$.

Dem: Por ser α raíz simple de $f(x)$ se cumple que $f(\alpha) = 0$ y $f'(\alpha) \neq 0$. Como $f'(\alpha) \in \mathbb{Z}_p[x]$ y $\alpha \in \mathbb{Z}_p$ es $0 < |f'(\alpha)| = p^{-t}$ para algún $t \in \mathbb{N}$.

Por otro lado, al ser $\alpha \in \mathbb{Z}_p$, se tiene que para cada n existe $a_n \in \mathbb{Z}$ tal que $\alpha \equiv a_n$ mód p^n. Sea $r = 2t + 1$ y $n \geq r$. Entonces

$$f(a_n) \equiv f(\alpha) = 0 \text{ mód } p^n \Rightarrow |f(a_n)| \leq p^{-n}$$

$$f'(a_n) \equiv f'(\alpha) \text{ mód } p^n \Rightarrow |f'(\alpha) - f(a)| \leq p^{-n} \leq p^{-r} < p^{-t}$$

Con esto y $|f'(\alpha)| = p^{-t}$, resulta que $|f'(a)| = p^{-t}$.

Por tanto, $|f(a)| \leq p^{-n} \leq p^{-r} < p^{-2t} = |f'(a)|^2$.

Una vez que hemos demostrado el lema de Hensel vamos a ver algunas de sus muchas aplicaciones.

2.5. Aplicaciones del lema de Hensel

2.5.1. Determinación y Cálculo de las Unidades de $\mathbb{Z}_p$

Proposición 2.5.1 *Un entero p-ádico a es una unidad de $\mathbb{Z}_p$ si y sólo si $a \not\equiv 0$ mód p.*

Dem: Se considera el polinomio $f(x) = ax - 1$. Es claro que la ecuación $f(x) = 0$ tiene solución en $\mathbb{Z}_p$ si y sólo si a es unidad en $\mathbb{Z}_p$.

Si $a \in \mathbb{Z}_p$ y $a \equiv 0$ mód p, es obvio que $|ax - 1| = 1$ para cada $x \in \mathbb{Z}_p$ y entonces $f(x)$ no tiene solución en $\mathbb{Z}_p$.

Si $a \equiv a_0$ mód p con $a_0 \neq 0$, existe b_0 tal que $a_0 b_0 \equiv 1$ mód p y, como $f'(x) = a$, entonces $|f'(b_0)| = 1$. Luego, el Lema de Hensel asegura que $f(x) = ax-1$ tiene solución única en $\mathbb{Z}_p$. Cuando a es unidad en $\mathbb{Z}_p$, en teoría, el método de Newton aplicado al polinomio $f(x)$ nos permite aproximarla.

Nos encontramos entonces con la siguiente situación

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = a_0 - \frac{aa_0 - 1}{a} = \frac{1}{a}$$

Y ¿qué hacemos ahora si no sabemos dividir y lo que queremos justamente es encontrar el inverso de a? Pues evitar esta división, considerando otro polinomio que nos da directamente el inverso de a: $g(x) = \frac{1}{x} - a$.

Si b_0 es el inverso de a_0 mód p, se cumple que $\frac{1}{b_0} \equiv a_0 \equiv a$ mód p con lo cual $|g(b_0)| < 1$ y $|g'(b_0)| = 1$. En una primera aproximación resulta

$$b_1 = b_0 - \frac{g(b_0)}{g'(b_0)} = b_0 + b_0^2 g(b_0) = b_0 + b_0^2 \left(\frac{1}{b_0} - a\right) = 2b_0 - b_0^2$$

2.5.2. Raíces cuadradas en $\mathbb{Q}_p$

Puesto que cada elemento $\alpha \in \mathbb{Q}_p$ se expresa de una única manera en la forma $p^r \frac{a}{b}$ con $r \in \mathbb{Z}$ y a, b unidades de $\mathbb{Z}_p$, cada cuadrado de $\mathbb{Q}_p$ es de la forma $p^{2r} \frac{a^2}{b^2}$; por tanto, para determinar los cuadrados de los elementos de $\mathbb{Q}_p$ bastará determinar los cuadrados de las unidades de $\mathbb{Z}_p$.

Proposición 2.5.2 *Sea p un primo impar y sea $\beta \in \mathbb{Z}_p$ con $|\beta| = 1$. Entonces, existe $\alpha \in \mathbb{Z}_p$ tal que $\beta = \alpha^2$ si y sólo si existe $a \in F_p^*$ tal que $\beta \equiv a^2$ mód p.*

Dem: Si existe $\alpha \in \mathbb{Z}_p$ tal que $\beta = \alpha^2$ y $\alpha \equiv a$ mód p con $a \in F_p^*$, es obvio que $\beta \equiv a^2$ mód p.

Si para un $a \in F_p^*$ se cumple que $\beta \equiv a^2$ mód p, para el polinomio $f(x) = x^2 - \beta \in \mathbb{Z}_p[x]$ se cumple que $|f(a)| < 1$ y $|f'(a)| = 1$. El lema de Hensel asegura que, en estas condiciones, existe $\alpha \in \mathbb{Z}_p$ tal que $\beta = \alpha^2$.

Si $p = 2$, el método anterior requiere de una mayor precisión ya que, en este caso, es $f'(\alpha) \equiv 0$ mód p. Por ello, este caso se debe considerar aparte.

Proposición 2.5.3 *Si β es una unidad de $\mathbb{Z}_2$ se cumple que $\beta = \alpha^2$ para algún $\alpha \in \mathbb{Z}_2$ si y sólo si $\beta \equiv 1$ mód 8.*

Dem: Si β es unidad de $\mathbb{Z}_2$ y $\beta \equiv 1$ mód 8, $\beta = 1 + 2^3\gamma$ para algún $\gamma \in \mathbb{Z}_2$. Entonces el polinomio $f(x) = x^2 - \beta$ cumple que $|f(1)| = |1 - \beta| \leq 2^{-3}$ y $|f'(1)| = 2^{-1}$. Entonces $|f_1(1)| < |f_1'(1)|^2$ y el Lema de Hensel asegura que $\beta = \alpha^2$ para algun $\alpha \in \mathbb{Z}_2$.

Recíprocamente, si β es unidad y $\beta = \alpha^2$ para algún $\alpha \in \mathbb{Z}_2$, α es también unidad y es de la forma $\alpha = 1 + 2\gamma$ con $\gamma \in \mathbb{Z}_2$. Entonces

$$\beta = \alpha^2 = (1 + 2\gamma)^2 = 1 + 4\gamma + 4\gamma^2 = 1 + 4\gamma(1 + \gamma) \equiv 1 \text{ mód } 8$$

ya que γ o $1 + \gamma \equiv 0$ mód 2.

Estamos ahora en condiciones de describir la estructura de los grupos $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ para cualquier primo p.

Proposición 2.5.4 *Si p es un primo impar, el grupo $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ tiene orden 4 y exponente 2, es decir es isomorfo a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Además, para cualquier $c \in \mathbb{Q}_p$ que sea resto no cuadrático módulo p, los elementos $1, p, c, pc$ forman un sistema completo de representantes para las clases de $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$*

Dem: Es obvio que cada elemento de $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ tiene orden 1 o 2 según que sea o no un cuadrado en $\mathbb{Q}_p^*$. Como en F_p la mitad de los elementos son cuadrados y la otra mitad no, se deduce de Proposición 2.5.2 que $\mathbb{Z}_p^*$ contiene elementos que no son cuadrados; entonces $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ contiene algún elemento de orden 2 y su exponente es 2.

Calculamos ahora las clases de $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$:

i) Si c es cualquier resto no cuadratico de F_p^*, las clases del grupo $F_p^*/(F_p^*)^2$ son F_p^* y cF_p^*.

ii) Si $a \in (\mathbb{Q}_p^*)^2$, debe ser $|a| = p^t$ con t entero par. Por tanto, los elementos p, c, pc no son cuadrados en $\mathbb{Q}_p^*$.

iii) Las clases representadas por $1, p, c, pc$ son distintas: una vez visto que p, c, pc no son cuadrados, basta notar que

$$\begin{aligned} p(\mathbb{Q}_p^*)^2 &= c(\mathbb{Q}_p^*)^2 \Leftrightarrow p^{-1}c \in (\mathbb{Q}_p^*)^2 \\ p(\mathbb{Q}_p^*)^2 &= pc(\mathbb{Q}_p^*)^2 \Leftrightarrow c \in (\mathbb{Q}_p^*)^2 \\ c(\mathbb{Q}_p^*)^2 &= pc(\mathbb{Q}_p^*)^2 \Leftrightarrow p \in (\mathbb{Q}_p^*)^2 \end{aligned}$$

iv) Sea $a \in \mathbb{Q}_p^*$.

Si $|a| = 1$, $a \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$ y $a \equiv a_0$ mód p con $a_0 \in F_p^*$. Se distinguen dos casos:

- Si $a_0 \in F_p^{*2}$, se deduce de la Proposición 2.5.2 que $a \in \mathbb{Z}_p^{*2} \subseteq \mathbb{Q}_p^{*2}$.
- Si $a_0 \in cF_p^{*2}$, $c^{-1}a_0 \in (F_p^*)^2$. Entonces, por la Proposición 2.5.2, resulta que $c^{-1}a \in \mathbb{Z}_p^{*2} \subseteq \mathbb{Q}_p^{*2}$ y $a \in c(\mathbb{Q}_p^*)^2$.

Si $|a| < 1$, existe $r > 0$ tal que $|ap^{-r}| = 1$ y, se deduce del caso anterior, que $ap^{-r} \in \mathbb{Q}_p^{*2}$ o $ap^{-r} \in c\mathbb{Q}_p^{*2}$. Pero

$$\begin{aligned} ap^{-r} \in \mathbb{Q}_p^{*2} &\quad \text{con } r \text{ par} &&\Rightarrow a \in \mathbb{Q}_p^{*2} \\ ap^{-r} \in \mathbb{Q}_p^{*2} &\quad \text{con } r \text{ impar} &&\Rightarrow ap^{-1} \in \mathbb{Q}_p^{*2} \Rightarrow a \in p\mathbb{Q}_p^{*2} \\ ap^{-r} \in c\mathbb{Q}_p^{*2} &\quad \text{con } r \text{ par} &&\Rightarrow a \in c\mathbb{Q}_p^{*2} \\ ap^{-r} \in c\mathbb{Q}_p^{*2} &\quad \text{con } r \text{ impar} &&\Rightarrow ap^{-1} \in c\mathbb{Q}_p^{*2} \Rightarrow a \in cp\mathbb{Q}_p^{*2} \end{aligned}$$

Si $|a| > 1$, es $a\mathbb{Q}_p^{*2} = a^{-1}\mathbb{Q}_p^{*2}$ con $|a^{-1}| < 1$ y se aplica el caso anterior.

En conclusión, $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, p, c, pc\}$ siendo c cualquier resto no cuadrático módulo p.

Corolario 2.5.1 *$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ tiene exponente 2 y orden 8, luego es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $-1, 5, 2$ es un conjunto de generadores.*

Dem: Para probar que el exponente de $\mathbb{Q}_2^{*2} \neq \mathbb{Q}_2^*$ es 2, basta encontrar un elemento de $\mathbb{Q}_2^*$ que no sea cuadrado (por ejemplo el 2 porque $|2| = 2^{-1}$).

Probamos ahora que $|\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}| = 8$. Sea $a \in \mathbb{Q}_2^*$.

- Si $|a| = 1$, $a \equiv 1$ mód 2 y $a \equiv 1, 3, 5, 7$ mód 8.

  Si $a \equiv 1$ mód 8, por la Proposición 2.5.3, $a \in \mathbb{Q}_2^{*2}$.

  Si $a \equiv 3$ mód 8, $3a \equiv 1$ mód 8 y por la Proposición 2.5.3, $3a \in \mathbb{Q}_2^{*2}$. Entonces $-15a \in -5\mathbb{Q}_2^{*2}$ pero, como $-15 \equiv 1$ mód 8, $-15 \in \mathbb{Q}_2^{*2}$ y entonces $a \in -5\mathbb{Q}_2^{*2}$.

  Si $a \equiv 5$ mód 8, $-3a \equiv 1$ mód 8 $\Rightarrow -3a \in \mathbb{Q}_2^{*2} \Rightarrow -15a \in 5\mathbb{Q}_2^{*2}$. Como $-15 \in \mathbb{Q}_2^{*2}$, es $a \in 5\mathbb{Q}_2^{*2}$.

  Si $a \equiv 7$ mód 8, $a \equiv -1$ mód 8 y $-a \in \mathbb{Q}_2^{*2}$. Por tanto, $a \in -\mathbb{Q}_2^{*2}$.

- Si $|a| < 1$, $a \equiv 0$ mód 2 $\Rightarrow a \equiv 0, 2, 4, 6$ mód 8.

  Si $a \equiv 0$ mód 8, $|a| \leq 2^{-3}$ y existe $r \geq 3$ tal que $|a2^{-r}| = 1$.

  Utilizando el caso anterior, se tiene:

$$a2^{-r} \in \mathbb{Q}_2^{*2} \Rightarrow \begin{cases} a \in \mathbb{Q}_2^{*2} & \text{si } r \text{ es par} \\ a \in 2\mathbb{Q}_2^{*2} & \text{si } r \text{ es impar} \end{cases}$$

$$a2^{-r} \in -5\mathbb{Q}_2^{*2} \Rightarrow \begin{cases} a \in -5\mathbb{Q}_2^{*2} & \text{si } r \text{ es par} \\ a \in -10\mathbb{Q}_2^{*2} & \text{si } r \text{ es impar} \end{cases}$$

$$a2^{-r} \in 5\mathbb{Q}_2^{*2} \Rightarrow \begin{cases} a \in 5\mathbb{Q}_2^{*2} & \text{si } r \text{ es par} \\ a \in 10\mathbb{Q}_2^{*2} & \text{si } r \text{ es impar} \end{cases}$$

$$a2^{-r} \in -\mathbb{Q}_2^{*2} \Rightarrow \begin{cases} a \in -\mathbb{Q}_2^{*2} & \text{si } r \text{ es par} \\ a \in -2\mathbb{Q}_2^{*2} & \text{si } r \text{ es impar} \end{cases}$$

  Si $a \equiv 2$ mód 8, es $|a| = 2^{-1}$ y $|a2^{-1}| = 1$. Entonces

$$\begin{aligned} a2^{-1} \in \mathbb{Q}_2^{*2} &\Rightarrow a \in 2\mathbb{Q}_2^{*2} \\ a2^{-1} \in -5\mathbb{Q}_2^{*2} &\Rightarrow a \in -10\mathbb{Q}_2^{*2} \\ a2^{-1} \in 5\mathbb{Q}_2^{*2} &\Rightarrow a \in 10\mathbb{Q}_2^{*2} \\ a2^{-1} \in -\mathbb{Q}_2^{*2} &\Rightarrow a \in -2\mathbb{Q}_2^{*2} \end{aligned}$$

  Si $a \equiv 4$ mód 8, es $|a| = 2^{-2}$ y $|a2^{-2}| = 1$. Entonces

$$\begin{aligned} a2^{-2} \in \mathbb{Q}_2^{*2} &\Rightarrow a \in \mathbb{Q}_2^{*2} \\ a2^{-2} \in -5\mathbb{Q}_2^{*2} &\Rightarrow a \in -5\mathbb{Q}_2^{*2} \\ a2^{-2} \in 5\mathbb{Q}_2^{*2} &\Rightarrow a \in 5\mathbb{Q}_2^{*2} \\ a2^{-2} \in -\mathbb{Q}_2^{*2} &\Rightarrow a \in -\mathbb{Q}_2^{*2} \end{aligned}$$

  Si $a \equiv 6$ mód 8, es $|a2^{-1}| = 1$ como en el caso $a \equiv 2$ mód 8.

- Si $|a| > 1$, $a\mathbb{Q}_2^{*2} = a^{-1}\mathbb{Q}_2^{*2}$ con $|a^{-1}| < 1$.

Por tanto, $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \{1, -1, 2, -2, 5, -5, 10, -10\} =< -1, 2, 5 >$.

Puesto que cada extensión cuadrática de un cuerpo K de característica 0 es de la forma $K(\sqrt{a})$ para algún $a \in K$ libre de cuadrados, se concluye ahora

Corolario 2.5.2 *Las extensiones cuadráticas de $\mathbb{Q}_p$ cuando p es primo impar son*

$$\mathbb{Q}_p(\sqrt{c}), \quad \mathbb{Q}_p(\sqrt{p}), \quad \mathbb{Q}_p(\sqrt{pc})$$

y cuando $p = 2$ son

$$\mathbb{Q}_2(\sqrt{-1}), \quad \mathbb{Q}_2(\sqrt{\pm 2}), \quad \mathbb{Q}_2(\sqrt{\pm 5}), \quad \mathbb{Q}_2(\sqrt{\pm 10})$$

2.5.3. Raíces de la unidad en $\mathbb{Q}_p$

Una interesante aplicación del lema de Hensel es determinar que raíces de la unidad se pueden encontrar en $\mathbb{Q}_p$. Recordemos que, dado un entero $n > 1$, se dice que un elemento ϵ en un cuerpo es una raíz n-ésima de la unidad si $\epsilon^n = 1$. Cuando se trata de elementos en un cuerpo p-ádico $\mathbb{Q}_p$, resulta que, como $\epsilon^n = 1 \Rightarrow |\epsilon| = 1$, toda raíz n-sima de la unidad en $\mathbb{Q}_p$ debe ser una unidad de $\mathbb{Z}_p$.

Proposición 2.5.5 *Para cada primo impar p, el polinomio $f(x) = x^{p-1} - 1$ tiene $p - 1$ raíces distintas en $\mathbb{Z}_p$. Este conjunto de raíces es un subgrupo cíclico de $\mathbb{Z}_p$ de orden $p - 1$ y se representa por E_{p-1}.*

Dem: Para cada $a \in F_p^*$, se cumple que $a^{p-1} = 1$. Por tanto, para el entero a se cumple que $a^{p-1} \equiv 1 \bmod p$ con lo cual, $|a| = 1$, $|f(a)| < 1$ y $|f'(a)| = |(p-1)a^{p-2}| = 1$.

El Lema de Hensel asegura entonces, que para cada $i \in \{1, \ldots, p-1\}$ existe un sólo $\alpha_i \in \mathbb{Z}_p$ tal que $\alpha_i^{p-1} = 1$ y $\alpha_i \equiv i \bmod p$.

El conjunto $E_{p-1} = \{\alpha_1, \ldots, \alpha_{p-1}\}$ es claramente un subgrupo de $\mathbb{Z}_p^*$ de orden $p - 1$ y, por ser un subgrupo finito de $\mathbb{Q}_p^*$, debe ser un grupo cíclico.

Proposición 2.5.6 *Si p es un primo impar las únicas raíces de la unidad en $\mathbb{Q}_p$ son las del conjunto E_{p-1}.*

Las únicas raíces n-simas de la unidad en $\mathbb{Q}_2$ son ± 1.

Dem: Sea E el conjunto formado por todas las raíces n-simas de la unidad existentes en $\mathbb{Q}_p^*$. Entonces E es un grupo multiplicativo contenido en $\mathbb{Z}_p^*$ que contiene a E_{p-1}. Se considera ahora la aplicación $\varphi : E \to F_p^*$ dada por $\alpha \mapsto \alpha \bmod p$. Por la Proposición 2.5.5, φ es epimorfismo ya que cada elemento de F_p^* es la imagen de alguno de $E_{p-1} \subseteq E$.

Probando ahora que φ es inyectiva, se deduce que

$$|E| = |F_p^*| = p - 1 = |E_{p-1}|$$

de donde resulta que $E = E_{p-1}$.

Si $\alpha \in Ker\ \varphi$, es $\varphi(\alpha) = 1$ y entonces debe ser $\alpha = 1 + pt$ para algún $t \in \mathbb{Z}_p$. Además, existe $n \in \mathbb{N}^*$ tal que $n = O(\alpha)$ y

$$1 = \alpha^n = (1 + pt)^n = 1 + npt + \binom{n}{2} p^2 t^2 + \cdots + p^n t^n$$

es decir,

$$0 = npt + \binom{n}{2} p^2 t^2 + \cdots + p^n t^n$$

y

$$0 = t\left(n + \binom{n}{2} pt + \cdots + p^{n-1} t^{n-1}\right)$$

Si $t \neq 0$, debe ser $n + \binom{n}{2} pt + \cdots + p^{n-1} t^{n-1} = 0 \in \mathbb{Z}_p$ con lo cual p/n. En este caso, sea $n = p^r m$ con $r > 0$ y $m \geq 1$ tal que $(p, m) = 1$. Si $\alpha_1 = \alpha^{p^r}$, $O(\alpha_1) = m$ y es claro que α^{p^r} es también de la forma $1 + pt_1$. Repitiendo ahora el proceso anterior se obtiene

$$1 = \alpha_1^m = (1 + pt_1)^m = 1 + mpt_1 + \binom{m}{2} p^2 t_1^2 + \cdots + p^m t_1^m$$

de donde

$$0 = mpt_1 + \binom{m}{2} p^2 t_1^2 + \cdots + p^m t_1^m$$

$$0 = t_1\left(m + \binom{m}{2} p^2 t_1 + \cdots + p^{m-1} t_1^{m-1}\right)$$

Como $(m, p) = 1$, debe ser ahora $t_1 = 0$, con lo cual $1 = \alpha_1 = \alpha^{p^r}$, es decir $O(\alpha) = n = p^r$.

Supongamos ahora que $\beta = \alpha^{p^{r-1}}$. Entonces $\beta^p = 1$ y $\beta \equiv 1 \bmod p$, luego β es de la forma $1 + pt_2$. Resulta que

$$1 = \beta^p = (1 + pt_2)^p = 1 + p^2 t_2 + \binom{p}{2} p^2 t_2^2 + \cdots + p^p t_2^p$$

$$0 = t_2 \left(p + \binom{p}{2} p t_2 + \cdots + p^{p-1} t_2^{p-1} \right)$$

Como $p \geq 3$ es

$$p + \binom{p}{2} p t_2 + \cdots + p^{p-1} t_2^{p-1} = p(1 + \binom{p}{2} t_2 + \cdots + p^{p-2} t_2^{p-1}) \neq 0$$

y resulta de nuevo que $t_2 = 0$, por tanto $\beta = 1 = \alpha^{p^{r-1}}$. Repitiendo el procedimiento se concluye que $\alpha^p = 1$ y $\alpha = 1$. Por tanto, φ es isomorfismo de grupos y $E = E_{p-1}$.

Sea ahora α una raíz de la unidad en $\mathbb{Q}_2$ de orden $n \geq 1$. Entonces $|\alpha| = 1$ y $\alpha = 1 + 2t$ para algún $t \in \mathbb{Z}_2$. De la igualdad

$$1 = (1 + 2t)^n = 1 + n2t + \binom{n}{2} (2t)^2 + \cdots + (2t)^n$$

resulta como antes, que $0 = t \left(n + \binom{n}{2} 2t + \cdots + 2^{n-1} t^{n-1} \right)$.

Si $t \neq 0$, debe ser n par. Si $n = 2^r m$ con m impar, $\beta = \alpha^{2^r}$ tiene orden m y $\beta = 1 + 2t_1$ con $t_1 \in \mathbb{Z}_2^*$.

De $1 = (1 + 2t_1)^m = 1 + 2t_1 m + \binom{m}{2} 4t_1^2 + \cdots + 2^m t_1^m$ resulta que

$$0 = t_1 (m + \binom{m}{2} 2t_1 + \cdots + 2^{m-1} t^{m-1})$$

Como $|m + \binom{m}{2} 2t_1 + \cdots + 2^{m-1} t^{m-1}| = 1$, es $m + \binom{m}{2} 2t_1 + \cdots + 2^{m-1} t^{m-1} \neq 0$ y $t_1 = 0$. Por tanto $\alpha^{2^r} = 1$ y $n = 2^r$.

Como en el caso anterior se prueba que

$$\alpha^{2^r} = 1 \Rightarrow \alpha^{2^{r-1}} = 1 \Rightarrow \ldots \Rightarrow \alpha^2 = 1$$

Entonces

$$1 = \alpha^2 = (1 + 2t)^2 \Rightarrow 0 = t(t + 1) \Rightarrow t = 0 \text{ o } t = 1$$

y resulta que $\alpha = 1$ o $\alpha = -1$.

Comentarios Finales

Para finalizar este trabajo vamos a hacer un breve comentario sobre lo que se conoce como "principio local-global", también conocido como Principio de Hasse.

Una de las consecuencias del lema de Hensel es que, dado un polinomio con coeficientes enteros, no es difícil decidir si tiene o no raíces en $\mathbb{Z}_p$, ya que es suficiente con buscar las raíces módulo p. Pues bien, algo parecido ocurre para $\mathbb{R}$, donde normalmente se puede saber si hay raíces por consideraciones de signo, es decir, si un polinomio tiene signos distintos en x_1 y en x_2 entonces hay una raíz entre esos dos números.

Pero supongamos ahora que queremos buscar raíces en $\mathbb{Q}$. Es claro que si tiene raíces en $\mathbb{Q}$ también las tiene en $\mathbb{Q}_p$ para cada primo p. Por tanto, si para algún primo no hay raíces p-ádicas, entonces tampoco hay raíces racionales.

Esta forma de pensar nos hace llegar a la analogía original de la que hablábamos en la introducción: los cuerpos p-ádicos (y también $\mathbb{R}$) son análogos a los cuerpos de las expansiones de Laurent y corresponden a información local cerca del primo p. El hecho de que las raíces en $\mathbb{Q}$ son automáticamente raíces en $\mathbb{Q}_p$ para todo primo p quiere decir que una raíz global es también raíz local en cada p y en $\mathbb{R}$. Pero es natural plantearse el caso contrario, es decir, saber cuando las raíces locales aseguran la existencia de una solución global.

Un ejemplo sencillo de esta situación que ya hemos expuesto es la propiedad de que un número $x \in \mathbb{Q}$ es cuadrado en $\mathbb{Q}$ si y sólo si es un cuadrado en $\mathbb{Q}_p$ para cada primo p.

El problema es mucho más interesante y complejo en el caso de las ecuaciones polinómicas en general: se dice que una ecuación tiene solución global cuando la tiene en $\mathbb{Q}$ y que tiene solución local en todas partes cuando la tiene en $\mathbb{R}$ y en cada cuerpo p-ádico. Es claro que para que exista solución

global es condición necesaria la existencia de solución local en todas partes. El recíproco es cierto solamente para tipos de ecuaciones muy determinados y constituye además un problema muy complejo y extenso que excede ampliamente el nivel del presente trabajo, por lo que terminamos citando en este sentido el siguiente resultado, fundamental en la Teoría de Números, que fue probado por Minkowski en el caso $K = \mathbb{Q}$ y generalizado por Hasse a un cuerpos de números.

Teorema 2.5.1 *(Teorema de Hasse-Minkowski)*
Una forma cuadrática $q(x_1, \ldots, x_n)$ sobre un cuerpo de números K posee una solución no trivial si y sólo si la posee en cada completado de K.

Bibliografía

[1] Gouvêa Fernando Q. "p-adic Numbers. An introduction". Springer-Verlag (1993).

[2] Cassels, J.W.S. "Local Fields". Cambridge University Press (1986).

[3] Robert, Alain M. "A Course in p-adic Analysis". Springer GTM 198 (2000).

[4] Schikhof W.H. "Ultrametric calculus. An introduction to p-adic analysis". Cambridge University Press (1984)

[5] O'Connor, J.J. y Robertson, E. F. "Kurt Hensel".School of Mathematics and Statistics University of St Andrews, Scotland.[Consulta: 10 octubre 2016]. Disponible en: http://www-history.mcs.st-andrews.ac.uk/Biographies/Hensel.html

[6] "The p-adic completion of ℚand Hensel's lemma". The University os Chicago. [Consulta: 14 noviembre 2016]. Disponible en: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/ REUPapers/Herwig.pdf

[7] Crivelli, F. "Absolute values, valuations and completion". Edición: 21 abril 2008 [Consulta: 15 octubre 2016]. Disponible en: http://www.sam.math.ethz.ch/education/bachelor/seminars/fs2008/algebra/Crivelli.pdf

[8] Oggier, Frédérique. [Consulta: 15 octubre 2016]. Disponible en: http://www1.spms.ntu.edu.sg/ frederique/antchap5.pdf