Trabajo monográfico

Teoría de los Números p-ádicos: Valuaciones, $\mathbb{Q}_p$ y sus Extensiones

Federico Fornesi

Marzo 2025

Orientador:

Gustavo Rama
IMERL-FING

Licenciatura en Matemática
Universidad de la República
Montevideo, Uruguay

Índice general

Introducción

La teoría de los números p-ádicos surge como una extensión natural de los números racionales, la cual proporciona una herramienta poderosa en diversas ramas de la teoría de números. Su origen se remonta a Kurt Hensel, quien a fines del siglo XIX introdujo estos números como una completación de los racionales distinta de los números reales. Estos "nuevos números" han permitido desarrollar enfoques profundos para problemas aritméticos y algebraicos, con aplicaciones que van desde la solubilidad de ecuaciones diofantinas hasta la formulación de conjeturas fundamentales en la teoría de la geometría aritmética.

Uno de los resultados clave que justifica el estudio de los números p-ádicos es el Teorema de Ostrowski, el cual clasifica todos los valores absolutos de los números racionales. Este teorema establece que todo valor absoluto es equivalente al valor absoluto trivial, al valor absoluto usual o a una de los infinitos valores absolutos p-ádicos. De este modo, los números p-ádicos aparecen de forma natural cuando se considera la idea de medir distancias en $\mathbb{Q}$.

El presente trabajo tiene como objetivo construir rigurosamente el cuerpo de los números p-ádicos, explorando su estructura topológica y algebraica.

Comenzaremos introduciendo la teoría de los valores absolutos y el Teorema de Ostrowski, para luego proceder con la construcción formal de $\mathbb{Q}_p$. Luego estudiaremos algunas de sus propiedades fundamentales para posteriormente abordar el Lema de Hensel, que nos proporcione información sobre la factorización de polinomios en cuerpos p-ádicos, y exploraremos sus aplicaciones, como la clasificación de cuadrados y no cuadrados en $\mathbb{Q}_p$, y la existencia de algunas raíces de la unidad.

Al final del capítulo 2 estudiaremos el comportamiento de las series y series de potencias en $\mathbb{Q}_p$. Continuaremos con el Teorema de Strassman, el cual nos permite comenzar a comprender el comportamiento de los ceros de las funciones definidas por series de potencias. Veremos una serie de corolarios útiles y como aplicación, nos permitirá terminar de decidir el problema de existencia de ciertas raíces de la unidad.

Posteriormente, veremos cómo extender el valor absoluto de $\mathbb{Q}_p$ a sus extensiones de cuerpos. Continuaremos con el estudio y clasificación de las extensiones finitas de $\mathbb{Q}_p$, seguido de la demostración de que la clausura algebraica de $\mathbb{Q}_p$ es de dimensión infinita

sobre $\mathbb{Q}_p$ y que no es completa respecto del valor absoluto extendido; por este motivo, consideraremos la completación de la clausura algebraica y probaremos que además de completa, es algebraicamente cerrada; obteniendo así, un "análogo" a $\mathbb{C}$ en ciertos sentidos, pero totalmente diferente en otros.

Culminaremos este trabajo monográfico, hablando un poco sobre el análisis en este nuevo cuerpo $\mathbb{C}_p$, centrándonos principalmente en el Teorema de Preparación de Weierstrass p-ádico, el cual es una generalización del Teorema de Strassman, y nos permite estudiar con mayor precisión el comportamiento de los ceros y la factorización de las funciones definidas por series de potencias (y polinomios); y los polígonos de Newton, los cuales (sustentados en el teorema de preparación), nos permiten obtener información sustancial sobre el tamaño y cantidad de los ceros de polinomios o series de potencias solamente conociendo el tamaño de sus coeficientes.

Capítulo 1

Preliminares

1.1 Valores absolutos

Definición 1.1.1. *Sea* $\Bbbk$ *un cuerpo, un valor absoluto en* $\Bbbk$ *es una función*

$$|\cdot| : \Bbbk \longrightarrow \mathbb{R}_{\geq 0}$$

que cumple las siguientes condiciones:

a) $|x| = 0$ *si y solo si* $x = 0$

b) $|xy| = |x||y| \quad \forall\, x, y \in \Bbbk$

c) $|x + y| \leq |x| + |y| \quad \forall\, x, y \in \Bbbk$

Diremos que un valor absoluto en $\Bbbk$ *es no arquimediano* [1] *si además cumple:*

d) $|x + y| \leq \text{máx}\{|x|, |y|\}$

en caso contrario diremos que es arquimediano.

Ejemplo 1.1.2.

a) Tomando $\Bbbk = \mathbb{Q}$ *y el valor absoluto usual definido por:*

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

Vamos a notar a este valor absoluto por $|\ |_\infty$

[1] Esta no es la definición de cuerpo no arquimediano.

b) Sea $\Bbbk$ *cualquier cuerpo, entonces definimos el valor absoluto trivial como:*

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

que es claramente no arquimediano.

Definición 1.1.3. *Dado un primo* $p \in \mathbb{Z}$*, la valuación p-ádica en* $\mathbb{Z}$ *es la función*

$$v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R}$$

definida de la siguiente manera: para cada $n \in \mathbb{Z}$*,* $n \neq 0$ *sea* $v_p(n)$ *el único entero positivo tal que*

$$n = p^{v_p(n)} n' \qquad con \quad p \nmid n'$$

Podemos extender esta definición de v_p *a* $\mathbb{Q}$ *como sigue: si* $x = a/b \in \mathbb{Q}^\times$

$$v_p(x) = v_p(a) - v_p(b)$$

y definimos $v_p(0) = +\infty$*, tomando la convención usual de que* $+\infty - n = +\infty$*.*

Lema 1.1.4. *Para todo* x *e* $y \in \mathbb{Q}$*, tenemos que:*

a) $v_p(xy) = v_p(x) + v_p(y)$

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

Demostración.

Escribamos $x = p^{v_p(x)} \cdot \frac{a}{b}$, $y = p^{v_p(y)} \cdot \frac{c}{d}$ con $p \nmid abcd$. Luego

a) $xy = p^{v_p(x)+v_p(y)} \cdot \frac{ac}{bd}$ y entonces $v_p(xy) = v_p(x) + v_p(y)$

b) Sin pérdida de generalidad, asumamos que $v_p(x) = \text{mín}\{v_p(x), v_p(y)\}$, entonces:

$$x+y = p^{v_p(x)}.\frac{a}{b} + p^{v_p(y)}.\frac{c}{d} = p^{v_p(x)} \left(\frac{a}{b} + p^{v_p(y)-v_p(x)} \cdot \frac{c}{d}\right) = p^{v_p(x)} \left(\frac{ad + bc \cdot p^{v_p(y)-v_p(x)}}{bd}\right)$$

Luego, como el denominador no es múltiplos de p, entonces $v_p(x + y) \geq v_p(x)$.

□

Definición 1.1.5. *Para todo* $x \in \mathbb{Q}$*, definimos el valor absoluto p-ádico de* x *de la siguiente forma:*

$$|x|_p = \begin{cases} p^{-v_p(x)} & si\ x \neq 0, \\ 0 & si\ x = 0, \end{cases}$$

Que está bien definido gracias al Lema 1.1.4 y por el mismo lema, podemos ver que $|\ |_p$ *es un valor absoluto no arquimediano.*

Lema 1.1.6 (Propiedades básicas)**.** *Sea* $|\ |$ *un valor absoluto cualquiera en un cuerpo* $\Bbbk$*, luego tenemos:*

a) $|1| = 1$

b) Si $x^n = 1$*, entonces* $|x| = 1$

c) $|-1| = 1$

d) $|-x| = |x| \ \ \forall x \in \Bbbk$

e) Si $\Bbbk$ *es un cuerpo finito, entonces* $|\ |$ *es el trivial.*

Demostración.

a) $|1| = |1^2| = |1|^2$, como el único real positivo que cumple que $\alpha^2 = \alpha$ es 1, entonces $|1| = 1$.

b) Si $x^n = 1$, entonces $|x^n| = |x|^n = 1$. Nuevamente, la única raíz positiva del polinomio $\alpha^n = \alpha$ es 1, por lo tanto $|x| = 1$.

c) Es un caso particular de lo anterior.

d) $|-x| = |-1|\,|x| = |x|$.

e) Supongamos que $\Bbbk$ tiene q elementos. Sea $x \in \Bbbk$ no nulo, luego $x^{q-1} = 1$ (pues $\Bbbk^\times$ tiene $q-1$ elementos) y entonces, por (b), $|x| = 1$, ergo $|\ |$ es el trivial. □

Lema 1.1.7. *Sea* $\Bbbk$ *un cuerpo con una función* $|\ |$ *que cumple las propiedades* (a) *y* (b) *de la definición 1.1.1, entonces son equivalentes:*

a) $|\ |$ *es un valor absoluto no arquimediano, es decir que vale* $|x+y| \leq \text{máx}\{|x|, |y|\}$

b) $|x+1| \leq \text{máx}\{|x|, 1\}$

c) $|x| \leq 1 \Longrightarrow |x-1| \leq 1$

Demostración.
$(a) \Longrightarrow (b)$: simplemente tomando $y = 1$.

$(b) \Longrightarrow (a)$: Si $y = 0$, (a) vale automáticamente. Sea $y \neq 0$, luego:

$$\left|\frac{x}{y} + 1\right| \leq \text{máx}\left\{\frac{|x|}{|y|}, 1\right\}$$

Ahora, multiplicando a ambos lados por $|y|$ queda (a).

$(a) \Longrightarrow (c)$: supongamos $|x| \leq 1$, luego:

$$|x-1| = |x+(-1)| \leq \text{máx}\{|x|, |-1|\} = \text{máx}\{|x|, |1|\} = 1$$

$(c) \Longrightarrow (b)$: Notemos lo siguiente:

$$|x| = |-x| \leq 1 \Longrightarrow |(-x)-1| = |x+1| \leq 1$$

es decir, que (c) implica que $|x| \leq 1 \Rightarrow |x+1| \leq 1$.
Ahora separemos por casos:

- si $|x| \leq 1$, entonces $\text{máx}\{|x|, 1\} = 1$ y por ende $|x+1| \leq 1 = \text{máx}\{|x|, 1\}$.
- si $|x| > 1$ luego $|\frac{1}{x}| < 1$ y entonces $|1 + \frac{1}{x}| \leq 1$. Por lo tanto $\left|\frac{x+1}{x}\right| \leq 1$ ergo $|x+1| \leq |x| = \text{máx}\{|x|, 1\}$.

□

Teorema 1.1.8. *Sea* $\Bbbk$ *un cuerpo y* $A \subset \Bbbk$ *la imagen de* $\mathbb{Z}$ *en* $\Bbbk$. *Un valor absoluto en* $\Bbbk$ *es no arquimediano si y solo si* $|a| \leq 1$ $\forall a \in A$.

Demostración.
Supongamos que $|\ |$ es no arquimediano. Procedemos por inducción:
Sabemos que $|\pm 1| = 1$. Supongamos que $|a| \leq 1$ luego $|a+1| \leq \text{máx}\{|a|, 1\} = 1$ entonces $|a| \leq 1$ para todo $a \in A$.

Para el reciproco supongamos que $|a| \leq 1$ $\forall a \in A$. Por el Lema 1.1.7 nos basta probar que para todo $x \in \Bbbk$, $|x+1| \leq \text{máx}\{|x|, 1\}$.
Sea m un entero positivo, luego :

$$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x^k|$$

como $\binom{m}{k}$ es un entero, tenemos que $\left|\binom{m}{k}\right| \leq 1$, entonces:

$$|x+1|^m \leq \sum_{k=0}^{m} |x|^k$$

Observar que el valor más grande que toma $|x|^k$ para $k = 0, 1, 2, ..., m$ es $|x|^m$ si $|x| > 1$ y es 1 si $|x| \leq 1$ (pues $x^0 = 1$). Por lo tanto, tenemos que

$$|x+1|^m \leq (m+1)\,\text{máx}\{1, |x|^m\}$$

Tomando la raíz m-ésima:

$$|x+1| \leq \sqrt[m]{m+1}\,\text{máx}\{1, |x|\}$$

Por último, como esto vale para todo m, tomando límite cuando $m \to \infty$, tenemos justamente que

$$|x+1| \leq \text{máx}\{1, |x|\}$$

□

1.2 Topología y Teorema de Ostrowski

Definición 1.2.1. *Sea $\Bbbk$ un cuerpo y $|\ |$ un valor absoluto en $\Bbbk$, definimos la métrica inducida en $\Bbbk$ por el valor absoluto de la siguiente forma:*

$$d(x,y) = |x-y| \quad \forall x, y \in \Bbbk.$$

Lema 1.2.2 (La desigualdad ultramétrica)**.** *Sea $|\ |$ un valor absoluto en $\Bbbk$ y $d(x,y)$ la métrica inducida. Luego $|\ |$ es no arquimediano si y solo si $\forall x, y, z \in \Bbbk$, tenemos que:*

$$d(x,y) \leq \text{máx}\{d(x,z), d(y,z)\}$$

Demostración.
Para el directo, simplemente tenemos la igualdad $x - y = (x - z) + (z - y)$ y aplicando el valor absoluto nos queda :

$$d(x,y) = |x-y| = |(x-z)+(z-y)| \leq \text{máx}\{|x-z|, |z-y|\} = \text{máx}\{d(x,z), d(z,y)\}$$

Para el recíproco, en la desigualdad ultramétrica tomamos $y = -y$ y $z = 0$, entonces :

$$|x+y| = d(x,-y) \leq \text{máx}\{d(x,0), d(-y,0)\} = \text{máx}\{|x|, |y|\}$$

□

Decimos que $\Bbbk$ es un espacio ultramétrico si es un cuerpo con un valor absoluto no arquimediano.

Proposición 1.2.3. *Sea $\Bbbk$ un cuerpo y $|\ |$ un valor absoluto no arquimediano en $\Bbbk$. Si $x, y \in \Bbbk$ y $|x| \neq |y|$, entonces:*

$$|x+y| = \text{máx}\{|x|, |y|\}$$

Demostración.
Sin pérdida de generalidad, supongamos que $|x| > |y|$, luego $|x+y| \leq |x|$. Por otro lado, $x = (x+y) - y$, entonces $|x| \leq \text{máx}\{|x+y|, |y|\}$. Pero ya sabemos que $|x| > |y|$ entonces para que la desigualdad anterior ocurra, $\text{máx}\{|x+y|, |y|\} = |x+y|$ por lo tanto $|x| \leq |x+y|$. Ergo, por la primera desigualdad, $|x+y| = |x|$. □

Corolario 1.2.4. *En un espacio ultramétrico, todos los triángulos son isósceles.*

Demostración.
Si $x, y, z \in \Bbbk$ son elementos de nuestro espacio (los vértices de nuestro triángulo) y $|x-y| = d(x,y) \neq d(y,z) = |y-z|$, entonces, como $(x-y)+(y-z) = (x-z)$, por la Proposición 1.2.3 $|x-z|$ es igual al más grande de los otros dos. □

Utilizando este corolario y la proposición, veamos una propiedad topológica importante de los espacios con métrica no arquimediana:

Proposición 1.2.5. *Sea $\Bbbk$ un cuerpo con un valor absoluto no arquimediano, $a \in \Bbbk$ y $r \in \mathbb{R}_{\geq 0}$ entonces vale lo siguiente:*

a) Si $b \in B(a,r) = \{x \in \Bbbk : d(x,a) < r\}$, entonces $B(a,r) = B(b,r)$, es decir que todo punto contenido en una bola abierta puede ser visto como el centro de esa bola abierta.

b) Si $b \in \overline{B}(a,r) = \{x \in \Bbbk : d(x,a) \leq r\}$, entonces $\overline{B}(a,r) = \overline{B}(b,r)$, es decir que todo punto contenido en una bola cerrada puede ser visto como el centro de esa bola cerrada.

c) El conjunto $B(a,r)$ es abierto y cerrado. Además tiene frontera vacía.

d) Si $r \neq 0$, el conjunto $\overline{B}(a,r)$ es abierto y cerrado y tiene frontera vacía.

e) Si $a, b \in \Bbbk$, $r, s \in \mathbb{R}^+$, entonces tenemos que $B(a,r) \cap B(b,s) \neq \emptyset$ si y solo si $B(a,r) \subset B(b,s)$ o $B(b,s) \supset B(a,r)$. Es decir que dos bolas abiertas son disjuntas o una contiene a la otra.

f) Si $a, b \in \Bbbk$, $r, s \in \mathbb{R}^+$, entonces tenemos que $\overline{B}(a,r) \cap \overline{B}(b,s) \neq \emptyset$ si y solo si $\overline{B}(a,r) \subset \overline{B}(b,s)$ o $\overline{B}(b,s) \supset \overline{B}(a,r)$. Es decir que dos bolas cerradas son disjuntas o una contiene a la otra.

Demostración.

a) Como $b \in B(a,r)$ entonces $|b-a| < r$. Luego sea $x \in B(a,r)$, es decir $|x-a| < r$. Por la propiedad no arquimediana tenemos que:
$$|x-b| \leq \text{máx}\{|x-a|, |b-a|\} < r$$
y por ende $x \in B(b,r)$; esto prueba que $B(a,r) \subset B(b,r)$. Para la otra inclusión, observar que si $b \in B(a,r)$ entonces $a \in B(b,r)$ y repetir lo anterior cambiando a y b.

b) Cambiar $<$ por $\leq$ en la demostración anterior.

c) Las bolas abiertas siempre son abiertos en cualquier espacio métrico; probemos que en el caso no arquimediano también son cerrados. Esto es equivalente a probar que su complemento $C = \{x \in \Bbbk : d(x,a) \geq r\}$ es abierto. Sea $y \in C$, es decir $|y-a| \geq r$. Tomemos $s < r$, probaremos que $B(y,s) \subset C$ y por ende que C es abierto. Sea $z \in B(y,s)$, luego $|z-y| < s < r \leq |y-a|$ por lo tanto, por la Proposición 1.2.3:
$$|z-a| = \text{máx}\{|z-y|, |y-a|\} = |y-a| \geq r$$
es decir, como queríamos probar $z \in C \ \forall \ z \in B(y,s)$.
La afirmación sobre la frontera es un hecho general sobre los conjuntos que son

abiertos y cerrados en espacios topológicos: Si un punto está en la frontera de $B(a,r)$, entonces cualquier entorno de ese punto contiene puntos de $B(a,r)$ y de C. Por ende, también está en la frontera de C. Como ambos $B(a,r)$ y C son cerrados, y los cerrados contienen a sus puntos frontera, concluimos que cualquier punto frontera pertenece a $B(a,r) \cap C = \emptyset$.

d) Análogo a lo anterior.

e) Podemos asumir sin pérdida de generalidad que $r \leq s$ (en caso contrario cambiar r por s en lo que sigue). Si la intersección es no vacía, entonces existe $c \in B(a,r) \cap B(b,s)$, luego, por (a), $B(a,r) = B(c,r) \subset B(c,s) = B(b,s)$, como queríamos probar.

f) Idéntico a (e) usando (b).

□

Esta última proposición deja completamente en evidencia que la topología de un espacio con una métrica no arquimediana es bastante distinta a la que estamos acostumbrados en $\mathbb{R}$. Para dejar esto aún más claro, tenemos la siguiente proposición:

Proposición 1.2.6. *Un cuerpo $\mathbb{k}$ con un valor absoluto no arquimediano es totalmente disconexo (es decir que sus componentes conexas son sus puntos).*

Demostración. Probaremos que si un conjunto contiene dos puntos distintos, entonces es disconexo.
Sea S un conjunto que contiene a dos puntos distintos x, y, y sea $r = |x - y|$. Definimos $U = B\left(x, \frac{r}{2}\right)$ y V su complemento. Notar que $x \in U \setminus V$ y que $y \in V \setminus U$. Luego tomamos los abiertos relativos $S \cap U$ y $S \cap V$, su unión da todo S y son disjuntos. Por lo tanto, todo conjunto que contenga al menos dos puntos es disconexo y por ende $\mathbb{k}$ es totalmente disconexo. □

Una vez comprendida la topología es natural que surja la siguiente definición:

Definición 1.2.7. *Dos valores absolutos $|\ |_1$ y $|\ |_2$ sobre un cuerpo $\mathbb{k}$ son equivalentes si definen la misma topología en $\mathbb{k}$, es decir si todo abierto respecto a uno es abierto respecto a otro.*

Veamos otras posibles definiciones que nos serán útiles en lo que sigue y en particular para probar el Teorema de Ostrowski 1.2.10:

Proposición 1.2.8. *Sean $|\ |_1$ y $|\ |_2$ dos valores absolutos no triviales sobre un cuerpo $\mathbb{k}$. Luego las siguientes afirmaciones son equivalentes:*

a) $|\ |_1$ y $|\ |_2$ son equivalentes.

b) Para cualquier sucesión (x_n) en $\mathbb{k}$, tenemos que $x_n \to a$ con respecto a $|\ |_1$ si y solo si $x_n \to a$ con respecto a $|\ |_2$

c) Para todo $x \in \mathbb{k}$, tenemos que $|x|_1 < 1$ si y solo si $|x|_2 < 1$

d) Existe un real positivo α tal que $\forall\ x \in \Bbbk$ tenemos que

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

DEMOSTRACIÓN.

- Que (a) implica (b) es claro, pues los abiertos definidos por $|\ |_1$ y $|\ |_2$ son los mismos.

- Para probar que (b) implica (c), basta observar que $\lim_{n\to\infty} x^n = 0$ con respecto a la topología inducida por $|\ |$ si y solo si $|x| < 1$.

- Supongamos que vale (c), Sea $x_0 \in \Bbbk$, $x_0 \neq 0$ tal que $|x_0|_1 < 1$, luego $|x_0|_2 < 1$. Entonces existe un real positivo α tal que $|x_0|_1 = |x_0|_2^{\alpha}$ (simplemente tomando $\alpha = \frac{\log|x_0|_1}{\log|x_0|_2}$). Sea ahora otro $x \in \Bbbk$, $x \neq 0$. Si $|x|_1 = |x_0|_1$, luego $|x|_2 = |x_0|_2$, porque en caso contrario x/x_0 o x_0/x tendrían $|\ |_2$ menor a 1 y sería absurdo pues tiene $|\ |_1$ igual a 1. Por lo tanto en este caso $|x|_1 = |x|_2^{\alpha}$.
  Supongamos ahora que $|x|_1 = 1$ luego $|x|_2 = 1$ ya que en caso contrario $|x|_2 < 1$ o $|1/x|_2 < 1$ lo cual implicaría que $|x|_1 < 1$ o $|1/x|_1 < 1$ (en ambos casos llegamos a un absurdo). Por lo tanto en este caso la ecuación $|x|_1 = |x|_1^{\alpha}$ se mantiene trivialmente.
  Consideremos ahora el caso en que $|x|_i \neq 1$ y $|x|_i \neq |x_0|_i$. Notar que la igualdad en la ecuación para algún x, implica que la igualdad vale para cualquier potencia entera de x. Con lo cual, sin pérdida de generalidad, podemos asumir $|x|_1 < 1$ (en caso contrario, trabajamos con $1/x$). Sea β tal que $|x|_1 = |x|_2^{\beta}$, es decir $\beta = \frac{\log|x|_1}{\log|x|_2}$, queremos probar que $\alpha = \beta$. Sean n y m dos enteros positivos, entonces tenemos que:

  $$|x|_1^n < |x_0|_1^m \iff \left|\frac{x^n}{x_0^m}\right|_1 < 1 \iff \left|\frac{x^n}{x_0^m}\right|_2 < 1 \iff |x|_2^n < |x_0|_2^m$$

  Tomando logaritmo y dividiendo en la primera y última ecuación tenemos:

  $$\frac{n}{m} < \frac{\log|x_0|_1}{\log|x|_1} \iff \frac{n}{m} < \frac{\log|x_0|_2}{\log|x|_2}$$

  Lo que nos dice que el conjunto de racionales menores al primer cociente es el mismo que el conjunto de racionales menores al segundo cociente, por ende:

  $$\frac{\log|x_0|_1}{\log|x|_1} = \frac{\log|x_0|_2}{\log|x|_2} \Longrightarrow \frac{\log|x_0|_1}{\log|x_0|_2} = \frac{\log|x|_1}{\log|x|_2} \Longrightarrow \alpha = \beta.$$

- Por último, asumamos (d) y probemos (a). Para probar que $|\ |_1$ y $|\ |_2$ generan la misma topología, basta probar que toda bola en una es una bola en otra. Pero por (d) tenemos que:

  $$|x-a|_1 < r \iff |x-a|_2^{\alpha} < r \iff |x-a|_2 < r^{1/\alpha}$$

  por lo que $B(a,r)$ para $|\ |_1$ es igual a $B(a, r^{1/\alpha})$ para $|\ |_2$.

□

Observación 1.2.9.

- *Si un valor absoluto $|\ |$ es equivalente al trivial, debe ser el trivial, pues $1^\alpha = 1$ y $0^\alpha = 0$.*

- *Si p y q son dos primos diferentes, el valor absoluto p-ádico y el valor absoluto q-ádico no son equivalentes, pues $|p|_p < 1$, pero $|p|_q = 1$.*

Ahora ya estamos en condiciones de probar el Teorema de Ostrowski:

Teorema 1.2.10 (**Ostrowski**). *Todo valor absoluto no trivial en $\mathbb{Q}$ es equivalente a uno de los valores absolutos $|\ |_p$ donde p primo o $p = \infty$.*

Demostración.

a) Supongamos primero que $|\ |$ es arquimediano. Queremos probar que es equivalente a $|\ |_\infty$.
Por el Teorema 1.1.8, sabemos que existe n_0 el menor entero positivo para el cual $|n_0| > 1$ (si no existiera $|\ |$ sería no arquimediano). Luego, existe un real positivo α tal que:

$$|n_0| = n_0^\alpha$$

simplemente tomando $\alpha = \frac{\log |n_0|}{\log n_0}$. Queremos probar que este α es el que realiza la equivalencia en la Proposición 1.2.8, es decir, queremos probar que $\forall\ x \in \mathbb{Q}$ $|x| = |x|_\infty^\alpha$.
Por la definición de valor absoluto y el Lema 1.1.6, es claro que basta probar la igualdad para los enteros positivos. Sea n un entero positivo cualquiera, escribamos n "en base n_0", es decir:

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + ... + a_k n_0^k$$

con $0 \leq a_i \leq n_0 - 1$ y $a_k \neq 0$. Ahora tomando valor absoluto:

$$\begin{aligned} |n| &= |a_0 + a_1 n_0 + a_2 n_0^2 + ... + a_k n_0^k| \\ &\leq |a_0| + |a_1| n_0^\alpha + |a_2| n_0^{2\alpha} + ... + |a_k| n_0^{k\alpha} \end{aligned}$$

Como elegimos n_0 siendo el menor entero positivo que cumplía que $|n_0| > 1$, sabemos que $|a_i| \leq 1$, por lo tanto:

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

Si llamamos $C = n_0^\alpha/(n_0^\alpha - 1)$, la cual es una constante positiva que no depende de n, tenemos que:

$$|n| \leq Cn_0^{k\alpha} \leq Cn^\alpha,$$

donde la última desigualdad se da pues $n_0^k \leq n$ por la expresión de n en base n_0. Esta desigualdad vale para todo n, entonces simplemente tomamos un n de la forma n^N y tenemos:

$$|n^N| \leq Cn^{N\alpha}$$

tomando raiz N-ésima

$$|n| \leq \sqrt[N]{C}n^\alpha.$$

Como esto vale para todo N y C no depende de n, tomando límite $N \to \infty$, $\sqrt[N]{C} \to 1$, y por lo tanto obtenemos la desigualdad $|n| \leq n^\alpha$.
Ahora nos queda probar la otra desigualdad. Para esto, tomamos nuevamente la expresión en base n_0

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + ... + a_k n_0^k.$$

Como $n_0^{k+1} > n \geq n_0^k$, tenemos que

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \leq |n| + |n_0^{k+1} - n|$$

por lo tanto

$$|n| \geq n_0^{(k+1)\alpha} - |n_0^{k+1} - n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha$$

donde en la última desigualdad, utilizamos la desigualdad probada anteriormente. Ahora, como $n_0^{k+1} > n \geq n_0^k$ tenemos que:

$$\begin{aligned} |n| &\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^\alpha \\ &= n_0^{(k+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \\ &= An_0^{(k+1)\alpha} \\ &> An^\alpha \end{aligned}$$

donde $A = 1 - (1 - 1/n_0)^\alpha$ no depende de n y es positiva. Nuevamente, esta desigualdad vale para todo n, entonces se la aplicamos a n^N y tenemos que:

$$|n^N| > An^{N\alpha}$$

tomando raíz N-ésima:

$$|n| > \sqrt[N]{A}n^\alpha.$$

Una vez más, esto vale para todo N ,y como A no depende de n, tomando límite $N \to \infty$ tenemos que $\sqrt[N]{A} \to 1$ y por ende $|n| \geq n^\alpha$.
Juntando estas dos desigualdades, obtenemos $|n| = n^\alpha$ y esto prueba que $|\ |$ es equivalente al valor absoluto usual $|\ |_\infty$.

b) Ahora supongamos que $|\ |$ es no arquimediano. Luego, por la Proposición 1.1.8, tenemos que $|n| \leq 1\ \forall\ n \in \mathbb{Z}$. Como $|\ |$ es no trivial, debe existir un mínimo entero positivo n_0 tal que $|n_0| < 1$.
Observemos que este n_0 debe ser primo: supongamos $n_0 = a \cdot b$, con a y b ambos menores a n_0. Por nuestra elección de n_0, debe pasar que $|a| = |b| = 1$, luego $1 > |n_0| = |a| \cdot |b| = 1$, lo que es absurdo. Por lo tanto, n_0 es primo, a partir de ahora $p = n_0$. Ahora lo que queremos probar es que $|\ |$ es equivalente a $|\ |_p$ (donde p es este primo particular).
Primero probaremos que si $n \in \mathbb{Z}$ no es divisible por p, entonces $|n| = 1$: dividiendo n por p, tenemos que $n = pq + r$ con $0 < r < p$. Por la minimalidad de p, tenemos que $|r| = 1$. Luego, recordando que por ser q entero y $|\ |$ no arquimediano, $|q| \leq 1$, tenemos que $|pq| < 1$ y por ende, por la Proposición 1.2.3 sigue que $|n| = 1$.
Finalmente, dado $n \in \mathbb{Z}$, escribimos $n = p^v n'$, y tenemos que:

$$|n| = |p|^v |n'| = |p|^v = c^{-v}$$

donde $c = |p|^{-1} > 1$. Por lo tanto $|\ |$ es equivalente al valor absoluto p-ádico (pues $c^{-v} = p^{-v \cdot \log_p c}$ y $\log_p c > 0$).

□

Este Teorema es la principal razón por la que uno quiere pensar al valor absoluto usual $|\ |_\infty$ como una especie de primo de $\mathbb{Q}$. Hay muchos contextos en la teoría de números en dónde es útil trabajar con "todos los primos", es decir, con la información obtenida mediante el estudio de cierto comportamiento en todos los valores absolutos sobre $\mathbb{Q}$. En cuánto a motivación, es como si el valor absoluto usual recogiera información relacionado con el signo y los otros valores absolutos sobre el comportamiento en cada primo. Un ejemplo clásico es el Teorema de Hasse-Minkowski, el cual se puede encontrar en [1]. El ejemplo más básico de este comportamiento es el siguiente:

Proposición 1.2.11 (Fórmula del Producto)**.** *Para todo $x \in \mathbb{Q}^\times$, tenemos que:*

$$\prod_{p \leq \infty} |x|_p = 1$$

Demostración. Claramente basta probar la proposición para x entero positivo, por lo tanto, escribimos $x = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$. Luego tenemos que $|x|_q = 1$ si $q \neq p_i$, $|x|_{p_i} = p_i^{-a_i}$ $\forall\ i = 1, 2, ..., k$ y $|x|_\infty = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$, luego el resultado es claro. □

Esta fórmula aunque simple, establece una profunda relación entre todos los valores absolutos sobre $\mathbb{Q}$. Por ejemplo, nos dice que si conocemos todos los valores absolutos salvo uno, entonces los podemos conocer todos. Este hecho resulta fundamental para ciertas aplicaciones, por ejemplo en el estudio de formas cuadráticas y sus representaciones.

1.3 Construcción de $\mathbb{Q}_p$

Recordemos algunas definiciones:

Definición 1.3.1. *Sea $\Bbbk$ un cuerpo y $|\ |$ un valor absoluto en $\Bbbk$:*

a) Una sucesión (x_n) en $\Bbbk$ se dice de Cauchy si para todo $\varepsilon > 0$ existe M tal que $|x_n - x_m| < \varepsilon$ siempre que $m, n \geq M$.

b) $\Bbbk$ es completo respecto a $|\ |$ si toda sucesión de Cauchy converge en $\Bbbk$.

Recordamos estas definiciones, pues como uno ve en los cursos iniciales de la carrera, $\mathbb{R}$ es la completación de $\mathbb{Q}$ con respecto a $|\ |_\infty$, es decir:

- el valor absoluto $|\ |_\infty$ se extiende a $\mathbb{R}$.
- $\mathbb{R}$ es completo con respecto a la métrica dada por este valor absoluto.
- $\mathbb{Q}$ es denso en $\mathbb{R}$ respecto a la métrica inducida por $|\ |_\infty$.

El objetivo de esta sección es realizar una construcción similar, pero ahora con respecto a los valores absolutos no arquimedianos $|\ |_p$. A esta completación le llamaremos $\mathbb{Q}_p$. Veamos un lema que nos será útil en lo que sigue:

Lema 1.3.2. *Una sucesión (x_n) en un cuerpo $\Bbbk$ con un valor absoluto no arquimediano $|\ |$ es una sucesión de Cauchy si y solo si tenemos que*

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

Demostración. Es claro que si una sucesión es de Cauchy, entonces tenemos ese límite, con lo que solamente es necesario probar la otra implicación.
Sea $m = n + r > n$, tenemos entonces:

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

porque el valor absoluto es no arquimediano y sigue el resultado pues lo de la derecha es tan chico como uno quiera tomando n suficientemente grande. □

El siguiente paso es probar que $\mathbb{Q}$ no es completo respecto a los valores absolutos p-ádicos, es decir que el proceso de completación efectivamente agrega algo, para ello precisaremos un lema:

Lema 1.3.3.

a) Dado $p \neq 2$ primo y $a, x_0 \in \mathbb{Z}$, tal que $0 \leq x_0 \leq p-1$ es una solución de la ecuación $X^2 \equiv a \pmod{p}$ y tal que p no divide a a, entonces existe una única sucesión $(x_n) \subset \mathbb{Z}$ tal que

$$x_n \equiv x_{n-1} \ (mod\ p^n) \quad y \quad x_n^2 \equiv a \ (mod\ p^{n+1})$$

b) Si $p = 2$, existe una única sucesión (x_n) tal que

$$x_n \equiv x_{n-1} \ (mod\ 2^n) \quad y \quad x_n^3 \equiv 3 \ (mod\ 2^{n+1})$$

Demostración.

a) Procedamos por inducción. Veamos primero que dado x_0 existe un x_1 que cumple lo que queremos. Como queremos que $x_1 \equiv x_0 (mod\ p)$, entonces sabemos que de existir, $x_1 = x_0 + kp$ con $0 \leq k \leq p-1$. Luego utilizando la segunda congruencia, tenemos que $x_1^2 = (x_0 + kp)^2 \equiv a (mod\ p^2)$. Operando y reduciendo módulo p^2:

$$x_0^2 + 2kx_0p \equiv a\ (mod\ p^2)$$

Luego,

$$2kx_0p \equiv a - x_0^2\ (mod\ p^2) \iff 2kx_0 \equiv \left(\frac{a - x_0^2}{p}\right)\ (mod\ p),$$

pues $a - x_0^2$ es divisible por p.
Por último, como $p \neq 2$ y $x_0 \not\equiv 0\ (mod\ p)$, existe un único valor k que satisface la equivalencia anterior y por ende un único x_1.
Supongamos ahora que vale para $n-1$, entonces tenemos que de existir, $x_n = x_{n-1} + kp^n$ con $0 \leq k \leq p^{n-1}$ (aunque como veremos, podemos tomar $0 \leq k \leq p-1$). Luego, utilizando la segunda congruencia, nuevamente tenemos que $x_n^2 = (x_{n-1} + kp^n)^2 \equiv a (mod\ p^{n+1})$. Operando y reduciendo módulo p^{n+1}:

$$x_{n-1}^2 + 2kx_{n-1}p^n \equiv a\ (mod\ p^{n+1}).$$

Luego,

$$2kx_{n-1}p^n \equiv a - x_{n-1}^2\ (mod\ p^{n+1}) \iff 2kx_{n-1} \equiv \left(\frac{a - x_{n-1}^2}{p^n}\right)\ (mod\ p),$$

pues $a - x_{n-1}^2 \equiv 0\ (mod\ p^n)$.
Nuevamente, como $p \neq 2$ y $x_{n-1} \not\equiv 0\ (mod\ p)$, podemos hallar un único k que cumpla la ecuación anterior y por ende un único x_n.

b) Claramente $x_0 = 1$. Luego, al igual que antes, procedamos por inducción (solo realizaremos la construcción de x_1, pues al igual que en la parte (a), la construcción es análoga en cada paso.
Como queremos que $x_1 \equiv x_0\ (mod\ 2)$, entonces sabemos que de existir, $x_1 = x_0 + 2k$ con $0 \leq k \leq 1$. Luego, utilizando la segunda congruencia, tenemos que $x_1^3 = (x_0 + 2k)^3 \equiv 3\ (mod\ 4)$. Operando y reduciendo módulo 4:

$$x_0^3 + 3x_0^2 2k \equiv 3\ (mod\ 4).$$

Luego,

$$3kx_0 2 \equiv 3 - x_0^3\ (mod\ 4) \iff 3kx_0 \equiv \left(\frac{3 - x_0^3}{2}\right)\ (mod\ 2)$$

pues $3 - x_0^3$ es divisible por 2.
Como 3 y $x_0 = 1$ son invertibles, podemos despejar un único k de la equivalencia y por ende un único x_1.

□

Notemos que la demostración de (a) no funciona para $p = 2$ pues al desarrollar el cuadrado nos aparece un 2 que no quedaría invertible. Este lema es un caso particular del Lema de Hensel del cual hablaremos en el siguiente capítulo.
Utilizaremos esta forma particular para probar que $\mathbb{Q}$ no es completo:

Proposición 1.3.4. *$\mathbb{Q}$ no es completo respecto a ninguno de sus valores absolutos no triviales.*

Demostración. Por el Teorema de Ostrowski, basta con verificar la afirmación para $|\ |_p$ con $p \leq \infty$. Que $\mathbb{Q}$ no es completo para $|\ |_\infty$ es bien conocido, por lo tanto, veremos qué pasa con los valores absolutos p-ádicos.
Sea p primo, queremos construir una sucesión de Cauchy que no tenga límite en $\mathbb{Q}$. Para construir la sucesión de Cauchy que precisamos, basta encontrar una sucesión (que cumpla ciertas condiciones) de soluciones módulo p^n de una ecuación que no tenga soluciones en $\mathbb{Q}$.
Supongamos que $p \neq 2$. Sea a un entero tal que:

- a no es cuadrado en $\mathbb{Q}$
- p no divide a a
- a es un residuo cuadrático módulo p, i.e, la ecuación de congruencia $X^2 \equiv a\ (mod\ p)$ tiene solución.

Por ejemplo, elegimos un cuadrado en $\mathbb{Z}$ que no sea múltiplo de p y le sumamos un múltiplo de p para que cumpla lo que queremos.
Ahora podemos construir una sucesión de Cauchy (respecto a $|\ |_p$) siguiendo el lema anterior, es decir:

- sea x_0 una solución de $X^2 \equiv a\ (mod\ p)$
- elegimos x_n tal que
$$x_n \equiv x_{n-1}\ (mod\ p^n) \quad \text{y} \quad x_n^2 \equiv a\ (mod\ p^{n+1})$$

El siguiente paso es probar que esta sucesión efectivamente es de Cauchy.
Por la construcción, es claro que
$$|x_{n+1} - x_n|_p = |kp^{n+1}|_p \leq p^{-(n+1)} \to 0$$
lo que muestra, gracias al Lema 1.3.2 que la sucesión (x_n) es de Cauchy.
Por otro lado, tambien sabemos que:
$$|x_n^2 - a|_p = |hp^{n+1}|_p \leq p^{-(n+1)} \to 0,$$
por lo que el límite, en caso de existir, debería ser una raiz cuadrada de a. Como a no es un cuadrado en $\mathbb{Q}$, entonces no existe el límite en $\mathbb{Q}$, lo que prueba que $\mathbb{Q}$ no es completo respecto a $|\ |_p$.

Consideremos $p = 2$ y construyamos la sucesión siguiendo nuevamente el lema anterior, es decir:

- sea $y_0 = 1$ una solución de $X^3 \equiv 3 \ (mod\ 2)$
- elegimos y_n tal que

$$y_n \equiv y_{n-1} \ (mod\ 2^n) \quad \text{y} \quad y_n^3 \equiv 3 \ (mod\ 2^{n+1})$$

Probemos que la sucesión (y_n) es de Cauchy. Por la construcción, es claro que

$$|y_{n+1} - y_n|_2 = |k2^{n+1}|_2 \leq 2^{-(n+1)} \to 0$$

lo que nuevamente muestra gracias al Lema 1.3.2 que la sucesión (y_n) es de Cauchy. Por otro lado, sabemos que:

$$|y_n^3 - 3|_2 = |h2^{n+1}|_2 \leq 2^{-(n+1)} \to 0,$$

por lo que el límite, en caso de existir, debería ser una raíz cúbica de 3. Como 3 no es un cubo en $\mathbb{Q}$, entonces no existe el límite en $\mathbb{Q}$ y por ende $\mathbb{Q}$ no es completo respecto a $|\ |_2$. □

Ahora construyamos la completación de $\mathbb{Q}$ con respecto a sus valores absolutos p-ádicos. Para eso precisaremos algunas definiciones y propiedades que recordaremos a continuación.

Definición 1.3.5. *Dado $|\ |_p$, denotamos por $\mathcal{C}$ o $\mathcal{C}_p$ si queremos enfatizar el primo al que hacemos referencia, al conjunto de todas las sucesiones de Cauchy en $\mathbb{Q}$:*

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

Observación 1.3.6. *Definiendo*

$$(x_n) + (y_n) = (x_n + y_n)$$
$$(x_n) \cdot (y_n) = (x_n y_n),$$

a) $\mathcal{C}$ es un anillo conmutativo con unidad.[2]
b) Los invertibles en $\mathcal{C}$ son justamente aquellas sucesiones de Cauchy que están "lejos"de cero, es decir para las que existe una cota $b > 0$ tal que $|x_n| > b$ para todo n.
c) $\mathcal{C}$ tiene divisores de cero; por ejemplo la sucesión $0, p, 0, p^2, 0, p^3, 0...$ y la sucesión $p, 0, p^2, 0, p^3, 0, p^4, ...$ multiplicadas dan el neutro y ninguna es el neutro.

La completación de $\mathbb{Q}$, será este anillo con algunas modificaciones que veremos más adelante, pero lo que queremos verificar ahora es que este anillo $\mathcal{C}$ contiene a los racionales. Para esto, basta con observar que si $x \in \mathbb{Q}$ entonces la sucesión constante igual a x es una sucesión de Cauchy. Notamos a esta sucesión como $\tilde{x}$.
Luego, es claro de la definición que tenemos un morfismo de anillos inyectivo de $\mathbb{Q}$ en $\mathcal{C}$ definido por $x \to \tilde{x}$.

El problema con $\mathcal{C}$, es que hay varias sucesiones (cuyos términos se acercan) que deberían tener el mismo límite, pero son elementos distintos en $\mathcal{C}$. Para arreglar esto, simplemente pasamos al cociente por las sucesiones que tienden a cero, como mostramos a continuación.

[2]La demostración de que la suma y el producto de sucesiones de Cauchy es de Cauchy es análoga a la usual.

Definición 1.3.7. *Definimos $\mathcal{N} \subset \mathcal{C}$ como el ideal*

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

de sucesiones que tienden a cero respecto a $|\ |_p$.

Lema 1.3.8. *$\mathcal{N}$ es un ideal maximal de $\mathcal{C}$.*

Demostración. Sea $(x_n) \in \mathcal{C}$ una sucesión de Cauchy que no tiende a cero, y sea $I = \langle \mathcal{N}, (x_n) \rangle$ el ideal generado por $\mathcal{N}$ y por (x_n). Queremos probar que I debe ser $\mathcal{C}$. Lo haremos probando que la unidad $\tilde{1}$ pertenece a I.
Como (x_n) no tiende a cero y es una sucesión de Cauchy, existe un $c > 0$ y un entero N tal que $|x_n| \geq c > 0$ siempre que $n \geq N$. En particular, esto significa que $x_n \neq 0$ para $n \geq N$, entonces ahora definimos una nueva sucesión (y_n) tal que $y_n = 0$ si $n < N$ y $y_n = 1/x_n$ si $n \geq N$.
Veamos que (y_n) es una sucesión de Cauchy:

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

lo cual prueba gracias al Lema 1.3.2 que $(y_n) \in \mathcal{C}$. Notemos que

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

Lo que nos dice que si restamos la sucesión producto $(x_n)(y_n)$ a la sucesión constante $\tilde{1}$, obtenemos una sucesión que tiende a cero, es decir: $\tilde{1} - (x_n)(y_n) \in \mathcal{N}$. Pero esto nos dice que $\tilde{1}$ puede ser escrita como un múltiplo de (x_n) más un elemento de $\mathcal{N}$, y por lo tanto $\tilde{1} \in I$. □

Ahora sí, podemos definir $\mathbb{Q}_p$

Definición 1.3.9. *Definimos el cuerpo de los números p-ádicos como el siguiente cociente:*

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

Observar que dos sucesiones constantes no difieren por un elemento de $\mathcal{N}$, por lo que todavía tenemos la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, mandando un elemento $x \in \mathbb{Q}$ a la clase de equivalencia de la sucesión constante $\tilde{x}$.

Ahora veamos que este cuerpo $\mathbb{Q}_p$ cumple las propiedades de las completaciones. Lo primero que vamos a demostrar es que el valor absoluto $|\ |_p$ se extiende a $\mathbb{Q}_p$.

Lema 1.3.10. *Sea $(x_n) \in \mathcal{C}$, $(x_n) \notin \mathcal{N}$. La sucesión de números reales $|x_n|_p$ es constante a partir de un punto, es decir, existe un N tal que $|x_n|_p = |x_m|_p$ para todo $m, n \geq N$.*

Demostración. Como (x_n) es de Cauchy y no tiende a cero, podemos encontrar un c y un N_1 tal que $n \geq N_1 \Longrightarrow |x_n|_p \geq c > 0$.
Por otro lado, existe un N_2 tal que $n, m \geq N_2 \Longrightarrow |x_n - x_m|_p < c$.
Luego, tomando $N = \max\{N_1, N_2\}$ tenemos que

$$n, m \geq N \Longrightarrow |x_n - x_m|_p \leq c < \max\{|x_n|_p, |x_m|_p\},$$

de lo cual obtenemos que $|x_n|_p = |x_m|_p$ debido a la Proposición 1.2.3. □

El lema anterior nos da la intuición necesaria para poder definir el valor absoluto p-ádico en $\mathbb{Q}_p$.

Definición 1.3.11. *Sea $\lambda \in \mathbb{Q}_p$ y (x_n) una sucesión de Cauchy que representa a λ, entonces definimos*

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

El lema nos dice que el límite existe, pero recordemos que $\mathbb{Q}_p$ es un cociente, por lo que necesitamos probar que no depende del representante. Además necesitamos verificar que nuestra definición cumple las propiedades de un valor absoluto no arquimediano. Agrupamos todo esto en la siguiente proposición:

Proposición 1.3.12.

a) Sea $\lambda \in \mathbb{Q}_p$, luego si (x_n) e (y_n) son dos sucesiones equivalentes que representan λ, tenemos que

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

b) Sea $\lambda \in \mathbb{Q}_p$, luego $|\lambda|_p = 0$ si y solo si $\lambda = 0$.

c) $|\ |_p : \mathbb{Q}_p \longrightarrow \mathbb{R}_{\geq 0}$ es un valor absoluto no arquimediano.

d) La imagen de $|\ |_p$ sobre $\mathbb{Q}$ es igual a la imagen de $|\ |_p$ sobre $\mathbb{Q}_p$. Es decir, para todo $\lambda \in \mathbb{Q}_p$ distinto de cero, existe un $n \in \mathbb{Z}$ tal que $|\lambda|_p = p^{-n}$.

Demostración.

a) Que (x_n) e (y_n) sean dos sucesiones equivalentes, significa que $(x_n - y_n)$ es una sucesión que tiende a cero, luego

$$0 = \lim_{n\to\infty} |x_n - y_n|_p \geq \lim_{n\to\infty} |x_n|_p - |y_n|_p$$

donde en la última desigualdad estamos usando que $|\ |_p$ es un valor absoluto en $\mathbb{Q}$. Luego como ambos límites existen, tenemos lo que queremos.

b) Es claro pues $\lambda \in \mathbb{Q}_p$ es igual a cero, si y solo si (x_n) tiende a cero (dónde (x_n) es una sucesión de Cauchy que representa a λ).

c) Queda probar la propiedad multiplicativa y la desigualdad no arquimediana. Sean $\lambda, \mu \in \mathbb{Q}_p$, y (x_n) e (y_n) dos sucesiones que los representan respectivamente, luego

$$|\lambda\mu|_p = \lim_{n\to\infty} |x_n y_n|_p = \lim_{n\to\infty} |x_n|_p |y_n|_p = \lim_{n\to\infty} |x_n| \lim_{n\to\infty} |y_n| = |\lambda|_p |\mu|_p$$

donde la penúltima igualdad se cumple pues ambos límites existen.

De forma similar tenemos que

$$\begin{aligned} |\lambda + \mu|_p = \lim_{n\to\infty} |x_n + y_n|_p &\leq \lim_{n\to\infty} \text{máx}\{|x_n|_p, |y_n|_p\} \\ &= \text{máx}\{\lim_{n\to\infty} |x_n|_p, \lim_{n\to\infty} |y_n|_p\} \\ &= \text{máx}\{|\lambda|_p, |\mu|_p\}, \end{aligned}$$

donde nuevamente la penúltima igualdad se cumple pues ambos límites existen.

d) Gracias al Lema 1.3.10 sabemos que las sucesiones de valores absolutos p-ádicos son constantes a partir de un punto, por lo que el valor absoluto de un elemento $\lambda \in \mathbb{Q}_p$ coincide con el valor absoluto de algún elemento en $\mathbb{Q}$. La otra inclusión es clara pues como vimos, tomando las sucesiones constantes $\mathbb{Q} \subset \mathbb{Q}_p$ y el valor absoluto restringido a la imagen de $\mathbb{Q}$ claramente coincide con el definido originalmente sobre $\mathbb{Q}$.

□

Para verificar que efectivamente hemos obtenido una completación, debemos probar las últimas dos propiedades: que $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ y que $\mathbb{Q}_p$ es completo respecto al valor absoluto que acabamos de definir.

Proposición 1.3.13. *La imagen de $\mathbb{Q}$ bajo la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ es densa en $\mathbb{Q}_p$.*

Demostración. Necesitamos probar que cualquier bola abierta alrededor de un elemento $\lambda \in \mathbb{Q}_p$ contiene un elemento de (la imagen de) $\mathbb{Q}$, es decir una sucesión constante. Fijemos un radio ε. Sea $(x_n) \subset \mathbb{Q}$ una sucesión de Cauchy que represente a λ y sea $\varepsilon' < \varepsilon$. Por ser de Cauchy, sabemos que existe un N tal que $|x_n - x_m| < \varepsilon'$ siempre que $n, m \geq N$. Consideremos la sucesión constante $\tilde{y}$, con $y = x_N$. Queremos probar que $\tilde{y} \in B(\lambda, \varepsilon)$, es decir que $|\lambda - \tilde{y}|_p < \varepsilon$. Para esto, recordar que $\lambda - \tilde{y}$ es representado por la sucesión $(x_n - y)$, y entonces

$$|\lambda - \tilde{y}|_p = \lim_{n\to\infty} |x_n - y|_p.$$

Sabemos que para todo $n \geq N$ tenemos que

$$|x_n - y|_p = |x_n - x_N|_p < \varepsilon'$$

lo que en el límite es

$$\lim_{n\to\infty} |x_n - y|_p \leq \varepsilon' < \epsilon$$

ergo $\tilde{y} \in B(\lambda, \varepsilon)$. □

Nos queda probar que $\mathbb{Q}_p$ es completo.

Proposición 1.3.14. *$\mathbb{Q}_p$ es completo respecto a $|\ |_p$.*

Demostración. Sea $\lambda_1, \lambda_2, ..., \lambda_n, ...$ una sucesión de Cauchy de elementos de $\mathbb{Q}_p$, es decir que cada λ_i es una sucesión de Cauchy $(x_k^{(i)})$ de elementos de $\mathbb{Q}$.
Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, para cada i existe un elemento $y_i \in \mathbb{Q}$ tal que la sucesión constante $\tilde{y}_i \in \mathbb{Q}_p$ cumple que

$$|\lambda_i - \tilde{y}_i|_p < \frac{1}{i}.$$

Por lo que

$$\lim_{n\to\infty} |\lambda_n - \tilde{y}_n|_p = 0.$$

Como (λ_n) es de Cauchy, la sucesión $(\tilde{y}_n)$ es de Cauchy. Luego, como el valor absoluto de una sucesión constante es el valor absoluto de la constante, la sucesión (y_n) (una sucesión de números racionales) es de Cauchy, y por lo tanto define un elemento en $\mathbb{Q}_p$

al que llamaremos λ. Probaremos que λ es el límite de (λ_n).
Sea $\varepsilon > 0$. Como $\lambda = (y_n)$ es de Cauchy, existe un N tal que $n, m \geq N \Longrightarrow |y_m - y_n| < \frac{1}{2}\varepsilon$.
Consideremos la sucesión de sucesiones constantes $\tilde{y}_n$. El elemento $\lambda - \tilde{y}_n$ es representado por $(y_m - y_n)$, donde n está fijo y m varía. Si $n \geq N$ tenemos que

$$|\lambda - \tilde{y}_n|_p = \lim_{m\to\infty} |y_m - y_n|_p \leq \frac{1}{2}\varepsilon < \varepsilon.$$

Por lo que la sucesión $\lambda - (\tilde{y}_n)$ converge a 0 en $\mathbb{Q}_p$, o lo que es lo mismo, la sucesión de sucesiones constantes $(\tilde{y}_n)$ converge a $\lambda = (y_n)$.
Sabemos que $|\lambda_n - \tilde{y}_n|_p$ converge a cero y que $(\tilde{y}_n)$ converge a λ, luego como (λ_n) es de Cauchy converge a λ como queríamos probar. □

Con todo lo que acabamos de probar, concluimos con el siguiente teorema.

Teorema 1.3.15. *Para cada primo $p \in \mathbb{Z}$, existe un cuerpo $\mathbb{Q}_p$ con un valor absoluto no arquimediano $|\ |_p$ tal que:*

a) Existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, y el valor absoluto inducido por $|\ |_p$ en $\mathbb{Q}$ vía esta inclusión coincide con el valor absoluto p-ádico.

b) La imagen de $\mathbb{Q}$ bajo esta inclusión es densa en $\mathbb{Q}_p$ respecto al valor absoluto $|\ |_p$.

c) $\mathbb{Q}_p$ es completo respceto a este valor absoluto $|\ |_p$.

El cuerpo $\mathbb{Q}_p$ que satisface $(a), (b)$ y (c) es único salvo isomorfismos que preserven el valor absoluto.

Demostración. Ya hemos probado todo excepto la unicidad. Para esto, supongamos que tenemos otro cuerpo K que cumpla $(a), (b)$ y (c). Observar que si tenemos una sucesión de Cauchy (y_n) en $\mathbb{Q}$, luego podemos ver su imagen en $\mathbb{Q}_p$ y en K. Ambas serán sucesiones de Cauchy puesto que el valor absoluto no cambia. Teniendo esto en mente construiremos el isomorfismo entre estos dos cuerpos.
Sea $\lambda \in \mathbb{Q}_p$. Como $\mathbb{Q}$ es denso, existe una sucesión de Cauchy (y_n) con $y_n \in \mathbb{Q}$ cuyo límite es λ. Como los $y_n \in \mathbb{Q}$, podemos tomar sus imágenes en K, como el valor absoluto se preserva, esta será una sucesión de Cauchy en K y como K es completo esta sucesión converge a un elemento al que llamaremos $f(\lambda)$. Esto define una función $\mathbb{Q} \longrightarrow K$, que queremos probar es el isomorfismo buscado.
Como las operaciones son continuas es claro que f es un morfismo de cuerpos. Para probar que es una biyección, primero probaremos que f es continua.
Observar que el valor absoluto es continuo ya que $|a - b| \geq ||a| - |b||$. Luego f preserva el valor absoluto:

$$|f(\lambda)|^{(K)} = |\lim y_n|^{(K)} = \lim |y_n|^{(K)} = \lim |y_n|^{(\mathbb{Q}_p)} = |\lambda|^{(\mathbb{Q}_p)}.$$

Para probar continuidad, supongamos $x \in \mathbb{Q}_p$ y una sucesión $(x_n) \subset \mathbb{Q}_p$ tal que $x_n \to x$. Queremos probar que $f(x_n) \to f(x)$.
Recordar que como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ para todo n existe una sucesión $(x_n^j) \subset \mathbb{Q}$ tal que

$x_n = \lim_j x_n^j$.

Afirmación: existe una subsucesión (c_n) de $\mathbb{Z}$ tal que $\lim_n x_n^{c_n} = x$.

Demostración: Dado n, tomamos c_n tal que $c_n > c_{n-1}$ y que

$$|x_n^j - x_n| < \frac{1}{n} \qquad \forall\, j \geq c_n$$

Luego,

$$|x_n^{c_n} - x| \leq |x_n^{c_n} - x_n| + |x_n - x| \leq \frac{1}{n} + |x_n - x| \underset{n\to\infty}{\longrightarrow} 0.$$

Ahora que tenemos esta sucesión (c_n), sabemos que $f(x) = \lim_n x_n^{c_n} \in K$ por definición de $f(x)$. Recordar que queremos probar que $\lim_n f(x_n) = f(x)$. Pero ahora esto es claro pues:

$$\begin{aligned} |f(x_n) - f(x)|^K &\leq |f(x_n) - x_n^{c_n}|^K + |f(x) - x_n^{c_n}|^K = |f(x_n - x_n^{c_n})|^K + |f(x - x_n^{c_n})|^K \\ &= |x_n - x_n^{c_n}|^{\mathbb{Q}_p} + |x - x_n^{c_n}|^{\mathbb{Q}_p} \underset{n\to\infty}{\longrightarrow} 0 \end{aligned}$$

Donde en la primera igualdad usamos que f es un morfismo y en la segunda usamos que f preserva valor absoluto.
Una vez que tenemos que f es continua, si realizamos la construcción de forma análoga en el otro sentido, tenemos una función $g : K \longrightarrow \mathbb{Q}_p$ que de forma análoga se prueba que cumple las mismas propiedades que f, es decir, es un morfismo, respeta el valor absoluto, es continua y es la identidad si nos restringimos a la imagen de $\mathbb{Q}$ en K. Por último , f es biyectiva pues $g \circ f$ y $f \circ g$ son funciones continuas que restrictas a $\mathbb{Q}$ dan la identidad y como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ y en K, deben de ser la identidad. $\square$

Capítulo 2

Propiedades fundamentales de $\mathbb{Q}_p$

2.1 Enteros p-ádicos

Definición 2.1.1. *Sea $\Bbbk$ un cuerpo y $|\ |$ un valor absoluto no aquimediano en $\Bbbk$. Al subanillo*

$$\mathcal{O} = \mathcal{O}_{\Bbbk} := \overline{B}(0,1) = \{x \in \Bbbk : |x| \leq 1\} \subset \Bbbk$$

le llamaremos el anillo de valuación de $|\ |$. Al ideal maximal de $\mathcal{O}$

$$\mathfrak{p} = \mathfrak{p}_{\Bbbk} := B(0,1) = \{x \in \Bbbk : |x| < 1\} \subset \mathcal{O}$$

le llamaremos el ideal de valuación de $|\ |$. Al cociente:

$$\kappa = \mathcal{O}/\mathfrak{p}$$

le llamaremos el cuerpo residual o de residuos de $|\ |$.

Observación 2.1.2. *Todo elemento de $\mathcal{O} - \mathfrak{p}$ es invertible en $\mathcal{O}$ pues tiene valor absoluto igual a uno.*

Definición 2.1.3. *El anillo de enteros p-ádicos es el anillo de valuación*

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

Proposición 2.1.4. *El anillo $\mathbb{Z}_p$ de enteros p-ádicos es un anillo local cuyo único ideal maximal es el ideal principal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Más aún:*

a) $\mathbb{Q} \ \cap \ \mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q} : (a,b) = 1,\ p \nmid b\}$.

b) La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene imagen densa. Específicamente, dado $x \in \mathbb{Z}_p$ y $n \geq 1$, existe un $\alpha \in \mathbb{Z}$, $0 \leq \alpha \leq p^n - 1$, tal que $|x - \alpha|_p \leq p^{-n}$. Además este entero α es único.

c) Para todo $x \in \mathbb{Z}_p$, existe una sucesión de Cauchy (α_n) que converge a x y cumple lo siguiente:

- *$\alpha_n \in \mathbb{Z}$ y cumple que $0 \leq \alpha_n \leq p^n - 1$*
- *para todo $n \geq 2$ se cumple que $\alpha_n \equiv \alpha_{n-1}$ $(mod\ p^{n-1})$.*

La sucesión (α_n) con estas propiedades es única.

DEMOSTRACIÓN. Para comenzar, $\mathbb{Z}_p$ es un anillo de valuación y por la Observación 2.1.2 es un anillo local. Para ver que el ideal de valuación es generado por p, simplemente notar que si $|x|_p < 1$ entonces $|x|_p \leq \frac{1}{p}$ (debido a la Proposición 1.3.12), luego como $|p|_p = 1/p$, tenemos que $\left|\frac{x}{p}\right|_p \leq 1$ y por lo tanto $x \in p\mathbb{Z}_p$ pues $x = p \cdot \frac{x}{p}$. Esto prueba que el ideal de valuación está contenido en $p\mathbb{Z}_p \neq \mathbb{Z}_p$, luego como el ideal de valuación es maximal tenemos la igualdad.
Probemos la siguientes afirmaciones:

a) Es claro pues $\mathbb{Q} \cap \mathbb{Z}_p = \{x \in \mathbb{Q} : |x|_p \leq 1\}$ que es justamente el conjunto descrito.

b) Sea $x \in \mathbb{Z}_p$ y $n \geq 1$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, podemos encontrar un racional a/b tal que
$$\left|x - \frac{a}{b}\right|_p \leq p^{-n} < 1.$$
La idea es probar que en realidad podemos elegir un entero.
Notemos que para a/b como antes tenemos que
$$\left|\frac{a}{b}\right|_p \leq \text{máx}\left\{|x|_p\ , \left|x - \frac{a}{b}\right|_p\right\} \leq 1$$
lo que nos dice que $a/b \in \mathbb{Q} \cap \mathbb{Z}_p$, es decir que $p \nmid b$. Entonces b es coprimo con p, y en particular con p^n, luego existe un entero $c \in \mathbb{Z}$ único módulo p^n tal que $bc \equiv 1$ $(mod\ p^n)$. Por lo tanto puesto que $a - abc \equiv 0$ $(mod\ p^n)$ tenemos que
$$\left|\frac{a}{b} - ac\right|_p \leq p^{-n},$$
donde claramente $ac \in \mathbb{Z}$. Luego basta tomar α como el único entero tal que
$$0 \leq \alpha \leq p^n - 1 \qquad \text{y} \qquad \alpha \equiv ac\ (mod\ p^n).$$
Para la unicidad, supongamos que existen $0 \leq \alpha, \alpha' \leq p^n - 1$, tal que $|x - \alpha|_p \leq p^{-n}$ y $|x - \alpha'|_p \leq p^{-n}$, luego
$$|\alpha - \alpha'|_p \leq \text{máx}\left\{|x - \alpha|_p\ ,\ |x - \alpha'|_p\right\} \leq p^{-n} \Rightarrow \alpha \equiv \alpha'\ (mod\ p^n) \Rightarrow \alpha = \alpha'.$$

c) Sigue directamente de aplicar (b) a la sucesión de enteros $n = 1, 2, ...$, para la unicidad, notar que en cada paso la elección es única módulo p^n. Por último,

supongamos que tenemos los α_n definidos a partir de (b), es decir que $|x-\alpha_n|_p \leq p^{-n}$ y que $|x-\alpha_{n-1}|_p \leq p^{-(n-1)}$, luego

$$|\alpha_n - \alpha_{n-1}|_p \leq \max\{|\alpha_n - x|_p\ ,\ |x-\alpha_{n-1}|_p\} \leq p^{-(n-1)} \Rightarrow \alpha_n \equiv \alpha_{n-1}\ (mod\ p^{n-1}).$$

□

Corolario 2.1.5. *$\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, es decir, $\forall\ x \in \mathbb{Q}_p$, existe $n \geq 0$ tal que $p^n x \in \mathbb{Z}_p$. El mapa $\mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ dado por $x \mapsto px$ es un homeomorfismo. La familia de conjuntos de la forma $p^n\mathbb{Z}_p$, $n \in \mathbb{Z}$ es una familia fundamental de entornos de $0 \in \mathbb{Q}_p$, es decir que para todo entorno U del 0 existe un n tal que $p^n\mathbb{Z} \subset U$. Además, esta familia cubre todo $\mathbb{Q}_p$.*

Demostración. Sea $x \in \mathbb{Q}_p$, si $x = 0$ es claro pues $0 \in \mathbb{Z}_p$, en otro caso, existe un n_0 tal que $|x|_p = p^{-n_0}$, luego si $n \geq n_0$, $|xp^n|_p = |x|_p p^{-n} \leq p^{-n_0}p^n = 1$, por lo que $xp^n \in \mathbb{Z}_p$.
Que la familia cubre $\mathbb{Q}_p$ se deduce fácilmente de lo anterior ya que si $p^n x \in \mathbb{Z}_p$, entonces $x \in p^{-n}\mathbb{Z}_p$ y esto vale para todo $x \in \mathbb{Q}_p$. La multiplicación por p es claramente un homeomorfismo pues las operaciones del cuerpo son funciones continuas y la inversa de multiplicar por p es simplemente multiplicar por $1/p$ que es continua por la misma razón. Para la última parte, sea U un entorno del 0, luego existe un $r > 0$ tal que $B(0,r) \subset U$. Finalmente, basta tomar n suficientemente grande tal que $p^{-n} < r$ ya que luego $p^n\mathbb{Z}_p \subset B(0,r)$ y los $p^n\mathbb{Z}_p$ son abiertos ya que $\mathbb{Z}_p$ es abierto y multiplicar por p es un homeomorfismo. □

Este último corolario nos permite dar una definición natural de $v_p(x)$: Sea n_0 el entero más grande tal que $x \in p^{n_0}\mathbb{Z}_p$, luego definimos $v_p(x) := n_0$. Es claro por el corolario que $|x| = p^{-v_p(x)}$.

Corolario 2.1.6. *Para todo $n \geq 1$, la siguiente sucesión de grupos es exacta*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\pi} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

donde el mapa p^n es el mapa $x \mapsto p^n x$ y el mapa π es tal que $x \mapsto \alpha$ dónde α es el único entero que cumple que $0 \leq \alpha \leq p^n - 1$ y $|x-\alpha| \leq p^{-n}$. Además los mapas son continuos (donde le damos a $\mathbb{Z}/p^n\mathbb{Z}$ la topología discreta). En particular

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Demostración. Tenemos que probar varias cosas:

- el mapa p^n es inyectivo: $p^n x = 0 \Rightarrow x = 0$, por lo que efectivamente es inyectivo.

- el mapa π es morfismo de grupos sobreyectivo: $\pi(0) = 0$ ya que la imagen de un entero es el propio entero módulo p^n. Esta última afirmación nos prueba trivialmente que el mapa π es sobreyectivo.
  Sean a y b dos elementos en $\mathbb{Z}_p$, queremos probar que $\pi(a+b) \equiv \pi(a) +$

$\pi(b)$ $(mod\ p^n)$. Por definición de π, sabemos que

$$|a+b-\pi(a+b)|_p \leq p^{-n} \qquad y \qquad |a+b-\pi(a)-\pi(b)|_p \leq p^{-n}.$$

Luego

$$|\pi(a+b)-\pi(a)-\pi(b)|_p \leq \text{máx}\left\{|\pi(a+b)-a-b|_p\ ,\ |a+b-\pi(a)-\pi(b)|_p\right\} \leq p^{-n},$$

lo que nos dice que $\pi(a+b) \equiv \pi(a)+\pi(b)$ $(mod\ p^n)$ como queríamos probar.

- que $ker(\pi) = p^n\mathbb{Z}_p$: sabemos que $\pi(x) = 0 \iff |x-0|_p = |x|_p \leq p^{-n} \iff x \in p^n\mathbb{Z}$, por lo que $x \in ker(\pi) \iff x \in p^n\mathbb{Z}_p$.

- ya sabemos que el mapa p^n es continuo así que solamente habría que probar que π es continuo: pero π es claramente continuo pues

$$\pi^{-1}(\alpha) = \{x : |x-\alpha|_p \leq p^{-n}\} = \overline{B}(\alpha, p^{-n})$$

que es abierto.

□

Corolario 2.1.7. *$\mathbb{Z}_p$ es compacto y $\mathbb{Q}_p$ es localmente compacto, es decir, todo $x \in \mathbb{Q}_p$ tiene un entorno compacto.*

Demostración. Como $\mathbb{Z}_p$ es un entorno del cero, si probamos que es compacto ya estamos, pues dado $x \in \mathbb{Q}_p$, $x + \mathbb{Z}_p$ será un entorno compacto de x ya que las operaciones son continuas.

Recordar de topología que en un espacio métrico, un conjunto X es compacto si y solo si es completo y totalmente acotado (para todo $\varepsilon > 0$, existe un cubrimiento finito de X por bolas de radio ε).

Ya sabemos que $\mathbb{Z}_p$ es completo pues es un cerrado en $\mathbb{Q}_p$, por lo que solamente queda probar que es totalmente acotado. Es suficiente verificar esta propiedad para todo $\varepsilon = p^{-n}$, $n \geq 0$. Pero recordemos que $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ y que las coclases de $p^n\mathbb{Z}_p$ en $\mathbb{Z}_p$ son bolas de la topología p-ádica. Es decir, que si a varía entre $0, 1, ..., p^n - 1$, las p^n bolas

$$a + p^n\mathbb{Z}_p = \{a + p^n x : x \in \mathbb{Z}_p\} = \{y \in \mathbb{Z}_p : |y-a|_p \leq p^{-n}\} = \overline{B}(a, p^{-n})$$

cubren $\mathbb{Z}_p$.

□

Definición 2.1.8. *Llamaremos a los elementos invertibles de $\mathbb{Z}_p$, las unidades p-ádicas o simplemente unidades. Notaremos a este conjunto como $\mathbb{Z}_p^\times$*

Observación 2.1.9. *Como $x \in \mathbb{Z}_p$ significa que $|x| \leq 1$ y si x es una unidad, entonces $x^{-1} \in \mathbb{Z}_p$, por ende:*

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

Luego

$$\mathbb{Z}_p^\times \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid ab \right\}.$$

Por último, notar que $\mathbb{Z}_p^\times = \overline{B}(0,1) \cap B(0,1)^c$ ambos cerrados, entonces es un cerrado de $\mathbb{Z}_p$ y por ende es compacto.

Hasta este momento los elementos de $\mathbb{Q}_p$ son difíciles de manejar pues solamente conocemos $\mathbb{Q}_p$ vía sus propiedades. Por eso a continuación, daremos una descripción más tangible de los elementos de $\mathbb{Q}_p$.

Comenzamos con la parte (c) de la Proposición 2.1.4, que nos dice que dado un $x \in \mathbb{Z}_p$, podemos encontrar una única sucesión de Cauchy que converge a x que cumple las siguientes propiedades:

- $\alpha_n \in \mathbb{Z}$, $0 \leq \alpha_n \leq p^n - 1$
- $\alpha_{n+1} \equiv \alpha_n \ (mod\ p^n)$.

Por otro lado, si tenemos una sucesión que cumple las anteriores propiedades (α_n), entonces es una sucesión de Cauchy, pues $|\alpha_{n+1} - \alpha_n| \leq p^{-n}$ gracias a la segunda propiedad. Por lo tanto, como $\mathbb{Z}_p$ es completo, converge.
Es decir que podemos identificar los elementos de $\mathbb{Z}_p$ como una sucesión que cumpla estas propiedades.

Escribamos los α_n en base p. Observar que la condición $\alpha_{n+1} \equiv \alpha_n \ (mod\ p^n)$ nos dice que los últimos dígitos de ambos números son los mismos escritos en base p. Por lo que obtenemos algo así:

$$\begin{aligned} \alpha_1 &= b_0 & 0 \leq b_0 \leq p-1 \\ \alpha_2 &= b_0 + b_1 p & 0 \leq b_1 \leq p-1 \\ \alpha_3 &= b_0 + b_1 p + b_2 p^2 & 0 \leq b_2 \leq p-1 \end{aligned}$$

y siguiendo para todo n. Lo anterior puede ser visto como las sumas parciales de una serie, entonces obtenemos el siguiente lema.

Lema 2.1.10. *Dado $x \in \mathbb{Z}_p$, la serie*

$$b_0 + b_1 p + b_2 p^2 + ... + b_n p^n + ...$$

obtenida como antes, converge a x, es decir,

$$x = b_0 + b_1 p + b_2 p^2 + ...$$

DEMOSTRACIÓN. Recordar que una serie converge a x si y solo si sus sumas parciales convergen a x. Pero las sumas parciales de nuestra serie son exactamente los α_n que ya sabemos que convergen a x. □

Dejamos asentado lo anterior en la siguiente proposición.

Proposición 2.1.11. *Todo $x \in \mathbb{Z}_p$ puede ser escrito de la forma*

$$x = b_0 + b_1 p + b_2 p^2 + ... + b_n p^n + ..$$

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

DEMOSTRACIÓN. Lo único que queda por probar es la unicidad, pero esta es clara pues los α_n eran únicos y por lo tanto los b_n también. □

Corolario 2.1.12. *Todo $x \in \mathbb{Q}_p$ puede ser escrito de la forma*

$$x = b_{-m}p^{-m} + ... + b_{-1}p^{-1} + b_0 + b_1 p + b_2 p^2 + ... + b_n p^n + ... = \sum_{n \geq -m} b_n p^n$$

con $0 \leq b_n \leq p-1$, $b_{-m} \neq 0$ y $-m = v_p(x)$. Además, esta representación es única.

DEMOSTRACIÓN. Recordar que todo elemento de $\mathbb{Q}_p$ puede ser escrito de la forma $p^m y$ con $y \in \mathbb{Z}_p^\times$ y $m \in \mathbb{Z}$. Luego, si expresamos y como una serie de potencias en p y multiplicamos por p^m obtenemos una serie de potencias donde algunos términos pueden ser negativos. La unicidad de esta representación viene del hecho de que la representación de y es única.
El enunciado sobre $v_p(x)$, es claro pues

$$x = p^{-m}(b_{-m} + b_{-m+1}\ p\ + b_{-m+2}\ p^2\ + ...) \in p^{-m}\mathbb{Z}_p$$

pero $x \notin p^{-m+1}\mathbb{Z}_p$ pues a la suma no le queda ningún factor p, por ende $-m = v_p(x)$.
□

Ahora que ya sabemos como representar a los elementos de $\mathbb{Q}_p$, antes de pasar a la siguiente sección, veremos una última propiedad topológica que cumplen los $\mathbb{Q}_p$ que nos hará darnos cuenta (si todavía no lo habíamos hecho) que tienen una geometría muy diferente a la usual.
Para esto recordemos un teorema de topología:

Teorema 2.1.13. *Todo espacio métrico no vacío compacto, perfecto y totalmente disconexo es homeomorfo al conjunto de Cantor.*

Corolario 2.1.14. *$\mathbb{Z}_p$ es homeomorfo al conjunto de Cantor para todo primo p.*

DEMOSTRACIÓN. Ya han sido probadas todas las condiciones del Teorema 2.1.13. □

2.2 Lema de Hensel

Definición 2.2.1. *Sea $F(X) = a_0+a_1X+a_2X^2+...+a_nX^n$ un polinomio con coeficientes $a_i \in R$, donde R es un anillo con unidad. La derivada formal de $F(X)$ es*

$$F'(X) = a_1 + 2a_2X + ... + na_nX^{n-1}.$$

Teorema 2.2.2 (Lema de Hensel)**.** *Sea $F(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ un polinomio con coeficientes en $\mathbb{Z}_p$. Supongamos que existe un entero p-ádico $\alpha_1 \in \mathbb{Z}_p$ tal que*

$$F(\alpha_1) \equiv 0 \ (mod\ p\mathbb{Z}_p)$$

y

$$F'(\alpha_1) \not\equiv 0 \ (mod\ p\mathbb{Z}_p)$$

donde $F'(X)$ es la derivada formal de $F(X)$. Entonces existe un único entero p-ádico $\alpha \in \mathbb{Z}_p$ tal que $\alpha \equiv \alpha_1 \ (mod\ p\mathbb{Z}_p)$ y $F(\alpha) = 0$.

Demostración. La idea para probar que la raíz α existe, es construir una sucesión de Cauchy de enteros que converja a una raíz.
Construiremos una sucesión de enteros p-ádicos $\alpha_1, \alpha_2, .., \alpha_n, ...$ tal que para todo $n \geq 1$ se cumpla que

a) $F(\alpha_n) \equiv 0 \ (mod\ p^n)$

b) $\alpha_{n+1} \equiv \alpha_n \ (mod\ p^n)$

Como ya hemos visto, la condición (b) nos asegurará que la sucesión es de Cauchy y que por lo tanto converge. Su límite α cumplirá por construcción que $\alpha \equiv \alpha_1 \ (mod\ p)$. Como los polinomios son funciones continuas (pues son una combinación finita de las operaciones del anillo), y gracias a la condición (a) tenemos que $|F(\alpha_n)|_p \leq p^{-n}$, pasando al límite obtenemos que $|F(\alpha)|_p \leq 0$ y esto pasa si y solo si $F(\alpha) = 0$ como queríamos probar. Recíprocamente, una raíz α determinará una sucesión α_n que cumpla (a) y (b) (simplemente tomando sus sumas parciales). Por lo tanto, solo nos queda construir la sucesión α_n y el teorema estará probado.

Por hipótesis del teorema, partimos con α_1, notar que si queremos que α_2 cumpla (b) , entonces

$$\alpha_2 = \alpha_1 + b_1p$$

para algún $b_1 \in \mathbb{Z}_p$. Si sustituimos esta expresión en el polinomio $F(X)$ y hacemos la «expansión de Taylor», obtenemos lo siguiente:

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1 p) \\ &= F(\alpha_1) + F'(\alpha_1) b_1 p + \text{términos en } p^2 \\ &\equiv F(\alpha_1) + F'(\alpha_1) b_1 p \pmod{p^2} \end{aligned}$$

Para probar que podemos encontrar α_2 que cumpla lo pedido, basta con probar que podemos encontrar b_1 tal que

$$F(\alpha_1) + F'(\alpha_1) b_1 p \equiv 0 \ (mod\ p^2).$$

Sabemos que $F(\alpha_1) \equiv 0 \ (mod\ p)$, es decir $F(\alpha_1) = px$ para algún $x \in \mathbb{Z}_p$. Sustituyendo, tenemos que

$$px + F'(\alpha_1) b_1 p \equiv 0 \ (mod\ p^2),$$

que dividiendo por p nos queda

$$x + F'(\alpha_1) b_1 \equiv 0 \ (mod\ p)$$

que como $F'(\alpha_1)$ no es divisible por p, existe una única solución para b_1 módulo p que es:

$$b_1 \equiv -x(F'(\alpha_1))^{-1} \pmod{p}.$$

Podemos tomar $b_1 \in \mathbb{Z}$ tal que $0 \leq b_1 \leq p-1$ y entonces b_1 es único. Entonces, para este b_1 encontrado, definimos $\alpha_2 = \alpha_1 + b_1 p$.
Acabamos de probar como construir α_2 dado α_1, pero el mismo proceso nos sirve para construir α_n dado α_{n-1}. Por lo tanto construimos la sucesión que cumple (a) y (b), y es única pues en cada paso la elección de los b_n es única.

□

Notando que en cada paso suponemos que α_{n+1} es de la forma $\alpha_n + p^n b_n$ y que $F(\alpha_n) = p^n x$ para luego despejar $b_n = x(F'(\alpha_n))^{-1}$ [1]. Luego, si juntamos todo:

$$\alpha_{n+1} = \alpha_n - p^n \frac{F(\alpha_n)}{p^n} (F'(\alpha_n))^{-1} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)}.$$

[1] Notar que $F'(\alpha_n) \neq 0$ pues $F'(\alpha_n) \equiv F'(\alpha_1) \not\equiv 0 \pmod{p}$.

Por lo que podemos escribir el Lema de Hensel de esta otra forma (similar al Método de Newton de aproximación de raíces):

Teorema 2.2.3 (Lema de Hensel)**.** *Sea $F(X) = a_0 + a_1X + ... + a_nX^n$ un polinomio con coeficientes en $\mathbb{Z}_p$. Supongamos que existe un entero p-ádico $\alpha_1 \in \mathbb{Z}_p$ tal que $|F(\alpha_1)|_p < 1$ y $|F'(\alpha_1)|_p = 1$. Entonces definiendo para cada $n \geq 1$*

$$\alpha_{n+1} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)},$$

obtenemos una sucesión convergente cuyo límite $\alpha \in \mathbb{Z}_p$ es el único entero p-ádico tal que $|\alpha - \alpha_1|_p < 1$ y $F(\alpha) = 0$.

Veamos una forma del Lema de Hensel con las hipótesis un poco debilitadas que nos será útil en algunos casos en los cuales no podamos aplicar directamente la primera versión.

Teorema 2.2.4 (Lema de Hensel 2)**.** *Sea $F(X) \in \mathbb{Z}_p[X]$ y supongamos que existe un $\alpha_0 \in \mathbb{Z}_p$ tal que*

$$|F(\alpha_0)|_p < |F'(\alpha_0)|_p^2.$$

Entonces, existe $\alpha \in \mathbb{Z}_p$ tal que $F(\alpha) = 0$.

Demostración. Recordemos que por la expansión de Taylor de F, tenemos la siguiente identidad:

$$F(X + Y) = F(X) + F_1(X)Y + F_2(X)Y^2 + ...$$

donde $F_1 = F'$ y $F_j(X) \in \mathbb{Z}_p[X]$.

Por otro lado, observar que $-F(\alpha_0)/F'(\alpha_0) \in \mathbb{Z}_p$ ya que en caso contrario tendríamos que

$$1 > \frac{|F(\alpha_0)|_p}{|F'(\alpha_0)|_p^2} > \frac{1}{|F'(\alpha_0)|_p} \geq 1$$

lo que sería absurdo.
Luego, sustituyendo $X = \alpha_0$ e $Y = d = -F(\alpha_0)/F'(\alpha_0)$ lo cual anula los términos lineales en Y, obtenemos

$$\begin{aligned} |F(\alpha_0 + d)|_p &\leq \max_{j \geq 2} |F_j(\alpha_0)d^j|_p \\ &\leq |d|_p^2 \\ &= \frac{|F(\alpha_0)|_p^2}{|F'(\alpha_0)|_p^2} \\ &< |F(\alpha_0)|_p \end{aligned}$$

donde la última desigualdad es gracias a la hipótesis.
Realizando la «expansión de Taylor» pero ahora para $F'(X)$ y sustituyendo nuevamente $X = \alpha_0$ e $Y = d$, obtenemos

$$|F'(\alpha_0 + d) - F'(\alpha_0)|_p \leq |d| < |F'(\alpha_0)|_p,$$

donde nuevamente, la última desigualdad es gracias a la hipótesis. Por lo tanto, gracias a la Proposición 1.2.3 tenemos que

$$|F'(\alpha_0 + d)|_p = |F'(\alpha_0)|_p.$$

Construimos ahora la sucesión que va a tender a α de la siguiente forma :

$$\begin{aligned} d_j &= -F(\alpha_j)/F'(\alpha_j) \\ \alpha_{j+1} &= \alpha_j + d_j. \end{aligned}$$

Luego, por la cuenta anterior, tenemos que $|F'(\alpha_j)|_p = |F'(\alpha_0)|_p$ para todo j. También tenemos que

$$|F(\alpha_0)|_p > |F(\alpha_1)|_p > |F(\alpha_2)|_p > ...$$

Por lo tanto $d_j \to 0$ p-adicamente y entonces los α_j convergen a un límite $\alpha \in \mathbb{Z}_p$ (pensar que $\alpha = \alpha_0 + \sum_{n\geq 0}^{\infty} d_j$ y aplicar el Corolario 2.3.1).

Finalmente, por la cadena de desigualdades anterior y usando que tenemos un valor absoluto discreto, tenemos que $F(\alpha_j) \to 0$, ergo $F(\alpha) = 0$ como queríamos probar. □

Un ejemplo en donde la versión dos es necesaria, es la ecuación $X^2 - 17$, cuya derivada es $2X$ y por lo tanto nunca satisface la condición $F'(\alpha_1) \neq 0$ $(mod\ 2)$. Pero si tomamos $\alpha_1 = 1$, vemos que $|F(\alpha_1)| = 2^{-4}$ y que $|F'(\alpha_1)| = 2^{-1}$, por lo tanto por la versión dos, podemos concluir que $X^2 - 17$ tiene raíces en $\mathbb{Q}_2$.

A continuación, veremos dos aplicaciones del Lema de Hensel. En la primera veremos cuáles raíces de la unidad existen en $\mathbb{Q}_p$ y en la segunda encontraremos todos los cuadrados en $\mathbb{Q}_p$.

Recordemos que un elemento ζ en un cuerpo es una m-ésima raíz de la unidad si $\zeta^m = 1$; y es una m-ésima raíz primitiva de la unidad si además cumple que $\zeta^n \neq 1$ para $0 < n < m$.
Antes de comenzar, observar que una raíz de la unidad siempre tiene valor absoluto igual a 1 ya que $|\zeta|^m = |\zeta^m| = 1$.

Proposición 2.2.5. *Para todo primo p y cualquier entero m no divisible por p existe una raíz m-ésima primitiva de la unidad en $\mathbb{Z}_p$ si y solo si m divide a $p - 1$.*

Demostración. Recordemos que el conjunto de enteros invertibles módulo p es un grupo cíclico de orden $p-1$. Sea g un generador. Si $m \mid p-1$, entonces $g^{(p-1)/m}$ es un elemento de orden m y además genera el grupo cíclico de elementos de orden m. Entonces, para cada m que divide a $p-1$, podemos encontrar m raíces distintas (no congruentes entre sí) de $X^m - 1 \equiv 0 \ (mod\ p)$, y por lo tanto, por el Lema de Hensel, pues para esas m raíces módulo p no se anula mX^{m-1}, tenemos entonces m raíces diferentes de $X^m - 1$ en $\mathbb{Z}_p$, las cuales son las m raíces de la unidad.
Nos queda probar que no hay otras raíces de la unidad aparte de la descritas anteriormente.
Supongamos que existe $\zeta \in \mathbb{Z}_p$ tal que $\zeta^k = 1$ y que $p \nmid k$. Luego, en particular $\zeta^k \equiv 1 \ (mod\ p)$. Entonces si m es el orden de ζ en el grupo, se cumple que $\zeta^m \equiv 1 \ (mod\ p)$ y $m \mid p-1$. Por el Lema de Hensel, existe un único $\zeta_1 \equiv \zeta \ (mod\ p)$ tal que $\zeta_1^m = 1$. Pero como m divide a k, ζ_1 es raíz de $X^k - 1$, y es congruente mod p con ζ. Por lo tanto, por la unicidad del Lema de Hensel, $\zeta_1 = \zeta$, por lo que ζ es una raíz m-ésima primitiva de la unidad con m dividiendo a $p-1$.

□

Notar que si m divide a $p-1$, entonces las m-ésimas raíces de la unidad también son $(p-1)$-ésimas raíces de la unidad, por lo tanto, a la luz de la proposición anterior, concluimos que las raíces de la unidad en $\mathbb{Q}_p$ de orden coprimo con p son exactamente las raíces $(p-1)$-ésimas de la unidad. Esto determina todas las raíces de la unidad en $\mathbb{Q}_p$ excepto posiblemente las p^n-ésimas raíces de la unidad. Probaremos más adelante en la Sección 2.3 que no existen en $\mathbb{Q}_p$ excepto cuando $p = 2$ donde solamente tendremos las triviales $1, -1$.

Veamos la segunda aplicación y determinemos los cuadrados en $\mathbb{Q}_p$.

Proposición 2.2.6. *Sea $p \neq 2$ primo, y sea $b \in \mathbb{Z}_p^\times$. Si existe $\alpha_1 \in \mathbb{Z}_p$ tal que $\alpha_1^2 \equiv b \ (mod\ p\mathbb{Z}_p)$, entonces b es el cuadrado de un elemento de $\mathbb{Z}_p^\times$.*

Demostración. Aplicamos el Lema de Hensel al polinomio $X^2 - b$ pues como $p \neq 2$ y $b \in \mathbb{Z}_p^\times$, $2\alpha_1 \not\equiv 0 \ (mod\ p)$. □

Luego extendemos el resultado a $\mathbb{Q}_p^\times$ notando que podemos escribir a cualquier elemento $x \in \mathbb{Q}_p^\times$ como $x = p^{v_p(x)}x'$ con $x' \in \mathbb{Z}_p^\times$. Por lo tanto, como mencionamos en el siguiente resultado, x es un cuadrado en $\mathbb{Q}_p^\times$ si $v_p(x)$ es par y x' es un cuadrado en $\mathbb{Z}_p^\times$.

Corolario 2.2.7. *Sea $p \neq 2$ primo. Entonces $x \in \mathbb{Q}_p$ es un cuadrado si y solo si puede ser escrito de la forma $x = p^{2n}y^2$ con $n \in \mathbb{Z}$ e $y \in \mathbb{Z}_p^\times$. El grupo cociente $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ tiene orden cuatro. Si $c \in \mathbb{Z}_p^\times$ es un elemento cuya reducción módulo p no es un cuadrado, entonces el conjunto $\{1, p, c, cp\}$ es un sistema completo de representantes del cociente.*

Demostración. La primera parte es el párrafo anterior.
La afirmación que clarifica la segunda parte es la siguiente:

Afirmación: Dado $x,\ y \in \mathbb{Z}_p^\times$ no cuadrados, entonces xy^{-1} es cuadrado.

Demostración: Por la Proposición 2.2.6 basta ver que el residuo de xy^{-1} es cuadrático módulo p. Sean a y b los residuos de x e y módulo p respectivamente. Luego, sabemos que a y b no son cuadrados módulo p, por lo que

$$\left(\frac{a}{p}\right) = -1 \qquad \text{y} \qquad \left(\frac{b}{p}\right) = \left(\frac{b^{-1}}{p}\right) = -1,$$

donde $\left(\frac{\cdot}{p}\right)$ es el símbolo de Legendre. Luego, como el símbolo de Legendre es multiplicativo, tenemos que

$$\left(\frac{ab^{-1}}{p}\right) = 1$$

por lo que ab^{-1} es cuadrado módulo p.

Una vez que tenemos esto, y recordando que dado $x \in \mathbb{Q}_p^\times$ puede ser escrito como $x = p^{v_p(x)}x'$, por la parte anterior, tenemos que x es cuadrado si y solo si $v_p(x)$ es par y $x' = z^2$ para algún $z \in \mathbb{Z}_p^\times$, con lo que tomando cociente por esto, tenemos las siguientes opciones:

- $v_p(x)$ es par y x' es cuadrado en $\mathbb{Z}_p^\times$, por lo que x está en la clase del 1.
- $v_p(x)$ es par y x' no es cuadrado, por lo que x está en la misma clase que x' que al no ser cuadrado y gracias a la Afirmación, está en la misma clase que el c no cuadrado escogido.
- $v_p(x)$ es impar y x' es cuadrado, por lo que x está en la clase de p.
- $v_p(x)$ es impar y x' no es cuadrado, luego x está en la clase de px' que nuevamente gracias a la afirmación, sabemos que está en la clase de pc.

□

Para $p = 2$ necesitaremos usar la segunda versión del Lema de Hensel, pues $F'(\alpha_1) = 2\alpha_1$ siempre es 0 módulo 2. Entonces surje la siguiente proposición.

Proposición 2.2.8. *$b \in \mathbb{Z}_2^\times$ es un cuadrado en $\mathbb{Z}_2$ si y solo si $b \equiv 1 \ (mod\ 8\mathbb{Z}_2)$.*

Demostración. Supongamos $b \equiv 1 \ (mod\ 8)$, queremos probar que el polinomio $F(X) = X^2 - b$ tiene raíces en $\mathbb{Z}_p$. Como dijimos anteriormente, apliquemos el Lema de Hensel 2. Si tomamos $\alpha_1 = 1$, tenemos que $F(1) = 1^2 - b \equiv 0 \ (mod\ 8)$ es decir $|F(1)|_2 \leq 2^{-3}$. Por otro lado, evaluando en la derivada tenemos que $F'(1) = 2$, entonces $|F'(1)|_2 = 2^{-1}$, luego aplicando el Lema de Hensel tenemos que F tiene raíces y por ende b es cuadrado.

Ahora supongamos $b \in (\mathbb{Z}_2^\times)^2$, entonces $b = (1 + 2x)^2$ para algún $x \in \mathbb{Z}_2$, entonces $b = 1 + 4(x + x^2)$. Pero como estamos en $\mathbb{Z}_2$ tenemos dos opciones, $x \equiv 1 \ (mod\ 2)$ ó $x \equiv 0 \ (mod\ 2)$, en cualquiera de lo casos tenemos que $x + x^2 \equiv 0 \ (mod\ 2)$, por lo que $b = 1 + 8x'$ con $x' \in \mathbb{Z}_2$ como queríamos probar.

□

Luego, al igual que en el caso p impar, tenemos el siguiente corolario:

Corolario 2.2.9. *$x \in \mathbb{Q}_2^\times$ es un cuadrado si y solo si puede ser escrito como $x = 2^{2n}y$ con $n \in \mathbb{Z}$ e $y \in 1 + 8\mathbb{Z}_2$. El grupo cociente $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ tiene orden ocho y un sistema completo de representantes es el conjunto $\{1, -1, 5, -5, 2, -2, 10, -10\}$.*

Demostración. La primer parte es clara gracias a la proposición anterior y un razonamiento análogo a la primer parte para el caso p impar.

Para la segunda parte, recordemos que $x \in \mathbb{Q}_2^\times$ puede ser escrito de la forma $x = 2^{v_2(x)}y$ con $y \in \mathbb{Z}_2^\times$. Luego tomando cociente por cuadrados tenemos las siguientes opciones:

- $v_2(x)$ es par e y es cuadrado, entonces x está en la clase del 1.
- $v_2(x)$ es par e y no es cuadrado, entonces x está en la misma clase que y, que al no ser cuadrado, entonces es -5 , 5 , ó -1 módulo 8.
- $v_2(x)$ es impar e y no es cuadrado, entonces x está en la misma clase que $2y$, que al ser no cuadrado y, entonces son las clases $2 \cdot (-5)$, $2 \cdot 5$, $2 \cdot (-1)$, es decir -10, 10 y -2.
- $v_2(x)$ es impar e y es cuadrado, entonces x está en la clase del 2.

□

Para terminar con esta sección, veremos una última versión más general del Lema de Hensel. La idea es reinterpretar el Lema de Hensel como que si un polinomio factoriza módulo p y uno de los factores es de la forma $(X - \alpha)$, es decir

$$f(X) \equiv (X - \alpha)g(X) \quad (mod\ p),$$

entonces bajo algunas condiciones, existe una factorización parecida en $\mathbb{Z}_p$. La condición $f'(\alpha) \not\equiv 0\ (mod\ p)$ nos dice que α no es una raíz doble módulo p, es decir, que el factor $g(X)$ no es divisible por $X - \alpha$. El teorema que veremos a continuación generaliza lo anterior para cualquier factorización del polinomio f.
Pero antes veamos la siguiente definición:

Definición 2.2.10. *Sean $g(X)$ y $h(X)$ dos polinomios en $\mathbb{Z}_p[X]$. Sean $\overline{g}(X)$ y $\overline{h}(X) \in \mathbb{F}_p[X]$ los polinomios obtenidos luego de reducir módulo p. Entonces decimos que g y h son coprimos módulo p si $\gcd(\overline{g}, \overline{h}) = 1$ en $\mathbb{F}_p[X]$, o lo que es lo mismo (usando el algoritmo extendido de Euclides), si existen polinomios $a(X), b(X) \in \mathbb{Z}_p[X]$ tal que*

$$a(X)g(X) + b(X)h(X) \equiv 1 \quad (mod\ p).$$

Teorema 2.2.11 (Lema de Hensel para Polinomios)**.** *Sea $f(X) \in \mathbb{Z}_p[X]$. Supongamos que existen polinomios $g_1(X)$ y $h_1(X) \in \mathbb{Z}_p[X]$ tales que*

a) $g_1(X)$ es mónico,

b) $g_1(X)$ y $h_1(X)$ son coprimos módulo p,

c) $f(X) \equiv g_1(X)h_1(X) \pmod{p}$.

Entonces existen polinomios $g(X),\ h(X) \in \mathbb{Z}_p[X]$ tales que

a) $g(X)$ es mónico,

b) $g(X) \equiv g_1(X) \pmod{p}$ y $h(X) \equiv h_1(X) \pmod{p}$,

c) $f(X) = g(X)h(X)$.

Demostración. Notar que pedir que $g(X)$ sea mónico implica que $gr\,(g(X)) = gr\,(g_1(X))$. Sea d el grado de $f(X)$ y m el grado de $g_1(X)$. Entonces podemos asumir que $gr(h_1) \leq d - m$ ya que realmente solo importa la reducción módulo p de h_1 (notar que podría ser menor si el coeficiente principal de f fuera múltiplo de p).
La idea es construir dos sucesiones de polinomios $g_n(X)$ y $h_n(X)$ tales que

a) cada g_n sea mónico y de grado m

b) $g_{n+1} \equiv g_n \pmod{p^n}$ y $h_{n+1} \equiv h_n \pmod{p^n}$,

c) $f(X) \equiv g_n(X)h_n(X) \pmod{p^n}$.

Si podemos encontrar esas sucesiones, claramente terminamos, pues tomando límite encontramos los polinomios $g(X)$ y $h(X)$ buscados. En otras palabras, los coeficientes de $g(X)$ serán el límite de los respectivos coeficientes de $g_n(X)$.
Veamos como hallar g_2 y h_2. Como queremos que los polinomios g sean congruentes, entonces queremos que

$$g_2(X) = g_1(X) + p\ r_1(X)$$

para algún polinomio $r_1(X) \in \mathbb{Z}_p[X]$. De la misma forma

$$h_2(X) = h_1(X) + p\ s_1(X).$$

Para probar que g_2 y h_2 existen, debemos probar que es posible encontrar r_1 y s_1 que cumplan la condición (c), es decir:

$$f(X) \equiv g_2(X)h_2(X) \pmod{p^2},$$

que sustituyendo,

$$f(X) \equiv (g_1(X) + p\ r_1(X))(h_1(X) + p\ s_1(X)) \quad (mod\ p^2).$$

Desarrollando obtenemos

$$\begin{aligned} f(X) &\equiv g_1(X)h_1(X) + p\ r_1(X)h_1(X) + p\ s_1(X)g_1(X) + p^2\ r_1(X)s_1(X) \\ &\equiv g_1(X)h_1(X) + p\ r_1(X)h_1(X) + p\ s_1(X)g_1(X) \quad (mod\ p^2) \end{aligned}$$

Recordemos que $f(X) \equiv g_1(X)h_1(X)\ (mod\ p)$, por lo que

$$f(X) - g_1(X)h_1(X) = p\ k_1(X)$$

para algún $k_1(X) \in \mathbb{Z}_p[X]$. Sustituyendo tenemos que

$$p\ k_1(X) \equiv p\ r_1(X)h_1(X) + p\ s_1(X)g_1(X) \quad (mod\ p^2)$$

que dividiendo por p nos queda

$$k_1(X) \equiv r_1(X)h_1(X) + s_1(X)g_1(X) \quad (mod\ p).$$

Esta es la ecuación que tenemos que resolver para determinar r_1 y s_1.
Recordemos que asumimos que g_1 y h_1 son coprimos módulo p. Esto significa que existen $a(X),\ b(X) \in \mathbb{Z}_p[X]$ tal que $a(X)g_1(X) + b(X)h_1(X) \equiv 1\ (mod\ p)$. Consideremos entonces lo polinomios

$$\tilde{r}_1(X) = b(X)k_1(X) \qquad y \qquad \tilde{s}_1(X) = a(X)k_1(X)$$

Estos polinomios claramente verifican la ecuación anterior, es decir

$$k_1(X) \equiv \tilde{r}_1(X)h_1(X) + \tilde{s}_1(X)g_1(X) \quad (mod\ p)$$

pero el problema está en que no tenemos control sobre el grado de $\tilde{r}_1(X)$; si el grado fuera mayor que m, luego $g_1(X) + p\tilde{r}_1(X)$ no sería mónico de grado m.
Para arreglar esto, dividamos $\tilde{r}_1(X)$ por $g_1(X)$, y sea $r_1(X)$ el resto:

$$\tilde{r}_1(X) = g_1(X)q(X) + r_1(X).$$

Ahora sabemos que $gr(r_1(X)) < gr(g_1(X))$. Luego si consideramos $s_1(X) = \tilde{s}_1(X) +$

$h_1(X)q(X)$, verifica la ecuación:

$$\begin{aligned} r_1(X)h_1(X) + s_1(X)g_1(X) &\equiv (\tilde{r}_1(X) - g_1(X)q(X))h_1(X) + (\tilde{s}_1(X) + h_1(X)q(X))g_1(X) \\ &\equiv \tilde{r}_1(X)h_1(X) - g_1(X)q(X)h_1(X) + \tilde{s}_1(X)g_1(X) + h_1(X)q(X)g_1(X) \\ &\equiv \tilde{r}_1(X)h_1(X) + \tilde{s}_1(X)g_1(X) \\ &\equiv k_1(X) \quad (mod\ p). \end{aligned}$$

Con esto probamos que g_2 y h_2 existen. Como son congruentes a g_1 y h_1 respectivamente, entonces también son coprimos módulo p, por lo que el siguiente paso es exactamente análogo cambiando los subíndices y los exponentes. □

2.3 Algo de Análisis en $\mathbb{Q}_p$ y el Teorema de Strassman

Comencemos esta sección comentando brevemente que pasa con la teoría de las derivadas y antiderivadas en $\mathbb{Q}_p$. Veremos con un ejemplo que esta teoría no sirve tanto como sí lo hace en el caso real. El principal problema, es que en $\mathbb{R}$ si una función tiene derivada cero, entonces la función es localmente constante, esto falla en $\mathbb{Q}_p$, veamos el siguiente ejemplo:

sea $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ que lleva

$$x = a_0 + a_1p + a_2p^2 + a_3p^3 + \cdots + a_np^n + \cdots$$

a

$$f(x) = a_0 + a_1p^2 + a_2p^4 + a_3p^6 + \cdots + a_np^{2n} + \cdots$$

Veamos que esta función es inyectiva (y por lo tanto no es localmente constante en ningún lado) y que $f'(x) = 0$ para todo x:
La inyectividad es clara pues si $f(x) = f(y)$ con $x = \sum_{n=0}^{\infty} a_np^n$ e $y = \sum_{n=0}^{\infty} b_np^n$, entonces tenemos que $a_n = b_n$ para todo n y por ende $x = y$.

Para la parte de la derivada [2], estimemos $|f(x) - f(y)|$ y veamos qué relación tiene con $|x - y|$. Como estamos trabajando en $\mathbb{Z}_p$, podemos asumir que $|x - y| = p^{-k}$ para algún $k \geq 0$, por lo que la expansión p-ádica de x e y deben ser iguales hasta el dígito $(k - 1)$. Por lo tanto, por la definición de f, las expansiones de $f(x)$ y $f(y)$ deben coincidir hasta

[2] Como límite del cociente incremental.

el dígito $(2k-1)$, es decir que $|f(x)-f(y)| \leq p^{-2k}$. Entonces tenemos que para todo $x, y \in \mathbb{Z}_p$, tenemos

$$|f(x)-f(y)| \leq |x-y|^2.$$

Pero luego

$$\left|\frac{f(x)-f(y)}{x-y}\right| \leq |x-y|,$$

que tiene a cero cuando $y \to x$, por lo tanto $f'(x)=0$.

Como dijimos, este es uno de los principales problemas de la derivada en el análisis p-ádico: que una función tenga derivada cero no implica que sea localmente constante.
Lo que se rompe en la demostración es el hecho de que el teorema del valor medio no es cierto en el contexto p-ádico:
Lo que diría un Teorema del valor medio p-ádico: Si una función $f(X)$ es derivable con derivada continua en $U \subset \mathbb{Q}_p$ y si $|f'(x)| \leq M$ para todo $x \in U$, entonces para todos $a, b \in U$ tenemos que

$$|f(b)-f(a)| \leq M|b-a|.$$

Pero como digimos anteriormente, esto es falso. Tomemos $U=\mathbb{Z}_p$, $f(x)=x^p$, $a=1$ y $b=0$. Luego [3] $f'(x)=px^{p-1}$, por lo que tenemos que $|f'(x)| \leq p^{-1} \quad \forall\, x \in U$. Pero $f(1)-f(0)=1$, es decir

$$|f(1)-f(0)| = 1 > \frac{1}{p} = \frac{1}{p}|1-0|$$

lo cual contradice nuestro «Teorema del valor medio».
En particular esto nos dice que si tenemos dos funciones con la misma derivada, no necesariamente difieren por una constante. Es decir que la teoría de las antiderivadas tampoco funciona muy bien.

Continuemos esta sección estudiando el comportamiento de las series en $\mathbb{Q}_p$. Para ello, recordemos el Lema 1.3.2, que claramente aplica con $\Bbbk = \mathbb{Q}_p$. Entonces tenemos el siguiente corolario:

Corolario 2.3.1. *Una serie* $\sum_{n=0}^{\infty} a_n$ *con* $a_n \in \mathbb{Q}_p$ *es convergente si y solo si*

$$\lim_{n\to\infty} a_n = 0,$$

[3] Se puede probar que la derivada como límite del cociente incremental de un polinomio coincide con su derivada formal, tal y como sucede en el caso no arquimediano.

y en tal caso, también tenemos

$$\left|\sum_{n=0}^{\infty} a_n\right| \leq \max_n |a_n|.$$

DEMOSTRACIÓN. Una serie converge cuando la sucesión de sus sumas parciales converge. Como $\mathbb{Q}_p$ es completo esto pasa si y solo si la sucesión de sus sumas parciales es de Cauchy y por el Lema 1.3.2 esto pasa si y solo si la diferencia de dos consecutivos tiende a cero, pero la diferencia de la n-ésima y la $(n-1)$-ésima suma parcial es justamente a_n, por lo que tenemos la primer parte.

Notar que si $\sum_{n=0}^{\infty} a_n = 0$ entonces la desigualdad no dice nada pues cualquier valor absoluto es mayor o igual a cero. Si no, para cualquier suma parcial tenemos que

$$\left|\sum_{n=0}^{N} a_n\right| \leq \max_{0\leq n\leq N} |a_n|$$

por ser un valor absoluto no arquimediano. Por otro lado, tenemos que para un N suficientemente grande vale que

$$\max_{0\leq n\leq N} |a_n| = \max_n |a_n|$$

pues los a_n tienden a cero. Luego:

$$\left|\sum_{n=0}^{\infty} a_n\right| = \left|\sum_{n=0}^{N} a_n\right|$$

por el Lema 1.3.10.

□

Por lo que en $\mathbb{Q}_p$ es mucho más fácil decidir cuándo una serie es convergente que en $\mathbb{R}$. Otro ejemplo en dónde las cosas son más sencillas en el caso no arquimediano es un teorema sobre las dobles series e intercambiar sus ordenes. Es decir que queremos considerar

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)$$

y

$$\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$$

y dar una condición para que sean iguales.

Antes de ello, veamos una definición y un lema que nos será útil.

Definición 2.3.2. *Dada una sucesión (b_{ij}), diremos que*

$$\lim_{i\to\infty} b_{ij} = 0 \quad \textit{uniformemente en } j$$

si dado $\varepsilon > 0$ existe N que no depende de j tal que

$$i \geq N \Longrightarrow |b_{ij}| < \varepsilon.$$

Lema 2.3.3. *Sea $(b_{ij}) \subset \mathbb{Q}_p$. Son equivalentes:*

a) Para todo i, $\lim_{j\to\infty} b_{ij} = 0$, y $\lim_{i\to\infty} b_{ij} = 0$ uniformemente en j.

b) Dado ε existe N dependiendo solo de ε tal que

$$\text{máx}\{i, j\} \geq N \Longrightarrow |b_{ij}| < \varepsilon$$

c) $\lim_{i\to\infty} b_{ij} = 0$ uniformemente en j y $\lim_{j\to\infty} b_{ij} = 0$ uniformemente en i

Demostración. Es claro que (b) implica (c) y también es claro que (c) implica (a), por lo que nos queda probar que (a) implica (b).
Asumamos (a). Sea $\varepsilon > 0$, la uniformidad en j nos dice que existe N_0 que depende de ε pero no de j, tal que $|b_{ij}| < \varepsilon$ si $i \geq N_0$. La convergencia en i nos dice que existe un $N_1(i)$ tal que si $j \geq N_1(i)$ entonces $|b_{ij}| < \varepsilon$. Tomemos entonces

$$N = N(\varepsilon) = \text{máx}\{N_0, N_1(0), N_1(1), ..., N_1(N_0 - 1)\}$$

Probemos que este N cumple lo que queremos: si $\text{máx}\{i, j\} \geq N$, entonces o $i \geq N_0$ en cuyo caso $|b_{ij}| < \varepsilon$ sin importar quien sea j, ó $i < N_0$ y $j \geq N$, en cuyo caso $i \in \{0, 1, 2, ..., N_0-1\}$ y j es más grande que el correspondiente N_1, por lo que nuevamente $|b_{ij}| < \varepsilon$.

□

Observar que este lema también es válido en el caso arquimediano, pero en la demostración del teorema de las dobles series que veremos a continuación, sí será necesario la propiedad no arquimediana y la usaremos en repetidas ocasiones.

Teorema 2.3.4. *Sea $(b_{ij}) \subset \mathbb{Q}_p$ y supongamos*

a) Para todo i, $\lim_{j\to\infty} b_{ij} = 0$,

b) $\lim_{i\to\infty} b_{ij} = 0$ uniformemente en j.

Entonces las dos series

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) \qquad y \qquad \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$$

convergen y son iguales.

Demostración. Por el lema sabemos que dado ε existe N tal que si $\max\{i,j\} \geq N$ entonces $|b_{ij}| < \varepsilon$. En particular b_{ij} tiende a cero para todo i cuando $j \to \infty$ y también al revés, es decir b_{ij} tiende a cero para todo j cuando $i \to \infty$, lo que significa que las sumas internas

$$\sum_{j=0}^{\infty} b_{ij} \qquad y \qquad \sum_{i=0}^{\infty} b_{ij}$$

convergen (la primera para todo i y la segunda para todo j). Además por el Corolario 2.3.1 tenemos que para $i \geq N$

$$\left|\sum_{j=0}^{\infty} b_{ij}\right| \leq \max_{j}\{|b_{ij}|\} < \varepsilon.$$

De igual forma, para $j \geq N$ tenemos

$$\left|\sum_{i=0}^{\infty} b_{ij}\right| \leq \max_{i}\{|b_{ij}|\} < \varepsilon.$$

En particular vemos que

$$\lim_{i\to\infty}\sum_{j=0}^{\infty} b_{ij} = 0 \qquad y \qquad \lim_{j\to\infty}\sum_{i=0}^{\infty} b_{ij} = 0$$

por lo tanto, ambas dobles series convergen ya que sus términos tienden a cero.
Nos queda probar que ambas sumas valen lo mismo, para esto, dado ε seguimos usando el mismo N que antes, es decir tal que $|b_{ij}| < \varepsilon$ si i o $j \geq N$.
Comencemos por notar la siguiente igualdad:

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right)\right| = \left|\sum_{i=0}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right) + \sum_{i=N+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right|.$$

Pero sabemos que si $j \geq N+1$ entonces $|b_{ij}| < \varepsilon$ para todo i, por lo que por el Corolario 2.3.1 tenemos que $\left|\sum_{j=N+1}^{\infty} b_{ij}\right| < \varepsilon$ para todo i. Luego, por la desigualdad ultramétrica

tenemos que

$$\left|\sum_{i=0}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right)\right| < \varepsilon$$

.

De forma similar, si $i \geq N+1$ tenemos que $|b_{ij}| < \varepsilon$ para todo j, por lo que por el Corolario 2.3.1 tenemos que $\left|\sum_{j=0}^{\infty} b_{ij}\right| < \varepsilon$- Luego, nuevamente por el Corolario 2.3.1 tenemos que

$$\left|\sum_{i=N+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right| < \varepsilon.$$

Por lo que una vez más por la desigualdad ultramétrica, tenemos que

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right)\right| = \left|\sum_{i=0}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right) + \sum_{i=N+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right| < \varepsilon.$$

Para terminar, si cambiamos i y j y repetimos un razonamiento análogo para la otra doble serie obtenemos

$$\left|\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right) - \sum_{j=0}^{N}\left(\sum_{i=0}^{N} b_{ij}\right)\right|$$

y como claramente podemos cambiar el orden de las sumas en el caso finito, nuevamente por la desigualdad ultramétrica, obtenemos que

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right| < \varepsilon.$$

Como tenemos esto para todo ε, entonces las dos doble series son iguales.

□

Ahora que vimos algunas propiedades elementales de las series en general, enfoquémonos en las series de potencia y en las funciones que estas definen.
Consideremos entonces una serie de potencias con coeficientes en $\mathbb{Q}_p$:

$$f(X) = \sum_{n=0}^{\infty} a_n X^n.$$

Dado $x \in \mathbb{Q}_p$, queremos considerar $f(x)$, que es la serie $\sum a_n x^n$ que ya sabemos que converge si y solo si $|a_n x^n| \to 0$. Como en el caso clásico, el conjunto de todos estos x es un disco cuyo radio es el habitual, pero tenemos mayor control sobre lo que sucede en

el borde de este disco.

Proposición 2.3.5. *Sea* $f(X) = \sum_{n=0}^{\infty} a_n X^n$ *con* $(a_n) \subset \mathbb{Q}_p$. *Definimos*

$$\rho = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|}},$$

donde si el el límite superior es cero o infinito entonces ρ *es infinito o cero respectivamente, por lo que* $0 \leq \rho \leq \infty$. *Entonces tenemos :*

a) Si $\rho = 0$ *entonces* $f(x)$ *converge solamente en* $x = 0$

b) Si $\rho = \infty$, *entonces* $f(x)$ *converge para todo* $x \in \mathbb{Q}_p$.

c) Si $0 < \rho < \infty$ *y* $\lim_{n\to\infty} |a_n|\rho^n = 0$, *entonces* $f(x)$ *converge si y solo si* $|x| \leq \rho$.

d) Si $0 < \rho < \infty$ *y* $|a_n|\rho^n$ *no tiende a cero, entonces* $f(x)$ *converge si y solo si* $|x| < \rho$.

Demostración. Ya sabemos que la región de convergencia es

$$\left\{x \in \mathbb{Q}_p : \lim_{n\to\infty} |a_n x^n| = 0\right\},$$

así que la idea es dar una descripción más precisa. Para arrancar, es claro que $f(0)$ converge. Luego, si $|x| > \rho$, entonces $|a_n||x^n|$ no tiende a cero: por la definición de ρ, existen infinitos valores de n para los cuales $|a_n|$ está cerca de $1/\rho^n$ y como $|x| > \rho$, tenemos que $(|x|/\rho)^n$ es arbitrariamente grande cuando n crece y por lo tanto no tiende a cero.
De manera similar, si $|x| < \rho$, sea ρ_1 tal que $|x| < \rho_1 < \rho$, luego $|x|/\rho_1 < 1$. Por otro lado, tenemos que $|a_n| < 1/\rho_1^n$ (que es mayor estricto que $1/\rho^n$), por lo tanto, $|a_n x^n| \leq |x|^n/\rho_1^n$, ergo $|a_n x^n| \to 0$.
Para terminar, el caso cuando $|x| = \rho$, es claro cuando converge o no pues es justamente el enunciado del Corolario 2.3.1.

□

Veamos que las funciones definidas por series de potencias tienen un comportamiento más amigable que las funciones en general en $\mathbb{Q}_p$.
Comencemos por notar que son continuas:

Lema 2.3.6. *Sea* $f(X) = \sum a_n X^n$ *una serie de potencias con coeficientes en* $\mathbb{Q}_p$. *Si* $f(x)$ *converge cuando* $|x| \leq r$, *luego la función* $f : \overline{B}(0,r) \longrightarrow \mathbb{Q}_p$ *definida por* $x \mapsto f(x)$ *es acotada y uniformemente continua.*

Demostración. Como f converge en $\overline{B}(0,r)$, entonces sabemos que $|a_n|r^n \to 0$, por lo que $M_r = \max_{n\geq 0} |a_n|r^n$ es finito.

Probemos primero que $f(x)$ es acotada en $\overline{B}(0,r)$: como $|x| \leq r$, tenemos que

$$|f(x)| = \left|\sum_{n=0}^{\infty} a_n x^n\right| \leq \text{máx}\{|a_n x^n|\} \leq \text{máx}\{|a_n| r^n\} = M_r.$$

Entonces nos queda probar la continuidad uniforme. Supongamos $x, y \in \overline{B}(0,r)$. Luego si restamos $f(x) - f(y)$ tenemos que:

$$\begin{aligned} f(x) - f(y) &= \sum_{n=1}^{\infty} a_n (x^n - y^n) \\ &= \sum_{n=1}^{\infty} a_n (x-y)(x^{n-1} + x^{n-2}y + ... + y^{n-1}) \\ &= (x-y) \sum_{n=1}^{\infty} a_n (x^{n-1} + x^{n-2}y + ... + y^{n-1}). \end{aligned}$$

Pero

$$|x^{n-1} + x^{n-2}y + ... + y^{n-1}| \leq \max_{0 \leq i \leq n-1} \{|x|^{n-1-i}|y|^i\} \leq r^{n-1}$$

y por lo tanto,

$$\left|\sum_{n=1}^{\infty} a_n (x^{n-1} + x^{n-2}y + ... + y^{n-1})\right| \leq \text{máx}\{|a_n| r^{n-1}\} = \frac{1}{r} M_r.$$

Entonces tenemos que $|f(x) - f(y)| \leq \frac{1}{r} M_r |x - y|$, lo que prueba que f es uniformemente continua en $\overline{B}(0,r)$.

□

Como en el caso clásico, podemos cambiar el centro de la expansión de la serie, es decir escribir la función como una serie de potencias en $X - \alpha$ para algún α en la zona de convergencia. En el caso clásico, las series resultantes pueden tener una región de convergencia distinta, lo que da lugar a lo que llamamos continuación analítica, sin embargo, como veremos en la proposición que sigue, en $\mathbb{Q}_p$, las regiones de convergencia coinciden y por ende no tenemos continuación analítica.

Proposición 2.3.7. *Sea $f(X) = \sum a_n X^n$ una serie de potencias con coeficientes en $\mathbb{Q}_p$ y sea $\alpha \in \mathbb{Q}_p$, $\alpha \neq 0$ un punto para el cual $f(\alpha)$ converge. Para cada $m \geq 0$ definimos*

$$b_m = \sum_{n \geq m} \binom{n}{m} a_n \alpha^{n-m},$$

y consideremos la serie de potencias

$$g(X) = \sum_{m=0}^{\infty} b_m (X - \alpha)^m.$$

Entonces

a) La serie que define b_m converge para todo m.

b) Las series de potencias $f(X)$ y $g(X)$ tienen la misma región de convergencia.

c) Para todo λ en la región de convergencia tenemos que $g(\lambda) = f(\lambda)$.

DEMOSTRACIÓN. Para (a), simplemente usamos el hecho de los coeficiente binomiales son enteros y que α pertenece a la región de convergencia de $f(X)$:

$$\left| \binom{n}{m} a_n \alpha^{n-m} \right| \leq |a_n \alpha^{n-m}| = |\alpha|^{-m} \cdot |a_n \alpha^n| \to 0,$$

luego por el Corolario 2.3.1 tenemos que b_m converge.
Para (b) y (c), tomemos λ en la región de convergencia de $f(X)$, luego

$$f(\lambda) = \sum_n a_n (\lambda - \alpha + \alpha)^n = \sum_n \sum_{m \leq n} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m.$$

Notar que si pudieramos intercambiar las sumas ya estaría pues nos quedaría justamente $g(\lambda)$. Para ello, necesitamos probar que estamos en las hipótesis del Teorema 2.3.4. Para esto, definamos

$$\beta_{nm} = \begin{cases} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m & \text{si } m \leq n \\ \\ 0 & \text{si } m > n \end{cases}$$

Entonces tenemos que probar que β_{nm} cumple las condiciones del Teorema. Primero notar que

$$|\beta_{nm}| = \left| \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m \right| \leq |a_n \alpha^{n-m} (\lambda - \alpha)^m|,$$

por lo que nos basta con acotar la parte derecha de la desigualdad. Para esto, recordar que la región de convergencia es un disco de algún radio ρ. Como λ y α están en la región de convergencia, existe r tal que el disco cerrado de radio r está contenido en la región de convergencia y $|\lambda| \leq r$ y $|\alpha| \leq r$. Luego tenemos

$$|\beta_{nm}| \leq |a_n \alpha^{n-m} (\lambda - \alpha)^m| \leq |a_n| r^{n-m} r^m = |a_n| r^n,$$

lo cual es independiente de m y tiende a cero cuando $n \to \infty$. Esto prueba que β_{nm} tiende uniformemente a cero en m. La otra condición es trivial pues si $m > n$ $\beta_{nm} = 0$ que claramente tiende a cero cuando $m \to \infty$.
Como dijimos antes, cambiando el orden de las sumas nos da la expresión correspondiente a $g(\lambda)$ por lo tanto $f(\lambda) = g(\lambda)$; esto también nos prueba que g converge siempre que lo haga f, para terminar (b), cambiamos f por g y repetimos el argumento lo que nos prueba que las regiones de convergencia coinciden.

□

Por la proposición anterior vemos que no podemos hablar de continuaciones analíticas de funciones definidas por series de potencias, por lo que nos olvidaremos de pensar en lo global y estudiaremos cómo se comportan dichas funciones en una bola cerrada contenida en la región de convergencia.
Para comenzar con esto, veamos una condición para que dos series de potencias que coinciden en ciertos puntos tengan que ser necesariamente la misma.

Proposición 2.3.8. *Sean $f(X)$ y $g(X)$ dos series de potencias. Supongamos que existe una sucesión (x_m) no constante a partir de un punto que converge a cero en $\mathbb{Q}_p$ y que cumple que $f(x_m) = g(x_m)$ para todo m. Entonces $f(X) = g(X)$, es decir tienen los mismos coeficientes.*

Demostración. Reemplazando (x_m) por una subsucesión de ser necesario, podemos asumir que $x_m \neq 0$ para todo m. Si consideramos la serie $h(X) = f(X) - g(X) = \sum a_n X^n$, entonces tenemos que $h(x_m) = 0$ para todo m, y lo que queremos probar es que $a_n = 0$ para todo n. Supongamos que no, entonces sea r el menor índice para el cual $a_r \neq 0$, por lo tanto

$$\begin{aligned} h(X) &= a_r X^r + a_{r+1} X^{r+1} + a_{r+2} X^{r+2} + ... \\ &= X^r (a_r + a_{r+1} X + a_{r+2} X^2 + ...) \\ &= X^r h_1(X) \end{aligned}$$

donde $h_1(0) = a_r \neq 0$. Como h_1 es una función definida por una serie de potencias es continua y por lo tanto $h_1(x_m) \to a_r$ cuando $m \to \infty$; en particular $h_1(x_m)$ no es cero para m suficientemente grande. Pero entonces, como sabemos que $x_m \neq 0$, $h(x_m) = x_m^r h_1(x_m)$ es distinto de cero para m suficientemente grande, lo cual es absurdo.
□

Como vimos, que dos funciones cualesquiera tengan misma derivada, no implica que su diferencia sea una constante, pero como veremos a continuación, en el caso de funciones definidas por series de potencias, esto sí es cierto.
Este resultado será un corolario de la siguiente proposición:

Proposición 2.3.9. *Sea $f(X) = \sum a_n X^n$ una serie de potencias con radio de convergencia distinto de cero, y sea $f'(X) = \sum n a_n X^{n-1}$ su derivada formal. Entonces, dado $x \in \mathbb{Q}_p$, si $f(x)$ converge también lo hace $f'(x)$ y además tenemos que*

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

Demostración. Primero que todo, notemos que efectivamente existen elementos $h \to 0$ para los cuales $f(x+h)$ converge pues la zona de convergencia es una bola centrada en el origen y gracias a la desigualdad ultramétrica, si h está en la región de convergencia, $x+h$ también. Por lo tanto, el límite planteado tiene sentido.
Que $f(x)$ converja es equivalente a que $a_n x^n \to 0$. Si $x = 0$ es claro que $f'(x)$ converge. Si $x \neq 0$ tenemos que

$$|n a_n x^{n-1}| \leq |a_n x^{n-1}| = \frac{1}{|x|} |a_n x^n| \to 0,$$

por lo que $f'(x)$ converge.
Sea r tal que $\overline{B}(0,r)$ está contenida en la región de convergencia de f y $|x| \leq r$. Como nos importa solamente h cerca de cero, podemos asumir que $|h| < r$.
Por otro lado tenemos que

$$f(x+h) = \sum_{n=0}^{\infty} a_n (x+h)^n = \sum_{n=0}^{\infty} a_n \sum_{m=0}^{n} \binom{n}{m} x^{n-m} h^m.$$

Restando $f(x)$ y dividendo por h

$$\frac{f(x+h) - f(x)}{h} = \sum_{n=1}^{\infty} \sum_{m=1}^{n} a_n \binom{n}{m} x^{n-m} h^{m-1}.$$

Nos queda tomar límites de ambos lados para obtener lo que queremos, pero en la derecha para poder pasar el límite para adentro, necesitamos probar que el término principal tiende a cero uniformemente en h:
Como tenemos que $|x| \leq r$ y $|h| \leq r$, entonces

$$\left| a_n \binom{n}{m} x^{n-m} h^{m-1} \right| \leq |a_n| r^{n-1}.$$

Por otro lado la serie converge cuando $|x| = r$, es decir $|a_n| r^n \to 0$, pero esto significa que $|a_n| r^{n-1} \to 0$ (pues r es una constante distinta de cero). Es decir que dado $\varepsilon > 0$, existe N tal que $n \geq N$ implica $|a_n| r^{n-1} < \varepsilon$, lo que implica que

$$\left| a_n \binom{n}{m} x^{n-m} h^{m-1} \right| \leq \varepsilon$$

para todo $h \leq r$. Entonces, como anticipamos, podemos tomar límite dentro de la sumatoria y por ende obtenemos que

$$\lim_{h\to 0} \frac{f(x+h)-f(x)}{h} = \sum_{n=1}^{\infty} n a_n x^{n-1}.$$

□

Observación 2.3.10. *El radio de convergencia de $f(X)$ y de $f'(X)$ es el mismo: primero observamos que $f'(x) = \sum n a_n x^{n-1}$ converge si y solo si $xf'(x) = \sum n a_n x^n$ converge. Por lo tanto lo único que hay que probar es que*

$$\limsup_{n\to\infty} \sqrt[n]{|a_n|_p} = \limsup_{n\to\infty} \sqrt[n]{|na_n|_p}.$$

Pero claramente si $\lim_{n\to\infty} |n|_p^{1/n} = 1$ implica lo anterior. Por último, para probar esto, solo hace falta observar que $1/n \leq |n|_p \leq 1$, ya que luego tenemos

$$n^{-1/n} \leq |n|_p^{1/n} \leq 1,$$

que por el teorema de la función comprendida conseguimos lo que queríamos (ya que claramente $n^{-1/n} \to 1$).

Ahora sí, el corolario que habíamos anticipado.

Corolario 2.3.11. *Supongamos $f(X)$ y $g(X)$ dos series de potencias que convergen para $|x| < \rho$. Si $f'(x) = g'(x)$ para todo $|x| < \rho$, entonces existe una constante $c \in \mathbb{Q}_p$ tal que $f(X) = g(X) + c$ como series de potencias. En particular, $f(X)$ y $g(X)$ tiene el mismo disco de convergencia y por ende tenemos $f(x) = g(x) + c$ para todo x en el disco de convergencia.*

Demostración. Sea $f(X) = \sum a_n X^n$, $g(X) = \sum b_n X^n$, y sean $f'(X)$ y $g'(X)$ sus derivadas formales. Por la Proposición 2.3.9 sabemos que siempre que $|x| < \rho$, tenemos que

$$\sum_{n=1}^{\infty} n a_n x^{n-1} = \sum_{n=1}^{\infty} n b_n x^{n-1}.$$

Luego, por la Proposición 2.3.8, podemos concluir que $a_n = b_n$ para todo $n \geq 1$, luego las dos series son iguales excepto en el término sin X, es decir, difieren en una constante como queríamos probar.

□

Una vez probadas algunas propiedades elementales que cumplen las series de potencias en $\mathbb{Q}_p$, veremos un resultado fundamental sobre el comportamiento de los ceros de las funciones definidas por series de potencias en $\mathbb{Q}_p$.

Teorema 2.3.12 (Teorema de Strassman)**.** *Sea*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n$$

una serie de potencias no nula con coeficientes en $\mathbb{Q}_p$ y supongamos que $\lim_{n\to\infty} a_n = 0$ (lo que nos dice que $f(x)$ converge para todo $x \in \mathbb{Z}_p$). Sea N el entero definido por las siguientes condiciones

$$|a_N| = \max_n |a_n| \qquad y \qquad |a_n| < |a_N| \quad \text{para todo } n > N.$$

Entonces, la función $f : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ definida por $x \mapsto f(x)$ tiene a lo mucho N ceros.

Demostración. La existencia de un N que cumpla las condiciones se debe a que la serie es no nula y los coeficientes tienden a cero.
Haremos inducción en N.
Si $N = 0$, entonces tenemos que $|a_0| > |a_n|$ para todo $n \geq 1$. Lo que queremos probar es que en este caso no hay ceros, es decir $f(x) \neq 0$ para todo $x \in \mathbb{Z}_p$. Supongamos que tenemos $f(x) = 0$ para algún x, luego

$$\begin{aligned} |a_0| &= |a_1 x + a_2 x^2 + ...| \\ &\leq \max_{n\geq 1} |a_n x^n| \\ &\leq \max_{n\geq 1} |a_n|. \end{aligned}$$

Pero esto es absurdo pues $|a_0| > |a_n|$ para todo $n \geq 1$.

Supongamos $N > 0$. Sea $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$, y sea $x \in \mathbb{Z}_p$ cualquiera, luego tenemos

$$f(x) = f(x) - f(\alpha) = \sum_{n\geq 1} a_n (x^n - \alpha^n) = (x - \alpha) \sum_{n\geq 1} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}.$$

Observemos que si $c_{nj} = a_n x^j \alpha^{n-1-j}$, como x y α están en $\mathbb{Z}_p$, tenemos que $|c_{nj}| \leq |a_n| \to 0$ cuando $n \to \infty$. Además, $c_{nj} = 0$ si $j \geq n$. Luego estamos en las hipótesis del Teorema 2.3.4 con lo que podemos reordenar las series y obtenemos entonces

$$f(x) = (x - \alpha) \sum_{j=0}^{\infty} b_j x^j = (x - \alpha) g(x),$$

donde los coeficiente b_j son

$$b_j = \sum_{k=0}^{\infty} a_{j+1+k} \alpha^k.$$

Es claro que los b_j tienden a cero pues $|b_j| \leq \max_k |a_{j+1+k}| \to 0$ cuando $j \to \infty$. También es claro que no son todos cero, pues de lo contrario $f(X)$ sería la serie nula. Por lo tanto, $g(X)$ satisface las hipótesis del teorema.
Para hacer la inducción precisamos encontrar el último b_j con máximo valor absoluto. Primero notar que todos los $|b_j|$ están acotados por $|a_N|$ por la misma desigualdad del límite. Por otro lado, como $|\alpha| \leq 1$ tenemos que $|a_{N+i}\alpha^i| \leq |a_{N+i}| \leq |\alpha_N|$ para todo $i \geq 1$, por lo que por la Proposición 1.2.3 tenemos que

$$|b_{N-1}| = |a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + ...| = |a_N|.$$

Además, si $j \geq N$, tenemos

$$|b_j| \leq \max_{k\geq 0} |a_{j+k+1}| \leq \max_{j\geq N+1} |a_j| < |a_N|.$$

Esto prueba entonces que el b_j que satisface las hipótesis del Teorema de Strassman es b_{N-1}, luego por inducción tenemos que $g(X)$ tiene a lo mucho $N-1$ ceros en $\mathbb{Z}_p$ y por ende $f(X)$ tiene a lo mucho N ceros (los de $g(X)$ y α).

□

A continuación, veremos una serie de corolarios del Teorema de Strassman.

Corolario 2.3.13. *Sea $f(X) = \sum a_n X^n$ una serie de potencias no nula que converge en $\mathbb{Z}_p$, y sean $\alpha_1, \alpha_2, ..., \alpha_m$ sus raíces en $\mathbb{Z}_p$. Entonces existe una serie de potencias $g(X)$ que converge en $\mathbb{Z}_p$ y no tiene ceros en $\mathbb{Z}_p$ tal que*

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_m) g(X).$$

Demostración. Es claro por la demostración del Teorema. □

Como $\mathbb{Z}_p$ es la bola unidad cerrada, podemos extender el resultado a otros discos simplemente reescalando.

Corolario 2.3.14. *Sea $f(X) = \sum a_n X^n$ una serie de potencias no nula que converge en $p^m\mathbb{Z}_p$ para algún $m \in \mathbb{Z}$. Entonces $f(X)$ tiene una cantidad finita de ceros en $p^m\mathbb{Z}_p$.*

Demostración. Definimos $g(X) = f(p^m X) = \sum a_n p^{mn} X^n$. Como $f(X)$ converge en $p^m\mathbb{Z}_p$, entonces $g(x)$ converge para $x \in \mathbb{Z}_p$, luego aplicando el Teorema de Strassman a $g(X)$ tenemos la finitud de los ceros de f. □

El teorema de Strassman nos permite dar una nueva versión de la Proposición 2.3.8.

Corolario 2.3.15. *Sea $f(X) = \sum a_n X^n$ y $g(X) = \sum b_n X^n$ dos series de potencias que convergen en $p^m\mathbb{Z}_p$. Si existen infinitos $\alpha \in p^m\mathbb{Z}_p$ tal que $f(\alpha) = g(\alpha)$, entonces $a_n = b_n$ para todo $n \geq 0$.*

Demostración. Por el corolario anterior, sabemos que si $f(X) - g(X)$ no es la serie nula, debería tener finitos ceros, pero por hipótesis tiene infinitos, luego es la serie nula y por tanto $a_n = b_n$ para todo n. □

Un corolario muy importante del Teorema de Strassman es el siguiente:

Corolario 2.3.16. *Sea $f(X) = \sum a_n X^n$ una serie de potencias que converga en $p^m\mathbb{Z}_p$. Si la función $p^m\mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ que manda $x \mapsto f(x)$ es periódica, es decir, existe c tal que $f(x+c) = f(x)$ para todo $x \in p^m\mathbb{Z}_p$, entonces $f(X)$ es constante.*

Demostración. La serie $f(X) - f(0)$ tiene ceros en nc para todo $n \in \mathbb{Z}$. Como $c \in p^m\mathbb{Z}_p$, entonces $nc \in p^m\mathbb{Z}_p$, por ende $f(X) - f(0)$ tiene infinitos ceros, ergo $f(X) - f(0)$ debe ser la serie nula, es decir $f(x)$ es constante. □

Esto nos sigue mostrando que el comportamiento en $\mathbb{Q}_p$ es totalmente distinto al del caso clásico en dónde tenemos funciones analíticas periódicas no constantes como el seno y el coseno.
Por último, veremos que aunque la periodicidad se comporta de manera distinta que en el caso clásico, los ceros de las funciones enteras se comportan de manera similar en ambos caso:

Corolario 2.3.17. *Sea $f(X) = \sum a_n X^n$ una serie de potencias entera, es decir que $f(x)$ converge para todo $x \in \mathbb{Q}_p$. Entonces $f(X)$ tiene a lo mucho una cantidad numerable de ceros. Más aún, si el conjunto de ceros no es finito, entonces la sucesión formada por los ceros tiende a infinito.*

Demostración. Ambos hechos son claros, pues en cada disco acotado $p^m\mathbb{Z}_p$ tiene finitos ceros. □

Para terminar con esta sección y capítulo, veremos una aplicación del Teorema de Strassman, con la cual probaremos que no hay raíces p-ésimas de la unidad para $p \neq 2$ y para $p = 2$ no hay raíces cuartas de la unidad.
Para eso, comencemos definiendo la función logaritmo mediante la serie de potencias clásica:

$$\log(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}.$$

Aplicamos la fórmula para el radio de convergencia:

$$\sqrt[n]{|a_n|} = \sqrt[n]{\left|\frac{1}{n}\right|} = p^{v_p(n)/n} \to 1,$$

luego $\rho = 1$. Para decidir si converge para la bola abierta o cerrada de radio 1, basta observar que cuando $|x| = 1$, tenemos que $|a_n x^n| = |a_n| = |1/n|$ no tiende a cero (pues es igual a 1 siempre que p no divida a n). Definimos entonces el logaritmo p-ádico:

Definición 2.3.18. *Sea $U_1 = B(1,1) = 1 + p\mathbb{Z}_p$. Definimos el logaritmo p-ádico de $x \in U_1$ como*

$$\log_p(x) = \log(1 + (x-1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}.$$

Se puede probar que vale

$$\log_p(xy) = \log_p(x) + \log_p(y).$$

Consideremos el siguiente lema que será nuestra herramienta principal para probar lo que queremos.

Lema 2.3.19. *Si $p \neq 2$, entonces $\log_p(x) = 0 \iff x = 1$. Si $p = 2$, $\log_p(x) = 0 \iff x = \pm 1$.*

Demostración. Definimos la serie de potencias $f(X) = \log(1+pX)$, la cual claramente converge para $x \in \mathbb{Z}_p$. Uno puede fácilmente notar que el último N para el cual el coeficiente a_N tiene valor absoluto máximo, es $N = 1$ si $p \neq 2$ y $N = 2$ si $p = 2$. □

Ahora sí, procedemos con el último resultado de este capítulo:

Proposición 2.3.20. *Si $p \neq 2$, entonces $x^p = 1$ con $x \in \mathbb{Q}_p$ implica que $x = 1$; por ende no existen raíces p-ésimas de la unidad diferentes de 1 en $\mathbb{Q}_p$.*

Si $p = 2$, entonces $x^4 = 1$ con $x \in \mathbb{Q}_2$ implica que $x = \pm 1$; por ende las únicas raíces 2^n-ésimas de la unidad son 1 y -1.

Demostración. Como mencionamos anteriormente cuando hablamos sobre las raíces de la unidad, las raíces p-ésimas de existir tienen que pertenecer a $1 + p\mathbb{Z}_p$. Supongamos que $x^p = 1$, entonces claramente $\log_p(x) = 0$ (podemos aplicar la función logaritmo pues estamos en su región de convergencia), luego por el lema anterior concluimos que $x = 1$ como queríamos probar.
Para $p = 2$ es exactamente lo mismo, pues si $x^4 = 1$, entonces $\log_2(x) = 0$ y por el lema anterior, $x = \pm 1$. □

Capítulo 3

Extensiones de $\mathbb{Q}_p$ y construcción de $\mathbb{C}_p$

El principal objetivo de este capítulo es construir una extensión de $\mathbb{Q}_p$ que sea algebraicamente cerrada, tenga un valor absoluto extendido y sea completa respecto a este valor absoluto. A esta extensión la llamaremos $\mathbb{C}_p$. Como veremos, al contrario que en $\mathbb{R}$, esta extensión no será finita ni tan sencilla de construir como en el caso clásico. De todas formas, comenzaremos estudiando las extensiones finitas y sus comportamientos con respecto al valor absoluto para luego realizar la construcción de $\mathbb{C}_p$ y concluir extendiendo algunos resultados importantes ya vistos como el Lema de Hensel.

3.1 Nociones básicas de espacios vectoriales normados

Recordemos la siguiente definición:

Definición 3.1.1. *Sea $\Bbbk$ un cuerpo de característica cero completo respecto a un valor absoluto $|\ |$. Una norma en un $\Bbbk$ espacio vectorial V es una función*

$$\|\ \| : V \longrightarrow \mathbb{R}_{\geq 0}$$

que verifica las siguientes propiedades:

a) $\|v\| = 0$ *si y solo si* $v = 0$.

b) $\|v + w\| \leq \|v\| + \|w\|$ *para cualesquiera* $v, w \in V$.

c) $\|\lambda v\| = |\lambda|\|v\|$ *para todo* $v \in V$ *y* $\lambda \in \Bbbk$

Definimos entonces una métrica en V como $d(v, w) = \|v - w\|$.

Ejemplo 3.1.2. *Asumamos V de dimensión finita y $\{v_1, v_2, ...v_n\}$ una base. Entonces tenemos los siguientes ejemplos de normas:*

a) $\|a_1v_1 + a_2v_2 + ... + a_nv_n\|_\infty = \max\limits_{1\leq i\leq n} |a_i|$ *a la que llamamos norma del supremo.*

b) Para cada $r \geq 1$, definimos la r-norma como
$\|a_1v_1 + a_2v_2 + ...a_nv_n\|_r = (|a_1|^r + |a_2|^r + ... + |a_n|^r)^{1/r}$.

Una vez que tenemos definida una métrica, nos podemos preguntar sobre si el espacio es completo o no respecto de esa métrica. Los siguientes resultados responden totalmente esta pregunta.

Proposición 3.1.3. *Sea V un espacio vectorial de dimensión finita sobre $\Bbbk$ un cuerpo completo. Sea $\{v_1, v_2, ..., v_m\}$ una base de V y sea $\| \ \|$ la norma del supremo con respecto a esa base. Entonces V es completo. Específicamente, una sucesión de Cauchy (w_n) con*

$$w_n = a_{1n}v_1 + a_{2n}v_2 + ... + a_{mn}v_m$$

converge si y solo si las sucesiones de sus coeficientes $(a_{1n}), (a_{2n}), ..., (a_{mn})$ son Cauchy en $\Bbbk$ y el límite de w_n es simplemente tomar límite en los coeficientes:

$$\lim_{n\to\infty} w_n = (\lim_{n\to\infty} a_{1n})v_1 + (\lim_{n\to\infty} a_{2n})v_2 + ... + (\lim_{n\to\infty} a_{mn})v_m.$$

Demostración. Como la norma es simplemente tomar el coeficiente de valor absoluto más grande, decir que $\|w_{n_1} - w_{n_2}\|$ tiende a cero es lo mismo que decir que todas las diferencias $a_{in_1} - a_{in_2}$ también tienden a cero. Entonces es claro el resultado.

□

Definición 3.1.4. *Decimos que dos normas $\| \ \|_1$ y $\| \ \|_2$ sobre un $\Bbbk$ espacio vectorial V son equivalentes si definen la misma topología, o equivalentemente, existen reales $C, D \geq 0$ tal que para todo $v \in V$ tenemos*

$$\|v\|_1 \leq C\|v\|_2 \qquad y \qquad \|v\|_2 \leq D\|v\|_1$$

Con el siguiente teorema probaremos que todas las normas definidas sobre un espacio vectorial de dimensión finita son equivalentes, y por tanto, por la proposición anterior, todas son completas.

Teorema 3.1.5. *Sea V un espacio vectorial de dimensión finita sobre un cuerpo completo $\Bbbk$. Entonces todas las normas en V son equivalentes.*

Demostración. Fijemos una base $\{v_1, v_2, ..., v_n\}$, sea $\| \ \|_\infty$ la norma del supremo y $\| \ \|$ otra norma cualquiera. Queremos probar que $\| \ \|$ es equivalente a la $\| \ \|_\infty$, es decir que

existen C y D tales que

$$\|v\| \leq C\|v\|_\infty \qquad \text{y} \qquad \|v\|_\infty \leq D\|v\|.$$

Comencemos probando la primera desigualdad: sea $v = a_1v_1 + ... + a_nv_n$. Luego

$$\begin{aligned}\|v\| &= \|a_1v_1 + ... + a_nv_n\| \\ &\leq |a_1|\|v_1\| + ... + |a_n|\|v_n\| \\ &\leq n \cdot \text{máx}\{|a_i|\} \cdot \text{máx}\{\|v_i\|\} = C \,\text{máx}\, |a_i| = C\|v\|_\infty\end{aligned}$$

donde tomamos $C = n \,\text{máx}\, \|v_i\|$.

Para la otra desigualdad haremos inducción en la dimensión de V. La desigualdad es trivialmente cierta para espacios de dimensión 1, ya que si $\{v\}$ es la base, basta tomar $D = 1/\|v\|$.
Para el paso inductivo asumamos que el teorema es cierto para espacios de dimensión $n-1$, en particular que todo espacio normado de dimensión $n-1$ es completo.
Supongamos que no existe D que cumpla la desigualdad, entonces $\|w\|/\|w\|_\infty$ está arbitrariamente cerca de cero cuando w varía en los vectores no nulos de V. Es decir que dado $m \in \mathbb{Z}^+$, existe un vector w_m tal que

$$\|w_m\| < \frac{1}{m}\|w_m\|_\infty.$$

Recordar que por definición, la norma del supremo de w_m es igual al máximo de los valores absolutos de los coeficiente de su expansión en la base, luego como la base es finita, debe existir un índice i tal que $\|w_m\|_\infty$ es igual al valor absoluto del coeficiente i-ésimo para infinitos m. A menos de reordenar la base, podemos suponer que $i = n$.
Sean $m_1 < m_2 < ... < m_k$ la sucesión de los m´s que cumplen lo anterior, es decir que si b_k es el n-ésimo coeficiente de w_{m_k} en su expresión en la base, entonces tenemos que $\|w_{m_k}\|_\infty = |b_k|$.
Consideremos entonces los vectores $b_k^{-1}w_{m_k}$. Estos cumplen que pueden ser escritos de la forma $b_k^{-1}w_{m_k} = u_k + v_n$ donde u_k vive en el subespacio W generado por los primeros $n-1$ vectores. Además tenemos que

$$\|u_k + v_n\| = \|b_k^{-1}w_{m_k}\| = |b_k|^{-1}\|w_{m_k}\| = \frac{\|w_{m_k}\|}{\|w_{m_k}\|_\infty} < \frac{1}{m_k}.$$

Luego

$$\|u_{k+1} - u_k\| \leq \|u_{k+1} + v_n\| + \|u_k + v_n\| < \frac{1}{m_{k+1}} + \frac{1}{m_k},$$

como los m_k son una sucesión creciente, entonce tenemos que $\|u_{k+1} - u_k\| \to 0$ cuando $k \to \infty$. Por lo tanto los u_k son una sucesión de Cauchy en el subespacio W de dimensión $n-1$. Luego por la hipótesis de inducción, sabemos que W es completo, entonces existe $u \in W$ tal que $u_k \to u$. Pero entonces tenemos

$$\|u + v_n\| = \lim_k \|u_k + v_n\| = 0,$$

lo que nos dice que $u = -v_n$, pero esto es un absurdo pues $v_n \notin W$, ergo debe de existir D que verifique la desigualdad.

□

Otra hecho que nos será de utilidad más adelante es que si tenemos un espacio vectorial de dimensión finita normado, y el cuerpo es localmente compacto, entonces el espacio vectorial también será localmente compacto. Es decir que la compacidad local se "transfiere"del cuerpo al espacio vectorial. Esto nos servirá, ya que recordemos que $\mathbb{Q}_p$ es localmente compacto, entonces gracias a este hecho, sus extensiones finitas también lo serán. Probemos este hecho:

Proposición 3.1.6. *Sea* $\Bbbk$ *un cuerpo completo localmente compacto, y* V *un espacio vectorial normado de dimensión finita sobre* $\Bbbk$*. Entonces* V *es localmente compacto.*

Demostración. Para probar que V es localmente compacto, nos basta con probar que $B = \{v \in V : \|v\| \leq 1\}$ es compacta. Por el teorema anterior, sabemos que podemos tomar cualquier norma pues todas son equivalentes y ser localmente compacto es una propiedad topológica. Utilizaremos entonces la norma del supremo con respecto a una base fija $\{v_1, v_2, .., v_n\}$. Luego un vector $v = a_1v_1 + a_2v_2 + ... + a_nv_n$ pertenece a B si y solo si todos los a_i pertenecen a la bola unidad cerrada en $\Bbbk$.
Recordemos una vez más que para probar que un conjunto es compacto, basta con probar que es completo y totalmente acotado.
Que B es completo es claro pues es un cerrado dentro del espacio V que es completo. Para probar que B es totalmente acotado usaremos que la bola unidad en $\Bbbk$ es localmente acotada. Dado ε, tomamos un cubrimiento finito por bolas de radio ε de la bola unidad de $\Bbbk$. Sean $c_1, c_1, ..., c_N$ los centros de esas bolas. Luego, consideremos en V los N^n vectores que tienen en cada coordenada de la base alguno de estos c_i. Consideremos entonces las bolas de radio ε centradas en estos vectores.

Afirmación: Estas bolas cubren B.

Demostración: Sea $v = a_1v_1 + a_2v_2 + ... + a_nv_n \in B$, como los coeficientes a_j están en la bola unidad en $\Bbbk$, sabemos que para cada a_j hay un c_i que está a distancia menor que ε; llamemos c_{i_j} al que verifica esto. Luego

$$\|(a_1v_1 + a_2v_2 + ... + a_nv_n) - (c_{i_1}v_1 + c_{i_2}v_2 + ... + c_{i_n}v_n)\|_\infty =$$

$$= \|(a_1 - c_{i_1})v_1 + (a_2 - c_{i_2})v_2 + ... + (a_n - c_{i_n})v_n\|_\infty =$$

$$= \text{máx}\{|a_1 - c_{i_1}|, |a_2 - c_{i_2}|, ..., |a_n - c_{i_n}| < \varepsilon.$$

Lo que prueba lo que queríamos y por ende B es compacto.

□

3.2 Extendiendo el valor absoluto p-ádico

Ahora que tenemos estas herramientas básicas, vamos a lo que nos interesa, las extensiones de $\mathbb{Q}_p$. Nuestro objetivo en esta sección es construir un valor absoluto p-ádico en las extensiones finitas de $\mathbb{Q}_p$ que por supuesto extienda al valor absoluto sobre $\mathbb{Q}_p$. Además probaremos que fijada una extensión este valor absoluto es único y que sus restricciones coinciden.
Comencemos con un corolario de lo probado en la sección anterior.

Corolario 3.2.1. *Sea K una extensión finita de $\mathbb{Q}_p$. Si existe un valor absoluto $|\ |$ en K que extienda el valor absoluto en $\mathbb{Q}_p$, entonces*

a) K es completo respecto a $|\ |$.

b) Dada una sucesión en K, podemos calcular su límite mediante calcular los límites de sus coeficientes respecto a una base dada $\{x_1, x_2, ..., x_n\}$ de K como $\mathbb{Q}_p$ espacio vectorial.

Demostración. Aplicación directa del Teorema 3.1.5 y la Proposición 3.1.3 pues un valor absoluto en K que extiende al valor absoluto en $\mathbb{Q}_p$ es una norma en K.

□

Este corolario nos deja un resultado importante.

Corolario 3.2.2. *Existe a lo mucho un valor absoluto en K que extiende al valor absoluto p-ádico en $\mathbb{Q}_p$.*

Demostración. Supongamos que tenemos dos valores absolutos en K que extienden al valor absoluto p-ádico, $|\ |_1$ y $|\ |_2$. Primero probaremos que son equivalentes. Para probar que son equivalentes, por La Proposición 1.2.8 tenemos que probar que para todo $x \in K$ tenemos que $|x|_1 < 1 \iff |x|_2 < 1$. Para ver esto, recordemos que $|x|_i < 1$ si y solo si $x^n \to 0$ con respecto a la topología definida por $|\ |_i$, pero ya sabemos que $|\ |_1$ y $|\ |_2$ son equivalentes como normas en el espacio vectorial K, luego definen la misma topología, y por lo tanto tenemos convergencia respecto de una si y solo si la tenemos respecto de

la otra, que es lo que queríamos probar.
Como $|\ |_1$ y $|\ |_2$ son equivalentes como valores absolutos, nuevamente por la Proposición 1.2.8, sabemos que existe un real α tal que $|x|_1 = |x|_2^\alpha$ para todo $x \in K$. Pero sabemos que $|x|_1$ y $|x|_2$ son iguales si $x \in \mathbb{Q}_p$, luego $\alpha = 1$ y por ende los valores absolutos coinciden.

□

Una consecuencia de la unicidad es que si tenemos dos extensiones K y L tal que $\mathbb{Q}_p \subset L \subset K$ y existen valores absolutos $|\ |_L$ en L y $|\ |_K$ en K que extienden al valor absoluto p-ádico, entonces la restricción de $|\ |_K$ a los elementos de L es un valor absoluto en L que extiende al p-ádico, entonces debe de coincidir con $|\ |_L$. Es decir, para todo $x \in L \subset K$, tenemos que $|x|_L = |x|_K$.

Antes de continuar recordamos algunas definiciones y propiedades de la teoría de cuerpos.
Sean K y F cuerpos de característica cero tales que $F \subset K$ y $[K : F] < \infty$. Sea C la clausura algebraica de F. Decimos que la extensión K/F es normal si todos los morfismos $\sigma : K \longrightarrow C$ que son la identidad en F tienen la misma imagen (es decir K visto dentro de C).
Si la extensión es normal, podemos pensar a los σ como automorfismos de K que inducen la identidad en F. Como estamos en una extensión normal finita, sabemos que los σ forman un grupo finito (que es justamente el grupo de Galois de la extensión).
Un resultado sencillo es que dada una extensión finita K/F, existe una extensión finita normal de F que contiene a K. Esto nos será muy útil para construir el valor absoluto, porque nos dice gracias a lo dicho anteriormente, que podemos suponer que las extensiones son normales ya que luego simplemente habría que restringir el valor absoluto.
Definamos entonces la herramienta fundamental que nos permitirá construir nuestro valor absoluto.

Proposición 3.2.3 (**Definición de** $N_{K/F}$)**.** *Sea K un extensión finita de F. Definimos la función norma de K a F $N_{K/F} : K \to F$, de las siguientes formas (que son equivalentes):*

a) Dado $\alpha \in K$, pensemos a K como un espacio vectorial de dimensión finita sobre F, y consideremos el mapa lineal de K en K dado por multiplicar por α. Como es lineal, le corresponde una matriz; entonces definimos $N_{K/F}(\alpha)$ como el determinante de esa matriz.

b) Sea $\alpha \in K$. Consideremos entonces la subextensión $F(\alpha)$, y sea $r = [K : F(\alpha)]$ el grado de K sobre $F(\alpha)$. Si $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in F[X]$ es el polinomio minimal de α sobre F, entonces definimos $N_{K/F}(\alpha) = (-1)^{nr}a_0^r$.

c) Si la extensión K/F es normal, entonces podemos definir $N_{K/F}(\alpha)$ como el producto de todos los $\sigma(\alpha)$, donde σ recorre el grupo de Galois de K/F.

DEMOSTRACIÓN. Tenemos que ver que las tres definiciones dadas son efectivamente equivalentes. Comencemos probando $(a) \iff (b)$. Para esto, basta con calcular $N_{K/F}$ como en (a) y ver que coincide con la definición de (b).
Comencemos por el caso en el que $K = F(\alpha)$. Luego, sabemos que $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base de K como F espacio vectorial. Por otro lado, del polinomio minimal f, podemos despejar que $\alpha^n = \sum_{k=0}^{n-1} -a_i\alpha^i$. Entonces si consideramos el mapa multiplicar por α y escribimos su matriz asociada en esa base, obtenemos la matriz $n \times n$:

$$A = \begin{pmatrix} 0 & 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & 0 & ... & 0 & -a_1 \\ 0 & 1 & 0 & ... & 0 & -a_2 \\ 0 & 0 & 1 & ... & 0 & -a_3 \\ . & & & . & & . \\ . & & & . & & . \\ . & & & . & & . \\ 0 & 0 & 0 & ... & 1 & -a_{n-1} \end{pmatrix}.$$

Luego, calculando su determinante (por ejemplo por la primer fila), obtenemos que $\det(A) = (-a_0) \times (-1)^{n+1} = a_0(-1)^{n+2} = a_0(-1)^n$ como queríamos probar.

Supongamos ahora que $K \neq F(\alpha)$, $n = [F(\alpha) : F]$ y $r = [K : F(\alpha)]$. Podemos entonces encontrar una base $\{b_1, b_2, ..., b_r\}$ de K como $F(\alpha)$ espacio vectorial. Nuevamente recordar que $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ es una base de $F(\alpha)$ como F-espacio, por lo tanto, $\{\alpha^i b_j : i = 0, 1, .., n-1 \quad \text{y} \quad j = 1, 2, ..., r\}$ es base de K como F-espacio. Luego, la matriz asociada al mapa multiplicar por α en esta base es la siguiente matriz de $nr \times nr$:

$$B = \begin{pmatrix} A & O & O & ... & O & O \\ O & A & O & ... & O & O \\ O & O & A & ... & O & O \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ O & O & O & ... & A & O \\ O & O & O & ... & O & A \end{pmatrix},$$

donde O es la matriz nula y A es la matriz de la parte anterior. Entonces

$$\det(B) = (\det(A))^r = (a_0(-1)^n)^r = (-1)^{nr}a_0^r.$$

Supongamos que la extensión es normal y probemos $(b) \iff (c)$, para esto, nuevamente, lo único que hay que hacer es calcular $N_{K/F}$ como en (c) y ver que da lo mismo que en (b).
Como K tiene grado r sobre el cuerpo intermedio $F(\alpha)$, entonces $H = Gal(K/F(\alpha))$ subgrupo de $Gal(K/F)$, tiene orden r. Luego, si consideramos el cociente $Gal(K/F)/H$, cada clase lateral del subgrupo H actúa fijando una raíz específica de $f(x)$. Entonces, como H tiene r elementos, en el producto que tenemos que considerar aparece cada raíz de f elevada a la r. Por lo tanto, si $f(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ en K, tenemos que :

$$\prod_{\sigma \in Gal(K/F)} \sigma(\alpha) = \prod_{i=1}^{n} \alpha_i^r = \left(\prod_{i=1}^{n} \alpha_i \right)^r = ((-1)^n a_0)^r = (-1)^{nr} a_0^r,$$

como queríamos probar. □

Observación 3.2.4.

- *Si $\alpha \in F$, entonces $N_{K/F} = \alpha^n$ donde $n = [K : F]$.*
- *Las normas son multiplicativas (pues los determinantes lo son). Es decir $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$ para todo $\alpha, \beta \in K$.*
- *Si tenemos tres cuerpos $F \subset L \subset K$, entonces para todo $\alpha \in K$ tenemos que*

$$N_{L/F}(N_{K/L}(\alpha)) = N_{K/F}(\alpha)$$

Para ver que la norma va a tener un papel central al la hora de construir el valor absoluto notemos lo siguiente: Supongamos que $K/\mathbb{Q}_p$ es una extensión normal y sea σ un automorfismo. Si $|\ |$ es un valor absoluto en K, entonces la función que manda $x \mapsto |\sigma(x)|$ es también un valor absoluto en K, y también nos da el valor absoluto p-ádico sobre $\mathbb{Q}_p$ pues σ es la identidad en $\mathbb{Q}_p$. Pero como ya probamos, hay a lo mucho un valor absoluto que cumple lo anterior, entonces debemos tener que $|\sigma(x)| = |x|$ para todo $x \in K$. Luego, multiplicando sobre todos los σ's (y recordando que hay exactamente $n = [K : \mathbb{Q}_p]$) tenemos que

$$\left| \prod_{\sigma} \sigma(x) \right| = |x|^n.$$

Como el producto es igual a la norma, concluimos que

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

lo que nos da una fórmula para el valor absoluto en K que solo depende del valor absoluto p-ádico, pues la norma es un elemento en $\mathbb{Q}_p$.
Lo anterior solamente nos sirve en el caso en el que la extensión es normal. Veremos a continuación que en realidad esta construcción funciona para toda extensión finita de $\mathbb{Q}_p$.

Para ello, comencemos con el siguiente lema, que nos dice que el valor de $\sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|}$ es igual para todo cuerpo K que contenga a x.

Lema 3.2.5. *Sean L y K extensiones finitas de $\mathbb{Q}_p$ tales que $\mathbb{Q}_p \subset L \subset K$. Sea $x \in L$, $m = [L : \mathbb{Q}_p]$ y $n = [K : \mathbb{Q}_p]$. Entonces tenemos que*

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

Demostración. Sabemos que $N_{L/\mathbb{Q}_p}(N_{K/L}(x)) = N_{K/\mathbb{Q}_p}(x)$ y que $N_{K/L}(x) = x^{[K:L]}$ (pues $x \in L$). Recordando que $[K : \mathbb{Q}_p] = [K : L][L : \mathbb{Q}_p]$, es decir que $[K : L] = \frac{n}{m} \in \mathbb{Z}^+$, tenemos que

$$N_{K/\mathbb{Q}_p}(x) = N_{L/\mathbb{Q}_p}(x^{\frac{n}{m}}) = (N_{L/\mathbb{Q}_p}(x))^{\frac{n}{m}}.$$

Luego, como todo vive en $\mathbb{Q}_p$, tomando valor absoluto y raíz n-ésima, tenemos lo que queremos.

□

Probemos entonces que efectivamente esa fórmula nos define un valor absoluto:

Teorema 3.2.6. *Dada una extensión finita $K/\mathbb{Q}_p$ de grado n , la función $|\ | : K \longrightarrow \mathbb{R}_{\geq 0}$ dada por*

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

es un valor absoluto no arquimediano en K que extiende al valor absoluto p-ádico de $\mathbb{Q}_p$.

Demostración. Primero notemos que $|x| = 0$ si y solo si $N_{K/\mathbb{Q}_p}(x) = 0$, lo cual solo pasa si multiplicar por x no es invertible; como K es un cuerpo, esto solo pasa si $x = 0$. Por otro lado, como $N_{K/\mathbb{Q}_p}(xy) = N_{K/\mathbb{Q}_p}(x)N_{K/\mathbb{Q}_p}(y)$, entonces

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

Además, si $x \in \mathbb{Q}_p$, entonces $N_{K/\mathbb{Q}_p}(x) = x^n$, por lo tanto, $|x| = \sqrt[n]{|x|_p^n} = |x|_p$ pues el valor absoluto es un real no negativo.
Para terminar, nos queda probar la propiedad no arquimediana. Para esto probaremos la condición (c) del Lema 1.1.7. Por la definición de $|\ |$, es claro que $|x| \leq 1 \iff |N_{K/\mathbb{Q}_p}(x)|_p \leq 1$. Por lo tanto, queremos probar que

$$|N_{K/\mathbb{Q}_p}(x)|_p \leq 1 \Longrightarrow |N_{K/\mathbb{Q}_p}(x-1)|_p \leq 1,$$

o dicho de otro modo, que

$$N_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p \Longrightarrow N_{K/\mathbb{Q}_p}(x-1) \in \mathbb{Z}_p.$$

Para esto, usaremos la definición de la norma que involucra al polinomio minimal. Por el Lema anterior, podemos asumir que $K = \mathbb{Q}_p(x)$, el menor cuerpo que contiene a x (y por lo tanto, también a $x-1$). Sea $f(X) = X^n + a_{n-1}X^{n-1} + .. + a_1X + a_0$ el polinomio minimal de x. Como $\mathbb{Q}_p(x) = \mathbb{Q}_p(x-1)$, el polinomio minimal de $x-1$ debe tener el mismo grado que f y tener a $x-1$ como raíz; entonces el polinomio minimal tiene que ser

$$\begin{aligned} f(X+1) &= (X+1)^n + a_{n-1}(X+1)^{n-1} + ... + a_1(X+1) + a_0 \\ &= X^n + (a_{n-1}+n)X^{n-1} + ... + (1 + a_{n-1} + ... + a_1 + a_0). \end{aligned}$$

Por lo tanto, usando la segunda definición de la norma, tenemos que

$$N_{K/\mathbb{Q}_p}(x) = (-1)^n a_0$$

y

$$N_{K/\mathbb{Q}_p}(x-1) = (-1)^n(1 + a_{n-1} + \cdots + a_1 + a_0).$$

Entonces para probar lo que queremos, necesitamos probar que si $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ es un polinomio irreducible y $a_0 \in \mathbb{Z}_p$, entonces $(1 + a_{n-1} + ... + a_1 + a_0) \in \mathbb{Z}_p$. Probaremos algo más fuerte en la siguiente afirmación y por ende quedará la demostración del Teorema.

Afirmación: Si $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ es un polinomio irreducible con coeficientes en $\mathbb{Q}_p$, y $a_0 \in \mathbb{Z}_p$, entonces todos los coeficientes $a_{n-1}, ..., a_1, a_0$ pertenecen a $\mathbb{Z}_p$.

Demostración: La idea es usar el Lema de Hensel para polinomios, para probar que si alguno de los coeficientes no están en $\mathbb{Z}_p$, entonces $f(X)$ es reducible.
Sea $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ y asumamos que $a_0 \in \mathbb{Z}_p$ y que algún $a_j \notin \mathbb{Z}_p$. Sea m el exponente más chico tal que $p^m a_i \in \mathbb{Z}_p$ para todo i. Luego multiplicando por p^m definimos

$$g(X) = p^m f(X) = b_n X^n + b_{n-1}X^{n-1} + ... + b_1X + b_0,$$

donde $b_i = p^m a_i$ y como f es mónico, $b_n = p^m$. Por nuestra elección de m, tenemos que todos los b_i pertenecen a $\mathbb{Z}_p$ y por lo menos uno no es divisible por p. Sea k el i más chico tal que b_i no es divisible por p. Luego tenemos que $0 < k < n$, y reduciendo módulo p

$$g(X) \equiv (b_n X^{n-k} + ... + b_k)X^k \quad (mod\ p).$$

Como $b_k \not\equiv 0\ (mod\ p)$, claramente los dos factores son coprimos módulo p. Entonces, por el Lema de Hensel para polinomios, tenemos que $g(X) = p^m f(X)$ es reducible y por lo

tanto $f(X)$ lo es. Esta contradicción prueba la Afirmación y por lo tanto el Teorema. □

Entonces hemos probado que dada una extensión finita K de $\mathbb{Q}_p$, existe un único valor absoluto en K que extiende al valor absoluto p-ádico de $\mathbb{Q}_p$; le llamaremos a este, el valor absoluto p-ádico en K.

Consideremos la clausura algebraica de $\mathbb{Q}_p$, a la que denotamos como $\overline{\mathbb{Q}_p}$. La construcción ya hecha, nos permite construir un valor absoluto en $\overline{\mathbb{Q}_p}$. La idea es la siguiente: dado $x \in \overline{\mathbb{Q}_p}$, la extensión $\mathbb{Q}_p(x)$ es finita, luego, como x vive en una extensión finita, podemos definir $|x|$ usando el único valor absoluto en $\mathbb{Q}_p(x)$ que extiende al p-ádico de $\mathbb{Q}_p$. Pero ya sabemos que este valor absoluto no depende de la extensión, por lo que tiene sentido hablar del valor absoluto de un elemento $x \in \overline{\mathbb{Q}_p}$. Por lo tanto, tenemos una función $|\ | : \overline{\mathbb{Q}}_p \longrightarrow \mathbb{R}_{\geq 0}$ que es un valor absoluto que extiende al de $\mathbb{Q}_p$ y por la construcción es claramente único.

En la Sección 3.4 veremos que $\overline{\mathbb{Q}}_p$ no es completo respecto a este valor absoluto; pero para terminar esta sección, probaremos que $\overline{\mathbb{Q}}_p$ es una extensión infinita de $\mathbb{Q}_p$. Para probar esto, nos basta con probar que existen polinomios irreducibles de grado arbitrariamente grande en $\mathbb{Q}_p$, pues la raíz de un polinomio irreducible de grado n nos genera una extensión de grado n y por lo tanto, $\overline{\mathbb{Q}}_p$ contendría extensiones de grado n para n arbitrariamente grande.
Para probar esto, precisaremos el Lema de Gauss, el cual recordamos a continuación.

Lema 3.2.7 (Lema de Gauss en $\mathbb{Q}_p$)**.** *Sea $f(X) \in \mathbb{Z}_p[X]$ tal que f se factoriza (de una forma no trivial) en $\mathbb{Q}_p[X]$, es decir*

$$f(X) = g(X)h(X)$$

con $g(X), h(X) \in \mathbb{Q}_p[X]$ y no constantes. Entonces, existen polinomios no constantes $g_0(X), h_0(X) \in \mathbb{Z}_p[X]$ tal que $f(X) = g_0(X)h_0(X)$.

En particular:

Corolario 3.2.8. *Sea $f(X) \in \mathbb{Z}_p[X]$ un polinomio mónico cuya reducción módulo p es irreducible en $\mathbb{F}_p[X]$. Entonces $f(X)$ es irreducible en $\mathbb{Q}_p[X]$.*

Demostración. Si $f(X)$ factoriza sobre $\mathbb{Q}_p$, entonces factoriza sobre $\mathbb{Z}_p$ por el Lema de Gauss; luego, reduciendo módulo p tenemos una factorización sobre $\mathbb{F}_p$ (no trivial pues f era mónico y por lo tanto también sus factores en $\mathbb{Z}_p$), lo cual es un absurdo.

□

Por último, recordemos el siguiente resultado: Para todo $n > 0$ existe un polinomio mónico irreducible de grado n en $\mathbb{F}_p[X]$ cuyas raíces generan la única extensión de grado n de $\mathbb{F}_p$.
Luego, dado $f(X)$, un polinomio de grado n que cumple lo anterior, tomando cualquier levantado de f a un polinomio mónico en $\mathbb{Z}_p[X]$ (por ejemplo f visto en $\mathbb{Z}_p[X]$), nos da

un polinomio irreducible de grado n en $\mathbb{Q}_p[X]$ (gracias al corolario anterior).
Por lo tanto, hemos probado que dado n, existen polinomios irreducibles de grado n en $\mathbb{Q}_p[X]$. Esto implica, como dijimos anteriormente, el siguiente resultado:

Corolario 3.2.9. *$\overline{\mathbb{Q}}_p$ es una extensión infinita de $\mathbb{Q}_p$.*

Este resultado nos permite, una vez más, ver el contraste en el comportamiento entre $\mathbb{R}$ y $\mathbb{Q}_p$, pues la clausura algebraica de $\mathbb{R}$ es $\mathbb{C}$ que es una extensión de grado dos y por lo tanto, es automáticamente completa respecto al valor absoluto infinito extendido.

Otra posible prueba de este hecho, es utilizando el Criterio de irreducibilidad de Eisenstein el cual enunciamos a continuación en nuestro contexto.

Proposición 3.2.10 (Criterio de irreducibilidad de Eisenstein)**.** *Sea*

$$f(X) = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}_p$$

un polinomio que satisface las siguientes condiciones:

a) $|a_n| = 1$,

b) $|a_i| < 1$ *para* $0 \leq i < n$,

c) $|a_0| = 1/p$.

Entonces $f(X)$ es irreducible sobre $\mathbb{Q}_p$.

Luego, es claro que podemos construir polinomios de grado tan grande como uno quiera que cumplan las condiciones del Criterio de Eisenstein y por lo tanto, nuevamente tenemos que $\overline{\mathbb{Q}}_p$ es una extensión infinita de $\mathbb{Q}_p$.

3.3 Extensiones finitas

El primer objetivo de esta sección es obtener información sobre las extensiones finitas de $\mathbb{Q}_p$. En particular, queremos ver cuánto de la estructura que vimos que tiene $\mathbb{Q}_p$ se extiende.
El segundo objetivo es encontrar una clasificación de las extensiones de $\mathbb{Q}_p$ y brindar una descripción sobre las propiedades que cumplen cada uno de los posibles tipos de extensión.

En esta sección K denotará una extensión finita de grado n de $\mathbb{Q}_p$ y $|\ | = |\ |_p$ será el valor absoluto p-ádico extendido a K.
Ya sabemos que K es localmente compacto y completo respecto al valor absoluto p-ádico y tenemos una fórmula para calcular explícitamente el valor absoluto de un elemento en función de la norma y del valor absoluto en $\mathbb{Q}_p$.
A continuación, probaremos que este valor absoluto extendido es discreto [1]. Recordemos

[1] En el sentido de que la valuación que lo define es discreta.

que en $\mathbb{Q}_p$, el valor absoluto de un elemento no nulo siempre era de la forma p^v con v un entero. Mirando la fórmula del valor absoluto en K:

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

vemos que el valor absoluto de un elemento no nulo $x \in K$ es de la forma p^v donde $v \in \frac{1}{n}\mathbb{Z}$ pues estamos tomando raíz n-ésima del valor absoluto de un elemento de $\mathbb{Q}_p$. Esto nos permite definir:

Definición 3.3.1. *Sea K una extensión finita de $\mathbb{Q}_p$ y $|\ |$ el valor absoluto p-ádico en K. Para todo $x \in K$, $x \neq 0$, definimos la valuación p-ádica $v_p(x)$ como el único número racional que cumple que*

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

Extendemos la definición formalmente a todo K, diciendo que $v_p(0) = \infty$.

Observación 3.3.2. *Es claro que v_p es una valuación en el sentido de que:*

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

b) $v_p(xy) = v_p(x) + v_p(y)$,

usando la convención usual cuando una de los elementos es cero.
Además, tenemos la siguiente fórmula que se deduce de la definición del valor absoluto :

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

dónde en la derecha tenemos la valuación p-ádica en $\mathbb{Q}_p$.

Sabemos que la imagen de v_p está contenida en $\frac{1}{n}\mathbb{Z}$, pero no sabemos todavía cómo es exactamente. El siguiente resultado nos da una descripción más precisa de la imagen de v_p.

Proposición 3.3.3. *La valuación p-ádica v_p es un homomorfismo del grupo multiplicativo $K^\times$ al grupo aditivo $\mathbb{Q}$. Su imagen es de la forma $\frac{1}{e}\mathbb{Z}$ donde e es un divisor de $n = [K : \mathbb{Q}_p]$.*

Demostración. Que v_p es un morfismo es la parte (b) de la observación anterior; por lo tanto su imagen es un subgrupo aditivo de $\mathbb{Q}$. Ya sabemos que la imagen está contenida en $\frac{1}{n}\mathbb{Z}$ y que contiene a $\mathbb{Z}$ pues la imagen de de v_p restricta a $\mathbb{Q}_p^\times$ contiene a $\mathbb{Z}$. Sea $x \in K$ tal que $v_p(x) = \frac{d}{e}$ con $(d, e) = 1$ y e sea lo más grande posible (es claro que los denominadores están acotados pues e tiene que ser un divisor de n). Luego, como d y e son coprimos, existe un múltiplo de d congruente con 1 módulo e, es decir, existen r y s

tales que $rd = 1 + se$. Pero entonces

$$r\frac{d}{e} = \frac{1+se}{e} = \frac{1}{e} + s$$

está en la imagen. Como $s \in \mathbb{Z}$, entonces $1/e$ tiene que estar en la imagen. Como e era el denominador más grande en la imagen, entonces la imagen debe ser exactamente $\frac{1}{e}\mathbb{Z}$.

□

Definición 3.3.4. *Sea $K/\mathbb{Q}_p$ una extensión finita, y sea $e = e(K/\mathbb{Q}_p)$ el único entero positivo (que divide a $n = [K : \mathbb{Q}_p]$) que cumple que*

$$v_p(K^\times) = \frac{1}{e}\mathbb{Z}.$$

Decimos que e es el índice de ramificación de K sobre $\mathbb{Q}_p$. Decimos que la extensión $K/\mathbb{Q}_p$ es :

- *no ramificada si $e = 1$,*
- *ramificada si $e > 1$, y*
- *totalmente ramificada si $e = n$.*

Por último, definimos $f = f(K/\mathbb{Q}_p) = n/e$ el grado residual de K sobre $\mathbb{Q}_p$ (veremos en el Teorema 3.3.8 el porqué de este nombre).

Ejemplo 3.3.5. *Veamos un ejemplo de cada caso:*

a) Como 2 no es cuadrado módulo 5, por Hensel sabemos que 2 no es cuadrado en $\mathbb{Q}_5$. Luego la extensión $\mathbb{Q}_5(\sqrt{2})$ es una extensión de grado 2 con base $\{1, \sqrt{2}\}$. Luego, sabemos que dado un elemento $a + b\sqrt{2} \in \mathbb{Q}_5(\sqrt{2})$,

$$\begin{aligned} v_5(a+b\sqrt{2}) &= \frac{1}{2}v_5(N_{Q_5(\sqrt{2})}(a+b\sqrt{2})) \\ &= \frac{1}{2}v_5((a+b\sqrt{2})(a-b\sqrt{2})) \\ &= \frac{1}{2}v_5(a^2-2b^2). \end{aligned}$$

Lo que queremos probar es que esta extensión es no ramificada, es decir $e = 1$. Para ello, tenemos que ver que para todo $a, b \in \mathbb{Q}_p$, $v_5(a^2 - 2b^2) \geq 2$ o que $v_5(a^2 - 2b^2) = 0$. Para esto, basta estudiar los posibles casos módulo $25 = 5^2$ y observar que en todos los posibles casos (finitos casos) $a^2 - 2b^2$ es múltiplo de 25 o ni siquiera es múltiplo de 5. En este caso en particular, nos basta estudiar módulo 5, ya que el único momento en el que $a^2 - 2b^2 \equiv 0 \pmod 5$ es cuando $a \equiv$

$b \equiv 0 \ (mod\ 5)$ *y como aparecen al cuadrado, implica que* $a^2 - 2b^2 \equiv 0 \ (mod\ 25)$.

b) Para el segundo ejemplo, tomemos nuevamente $p = 5$. *Luego es claro que* 5 *no es cuadrado en* $\mathbb{Q}_5$, *por lo que* $\mathbb{Q}_5(\sqrt{5})$ *es una extensión de grado* 2 *con base* $\{1, \sqrt{5}\}$. *En este caso, como* e *tiene que ser un divisor del grado de la extensión,* $e = 1$ *o* $e = 2$. *Para probar que* $e = 2$, *nos basta con encontrar un elemento en* $\mathbb{Q}_5(\sqrt{5})$ *que que cumpla que su valuación sea* $1/2$. *Para esto, consideremos el elemento* $\sqrt{5}$. *Luego*

$$v_5(\sqrt{5}) = \frac{1}{2}v_5(N_{Q_5(\sqrt{5})}(\sqrt{5})) = \frac{1}{2}v_5((\sqrt{5})(-\sqrt{5})) = \frac{1}{2}v_5(-5) = \frac{1}{2}$$

como uno esperaría. Luego $e = 2$ *y por ende esta extensión es una extensión totalmente ramificada.*

c) El tercer ejemplo es un poco más complicado. Tomemos $p = 3$ *y adjuntemos a* $\mathbb{Q}_3$, *una raíz cúbica primitiva de la unidad* ζ *y la raíz cuadrada de dos; es decir, consideremos* $F = \mathbb{Q}_3(\zeta, \sqrt{2})$. F *es una extensión de grado 4, con base* $\{1, \zeta, \sqrt{2}, \zeta\sqrt{2}\}$. *Lo que queremos ver, es que en este ejemplo tenemos una extensión ramificada pero no totalmente ramificada (es decir, que* $e = 2$). *Para esto comencemos por calcular la valuación de* $x = 1 - \zeta$:

$$N_{F/\mathbb{Q}_3}(1-\zeta) = N_{Q_3(\zeta)/\mathbb{Q}_3}(N_{F/\mathbb{Q}_3(\zeta)}(1-\zeta)) = N_{Q_3(\zeta)/\mathbb{Q}_3}(1-\zeta)^2.$$

(Recordar que F *es una extensión de grado* 2 *de* $\mathbb{Q}_3(\zeta)$.*) Luego, para calcular la norma tomamos la base* $\{1, \zeta\}$ *de* $\mathbb{Q}_3(\zeta)$ *sobre* $\mathbb{Q}_3$, *con lo que la matriz de multiplicar por* $1 - \zeta$ *es*

$$\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix},$$

cuyo determinante es 3. *Entonces tenemos que* $N_{F/\mathbb{Q}_3}(1 - \zeta) = 9$ *y por lo tanto*

$$v_3(1-\zeta) = \frac{1}{4}v_3(9) = \frac{1}{2}.$$

Por otro lado, se puede probar de forma análoga al ejemplo (a) *que la extensión* $\mathbb{Q}_3(\sqrt{2})$ *es no ramificada; por lo tanto el índice de ramificación de* F *es* 1 *o* 2, *pero como* $v_3(1 - \zeta) = \frac{1}{2}$, *entonces* $e(F/\mathbb{Q}_3) = 2$.

En $\mathbb{Q}_p$, el número p juega un rol sumamente importante, pues es un elemento con la valuación positiva más chica posible, $v_p(p) = 1$. Esto significaba que cualquier elemento en $x \in \mathbb{Z}_p$ con $v_p(x) > 0$ era divisible por p y de hecho, $v_p(x)$ expresaba la multiplicidad de un elemento; es decir que cualquier elemento $x \in \mathbb{Q}_p$ puede ser escrito de la forma $x = p^{v_p(x)}u$ donde u es un elemento tal que $v_p(u) = 0$.
Para poder hacer algo similar en K, necesitamos un elemento cuya valuación sea exactamente $1/e$; pero $1/e$ esta en el grupo de valuación, por lo que existe un elemento que cumpla lo anterior.

Definición 3.3.6. *Sea $K/\mathbb{Q}_p$ una extensión finita, y sea $e = e(K/\mathbb{Q}_p)$. Entonces decimos que un elemento π que cumpla que $v_p(\pi) = 1/e$ es un uniformizador.*

Observemos que hay muchos uniformizadores en K, al igual que e $\mathbb{Z}_p$ hay muchos elementos con valuación igual a 1. A partir de ahora, fijamos un uniformizador cualquiera π, y en el caso de no ramificación ($e = 1$), tomaremos $\pi = p$.

A continuación, describiremos la estructura algebraica en K. Para esto, fijemos algo de notación: sea $\mathcal{O} = \mathcal{O}_K = \{x \in K : v_p(x) \geq 0\}$, el anillo de valuación de K, y $\mathfrak{p} = \mathfrak{p}_K = \{x \in K : v_p(x) > 0\}$, su ideal maximal.
Como vimos en la Sección 2.1, $\mathcal{O}_K$ es un anillo local y su cuerpo de residuos es el cociente $\kappa = \mathcal{O}_K/\mathfrak{p}_K$. Luego, tenemos la siguiente proposición.

Proposición 3.3.7. *Sea π un uniformizador fijo en K. Entonces:*

a) El ideal $\mathfrak{p} \subset \mathcal{O}$ es principal y π es un generador.

b) Todo elemento $x \in K^\times$ puede ser escrito de la forma $x = u\pi^{ev_p(x)}$, donde $u \in \mathcal{O}_K^\times$ es una unidad, es decir $v_p(u) = 0$. En particular, $K = \mathcal{O}_K[\frac{1}{\pi}]$.

c) El cuerpo de residuos κ es una extensión finita de $\mathbb{F}_p$ de grado menor o igual al grado $[K : \mathbb{Q}_p]$.

d) Todo elemento de $\mathcal{O}_K$ es la raíz de un polinomio mónico con coeficientes en $\mathbb{Z}_p$.

e) Recíprocamente, si $x \in K$ es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}_p$, entonces $x \in \mathcal{O}_K$.

f) $\mathcal{O}$ es un anillo topológico compacto. Los conjuntos $\pi^m\mathcal{O}$, $m \in \mathbb{Z}$, son una familia fundamental de entornos de cero en K. K es un espacio topológico localmente compacto, totalmente disconexo y Hausdorff.

g) Sea q el número de elementos del cuerpo residual κ, y sea $A = \{c_1, c_2, ..., c_q\} \subset \mathcal{O}$ un conjunto de representantes de κ. Entonces, todo elemento $x \in K$ tiene una representación única como expansión p-ádica (o π-ádica):

$$x = \sum_{i=-m}^{\infty} a_i \pi^i,$$

donde cada $a_i \in A$.

Demostración.

a) Notemos que como $\mathfrak{p}$ es un ideal maximal, nos basta con probar que esta contenido dentro de $\pi\mathcal{O}$ para probar la afirmación. Pero esto es sencillo pues

$$\begin{aligned} x \in \mathfrak{p} &\Longrightarrow v_p(x) > 0 \Longrightarrow v_p(x) \geq 1/e \\ &\Longrightarrow v_p(\pi^{-1}x) \geq 0 \Longrightarrow \pi^{-1}x \in \mathcal{O} \\ &\Longrightarrow x \in \pi\mathcal{O}. \end{aligned}$$

b) Nos basta con probar que

$$\frac{x}{\pi^{ev_p(x)}}$$

es una unidad, es decir que tiene valuación cero. Pero esto es claro pues

$$\begin{aligned} v_p\left(\frac{x}{\pi^{ev_p(x)}}\right) = v_p(x) + v_p(\pi^{-ev_p(x)}) &= v_p(x) + (-ev_p(x))v_p(\pi) \\ &= v_p(x) - v_p(x) \cdot e \cdot \frac{1}{e} \\ &= 0. \end{aligned}$$

c) Primero veamos que efectivamente $\kappa = \mathcal{O}_K/\mathfrak{p}$ es una extensión de $\mathbb{F}_p$. Para ello consideremos el morfismo de anillos $\varphi : \mathbb{Z}_p \longrightarrow \mathcal{O}/\mathfrak{p}$ dado por $x \mapsto x$ (mód $\mathfrak{p}$) (recordar que $\mathbb{Z}_p \subset \mathcal{O}$). Ahora observemos lo siguiente:

$$\ker\varphi = \{x \in \mathbb{Z}_p : x \in \mathfrak{p}\} = \{x \in \mathbb{Z}_p : x \in \pi\mathcal{O}\} = \mathbb{Z}_p \cap \pi\mathcal{O} = p\mathbb{Z}_p,$$

donde la última igualdad se da pues $x \in \mathbb{Z}_p \cap \pi\mathcal{O} \iff v_p(x) \in \mathbb{Z}$ y $v_p(x) \geq 1/e \iff v_p(x) \geq 1$. Luego, como $\ker\varphi \subset \mathfrak{p}$, por el teorema de isomorfismo de anillos, sabemos que existe un morfismo de cuerpos $\tilde{\varphi} : \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p \longrightarrow \mathcal{O}/\mathfrak{p}$ tal que $red_p \circ \tilde{\varphi} = \varphi$ donde red_p es el mapa reducción módulo $p\mathbb{Z}_p$ de $\mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p\mathbb{Z}_p$. Como los morfismos de cuerpos son inyectivos, sabemos que κ es una extensión de $\mathbb{F}_p$.
Supongamos que tenemos un subconjunto $\{x_1, ..., x_m\}$ de K linealmente dependiente sobre $\mathbb{Q}_p$, es decir que

$$\sum_{i=1}^{m} a_i x_i = 0$$

donde los a_i pertenecen a $\mathbb{Q}_p$, luego, a menos de multiplicar por potencias suficientemente grandes de p y de π, podemos suponer que los $x_i \in \mathcal{O}_K$, que los $a_i \in \mathbb{Z}_p$ y que existe un k tal que $a_k \notin p\mathbb{Z}_p$. Entonces si $\tilde{a}_i$ y $\tilde{x}_i$ son las reducciones módulo $\mathfrak{p}$ de los a_i y los x_i, tenemos que

$$\sum_{i=1}^{m} \tilde{a}_i \tilde{x}_i \equiv 0 \pmod{\mathfrak{p}},$$

en donde gracias a la definición de $\tilde{\varphi}$, tenemos que $\tilde{a}_i \in \mathbb{F}_p$, $\tilde{a}_k \neq 0$ y $\tilde{x} \in \kappa$; por lo que obtenemos un conjunto de κ linealmente dependiente sobre $\mathbb{F}_p$. Luego $[\kappa : \mathbb{F}_p] \leq [K : \mathbb{Q}_p]$.

d) Sea $\alpha \in \mathcal{O}$, y sea $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ su polinomio minimal sobre $\mathbb{Q}_p$. Luego, como $\alpha \in \mathcal{O}$, sabemos que $v_p(\alpha) \geq 0$, lo que implica (por la definición de la valuación) que

$$v_p(N_{K/\mathbb{Q}_p}(\alpha)) \geq 0.$$

Además, si $r = [K : \mathbb{Q}_p(\alpha)]$, sabemos que $N_{K/\mathbb{Q}_p}(\alpha) = (-1)^{nr}a_0^r$; luego, juntando todo, tenemos

$$0 \leq v_p(N_{K/\mathbb{Q}_p}(\alpha)) = v_p((-1)^{nr}a_0^r) = v_p(a_0^r) = v_p(a_0)^r,$$

por lo tanto, $v_p(a_0) \geq 0$; es decir que $a_0 \in \mathbb{Z}_p$. Finalizamos aplicando la Afirmación dentro del Lema 3.2.5.

e) Observar que podemos suponer que el polinomio f mónico con coeficientes en $\mathbb{Z}_p$ que tiene como raíz a x es el polinomio minimal de x sobre $\mathbb{Q}_p$, ya que si no lo fuera, gracias al Lema de Gauss, podemos hallar una factorización en $\mathbb{Z}[X]$, y ahora uno de estos tiene como raíz a x. Seguimos este procedimiento hasta llegar a un polinomio mónico, irreducible y con coeficientes en $\mathbb{Z}_p$ que tenga como raíz a x, es decir el polinomio minimal de x sobre $\mathbb{Q}_p$. Luego, por la definición de la valuación, tenemos que

$$v_p(x) = \frac{1}{[K : \mathbb{Q}_p]} v_p(N(\alpha)),$$

donde sabemos que $N(\alpha)$ es a menos de signo, una potencia del término independiente del polinomio, que sabemos que está en $\mathbb{Z}_p$, entonces, $v_p(\alpha) \geq 0$ como queríamos probar.

Las pruebas de (f) y (g) son totalmente análogas a las realizadas para $\mathbb{Q}_p$.

□

Ahora que sabemos que κ es una extensión finita de $\mathbb{F}_p$, relacionaremos su grado de extensión con un número el cuál ya hemos definido.

Teorema 3.3.8. *Si $f = f(K/\mathbb{Q}_p)$ es el grado residual de K sobre $\mathbb{Q}_p$, entonces $[\kappa : \mathbb{F}_p] = f$. En particular $\kappa = \mathbb{F}_{p^f}$ es el cuerpo con p^f elementos.*

Demostración. Sean $m = [\kappa : \mathbb{F}_p]$ y $e = e(K/\mathbb{Q}_p)$ el índice de ramificación. Lo que queremos probar es que $e \cdot m = n = [K : \mathbb{Q}_p]$. Primero que nada, sean $\alpha_1, \alpha_1, ..., \alpha_m \in \mathcal{O}_K$ tales que sus imágenes al cociente $\tilde{\alpha}_1, \tilde{\alpha}_2, ..., \tilde{\alpha}_m \in \kappa$ sean una base de κ sobre $\mathbb{F}_p$. Como vimos en la prueba de la parte (c) de la proposición anterior, los α's tiene que ser linealmente independientes sobre $\mathbb{Q}_p$. Para probar el teorema, veremos cómo completar este conjunto a una base de K sobre $\mathbb{Q}_p$.
La idea es usar el uniformizador π considerando los siguientes elementos:

$$\begin{aligned}
&\alpha_1, \alpha_2, ..., \alpha_m,\\
&\pi\alpha_1, \pi\alpha_2, ..., \pi\alpha_m,\\
&\pi^2\alpha_1, \pi^2\alpha_2, ..., \pi^2\alpha_m,\\
&...,\\
&\pi^{e-1}\alpha_1, \pi^{e-1}\alpha_2, ..., \pi^{e-1}\alpha_m.
\end{aligned}$$

Lo que queremos probar es que estos elementos forman una base de K sobre $\mathbb{Q}_p$, y por ende tendríamos el teorema.
Primero observar que si todo elemento de $\mathcal{O}_K$ es una combinación lineal de los $\pi^i\alpha_j$ sobre $\mathbb{Q}_p$, entonces todo elemento de K también lo es, pues para todo $x \in K$, podemos encontrar un r tal que $p^r x \in \mathcal{O}_K$ y por ende, basta con dividir la combinación lineal que representa este elemento por p^r para hallar una que represente a x.
Consideremos entonces $x \in \mathcal{O}_K$. Probaremos a continuación que x es una combinación lineal de los $\pi^i\alpha_j$ con coeficientes en $\mathbb{Z}_p$, lo que nos probará que el conjunto es un generador de K como $\mathbb{Q}_p$ espacio vectorial.
Primero, reduciendo módulo π, sabemos que podemos escribir $\tilde{x}$ como una combinación de los $\tilde{\alpha}_j$; es decir que tenemos que

$$x = x_{0,1}\alpha_1 + x_{0,2}\alpha_2 + ... + x_{0,m}\alpha_m + \text{un múltiplo de } \pi,$$

donde los $x_{0,j} \in \mathbb{Z}_p$.(Cuando nos referimos a un múltiplo de π, nos referimos a que es de la forma πy con $y \in \mathcal{O}_K$). Ahora, repitiendo el mismo razonamiento con el múltiplo de π, obtenemos que

$$\begin{aligned}
x = {} & x_{0,1}\alpha_1 + x_{0,2}\alpha_2 + ... + x_{0,m}\alpha_m\\
& + x_{1,1}\pi\alpha_1 + x_{1,2}\pi\alpha_2 + ... + x_{1,m}\pi\alpha_m\\
& + \text{un múltiplo de } \pi^2.
\end{aligned}$$

Repitiendo esto e veces, y recordando que π^e y p difieren por una unidad (porque tienen igual valuación), entonces podemos escribir a x de la siguiente forma:

$$\begin{aligned} x = {} & x_{0,1}\alpha_1 + x_{0,2}\alpha_2 + ... + x_{0,m}\alpha_m \\ & + x_{1,1}\pi\alpha_1 + x_{1,2}\pi\alpha_2 + ... + x_{1,m}\pi\alpha_m \\ & + \cdots \\ & + x_{e-1,1}\pi^{e-1}\alpha_1 + x_{e-1,2}\pi^{e-1}\alpha_2 + \cdots + x_{e-1,m}\pi^{e-1}\alpha_m \\ & + px', \end{aligned}$$

donde todos los coeficientes $x_{i,j}$ están en $\mathbb{Z}_p$ y $x' \in \mathcal{O}_K$. Ahora, si aplicamos el mismo razonamiento a x', obtenemos nuevos coeficientes $x_{i,j} + px'_{i,j}$, para los cuales la igualdad tenemos igualdad a x módulo p^2. Continuando con este procedimiento, para cada (i, j) obtenemos la siguiente serie convergente en $\mathbb{Z}_p$:

$$x_{i,j} + px'_{i,j} + p^2x''_{i,j} + \cdots$$

Sea $y_{i,j} \in \mathbb{Z}_p$ la suma de la serie anterior, luego tenemos que

$$x = \sum_{i=0}^{e-1}\sum_{j=1}^{m} y_{i,j}\pi^i\alpha_j,$$

lo que nos prueba que x es una combinación lineal sobre $\mathbb{Z}_p$ de los $\pi^i\alpha_j$.
Para probar que los $\pi^i\alpha_j$ son linealmente independientes sobre $\mathbb{Q}_p$, asumamos por absurdo que existe un relación de dependencia

$$\sum_{i,j} x_{i,j}\pi^i\alpha_j = 0$$

con $x_{i,j} \in \mathbb{Q}_p$. Como no todos los coeficientes son cero, podemos reescalar la igualdad para asegurarnos de que todos los $x_{i,j}$ pertenezcan a $\mathbb{Z}_p$ y que por lo menos uno no sea divisible por p (es decir que no pertenezca a $p\mathbb{Z}_p$).
Reduciendo la ecuación módulo π, obtenemos una relación de dependencia para los $\tilde{\alpha}_j$ sobre $\mathbb{F}_p$; la cual debe ser trivial pues los $\tilde{\alpha}_j$ son una base. Por lo tanto, todos los coeficientes $x_{0,j}$ deben reducir a cero, es decir, deben ser múltiplos de p. Si $e = 1$ esto contradice nuestra hipótesis de que al menos uno debía ser una unidad.
Si $e > 1$, sabemos que todos los $x_{0,j}$ son divisibles por p, por lo tanto, también lo son por π. Esto hace que toda la parte izquierda sea divisible por π; por lo tanto dividimos por π. Observemos que los $x_{0,j}/\pi$ todavía son múltiplos de π pues tienen valuación de al menos $1 - \frac{1}{e} > 0$. Ahora reducimos módulo π otra vez y usando el mismo razonamiento de antes, concluimos que los $x_{1,j}$ deben ser divisibles por p. Si $e = 2$ obtenemos nuevamente una contradicción.
Continuando de esta forma, obtenemos que todos los $x_{i,j}$ son divisibles por p, lo que contradice nuestra hipótesis de que al menos uno era una unidad. Por lo tanto, no puede existir una relación de dependencia y por ende nuestros elementos son linealmente

independientes.

□

Luego de este teorema, lo que sabemos es que el grado $n = [K : \mathbb{Q}_p]$ de una extensión finita de $\mathbb{Q}_p$ se puede escribir como $n = e \cdot f$, donde e mide de cierta forma el cambio en la imagen de la valuación p-ádica y $f = [\kappa : \mathbb{F}_p]$ mide el cambio en el cuerpo residual.

A continuación, consideraremos los casos en los que $e = n$ y $e = 1$, es decir cuando la extensión es totalmente ramificada y cuando no es ramificada.
Comencemos con el caso en el que $e = n$.

Proposición 3.3.9. *Sea $K/\mathbb{Q}_p$ un extensión finita totalmente ramificada de $\mathbb{Q}_p$, es decir $e = n = [K : \mathbb{Q}_p]$. Entonces $K = \mathbb{Q}_p(\pi)$, donde π es un uniformizador. Más aún, π es una raíz de un polinomio*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Q}_p[X]$$

que satisface las condiciones del criterio de irreducibilidad de Eisenstein, es decir $p \mid a_i$ para $0 \leq i < n$ y $p^2 \nmid a_0$.

Demostración. Sea π un uniformizador, es decir que $v_p(\pi) = 1/n$ o equivalentemente, $|\pi| = p^{-1/n}$. Sea $f(X)$ el polinomio minimal de π sobre $\mathbb{Q}_p$. Sea s el grado de $f(X)$ (el cual debe de ser un divisor de n) y a_0 su término independiente. Si $r = n/s$, entonces la norma de π es $(-1)^{nr}a_0^r$; lo que nos da la ecuación

$$p^{-1/n} = |\pi| = \sqrt[n]{|a_0^r|} = \sqrt[s]{|a_0|}.$$

Por otro lado, como $a_0 \in \mathbb{Q}_p$, su valor absoluto es una potencia entera de p, digamos $|a_0| = p^{-k}$ con $k \in \mathbb{Z}$. Luego, de la ecuación, tenemos que $\frac{s}{n} = k$, como k es entero y $0 < s \leq n$, concluimos que $s = n$ (es decir que el grado de $f(X)$ es n), y que $|a_0| = p^{-1}$ (es decir que $p \mid a_0$ pero $p^2 \nmid a_0$ como queríamos).
Como el grado del polinomio irreducible de π es n, entonces la extensión $\mathbb{Q}_p(\pi)$ es de grado n, y por lo tanto tenemos que $K = \mathbb{Q}_p(\pi)$. Nos queda probar que $p \mid a_i$ para $0 < i < n$. Para esto consideremos $\pi = \pi_1, \pi_2, ..., \pi_n$ las raíces de $f(X)$. Observar que todas las raíces tienen el mismo polinomio minimal, por lo tanto tienen la misma norma y por lo tanto, el mismo valor absoluto. En particular tenemos que $|\pi_i| < 1$ para todo i. Luego, sabemos que los coeficientes de $f(X)$ son sumas de productos de las raíces; por lo tanto tenemos que $|a_i| < 1$ para todo $0 \leq i < n$, como queríamos probar.

□

Este es un resultado importante, pero solamente nos ofrece una descripción parcial de las extensiones totalmente ramificadas de $\mathbb{Q}_p$, pues no tenemos ninguna manera de decidir cuándo dos polinomios de Eisenstein diferentes nos producen la misma extensión. Esto lo podremos hacer utilizando el Lema de Krasner que veremos en la próxima sección, y gracias al Corolario 3.4.4 que lo sigue, resulta que para cada n existen finitas extensiones

totalmente ramificadas (distintas) de grado n.

Para probar algo similar en el caso de las extensiones no ramificadas, precisaremos el siguiente teorema, que no es ni más ni menos que el Lema de Hensel para extensiones finitas:

Teorema 3.3.10 (Lema de Hensel)**.** *Sean K una extensión finita de $\mathbb{Q}_p$, π un uniformizador y $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polinomio con coeficientes en $\mathcal{O}_K$. Supongamos que existe $\alpha_1 \in \mathcal{O}_K$ tal que*

$$F(\alpha_1) \equiv 0 \pmod{\pi},$$

y

$$F'(\alpha_1) \not\equiv 0 \pmod{\pi},$$

donde $F'(X)$ es la derivada formal de $F(X)$. Entonces existe $\alpha \in \mathcal{O}_K$ tal que $\alpha \equiv \alpha_1 \pmod{\pi}$ y $F(\alpha) = 0$.

La prueba es exactamente la misma que la del Teorema 2.2.2, cambiando todas las p por π.

Al igual que antes, el Lema de Hensel nos permite obtener raíces de la unidad en K con un argumento parecido al de $\mathbb{Q}_p$.
Es preciso para el argumento que sigue que recordemos que los elementos no nulos de un cuerpo finito forman un grupo cíclico. En particular, los elementos no nulos del cuerpo residual κ forman un grupo cíclico con $p^f - 1$ elementos. Lo cual implica que para cada m que divida a $p^f - 1$ hay exactamente m raíces de de $F_m(X) = X^m - 1$ en $\kappa^\times$. Tomando cualquier levantado a $\mathcal{O}_K$ de cada una de esas raíces, obtenemos m raíces módulo π no congruentes entre sí. Luego, podemos aplicar el Lema de Hensel, pues la derivada $F'_m(X) = mX^{m-1}$ no será cero módulo π pues m es un divisor de $p^f - 1$ (y por tanto no divisible por p) y nuestras raíces módulo π son unidades. Por lo tanto, probamos que existen m raíces m-ésimas de la unidad no congruentes entre sí (y por ende diferentes) en $\mathcal{O}_K^\times$.
Como esto vale para todo m que divide a $p^f - 1$, tenemos que K contiene a todas las $(p^f - 1)$-ésimas raíces de la unidad. Expresamos este resultado en el siguiente corolario:

Corolario 3.3.11. *Sea $K/\mathbb{Q}_p$ una extensión finita, y sea $f = f(K/\mathbb{Q}_p)$. Entonces $\mathcal{O}_K^\times$ contiene al grupo cíclico de las $(p^f - 1)$-ésimas raíces de la unidad.*

Es claro que si K contiene a las $(p^f - 1)$-ésimas raíces de la unidad, entonces en particular contiene todas las m-ésimas raíces de la unidad para todo m que divida a $p^f - 1$. Entonces nos queda por estudiar qué pasa con las m-ésimas raíces de la unidad cuando

m es coprimo con $p^f - 1$. Comencemos por observar que estas deben ser 1-unidades, es decir que su reducción módulo π es igual a 1. Esto es así pues si $x^m = 1$ entonces $x^m \equiv 1 \pmod{\pi}$, luego como el grupo de invertibles es cíclico, existe un generador g (de orden $p^f - 1$); por lo que tenemos que $x \equiv g^k \pmod{\pi}$ para algún $0 \leq k < p^f - 1$ entero. Luego tenemos que $g^{km} \equiv 1 \pmod{\pi}$, por lo tanto, como g era un generador, tenemos que $p^f - 1 \mid km$, pero m era coprimo con $p^f - 1$, entonces $p^f - 1 \mid k$, pero entonces $x \equiv g^k \equiv 1 \pmod{\pi}$ como queríamos probar.
Lo siguiente que queremos probar es que las únicas posibles m-ésimas raíces de la unidad con m coprimo con $p^f - 1$ son aquellas en las que m es una potencia de p. Para esto precisaremos el siguiente lema:

Lema 3.3.12. *Si $x \equiv 1 \pmod{\pi}$, entonces $x^p \equiv 1 \pmod{\pi^2}$ y más en general $x^{p^r} \equiv 1 \pmod{\pi^{r+1}}$.*

Demostración. Como $x \equiv 1 \pmod{\pi}$, entonces $x = 1 + \pi u$ con u una unidad. Luego

$$x^p = (1 + \pi u)^p = \sum_{k=0}^{p} \binom{p}{k} \pi^k u^k = 1 + p\pi u + \text{un múltiplo de } \pi^2.$$

Recordando que $p = \pi^e r$ donde e es el índice de ramificación que es un entero mayor o igual a 1 y r es una unidad, tenemos que $p\pi u \equiv 0 \pmod{\pi^2}$ y por ende $x^p \equiv 1 \pmod{\pi^2}$ como queríamos probar.
Para el caso en general procedemos por inducción. Suponemos que la afirmación es valida para p^r y queremos probar que también lo es para p^{r+1}, es decir que sabemos que $x^{p^r} \equiv 1 \pmod{\pi^{r+1}}$ y queremos probar que $x^{p^{r+1}} \equiv 1 \pmod{\pi^{r+2}}$. Por hipótesis de inducción, sabemos que $x = 1 + \pi^{r+1} u$ con u unidad, luego

$$x^{p^{r+1}} = (1 + \pi^{r+1} u)^p = \sum_{k=0}^{p} \binom{p}{k} \pi^{(r+1)k} u^{(r+1)k} = 1 + p\pi^{r+1} u^{r+1} + \text{un múltiplo de } \pi^{r+2}.$$

Luego, por el mismo motivo que antes $p\pi^{r+1} u^{r+1} \equiv 0 \pmod{\pi^{r+2}}$ y por ende $x^{p^{r+1}} \equiv 1 \pmod{\pi^{r+2}}$. □

Una vez que tenemos este lema, es sencillo probar que de existir las raíces m-ésimas con m coprimo con $p^f - 1$, se debe tener que m es una potencia de p.
Supongamos que ζ es una 1-unidad y que $\zeta^m = 1$ con m coprimo con p. Sea r tal que $p^r \equiv 1 \pmod{m}$, luego tenemos que

$$\zeta = \zeta^{p^r} \equiv 1 \pmod{\pi^{r+1}}.$$

Cambiando r por un múltiplo, tenemos que ζ es congruente con 1 módulo una potencia arbitrariamente grande de π, por lo que $\zeta = 1$.

Resumiendo lo que probamos: si $f = f(K/\mathbb{Q}_p)$, entonces K contiene $p^f - 1$ raíces $p^f - 1$-ésimas de la unidad no congruentes entre sí, y posiblemente algunas (potencia de p)-ésimas raíces de la unidad, las cuales serían 1-unidades.

Ahora sí estamos en condiciones de describir las extensiones no ramificadas de $\mathbb{Q}_p$.

Proposición 3.3.13. *Para cada $f \in \mathbb{Z}^+$ existe una única extensión no ramificada de grado f, la cual puede ser obtenida adjuntando a $\mathbb{Q}_p$ una raíz (p^f-1)-ésima primitiva de la unidad.*

Cuando decimos que "existe una única extensión" nos referimos a que si fijamos una clausura algebraica $\overline{\mathbb{Q}}_p$ entonces existe un único cuerpo $K \subset \overline{\mathbb{Q}}_p$ no ramificado de grado f sobre $\mathbb{Q}_p$.

Demostración. Sea $\tilde{\alpha}$ un generador del grupo cíclico de los elementos no nulos de $\mathbb{F}_{p^f}$, luego $\mathbb{F}_{p^f} = \mathbb{F}_p(\tilde{\alpha})$ es una extensión de grado f. Sea $\overline{g}(X) = X^f + \overline{a}_{f-1}X^{f-1} + \cdots + \overline{a}_1 X + \overline{a}_0$ el polinomio minimal de $\overline{\alpha}$ sobre $\mathbb{F}_p$. Sea $g(X)$ un polinomio mónico cuya reducción módulo p sea $\overline{g}(X)$, luego, por el Corolario 3.2.8, $g(X)$ es un polinomio irreducible sobre $\mathbb{Q}_p$. Si α es una raíz de $g(X)$, entonces $K = \mathbb{Q}_p(\alpha)$ es una extensión de grado f. El cuerpo de residuos κ de K claramente contiene una raíz de $\overline{g}(X)$ (la reducción de α módulo $\mathfrak{p}_K$), por lo tanto, $[\kappa : \mathbb{F}_p] \geq f$. Por otro lado, sabemos que $f = [K : \mathbb{Q}_p] \geq [\kappa : \mathbb{F}_p]$ por la Proposición 3.3.7; por lo tanto tenemos que $[\kappa : \mathbb{F}_p] = f = [K : \mathbb{Q}_p]$, es decir, $K/\mathbb{Q}_p$ es una extensión no ramificada y $\kappa = \mathbb{F}_{p^f}$.
Esto nos prueba que siempre existe una extensión no ramificada de grado f. Todavía nos falta probar la unicidad. Para esto, probaremos que cualquier extensión $K/\mathbb{Q}_p$ no ramificada y de grado de f tiene que ser igual a la extensión que se obtiene adjuntando una raíz (p^f-1)-ésima primitiva de la unidad.
Por el corolario anterior, ya sabemos que K contiene todas las p^f-1-ésimas raíces de la unidad, por lo que para probar la igualdad, nos basta con probar que la menor extensión de $\mathbb{Q}_p$ que contiene a las (p^f-1)-ésimas raíces de la unidad es de grado f.
Sea β una (p^f-1)-ésima raíz primitiva de la unidad en K. Entonces tenemos que $\mathbb{Q}_p \subset \mathbb{Q}_p(\beta) \subset K$. Por otro lado, las potencias de β son exactamente todas las (p^f-1)-ésimas raíces de la unidad, y por el Lema de Hensel, sabemos que son todas distintas módulo $\mathfrak{p}_K$. Luego, el cuerpo de residuos de la extensión $\mathbb{Q}_p(\beta)/\mathbb{Q}_p$ tiene al menos p^f elementos (las p^f-1 congruencias distintas de las raíces de la unidad y el nulo), entonces el grado del cuerpo residual de $\mathbb{Q}_p(\beta)/\mathbb{Q}_p$ es mayor o igal a f y por ende $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \geq f$. Como $K/\mathbb{Q}_p$ es de grado f, tenemos que $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] = f$ y por ende $K = \mathbb{Q}_p(\beta)$.
Por último, las raíces del polinomio minimal de β sobre $\mathbb{Q}_p$ son exactamente las (p^f-1)-ésimas raíces de la unidad, las cuales son potencias de β, por ende la extensión $K = \mathbb{Q}_p(\beta)$ es normal y por ende fijada la clausura algebraica es única.

□

Una vez que sabemos que existe una única extensión no ramificada dado un grado fijo, junto con el lema de Hensel, surge el siguiente corolario.

Corolario 3.3.14. *Sean K una extensión finita de $\mathbb{Q}_p$ y f un entero positivo. Sea $m = p^f - 1$. Si existen $c \in K$ y ζ una raíz m-ésima primitiva de la unidad en $\overline{\mathbb{Q}}_p$ tal que $c \equiv \zeta$ (mód p), entonces K contiene a la extensión no ramificada de grado f de $\mathbb{Q}_p$.*

Demostración. Sea $F(X)$ el polinomio minimal de ζ sobre $\mathbb{Q}_p$. Luego, sabemos que $X^m-1 = F(X)g(X)$ para algún $g(X) \in \mathbb{Q}_p[X]$. Derivando, tenemos que $(p^f-1)X^{m-1} = F'(X)g(X) + F(X)g'(X)$. Como $c \equiv \zeta \pmod p$, sabemos que $F(c) \equiv 0 \pmod p$ y que $(p^f-1)c^{m-1} \not\equiv 0 \pmod p$. Luego tenemos

$$0 \not\equiv (p^f-1)c^{m-1} \equiv F'(c)g(c) + F(c)g'(c) \equiv F'(c)g(c) \pmod p,$$

entonces $F'(c) \not\equiv 0 \pmod p$. Para terminar, por el Lema de Hensel tenemos que K contiene una raíz de $F(X)$, es decir una raíz m-ésima primitiva de la unidad. Por lo tanto, por la proposición anterior, K contiene a la extensión no ramificada de grado f. □

Como sabemos que existe una única extensión no ramificada de cada grado, lo que podemos hacer es considerar la unión de todas ellas; lo que claramente nos da una extensión infinita de $\mathbb{Q}_p$ que contiene a todas las extensiones no ramificadas de $\mathbb{Q}_p$. Llamaremos a esta extensión **la extensión maximal no ramificada de** $\mathbb{Q}_p$, y la denotaremos como $\mathbb{Q}_p^{\text{unr}}$.
Notemos que esta extensión a pesar de ser infinita, es claramente distinta a $\overline{\mathbb{Q}}_p$, pero sí comparten algunas propiedades. Algo que las diferencia es que la imagen de v_p sobre $\mathbb{Q}_p^{\text{unr}}$ es $\mathbb{Z}$, pues cada uno de sus elementos se encuentran en una extensión finita no ramificada y la valuación restricta a la extensión correspondiente tiene imagen $\mathbb{Z}$; por otro lado, la imagen de v_p sobre $\overline{\mathbb{Q}}_p$ es $\mathbb{Q}$ pues contiene extensiones con índice de ramificación tan grande como uno quiera y por ende los denominadores de las imágenes de v_p también son tan grandes como uno quiera.
Una propiedad que comparten, es que ambas tiene el mismo cuerpo residual, que es la clausura algebraica de $\mathbb{F}_p$. Esto se debe a que ambos cuerpo $\mathbb{Q}_p^{\text{unr}}$ y $\overline{\mathbb{Q}}_p$ contienen extensiones finitas de $\mathbb{Q}_p$ con grado residual arbitrariamente grande.

Para terminar esta sección, veremos como la mayoría del análisis se extiende a las extensiones finitas de $\mathbb{Q}_p$; casi todas las demostraciones de los siguientes hechos son análogas a las realizadas en $\mathbb{Q}_p$, cambiando todo argumento que usara que p era un uniformizador para $\mathbb{Z}_p$, por π siendo π un uniformizador para $\mathcal{O}_K$.

Teorema 3.3.15 (Análisis en extensiones finitas)**.** *Sea K una extensión finita de $\mathbb{Q}_p$ y sea $|\ |$ la única extensión del valor absoluto p-ádico en K. Entonces:*

a) Una sucesión (a_n) en K es de Cauchy si y solo si

$$\lim_{n\to\infty} |a_{n+1} - a_n| = 0.$$

b) Si una sucesión (a_n) converge a un elemento a no nulo, entonces $|a_n| = |a|$ para n suficientemente grande.

c) Una serie $\sum a_n$ en K converge si y solo si su término general tiende a cero.

d) El Teorema 2.3.4 sigue valiendo para las series dobles en K.

e) Una serie de potencias $f(X) = \sum a_n X^n$ con coeficientes $a_n \in K$, define una función continua en una bola abierta de radio $\rho = 1/\limsup \sqrt[n]{|a_n|}$ y la función se extiende a la bola cerrada de radio ρ si y solo si $|a_n|\rho^n \to 0$.

f) Las funciones definidas por series de potencia son derivables y su derivada está definida por la derivada formal de la serie original.

g) Sean $f(X) = \sum a_n X^n$ y $g(X) = \sum b_n X^n$ dos series de potencias con coeficientes en K, luego si existe una sucesión (x_m) convergente contenida en la intersección de los discos de convergencia de f y g tal que $f(x_m) = g(x_m)$ para todo m, entonces $a : n = b_n$ para todo n.

h) El Teorema de Strassman y su corolarios se mantienen reemplazando $\mathbb{Q}_p$ por K y $\mathbb{Z}_p$ por $\mathcal{O}_K$.

3.4 Construcción de $\mathbb{C}_p$

En esta sección, comenzaremos considerando la clausura algebraica $\overline{\mathbb{Q}}_p$, para la cual ya construimos su valor absoluto. Probaremos que no es completa con respecto a este valor absoluto, por lo que nos iremos a su completación y probaremos que esta última sí es algebraicamente cerrada (además de completa claro esta).
Para esto, necesitaremos el Lema de Krasner y uno de sus corolarios lo cuales probamos a continuación, pero antes recordamos la siguiente definición.

Definición 3.4.1. *Sea K un subcuerpo de $\overline{\mathbb{Q}}_p$. Dos elementos a y a' de $\overline{\mathbb{Q}}_p$ son conjugados sobre K si ambos son raíces del mismo polinomio mónico irreducible con coeficientes en K.*
Otra forma de decir esto, es que dos elementos son conjugados cuando existe un automorfismo $\sigma : \overline{\mathbb{Q}}_p \longrightarrow \overline{\mathbb{Q}}_p$ que induce la identidad en K y hace corresponder a y a'.

Observación 3.4.2. *Por cualquiera de las dos definiciones, es claro que dos elementos conjugados tiene el mismo valor absoluto.*

Teorema 3.4.3 (Lema de Krasner)**.** *Sea K un cuerpo de característica cero completo respecto de un valor absoluto no arquimediano, y sean a y b elementos de la clausura algebraica de K. Sean $a_1 = a, a_2, ..., a_n$ los conjugados de a sobre K. Supongamos que $|b - a| < |a - a_i|$ para todo $i = 2, 3, ..., n$, entonces $K(a) \subset K(b)$.*

Demostración. Sea $L = K(b)$ y supongamos que el teorema es falso, es decir que $a \notin L$. Entonces consideremos la extensión $L(a)$; como estamos asumiendo que $a \notin L$,

entonces $m = [L(a) : L] > 1$. Entonces existen m morfismos $\sigma : L(a) \longrightarrow \overline{K}$ que son la identidad en L (y que asignan a a uno de sus conjugados). Hay por lo menos un σ para el cual $\sigma(a) \neq a$; le llamaremos σ_0. Como ya sabemos, por la unicidad del valor absoluto, tenemos que $|\sigma(x)| = |x|$ para todo σ y para todo $x \in \overline{K}$, entonces tenemos

$$|\sigma_0(b-a)| = |\sigma_0(b) - \sigma_0(a)| = |b-a|.$$

Pero σ_0 fija L y $b \in L$, por lo tanto $\sigma(b) = b$ y la igualdad anterior nos queda de la siguiente forma

$$|b - \sigma_0(a)| = |b-a|.$$

Pero entonces

$$|a - \sigma_0(a)| \leq \text{máx}\{|a-b|, |b-\sigma_0(a)|\} = \text{máx}\{|a-b|, |b-a|\} = |b-a|,$$

y esto es un absurdo pues por hipótesis b estaba más cerca de a que cualquiera de sus conjugados, por ende $a \in L$ y por lo tanto $K(a) \subset K(b)$. □

Corolario 3.4.4. *Sea K un cuerpo de característica cero completo respecto a un valor absoluto no arquimediano y sea $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un polinomio irreducible con coeficientes en K. Sea λ una raíz de $f(X)$ y consideremos $L = K(\lambda)$. Entonces existe un $\varepsilon > 0$ tal que vale lo siguiente:*

Si $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$ es un polinomio con coeficientes en K que cumple que

$$|a_i - b_i| < \varepsilon \qquad \textit{para todo } i = 0, 1, ..., n-1,$$

entonces $g(X)$ es irreducible sobre K y tiene una raíz en L.

Demostración. La siguiente prueba consta de dos partes, en la primera probaremos que bajo ciertas condiciones la conclusión vale y luego probaremos que existe un ε para el cual esas condiciones son ciertas.
Como f es irreducible, tenemos que $[L : K] = n$; sean entonces $\lambda_1 = \lambda, \lambda_2, ..., \lambda_n$ las raíces de $f(X)$ en $\overline{K}$, y sea

$$r = \min_{i \neq j} |\lambda_i - \lambda_j|.$$

Sean también $\mu_1, \mu_2, ..., \mu_n$ las raíces (listadas con multiplicidad a priori) de $g(X)$ en $\overline{K}$, por lo que $g(X) = \prod (X - \mu_j)$. Definamos entonces

$$D = \prod_i g(\lambda_i) = \prod_{i,j} (\lambda_i - \mu_j).$$

Afirmación 1: Si $|D| < r^{n^2}$, entonces $g(X)$ es irreducible sobre K y tiene una raíz en

$L = K(\lambda)$.

Prueba de la Afirmación 1: Si $|D| < r^{n^2}$, entonces al menos uno de los n^2 factores de D tiene que tener valor absoluto menor que r, es decir, existe un par (i, j) tal que $|\lambda_i - \mu_j| < r$. Como r es el mínimo de las distancias entre los λ_k que es menor o igual al mínimo de las distancias entre λ_i y sus conjugados, podemos aplicar el Lema de Krasner para concluir que $K(\lambda_i) \subset K(\mu_j)$. Por lo tanto

$$[K(\mu_j) : K] \geq [K(\lambda_i) : K] = n.$$

Pero μ_j es una raíz de un polinomio de grado n, por lo tanto, la única manera en que la desigualdad se cumpla es si el polinomio $g(X)$ es irreducible y el grado de la extensión $K(\mu_j)/K$ es exactamente n. Como ambos cuerpos son de grado n y uno está contenido en el otro, tenemos que deben ser iguales.
Por lo tanto, hemos probado que $g(X)$ es irreducible y que $K(\lambda_i) = K(\mu_j)$. Si $i = 1$ es lo que queríamos probar, sino, sabemos que existe un automorfismo de $\overline{K}$ que manda λ_i a λ, y este automorfismo tiene que mandar μ_j a otra raíz μ de $g(X)$. Por último, aplicando este automorfismo a la igualdad $K(\lambda_i) = K(\mu_j)$ tenemos $K(\lambda) = K(\mu)$, por lo que $g(X)$ tiene una raíz en L como queríamos probar.

Afirmación 2: Existe $\varepsilon > 0$ tal que si $|a_i - b_i| < \varepsilon$, entonces $|D| < r^{n^2}$.

Demostración Afirmación 2: Definamos la función

$$\phi : K^{n-1} \times K^{n-1} \longrightarrow \overline{K},$$

como la función que manda $(a_0, a_1, ..., a_{n-1}, b_0, b_1, ..., b_{n-1}) \mapsto D$, dónde D es el nuevo D definido por los coeficientes de los nuevos polinomios f y g. El número D, es conocido como la resultante de los polinomios f y g, y se puede probar que es un polinomio en $a_0, a_1, .., a_{n-1}, b_0, b_1, ..., b_{n-1}$. Sabemos entonces que el mapa ϕ es continuo. Además, es claro que $\phi(a_0, a_1, .., a_{n-1}, a_0, a_1, ..., a_{n-1}) = 0$; por lo tanto, por continuidad de ϕ, sabemos que podemos hacer el D tan chico como queramos eligiendo los b's suficientemente cerca de los a's.
Por lo tanto, queda probado el corolario.

□

Procederemos entonces a probar uno de los grandes resultados de esta sección.

Teorema 3.4.5. *La clausura algebraica $\overline{\mathbb{Q}}_p$ no es completa respecto al valor absoluto p-ádico.*

Demostración. Para probar el teorema, nos basta con construir una sucesión de Cauchy en $\overline{\mathbb{Q}}_p$ que no converja. Como las extensiones finitas de $\mathbb{Q}_p$ son completas, esta sucesión tendrá que tener elementos de extensiones cada vez más grandes. La idea va a ser construir una serie cuyo término general tienda a cero pero no converja, esto nos basta gracias al Lema 1.3.2.

Sean $f_0, f_1, f_2, ...$ enteros tales que $f_i < f_{i+1}$ y $f_i \mid f_{i+1}$. Para cada i, sean $m_i = p^{f_i} - 1$ y ζ_i una raíz m_i-ésima primitiva de la unidad. Entonces, $\mathbb{Q}_p(\zeta_i)$ es la única extensión no ramificada de grado f_i.
Construyamos ahora la serie

$$\sum_{i=0}^{\infty} \zeta_i p^i.$$

Su término independiente claramente tiende a cero y por ende sus sumas parciales forman una sucesión de Cauchy en $\overline{\mathbb{Q}}_p$. Queremos probar que esta serie no tiene un límite en $\overline{\mathbb{Q}}_p$.
Supongamos por absurdo que la serie converge, y sea $c \in \overline{\mathbb{Q}}_p$ su límite. Como $c \in \overline{\mathbb{Q}}_p$, tiene que ser la raíz de un polinomio irreducible sobre $\mathbb{Q}_p$. Supongamos que ese polinomio tiene grado d, es decir $[\mathbb{Q}_p(c) : \mathbb{Q}_p] = d$.
Por otro lado, tenemos que

$$c = \zeta_0 + \zeta_1 p + \zeta_2 p^2 + ...,$$

por lo tanto, $c \equiv \zeta_0 \pmod{p}$. Por el Corolario 3.3.14, tenemos entonces que $\mathbb{Q}_p(\zeta_0) \subset \mathbb{Q}_p(c)$, lo que implica que

$$d = [\mathbb{Q}_p(c) : \mathbb{Q}_p] \geq [\mathbb{Q}_p(\zeta_0) : \mathbb{Q}_p] = f_0.$$

Ahora definamos $c_1 = (c - \zeta_0)/p$. Como $\zeta_0 \in \mathbb{Q}_p(c)$, tenemos que $c_1 \in \mathbb{Q}_p(c)$. Pero claramente $c_1 \equiv \zeta_1 \pmod{p}$, por lo que usando nuevamente el Corolario 3.3.14, tenemos que $\mathbb{Q}_p(\zeta_1) \subset \mathbb{Q}_p(c)$, y por lo tanto $d \geq f_1$.
Continuando de esta forma, tenemos que $d > f_i$ para todo i, lo cual es un absurdo pues $f \to \infty$. Por ende, la serie no converge y por lo tanto $\overline{\mathbb{Q}}_p$ no es completo.
□

De hecho, observando que los ζ_i de hecho pertenecen a $\mathbb{Q}_p^{\text{unr}}$, tenemos probado también el siguiente teorema.

Teorema 3.4.6. *La extensión maximal no ramificada $\mathbb{Q}_p^{unr}$ de $\mathbb{Q}_p$, no es completa respecto al valor absoluto p-ádico.*

Como $\overline{\mathbb{Q}}_p$ no es completo, para obtener un cuerpo algebraicamente cerrado y completo, necesitamos completar $\overline{\mathbb{Q}}_p$. Realizando una construcción análoga a la del Capítulo 1, terminamos con la siguiente proposición:

Proposición 3.4.7. *Existe un cuerpo $\mathbb{C}_p$ y un valor absoluto $|\ |$ en $\mathbb{C}_p$ tales que:*

- $\mathbb{C}_p$ *contiene a* $\overline{\mathbb{Q}}_p$ *y la restricción de* $|\ |$ *a* $\overline{\mathbb{Q}}_p$ *coincide con el valor absoluto p-ádico.*
- $\mathbb{C}_p$ *es completo respecto a* $|\ |$.
- $\overline{\mathbb{Q}}_p$ *es denso en* $\mathbb{C}_p$.

Recordemos que siempre que tengamos una sucesión convergente $x_n \to x \neq 0$ en un cuerpo con un valor absoluto no arquimediano, entonces existe un N tal que $|x_n| = |x|$ para todo $n \geq N$. Esto significa que el conjunto de posibles valores absolutos en $\mathbb{C}_p$ es exactamente el mismo que en $\overline{\mathbb{Q}}_p$. Es decir:

Proposición 3.4.8. *Si* $x \in \mathbb{C}_p$, $x \neq 0$, *entonces existe un* $v \in \mathbb{Q}$ *tal que* $|x| = p^{-v}$. *En otras palabras, la valuación p-ádica se extiende a* $\mathbb{C}_p$ *y su imagen es* $\mathbb{Q}$.

Escribimos $\mathfrak{O}$ para el anillo de valuación de $\mathbb{C}_p$, es decir

$$\mathfrak{O} = \{x \in \mathbb{C}_p : |x| \leq 1\}.$$

Que contiene a su ideal de valuación

$$\mathfrak{B} = \{x \in \mathbb{C}_p : |x| \leq 1\}.$$

Como siempre, $\mathfrak{O}$ es una anillo local.
Probemos que $\mathbb{C}_p$ es efectivamente lo que estábamos buscando, es decir, que es algebraicamente cerrado.

Teorema 3.4.9. $\mathbb{C}_p$ *es algebraicamente cerrado.*

Demostración. Sea $f(X)$ un polinomio irreducible con coeficientes en $\mathbb{C}_p$. Como $\overline{\mathbb{Q}}_p$ es denso en $\mathbb{C}_p$, podemos encontrar polinomios del mismo grado que $f(X)$, con coeficientes en $\overline{\mathbb{Q}}_p$ tan cercanos como queramos de los coeficientes de $f(X)$. Luego, por el Corolario 3.4.4, si elegimos un $f_0(X)$ con los coeficientes suficientemente cerca de los de $f(X)$, $f_0(X)$ será irreducible en $\mathbb{C}_p$, y como sus coeficientes están en $\overline{\mathbb{Q}}_p$, de hecho es irreducible sobre $\overline{\mathbb{Q}}_p$. Como $\overline{\mathbb{Q}}_p$ es algebraicamente cerrado, entonces $f_0(X)$ tiene que ser de grado 1. Como $f(X)$ y $f_0(X)$ tenían el mismo grado, entonces $f(X)$ es de grado uno.
Por ende, todos los polinomios irreducibles sobre $\mathbb{C}_p$ tiene que ser de grado uno, ergo, $\mathbb{C}_p$ es algebraicamente cerrado. □

Capítulo 4

Análisis en $\mathbb{C}_p$

En este capítulo veremos una introducción al análisis en $\mathbb{C}_p$. En la primera sección veremos que casi todo lo hecho anteriormente para $\mathbb{Q}_p$ se extiende a $\mathbb{C}_p$, de forma similar a como lo hacía para extensiones finitas. En la segunda sección definiremos una norma en el espacio de polinomios y series de potencias, para luego enunciar el Teorema de preparación de Weierstrass p-ádico y ver una aplicación para el estudio de las funciones enteras en $\mathbb{C}_p$. Por último, en la tercera sección hablaremos un poco sobre la teoría de los polígonos de Newton.

4.1 Casi todo se extiende

Teorema 4.1.1. *Se tienen las siguientes propiedades:*

a) Una sucesión (a_n) en $\mathbb{C}_p$ es de Cauchy si y solo si

$$\lim_{n\to\infty} |a_{n+1} - a_n| = 0.$$

b) Si una sucesión (a_n) converge a un elemento $a \neq 0$, entonces tenemos que $|a_n| = |a|$ para n suficientemente grande.

c) Una serie $\sum a_n$ con $a_n \in \mathbb{C}_p$ converge si y solo si su término general tiende a cero.

d) El Teorema 2.3.4 se mantiene para las dobles series en $\mathbb{C}_p$.

e) Una serie de potencias $f(X) = \sum a_n X^n$ con coeficientes $a_n \in \mathbb{C}_p$ define una función continua en una bola abierta de radio $\rho = 1/\limsup \sqrt[n]{|a_n|}$. La función se extiende a la bola cerrada si y solo si $|a_n|\rho^n \to 0$.

f) Dada una serie de potencias $f(X) = \sum a_n X^n$ *con radio de convergencia* ρ*, podemos definir una función en la bola abierta (o quizás cerrada) de radio* ρ *alrededor de* $\alpha \in \mathbb{C}_p$ *de la siguiente forma:*

$$f(x) = \sum a_n (x - \alpha)^n$$

para todo $x \in B(\alpha, \rho)$ *(o quizás* $\overline{B}(\alpha, \rho)$*).*

g) Las funciones definidas por series de potencias son derivables y su derivada coincide con la función definida por su derivada formal.

h) Si $f(X) = \sum a_n X^n$ *y* $g(X) = \sum a_n X^n$ *son series de potencias con coeficientes en* $\mathbb{C}_p$*, y existe una sucesión* (x_m) *convergente contenida en la intersección de los discos de convergencia de* f *y* g *tal que* $f(x_m) = g(x_m)$ *para todo* m*, entonces* $a_n = b_n$ *para todo* n*.*

i) El Teorema de Strassman y sus corolarios se mantienen simplemente reemplazando $\mathbb{Q}_p$ *por* $\mathbb{C}_p$ *y* $\mathbb{Z}_p$ *por* $\mathfrak{O}$*.*

Otros resultados importantes que se pueden extender a $\mathbb{C}_p$, son las variantes de Lema de Hensel. La idea es no usar las versiones con uniformizadores, ya que en $\mathbb{C}_p$ no lo tenemos; en vez de eso simplemente podemos cambiar por $\pmod{\mathfrak{B}}$ o trabajar con el valor absoluto.

Teorema 4.1.2 (Lema de Hensel en $\mathbb{C}_p$)**.** *Sea* $F(X) = a_0 + a_1 X + \cdots + a_n X^n$ *un polinomio con coeficientes en* $\mathfrak{O}$*. Supongamos que existe un* $\alpha_1 \in \mathfrak{O}$ *tal que*

$$|F(\alpha_1)| < 1 \qquad y \qquad |F'(\alpha_1)| = 1.$$

Entonces existe un $\alpha \in \mathfrak{O}$ *tal que* $|\alpha - \alpha_1| < 1$ *y* $F(\alpha) = 0$*.*

Teorema 4.1.3 (Lema de Hensel para polinomios en $\mathbb{C}_p$)**.** *Sea* $f(X) \in \mathfrak{O}[X]$ *y supongamos que existen polinomios* $g_1(X)$ *y* $h_1(X)$ *en* $\mathfrak{O}[X]$ *tales que*

a) $g_1(X)$ *es mónico.*

b) $g_1(X)$ *y* $h_1(X)$ *son coprimos módulo* $\mathfrak{B}$*.*

c) $f(X) \equiv g_1(X) h_1(X) \pmod{\mathfrak{B}}$*.*

Entonces existen polinomios $g(X)$ *y* $h(X)$ *en* $\mathfrak{O}[X]$ *tales que*

a) $g(X)$ *es mónico.*

b) $g(X) \equiv g_1(X) \pmod{\mathfrak{B}}$ *y* $h(X) \equiv h_1(X) \pmod{\mathfrak{B}}$.

c) $f(X) = g(X)h(X)$.

4.2 Teorema de Preparación de Weierstrass p-ádico

El objetivo de esta sección es dar las bases para poder enunciar y probar una versión del Teorema de preparación de Weierstrass para polinomios y luego enunciar una serie de lemas los cuales probaran el Teorema de preparación de Weiertrass (para series) replicando la demostración de su versión para polinomios. Por último, utilizaremos el Teorema de preparación de Weierstrass para describir a las funciones enteras de $\mathbb{C}_p$.

Lo que sigue, en realidad vale para cualquier extensión completa de $\mathbb{Q}_p$, y como en algunos contextos puede ser útil, lo haremos lo más general posible. Sea K una extensión completa de $\mathbb{Q}_p$, $\mathcal{O}$ su anillo de valuación, es decir, $\mathcal{O} = \{x \in K : |x| \leq 1\}$, y $\mathbb{F}$ su cuerpo de residuos.
El primer paso es definir una norma en el espacio de polinomios:

Proposición 4.2.1. *Sea $c > 0$ un número real. Definimos entonces una función $\| \ \|_c : K[X] \longrightarrow \mathbb{R}_{\geq 0}$ de la siguiente forma: sea $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomio con coeficientes en K, entonces*

$$\|f(X)\|_c = \max_i |a_i|c^i.$$

Entonces tenemos que

a) $\|f(X)\|_c = 0$ *si y solo si* $f(X)$ *es idénticamente nulo.*

b) $\|f(X) + g(X)\|_c \leq \max\{\|f(X)\|_c, \|g(X)\|_c\}$.

c) $\|f(X)g(X)\|_c = \|f(X)\|_c\|g(X)\|_c$.

d) Si $f(X) = a_0$ es un polinomio constante, entonces $\|f(X)\|_c = |a_0|$. Es decir, $\| \ \|_c$ induce el valor absoluto p-ádico en las constantes.

e) Si $|x| \leq c$, entonces $|f(x)| \leq \|f(X)\|_c$.

f) La función $\| \ \|_c$ se extiende a un valor absoluto no arquimediano en el cuerpo de funciones racionales $K(X)$.

A continuación veremos un lema fundamental que nos permitirá probar la versión para polinomios del Teorema de preparación de Weierstrass.

Lema 4.2.2. *Sea $c > 0$, y sea $\| \ \| = \| \ \|_c$. Sea $f(X) \in K[X]$ un polinomio cualquiera, y sea*

$$g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_NX^N$$

un polinomio de grado N con coeficientes en K tal que $\|g(X)\| = |b_N|c^N$. (Es decir, que el máximo de $|b_n|c^n$ se da en el último coeficiente). Sean $q(X)$ y $r(X)$ el cociente y el resto que se obtienen al dividir $f(X)$ por $g(X)$, es decir

$$f(X) = g(X)q(X) + r(X) \qquad y \qquad gr(r(X)) < N.$$

Entonces tenemos que

$$\|f(X)\| \geq \|q(X)\|\|g(X)\| \qquad y \qquad \|f(X)\| \geq \|r(X)\|.$$

Demostración. Primero probaremos la proposición para $c = 1$.
Si $c = 1$, entonces $|b_N| = \text{máx}|b_i|$. Multiplicando $g(X)$ por algún elemento en K de ser necesario, podemos asumir que $|b_N| = 1$. De igual manera, podemos multiplicar la ecuación $f(X) = q(X)g(X) + r(X)$ por algún elemento de K para tener que $\text{máx}\{\|q(X)\|, \|r(x)\|\} = 1$, lo cual implica que $\|f(X)\| \leq 1$. Entonces, lo que dice el lema luego de estas dos reducciones, es que $\|f(X)\| = 1$.
Supongamos que no, es decir, que todo coeficiente de $f(X)$ tiene valor absoluto menor a 1, por lo tanto, todos pertenecen al ideal de valuación $\mathfrak{p}$. En lo que sigue, las barras significan reducir módulo $\mathfrak{p}$. Entonces tenemos

$$0 = \overline{f}(X) = \overline{g}(X)\overline{q}(X) + \overline{r}(X).$$

Pero como $|b_N| = 1$, tenemos que

$$gr(\overline{g}(X)) = N > gr(r(X)) \geq gr(\overline{r}(X)).$$

Pero entonces $\overline{q}(X) = 0$, lo cual implica que $\overline{r}(X) = 0$. Pero esto contradice el hecho de que $\text{máx}\{\|q(X)\|, \|r(x)\|\} = 1$.
Hemos entonces probado el lema para el caso $c = 1$.
Antes de continuar, observar que la norma definida sobre los polinomios no depende del cuerpo en el que estemos trabajando, pues el valor absoluto p-ádico no lo hacía. Luego, como nuestro lema es sobre normas, podemos asumir que $K = \mathbb{C}_p$. Lo precisaremos porque a continuación consideraremos elementos con valor absoluto p^r con $r \in \mathbb{Q}$ y sabemos que en $\mathbb{C}_p$ dichos elementos existen.

Supongamos $c \neq 1$, pero $c = p^r$ para algún $r \in \mathbb{Q}$. Sea $\alpha \in \mathbb{C}_p$ tal que $|\alpha| = c$. Consideremos entonces los polinomios $f_1(X) = f(\alpha X)$ y $g_1(X) = g(\alpha X)$. Entonces $\|f_1(X)\|_1 = \|f(X)\|_c$ y $\|g_1(X)\|_1 = \|g(X)\|_c$. Luego, aplicando la parte anterior a $f_1(X)$ y $g_1(X)$, obtenemos las desigualdades del lema.

Supongamos por último que $c \neq p^r$ con $r \in \mathbb{Q}$. Como los números de la forma p^r son densos en $\mathbb{R}_{\geq 0}$, existe una sucesión (c_i) de números reales de la forma $c_i = p^{r_i}$ con $r_i \in \mathbb{Q}$ tales que $c_i \to c$. Entonces claramente tenemos que $\|f(X)\|_{c_i} \to \|f(X)\|_c$, por lo tanto, usamos que la parte anterior vale para cada c_i y tomamos límite. □

A continuación probaremos la versión para polinomios del Teorema de Preparación de Weierstrass.

Teorema 4.2.3. *Sea $c > 0$ y $\| \ \| = \| \ \|_c$. Sea $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomio en $K[X]$. Supongamos que existe un entero $0 < N < n$ tal que*

$$\|f(X)\| = |a_N|c^N \qquad y \qquad \|f(X)\| > |a_j|c^j \quad \text{para todo } j > N.$$

Entonces existen polinomios $g(X)$ de grado N, y $h(X)$ de grado $n - N$ con coeficientes en K tales que $f(X) = g(X)h(X)$. Más aún, tenemos que

$$\|g(X)\| = \|f(X)\| \qquad y \qquad \|h(X) - 1\| < 1.$$

Demostración. La idea es comenzar una factorización aproximada e ir mejorandola. Si probamos por inducción de que esto siempre lo podemos hacer, tendremos una sucesión convergente de polinomios que en el límite nos dará la factorización que buscamos. Comenzaremos describiendo el paso inductivo y luego probaremos la base inductiva.

Sea $\delta < 1$ un real. Supongamos que en tenemos polinomios $h_i(X)$ y $g_i(X)$ tales que:

a) $gr(g_i(X)) = N$ y $gr(h_i(X)) \leq n - N$.

b) $\|f(X) - g_i(X)\| \leq \delta\|f(X)\|$ y $\|h_i(X) - 1\| \leq \delta$

c) $\|f(X) - g_i(X)h_i(X)\|_c \leq \delta^i\|f(X)\|$.

d) $g_i(X) = a_NX^N +$ términos de grado menor y $\|g_i(X)\| = |a_N|c^N$.

Describamos a continuación cómo obtener dos polinomios que sean una mejor aproximación.
Primero, como $\| \ \|$ satisface la propiedad no arquimediana ("todos los triángulos son isósceles "), la condición $\|f(X) - g_i(X)\| \leq \delta\|f(X)\|$ implica (como δ es menor que 1) que $\|f(X)\| = \|g_i(X)\|$.
Si dividimos $f(X) - g_i(X)h_i(X)$ por $g_i(X)$, obtenemos

$$f(X) - g_i(X)h_i(X) = q(X)g_i(X) + r(X),$$

donde $gr(r(X)) < N$ y por ende $gr(q(X)) \leq n - N$. Como sabemos que $g_i(X)$ cumple la condición (d), el lema anterior nos da las siguientes desigualdades:

$$\|q(X)\| \leq \frac{\|f(X) - g_i(X)h_i(X)\|}{\|g_i(X)\|} = \frac{\|f(X) - g_i(X)h_i(X)\|}{\|f(X)\|} \leq \delta^i \leq \delta,$$

y

$$\|r(X)\| \leq \|f(X) - g_i(X)h_i(X)\| \leq \delta^i \|f(X)\| \leq \delta \|f(X)\|.$$

Entonces definimos

$$g_{i+1}(X) = g_i(X) + r(X) \qquad \text{y} \qquad h_{i+1}(X) = h_i(X) + q(X).$$

Afirmamos que estos cumplen lo que queremos.
Como $gr(r(X)) < N$, entonces $gr(g_{i+1}(X)) = N$. De igual forma, como el grado de $q(X) \leq n - N$, entonces $gr(h_{i+1}) \leq n - N$. Esto prueba que los nuevos polinomios verifican la primer propiedad.
Por otro lado, tenemos que

$$\begin{aligned} \|f(X) - g_{i+1}(X)\| &= \|f(X) - g_i(X) - r(X)\| \\ &\leq \text{máx}\{\|f(X) - g_i(X)\|, \|r(X)\|\} \\ &\leq \delta \|f(X)\|. \end{aligned}$$

De forma similar,

$$\begin{aligned} \|h_{i+1}(X) - 1\| &= \|h_i(X) - 1 + q(X)\| \\ &\leq \text{máx}\{\|h_i(X) - 1\|, \|q(X)\|\} \\ &\leq \delta. \end{aligned}$$

Esto nos prueba que los nuevos polinomios satisfacen la segunda condición.
Ahora verifiquemos que efectivamente son una mejor aproximación (es decir que verifican (c) pero con $i + 1$):

$$\begin{aligned} f(X) - g_{i+1}(X)h_{i+1}(X) &= f(X) - (g_i(X) + r(X))(h_i(X) + q(X)) \\ &= f(X) - g_i(X)h_i(X) - q(X)g_i(X) - r(X)h_i(X) - r(X)q(X) \\ &= r(X)(1 - h_i(X) - q(X)), \end{aligned}$$

lo que nos da que

$$\begin{aligned} \|f(X) - g_{i+1}(X)h_{i+1}(X)\| &= \|r(X)\|\|(1 - h_i(X)) - q(X)\| \\ &\leq \delta^i \|f(X)\| \,\text{máx}\{\|1 - h_i(X)\|, \|q(X)\|\} \\ &\leq \delta^{i+1} \|(X)\|. \end{aligned}$$

Para la última condición, primero notemos que como $gr(r(X)) < N$, sumandoselo a $g_i(X)$ que tiene grado N, no cambia el término líder, es decir $g_{i+1}(X) = a_N X^N +$

términos de menos grado. Luego, como $\|f(X) - g_{i+1}(X)\| \leq \delta\|f(X)\|$ y $\delta < 1$, tenemos que $\|g_{i+1}(X)\| = \|f(X)\| = |a_N|c^N$.
Esto significa que $g_{i+1}(X)$ y $h_{i+1}(X)$ satisfacen todas nuestras propiedades reemplazando δ^i por δ^{i+1}.
Para verificar que estos polinomios efectivamente forman sucesiones de Cauchy, observemos que la desigualdad $\|q(X)\| \leq \delta^i$, es lo mismo que decir que

$$\|h_i(X) - h_{i+1}(X)\| \leq \delta^i.$$

De forma similar, la desigualdad $\|r(X)\| \leq \delta^i\|f(X)\|$ es lo mismo que

$$\|g_i(X) - g_{i+1}(X)\| \leq \delta^i\|f(X)\|.$$

Como $\delta < 1$ y la norma de $f(X)$ es fija, estas desigualdades nos prueban que las sucesiones $(g_i(X))$ y $(h_i(X))$ son sucesiones de Cauchy respecto a la norma $\| \ \|$.
Como una sucesión de Cauchy de polinomios de grado acotado es convergente respecto a $\| \ \|$, pues al ser acotado el grado podemos pensar a los polinomios como tuplas en $\mathbb{C}_p^k$ para algún k, y este espacio es claramente completo respecto a la norma (razonamiento similar al de la Proposición 3.1.3), tenemos entonces que nuestras sucesiones convergen a los polinomios buscados $g(X)$ y $h(X)$.

Solamente nos queda hallar nuestras primeras aproximaciones, es decir un $\delta < 1$ y un par inicial $g_1(X)$ y $h_1(X)$.
La hipótesis es que $\|f(X)\| = |a_N|c^N$ y que los términos de grado más grande son más chicos a la norma. Entonces, si restamos a $f(X)$ su parte de hasta grado N, el polinomio resultante tiene norma menor, es decir

$$\|f(X) - \sum_{i=0}^{N} a_i X^i\| < \|f(X)\|.$$

Sea δ tal que

$$\|f(X) - \sum_{i=0}^{N} a_i X^i\| = \delta\|f(X)\|.$$

Entonces claramente $0 < \delta < 1$. Definamos entonces $g_1(X) = \sum_{i=0}^{N} a_i X^i$ y $h_1(X) = 1$.
Claramente estos verifican las condiciones $(a) - (d)$.

□

Como el Teorema de Preparación de Weierstrass habla sobre series, la idea es hacer un razonamiento parecido al que hicimos recién, pero trabajando en el anillo $K[[X]]$ en vez de en $K[X]$. Por supuesto, ahora nos aparece el tema de la convergencia.

Definición 4.2.4. *Sea $c > 0$ real. Definimos A_c, como el subanillo de series de potencias $\sum a_n X^n \in K[[X]]$ tales que $\lim |a_n|c^n = 0$ (es decir, las series de potencias que convergen en $\overline{B}(0, c)$)*

Definimos ahora la norma en este espacio de series de potencias, y algunas de sus propiedades de forma análoga a la Proposición 4.2.1.

Proposición 4.2.5. *Sea $c > 0$ un número real. Definimos entonces una función $\| \ \|_c : A_c \longrightarrow \mathbb{R}_{\geq 0}$ de la siguiente forma: sea $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n + ...$ un elemento de A_c, entonces*

$$\|f(X)\|_c = \max_n |a_n|c^n.$$

Entonces tenemos que

a) $\|f(X)\|_c = 0$ *si y solo si* $f(X)$ *es idénticamente nulo.*

b) $\|f(X) + g(X)\|_c \leq \max\{\|f(X)\|_c, \|g(X)\|_c\}$.

c) $\|f(X)g(X)\|_c = \|f(X)\|_c\|g(X)\|_c$.

d) $\| \ \|_c$ *induce el valor absoluto p-ádico en las series de potencias constantes.*

e) Si $|x| \leq c$, *entonces* $|f(x)| \leq \|f(X)\|_c$.

f) La función $\| \ \|_c$ *se extiende a un valor absoluto no arquimediano en el cuerpo de funciones racionales* $K(X)$.

Ahora estamos en condiciones de enunciar el teorema central de esta sección (comenzaremos enunciandolo para $c = 1$).

Teorema 4.2.6 (Teorema de Preparación de Weierstrass p-ádico)**.** *Sea $f(X) = \sum a_n X^n$ una serie de potencias con coeficientes en K tal que $a_n \to 0$, es decir, que $f(x)$ converge para $x \in \mathcal{O}$. Sea N el entero que cumple que*

$$|a_N| = \max |a_n| \qquad y \qquad |a_n| < |a_N| \quad \text{para todo } n > N.$$

Entonces existe un polinomio

$$g(X) = b_0 + b_1X + \cdots + b_NX^N$$

de grado N con coeficientes en K, y una serie de potencias con coeficientes en K

$$h(X) = 1 + c_1X + c_2X^2 + ...,$$

tales que:

a) $f(X) = g(X)h(X)$.

b) $|b_N| = \max |b_n|$, *es decir* $\|g(X)\| = |b_N|$.

c) $\lim_{n\to\infty} c_n = 0$, *es decir,* $h(x)$ *converge para todo* $x \in \mathcal{O}$.

d) $|c_n| < 1$ *para todo* $n \geq 1$, *es decir,* $\|h(X) - 1\| < 1$.

e) $\|f(X) - g(X)\| < 1$.

En particular $h(X)$ *no tiene ceros en* $\mathcal{O}$.

Este teorema, se puede ver como una generalización del Teorema de Strassman, ya que como $h(X)$ no tiene ceros, es claro que los ceros de $f(X)$ son ceros de $g(X)$ y por ende hay a lo mucho N. De hecho, si nos movemos a $\mathbb{C}_p$, podemos decir más, pues como $\mathbb{C}_p$ es algebraicamente cerrado, tenemos que, contando multiplicidad, $g(X)$ tiene exactamente N ceros en $\mathbb{C}_p$, y como probamos a continuación, la condición en sus coeficientes nos asegura que todas sus raíces están en $\mathcal{O}$. Por lo tanto, tenemos que contando multiplicidad, $f(X)$ tiene exactamente N ceros en $\mathcal{O}$, lo que nos da una versión más fuerte del Teorema de Strassman.

Proposición 4.2.7. *Si un polinomio* $g(X) = b_0 + b_1X + \cdots + b_NX^N$ *en* $K[X]$ *cumple que* $|b_N| = \max |b_n|$, *y si* $g(\alpha) = 0$, *entonces* $|\alpha| \leq 1$.

Demostración. Dividiendo $g(X)$ por b_N, obtenemos un polinomio mónico cuyos coeficientes tienen valor absoluto menor o igual a 1. Por lo tanto, nos basta con probar que si $g(X) = b_0 + b_1X + \cdot + X^N$ es tal que $|b_i| \leq 1$ para todo i y α es una raíz de $g(X)$ entonces $|\alpha| \leq 1$. Para esto, sustituyendo por α en $g(X)$ obtenemos

$$\alpha^N = -(b_{N-1}\alpha^{N-1} + \cdots + b_1\alpha + b_0).$$

Luego

$$|\alpha|^N \leq \max_{0\leq i\leq N-1}\{|b_i||\alpha|^i\},$$

y, como $|b_i| \leq 1$, tenemos que

$$|\alpha|^N \leq \max_{0\leq i\leq N-1}\{|\alpha|^i\}.$$

Por lo tanto $|\alpha| \leq 1$. □

A continuación daremos un punteo de un posible proceso para probar el Teorema de Preparación de Weierstras:

a) Primero tendríamos que probar que A_1 es completo respecto a la norma $\| \ \|_1$.

b) Luego habría que probar que el espacio de polinomios $K[X]$ es denso en A_1 respecto a la topología definida por la norma.

c) A continuación, tendríamos que usar la completitud y la densidad de los polinomios de A_1 para probar el siguiente lema central, el cual es una versión del Lema 4.2.2 pero para series:

Lema 4.2.8. *Sea $f(X) \in A_1$ y $g(X) = b_0 + b_1X + \cdots + b_NX^N$ un polinomio en $K[X]$ tal que $|b_N| = \max |b_i|$. Entonces existe una serie de potencias $q(X) \in A_1$ y un polinomio $r(X) \in K[X]$ de grado N tal que*

$$f(X) = g(X)q(X) + r(X),$$

donde $q(X)$ y $r(X)$ verifican que

$$\|f(X)\|_1 \geq \|g(X)\|_1\|q(X)\|_1 \qquad y \qquad \|f(X)\|_1 \geq \|r(X)\|_1.$$

d) Para terminar, simplemente habría que repetir exactamente la demostración del Teorema 4.2.3 sustituyendo los usos del Lema 4.2.2 por el lema de la parte anterior.

Para probar la versión más general del Teorema de Preparación de Weierstrass p-ádico que enunciamos a continuación, habría que generalizar el Lema 4.2.8 para cualquier c, utilizando el mismo truco que en el Lema 4.2.2.

Teorema 4.2.9 (Teorema de Preparación de Weierstrass p-ádico 2)**.** *Sea c un real positivo, y $f(X) = \sum a_nX^n$, una serie en $K[[X]]$ tal que $|a_n|c^n \to 0$, es decir, que $f(x)$ converge para $x \in \overline{B}(0, c)$. Sea N el entero definido por las siguientes condiciones:*

$$|a_N|c^N = \max |a_n|c^n = \|f(X)\|_c \qquad y \qquad |a_n|c^n < |a_N|c^N \quad \text{para todo } n > N.$$

Entonces existe un polinomio

$$g(X) = b_0 + b_1X + \cdots + b_NX^N$$

de grado N con coeficientes en K y una serie de potencias

$$h(X) = 1 + d_1X + d_2X^2 + ...$$

con coeficientes en K, tales que:

a) $f(X) = g(X)h(X)$.

b) $|b_N|c^N = \max |b_n|c^n$, *es decir,* $\|g(X)\|_c = |b_N|c^N$.

c) $h(X) \in A_c$.

d) $|d_n|c^n < 1$ *para todo* $n \geq 1$, *es decir* $\|h(X) - 1\|_c < 1$.

e) $\|f(X) - g(X)\| < 1$.

En particular, $h(X)$ *no tiene ceros en* $\overline{B}(0, c)$.

Para terminar esta sección veremos una aplicación del Teorema de Preparación de Weierstrass para describir las series de potencias p-ádicas que definen una función entera, es decir, que la región de convergencia es todo $\mathbb{C}_p$. Vemos primero una condición para que una serie defina una función entera.

Lema 4.2.10. *La serie* $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ...$ *define una función entera si y solo si*

$$\lim_{n\to\infty} \frac{v_p(a_n)}{n} = +\infty.$$

Demostración. $f(X)$ es una función entera si y solo si $|a_n|c^n \to 0$ para todo $c \in \mathbb{R}$. O lo que es lo mismo, si $v_p(c) = k$, entonces $v_p(a_n) - kn \to +\infty$ para todo $k \in \mathbb{Q}$. En particular, $v_p(a_n)/n > k$ para n suficientemente grande, y por ende $v_p(a_n)/n \to \infty$.

Recíprocamente, supongamos $\lim_{n\to\infty} \frac{v_p(a_n)}{n} = \infty$, entonces para todo $k \in \mathbb{Q}$ definimos $M > k$.
Entonces, $v_p(a_n)/n > M$ para n suficientemente grande, por lo tanto

$$\frac{v_p(a_n) - kn}{n} = \frac{v_p(a_n)}{n} - k > M - k$$

para n suficientemente grande. Luego, multiplicando por n, tenemos que $v_p(a_n) - kn > (M - k)n \to +\infty$. Como k era arbitrario, $f(X)$ es entera. □

Supongamos entonces que tenemos una serie de potencias que define una función entera. Si $a_0 = 0$, podemos factorizar una potencia de X de tal forma que la serie restante tengo coeficiente independiente no nulo. Además, dividiendo por el término independiente, obtenemos una serie cuyo término independiente es igual a 1. Consideremos entonces a partir de ahora, una serie

$$f(X) = 1 + a_1X + a_2X^2 + ...$$

tal que $v_p(a_n)/n \to \infty$. La idea para entender los ceros de $f(X)$, es aplicar el Teorema

de Preparación de Weierstrass para bolas cada vez más grandes.
Comencemos entonces con la bola unitaria: una aplicación directa del teorema, nos dice que podemos factorizar $f(X)$ como $g_0(X)h_0(X)$, donde $g_0(X)$ es un polinomio y $h_0(X)$ es una serie de potencias de la forma $1 + b_1X + b_2X^2 + ...$ con $|b_i| < 1$. Como $\mathbb{C}_p$ es algebraicamente cerrado, $g_0(X)$ se factoriza totalmente, por lo que podemos escribir:

$$g_0(X) = \prod_{i=1}^{N}(1 - \lambda_i X),$$

donde los λ_i son los inversos de las raíces de $g_0(X)$, pues estamos asumiendo que $a_0 = 1$. Entonces

$$f(X) = h_0(X) \cdot \prod_{i=1}^{N}(1 - \lambda_i X),$$

donde $\|h_0(X) - 1\| < 1$.
Consideremos ahora la bola cerrada de centro cero y radio p. Aplicando la versión general del Teorema de Preparación de Weierstrass, obtenemos que

$$f(X) = g_1(X)(1 + d_1X + d_2X^2 + ...),$$

donde, $|d_i| < 1/p^i$. Luego, como $g_1(X)$ es un polinomio cuyas raíces son raíces de $f(X)$ en la bola cerrada de radio p, tenemos que $g_1(X)$ es divisible por $g_0(X)$. Por lo tanto, podemos escribir

$$g_1(X) = \prod_{i=1}^{N_1}(1 - \lambda_i X),$$

donde los λ_i son los inversos de las raíces de $f(X)$ en la bola cerrada de radio p. En conclusión, podemos escribir

$$f(X) = h_1(X) \cdot \prod_{i=1}^{N_1}(1 - \lambda_i X).$$

Las desigualdades en los d_i, nos dicen que $\|h_1(X) - 1\|_p < 1$, es decir $\|h_1(X) - 1\| < 1/p$. Luego, trabajando en bolas cada vez más grandes, la parte del polinomio tiene una expresión de producto cada vez más grande, y los λ_i que aparecen en el producto son los inversos de raíces con valor absoluto cada vez más grande, con lo que los λ_i son cada vez más chicos. Además, los otros factores están cada vez más cerca de 1 (con la norma $\| \ \|_1$, por lo que en el límite solamente nos queda el producto. Entonces hemos probado (sin realizar las cuentas formales necesarias):

Proposición 4.2.11. *Sea $f(X) = 1 + a_1X + a_2X^2 + ...$ un serie de potencias con coeficientes en $\mathbb{C}_p$ que define una función entera. Entonces $f(X)$ tiene un número finito de ceros en cualquier bola cerrada alrededor del origen, y por ende una cantidad numerable*

de ceros en $\mathbb{C}_p$. Los inversos de esas raíces, forman una sucesión (λ_i) que tiende a cero, y $f(X)$ puede ser escrito como

$$f(X) = \prod_{i=1}^{\infty} (1 - \lambda_i X),$$

con convergencia en la métrica $\| \ \|_c$ para todo c.

Demostración. Ya hemos "probado" la parte de convergencia para $c = 1$, pero como $f(X)$ es entera, podemos hacer un simple cambio de variable $X = \alpha X$ con $|\alpha| = c$ si $c = p^r$ con $r \in \mathbb{Q}$ y luego usar la densidad de estos para extender el resultado a $c \in \mathbb{R}_{\geq 0}$ y tendremos entonces la convergencia para $\| \ \|_c$ □

Para terminar esta sección, presentamos el resultado para las series de potencias enteras en general.

Corolario 4.2.12. *Sea $f(X)$ una serie de potencias con coeficientes en $\mathbb{C}_p$ que define una función entera, entonces $f(X)$ puede ser escrita como el siguiente producto:*

$$f(X) = aX^r \prod_{i=1}^{\infty} (1 - \lambda_i X),$$

donde $a \in \mathbb{C}_p$, $r \in \mathbb{Z}_{\geq 0}$, y λ_i son los inversos de las raíces no nulas de $f(X)$.

4.3 Polígonos de Newton

La idea de esta sección es usar lo que vimos en la anterior, para obtener información relevante sobre los ceros de polinomios o series de potencias con coeficientes en un cuerpo p-ádico K el cual sea completo. Al igual que en la sección anterior, veremos los resultados en profundidad para los polinomios y luego mencionaremos brevemente los resultados que se tienen para series.

Consideremos entonces $f(X) \in K[X]$. Como estamos interesados en entender los ceros de $f(X)$, en caso de que tenga raíz cero, sacamos de factor común la potencia de X más grande posible, y nos concentraremos en estudiar el otro factor; es decir, que en lo que sigue, vamos a asumir que nuestros polinomios tienen término independiente no nulo. Luego, al dividir a $f(X)$ por su término independiente (ahora no nulo), los ceros se mantienen, por lo que podemos, y vamos a asumir que $f(X) = 1 + a_1 X + \cdots + a_n X^n$.

Para presentar nuestra definición, comencemos por graficar en un par de ejes cartesianos[1] los puntos $(0, 0)$ y los puntos $(i, v_p(a_i))$ para cada $1 \leq i \leq n$ tal que $a_i \neq 0$. Entonces, definimos formalmente el polígono de Newton de $f(X)$ como la frontera inferior de la clausura convexa del conjunto de puntos antes descrito. En la práctica, pensaremos que el **Polígono de Newton de $f(X)$ se define de la siguiente forma** :

[1] En $\mathbb{R}^2$.

1) Comencemos considerando la semirrecta vertical que forma la parte negativa del eje y.

2) Imaginemos que rotamos esa semirrecta con eje en el origen y de forma antihoraria hasta que nos encontramos con uno de los puntos que graficamos.

3) En el momento en el que chocamos con un nuevo punto, "partimos" la recta y comenzamos a rotar nuevamente pero ahora con eje este nuevo punto. Continuamos rotando hasta que un nuevo punto sea encontrado.

4) Continuamos este procedimiento hasta que todos los puntos hayan sido "chocados" o estén estrictamente por arriba de una porción del polígono.

5) "Recortamos" la parte que la recta que sobra luego de haber encontrado el último punto.

Notemos que el polígono solamente depende de $v_p(a_i)$, lo cual no depende del cuerpo en el que pensemos a los a_i.
Veamos un ejemplo para asegurarnos de haber entendido la definición:

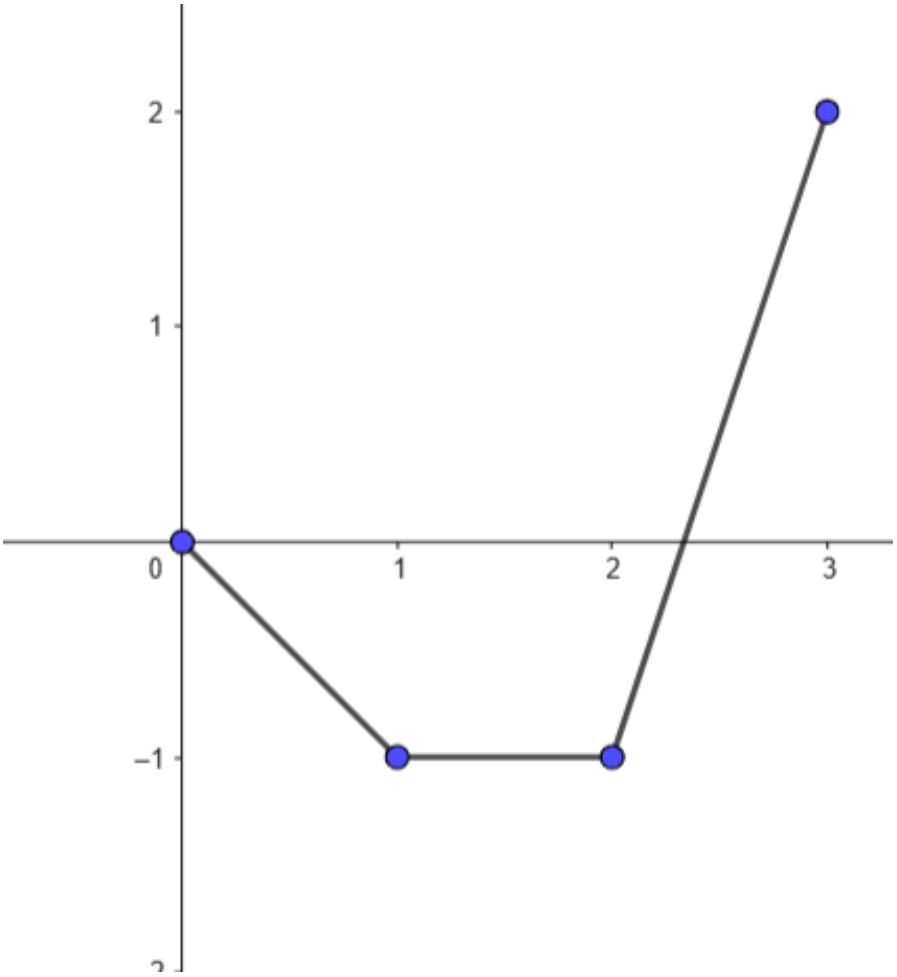
Sea $p = 3$ y consideremos el polinomio

$$f(X) = 9X^3 - \frac{55}{3}X^2 - \frac{79}{3}X + 1 = 9(X+1)\left(X - \frac{1}{27}\right)(X-3).$$

Luego, los puntos a graficar son

$$(0,0) \quad (1,-1) \quad (2,-1) \quad (3,2).$$

Luego, el proceso de la rotación nos da el siguiente polígono:



Como veremos a continuación, el Polígono de Newton contiene información sobre las raíces del polinomio. Antes de comenzar el estudio, definamos tres conceptos que nos serán útiles:

a) Decimos que las pendientes de los segmentos de recta que forman el polígono son las pendientes de Newton de $f(X)$.

b) La longitud de cada pendiente queda definida mediante la distancia que hay entre las proyecciones al eje x de los vértices del segmento correspondiente.

c) Los puntos de quiebre son los valores de i para los cuales el punto $(i, v_p(a_i))$ es un vértice del polígono.

En nuestro ejemplo, las pendientes son $-1, 0$ y 3, sus longitudes son todas 1; los puntos de quiebre se dan en $0, 1, 2$ y 3.

Notemos que la suma de las longitudes siempre va a ser igual al grado del polinomio y que $(0,0)$ y $(n, v_p(a_n))$ siempre van a ser vértices del polígono. También es claro por nuestra construcción que las pendientes forman una sucesión (finita) creciente.

Comencemos estudiando el primer segmento del polígono de Newton. Si este segmento tiene pendiente m, entonces conecta al punto $(0,0)$ con el punto (i, mi). Esto significa que no hay puntos por debajo de la recta $y = mx$; es decir, $v_p(a_j) \geq mj$ para todo j. Por otro lado, el punto (i, mi) nos está diciendo que $v_p(a_i) = mi$. Por último, el hecho de que se de un vértice en ese punto, nos dice que los demás puntos están por arriba de la recta que define, es decir que $v_p(a_j) > mj$ si $j > i$.
Escribiendo estos tres datos en función del valor absoluto obtenemos lo siguiente:

- $|a_j| \leq p^{-mj}$ para todo j, lo cual podemos escribir como $|a_j|(p^m)^j \leq 1$ para todo j.
- $|a_i| = p^{-mi}$, es decir, $|a_i|(p^m)^i = 1$.
- $|a_j| < p^{-mj}$ si $j > i$, lo cual podemos escribir como $|a_j|(p^m)^j$ si $j > i$.

Si nombramos $c = p^m$, podemos reescribir lo anterior en función de la norma c:

- $\|f(X)\|_c = 1$.
- i es el entero más grande tal que $\|f(X)\|_c = |a_i|c^i$.

En otras palabras, si tomamos $c = p^m$, entonces $\|f(X)\|_c = 1$ e i es el número que cumple las condiciones del Teorema 4.2.3. En particular, si i es menor al grado de $f(X)$, entonces $f(X)$ es divisible por un polinomio de grado i.
Consideremos entonces la siguiente definición:

Definición 4.3.1. *Un polinomio $f(X) \in K[X]$ es puro si su polígono de Newton tiene solo una pendiente. Si tiene pendiente m, decimos que $f(X)$ es puro de pendiente m.*

Luego tenemos el siguiente resultado:

Proposición 4.3.2. *Los polinomios irreducibles son puros.*

Juntando todo lo que dijimos hasta ahora y usando el Teorema 4.2.3 tenemos la siguiente proposición.

Proposición 4.3.3. *Sea $f(X) = 1 + a_1X + \cdots + a_nX^n \in K[X]$ tal que el primer vértice en su Polígono de Newton se da en (i, mi). Entonces existen polinomios $g(X), h(X) \in K[X]$ tales que :*

a) $f(X) = g(X)h(X)$.

b) $g(X)$ tiene grado i y es puro de pendiente m.

c) $h(X)$ no tiene ceros en $\overline{B}(0, p^m)$.

Consideremos el siguiente lema que nos da más información sobre los ceros de $f(X)$.

Lema 4.3.4. *Sea $f(X) = 1 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$ tal que el primer vértice en su Polígono de Newton se da en (i, mi). Sea $0 < c < p^m$ un real cualquiera. Entonces $\|f(X)\|_c = 1$ y $\|f(X) - 1\|_c < 1$. En particular, $f(X)$ no tiene ceros en la bola cerrada de radio c y centro 0 en $\mathbb{C}_p$.*

Demostración. Observar que si tenemos probado que $\|f(X) - 1\|_c < 1$, entonces para todo $x \in \mathbb{C}_p$ tal que $|x| \leq c$, tenemos que $|f(x) - 1| < 1$, lo cual claramente implica que $f(x) \neq 0$.
Además, por la Proposición 1.2.3, tenemos que si $\|f(X)-1\|_c < 1$, entonces $\|f(X)\|_c = 1$. Por lo tanto, solamente queda probar la desigualdad.
Una recta que pasa por el origen de pendiente $m_1 < m$ pasa por debajo de todos los puntos del polígono, cortandolo solamente en el punto $(0, 0)$. Esto significa que $v_p(a_j) > m_1 j$ para todo $j > 0$, que en términos del valor absoluto, significa que $|a_j| < p^{-m_1 j}$, o lo que es lo mismo, $|a_j|(p^{m_1})^j < 1$ para todo $j > 0$. Como $a_0 = 1$, el término independiente de $f(X) - 1$ es cero y por ende $|a_0 - 1| < 1$. Concluimos entonces que $\|f(X) - 1\|_c < 1$ para todo $c < p^{m_1}$, y por la densidad de $\mathbb{Q}$ en $\mathbb{R}$, tenemos la desigualdad del lema para todo $c \in \mathbb{R}$.

□

De hecho, como las raíces de $g(X)$ son raíces de $f(X)$ (siguiendo la notación de la Proposición 4.3.3), tenemos que $g(X)$ no tiene raíces de valor absoluto menor que p^m.
Por otro lado, si $\alpha_1, \alpha_2, ..., \alpha_i$ son las raíces de $g(X)$ en $\mathbb{C}_p$ (contando multiplicidad), entonces $g(X) = \prod_{k=1}^{i}(1 - \alpha_k^{-1}X)$, y por lo tanto, el coeficiente principal de $g(X)$ es igual a $(\alpha_1\alpha_2...\alpha_i)^{-1}$. Como $g(X)$ es puro, sabemos que este coeficiente tiene que tener valuación mi; como ya sabemos que $v_p(\alpha_j) \leq -m$, tenemos que $v_p(\alpha_j) = -m$ para todo j, es decir, todas las raíces de $g(X)$ tienen valor absoluto p^m.
Juntando el lema y lo anterior tenemos la siguiente proposición:

Proposición 4.3.5. *Sea $f(X) = 1 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$ tal que el primer vértice en su Polígono de Newton se da en (i, mi). Entonces $f(X)$ no tiene raíces con valor absoluto menor que p^m y tiene exactamente i raíces (contadas con multiplicidad en $\mathbb{C}_p$) con valor absoluto p^m.*

Estudiemos ahora el segundo segmento. Asumamos que hay vértices en los puntos (i, mi) y $(k, mi + m'(k - i))$, es decir que la primera pendiente es m de longitud i y la segunda es m' y tiene longitud $k - i$.
Tenemos que la recta que pasa por (i, mi) con pendiente m' tiene ecuación

$$y = mi + m'(x - i),$$

y sabemos lo siguiente:

- (i, mi) y $(k, mi + m'(k - i))$ están en la recta; en otras palabras, $v_p(a_i) = mi$ y $v_p(a_k) = mi + m'(k - i)$.
- Todos los puntos entre i y k están por arriba de la recta, es decir, $v_p(a_j) \geq m'(j - i) + mi$ si $i < j < k$.
- Todos los puntos después de k están estrictamente por arriba de la recta, es decir, $v_p(a_j) > m'(j - i) + mi$ si $j > k$. Además, la misma desigualdad vale para $j < i$.

Luego, escribiendo lo anterior en función del valor absoluto y tomando $c = p^{m'}$:

- $|a_j|c^j \leq p^{(m'-m)i}$ para todo j.
- $|a_k|c^k = p^{(m'-m)i}$.
- $|a_j|c^j < p^{(m'-m)i}$ si $j > k$.

Por último, en términos de la norma, tenemos que $\|f(X)\|_c = p^{(m'-m)i} > 1$ y que k es el número entero que cumple las condiciones del Teorema 4.2.3. Por lo tanto, podemos factorizar nuevamente $f(X)$ y realizando un proceso totalmente análogo a lo anterior, podemos concluir que $f(X)$ tiene exactamente k raíces en la bola cerrada de radio $p^{m'}$, i de las cuales tienen valor absoluto p^m, y $k - i$ tienen valor absoluto $p^{m'}$.
Repitiendo este argumento para cada vértice, tenemos el siguiente teorema:

Teorema 4.3.6. *Sea $f(X) = 1 + a_1X + ... + a_nX^n \in K[X]$, sean $m_1, m_2, ..., m_r$ las pendientes de su polígono de Newton (en orden creciente), y sean $i_1, i_2, ..., i_r$ sus correspondientes longitudes. Entonces, para cada $1 \leq k \leq r$, $f(X)$ tiene exactamente i_k raíces en $\mathbb{C}_p$ (contando multiplicidad) de valor absoluto p^{m_k}.*

Aplicando este teorema al ejemplo $f(X) = 9X^3 - \frac{55}{3}X^2 - \frac{79}{3}X + 1$, concluimos que f tiene una raíz de valor absoluto 3^{-1}, otra de valor absoluto $3^0 = 1$ y una última de valor absoluto 3^3; factorizando f vemos que estas raíces son $3, -1$ y $\frac{1}{27}$ respectivamente.

De una forma similar, se pueden definir los polígonos de Newton para series de potencias (prácticamente de la misma forma) teniendo cuidado con algunos casos degenerados, y siguiendo un razonamiento similar al anterior pero usando el Teorema de Preparación de Weierstrass p-ádico en vez del Teorema 4.2.3, obtenemos el siguiente teorema:

Teorema 4.3.7. *Sea $f(X) = 1 + a_1X + a_2X^2 + ...$ una serie de potencias que converge en la bola cerrada de radio $c = p^m$. Sean $m_1, m_2, ..., m_k$ las pendiente menores o iguales a m de su polígono de Newton, y sean $i_1, i_2, ..., i_k$ sus respectivas longitudes. Entonces, para cada j, $f(X)$ tiene i_j ceros con valor absoluto p^{m_j} y no hay otros ceros en la bola cerrada de radio p^m.*

Bibliografía

[1] J. W. S. Cassels. *Rational Quadratic Forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, London-New York, 1978.

[2] J. W. S. Cassels. *Local Fields*. Cambridge University Press, Cambridge, UK, 1st edition, 1986.

[3] F. Q. Gouvea. *p-adic Numbers: An Introduction*. Universitext. Springer-Verlag, Berlin, 3rd edition, 1997.

[4] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta Functions*. Graduate Texts in Mathematics. Springer, Berlin, 2nd edition, 1994.

[5] S. Lang. *Algebra*. Springer, New York, 3rd edition, 2002.