USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Teorema de Hasse-Minkowski

Javier Polo Noche

2022/2023

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Teorema de Hasse-Minkowski

Javier Polo Noche

Junio, 2023

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Teorema de Hasse-Minkowski
Breve descrición do contido
En xeral, non é nada fácil decidir se formas cuadráticas racionais representan un número racional dado sobre $\mathbb{Q}$. Por exemplo, os puntos racionais da circunferencia unidade $x^2 + y^2 = 1$ son $(\frac{-t^2+1}{t^2+1}, \frac{2t}{t^2+1})$ e $(-1, 0)$. Ademais do valor absoluto habitual en $\mathbb{Q}$, para cada primo p existe outro valor absoluto sobre $\mathbb{Q}$ chamado o valor absoluto p-ádico. Ao completar $\mathbb{Q}$ con respecto a este valor absoluto p-ádico obtense un corpo completo chamado o corpo dos p-ádicos, denotado por $\mathbb{Q}_p$. En teoría de números, os corpos dos p-ádicos son tan importantes como o corpo completo $\mathbb{R}$ dos números reais. Este TFG pretende dar unha perspectiva do teorema de Hasse-Minkowski que establece: Sexa $q(x_1, \ldots, x_n)$ unha forma cuadrática sobre $\mathbb{Q}$ en calquera dimensión $n \geq 1$. (1) Dado $r \in \mathbb{Q}^*$, a ecuación $q(x_1, \ldots, x_n) = r$ é resoluble sobre $\mathbb{Q}$ se e só se é resoluble sobre $\mathbb{R}$ e para todo $\mathbb{Q}_p$. (2) A ecuación $q(x_1, \ldots, x_n) = 0$ é resoluble de forma non trivial sobre se e só se é resoluble de forma non trivial sobre $\mathbb{R}$ e para todo $\mathbb{Q}_p$.
Bibliografía
A. Gamzon, The Hasse-Minkowski theorem, Honors Scholar Theses 17, University of Connecticut, OpenCommons@UConn, 2006. `https://opencommons.uconn.edu/srhonors_theses/17` J.-P. Serre, A course in Arithmetic, GTM 7, Springer-Verlag, 1973
Recomendacións (non vinculantes)

Índice

Resumen

En este trabajo enunciaremos y demostraremos el Teorema de Hasse-Minkowski. Este resultado es muy importante en teoría de números, al permitir determinar la existencia de soluciones racionales de ecuaciones dadas por formas cuadráticas. Para ello primeramente, recordaremos algunas nociones algebraicas sobre cuerpos finitos, formas cuadráticas, y sobre el Símbolo de Legendre y la Ley de Reciprocidad Cuadrática. Luego introduciremos el cuerpo de los números p-ádicos a partir del estudio de los valores absolutos sobre cuerpos y analizaremos en profundidad su estructura y propiedades básicas. Además, veremos cómo se comportan las soluciones de polinomios sobre ellos a lo largo de diferentes resultados, entre los que destaca el Lema de Hensel. A continuación definiremos el Símbolo de Hilbert y obtendremos algunos resultados de utilidad, estableciendo una relación entre este símbolo y el de Legendre. Finalmente, estudiaremos los cuerpos locales y las formas cuadráticas sobre los mismos. Todos estos conceptos y resultados trabajados nos permitirán probar el Teorema de Hasse-Minkowski y ver algún ejemplo de aplicación a formas cuadráticas concretas y a otros resultados de teoría de números sobre sumas de cuadrados de números enteros.

Abstract

In this work we will formulate and prove the Hasse-Minkowski Theorem. This result is very important in number theory, as it allows to determine the existence of rational solutions of equations given by quadratic forms. To do so, we will first recall some algebraic notions of finite fields, quadratic forms, and about the Legendre Symbol and the Quadratic Reciprocity Law. Then we will introduce the field of the p-adic numbers from the study of the absolute values on fields and we will analyze in depth its structure and basic properties. In addition, we will see how the solutions of polynomials on them behave throughout different results, among which Hensel's Lemma stands out. Next, we will define the Hilbert Symbol and obtain some useful

results, establishing a relationship between this symbol and the Legendre symbol. Finally, we will study the local fields and the quadratic forms on them. All these concepts and results worked will allow us to prove the Hasse-Minkowski Theorem and see some examples of application to concrete quadratic forms and other results of number theory on sums of squares of integers.

Introducción

El Teorema de Hasse-Minkowski, también conocido como Principio Local-Global de Hasse, es un resultado muy importante en el ámbito de la teoría de números. El enunciado de este resultado afirma que si Q es una forma cuadrática con coeficientes racionales en n variables, entonces la ecuación $Q = r$, $r \in \mathbb{Q}$, es resoluble sobre $\mathbb{Q}$ (y en el caso $r = 0$, resoluble de forma no trivial) si, y solo si, lo es sobre $\mathbb{R}$ y sobre $\mathbb{Q}_p$ (donde p es un entero primo y $\mathbb{Q}_p$ denota al cuerpo de los racionales p-ádicos) para todo primo p. Tal y como se explica en [6], [7] y [16], en la segunda mitad del siglo XIX el matemático Hermann Minkowski realizó un profundo estudio de la teoría de formas cuadráticas sobre los racionales. En particular, demostró un resultado que afirmaba que cualquier forma cuadrática con coeficientes racionales tiene ceros racionales no triviales si, y solo si, tiene algún cero no trivial sobre $\mathbb{R}$ y sobre todos los anillos de la forma $\mathbb{Z}/p^n\mathbb{Z}$, con p un número primo y n entero positivo. En el momento de proporcionar este resultado Minkowski no podía utilizar ninguna propiedad ni notación relativa a los p-ádicos, puesto que estos todavía no habían sido creados. Quien se encargó de introducirlos fue Kurt Hensel a comienzos del siglo XX. Años después, el matemático Helmut Hasse se encontraba haciendo su tesis bajo la supervisión del propio Hensel, y este le indicó que podía volver a demostrar resultados teoría de números empleando el lenguaje y las propiedades de los números p-ádicos. Así, en 1921 demostró el Teorema de Hasse-Minkowski para formas cuadráticas sobre los números racionales, un resultado equivalente al de Minkowski de unas décadas antes, pero empleando herramientas de los p-ádicos. En 1924 lo extendería a otros cuerpos.

La idea detrás de este resultado es habitual en matemáticas y supone el origen de una de las denominaciones del resultado: analizar lo "local" para obtener información "global". Por ejemplo, para que una ecuación diofántica posea soluciones enteras debe tenerlas sobre $\mathbb{R}$ y sobre cualquier anillo $\mathbb{Z}/p^n\mathbb{Z}$, donde p es un primo y $n \in \mathbb{Z}^+$. Por tanto, si al realizar la reducción de la ecuación esta no tiene soluciones podremos concluir que tampoco las tiene el inicial. En el caso del Teorema de Hasse-Minkowski ocurriría algo análogo: si probásemos que una ecuación dada por una forma cuadrática de la forma descrita en el párrafo anterior no posee solución racional sobre algún $\mathbb{Q}_p$ (que forman parte de los conocidos como "cuerpos locales") o sobre $\mathbb{R}$, tampoco la tendría sobre $\mathbb{Q}$.

El objetivo de este trabajo es enunciar y demostrar el Teorema de Hasse-Minkowski, siendo necesario estudiar antes diversos conceptos algebraicos. Para ello, el trabajo se divide en cinco capítulos cuya estructura y contenido describimos a continuación.

El Capítulo 1 contiene tres partes diferenciadas. En la primera hacemos un repaso sobre los cuerpos finitos y sus propiedades. Posteriormente trabajamos algunos resultados relacionados con las ecuaciones y los polinomios sobre cuerpos finitos, entre los que destaca el Teorema de Chevalley-Warning, que nos permitirá concluir que todas las formas cuadráticas con tres o más variables sobre un cuerpo finito tienen al menos un cero no trivial. La segunda sección está dedicada a la Ley de Reciprocidad Cuadrática y sus propiedades fundamentales que emplearemos, esencialmente, en el Capítulo 3. En la tercera y última parte revisamos definiciones y resultados básicos relativos a las formas cuadráticas.

El Capítulo 2 trata sobre los números p-ádicos. El primero en introducirlos fue el matemático Kurt Hensel a comienzos del siglo XX. Constituyen una completación de $\mathbb{Q}$ diferente de la considerada más habitualmente ($\mathbb{R}$). Como el primero, este capítulo se estructura en tres partes. En la primera se estudian los valores absolutos sobre el cuerpo $\mathbb{Q}$, poniendo especial énfasis en el valor absoluto p-ádico que dará lugar a los racionales p-ádicos. Enunciamos y demostramos el Teorema de Ostrowski, que sirve para caracterizar todos los valores absolutos sobre $\mathbb{Q}$ en función del valor absoluto usual y de los valores absolutos p-ádicos. La sección finaliza estudiando la completitud de $\mathbb{Q}$ respecto de los valores absolutos p-ádicos. La segunda sección, más breve que la primera, se dedica a estudiar el cuerpo de los números p-ádicos, en particular las unidades y cuadrados del mismo. La tercera parte tiene como objetivo analizar propiedades y resultados de los polinomios sobre los enteros p-ádicos ($\mathbb{Z}_p$), entre los que sobresale el Lema de Hensel, muy útil para ver ejemplos concretos de aplicación del Teorema de Hasse-Minkowski.

El Capítulo 3 trata el Símbolo de Hilbert, que lleva el nombre del reconocido matemático alemán que lo introdujo a finales del siglo XIX. Dados dos elementos no nulos sobre un cierto cuerpo, el Símbolo de Hilbert indica si la ecuación dada al igualar un polinomio de segundo grado en tres variables (en el que aparecen dichos valores como coeficientes de dos de ellas) tiene alguna solución no trivial con valores en dicho cuerpo (vale 1 en ese caso) o no (valdrá -1). Las propiedades que aquí trabajaremos serán utilizadas en los Capítulos 4 y 5. Entre los resultados demostrados destaca un teorema que relaciona el Símbolo de Hilbert con el de Legendre.

En el Capítulo 4 realizamos una introducción a los cuerpos locales y estudiamos las formas cuadráticas sobre ellos. Para esto último empleamos propiedades vistas en el Capítulo 3 y definimos el Invariante de Hasse como producto de unos ciertos símbolos de Hilbert. Los resultados que veamos sobre formas cuadráticas en cuerpos locales serán también de utilidad para el Teorema de Hasse-Minkowski, ya que tratarán fundamentalmente sobre ceros de dichas formas cuadráticas o sobre si estas representan unos ciertos valores.

El Capítulo 5 contiene la demostración del Teorema de Hasse-Minkowski. La demostración se realiza distinguiendo varios casos en función de la dimensión de la forma cuadrática. A continuación vemos un ejemplo de aplicación del resultado a una forma cuadrática concreta. Finalmente, utilizando el teorema demostramos un resultado conocido referente a sumas de cuadrados que nos permite deducir otros dos de la misma temática.

Capítulo 1

Preliminares

1.1. Cuerpos Finitos

El objetivo de esta primera sección es revisar algunos conceptos y resultados básicos relacionados con cuerpos finitos y con las ecuaciones sobre ellos, que se pueden encontrar en referencias como [1] y [14].

Definición 1.1. Dado un cuerpo K se denomina subcuerpo primo de K al menor subcuerpo de K que contiene a 1_K.

Dado un cuerpo K arbitrario se puede definir la siguiente aplicación:

$$f : \mathbb{Z} \longrightarrow K,\ f(n) = n \cdot 1_K$$

Se trata del homomorfismo de anillos que se utiliza para definir el concepto de característica de un cuerpo. Para este homomorfismo hay dos posibilidades:

- $\ker f = \{0\}$, en cuyo caso la aplicación se puede extender a $\mathbb{Q}$. La característica de K aquí es 0.
- $\ker f \neq \{0\}$, y entonces $\ker f = n\mathbb{Z}$, con n el menor entero positivo que se encuentra en el núcleo. Se puede probar que en esta situación n será un número primo y el cuerpo tendrá característica n.

Así, la imagen de $\mathbb{Z}$ por la aplicación definida previamente es un dominio entero y será isomorfa a $\mathbb{Z}$ o a $\mathbb{Z}/p\mathbb{Z}$, p primo. El cuerpo de fracciones será isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}/p\mathbb{Z}$, respectivamente. En el primer caso se dice que el cuerpo K tiene característica 0, y se escribe como $\mathrm{char}(K) = 0$; en el segundo, que es de característica p.

Observación 1.2. En un cuerpo de característica p, p es el menor entero positivo m que verifica que $m \cdot 1_K = 0$. Cuando el cuerpo es de característica p el subcuerpo primo de K se corresponde con $f(\mathbb{Z})$ y se denota por F_p.

Proposición 1.3. *Sea K es un cuerpo de característica p. Consideremos la aplicación*

$$f : K \longrightarrow K,\ f(x) = x^p.$$

Se tiene que f es un homomorfismo de cuerpos y que para todo $y \in F_p$, $f(y) = y$.

Demostración. Es obvio que $f(xy) = f(x)f(y)$. Veamos que $f(x+y) = f(x) + f(y)$.

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$$

Puesto que, en la expresión anterior, si $i \neq 0, p$, $\binom{p}{i}$ es múltiplo de p. En consecuencia $(x+y)^p = x^p + y^p$.
Falta ahora ver que para todo $y \in F_p$ $f(y) = y$. En efecto, si $y \in F_p$ entonces existe un m entero tal que $0 < m < p$. En ese caso $y = m \cdot 1_K$, por lo que

$$f(y) = f(1_K) + \cdots + f(1_K) = 1_K + \cdots + 1_K = y$$

□

El siguiente resultado caracteriza los cuerpos finitos.

Teorema 1.4. *Sea K un cuerpo finito de q elementos. Se tiene que:*

1. *Si el cuerpo K tiene característica p y $[K : F_p] = n$ (donde $[\ :\ ]$ denota al grado de la extensión de cuerpos) entonces el cardinal de K es $q = p^n$.*
2. *Sean p un primo, $q = p^n$ con n entero positivo y Ω un cuerpo algebraicamente cerrado de característica p. Entonces existe un único subcuerpo F de Ω con q elementos, que coincide precisamente con el conjunto de raíces del polinomio $X^q - X$.*

Demostración. Comprobemos las dos afirmaciones:

1. Como el cuerpo tiene característica p su subcuerpo primo F_p es isomorfo a $\mathbb{Z}/p\mathbb{Z}$. La extensión $[K : F_p]$ es finita y si su grado es n se deduce que $|K| = p^n$.
2. Sea Ω un cuerpo algebraicamente cerrado con característica p. La proposición anterior permite asegurar que la aplicación $x \mapsto x^q, q = p^n$ es un automorfismo de Ω (resulta de componer n veces el homomorfismo $x \mapsto x^p$), y aquellos elementos que quedan fijos por el

automorfismo son precisamente $F = \{x \text{ tales que } x^q = x\} = \{x \text{ tales que } x^q - x = 0\}$. Por otro lado, la derivada del polinomio $X^q - X$ es $qX^{q-1} - 1$. Ahora bien,

$$qX^{q-1} - 1 = p \cdot p^{n-1}X^{q-1} - 1 = -1 \neq 0,$$

por lo que como Ω es algebraicamente cerrado podemos deducir que el polinomio $X^q - X$ tiene exactamente q raíces distintas, de lo que se concluye $|F| = q$. Para ver que es el único, supongamos que existe otro subcuerpo H de Ω con q elementos, entonces el grupo multiplicativo H^* tiene $q-1$ elementos. Por tanto, si $x \in H^*$ entonces $x^{q-1} = 1$, lo cual equivale a que $x^q - x = 0$, es decir $H \subset F$, y como $|H| = |F|$, $H = F$.

□

Observación 1.5. Al cuerpo F del resultado anterior se le suele denotar por F_q (cuando tiene q elementos).

Proposición 1.6. *Todos los cuerpos finitos de $q = p^n$ elementos son isomorfos.*

Sea $q = p^n, n \in \mathbb{Z}^+$ y p primo.

Teorema 1.7. *El grupo multiplicativo F_q^* de un cuerpo F_q (de q elementos) es un grupo cíclico de $q-1$ elementos.*

Ecuaciones sobre un Cuerpo Finito

En esta parte p será un entero primo, q una potencia de p y K un cuerpo de q elementos (K tiene característica p).

Lema 1.8. *Sea m un entero no negativo. Entonces* $\displaystyle\sum_{x \in K} x^m = \begin{cases} -1 & \text{si } m \neq 0 \text{ y múltiplo de } q-1 \\ 0 & \text{en otro caso} \end{cases}$

Observación 1.9. Supondremos $x^m = 1$ si $m = 0$, incluyendo el caso $x = 0$.

Demostración. Distinguimos varios casos:

- Si $m \neq 0$ y divisible por $q-1$ entonces $0^m = 0$ y $x^m = 1$ para todo $x \neq 0$, ya que en ese caso $x \in K^*$, $|K^*| = q-1$, K^* es un grupo cíclico y m es múltiplo de $q-1$. En consecuencia $\displaystyle\sum_{x \in K} x^m = (q-1) \cdot 1 = -1$.
- $m = 0$. En ese caso $x^m = 1$, $x \in K$ por lo que $\displaystyle\sum_{x \in K} x^m = q \cdot 1 = 0$ por ser K de característica p.

- Si $m \neq 0$ y no es divisible por $q-1$ como K^* es cíclico de orden $q-1$ existirá un elemento $y \in K^*$ tal que $y^m \neq 1$. Si denotamos por S la suma del enunciado,

$$S = \sum_{x \in K^*} x^m = \sum_{x \in K^*} y^m x^m = y^m \sum_{x \in K^*} x^m = y^m S.$$

  Por tanto, $(1-y^m)S = 0$, y como $1 - y^m \neq 0$, $S = 0$.

□

Teorema 1.10 (Chevalley-Warning)**.** *Sean $f_\alpha \in K[X_1, \ldots, X_n]$ polinomios en n variables tal que $\sum_\alpha \deg(f_\alpha) < n$ (donde $\deg(f_\alpha) < n$ denota al grado del polinomio f_α). Si V es el conjunto de raíces comunes de todos los polinomios en K^n entonces $|V| \equiv 0 \,(\text{mód}\, p)$.*

Demostración. Sea $x \in K^n$ y denotemos por $P = \prod_\alpha (1 - f_\alpha^{q-1})$. Si $x \in V$ entonces $f_\alpha(x) = 0$ para cualquier α, luego $P = 1$ en ese caso. Si $x \notin V$ entonces existe α de forma que $f_\alpha(x) \neq 0$, por lo que $f_\alpha^{q-1}(x) = 1$ y $P = 0$.
Ahora, dado un polinomio g denotemos por $S(g) = \sum_{x \in K^n} g(x)$. Por tanto, $|V| \equiv S(P) \pmod p$, ya que, como vimos antes, si $x \in V$, $P = 1$ y si $x \notin V$, $P = 0$ y el cuerpo K es de característica p. Solo queda comprobar que $S(P) = 0$. Como $\sum_\alpha \deg(f_\alpha) < n$ $\deg(P) < (q-1) \cdot n$, P debe ser combinación lineal de monomios de la forma $X^m = X^{m_1} \cdots X^{m_n}$ con $m_1, \ldots, m_n$ cumpliendo que $\sum_{i=1}^n m_i < n \cdot (q-1)$. Será suficiente probar que para alguno de los monomios X^{m_j} $S(X^{m_j})$ vale 0, pero ello se concluye del Lema 1.8 (ya que existirá algún $m_j < q-1$). □

Corolario 1.11. *Si $\sum_\alpha \deg(f_\alpha) < n$ y si las f_α tienen términos no constantes, entonces los polinomios f_α tienen un cero común no trivial.*

Demostración. Se concluye de que si $V = \{0\}$ entonces $|V|$ no sería divisible por p (lo cual sería contradictorio con el teorema anterior). □

Corolario 1.12. *Todas las formas cuadráticas de al menos 3 variables sobre el cuerpo K tienen un cero no trivial.*

Observación 1.13. A pesar de que todavía no se ha proporcionado la definición del concepto de forma cuadrática (se trata con posterioridad en este capítulo y seguramente ya sea conocida para el lector), el Corolario 1.12 se ha incluido aquí al tratarse de un resultado que se deduce a partir de los que se estudian con anterioridad en esta sección.

1.2. Ley de Reciprocidad Cuadrática

Vamos ahora a trabajar un resultado fundamental en teoría de números, la Ley de Reciprocidad Cuadrática. Dicho resultado tiene relación con el concepto de Símbolo de Legendre, que esencialmente viene a indicar si una cierta ecuación de grado 2 tiene solución módulo un cierto número primo. Las propiedades del Símbolo de Legendre y la Ley de Reciprocidad Cuadrática son importantes para trabajar propiedades del Símbolo de Hilbert, que constituye un concepto fundamental en la demostración del Teorema de Hasse-Minkowski, y que veremos en profundidad en el tercer capítulo. Las referencias seguidas para esta sección son [11] y [14].

Sea q una potencia de un primo p.

Teorema 1.14. *Si $p = 2$ entonces todos los elementos de F_q (manteniendo la notación de la sección anterior) son cuadrados. Si $p \neq 2$ entonces los cuadrados de F_q^* forman un subgrupo de índice 2 en F_q^*. Este subgrupo coincide con el núcleo del homomorfismo $x \mapsto x^{\frac{q-1}{2}} \in \{+1, -1\}$.*

Demostración. La primera afirmación se concluye de que el homomorfismo $x \mapsto x^2$ es un automorfismo de F_q.
En cuanto a la segunda, sea Ω una clausura algebraica de F_q. Si $x \in F_q^*$ existirá un $y \in \Omega$ tal que $y^2 = x$. En ese caso

$$y^{q-1} = x^{\frac{q-1}{2}} = \pm 1$$

ya que $x \in F_q^*$ y F_q^* es un grupo de orden $q-1$, por lo que $1 = x^{q-1} = x^{(\frac{q-1}{2})\cdot 2}$, y entonces $x^{\frac{q-1}{2}} = 1$ o $x^{\frac{q-1}{2}} = -1$, y esto último se justifica con que estamos suponiendo que la característica del cuerpo es $p \neq 2$. De lo anterior también podemos deducir que $x \in F_q^{*2}(x \text{ es cuadrado}) \iff y \in F_q^* \iff y = 1$. Por tanto, F_q^{*2} es el núcleo del homomorfismo $x \mapsto x^{\frac{q-1}{2}}$ y como F_q^* tiene $q-1$ elementos quedaría probado que F_q^{*2} tiene índice 2. □

Observación 1.15. De la demostración anterior se concluye que $F_q^*/F_q^{*2} \simeq \mathbb{Z}/2\mathbb{Z}$.

Definición 1.16. Sea p un primo impar y $x \in F_p^*$, es decir $x \not\equiv 0 \,(\text{mód}\, p)$. Se define el Símbolo de Legendre de x, y se denota por $\left(\frac{x}{p}\right)$, como el entero $x^{\frac{p-1}{2}}$ que, como se vio previamente, solo toma los valores 1 y -1.

Observación 1.17. Se suele extender la definición a todo F_p escribiendo que $\left(\frac{0}{p}\right) = 0$.

La Definición 1.16 es útil para relacionar el Símbolo de Legendre con lo visto anteriormente. No obstante, en la literatura suele ser más habitual la que se explica a continuación, además de que con ella puede quedar más clara la "utilidad" de este concepto. Ambas definiciones son equivalentes.

Definición 1.18. Dados $a \in \mathbb{Z}$, p un primo impar tal que a y p son coprimos, se define el Símbolo de Legendre $\left(\frac{a}{p}\right)$ como

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{si la congruencia } x^2 \equiv a \,(\text{mód } p) \text{ tiene solución,} \\ -1, & \text{si la congruencia } x^2 \equiv a \,(\text{mód } p) \text{ no tiene solución.} \end{cases}$$

Cuando la congruencia tiene solución, es decir, cuando el Símbolo de Legendre vale 1, se dice que a es un residuo cuadrático módulo p; en caso contrario no lo sería. De forma análoga a la Observación 1.17, si a fuese múltiplo de p, $\left(\frac{a}{p}\right) = 0$.

Observación 1.19. Las Definiciones 1.16 y 1.18 son equivalentes ya que la congruencia $x^2 \equiv a \,(\text{mód } p)$ tiene solución si, y solo si, tiene solución la ecuación $\bar{x}^2 = \bar{a} \equiv a \,(\text{mód } p) \in F_p^*$ tiene solución en F_p. Además, si $a \equiv b \,(\text{mód } p)$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

La siguiente es una propiedad fundamental del Símbolo de Legendre.

Teorema 1.20 (Criterio de Euler)**.** *Sean p un primo impar y $a \in \mathbb{Z}$. Se verifica que*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \,(\text{mód } p)$$

Proposición 1.21. *Sean p un primo impar y $a, b \in \mathbb{Z}$. Se verifica que*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Siguiendo la notación de [14] definamos, dado $n \in \mathbb{Z}$, los siguientes elementos:

- $\epsilon(n) \equiv \frac{n-1}{2} \,(\text{mód } 2) = \begin{cases} 0 & \text{si } n \equiv 1 \,(\text{mód } 4) \\ 1 & \text{si } n \equiv -1 \,(\text{mód } 4) \end{cases}$
- $\omega(n) \equiv \frac{n^2-1}{8} \,(\text{mód } 2) = \begin{cases} 0 & \text{si } n \equiv \pm 1 \,(\text{mód } 8) \\ 1 & \text{si } n \equiv \pm 3 \,(\text{mód } 8) \end{cases}$

$\epsilon(n)$ y $\omega(n)$ son homomorfismos de grupos entre $\mathbb{Z}/2\mathbb{Z}$ y las unidades de $\mathbb{Z}/4\mathbb{Z}$ y $\mathbb{Z}/8\mathbb{Z}$.

Proposición 1.22. *Se verifican:*

1. $\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$
2. $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$

Teorema 1.23 (Ley de Reciprocidad Cuadrática de Gauss)**.** *Sean p y l primos impares distintos entre si. Se tiene que*

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

Las demostraciones de este resultado y de las propiedades del Símbolo de Legendre se pueden encontrar en [11] y [14]. Tal y como hemos comentado al comienzo de la sección, los conceptos y resultados explicados para la Ley de Reciprocidad Cuadrática son importantes para la sección sobre el Símbolo de Hilbert, que posee mucha relación con la Ley de Reciprocidad Cuadrática (y se puede considerar una generalización de la misma).

1.3. Fundamentos de Formas Cuadráticas

Para finalizar con este capítulo revisaremos conceptos y resultados fundamentales sobre formas cuadráticas, centrándonos especialmente en aquellas propiedades que necesitamos para ver todo lo relacionado con el Teorema de Hasse-Minkowski, y que podemos encontrar en [2] y [14].

Definición 1.24. Sea A un anillo conmutativo y V un módulo sobre él. Una aplicación $Q : V \to A$ se dice que es una forma cuadrática en V si verifica:

- $Q(av) = a^2Q(v)$ para todo $a \in A$ y para todo $v \in V$.
- La aplicación definida sobre $V \times V$ como $(v_1, v_2) \mapsto Q(v_1 + v_2) - Q(v_1) - Q(v_2)$ es bilineal.

El par (V, Q) se denomina módulo cuadrático. El caso que interesará en este trabajo es aquel en el que A sea un cuerpo de característica distinta de 2 y V un A-módulo, es decir, trabajaremos el caso de los espacios vectoriales (que supondremos de dimensión finita).

Definición 1.25. Si consideramos Q una forma cuadrática, la aplicación $(x, y) \mapsto x \cdot y$, donde

$$x \cdot y = \frac{1}{2}[Q(x + y) - Q(x) - Q(y)]$$

es una aplicación bilineal que se denomina producto escalar asociado a la forma cuadrática Q.

Definición 1.26. Dados dos módulos cuadráticos (V, Q) y (V', Q') se dice que una aplicación lineal $f : V \to V'$ es un morfismo métrico de (V, Q) en (V', Q') si $Q' \circ f = Q$.

Definición 1.27. Si V es un espacio vectorial y Q una forma cuadrática en él y $\{e_i\}_{i=1}^n$ es una base V, se define la matriz asociada a Q como $A = (a_{ij})$, donde $a_{ij} = e_i \cdot e_j$ y para un $x = \sum_{i=1}^{n} x_i e_i$ se tiene que $Q(x) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$

Observación 1.28. Si se realiza un cambio de base a través de una matriz X (que debe ser invertible) la nueva matriz $A' = XAX^t$, y su determinante es $\det(A') = \det(A)\det(X)^2$.

Definición 1.29. En la observación anterior, el valor de $\det(X)^2$ se denomina discriminante de la forma cuadrática Q, y se denota por $\mathrm{disc}(Q)$.

Definición 1.30. Sea (V, Q) un módulo cuadrático sobre un cuerpo K. Dos elementos x, y se dice que son ortogonales si $x \cdot y = 0$. El conjunto de elementos ortogonales a un subconjunto V_1 de V se denota por V_1^0. Dos subespacios V_1 y V_2 son ortogonales si $x \cdot y = 0$ para todo $x \in V_1$ e $y \in V_2$. V^0 se denomina radical de V (se denota por $\mathrm{rad}(V)$), y si $V^0 = \{0\}$ se dice que Q es no degenerada.

Proposición 1.31. *Una forma cuadrática es no degenerada si, y solo si, su discriminante es no nulo.*

Definición 1.32. Una base de un módulo cuadrático se dice ortogonal si sus elementos son ortogonales dos a dos.

Teorema 1.33. *Todo módulo cuadrático admite una base ortogonal.*

Definición 1.34. Sean $U_1, \ldots, U_n$ subespacios de V. Se dice que V es suma ortogonal directa de los subespacios U_i si U_i es ortogonal a U_j para todo $j \neq i$ y además $V = U_1 + \cdots + U_n$.

Observación 1.35. En relación a la definición anterior, si un $x \in V$ tiene componentes x_i, con $x_i \in U_i$ entonces $Q(x) = \sum Q_{|_{U_i}}(x_i)$.

Definición 1.36. Dado un módulo cuadrático (V, Q) un elemento $x \in V \setminus \{0\}$ se dice isotrópico o anulador si $Q(x) = 0$. Un subespacio de V se dirá isotrópico si todos sus elementos son isotrópicos.

Definición 1.37. Un módulo cuadrático que posee una base formada por dos elementos x e y tales que $x \cdot y \neq 0$ se denomina plano hiperbólico.

Definición 1.38. Una forma cuadrática $Q : V \to A$ se dice universal si $Q(V) = A$.

Teorema 1.39. *Una forma cuadrática no degenerada con un vector isotrópico es universal.*

Definición 1.40. Dos formas cuadráticas Q y Q' se dicen equivalentes si sus módulos cuadráticos son isomorfos. En ese caso escribimos $Q \sim Q'$.

Definición 1.41. Sean $Q_1(X_1, \ldots, X_n)$ y $Q_2(X_1, \ldots, X_m)$ sendas formas cuadráticas en n y m variables, respectivamente. Se denota por $Q_1 + Q_2$ a la forma cuadrática $Q_1(X_1, \ldots, X_n) + Q_2(X_{n+1}, \ldots, X_{n+m})$ en $n + m$ variables, donde la operación suma es ortogonal.

Definición 1.42. Una forma cuadrática $Q(X_1, X_2)$ en dos variables se dice hiperbólica si $Q \sim X_1^2 - X_2^2$.

Observación 1.43. La definición anterior la podemos relacionar con la Definición 1.37 en el sentido en que una forma cuadrática sobre un cuerpo K será hiperbólica si el módulo cuadrático (K^2, Q) es un plano hiperbólico.

Teorema 1.44. *Toda forma cuadrática degenerada posee un vector isotrópico.*

Definición 1.45. Diremos que una forma cuadrática $Q(X_1, \ldots, X_n)$ sobre un cuerpo K representa a un elemento $a \in K$ si existe un $x \in K^n, x \neq 0$, de forma que $Q(x) = a$.

Observación 1.46. De la definición anterior se concluye que una forma cuadrática representará al 0 si, y solo si, el módulo cuadrático posee un elemento isotrópico no nulo.

Teorema 1.47. *Si Q representa a 0 y es no degenerada se tiene que $Q \sim Q_1 + Q_2$, donde Q_1 es hiperbólica. Se puede afirmar también que Q es universal.*

Corolario 1.48. *Sea $Q = Q(X_1, X_2, \ldots, X_{n-1})$ una forma cuadrática no degenerada y sea $a \in K^*$. Los siguientes enunciados son equivalentes:*

1. *Q representa a a.*
2. *$Q \sim Q_1 + aZ^2$, donde Q_1 es una forma cuadrática en $n-2$ variables.*
3. *La forma cuadrática $Q_2 = Q - aZ^2$ representa al 0.*

Corolario 1.49. *Si Q_1 y Q_2 son dos formas cuadráticas no degeneradas y $Q = Q_1 - Q_2$, los siguientes enunciados son equivalentes:*

1. *Q representa a 0.*
2. *Existe un $a \in K^*$ tal que $Q_1 - aZ^2$ y $Q_2 - aZ^2$ representan a 0.*
3. *Existe un $a \in K^*$ representado por Q_1 y Q_2.*

Teorema 1.50. *Sea Q una forma cuadrática en n variables sobre un cuerpo K. Entonces existen $a_1, a_2, \ldots, a_n \in K$ tal que $Q \sim a_1X_1^2 + \cdots + a_nX_n^2$.*

Definición 1.51. En relación al teorema anterior, se denomina rango de una forma cuadrática al número de índices a_i que son no nulos.

Definición 1.52. La dimensión de una forma cuadrática Q sobre V es la dimensión de V.

Observación 1.53. El rango de una forma cuadrática es n si, y solo si, su discriminante (que vale $a_1 \cdots a_n$) es no nulo, es decir, si, y solo si, la forma cuadrática es no degenerada.

La definición anterior posee un elevado interés al poder relacionarse con las sumas de cuadrados.

Corolario 1.54. *Sean Q_1 y Q_2 dos formas cuadráticas no degeneradas de rango mayor o igual que 1, y consideremos $Q = Q_1 - Q_2$. Son equivalentes:*

1. *Q representa al 0.*
2. *Existe un $a \in K^*$ representado por Q_1 y Q_2.*

Teorema 1.55. *Sean $Q = Q_1 + Q_2$ y $Q' = Q'_1 + Q'_2$ dos formas cuadráticas no degeneradas. Si $Q \sim Q'$ y $Q_1 \sim Q'_1$ entonces $Q_2 \sim Q'_2$.*

Corolario 1.56. *Si Q es una forma cuadrática no degenerada entonces $Q \sim Q_1 + \cdots + Q_n + Q'$, donde $Q_1, \ldots, Q_n$ son no degeneradas y Q' representa al 0. Además, la descomposición es única salvo equivalencias.*

Formas Cuadráticas sobre Cuerpos Finitos

Sea $p \neq 2$ un primo y q una potencia de p. Como en secciones anteriores, denotemos por F_q al cuerpo con q elementos.

Teorema 1.57. *Se tiene que:*

1. *Cualquier forma cuadrática sobre F_q de rango mayor o igual que 2 representa a todos los elementos de F_q^*.*
2. *Cualquier forma cuadrática sobre F_q de rango mayor o igual que 3 representa a todos los elementos de F_q.*

Demostración. Sean $a, b, c \in F_q \setminus \{0\}$. Veamos que $ax^2 + by^2 = c$ tiene solución. Sean $X = \{$elementos de F_q de la forma
$ax^2, x \in F_q\}$ e $Y = \{$elementos de F_q de la forma $c - by^2, y \in F_q\}$. Se puede ver que cada uno de los conjuntos tiene $\frac{q+1}{2}$, por lo que, si fuesen disjuntos, F_q debería tener al menos $q + 1$ elementos, lo cual es contradictorio. En consecuencia $A \cap B \neq \emptyset$, por lo que la ecuación debe tener solución. □

Observación 1.58. Recordemos que ya hemos enunciado con anterioridad un resultado importante para las formas cuadráticas sobre cuerpos finitos, el Corolario 1.12, que afirma que toda forma cuadrática sobre un cuerpo finito con tres o más variables tiene un cero no trivial.

Teorema 1.59. *Dado $a \in F_q^*$ un elemento que no es un cuadrado, se cumple que cualquier forma cuadrática no degenerada de rango n sobre F_q es equivalente a $X_1^2 + \cdots + X_{n-1}^2 + X_n^2$ o a $X_1^2 + \cdots + X_{n-1}^2 + aX_n^2$, dependiendo de si el discriminante es o no un cuadrado.*

Observación 1.60. Se trabaja con el discriminante como un elemento de $\frac{F_q^*}{F_q^{*2}}$.

Capítulo 2

Los Números p-ádicos

El enunciado del Teorema de Hasse-Minkowski hace referencia a la resolubilidad de unas ciertas ecuaciones sobre los números p-ádicos, $\mathbb{Q}_p$ (donde p es un número primo). El objetivo de este capítulo es, por tanto, estudiar los números p-ádicos, que además poseen una elevada importancia en Álgebra y Teoría de Números. Los p-ádicos, tal y como se analizará con posterioridad, son (otra) extensión del cuerpo de los racionales, $\mathbb{Q}$.

Veremos que los p-ádicos son (otra) extensión del cuerpo de los racionales, $\mathbb{Q}$. Por ello, en primer lugar analizaremos su construcción a partir de los valores absolutos p-ádicos sobre $\mathbb{Q}$. A continuación veremos que son un cuerpo y probaremos algún resultado de utilidad sobre sus unidades y sus cuadrados. Para acabar, estudiaremos propiedades de los polinomios sobre los enteros p-ádicos y sus raíces y enunciaremos el resultado enunciado por Minkowski equivalente al Teorema de Hasse-Minkowski que mencionamos en la Introducción.

Para este capítulo se han seguido varias fuentes: fundamentalmente, [3], [4], [11] y [14], y en menor medida [5], [8], [9],[10] (esta únicamente para algún aspecto topológico), [12] y [15].

A modo de introducción incluimos las siguientes definiciones.

Definición 2.1. Sean p un entero primo y $x \in \mathbb{Z}^+$. Se denomina expansión p-ádica de x a la expresión $\sum_{i=0}^{n} a_i p^i$, donde $a_i \in \{0, 1, \ldots, p-1\}$ para todo i. Todo entero positivo admite una expansión p-ádica.

Observación 2.2. Los a_i de la definición anterior se pueden pensar como elementos de F_p.

Definición 2.3. Sean p un entero primo. Un entero $p$ádico es una expresión de la forma $\sum_{i=0}^{\infty} a_i p^i$, donde $a_i \in \{0, 1, \ldots, p-1\}$ para todo i. El conjunto de todos los enteros p-ádicos se denota por $\mathbb{Z}_p$.

Podemos extender las expresiones anteriores a series de la forma $\sum_{i=-m}^{\infty} a_i p^i$, donde $m \in \mathbb{N}$ y a_i como en las definiciones anteriores. Esto da lugar a la siguiente definición.

Definición 2.4. A las series de la forma $\sum_{i=-m}^{\infty} a_i p^i$, con $m \in \mathbb{N}$ y $a_i \in \{0, 1, \ldots, p-1\}$ se les denomina números p-ádicos. El conjunto de los números p-ádicos se denota por $\mathbb{Q}_p$.

Todo racional admite una expansión en forma de número p-ádico.

2.1. Valores absolutos sobre $\mathbb{Q}$

Como ya explicamos, esta primera parte trata sobre los valores absolutos sobre $\mathbb{Q}$, con el objetivo de estudiar, en particular, los valores absolutos p-ádicos que dan lugar a $\mathbb{Q}_p$. No obstante, las definiciones y propiedades generales de los valores absolutos serán vistas para un cuerpo arbitrario K.

Definición 2.5. Un valor absoluto sobre un cuerpo K es una aplicación $|\ |\colon \to \mathbb{R}^+ \cup \{0\}$ que cumple:

1. $|x| \geq 0$ para todo $x \in K$ y $|x| = 0 \iff x = 0$ (definida positiva).
2. $|xy| = |x||y|$ para todo $x, y \in K$.
3. $|x + y| \leq |x| + |y|$ para todo $x, y \in K$ (desigualdad triangular).

Además un valor absoluto se dirá no arquimediano si verifica

4. $|x + y| \leq \text{máx}\{|x|, |y|\}$ para cualesquiera $x, y \in K$.

La condición de ser valor absoluto no arquimediano implica la tercera condición (desigualdad triangular) de la definición general de valor absoluto.

Definición 2.6. Si K es un cuerpo y $|\ |$ un valor absoluto, una completación del cuerpo K es una extensión de dicho cuerpo en la que toda sucesión de Cauchy de elementos de K es convergente.

Observación 2.7. Si consideramos el valor absoluto usual definido en el cuerpo de los racionales $\mathbb{Q}$, $|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$, la completación de $\mathbb{Q}$ con dicho valor absoluto es $\mathbb{R}$. Este valor absoluto se suele denotar como $|\ |_\infty$. No obstante, este no es el único valor absoluto que podemos considerar en $\mathbb{Q}$. Tomando otro obtendremos otra posible completación de $\mathbb{Q}$ que será precisamente el cuerpo de los números p-ádicos $\mathbb{Q}_p$.

Dado un $x \in \mathbb{Z} \setminus \{0\}$ y un p primo sabemos que existen $n, v \in \mathbb{Z}$ únicos de forma que $x = p^v n$ y $\text{mcd}(p, n) = 1$. Gracias a ello construimos la siguiente definición.

Definición 2.8. Dado un primo p se llama valoración p-ádica en $\mathbb{Z}$ a la aplicación $v_p : \mathbb{Z}\setminus\{0\} \longrightarrow \mathbb{Z}$, donde para cada $x \in \mathbb{Z}$, $v_p(x)$ es el entero v que indicábamos en las líneas anteriores, es decir, el único entero v que verifica que $x = p^v n$, con n y p enteros coprimos. Es posible extender esta definición a $\mathbb{Q} \setminus \{0\}$ (que denotaremos por $\mathbb{Q}^*$). Como todo racional se puede escribir en forma de fracción irreducible $\frac{x}{y}$, $x \in \mathbb{Z}$ e $y \in \mathbb{N} \setminus \{0\}$, definimos $v_p(\frac{x}{y}) = v_p(x) - v_p(y)$. Por convenio $v_p(0) = +\infty$.

Proposición 2.9. *Sean $a, b \in \mathbb{Q}$. La valoración p-ádica verifica las siguientes propiedades:*

- $v_p(ab) = v_p(a) + v_p(b)$.
- $v_p(a + b) \geq \text{mín}\{v_p(a), v_p(b)\}$.

Demostración. Si $a = 0$ o $b = 0$ es obvio. Supongamos $a \neq 0$ y $b \neq 0$.

- Si a y b son enteros se concluye directamente por definición. Si $a = \frac{x_1}{x_2}, b = \frac{y_1}{y_2}$ entonces $ab = \frac{x_1 y_1}{x_2 y_2}$. Por la Definición 2.8 $v_p(ab) = v_p(x_1 y_1) - v_p(x_2 y_2)$. Teniendo en cuenta que $x_1 y_1$ y $x_2 y_2$ son enteros y el enunciado se cumple, $v_p(ab) = v_p(x_1) + v_p(y_1) - v_p(x_2) - v_p(y_2) = v_p(x_1) - v_p(x_2) + v_p(y_1) - v_p(y_2) = v_p(a) + v_p(b)$.
- De nuevo, el caso entero se deduce fácilmente al factorizar teniendo en cuenta la mayor potencia de p que divide a a y b. Si $a = \frac{x_1}{x_2}, b = \frac{y_1}{y_2}$, entonces $a + b = \frac{x_1 y_2 + x_2 y_1}{x_2 y_2}$, luego $v_p(a + b) = v_p(\frac{x_1 y_2 + x_2 y_1}{x_2 y_2}) = v_p(x_1 y_2 + x_2 y_1) - v_p(x_2 y_2)$. Por un lado $v_p(x_1 y_2 + x_2 y_1) \geq \text{mín}\{v_p(x_1 y_2), v_p(x_2 y_1)\}$. Supongamos que $\text{mín}\{v_p(x_1 y_2), v_p(x_2 y_1)\} = v_p(x_1 y_2) = v_p(x_1) + v_p(y_2)$. Fijémonos en que entonces $v_p(a) \leq v_p(b)$, ya que como $\text{mín}\{v_p(x_1 y_2), v_p(x_2 y_1)\} = v_p(x_1 y_2) = v_p(x_1) + v_p(y_2)$ entonces $v_p(x_1) + v_p(y_2) \leq v_p(x_2) + v_p(y_1)$, lo cual equivale a que $v_p(x_1) - v_p(x_2) \leq v_p(y_1) - v_p(y_2)$, es decir, $v_p(a) \leq v_p(b)$. En ese caso, $v_p(x_1 y_2 + x_2 y_1) - v_p(x_2 y_2) \geq v_p(x_1 y_2) - v_p(x_2 y_2) = v_p(x_1) + v_p(y_2) - v_p(x_2) - v_p(y_2) = v_p(x_1) - v_p(x_2) = v_p(a) = \text{mín}\{v_p(a), v_p(b)\}$.

□

A continuación revisamos un concepto fundamental de Álgebra que tiene relación con las propiedades de la valoración p-ádicas.

Definición 2.10. Un anillo A se dice que es un anillo de valoración discreta (AVD) si es un dominio de ideales principales con un único ideal primo no nulo $\mathfrak{m}$ que será maximal. El cuerpo definido al realizar el cociente $A/\mathfrak{m}$ se denomina cuerpo de residuos de A.

Observación 2.11.

- Dado que hay un único ideal maximal (es decir, A es un anillo local) el conjunto $A \setminus \mathfrak{m}$ es un grupo multiplicativo que está formado por las unidades del anillo. Además, como el ideal es principal, existe un elemento $\pi \in A$ irreducible tal que $\mathfrak{m} = (\pi)$. Este elemento π se denomina uniformizante.
- Los ideales no nulos del anillo A serán de la forma (π^n) y todos los elementos no nulos del anillo se podrán expresar de la forma $u\pi^n$ con u una unidad y n un entero no negativo. Si $x = u\pi^n$ el entero n se denomina valoración del elemento x y se denota por $v(x)$.
- Sea K es el cuerpo de fracciones del anillo y $K^* = K \setminus \{0\}$. Si $x = \frac{a}{b}$ también podemos escribir $x = u\pi^n$, pero en este caso n podrá ser entero, positivo, negativo o nulo. Como en el caso anterior se escribirá $v(x) = n$.

Proposición 2.12 ([15])**.** *La aplicación valoración $v : (K^*, \cdot) \to \mathbb{Z}$ es un homomorfismo sobreyectivo y verifica que $v(x + y) \geq \text{ínf}\{v(x), v(y)\}$.*

Se suele tomar por convenio $v(0) = \infty$.

Proposición 2.13 ([15])**.** *Si K es un cuerpo y $v : K^* \to \mathbb{Z}$ es un homomorfismo que verifica las propiedades de la proposición anterior, entonces el conjunto $\{x \in K$ tales que $v(x) \geq 0\} \cup \{0\}$ es un anillo de valoración discreta con valoración asociada v.*

Veamos dos de ejemplos importantes de anillos de valoración.

Ejemplo 2.14.

1. Si p es un primo y $\mathbb{Z}_{(p)}$ es el subconjunto de $\mathbb{Q}$ formado por las fracciones cuyo denominador no es divisible por p. El cuerpo de residuos es precisamente el cuerpo finito con p elementos F_p. La valoración asociada, si $x \in \mathbb{Z}$, $v_p(x)$ es el exponente del primo p en la factorización en primos de x. Si $\frac{x}{y} \in \mathbb{Q}$ $v_p(\frac{x}{y}) = v_p(x) - v_p(y)$.
2. Si K es un cuerpo y $K((T))$ denota al cuerpo de las series de potencias en una variable sobre K, para una serie no nula $f(T) = \sum_{n \leq n_0} a_n T^n,\ a_n \in K, a_{n_0} \neq 0$ se define la valoración $v(f) = n_0$. Así obtenemos un anillo de valoración discreta cuyo cuerpo de residuos es K.

Observación 2.15. La valoración p-ádica verifica las propiedades necesarias para ser valoración de un anillo de valoración discreta, tal y como prueban los lemas vistos con anterioridad. Cuando comprobemos que $\mathbb{Q}_p$ es un cuerpo podremos aplicar la Proposición 2.13 y deducir que $\mathbb{Z}_p$ es un anillo de valoración discreta.

Continuando ahora con las propiedades de los valores absolutos sobre un cuerpo, y teniendo en cuenta las propiedades básicas, definimos a continuación, en base a la valoración p-ádica, el valor absoluto p-ádico sobre el cuerpo $\mathbb{Q}$.

Definición 2.16. Si $x \in \mathbb{Q}$ se define el valor absoluto p-ádico de x como $|x|_p = p^{-v_p(x)}$ si $x \neq 0$ y $|0|_p = 0$.

Observación 2.17. Fijémonos en que el valor absoluto p-ádico de un número será pequeño (respectivamente, grande) si su valoración p-ádica es grande (respectivamente, pequeña), es decir, si es "muy divisible" (respectivamente, "poco divisible") por p.

Proposición 2.18. *El valor absoluto p-ádico $|\cdot|_p$ verifica las propiedades para ser un valor absoluto sobre un cuerpo ($\mathbb{Q}$). Además, se trata de un valor absoluto no arquimediano.*

Demostración. Veamos que verifica las cuatro propiedades que aparecen en la definición anterior correspondiente para ser valor absoluto de tipo no arquimediano:

1. $|0|_p = 0$ por definición. Por otro lado, si $x \neq 0$, $|x|_p = p^{-v_p(x)} > 0$.

2. Por la Proposición 2.9, $|xx'|_p = p^{-v_p(xx')} = p^{-v_p(x)}p^{-v_p(x')} = |x|_p|x'|_p$.

3. De nuevo, por la Proposición 2.9, $|x + x'|_p = p^{-v_p(x+x')}$.

   Ahora bien, $v_p(a + b) \geq \min\{v_p(a), v_p(b)\} \implies -v_p(a + b) \leq -\min\{v_p(a), v_p(b)\}$. En consecuencia, $p^{-v_p(x+x')} \leq p^{-\min\{v_p(x),v_p(x')\}} \leq p^{-\min\{v_p(x),v_p(x')\}} + p^{-\max\{v_p(x),v_p(x')\}} = |x|_p + |x'|_p$.

4. $|x+x'|_p = p^{-v_p(x+x')} \leq p^{-\min\{v_p(x),v_p(x')\}} = \min\{p^{-v_p(x)}, p^{-v_p(x')}\} \leq \max\{p^{-v_p(x)}, p^{-v_p(x')}\} \leq \max\{|x|_p + |x'|_p\}$.

□

Observación 2.19. Las definiciones anteriores contribuyen a comprender mejor la definición de los números p-ádicos: los racionales p-ádicos, $\mathbb{Q}_p$, consisten en todos los números de la forma $x = \sum_{n=-m} a_n p^n$, $0 \leq a_n \leq p - 1$. $-m$ es justamente $v_p(x)$. Dos racionales p-ádicos x, y serán iguales si, y solo si, $|x - y|_p = 0$.

Gracias a los conceptos vistos hasta el momento sobre valores absolutos, podemos dar otro punto de vista para los enteros p-ádicos.

Definición 2.20. Los enteros p-ádicos, $\mathbb{Z}_p$, pueden definirse como el conjunto $\mathbb{Z}_p = \{x \in \mathbb{Q}_p, |x|_p \leq 1\}$ (lo cual equivale a que $x \in \mathbb{Q}_p$ y que $x = \sum_{n=0} a_n p^n$).

Veamos ahora algunos resultados previos sobre valores absolutos en cuerpos para poder enunciar y demostrar el Teorema de Ostrowski, que se trata de un resultado importante para los valores absolutos p-ádicos.

Lema 2.21. *Si K es un cuerpo y consideramos un valor absoluto $|\ |$ sobre él, entonces equivalen:*

1. *$|\ |$ es no arquimediano.*
2. *$|x+1| \leq \text{máx}\{|x|, 1\}$, $x \in K$.*

Demostración. La condición necesaria es sencilla: un valor absoluto es no arquimediano si verifica $|x+y| \leq \text{máx}\{|x|, |y|\}$. Por tanto, si el valor absoluto es no arquimediano tomando $y = 1$ obtenemos el resultado deseado. En cuanto a la condición suficiente, si $x = 0$ es trivial. Supongamos que $x \neq 0$ entonces $x = \frac{x_1}{x_2}$. En ese caso $|\frac{x_1}{x_2} + 1| \leq \text{máx}\{\frac{x_1}{x_2}, 1\}$. Multiplicando la expresión por x_2 concluimos que el valor absoluto debe ser no arquimediano. □

Teorema 2.22. *Si f es la aplicación definida previamente en el capítulo 1 para definir la característica de un cuerpo y $f(\mathbb{Z})$ es la imagen de $\mathbb{Z}$ por dicha aplicación, un valor absoluto $|\ |$ será no arquimediano si, y solo si, $|y| \leq 1$, $y \in f(\mathbb{Z})$. En particular, un valor absoluto en $\mathbb{Q}$ será no arquimediano si, y solo si, $|y| \leq 1$, para todo $y \in \mathbb{Z}$.*

Demostración. Veamos las dos implicaciones:

- "$\Longrightarrow$" $|\pm 1| = 1$. Si el valor absoluto es no arquimediano, entonces dado $y \in f(\mathbb{Z})$, $|y \pm 1| \leq \text{máx}\{|y|, |1|\}$. Por inducción se concluye entonces que $|y| \leq 1$, $y \in f(\mathbb{Z})$.
- "$\Longleftarrow$ " Sea $y \in f(\mathbb{Z}), |y| \leq 1$. Por el Lema 2.21 que el valor absoluto sea arquimediano equivale a comprobar que $|y+1| \leq \text{máx}\{|y|, 1\}$. Consideremos un entero positivo n. $|y+1|^n \leq |\sum_{i=0}^{n} \binom{n}{i}\ y^i| \leq |\sum_{i=0}^{n} \binom{n}{i}\ |y^i|$, por la desigualdad triangular.

  $\binom{n}{i}$ es un entero, luego $|\binom{n}{i}| \leq 1$, por lo que $|y+1|^n \leq \sum_{i=0}^{n} |y^i|$. Ahora bien, $|y+1|^n \leq \sum_{i=0}^{n} |y^i| \leq (n+1)\,\text{máx}\{1, |y|^n\}$.

Tomando raíces n-ésimas a ambos lados de la desigualdad obtenemos que

$$|y+1| \leq \sqrt[n]{n+1}\,\text{máx}\{1,|y|\}$$

Como esto se verifica para cualquier entero positivo, tomando límites cuando $n \to \infty$ obtenemos que $|y+1| \leq \text{máx}\{1,|y|\}$

□

Corolario 2.23. *Un valor absoluto sobre un cuerpo K es no arquimediano $\iff 1 = \sup\{|n|, n \in \mathbb{Z}\}$.*

Definición 2.24. Si K es un cuerpo y se consideran en él dos valores absolutos sobre él, se dice que dichos valores absolutos son equivalentes si generan la misma topología.

Lema 2.25 ([3])**.** *Dos valores absolutos $|\ |$ y $|\ |'$ sobre un cuerpo K son equivalentes si, y solo si, existe un número real positivo α que cumpla que $|x| = |x|'^{\alpha}$.*

Proposición 2.26. *Sea $a \in \mathbb{R}, a > 1$. Entonces $|x| = a^{-v_p(x)}$ define un valor absoluto no arquimediano equivalente al valor absoluto p-ádico $|\ |_p$.*

Demostración. Para ver que es no arquimediano basta utilizar el Teorema 2.22 y probar que $|x| \leq 1$ para cualquier racional x. Como $a > 1$, $\frac{1}{a} < 1$. En consecuencia, $a^{-v_p(x)} = \frac{1}{a^{v_p(x)}} < 1$, luego el valor absoluto es no arquimediano. Para ver que es equivalente utilizamos el Lema 2.25 y demostraremos que existe un número real positivo α que cumpla que $|x|_p = |x|^{\alpha}$. En efecto, basta tomar α de forma que $a^{\alpha} = p$ ya que entonces $|x|_p = p^{-v_p(x)} = a^{-a\alpha v_p(x)} = |x|^{\alpha}$. □

Definición 2.27. El valor absoluto trivial en $\mathbb{Q}$ es aquel en el que $|x| = 1$ si $x \neq 0$ y $|0| = 0$.

Ahora sí, enunciamos y demostramos el Teorema de Ostrowski. La importancia de este resultado reside en que caracteriza los valores absolutos que se puedan considerar sobre $\mathbb{Q}$, probando que un valor absoluto arquimediano sobre los racionales equivale al valor absoluto "usual", mientras que si es no arquimediano será equivalente a algún valor absoluto p-ádico.

Teorema 2.28 (Ostrowski)**.** *Si $|\ |$ es un valor absoluto no trivial sobre el cuerpo $\mathbb{Q}$ entonces dicho valor absoluto es equivalente a algún $|\ |_p$ con p primo o infinito. En particular, se verifica que:*

1. *Si el valor absoluto $|\ |$ es arquimediano entonces es equivalente al valor absoluto $|\ |_\infty$.*
2. *Si el valor absoluto $|\ |$ es no arquimediano entonces es equivalente a un valor absoluto $|\ |_p$ para algún primo p.*

Demostración. Comprobemos ambas afirmaciones.

1. Sean n y m enteros mayores que 1. Podemos escribir $m = \sum_{i=0}^{k} a_i n^k$ con $0 \leq a_i < n$. Por tanto,
$$|m| < n \cdot (1 + |n| + \cdots + |n|^k) \leq n \cdot (k+1) \cdot \text{máx}\{1, |n|^k\}.$$
Por otro lado, $m \geq n^k$, luego $\log m \geq k \cdot \log n$ y así $k \leq \frac{\log m}{\log n}$. Sustituyendo en lo anterior tenemos que
$$|m| < n \cdot \Big(\frac{\log m}{\log n} + 1\Big) \cdot \text{máx}\{1, |n|^{\frac{\log m}{\log n}}\}.$$
Esto permite deducir que si l es un entero positivo
$$|m^l| < n \cdot \Big(\frac{l \cdot \log m}{\log n} + 1\Big) \cdot \text{máx}\{1, |n|^{\frac{l \cdot \log m}{\log n}}\}.$$
La desigualdad anterior equivale a
$$|m| < n \cdot \Big(\frac{l \cdot \log m}{\log n} + 1\Big)^{\frac{1}{l}} \cdot \text{máx}\{1, |n|^{\frac{\log m}{\log n}}\}.$$
Tomando el límite cuando l tiende a infinito en la desigualdad anterior llegamos a que $|m| \leq \text{máx}\{1, |n|^{\frac{\log m}{\log n}}\}$. Dado que el valor absoluto es arquimediano existirá un m_0 entero tal que $|m_0| > 1$. Tomando $m = m_0$, tenemos que $|m| \leq |n|^{\frac{\log m}{\log n}}$, es decir $|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{n}}$. Por simetría podemos concluir que $|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{n}}$. Por tanto, $\frac{\log |m|}{\log m} = \frac{\log |n|}{\log n} = r$. Se cumple que $|n| = n^r$, es decir $|n| = |n|_\infty^r$, lo que permite probar gracias al Lema 2.25 que los valores absolutos son equivalentes.

2. Por el Teorema 2.22, dado que $|\ |$ es no arquimediano entonces $|n| \leq 1$, para todo $n \in \mathbb{Z}$. Si $|n| = 1$ para cualquier n entero entonces estaríamos ante el valor absoluto trivial. Por tanto, el conjunto $X = \{n \in \mathbb{Z} \text{ tales que } |n| < 1\}$ es no vacío. Veamos que X es un ideal: como el valor absoluto es no arquimediano, si $x_1, x_2 \in X$ $|x_1 + x_2| \leq \text{máx}\{|x_1|, |x_2|\} < 1$. Además, si $x \in X$ y $n \in \mathbb{Z}$ entonces $|nx| = |n||x| < 1$. Además, dicho ideal es primo: si $xy \in X$ entonces $|xy| < 1$. Como $|x||y| < 1$ $|x|$ o $|y|$, al menos uno de ellos, debe ser menor que 1 (y por tanto está en X). Además, el menor entero p que pertenezca al conjunto X será primo, ya que si $p = p_1 \cdot p_2$ (es decir, p_1, p_2 enteros menores que p) entonces $|p| = |p_1| \cdot |p_2| < 1$, luego $p_1 \in X$ o $p_2 \in X$, lo cual sería contradictorio con que p fuese el mínimo. En consecuencia $X = (p)$. Sea $|p| = \alpha$. Dado $q \in \mathbb{Q}$, existen $a, b \in \mathbb{Z} \setminus X$ y k entero de forma que $q = p^k \frac{a}{b}$. Por definición, $|a| = |b| = 1$. Por tanto, $|q| = \alpha^k = (\alpha^{-1})^{-k} = (\alpha^{-1})^{-v_p(r)}$, y α^{-1} es un real mayor que 1, por lo que aplicando el Lema 2.25 y la Proposición 2.26 concluimos el resultado.

□

Teorema 2.29 (Fórmula del Producto)**.** *Sea $x \in \mathbb{Q}^*$. Entonces* $\prod_{p \leq \infty} |x|_p = 1$.

Demostración. Es suficiente con estudiar el caso para un entero positivo ya que el resto de casos se deducen de él. Sea $x \in \mathbb{Z}^+$. Factorizando x en primos se tiene que $x = \prod_{i=1}^{n} p_i^{n_i}$. En ese caso tendremos:

$$\begin{cases} |x|_\infty = \prod_{i=1}^{n} p_i^{n_i}, & \\ |x|_{p_i} = p_i^{-n_i}, & i = 1, \ldots, n, \\ |x|_q = 1, & \text{si } q \neq p_i \ i = 1, \ldots, n. \end{cases}$$

□

Para finalizar esta sección vamos a ver que $\mathbb{Q}$ no es completo respecto del valor absoluto p-ádico y que los números p-ádicos son una completación.

Lema 2.30 ([3])**.** *Una sucesión de números racionales $\{x_n\}$ es de Cauchy respecto de un valor absoluto no arquimediano $|\ |$ si, y solo si,* $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

Teorema 2.31 ([3])**.** *$\mathbb{Q}$ no es completo respecto de ninguno de los valores absolutos $|\ |_p$ con p primo, ni para $|\ |_\infty$.*

Como $\mathbb{Q}$ no es completo, para construir una completación hay que "añadir" todos los límites de todas las sucesiones de Cauchy. Para ello nos serán útiles los siguientes conceptos.

Definición 2.32. Sea $|\ |_p$ un valor absoluto no arquimediano en $\mathbb{Q}$. Se denota por $\mathcal{C}$ o $\mathcal{C}_p$ al conjunto de sucesiones de Cauchy (respecto de $|\ |_p$) de $\mathbb{Q}$.

Observación 2.33. Definiendo las operaciones $\{x_n\} + \{y_n\} = \{x_n + y_n\}$ y $\{x_n\} \cdot \{y_n\} = \{x_n \cdot y_n\}$ se puede probar que $\mathcal{C}$ es un anillo conmutativo que no es un cuerpo.

Una vez definido esto, tiene sentido considerar que dos sucesiones de Cauchy con el mismo límite sean, en cierto modo, "equivalentes", por lo que cocientaremos el anillo respecto de un ideal para trabajar con las clases de equivalencia, siguiendo la idea que comentábamos previamente.

Definición 2.34. Se define $\mathcal{N} \subset \mathcal{C}_p$ como el ideal $\mathcal{N}$ de $\mathcal{C}_p$, $\mathcal{N} = \{\{x_n\} : \lim_{n\to\infty} |x_n|_p = 0\}$.

Proposición 2.35 ([3])**.** *$\mathcal{N}$ es un ideal maximal de $\mathcal{C}$.*

Con todo esto podemos redefinir el cuerpo de los números p-ádicos.

Definición 2.36. Se define el cuerpo de los números p-ádicos como $\mathbb{Q}_p = \mathcal{C}_p/\mathcal{N}$.

Observación 2.37. Definimos la inclusión de cuerpos $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ definiendo la clase de equivalencia de un racional como la sucesión constante con todos los términos iguales a ese racional.

Para deducir que considerando el valor absoluto $|\ |_p$ el cuerpo de los números p-ádicos es una completación de $\mathbb{Q}$ hay que comprobar que $|\ |_p$ extiende $\mathbb{Q}$ a $\mathbb{Q}_p$, que $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ y que $\mathbb{Q}_p$ es completo respecto a $|\ |_p$. Los siguientes resultados tienen ese objetivo.

Lema 2.38 ([3])**.** *Sea $\{x_n\} \subset \mathcal{C} \setminus \mathcal{N}$. Entonces la sucesión es estacionaria, es decir, existe un M de forma que si $n, m \geq M$ entonces $|x_m|_p = |x_n|_p$.*

Definición 2.39. Sea $\lambda \in \mathbb{Q}_p$. Si $\{x_n\}$ es una sucesión de Cauchy que representa a λ entonces se define

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

Está bien definido ya que si tomásemos otra sucesión que representase a λ el límite en infinito de la resta de ambas sería 0, con lo que se encontrarían en la misma clase de equivalencia.

Proposición 2.40. *La aplicación $|\ |_p : \mathbb{Q}_p \to \mathbb{R}^+ \cup \{0\}$ que lleva a cada $\lambda \in \mathbb{Q}_p$ en $|\lambda|_p$ define un valor absoluto no arquimediano.*

Lema 2.41 ([3])**.** *Si $|\ |_p$ denota la aplicación indicada en la proposición anterior, la imagen de $\mathbb{Q}_p$ por esa aplicación es la misma que la de $\mathbb{Q}$. Es decir, para todo $\lambda \in \mathbb{Q}_p \setminus \{0\}$ existe un entero n tal que $|\lambda|_p = p^{-n}$.*

Teorema 2.42 ([3])**.** *La imagen de $\mathbb{Q}$ por la aplicación inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ es un subconjunto denso en $\mathbb{Q}_p$.*

Teorema 2.43 ([3])**.** *$\mathbb{Q}_p$ es completo respecto de $|\ |_p$.*

Estos resultados son los que permiten concluir que el cuerpo $\mathbb{Q}_p$ (para un primo p) es una completación de $\mathbb{Q}$ considerando el valor absoluto p-ádico $|\ |_p$.

Ejemplo 2.44. $\mathbb{Z}_p$ es un anillo local con ideal maximal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$, y dicho ideal es principal. Si consideramos $\mathbb{Z}_p$ como subconjunto del cuerpo $\mathbb{Q}_p$ y tomamos como aplicación v la valoración p-ádica podemos aplicar la Proposición 2.13 y concluir, como ya habíamos indicado con anterioridad, que $\mathbb{Z}_p$ es un anillo de valoración discreta. Su ideal maximal es $p\mathbb{Z}_p$ y su cuerpo de residuos es el cuerpo finito de p elementos, F_p.

Observación 2.45. Teniendo en cuenta el Ejemplo 2.44, el conjunto de unidades de $\mathbb{Z}_p$ es $\mathbb{Z}_p \setminus p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p = 1\}$.

2.2. El cuerpo de los números p-ádicos

Comenzaremos reescribiendo el Lema 2.41, extendiendo la valoración p-ádica para todo el cuerpo $\mathbb{Q}_p$ de la siguiente forma:

Lema 2.46. *Para todo $\lambda \in \mathbb{Q}_p \setminus \{0\}$ existe un entero $v_p(\lambda)$ tal que $|\lambda|_p = p^{-v_p(\lambda)}$. Para extenderlo a todo $\mathbb{Q}_p$ tomamos $v_p(0) = \infty$*

A continuación se ven dos definiciones de conceptos algebraicos que serán de utilidad próximamente.

Definición 2.47. Una sucesión $A \xrightarrow{f} B \xrightarrow{g} C$ se dice exacta si $\ker f = \operatorname{Im} g$

Definición 2.48. Dado un primo p se dice que una sucesión $\{x_n\}_{n\geq 1}$ es coherente si verifica que $x_{n+1} \equiv x_n \,(\mathrm{mód}\, p^n)$

Proposición 2.49 ([3])**.** *El anillo de los enteros p-ádicos es un anillo local con ideal maximal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Dicho ideal es principal. Además, se verifican:*

1. $\mathbb{Q}_p \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.
2. *La aplicación inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ posee imagen densa: dados un $x \in \mathbb{Z}_p$ y un entero $n \geq 1$ existe un único entero no negativo $\alpha \leq p^{n-1}$ tal que $|x - \alpha|_p \leq p^{n-1}$.*
3. *Para todo $x \in \mathbb{Z}_p$ existe una sucesión de Cauchy $\{x_n\}$ convergente a x que cumple:*
   a) *x_n verifica que $0 \leq x_n \leq p^{n-1}$.*
   b) *Si $n \geq 1$ entonces $x_{n+1} \equiv x_n \,(\mathrm{mód}\, p^n)$ (la sucesión es coherente).*

Observación 2.50. Ya hemos visto que $\mathbb{Z}_p$ es un anillo de valoración discreta, en particular es un anillo local con ideal maximal único. Además, todo elemento de $\mathbb{Z}_p$ que no esté en el ideal maximal debe ser invertible. Por el Lema 2.41, si $|x|_p < 1$ entonces $|x|_p \leq \frac{1}{p}$. $|p|_p = \frac{1}{p}$, y entonces $|\frac{x}{p}|_p \leq 1$, por lo que $x \in p\mathbb{Z}_p$. Como el que buscamos es un ideal maximal, y acabamos de comprobar que este debe estar contenido en $p\mathbb{Z}_p$, el uniformizante de este anillo de valoración será precisamente p.

Corolario 2.51. $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$*: para todo $x \in \mathbb{Q}_p$ existe un entero no negativo n tal que $p^n x \in \mathbb{Z}_p$.*

Corolario 2.52. *Sea n un entero positivo. Se tiene que la sucesión*

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varphi_n} \mathbb{Z}/p^n\mathbb{Z} \to 0$$

es exacta, donde la aplicación $\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p$ lleva a cada $x \in \mathbb{Z}_p$ en $p^n x$, y la aplicación φ_n lleva a cada $x \in \mathbb{Z}_p$ en su "componente" n-ésima; es decir, lleva a cada $x \in \mathbb{Z}_p$ en el elemento x_n de la sucesión convergente a x definida en el tercer apartado de la Proposición 2.49. En particular, se tiene que $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Observación 2.53. Hemos visto con anterioridad la definición de sucesión exacta para el caso más sencillo posible, el formado por tres objetos. En el caso del corolario que precede a esta observación hay cinco, por lo que en dicho resultado que la sucesión sea exacta significa que:

- La aplicación $\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p$ es inyectiva, ya que su núcleo coincide con la imagen de la aplicación $0 \to \mathbb{Z}_p$.
- La imagen de la aplicación $\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p$ coincide con el núcleo de $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$, es decir, el núcleo de $\mathbb{Z}_p \xrightarrow{\varphi_n} \mathbb{Z}/p^n\mathbb{Z}$ es $p^n\mathbb{Z}_p$.
- El núcleo de $\mathbb{Z}/p^n\mathbb{Z} \to 0$, que es $\mathbb{Z}/p^n\mathbb{Z}$, coincide con la imagen de $\mathbb{Z}_p \xrightarrow{\varphi_n} \mathbb{Z}/p^n\mathbb{Z}$. Por tanto, la aplicación $\mathbb{Z}_p \xrightarrow{\varphi_n} \mathbb{Z}/p^n\mathbb{Z}$ sobreyectiva.

Vamos a continuar viendo propiedades con el objetivo de obtener más información sobre los racionales p-ádicos.
Ya vimos en la Proposición 2.49 que dado un $x \in \mathbb{Z}_p$ existe una sucesión de Cauchy $\{x_n\}$ convergente a x que cumple que $0 \leq x_n \leq p^{n-1}$ y que si $n \geq 1$ entonces $x_{n+1} \equiv x_n \,(\text{mód}\, p^n)$ (es coherente).
Dado n entero positivo, sea $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Podemos considerar la aplicación $\phi_n : A_n \to A_{n-1}$, $a \,(\text{mód}\, p^n) \longmapsto a \,(\text{mód}\, p^{n-1})$. Esta aplicación es un homomorfismo sobreyectivo de anillos cuyo núcleo es $p^{n-1}A_n$.
Ahora, si $\{\alpha_n\}_{n\in\mathbb{N}}$ es una sucesión de Cauchy convergente a un $x \in \mathbb{Z}_p$, para un n arbitrario podemos considerar de nuevo la "proyección" $\varphi_n : \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$, donde $\varphi_n(x) = \alpha_n \,(\text{mód}\, p^n)$.

Proposición 2.54 ([3])**.** *Sean φ_n y A_n las aplicaciones y los conjuntos definidos previamente, respectivamente. Podemos definir la aplicación inclusión $\varphi : \mathbb{Z}_p \hookrightarrow \prod_{n\geq 1} A_n$, que identifica a $\mathbb{Z}_p$ como anillo con una topología con el subanillo cerrado de $\prod_{n\geq 1} A_n$ formado por las sucesiones coherentes $\{x_n\}$ que cumplen que $\phi(x_n) = x_{n+1}$ para cualquier $n \geq 1$ (las operaciones usuales se pueden definir coordenada a coordenada).*

Observación 2.55. El límite del sistema proyectivo (A_n, ϕ_n) cuando n tiende a infinito se define como

$$\varprojlim(A_n, \phi_n) = \{\{x_n\}, x_n \in A_n : \phi(x_{n+1}) = \phi(x_n), n \geq 1\}$$

es decir, $x_{n+1} \equiv x_n \,(\text{mód}\, p^n)$. Se denomina límite proyectivo porque los elementos de los que calculamos el límite son cocientes (proyecciones) sucesivos.

Definición 2.56. Si consideramos los pares (A_n, ϕ_n) definidos ya con anterioridad, el anillo de enteros p-ádicos es el límite del sistema proyectivo (A_n, ϕ_n), es decir, $\mathbb{Z}_p = \varprojlim(A_n, \phi_n)$.

Lema 2.57 (Teorema de Tychonoff, [10])**.** *Un producto arbitrario de espacios topológicos compactos es compacto en la topología producto.*

Observación 2.58. Como hemos escrito antes, podemos considerar $\mathbb{Z}_p$ como subanillo de $\prod_{n\geq 1} A_n$. Si dotamos a los A_n de la topología discreta las aplicaciones φ_n y ϕ_n serán continuas. Si además dotamos a $\prod_{n\geq 1} A_n$ de la topología producto, entonces $\mathbb{Z}_p$ hereda una topología que lo convierte en un espacio compacto, por ser un espacio cerrado contenido en un producto de espacios compactos, que es compacto por el Lema 2.57.

El siguiente resultado nos proporciona condiciones y propiedades sobre los elementos invertibles de $\mathbb{Z}_p$.

Proposición 2.59. *Se verifican:*

1. *Para un elemento de $\mathbb{Z}_p$ (o equivalentemente, de A_n), ser invertible es equivale a no ser divisible por p.*

2. *Si U denota al grupo de elementos invertibles de $\mathbb{Z}_p$, todo elemento no nulo de $\mathbb{Z}_p$ se puede escribir de forma única como up^m, con $u \in U$ y m un entero no negativo. Es decir, $\mathbb{Z}_p$ es un dominio de factorización única (DFU) cuyo único elemento primo e irreducible es p. Los elementos de U se denominan unidades p-ádicas.*

Demostración. Comprobemos ambas afirmaciones:

1. Si $x \in \mathbb{Z}_p$ es invertible, entonces ya hemos visto que $|x|_p = 1$, es decir $1 = p^{-v_p(x)}$, por lo que $v_p(x) = 0$ y x no es divisible por p. La otra implicación basta probarla para A_n y se deducirá para $\mathbb{Z}_p$. Sea $x \in A_n \setminus pA_n$ ($x \in A_n$ no divisible por p), entonces la imagen en $A_1 = F_p$ (cuerpo finito con p elementos) es distinta de 0. Es decir, existen $y, z \in A_n$ de forma que $xy = 1 - pz$. En ese caso, $xy(1 + pz + \cdots + p^{n-1}z^{n-1}) = (1 - pz)(1 + pz + \cdots + p^{n-1}z^{n-1}) = 1 - p^n z^n = 1$, por lo que x es, en efecto, invertible.

2. Si $x \in \mathbb{Z}_p$ es no nulo, entonces existe un entero m suficientemente grande tal que $x = p^m u$, con u no divisible por p (es decir, por el apartado anterior, u es invertible, $u \in U$). La unicidad es obvia.

□

Observación 2.60. El entero m que aparece explicado en la proposición anterior es precisamente la valoración p-ádica del elemento x, que ya hemos detallado anteriormente.

Proposición 2.61 ([14])**.** *En $\mathbb{Z}_p$ podemos construir una topología definiendo la distancia $d(x, y) = e^{-v_p(x-y)}$. El anillo $\mathbb{Z}_p$ es un espacio métrico completo en el que $\mathbb{Z}$ es denso.*

Observación 2.62. En la topología construida en la proposición anterior, dado que hemos definido $v(0) = \infty$, los ideales $p^n\mathbb{Z}_p$ forman una base de entornos de 0 ($x \in p^n\mathbb{Z}_p \implies v(x) \geq n$).

Con todo lo que hemos visto podemos deducir que todo elemento x no nulo de $\mathbb{Q}_p$ (es decir, elemento de $\mathbb{Q}_p^*$) se puede escribir como $x = p^n u$, con $n \in \mathbb{Z}$ y $u \in U$ (n sería, de nuevo, la valoración p-ádica).
La siguiente proposición es similar a la última enunciada pero para $\mathbb{Q}_p$. Antes recordaremos la definición de espacio localmente compacto.

Definición 2.63. Un espacio topológico X se dice localmente compacto para cada punto $x \in X$ existe un conjunto compacto C_x que contiene a un entorno de x.

Proposición 2.64 ([14])**.** *Con la topología definida en la Proposición 2.61, el cuerpo $\mathbb{Q}_p$ es localmente compacto y contiene a $\mathbb{Z}_p$ como (subanillo) abierto. Además, con esta topología $\mathbb{Q}$ es denso en $\mathbb{Q}_p$.*

Volvemos ahora a la Proposición 2.59. En este resultado estudiábamos elementos invertibles de $\mathbb{Z}_p$. Desarrollaremos un poco más la teoría relativa a ellos a continuación, antes de pasar a un breve estudio de los cuadrados de $\mathbb{Q}_p$ y a la última sección sobre los polinomios en $\mathbb{Z}_p$.

Definición 2.65. Sea U el grupo de unidades de $\mathbb{Z}_p$. Para cada n entero positivo $U_n = 1 + p^n\mathbb{Z}_p$. Es posible identificar el cociente U/U_1 con el grupo multiplicativo F_p^* por ser este último cíclico con $p - 1$ elementos.

Observación 2.66.

- Los U_n forman una sucesión de grupos abiertos de U y $U = \varprojlim U/U_n$.
- Para cada n la aplicación $(1 + p^n x) \hookrightarrow (x \text{ módulo } p)$ proporciona un isomorfismo entre U_n/U_{n+1} y $\mathbb{Z}/p\mathbb{Z}$. Por inducción en n podemos deducir que el cociente U_1/U_n posee orden p^{n-1}.

Lema 2.67 ([14])**.** *Sea $0 \to A \to C \to B \to 0$ una sucesión exacta de grupos conmutativos, siendo A y B grupos finitos de orden a y b, respectivamente, con a y b coprimos entre sí. Sea $B' = \{x \in C : bx = 0\}$. Entonces $C = A \oplus B'$. Además, B' es el único subgrupo de C isomorfo a B.*

Continuando con la misma notación utilizada en esta sección enunciamos y probamos la siguiente proposición.

Proposición 2.68. *Si $V = \{x \in U : x^{p-1} = 1\}$, entonces V es el único subgrupo de U isomorfo a F_p^* y $U = V \times U_1$.*

Demostración. Aplicaremos el lema previo a la sucesión exacta

$$1 \to U_1/U_n \to U/U_n \to F_p^* \to 1$$

En efecto, los grupos U_1/U_n y F_p^* cumplen las hipótesis que se necesitan en el lema, puesto que poseen órdenes p^{n-1} y $p-1$, respectivamente. El lema garantiza la existencia de un único subgrupo de U/U_n que será isomorfo a F_p^*. Dicho subgrupo será denotado por V_n. Por otro lado, la proyección $U/U_n \to U/U_{n-1}$ permite construir un isomorfismo entre V_n y V_{n-1}. Puesto que $U = \varprojlim U/U_n$, por paso al límite obtendremos un subgrupo V de U que será isomorfo a F_p^*. Realizando el paso al límite y aplicando el lema tenemos que $U = U_1 \times V$. La unicidad de V se concluye porque los V_n también lo son. □

Observación 2.69. V se denomina grupo de representantes multiplicativos de F_p^*.

Corolario 2.70. *El cuerpo $\mathbb{Q}_p$ contiene las $(p-1)$-ésimas raíces de la unidad.*

Nos centraremos ahora en estudiar la estructura del grupo U_1.

Lema 2.71 ([14])**.** *Sea $x \in U_n \setminus U_{n+1}$, con $n \geq 1$ si $p \neq 2$ y $n \geq 2$ si $p = 2$. Entonces $x^p \in U_{n+1} \setminus U_{n+2}$.*

Proposición 2.72. *Se cumplen:*

1. *Si $p \neq 2$ entonces U_1 es isomorfo a $\mathbb{Z}_p$.*
2. *Si $p = 2$ $U_1 = \{1, -1\} \times U_2$, y U_2 es isomorfo a $\mathbb{Z}_2$.*

Demostración. Comprobemos los dos casos:

1. Si $p \neq 2$, sea $\alpha \in U_1 \setminus U_2$, $\alpha = 1+p$. Por el lema anterior $\alpha^{p^i} \in U_{i+1} \setminus U_{i+2}$. Si α_n es la clase de α en U_1/U_n, $\alpha_n^{p^{n-2}} \neq 1$ pero $\alpha_n^{p^{n-1}} = 1$, y como U_1/U_n es un grupo de orden p^{n-1}, entonces es grupo cíclico y α_n es un generador. Sea ahora el isomorfismo $\theta_{n,\alpha} : \mathbb{Z}/p^{n-1}\mathbb{Z} \to U_1/U_n$, $\theta_{n,\alpha}(z) = \alpha_n^z$. El siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\theta_{n+1,\alpha}} & U_1/U_{n+1} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^{n-1}\mathbb{Z} & \xrightarrow{\theta_{n,\alpha}} & U_1/U_n \end{array}$$

   De todo esto podemos concluir, pasando al límite, que los $\theta_{n,\alpha}$ definen un isomorfismo $\theta : \mathbb{Z}_p \to U_1$ (recordemos que $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z}$ y $U_1 = \varprojlim U_1/U_n$).

2. Supongamos que $p = 2$. Podemos tomar $\alpha \in U_2 \setminus U_3$. Como en el caso anterior, podemos definir los isomorfismos $\theta_{n,\alpha} : \mathbb{Z}/2^{n-2}\mathbb{Z} \to U_2/U_n$ que, de forma análoga, darán lugar a un isomorfismo $\theta : \mathbb{Z}_2 \to U_2$. U_1/U_2 es isomorfo a $\mathbb{Z}/2\mathbb{Z}$ por la Observación 2.66. El homomorfismo $U_1 \to U_1/U_2$ induce un isomorfismo de $\{1, -1\}$ en $\mathbb{Z}/2\mathbb{Z}$. Todo ello nos permite afirmar que $U_1 = \{1, -1\} \times U_2$.

□

Gracias a los resultados tenemos el siguiente teorema.

Teorema 2.73. *Fijado un primo p:*

1. *Si $p \neq 2$, $\mathbb{Q}_p^*$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.*
2. *Si $p = 2$, $\mathbb{Q}_p^*$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.*

Demostración. Ya sabemos que los elementos de $\mathbb{Q}_p^*$ se pueden escribir de forma única como up^n, donde u es unidad p-ádica y $n\mathbb{Z}$. Entonces $\mathbb{Q}_p^*$ y $\mathbb{Z} \times U$ son isomorfos. Por la Proposición 2.68, U es isomorfo a $U_1 \times V$, donde V es un grupo cíclico con $p-1$ elementos. El resultado se concluye aplicando la Proposición 2.72. □

Para finalizar la sección vamos a estudiar los cuadrados en el grupo $\mathbb{Q}_p^*$.

Teorema 2.74. *Si $p \neq 2$ y $x = p^n u$, $x \in \mathbb{Q}_p^*$, entonces x es cuadrado en $\mathbb{Q}_p^*$ si, y solo si, n es par y la clase de u en $U/U_1 = F_p^*$, que denotaremos por $\bar{u}$, es un cuadrado en F_p^*.*

Observación 2.75. La última condición equivale a que el Símbolo de Legendre para $\bar{u}$, la clase de u en U/U_1, que denotaremos por $\left(\frac{\bar{u}}{p}\right)$ vale 1.

Veamos ahora la demostración.

Demostración. Podemos descomponer $u = u_1 v$, con $u_1 \in U_1$ y $v \in V$. El teorema anterior establece que $\mathbb{Q}_p^*$ es isomorfo a $\mathbb{Z} \times V \times U_1$ si $p \neq 2$. Por tanto un elemento de $x = p^n u = p^n u_1 v \in \mathbb{Q}_p$ será cuadrado si, y solo si, n es par y u_1 y v son cuadrados. U_1 es isomorfo a $\mathbb{Z}_p$ y 2 es invertible en $\mathbb{Z}_p$, por lo que todos los elementos de U_1 son cuadrados. V es isomorfo a F_p^*, lo que concluye el resultado. □

Corolario 2.76. *Si $p \neq 2$, el grupo $\mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$, donde $\mathbb{Q}_p^{*^2}$ denota al conjunto de cuadrados de $\mathbb{Q}_p^*$, tiene como representantes a $\{1, u, p, up\}$, donde $u \in U$ verifica que $\left(\frac{u}{p}\right) = -1$.*

Teorema 2.77 ([14])**.** *Un $x \in p^n u \in \mathbb{Q}_2^*$ es cuadrado si, y solo si, n es par y $u \equiv 1 \pmod 8$.*

Corolario 2.78. *El grupo $\mathbb{Q}_2^*/\mathbb{Q}_2^{*^2}$ tiene como representantes $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.*

Observación 2.79. Los últimos dos teoremas muestran que $\mathbb{Q}_p^{*^2}$ es un subgrupo abierto de $\mathbb{Q}_p^*$.

2.3. Polinomios sobre $\mathbb{Z}_p$. Lema de Hensel

Una vez trabajadas las propiedades más importantes del cuerpo de los números p-ádicos, la última sección trata algunos resultados sobre ecuaciones y polinomios en el anillo de enteros p-ádicos. Muchos resultados sobre estos aspectos serán de utilidad para el del Símbolo de Hilbert, realizado en el siguiente capítulo.

Observación 2.80. A efectos de notación, si $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ es un polinomio en las variables $X_1, \ldots, X_m$ y coeficientes en $\mathbb{Z}_p$, y n es un entero positivo, f_n denota al polinomio con coeficientes en A_n ($A_n = \mathbb{Z}/p^n\mathbb{Z}$), es decir, la reducción módulo p^n del polinomio f.

Comencemos a trabajar ahora con estos polinomios.

Proposición 2.81 ([14]). *Sean $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ polinomios con coeficientes p-ádicos. Las siguientes condiciones son equivalentes:*

1. *Los $f^{(i)}$ poseen un cero común en $(\mathbb{Z}_p)^m$.*
2. *Para todo $n > 1$ los polinomios $f_n^{(i)}$ tienen un cero común en $(A_n)^m$.*

Definición 2.82. $x = (x_1, \ldots, x_n) \in (\mathbb{Z}_p)^m$ se dice primitivo si alguno de los x_i no es divisible por p.

Proposición 2.83 ([14]). *Sean $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ polinomios con coeficientes p-ádicos. Las siguientes condiciones son equivalentes:*

1. *Los $f^{(i)}$ tienen un cero no trivial común en $(\mathbb{Q}_p)^m$.*
2. *Los $f^{(i)}$ tienen un cero no trivial común primitivo en $(\mathbb{Z}_p)^m$.*
3. *Para todo $n > 1$ los polinomios $f_n^{(i)}$ tienen un cero común primitivo en $(A_n)^m$.*

El siguiente lema es un resultado que será de utilidad para pasar de una solución módulo p^n a una solución con coeficientes en $\mathbb{Z}_p$.

Lema 2.84 ([14]). *Sea $f \in \mathbb{Z}_p[X]$ y f' su derivada. Sean $x \in \mathbb{Z}_p$ y $n, k \in \mathbb{Z}$ tal que $0 \leq 2k < n$, $f(x) \equiv 0 \,(\text{mód}\, p^n)$ y $v_p(f'(x)) = k$. Entonces existe un $y \in \mathbb{Z}_p$ tal que $f(y) \equiv 0 \,(\text{mód}\, p^{n+1})$, $v_p(f'(y)) = k$ y $x \equiv y \,(\text{mód}\, p^{n-k})$.*

Teorema 2.85. *Sean $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x = (x_1, x_2, \ldots, x_m) \in \mathbb{Z}_p^m$ y $n, k, j \in \mathbb{Z}$ con $0 \leq j \leq m$. Supongamos también que $0 < 2k < n$ y que $f(x) \equiv 0 \,(\text{mód}\, p^n)$ y $v_p(\frac{\partial f}{\partial X_j}(x)) = k$. Entonces existe un cero y de f en $(\mathbb{Z}_p)^m$ congruente con x módulo p^{n-k}.*

Demostración. Supongamos $m = 1$. Si aplicamos el lema previo a un $x^{(0)} = x$ obtendremos un $x^{(1)} \in \mathbb{Z}_p$ que será congruente con $x^{(1)}$ módulo p^{n-k}. Además, verificará que $f(x^{(1)}) \equiv 0 \,(\text{mód}\, p^n)$ y que $v_p(f'(x^{(1)})) = k$. Reemplazando n por $n+1$ podríamos aplicar de nuevo el lema a $x^{(1)}$, y así sucesivamente, construyendo una sucesión $\{x^{(i)}\}_{i\in\mathbb{N}}$ que verifica que $f(x^{(1)}) \equiv 0 \,(\text{mód}\, p^{n+q})$ y $x^{(q+1)} \equiv x^{(q)} \,(\text{mód}\, p^{n+q-k})$.
La sucesión que hemos construido es de Cauchy. Si y es el límite de dicha sucesión, entonces $f(y) = 0$ e $y \equiv x \,(\text{mód}\, p^{n-k})$, lo que concluye el caso $m = 1$.

Si $m > 1$ se reduce en realidad al caso $m = 1$ procediendo del siguiente modo: si $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, denotamos por $\bar{f} \in \mathbb{Z}_p[X_j]$ al polinomio en una variable que resulta de sustituir en f las variables X_i por los valores x_i. Aplicando el caso $m = 1$, existe un y_j tal que $f(\bar{y_j}) = 0$ e $y_j \equiv x_j \,(\text{mód}\, p^{n-k})$. Así, si $y_i = x_i$ para todo $i \neq j$, $y = (y_1, \ldots, y_m)$ satisface la condición deseada. □

Corolario 2.86. *Un cero simple de la reducción módulo p de un polinomio f proporciona un cero de f con coeficientes en $\mathbb{Z}_p$ (recordemos que un cero simple es aquel en el que al menos una de las derivadas parciales del polinomio no se anula al evaluarla en dicho punto).*

Corolario 2.87. *Sea $p \neq 2$, y sea $\sum a_{ij}X_iX_j$, con $a_{ij} = a_{ji}$, una forma cuadrática con coeficientes en $\mathbb{Z}_p$ cuyo discriminante ($\det(a_{ij})$) es invertible. Si $a \in \mathbb{Z}_p$ entonces toda solución de la ecuación $f(x) \equiv a \,(\text{mód}\, p)$ proporciona una solución para $\mathbb{Z}_p$.*

Corolario 2.88. *Sea $p = 2$, y sea $\sum a_{ij}X_iX_j$, con $a_{ij} = a_{ji}$, una forma cuadrática con coeficientes en $\mathbb{Z}_2$. Sea $a \in \mathbb{Z}_2$. Si x es solución de $f(x) \equiv a \,(\text{ mód } 8)$ entonces x proporciona una solución general si x no anula $\frac{\partial f}{\partial X_j}$ en módulo 4. Esta última condición se alcanza si el discriminante es invertible.*

A continuación enunciamos y demostramos un resultado muy importante sobre polinomios en $\mathbb{Z}_p$, el Lema de Hensel, que nos va a permitir comprobar la resolubilidad de las ecuaciones sobre $\mathbb{Q}_p$ que aparecen en el enunciado del Teorema de Hasse-Minkowski.

Teorema 2.89 (Lema de Hensel)**.** *Sea $f \in \mathbb{Z}_p[X]$ un polinomio y f' su derivada. Supongamos que existe un entero p-ádico α_1 tal que $|f(\alpha_1)|_p < |f'(\alpha_1)|_p^2$. Entonces existe un único entero p-ádico α que verifique que $f(\alpha) \equiv 0$ y $\alpha \equiv \alpha_1 \,(\text{mód}\, p^{v_p(f(\alpha_1))-v_p(f'(\alpha_1))})$.*

Demostración. Veamos que dado α_1 podemos construir una sucesión coherente cuyo límite sea una raíz de dicho polinomio.
Sean $j = v_p(f(\alpha_1))$ y $k = v_p(f'(\alpha_1))$ con $0 \leq 2j < k$. Si $f(\alpha_1) = p^j u_1$ y $f'(\alpha_1) = p^k u_2$, con u_1 y u_2 unidades p-ádicas. Queremos probar que existe α tal que $\alpha \equiv \alpha_1 \,(\text{mód}\, p^{j-k})$ y $f(\alpha) \equiv$

$0\,(\text{mód}\,p^{j+1})$. Tomamos $\alpha = \alpha_1 + up^{j-k}$. Intentaremos encontrar un u adecuado. Realizando la expansión en Serie de Taylor:

$$f(\alpha) = f(\alpha_1) + f'(\alpha_1)up^{j-k} + \frac{1}{2!}f''(\alpha_1)u^2p^{2j-2k} + \text{ términos de orden } p^n.$$

Si p es impar $v_p(\frac{1}{2!}f''(\alpha_1)u^2p^{2j-2k}) \leq 2j-2k > 2j-j = j$. Por tanto $f(\alpha) \equiv f(\alpha_1) + f'(\alpha_1)up^{j-k}\,(\text{mód}\,p^{j+1})$. De esto deducimos que $f(\alpha) \equiv u_1p^j + uu_2p^j\,(\text{mód}\,p^{j+1})$. El objetivo era encontrar un u tal que $0 \equiv u_1p^j + uu_2p^j\,(\text{mód}\,p^{j+1})$ o, equivalentemente, tal que $0 \equiv u_1 + uu_2\,(\text{mód}\,p)$, que es resoluble por ser u_1 y u_2 unidades. El caso $p = 2$ es análogo. □

Para finalizar este capítulo vamos a enunciar un resultado propuesto por Minkowski que es equivalente al Teorema de Hasse-Minkowski.

Teorema 2.90 (Minkowski, [12])**.** *Sea $f(x_1, \ldots, x_n)$ una forma cuadrática con coeficientes racionales. $f(x_1, \ldots, x_n) \equiv 0\,(\text{mód}\,p^r)$ tiene solución no trivial para cualquier primo p y cualquier entero positivo r, y la ecuación $f(x_1, \ldots, x_n) = 0$ tiene solución no trivial sobre $\mathbb{R}$ si, y solo si, $f(x_1, \ldots, x_n) = 0$ tiene solución no trivial sobre $\mathbb{Q}$.*

Observación 2.91. Tal y como explicamos en la Introducción, Minkowski no podía emplear el lenguaje de los números p-ádicos porque estos todavía no habían sido introducidos por Hensel.

Capítulo 3

Símbolo de Hilbert

El Símbolo de Hilbert es similar al de Legendre en el sentido de que también nos indica la resolubilidad de ciertas ecuaciones cuadráticas sobre un cuerpo. De hecho, demostraremos un resultado que muestra al de Hilbert como una generalización del de Legendre.

En este capítulo el cuerpo K considerado será o $\mathbb{Q}_p$ o $\mathbb{R}$, y $K^* = K \setminus \{0\}$ como anteriormente. Se han seguido las referencias [4] y [14].

Definición 3.1. Si $a, b \in K^*$, se dice que:

- $(a, b) = 1$ si la ecuación $z^2 - ax^2 - by^2 = 0$ tiene una solución (z, x, y) no nula en K^3.
- $(a, b) = -1$ en otro caso.

(a, b) se denomina Símbolo de Hilbert de a y b relativo al cuerpo K.

Este concepto fue introducido por el propio David Hilbert en su obra *Zahlbreicht*, publicada en 1897, que trataba sobre Teoría de Números. Se considera una generalización del Símbolo de Legendre. Es muy importante en la demostración del Teorema de Hasse-Minkowski. Las siguientes proposiciones muestran algunas propiedades básicas del Símbolo de Hilbert.

Proposición 3.2. *Sean $a, b \in K^*$, y consideremos la extensión $K(\sqrt{b})$. Se cumple que $(a, b) = 1$ si, y solo si, a es de la forma $z^2 - by^2$ para ciertos $y, z \in K$.*

Demostración. Si b es el cuadrado de algún elemento en K entonces $K(\sqrt{b}) = K$, y bastaría tomar la terna con z dicho elemento, $x = 0$ e $y = 1$.
Si b no fuese cuadrado, supongamos que $(a, b) = 1$. Entonces $z^2 - ax^2 - by^2 = 0$ posee alguna

solución no nula en K^3. Veamos que $x \neq 0$. Si $x = 0$, $z^2 - by^2 = 0$ y $b = \frac{z^2}{y^2}$, pero entonces b sería un cuadrado. Así, $x \neq 0$. En ese caso, $z^2 - by^2 = ax^2$, es decir $\frac{z^2}{x^2} - b\frac{y^2}{x^2} = a$, por lo que a sería de la forma $\bar{z}^2 - \bar{y}^2 b$.
Veamos el recíproco. Si $a = z^2 - by^2$ para ciertos $z, y \in K$. En ese caso $z^2 - ax^2 - by^2 = 0$ tiene un cero $(z, 1, y)$. □

Observación 3.3. Si a verifica las condiciones de la proposición anterior a pertenece a lo que se conoce como el grupo de las normas de $K(\sqrt{b})$, que denotaremos por NK_b.

Proposición 3.4. *Si $a, b, c \in K^*$. Se verifican:*

1. $(a, b) = (b, a)$.
2. $(a, b^2) = 1$.
3. $(a, -a) = 1$ *y* $(a, 1 - a) = 1$.
4. *Si* $(a, b) = 1$, *entonces* $(ac, b) = (c, b)$.
5. $(a, b) = (a, -ab) = (a, (1 - a)b)$.

Demostración.

1. Inmediato por definición.
2. $(a, b) = 1$ si, y solo si, $z^2 - ax^2 - by^2 = 0$ tiene una solución (z, x, y) no nula en K^3. En particular, $(a, b^2) = 1$ si, y solo si, $z^2 - ax^2 - b^2y^2 = 0$ tiene una solución (z, x, y) no nula en K^3. El término $b^2y^2 \geq 0$, y $b \neq 0$. Por otra parte, $z^2 - ax^2 - b^2y^2 = 0 \iff z^2 = ax^2 + b^2y^2$, y para que exista solución necesitaremos que $ax^2 + b^2y^2 \geq 0$ (y obtendremos un z concreto a partir de los x e y fijados), pero para ello es suficiente tener en cuenta que $b^2 > 0$ y por tanto bastará con tomar los x e y adecuados para que $ax^2 + b^2y^2$ sea positivo.
3. $z^2 - ax^2 - (-a)y^2 = 0$ tiene como solución no nula en K^3 $(z, x, y) = (0, 1, 1)$. Por su parte, $z^2 - ax^2 - (1 - a)y^2 = 0$ tiene como solución no nula K^3 $(z, x, y) = (1, 1, 1)$.
4. Por la Proposición 3.2, si $(a, b) = 1$ entonces $a = z^2 - by^2$, con $y, z \in K$, es decir, a pertenece al grupo de normas de $K(\sqrt{b})$, NK_b, de modo que $ac \in NK_b^* \iff c \in NK_b^*$.
5. Por el tercer apartado de esta proposición, $(a, -a) = (a, 1 - a) = 1$. En consecuencia, por el cuarto apartado de esta proposición $(a, -ab) = (a, b)$ y $(a, (1 - a)b) = (a, b)$.

□

Observación 3.5. El apartado 4 de la proposición anterior es un caso particular de la bilinealidad del Símbolo de Hilbert: $(ac, b) = (a, b)(c, b)$. Esta propiedad se mencionará de nuevo más adelante.

Observación 3.6. El símbolo de Hilbert define una aplicación de $K^*/K^{*^2} \times K^*/K^{*^2}$ en $\{1, -1\}$, ya que si multiplicamos a y b por cuadrados en el cuerpo K (no necesariamente iguales) el símbolo de Hilbert permanece invariante.

Proposición 3.7. *Si $K = \mathbb{R}$, entonces $(a, b) = -1$ si a y b son negativos, mientras que $(a, b) = 1$ si alguno de los dos, a o b, es positivo.*

Demostración. Se concluye por definición, ya que si ambos son negativos $z^2 - ax^2 - by^2 \geq 0$. Si alguno a o b es alguno de ellos positivo es posible encontrar una terna no nula. Por ejemplo, si $a > 0$ y $b < 0$ podríamos tomar la terna $(\sqrt{\frac{-by^2}{a}}, y, 0)$. □

Teorema 3.8. *Supongamos $K = \mathbb{Q}_p$. Sean $a = p^n u$ y $b = p^m v$, donde u y v son unidades p-ádicas. Entonces se tiene que*

$$Si\ p = 2,\ (a, b) = (-1)^{\epsilon(u)\epsilon(v)+n\omega(v)+m\omega(u)}$$

$$Si\ p \neq 2,\ (a, b) = (-1)^{nm\epsilon(p)} \left(\frac{u}{p}\right)^m \left(\frac{v}{p}\right)^n$$

Observación 3.9. En el teorema anterior $\left(\frac{u}{p}\right)$ denota el Símbolo de Legendre y $\epsilon(n)$ y $\omega(n)$ los homomorfismos correspondientes, todo ello de la forma que se describe a partir de la Definición 1.16 de los Preliminares.

Para probar el teorema necesitamos el siguiente resultado:

Lema 3.10 ([14])**.** *Sea v una unidad p-ádica. Si la ecuación $z^2 - px^2 - vy^2 = 0$ tiene una solución no trivial en el cuerpo de los racionales p-ádicos, entonces tiene una solución (z_0, x_0, y_0) de forma que z_0 y y_0 son unidades p-ádicas y x_0 es un entero p-ádico.*

Ahora sí estamos en condiciones de demostrar el teorema.

Demostración. Veamos primero el caso $p \neq 2$
Trabajando en función de la paridad de m y n (por la definición de los Símbolos de Legendre y de Hilbert), y teniendo en cuenta que el Símbolo de Hilbert es simétrico, es suficiente con considerar los siguientes casos:

- $n \equiv m \equiv 0 \pmod 2$. En este caso nm es par, por lo que $nm\epsilon(p)$ será un número par para cualquier primo $p \neq 2$ considerado. En consecuencia, en la fórmula del enunciado del teorema, el lado derecho de la igualdad vale 1. Por tanto, hay que demostrar que $(a, b) = 1$.

Comprobar que $(a,b)=1$ en este caso equivale a ver que $(u,v)=1$ debido a la paridad de n y m. Ahora bien, por el Corolario 1.12, la forma cuadrática $z^2-ux^2-vy^2$ tiene un cero no trivial (módulo p). El discriminante de esta forma cuadrática es una unidad p-ádica, por lo que gracias a los Corolarios 2.86 y 2.87, del cero anterior podremos obtener una solución p-ádica.

- $n\equiv 1 \pmod 2$ y $m\equiv 0 \pmod 2$. Como en el caso anterior, nm es par. Demostrar que $(a,b)=1$ equivale a probar que $(pu,v)=\left(\frac{v}{p}\right)$. En el apartado anterior hemos probado que si u y v son unidades p-ádicas, $(u,v)=1$. Por la Proposición 3.4 $(pu,v)=(p,v)$, por lo que basta comprobar que $(p,v)=\left(\frac{v}{p}\right)$. Si v es un cuadrado, debido a la Proposición 3.4 y la definición del Símbolo de Legendre, ambos términos de la igualdad son iguales a 1. Si no, por el Teorema 2.74 y por la Observación 2.75, $\left(\frac{v}{p}\right)=-1$. Esto quiere decir que la congruencia $z^2\equiv v \pmod p$ no tiene solución. Entonces por el lema previo a la demostración la ecuación $z^2-px^2-vy^2=0$ no tiene ceros no triviales y $(p,v)=-1$. El caso $m\equiv 1 \pmod 2, n\equiv 0 \pmod 2$ es completamente análogo a este.

- $n\equiv m\equiv 1 \pmod 2$. Hay que comprobar que $(pu,pv)=(-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. Gracias a la Proposición 3.4 sabemos que $(pu,pv)=(pu,-p^2uv)=(pu,-uv)$. En el apartado anterior sabemos que $(pu,-uv)=(p,-uv)=\left(\frac{-uv}{p}\right)$, ya que $-uv$ es unidad p-ádica. Gracias a las propiedades del Símbolo de Legendre se concluye que

$$\left(\frac{-uv}{p}\right)=\left(\frac{-u}{p}\right)\left(\frac{v}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)=(-1)^{\epsilon(p)}\left(\frac{u}{p}\right)^m\left(\frac{v}{p}\right)^n$$

Una vez probado el caso $p\neq 2$ veamos qué ocurre si $p=2$. De nuevo consideramos 3 posibilidades en función m y n:

- $n\equiv m\equiv 0 \pmod 2$. Hay que probar que $(a,b)=(u,v)=(-1)^{\epsilon(u)\epsilon(v)}$. En base a las propiedades del Símbolo de Legendre y de ϵ, debemos comprobar que si u o v es equivalente a 1 en módulo 4 entonces $(a,b)=1$, y que su valor es -1 en cualquier otro caso. Supongamos primeramente que $u\equiv 1 \pmod 4$. Entonces o bien $u\equiv 1 \pmod 8$, y en ese caso, por el Teorema 2.77 u es cuadrado y $(a,b)=(u,v)=1$; o bien $u\equiv 5 \pmod 8$, y entonces como $u+4v\equiv 1 \pmod 8$ existe $u'\in U$ (como en el capítulo anterior, U denota al conjunto de unidades p-ádicas para un primo p) de forma que $u'^2=u+4v$. Por tanto $(u',1,2)$ sería cero no trivial de $z^2-ux^2-vy^2$ y $(a,b)=1$. Supongamos ahora que $u\equiv v\equiv 3\equiv -1 \pmod 4$. Entonces si $z^2-ux^2-vy^2$ tiene un cero primitivo (z_0,x_0,y_0) se verifica que $z_0^2+x_0^2+y_0^2\equiv 0 \pmod 4$, y z_0, x_0 e y_0 deben ser pares, pero ello contradice que el cero sea primitivo. Tendremos en esa situación que $(a,b)=-1$.

- $n\equiv 1 \pmod 2$ y $m\equiv 0 \pmod 2$. Al igual que antes, esta demostración es completamente análoga al caso en el que $m\equiv 1 \pmod 2$ y $n\equiv 0 \pmod 2$. Ahora hay que probar que

$(a,b) = (2u,v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$. Antes comprobemos que $(2,v) = (-1)^{\omega(v)}$, es decir, que $(2,v) = 1 \iff v \equiv \pm 1 \pmod 8$. Por el lema previo a esta demostración, si $(2,v) = 1$ entonces existen $x_0, y_0, z_0 \in \mathbb{Z}_2$ tal que $z_0^2 - 2x_0^2 - vy_0^2 = 0$ e y_0 y z_0 son unidades 2-ádicas. Entonces $y_0^2, z_0^2 \equiv 1 \pmod 8$ y $1 - 2x^2 - v \equiv 0 \pmod 8$. Dado que 0, 1 y 4 son los únicos cuadrados módulo 8, de la expresión anterior se concluye que o bien $v \equiv 1 \pmod 8$ (si $x \equiv 0$ o $x \equiv 4$ módulo 8), o bien $v \equiv -1 \pmod 8$ (si $x \equiv -1 \pmod 8$). En el primer caso v es un cuadrado y entonces $(2,v) = 1$. En el segundo, $z^2 - px^2 - vy^2$ tiene como cero $(1,1,1)$ (en módulo 8) y por los Corolarios 2.86 y 2.87, del cero anterior podremos obtener una solución p-ádica.

Probaremos ahora que $(2u,v) = (u,v)(2,v)$. Por la Proposición 3.4 se cumple la igualdad si $(u,v) = 1$ o $(2,v) = 1$. Falta comprobar lo que ocurre si $(u,v) = (2,v) = -1$, lo que es equivalente a que $z^2 - ux^2 - vy^2 = 0$ y $z^2 - 2x^2 - vy^2 = 0$ no tengan ceros no triviales. Es decir, $u \equiv -1$ o $3 \pmod 8$ y $v \equiv 3 \pmod 8$. Trabajando en módulo 8 considerando estos casos y teniendo en cuenta que $p = 2$ habría que estudiar las soluciones no triviales de $z^2 + 2x^2 - 3y^2 = 0$ y $z^2 - 6x^2 + 5y^2 = 0$ (sin pérdida de la generalidad estamos suponiendo que $u = -1$ y $v = 3$ en el primer caso que $u = -1$ y $v = -3$ en el segundo). Ambas ecuaciones tienen como solución no trivial $(1,1,1)$, por lo que $(2u,v) = 1$.

- $n \equiv m \equiv 1 \pmod 2$. Debemos comprobar que $(a,b) = (2u,2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)+\omega(u)}$. Razonando de forma similar a apartados anteriores, empleando la Proposición 3.4, tenemos que $(2u,2v) = (2u,-4uv) = (2u,-uv)$. No obstante, gracias a lo que hemos probado en el apartado anterior tenemos que

$$(2u,-uv) = (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)}$$

Trataremos de llegar a la expresión deseada a partir de la anterior empleando las propiedades de ϵ y ω. Por un lado, por definición, $\epsilon(-1) = 1$ y $\omega(-1) = 0$. ϵ y ω son homomorfismos de grupos. En particular, están definidos de sendos grupos multiplicativos ($\mathbb{Z}/4\mathbb{Z}^*$ y $\mathbb{Z}/8\mathbb{Z}^*$) en un grupo aditivo ($\mathbb{Z}/2\mathbb{Z}$). En consecuencia,

$$\epsilon(u)\epsilon(-uv) + \omega(-uv) = \epsilon(u)\epsilon(-1) + \epsilon(u)\epsilon(u) + \epsilon(u)\epsilon(v) + \omega(-1) + \omega(u) + \omega(v),$$

y como $\epsilon(-1) = 1$ y $\omega(-1) = 0$ basta comprobar que $\epsilon(u) + \epsilon(u)\epsilon(u) \equiv 0 \pmod 2$, pero esto se deduce precisamente de la definición de ϵ.

□

Teorema 3.11 ([14])**.** *El Símbolo de Hilbert es una forma bilineal no degenerada en el F_2-espacio vectorial K/K^*.*

A continuación se va a enunciar y demostrar un resultado muy importante que relaciona el Símbolo de Hilbert y los números p-ádicos y que se suele denominar Teorema de Hilbert, en honor

al matemático ya mencionado previamente. Para ello es necesario antes introducir la siguiente notación: sean $a, b \in \mathbb{Q}^*$, se denota por $(a,b)_p$ y $(a,b)_\infty$ a los Símbolos de Hilbert de las imágenes de estos elementos racionales no nulos en el cuerpo de los racionales p-ádicos y en el cuerpo de los reales, respectivamente (recordemos que se suele escribir $\mathbb{Q}_\infty = \mathbb{R}$).

Teorema 3.12 (Hilbert)**.** *Si $a, b \in \mathbb{Q}^*$ entonces $(a,b)_l = 1$ para casi todo $l \in V$ (es decir, para todo l excepto un número finito de ellos) y*

$$\prod_{l \in V} (a,b)_l = 1,$$

donde V denota al conjunto formado por todos los números primos e infinito.

Demostración. Teniendo en cuenta que el Símbolo de Hilbert es bilineal es suficiente considerar los casos en los que a o b valgan -1 o un número primo. Para conocer los valores del Símbolo de Hilbert en los casos de estudio será de utilidad el Teorema 3.8. De nuevo, consideraremos diferentes casos en función de los valores de a y b:

- $a = b = -1$. $(-1,-1)_\infty = -1$ ya que la ecuación $z^2 + x^2 + y^2 = 0$ no tiene ceros no triviales en $\mathbb{R}^3$. Sustituyendo en la fórmula del Teorema 3.8 para $p = 2$ obtenemos que $(a,b)_2 = -1$. Para cualquier primo p distinto de 2 tenemos que $(-1,-1)_p = 1$, ya que si $a = b = -1$ estamos ante el caso en el que $m = n = 0$ y $u = v = -1$. Entonces $\prod_{l \in V} (-1,-1)_l = 1$.
- Consideremos ahora el caso $a = -1$ y $b = q$, con q número primo (el caso $a = q$ y $b = -1$, además de ser análogo en demostración, da lugar a la misma conclusión por ser el Símbolo de Hilbert simétrico). Es decir, si $l = q$ estamos ante el caso $p = q$, $n = 0$, $m = 1$, $u = -1$ y $v = 1$, y si $l \neq q$ estamos ante el caso $n = 0$, $m = 0$, $u = -1$ y $v = q$. Si $q = 2$ entonces, por el Teorema 3.8 $(-1,2)_l = 1$ para cualquier l de V, ya que $(1,1,1)$ es cero no trivial de $z^2 + x^2 - 2y^2$ en cualquiera de los cuerpos considerados. Si $l, q \neq 2$ y $q \neq l$, entonces $(-1,q)_l = 1$ porque $m = n = 0$; si no, si $(-1,q)_2 = (-1)^{\epsilon(-1)\epsilon(q)} = (-1)^{\epsilon(q)}$. Si $q \neq 2$, nos encontramos en el caso $p = q$, $n = 0$, $m = 1$, $u = -1$ y $v = 1$ del Teorema 3.8, y entonces $(-1,q)_q = \left(\frac{-1}{q}\right) = (-1)^{\epsilon(q)}$, por la Proposición 1.22. En consecuencia, $(-1,q)_q(-1,q)_2 = 1$ para todo primo q, por lo que $\prod_{l \in V} (-1,q)_l = 1$ para cualquier primo q.
- $a = n$ y $b = n'$ con n y n' primos. Si son iguales, por la Proposición 3.4 $(n,n)_v = (-1,n)_v = (n,-1)_v$ ya que en dicho resultado se prueba que $(a,b) = (a,-ab)$, por lo que estudiar el caso $(n,n)_v$ coincidiría con estudiar el caso $(-1,n)_v$ que ya se ha trabajado en el apartado anterior. Si $n \neq n'$ y uno de ellos tiene valor 2 (podemos suponer sin perder la generalidad que es n, por la simetría del Símbolo de Hilbert), entonces si $v \neq 2, n'$ nos encontraremos en el caso $n = m = 0$ y $u = 2$ y $v = n'$, por lo que $(2,n')_v = 1$. Por

otro lado, $(2,n')_2 = (-1)^{\omega(n')}$, ya que en esta situación $n = 1$, $m = 0$, $u = 1$ y $v = n'$. $(2,n')_{n'} = (n',2)_{n'} = \left(\frac{2}{n'}\right) = (-1)^{\omega(n')}$ por la Proposición 1.22. Así el producto de todos los elementos es $(-1)^{2\omega(n')} = 1$.

Para finalizar con las posibilidades de este apartado, supongamos que n y n' son ambos distintos entre sí y diferentes de 2. Entonces, $(n,n')_l = 1$ para cualquier l diferente de n, n' y de 2, ya que estaremos en el caso $p \neq 2$ del Teorema 3.8 con los valores $n = m = 0$ y $u = n$ y $v = n'$. En los casos que quedan,

$$(n,n')_n = \left(\frac{n'}{n}\right),\ (n,n')_{n'} = \left(\frac{n}{n'}\right) \text{ y } (n,n')_2 = (-1)^{\epsilon(n)\epsilon(n')}$$

Pero por la Ley de Reciprocidad Cuadrática vista en los Preliminares, $\left(\frac{n}{n'}\right)\left(\frac{n'}{n}\right) = (-1)^{\epsilon(n)\epsilon(n')}$, por lo que el producto de estas 3 posibilidades

$$(-1)^{2\epsilon(n)\epsilon(n')} = 1,$$

de modo que $\prod_{l\in V}(n,n')_l = 1$.

□

Aunque lo más "relevante" del teorema anterior es el hecho de que el producto de todos los Símbolos de Hilbert da 1, a lo largo de la demostración también hemos comprobado en las diferentes situaciones posibles que $(a,b)_l = 1$ para todo $l \in V$ excepto para un número finito.

A continuación vamos a ver un resultado que será de utilidad en la demostración del Teorema de Hasse-Minkowski y que proporciona condiciones necesarias y suficientes sobre la existencia de números racionales para unos símbolos de Hilbert dados. Para ello antes enunciaremos algunos resultados previos que son necesarios.

Lema 3.13 (Teorema Chino de los Restos, [14]). *Sean $a_1,\dots,a_n$ y $m_1,\dots,m_n$ números enteros con m_i coprimo con m_j para todo $i \neq j$. Entonces el sistema de congruencias*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

tiene solución.

Lema 3.14 (Teorema de Aproximación, [14]). *Si denotamos de nuevo por V al conjunto formado por los números primos e infinito, consideremos $S \subset V$ subconjunto finito. Entonces se cumple*

que la imagen de $\mathbb{Q}$ *en* $\prod_{l\in S}\mathbb{Q}_l$ *es densa en dicho producto (considerando la topología producto de los* $\mathbb{Q}_l$*).*

Lema 3.15 (Teorema de las Progresiones Aritméticas de Dirichlet, [14])**.** *Si* a *y* n *son enteros coprimos positivos, entonces existen infinitos primos* p *tales que* $p \equiv a \pmod{m}$.

Ahora sí estamos en condiciones de enunciar y demostrar el siguiente teorema.

Teorema 3.16. *Sean* $(a_i)_{i\in I}$ *una familia finita de elementos de* $\mathbb{Q}^*$ *y* $(\epsilon_{i,v})_{i\in I, v\in V}$ *un conjunto de números iguales a* ± 1*. Para que exista un* $x \in \mathbb{Q}^*$ *de forma que* $(a_i, x)_v = \epsilon_{i,v}$ *para todo* $i \in I$ *y para todo* $v \in V$ *es necesario y suficiente que se cumplan las siguientes condiciones:*

1. *Casi todos los* $\epsilon_{i,v}$ *tienen valor 1.*
2. $\prod_{v\in V} \epsilon_{i,v} = 1$ *para todo* $i \in I$*.*
3. *Para todo* $v \in V$ *existe un* $x_v \in \mathbb{Q}_v$ *de forma que* $(a_i, x_v)_v = \epsilon_{i,v}$ *para todo* $i \in I$*.*

Demostración. En cuanto a la condición necesaria, los dos primeros apartados se concluyen del Teorema de Hilbert que aparece con anterioridad en esta misma sección. El tercer apartado es inmediato ya que bastaría tomar $x_v = x$. Probemos ahora la suficiencia.
Supongamos que tenemos $(\epsilon_{i,v})_{i\in I, v\in V}$ de números que valen ± 1 y que satisfacen las 3 condiciones enunciadas en el resultado. Consideremos también los $(a_i)_{i\in I}$ y supongamos, sin pérdida de la generalidad, que son todos enteros (bastaría multiplicar cada uno de los a_i por el cuadrado de algún entero). Consideremos S el subconjunto finito de V formado por 2, por los primos que aparecen en la factorización de los a_i y ∞. Denotemos por T el subconjunto finito de V de forma que existe algún $i \in I$ tal que $\epsilon_{i,v} = -1$. Estudiemos dos casos posibles por separado: si S y T son, o no, disjuntos.

- $S \cap T = \emptyset$. Sean
$$a = \prod_{t\in T,\ t\neq\infty} t \text{ y } n = 8 \prod_{s\in S,\ s\neq 2,\infty} s$$
Por hipótesis $S\cap T = \emptyset$, luego a y n deben ser enteros coprimos. Entonces, por el Teorema de Dirichlet (Lema 3.15) existe un primo p tal que $p \equiv a \pmod{n}$ (fijémonos en que entonces $p \notin S \cup T$). Veamos que si tomamos $x = ap$ entonces $(a_i, x)_v = \epsilon_{i,v}$ para todo $i \in I$ y para todo $v \in V$.
Si $v \in S$ entonces $\epsilon_{i,v} = 1$ para todo $i \in I$ porque $S \cap T = \emptyset$, y T por definición es el subconjunto de V de forma que existe $i \in I$ tal que $\epsilon_{i,v} = -1$. Debemos comprobar que $(a_i, x)_v = 1$ para todo $i \in I$. Si $v = \infty$ (es decir, considerar $\mathbb{Q}_\infty = \mathbb{R}$) por la Proposición 3.7

basta que alguno de los 2 elementos sea positivo para que el Símbolo de Hilbert tenga valor 1, y x lo es por definición. Si v es un primo l, entonces como $x \equiv a^2 \pmod{n}$, $x \equiv a^2 \pmod{8}$ si $l = 2$ y $x \equiv a^2 \pmod{l}$ si $l \neq 2$. Tanto x como a son unidades l-ádicas, por el Teorema 2.74 y el Teorema 2.77 x es cuadrado en $\mathbb{Q}_l^*$, y entonces $(a_i, x)_v = 1$.
Por otro lado, si $v = l \notin S$ entonces a_i es una unidad $l-$ádica para todo i, porque el conjunto S está formado por los primos en las factorizaciones presentes en la factorización de los a_i. Como $l \neq 2$ tenemos que $(a_i, b)_l = \left(\frac{a_i}{l}\right)^{v_l(b)}$ para todo $b \in \mathbb{Q}_l^*$ por el Teorema 3.8 (ya que estaríamos ante el caso $p = l \neq 2$, $n = 0$ y $m = v_l(b)$, donde v_l denota a la valoración l-ádica definida en la Definición 2.8). En particular, si $l \notin T \cup \{p\}$ x es unidad l-ádica y $v_l(x) = 0$, por lo que la expresión anterior permite deducir que $(a_i, x)_l = 1$. Además, $\epsilon_{i,l} = 1$ porque $l \notin T$. Por otro lado, si l estuviese en T entonces se tendría que $v_l(x) = 1$ y además, por la tercera condición del enunciado, existiría un $x_l \in \mathbb{Q}_l^*$ tal que $(a_i, x_l)_l = \epsilon_{i,l}$ para todo $i \in I$. Como $l \in T$ alguno de los $\epsilon_{i,l}$ vale -1 y $v_l(x_l)$ es impar, y por el Teorema 3.8, $(a_i, x)_l = \left(\dfrac{a_i}{l}\right) = (a_i, x_l)_l = \epsilon_{i,l}$ para todo $i \in I$ (ya que nos encontramos ante el caso $n = 0$, $m = 1$, $u = a_i$ y $v = 1$). Esto nos deja el caso $l = p$, que podemos concluir del resto empleando la fórmula del producto:

$$(a_i, x)_p = \prod_{v \neq p} (a_i, x)_v = \prod_{v \neq p} \epsilon_{i,v} = \epsilon_{i,p}$$

- Veamos la demostración en general: ya hemos visto al final del segundo capítulo que los cuadrados de $\mathbb{Q}_v^*$ forman un subgrupo abierto de $\mathbb{Q}_v^*$. Por el Teorema de Aproximación (Lema 3.14) existe $x' \in \mathbb{Q}^*$ tal que $\frac{x'}{x_v}$ es cuadrado en $\mathbb{Q}_v^*$ para todo $v \in S$. En particular se tiene que $(a_i, x')_v = (a_i, x_v)_v = \epsilon_{i,v}$ para todo $v \in S$ debido a que estamos suponiendo cierta la tercera condición del enunciado. Si escribimos $\eta_{i,v} = \epsilon_{i,v}(a_i, x')_v$, $\{\eta_{i,v}\}$ verifica las 3 condiciones del enunciado, por el Teorema de Hilbert y gracias a que los $\epsilon_{i,v}$ cumplen dichas condiciones. $\eta_{i,v} = 1$ si $v \in S$, porque si $v \in S$ $(a_i, x')_v = \epsilon_{i,v}$, y entonces $\eta_{i,v} = \epsilon_{i,v}^2 = 1$. Podemos considerar entonces el caso anterior para los $\{\eta_{i,v}\}$, y entonces existe un $y \in \mathbb{Q}^*$ tal que $(a_i, y)_v = \eta_{i,v}$ para todo $i \in I, v \in V$. Tomando $x = yx'$, x verificará las propiedades deseadas.

□

Capítulo 4

Cuerpos Locales

Este capítulo tiene dos partes. La primera es una introducción a los cuerpos locales, relacionándolos con lo trabajado en el segundo capítulo. La segunda estudia las formas cuadráticas sobre cuerpos locales, y los resultados trabajados en ella sirven como un paso previo para el Teorema de Hasse-Minkowski. Los contenidos analizados aquí se pueden encontrar en [2], [5], [11] y [14].

Definición 4.1. Sea $|\ |$ un valor absoluto no arquimediano en un cuerpo K. Escribiendo $v(x) = -\log|x|$ si $x \neq 0$ y $v(0) = \infty$. Esto nos proporciona una aplicación que verifica las siguientes propiedades:

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

Una aplicación que posee estas propiedades se denomina valoración exponencial en K. Para cada valoración exponencial obtenemos una valoración escribiendo $|x| = q^{-v(x)}$ para algún real fijado $q > 1$. Tal y como hemos visto en el capítulo 2, la valoración p-ádica es un ejemplo de valoración exponencial.

En base a la definición anterior tenemos el siguiente resultado:

Proposición 4.2 ([11])**.** *Se tiene:*

1. $\mathcal{O} = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$ *es un anillo.*
2. *El anillo* $\mathcal{O}$ *tiene como grupo de unidades a* $\mathcal{O}^* = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}$.

3. *K es un anillo local y su único ideal maximal es* $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^* = \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}$.

Observación 4.3. $\mathcal{O}$ es un dominio entero con cuerpo de fracciones K que tiene como propiedad que si $x \in K$ entonces $x \in \mathcal{O}$ o $x^{-1} \in \mathcal{O}$, y podemos expresar el ideal maximal como $\mathfrak{p} = \{x \in K : x \in \mathcal{O} \text{ y } x^{-1} \notin \mathcal{O}\}$. El cuerpo $\mathcal{O}/\mathfrak{p}$ se denomina cuerpo de residuos de $\mathcal{O}$.

Definición 4.4. Una valoración v sobre un cuerpo K se dice discreta si $v(K^*) = s\mathbb{Z}$ para algún s positivo.

Los anillos que nos interesan resultan un caso particular de los que hemos descrito hasta el momento: son los anillos de valoración discreta, de los que ya hemos hablado en el segundo capítulo, y que verifican en particular que $v(K^*) = \mathbb{Z}$. Además, son dominios de ideales principales y el uniformizante, que denotábamos por π es el generador de los ideales. Es decir, los ideales son de la forma $u\pi^n$ con u unidad, es decir, ideales de la forma $\mathfrak{p}^n = \{x \in \mathcal{O} : v(x) \geq n\}$. El uniformizante verificará, además, que $v(\pi) = 1$.

Observación 4.5. En general, si K es un cuerpo, el uniformizante π es el elemento que verifica que $|\pi| = \frac{1}{s}$, y se tratará del elemento con mayor valor absoluto menor que 1.

Proposición 4.6 ([11])**.** *$\mathfrak{p}^n/\mathfrak{p}^{n+1}$ y $\mathcal{O}/\mathfrak{p}$ son isomorfos.*

Ejemplo 4.7.

- Si $K = \mathbb{Q}_p$ entonces $\mathcal{O} = \mathbb{Z}_p$ y $\mathfrak{p} = p\mathbb{Z}_p$. Además, $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.
- Si $K = F((X))$ es el cuerpo de las series de Laurent de X sobre un cuerpo F, denotemos por $\text{ord}(f), f = a_n X^n \in K$ como el menor n tal que $a_n \neq 0$ (por convenio ord(0)=∞). Sabemos que podemos tomar un $c \in \mathbb{R}$, $c > 1$ tal que $|f| = c^{-\text{ord}(f)}$. En estas condiciones $\mathcal{O} = F[[X]]$, $\mathfrak{p} = (X)$ y $\mathcal{O}/\mathfrak{p}$ es isomorfo a F.

Observación 4.8. Tenemos las siguientes propiedades sobre cuadrados en el cuerpo de residuos que resultan de aplicar el Lema de Hensel:

- Si K es un cuerpo que no tiene característica 2 y $a \in \mathcal{O}^*$ es cuadrado en K, entonces a es cuadrado en $\mathcal{O}/\mathfrak{p}$. Basta aplicar el Lema de Hensel al polinomio $X^2 - a$.
- Si K tiene característica 0 y $\mathcal{O}/\mathfrak{p}$ tiene característica 2 $a\mathcal{O}$ es cuadrado en K si y solo si a es cuadrado módulo $4\mathfrak{p}$.

4.1. Cuerpos Locales

Definición 4.9. Un cuerpo local K es un cuerpo completo respecto de un valor absoluto discreto, no arquimediano y cuyo cuerpo de residuos es finito.

Siguiendo con la notación empleada anteriormente comprobemos cómo son los elementos de K. Denotemos por π al uniformizante y dado $\mathcal{O}/\mathfrak{p}$ consideremos S un conjunto de representantes de dicho conjunto cociente. Si $x \in K$ y $x \in \mathcal{O}$ entonces x tiene una expansión $\pi-$ádica única $x = c_0 + c_1\pi + c_2\pi^2 + \cdots$ donde los $c_i \in S$ están determinados de forma única por x. Si $x \in K \setminus \mathcal{O}$ entonces $x = y/\pi^m$, con $y \in \mathcal{O}$ y $m \geq 1$, y entonces $x = c_0\pi^{-m} + c_1\pi^{-m+1} \cdots$.

Proposición 4.10. *Si K es un cuerpo completo respecto de un valor absoluto no arquimediano no trivial y consideramos la topología inducida por dicho valor absoluto, entonces las 3 condiciones siguientes son equivalentes:*

1. *K es cuerpo local.*
2. *$\mathcal{O}$ es compacto.*
3. *K es localmente compacto.*

Demostración.
(1) $\implies$ (2). K es un espacio métrico con el valor absoluto considerado. Por tanto, para demostrar que $\mathcal{O}$ es compacto probaremos que es secuencialmente compacto, ya que esta propiedad equivale a la compacidad en espacios métricos. Sea S un conjunto de clases de representantes de $\mathfrak{p}$ y π el uniformizante. Sea A_n una sucesión en $\mathcal{O}$. Como K es local S es un conjunto finito, y entonces hay infinitos términos de K que tienen al primer coeficiente c_0 en común en su expansión π-ádica. Razonando de forma similar, infinitos términos de entre los que tienen a c_0 en común tendrá al segundo coeficiente de la expansión, c_1. Continuando así sucesivamente podemos concluir que A_n tiene una sucesión de Cauchy. Como K es completo esta sucesión es convergente, y como la sucesión está en $\mathcal{O}$, es convergente y $\mathcal{O}$ es cerrado en K (por definición), el límite de la sucesión también está en $\mathcal{O}$, es decir, $\mathcal{O}$ es secuencialmente compacto.

(2) $\implies$ (1). El ideal $\mathfrak{p}$ es abierto en $\mathcal{O}$, de modo que las clases $x + \mathfrak{p}$, $x \in \mathcal{O}$, forman un recubrimiento por abiertos de $\mathcal{O}/\mathfrak{p}$. Como por hipótesis $\mathcal{O}$ es compacto todo recubrimiento por abiertos posee un subrecubrimiento finito, por lo que $\mathcal{O}/\mathfrak{p}$ contará con un número finito de clases $x + \mathfrak{p}$, es decir, $\mathcal{O}/\mathfrak{p}$ es finito. Para ver ahora que es discreto, por reducción al absurdo, supongamos que no lo es; por definición y por la Observación 4.5, existe una sucesión en $\mathcal{O}$ de forma que $|x_1| < |x_2| < |x_3| < \cdots < 1$ y $\lim_{i\to\infty} |x_i| = 1$ (fijémonos en que la sucesión $\{x_i\}_{i\in\mathbb{N}}$ no tiene que ser necesariamente convergente). Puesto que $\mathcal{O}$ es compacto toda sucesión tiene una subsucesión convergente. Concretamente, la sucesión anterior tiene entonces una subsucesión convergente cuyo límite x tiene valor absoluto 1. Entonces si $|x - x_i| < 1$, como el valor absoluto es no arquimediano $|x_i| = 1$ para todo i, llegando a una contradicción. En consecuencia, es discreto.

(2) $\implies$ (3). Sea $y \in K$. Como $\mathcal{O}$ es un entorno compacto para el 0 y el homeomorfismo $f(x) = y + x$ va de K en sí mismo, $y + \mathcal{O}$ es un entorno compacto de y.

(3) $\implies$ (2). Sea A un entorno compacto del 0. Sea $\alpha \in \mathcal{O}$ que verifica que $0 < |\alpha| < 1$ y que $\alpha^n \to 0$ si $n \to \infty$. Como A es entorno de 0 a partir de un n suficientemente grande los conjuntos $\alpha^n\mathcal{O} = \{x : |x| \leq |\alpha|^n\}$ están contenidos en A. Los conjuntos $\alpha^n\mathcal{O}$ son cerrados en A, y como todo conjunto cerrado en un compacto es también compacto, los conjuntos $\alpha^n\mathcal{O}$ son compactos. Definiendo ahora el homeomorfismo $g : \alpha^n\mathcal{O} \to \mathcal{O}$, $g(x) = x\alpha^{-n}$ concluimos que $\mathcal{O}$ es compacto, al tratarse de la imagen de un conjunto compacto mediante una aplicación continua. □

A continuación veremos un resultado muy importante que nos permite caracterizar los cuerpos locales.

Teorema 4.11 ([5])**.** *Los cuerpos locales son las extensiones finitas de los cuerpos $\mathbb{Q}_p$ y $F_p((X))$, donde F_p denota al cuerpo finito de p elementos.*

4.2. Formas Cuadráticas sobre Cuerpos Locales

En esta parte, y salvo que se indique lo contrario, K será un cuerpo local de característica distinta de 2, π un uniformizante y $\mathcal{O}$ el anillo de enteros. A diferencia del cuerpo local K, el cuerpo de residuos sí podría tener característica 2. Para esta sección emplearemos conceptos y resultados sobre formas cuadráticas que ya hemos trabajado en el capítulo de Preliminares, así como propiedades del Símbolo de Hilbert.

Teorema 4.12. *Si Q es una forma cuadrática no degenerada sobre K. Entonces para alguna base se tiene que $Q(x_1, \ldots, x_n) = a_1x_1^2 + \cdots + a_rx_r^2 + \pi(a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2)$, donde a_i es unidad para todo $i = 1, \ldots, n$.*

Demostración. Sin pérdida de la generalidad podemos suponer que Q es una forma cuadrática diagonal, es decir, de la forma descrita en el Teorema 1.50, por lo que podemos escribir $Q(x_1, \ldots, x_n) = a_1'x_1^2 + \cdots + a_n'x_n^2$, $a_i' \in K^*$. Entonces o bien $a_i' = a_i\pi^{2e_i+1}$ o bien $a_i' = a_i\pi^{2e_i}$ y a_i unidad. Realizando ahora un cambio de variable de la forma $x_i' = x_i\pi^{e_i}$ y reajustando los vectores de la base obtenemos el resultado deseado. □

Definición 4.13. Un vector $(\alpha_1, \ldots, \alpha_n) \in \mathcal{O}^n$ se dice primitivo si para algún $i \in \{1, \ldots, n\}$ α_i es distinto de cero en el cuerpo de residuos.

Proposición 4.14 ([2])**.** *Toda forma cuadrática sobre un cuerpo local que posee un vector isotrópico tiene también un vector primitivo isotrópico.*

Teorema 4.15 ([2])**.** *Si el cuerpo de residuos de K tiene característica distinta de 2, entonces la ecuación $a_1x_1^2 + \cdots + a_rx_r^2 + \pi(a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2) = 0$, con $a_i \in \mathcal{O}^*$, tiene solución no trivial sobre K si, y solo si $a_1x_1^2 + \cdots + a_rx_r^2 = 0$ o $a_{r+1}x_{r+1}^2 + \cdots + a_nx_n^2 = 0$, al menos una de ellas, tiene solución no trivial sobre K.*

Teorema 4.16 ([2])**.** *Sean K un cuerpo local cuyo cuerpo de residuos tiene característica distinta de 2, y $\alpha, \beta, \gamma \in \mathcal{O}^*$. Entonces la forma cuadrática $\alpha x^2 + \beta y^2 + \gamma z^2$ tiene un vector isotrópico en K^3.*

Corolario 4.17. *Si el cuerpo de residuos de K tiene característica distinta de 2, entonces cualquier forma cuadrática de dimensión igual o superior a 5 tiene un vector isotrópico.*

Demostración. Basta centrarnos en el caso de las formas cuadráticas no degeneradas, ya que las formas cuadráticas degeneradas tienen siempre algún vector isotrópico. Sea Q una forma cuadrática no degenerada. Por el Teorema 4.12 podemos escribir $Q = Q_1 + \pi Q_2$ de forma que los coeficientes Q_1 y Q_2 estén en $\mathcal{O}^*$ y ambas formas sean diagonales. Puesto que $\dim Q_1 + \dim Q_2 \geq \dim Q = 5$ al menos una de las formas debe tener dimensión igual o superior a 3. Basta entonces considerar esta forma cuadrática y darle el valor 0 a todas las variables excepto 3. Esta forma cuadrática en 3 variables poseerá un vector isotrópico por el Teorema 4.16. □

Proposición 4.18 ([2])**.** *Sea K un cuerpo con cuerpo de residuos con característica 2. Consideremos la ecuación $a_1x_1^2 + \cdots + a_nx_n^2 = 0$, donde $a_i \in \mathcal{O}^*$ para todo $i \in \{1, \ldots, n\}$. Entonces la ecuación tiene solución no trivial sobre K^n si, y solo si, la congruencia $a_1x_1^2 + \cdots + a_nx_n^2 \equiv 0 \,(\text{ mód } 4\pi)$ tiene una solución primitiva.*

A continuación vamos a relacionar el Símbolo de Hilbert y las formas cuadráticas a través del siguiente concepto.

Definición 4.19. Sean K un cuerpo local de característica distinta de 2, o $K = \mathbb{R}$, y Q una forma cuadrática no degenerada de dimensión n sobre K equivalente a la forma cuadrática $a_1x_1^2 + \cdots + a_nx_n^2$, $a_i \in K$. El invariante de Hasse de Q se define como

$$c_K(Q) = \prod_{i<j} (a_i, a_j)_K \in \{1, -1\}$$

En el caso de que la dimensión sea 1 se toma por convención $c_K(Q) = 1$. El invariante de Hasse no depende de la base elegida.

Teorema 4.20 ([2])**.** *Sean K un cuerpo local de característica distinta de 2, o $K = \mathbb{R}$, y Q una forma cuadrática no degenerada de dimensión 2 sobre K. Entonces, dado $b \in K^*$, Q toma el valor b sobre K si, y solo si $(b, -\operatorname{disc}(Q))_K = c_K(Q)$.*

Teorema 4.21 ([2])**.** *Si K es un cuerpo de característica impar, entonces toda forma cuadrática de dimensión mayor o igual que 5 posee un vector isotrópico.*

Vamos a trabajar ahora con $K = \mathbb{Q}_p$, donde p es un entero primo, y con formas cuadráticas no degeneradas. El resultado nos proporciona condiciones del discriminante y del invariante de Hasse de una forma cuadrática para que esta tenga algún vector isotrópico, en función de su dimensión.

Teorema 4.22. *Una forma cuadrática Q de dimensión n representa a 0 si, y solo si:*

1. $n = 2$ *y* $\operatorname{disc}(Q) = 1$ *en* K^*/K^{*^2}.
2. $n = 3$ *y* $(-1, -\operatorname{disc}(Q))_K = c_K(Q)$.
3. $n = 4$ *y, o bien* $\operatorname{disc}(Q) \neq 1$, *o bien* $\operatorname{disc}(Q) = 1$ *y* $c_K(Q) = (-1, -1)$.
4. $n \geq 5$.

Demostración. Veamos la demostración para $n = 2, 3$. Q es equivalente a una forma cuadrática $a_1x_1^2 + \cdots + a_nx_n^2$.

1. $n = 2$. Q representa al 0 si, y solo si, existe $(k_1, k_2) \in K^2$ tal que $Q((k_1, k_2)) = a_1k_1^2 + a_2k_2^2 = 0$, es decir, $\frac{-a_1}{a_2}$ es cuadrado en K. Como $\frac{-a_1}{a_2} = -a_1a_2 = -\operatorname{disc}(Q)$, entonces $\operatorname{disc}(Q) = -1$ en K^*/K^{*^2}.

2. $n = 3$. $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ representa a 0 si, y solo si, la forma $-a_3a_1x_1^2 - a_3a_2x_2^2 - x_3^2$, que es equivalente a la forma $-a_3Q$, representa a 0. Por definición de Símbolo de Hilbert esto ocurre si, y solo si $(-a_3a_1, -a_3a_2)_K = 1$. Empleando las propiedades de la Proposición 3.4 y la bilinealidad podemos expandir la expresión de la siguiente forma:

   $$(-a_3a_1, -a_3a_2) = (-1, -a_3a_2)(a_3a_1, -a_3a_2) = (-1, -1)(-1, a_3)(-1, a_2)(-a_3a_2, a_3a_1).$$

   Además, desarrollando $(-a_3a_2, a_3a_1)$ llegamos a que

   $$(-a_3a_2, a_3a_1) = (-1, a_3a_1)(a_3a_2, a_3a_1) = (-1, a_3)(-1, a_1)(a_3, a_3)(a_1, a_3)(a_2, a_3)(a_1, a_2).$$

   En consecuencia tenemos que

   $$(-a_3a_1, -a_3a_2) = (-1, -1)(-1, a_3)^2(-1, a_2)(-1, a_1)(a_3, a_3)(a_1, a_3)(a_2, a_3)(a_1, a_2).$$

   $(-1, a_3)^2 = 1$ por definición de Símbolo de Hilbert. Por las propiedades ya vistas, $(a_3, a_3) = (-1, a_3)$. En consecuencia, podemos reescribir la expresión anterior como

   $$(-1, -1)(-1, a_2)(-1, a_1)(-1, a_3)(a_1, a_3)(a_2, a_3)(a_1, a_2) = (-1, a_1a_2a_3)(a_1, a_3)(a_2, a_3)(a_1, a_2).$$

   Tenemos entonces que Q representa a 0 si, y solo si, $(-1, -1)(-1, \operatorname{disc}(Q))_K c_K(Q) = (-1, -\operatorname{disc}(Q))_K c_K(Q) = 1$, lo cual equivale a que $(-1, -\operatorname{disc}(Q))_K = c_K(Q)$.

□

Si $a \in K^*/K^{*^2}$ podemos considerar, dada una forma cuadrática Q de dimensión n, la forma $Q_a = Q - aZ^2$ (de dimensión $n+1$). Ya hemos visto en el primer capítulo que Q_a representa al 0 si, y solo si, Q representa a a. Generalizando el teorema previo tenemos el siguiente resultado:

Corolario 4.23. *Si $a \in K^*/K^{*^2}$ y Q es una forma cuadrática de dimensión n, Q representa a a si, y solo si:*

1. $n = 1$ *y* $a = \operatorname{disc}(Q)$.
2. $n = 2$ *y* $(a, -\operatorname{disc}(Q))_K = c_K(Q)$.
3. $n = 3$ *y, o bien* $\operatorname{disc}(Q) \neq -a$, *o bien* $\operatorname{disc}(Q) = -a$ *y* $c_K(Q) = (-1, -\operatorname{disc}(Q))$.
4. $n \geq 4$.

Teorema 4.24 ([14])**.** *Dos formas cuadráticas con la misma dimensión tienen igual discriminante e invariante de Hasse coincidente entre ellas si, y solo si, son equivalentes.*

Para terminar vamos a ver un invariante propio de las formas cuadráticas sobre $\mathbb{R}$.

Definición 4.25. Sea Q una forma cuadrática de dimensión n sobre $\mathbb{R}$. Esta forma cuadrática será equivalente a otra de la forma $x_1^2 + \cdots + x_r^2 - y_1^2 - \cdots - y_s^2$, $r, s \in \mathbb{N}, r + s = n$. El par (r, s) se denomina signatura de Q. Se dice que Q es una forma cuadrática definida si $r = 0$ o $s = 0$, e indefinida en caso contrario. Precisamente, la forma cuadrática representa al 0 si, y solo si, es indefinida.

Capítulo 5

Teorema de Hasse-Minkowski

Con todos los contenidos y resultados trabajados en los cuatro capítulos anteriores vamos ahora a enunciar y demostrar el Teorema de Hasse-Minkowski. La demostración es bastante extensa y complicada, y la realizaremos distinguiendo varios casos en función de la dimensión de la forma cuadrática considerada. Tras la demostración veremos un ejemplo de aplicación del resultado a una forma cuadrática concreta. Para terminar, veremos algunos teoremas conocidos sobre sumas de enteros y de cuadrados que se pueden deducir del Teorema de Hasse-Minkowski. Las referencias fundamentales en este capítulo son [2], [4] y [14].

5.1. Teorema de Hasse-Minkowski

Teorema 5.1 (Hasse-Minkowski)**.** *Sea Q una forma cuadrática $Q(x_1, \ldots, x_n)$ sobre $\mathbb{Q}$ de dimensión $n \geq 1$. Entonces:*

1. *Dado $r \in \mathbb{Q}^*$, a ecuación $Q(x_1, \ldots, x_n) = r$ es resoluble sobre $\mathbb{Q}$ si, y solo si es resoluble sobre $\mathbb{R}$ y sobre todo $\mathbb{Q}_p$.*
2. *La ecuación $Q(x_1, \ldots, x_n) = 0$ es resoluble de forma no trivial sobre $\mathbb{Q}$ si, y solo si es resoluble de forma no trivial sobre $\mathbb{R}$ y sobre todo $\mathbb{Q}_p$ (donde ser resoluble de forma no trivial quiere decir que la solución no es el vector con todas las componentes nulas).*

Antes de pasar a la demostración vamos a realizar una serie de aclaraciones de importancia. Probaremos solo el segundo enunciado, ya que el primero se puede deducir del segundo gracias a que dados $a \in \mathbb{Q}$ y Q una forma cuadrática, la ecuación $Q = a$ tiene solución no trivial si, y solo si, la ecuación $az^2 - Q$ tiene una solución no trivial. Del mismo modo, consideraremos formas cuadráticas no degeneradas, por el Teorema 1.44.

Demostraremos el resultado por inducción en la dimensión de la forma cuadrática, distinguiendo varias posibilidades.

5.1.1. Caso $n = 2$

Teorema 5.2 (Hasse-Minkowski: caso $n = 2$)**.** *Sea $Q(x_1, x_2) = a_1x_1^2+a_2x_2^2$ una forma cuadrática, con $a_1, a_2 \in \mathbb{Q}^*$. Entonces la ecuación $Q(x_1, x_2) = 0$ es resoluble no trivialmente sobre $\mathbb{Q}$ si, y solo si, lo es sobre $\mathbb{Q}_p$ para todo $p \in V$, donde V es el conjunto formado por los números primos y el infinito (y tal y como se ha denotado con anterioridad, $\mathbb{Q}_\infty = \mathbb{R}$).*

Para probar este caso enunciaremos y demostraremos los dos siguientes resultados.

Teorema 5.3. *Si F es un cuerpo de característica impar, entonces la forma cuadrática $a_1x_1^2 + a_2x_2^2$ tiene un vector isotrópico sobre F si, y solo si, $\frac{-a_2}{a_1} \in F^{*^2}$.*

Demostración. Veamos la condición necesaria. Supongamos que la forma cuadrática es resoluble no trivialmente sobre F, y sea (x_0, y_0) una solución no trivial. Supondremos que ambas son no nulas (si una de ellas lo fuese la otra lo tendría que ser también necesariamente). En ese caso, despejando en la ecuación obtenemos que $\frac{-a_2}{a_1} = \frac{x_0^2}{y_0^2}$, es decir, $\frac{-a_2}{a_1} \in F^{*^2}$.
En el caso de la condición suficiente, si $\frac{-a_2}{a_1} = z_0^2 \in F^{*^2}$ entonces $(z_0, 1)$ es un vector isotrópico. □

En el Teorema 5.3 hemos visto una condición necesaria y suficiente para que una forma cuadrática con coeficientes sobre un cuerpo de característica distinta de 2 tenga un vector isotrópico. Dicha condición es que el opuesto del cociente del segundo coeficiente entre el primero sea un cuadrado en el cuerpo. El segundo teorema, que enunciamos y demostramos a continuación, proporciona una relación entre los cuadrados de $\mathbb{Q}$ y de $\mathbb{Q}_p$, $p \in V$.

Teorema 5.4. *Si $x \in \mathbb{Q}^*$, entonces x es cuadrado en $\mathbb{Q}$ si, y solo si, lo es para todo $\mathbb{Q}_p$, $p \in V$.*

Demostración. Puesto que $\mathbb{Q} \subset \mathbb{Q}_p$ para todo $p \in V$, únicamente basta con probar la condición suficiente. Supongamos que $x = \pm p_1^{e_1} \cdots p_k^{e_k}$, donde $p_i \neq p_j$ para todo $i \neq j$ y $p_1, \ldots, p_k$ son primos. Si x es cuadrado en cada $\mathbb{Q}_p$ entonces los e_i son pares para todo $i \in \{1, \ldots, k\}$. Como x es cuadrado en $\mathbb{Q}_\infty = \mathbb{R}$, necesariamente $x > 0$. Así x es cuadrado en $\mathbb{Q}$. □

Hemos probado que un racional es cuadrado si, y solo si, lo es para todo $\mathbb{Q}_p$, $p \in V$. En el Teorema 5.3 probamos que una forma cuadrática tiene vector isotrópico si, y solo si, el opuesto del cociente del segundo coeficiente entre el primero sea un cuadrado en el cuerpo, y por el

Teorema 5.4, este cociente será cuadrado en $\mathbb{Q}$ si, y solo si, lo es para todo $\mathbb{Q}_p$, $p \in V$. Puesto que considerar la ecuación que resulta de igualar la forma cuadrática a 0 equivale a considerar la existencia, o no, de vectores isotrópicos para dicha forma cuadrática, todo esto permite deducir el resultado deseado: dada $Q(x_1, x_2) = a_1x_1^2 + a_2x_2^2$ una forma cuadrática, con $a_1, a_2 \in \mathbb{Q}^*$, se tiene que la ecuación $Q(x_1, x_2) = 0$ es resoluble no trivialmente sobre $\mathbb{Q}$ si, y solo si, lo es sobre $\mathbb{Q}_p$ para todo $p \in V$.

5.1.2. Caso $n = 3$

Tal y como ocurre en el caso $n = 2$, basta probar la condición suficiente.

Teorema 5.5 (Hasse-Minkowski: caso $n = 3$)**.** *Sea $Q(x_1, x_2, x_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ una forma cuadrática, con $a_1, a_2, a_3 \in \mathbb{Q}^*$. Entonces la ecuación $Q(x_1, x_2, x_3) = 0$ es resoluble no trivialmente sobre $\mathbb{Q}$ si, y solo si, lo es sobre $\mathbb{Q}_p$ para todo $p \in V$, donde V es el conjunto formado por los números primos y el infinito (y tal y como se ha denotado con anterioridad, $\mathbb{Q}_\infty = \mathbb{R}$).*

En primer lugar veremos que podremos centrarnos a estudiar, sin pérdida de la generalidad, la forma cuadrática $x_3^2 - ax_1^2 - bx_2^2$, donde a y b son enteros libres de cuadrados.

Aunque hemos supuesto que a_1, a_2 y a_3 son racionales no nulos, multiplicándolos por un mismo entero podrían pasar a ser enteros no nulos. Si alguno de estos enteros resultantes no fuese libre de cuadrados se podría hacer un cambio de variable para que dejase de serlo (por ejemplo, si a_1 multiplica a x_1^2 y d^2 es un factor que multiplica a a_1, se podría escribir $a_1'(dx_1)^2$, donde $a_1' = \frac{a_1}{d^2}$). Por otra parte, dado que estamos suponiendo que la ecuación $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ tiene una solución en $\mathbb{R}^3$ (caso $\mathbb{Q}_\infty$), a_1, a_2 y a_3 no pueden tener todos el mismo signo. Es decir, dos de ellos deben posee un signo y el tercero otro distinto. Sin pérdida de la generalidad podemos suponer que $a_1, a_2 < 0$ y $a_3 > 0$ y, finalmente, mediante un cambio de variable, podemos tomar $a_3 = 1$ y a_1 y a_2 enteros libres de cuadrados. En este caso, podemos suponer también, sin pérdida de la generalidad, que $|a_1| \leq |a_2|$.

Teorema 5.6. *Si la ecuación $x_3^2 - ax_1^2 - bx_2^2 = 0$, donde a y b son enteros libres de cuadrados, tiene solución no trivial sobre $\mathbb{Q}_p$ para todo $p \in V$, entonces tiene una solución no trivial sobre $\mathbb{Q}$.*

Demostración. Lo veremos por inducción en el entero $|a| + |b| = m$ ($|\ |$ denota al valor absoluto usual sobre $\mathbb{R}$). Si $|a|+|b| = 2$, entonces $|a| = |b| = 1$, por lo que se trataría de estudiar una forma

cuadrática de expresión $x_3^2 \pm x_1^2 \pm x_2^2$. Ya hemos descartado anteriormente el caso con todos los signos positivos. Para el resto sí existirán soluciones no triviales y que resultan sencillas de encontrar. Por ejemplo, para $x_3^2 - x_1^2 + x_2^2$ se podría tomar $(1, 0, 1)$ (el resto de casos serían análogos).

Vamos a suponer ahora que $|a| + |b| > 2$. Por hipótesis, $|a| \leq |b|$, por lo que $|b| \geq 2$. Demostraremos que a es cuadrado módulo b. b y a son por hipótesis libres de cuadrados, de modo que por el Teorema Chino de los Restos bastará comprobar que a es cuadrado módulo cualquier primo que divida a b. Sea p un entero primo que divide a b. Veamos que a es cuadrado módulo p. Si $a \equiv 0 \,(\text{mód}\, p)$ se tiene trivialmente. Si no, a es unidad p-ádica, y en este caso existe una solución $(x_0, y_0, z_0) \in (\mathbb{Q}_p)^3$ que podemos suponer primitiva, por la Proposición 2.83. La ecuación $x_3^2 - ax_1^2 - bx_2^2 = 0$ en módulo p pasaría a ser $x_3^2 - ax_1^2 \equiv 0 \,(\text{mód}\, p)$. Veamos que x_0 es unidad p-ádica. Si no lo fuese, $x_0 \equiv 0 \,(\text{mód}\, p)$, y como $z_0^2 - ax_0^2 \equiv 0 \,(\text{mód}\, p)$, $z_0 \equiv 0 \,(\text{mód}\, p)$. Entonces, by_0^2 es divisible por p^2, y como b es libre de cuadrados, $y_0 \equiv 0 \,(\text{mód}\, p)$. Si $x_0, y_0, z_0 \equiv 0 \,(\text{mód}\, p)$ la solución no puede ser primitiva, lo cual es contradictorio. Por tanto, x_0 no es unidad p-ádica, y entonces como $ax_0^2 \equiv z_0^2 \,(\text{mód}\, p)$, a es cuadrado módulo p.

Sean $p_1, \ldots, p_k$ los primos que dividen a b. Como b es libre de cuadrados, $\mathbb{Z}/b\mathbb{Z} = \prod_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z}$, y entonces a es cuadrado módulo b, es decir, existen q, r tal que $a + bq = r^2$, es decir, $bq = r^2 - a$, y podemos tomar q tal que $|r| \leq \frac{|b|}{2}$. Por la Proposición 3.2 y la Observación 3.3 para bq, podemos concluir que $x_3^2 - ax_1^2 - bx_2^2 = 0$ tiene solución no trivial sobre un cuerpo si, y solo si, la tiene $x_3^2 - ax_1^2 - qx_2^2 = 0$. No obstante, tenemos que

$$|q| \leq \left|\frac{r^2 - a}{b}\right| \leq \frac{|b|^2}{4|b|} + \frac{|a|}{|b|} \leq \frac{|b|}{4} + 1,$$

ya que $|r| \leq |\frac{b}{2}|$ y $|a| \leq |b|$. Descomponiendo $q = q's^2$, donde q' es entero libre de cuadrados, podemos deducir de un modo análogo que $x_3^2 - ax_1^2 - qx_2^2 = 0$ tiene solución no trivial sobre un cuerpo si, y solo si, la tiene $x_3^2 - ax_1^2 - q'x_2^2 = 0$. Puesto que $|q'| < |b|$, $|a| + |q'| \leq |a| + |b|$, y aplicando la hipótesis de inducción $x_3^2 - ax_1^2 - q'x_2^2 = 0$ tiene alguna solución no trivial en $\mathbb{Q}$, lo cual implica que la forma cuadrática del enunciado también la posee. □

5.1.3. Caso $n = 4$

Teorema 5.7 (Hasse-Minkowski: caso $n = 4$). *Sea $Q(x_1, x_2, x_3, x_4) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ una forma cuadrática, con $a_1, a_2, a_3, a_4 \in \mathbb{Q}^*$. Entonces la ecuación $Q(x_1, x_2, x_3, x_4) = 0$ es resoluble no trivialmente sobre $\mathbb{Q}$ si, y solo si, lo es sobre $\mathbb{Q}_p$ para todo $p \in V$, donde V es el conjunto formado por los números primos y el infinito (y tal y como se ha denotado con anterioridad, $\mathbb{Q}_\infty = \mathbb{R}$).*

Demostración. Continuamos probando solo la condición suficiente. Podemos escribir como una forma cuadrática de la forma $ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)$, con $a, b, c, d \in \mathbb{Q}$. Sea $p \in V$. La ecuación $ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2) = 0$ tiene una solución no trivial en $(\mathbb{Q}_p)^4$. Por el Corolario 1.49, existe un x_p representado por $ax_1^2 + bx_2^2$ y por $cx_3^2 + dx_4^2$. Gracias al Corolario 4.23 (caso $n = 2$), esto equivale a que $(x_p, -ab)_p = (a, b)_p$ y $(x_p, -cd)_p = (c, d)_p$. Puesto que los valores posibles de las igualdades anteriores son 1 o -1 y que $\prod_{p \in V} (a, b)_p = 1$ y $\prod_{p \in V} (c, d)_p = 1$, podemos aplicar el Teorema 3.16 y deducir que existe un $x \in \mathbb{Q}^*$ tal que $(x, -ab)_p = (a, b)_p$ y $(x, -cd)_p = (c, d)_p$ para todo $p \in V$. En ese caso las formas cuadráticas $ax_1^2 + bx_2^2 - xy^2$ y $cx_3^2 + dx_4^2 - xy^2$ representan a 0, de lo cual se deduce que Q también lo hace. □

5.1.4. Caso $n \geq 5$

Sea $n \in \mathbb{Z}, n \geq 5$.

Teorema 5.8. *Sea $Q(x_1, \ldots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$ una forma cuadrática, con $a_1, \ldots, a_n \in \mathbb{Q}^*$. Entonces la ecuación $Q(x_1, \ldots, x_n) = 0$ es resoluble de forma no trivial sobre $\mathbb{Q}$ si, y solo si es resoluble de forma no trivial sobre $\mathbb{R}$ y sobre todo $\mathbb{Q}_p$ (donde ser resoluble de forma no trivial quiere decir que la solución no es el vector con todas las componentes nulas).*

Demostración. Lo haremos por inducción en n. Podemos descomponer Q como $Q = Q_1 - Q_2$, donde $Q_1(x_1, x_2) = a_1x_1^2 + a_2x_2^2$ y $Q_2(x_3, \ldots, x_n) = -(a_3x_3^2 + \cdots + a_nx_n^2)$. Sea $S = \{2, \infty\} \cup \{p : v_p(a_i) \neq 0$ para algún $i \geq 3\} \subset V$, donde v_p denota, como en el segundo capítulo, a la valoración p-ádica. Este conjunto es finito. Dado $v \in S$, por el Corolario 1.49 Q_1 y Q_2 representan a un α_v, por tener Q un vector isotrópico en $\mathbb{Q}_v$, por hipótesis. Por tanto, existe $x^v = (x_1^v, \ldots, x_n^v) \in \mathbb{Q}_v$ tal que $Q(x_1^v, x_2^v) = Q(x_3^v, \ldots, x_n^v) = \alpha_v$.

Por otro lado, gracias a varios resultados del segundo capítulo sabemos que $\mathbb{Q}_v^2$ es subgrupo abierto de $\mathbb{Q}_v$. En particular, los subconjuntos que contienen a α_v forman un abierto. Q_1 es continua, por lo que la imagen inversa de un abierto que contenga a α_v es un subconjunto abierto de $X_v \subset \mathbb{Q}_v \times \mathbb{Q}_v$. Por el Lema 3.14 existen $y_1, y_2 \in \mathbb{Q}$ tal que $(y_1, y_2) \in X_v$ para cada $v \in S$. Sea $Q_1(y_1, y_2) = \alpha$. $\alpha/\alpha_v \in \mathbb{Q}_v^2$ para cada $v \in S$. Sea ahora $Q_3 = \alpha z^2 - Q_2$. Sea $v \in V$. Si $v \in S$, Q_3 tiene un cero no trivial en $\mathbb{Q}_v$ ya que $\alpha/\alpha_v \in \mathbb{Q}_v^2$. Si $v \in V \setminus S$, puesto que la dimensión de Q_2 es $n - 2 \geq 3$, por el Teorema 4.16, podremos encontrar una solución no trivial para $Q_2 = 0$ (el Teorema 4.16 garantiza la existencia para tres variables, de modo que si $n > 5$ sería suficiente considerar tres de las variables de Q_2 y que el resto tomen el valor 0). Esto permite encontrar una solución no trivial para $Q_3 = 0$. En consecuencia, $Q_3 = 0$ tiene una solución no trivial para todo $v \in V$. Como la dimensión de Q_3 es $n - 1$, por la hipótesis de inducción, $Q_3 = 0$ tiene una

solución no trivial en $\mathbb{Q}$. Por tanto, la ecuación $Q_2 = \alpha$ tiene una solución no trivial en $\mathbb{Q}$, y $Q_1 = \alpha$, por definición de α, también. En conclusión, $Q = 0$ tiene igualmente una solución no trivial en $\mathbb{Q}$. □

Observación 5.9. No se ha podido establecer un resultado análogo al Teorema de Hasse-Minkowski para polinomios de grado mayor o igual que 3. El matemático Ernst Selmer demostró que la ecuación $3x^3 + 4y^3 + 5z^3 = 0$ tiene solución no trivial con valores en $\mathbb{Q}_p$ para todo $p \in V$, pero no la tiene en $\mathbb{Q}^3$. El desarollo completo realizado por este matemático se puede encontrar en [13].

5.2. Ejemplos y Aplicaciones

Vamos a ver un ejemplo de aplicación del Teorema de Hasse-Minkowski a una forma cuadrática concreta siguiendo el procedimiento empleado en [4].

Ejemplo 5.10. Consideremos la forma cuadrática $f(x, y, z) = 13x^2 - 2y^2 + 11z^2$. Utilizando el Teorema de Hasse-Minkowski y el Lema de Hensel vamos a comprobar que la ecuación $f = 0$ tiene alguna solución no trivial sobre $\mathbb{Q}^3$. Para ello veremos que tiene alguna solución no trivial sobre $(\mathbb{Q}_p)^3$ para todo $p \in V$. Distinguiremos varios casos:

- $p = \infty$ ($\mathbb{Q}_p = \mathbb{R}$). Una posible solución que se puede encontrar de forma sencilla es $(1, \sqrt{\frac{13}{2}}, 0)$.
- $p \in V \setminus \{\infty, 2, 11, 13\}$. Por el Corolario 1.12, existirá una solución (x_0, y_0, z_0) no trivial módulo p. Por ser esta solución no trivial alguna de las componentes no es divisible por p. Supongamos que es x_0 (si fuesen y_0 y z_0 serían similares). En ese caso, sea $f_1(x) = 13x^2 - 3y_0^2 + 11z_0^2$. $f_1(x_0) \equiv 0\,(\text{mód } p)$, por definición. Además $f_1'(x_0) = 26x_0 \not\equiv 0\,(\text{mód } p)$, ya que $p \neq 2, 13$. De ambas cosas concluimos que $v_p(f_1(x_0)) \geq 1$ y $v_p(f_1'(x_0)) \leq 0$. Como $|f_1(x_0)|_p = p^{-v_p(f_1(x_0))} \leq p^{-1}$ y $|f_1'(x_0)|_p^2 \geq p^0 = 1$, se cumplen las hipótesis del Lema de Hensel (Teorema 2.89), y entonces existe una solución $(\overline{x_0}, y_0, z_0) \in (\mathbb{Q}_p)^3$.
- $p = 2$. Sean $y_0 = 0$ y $z_0 = 1$. $f_2(x) = f(x, y_0, z_0) = 13x^2 + 11$ y $f_2'(x) = 26x$. $x_0 = 1$ es raíz de $f_2(x)$ y de $f_2'(x)$ módulo 2. Además, $v_2(f_2(1)) = 3$ y $v_2(f_2'(1)) = 1$. De nuevo se cumplen las hipótesis del Lema de Hensel, lo que garantiza la existencia de una solución $(\overline{x_0}, y_0, z_0) \in (\mathbb{Q}_2)^3$.
- $p = 11$. Tomando $y_0 = 1$ y $z_0 = 0$ tenemos que $f_3(x) = f(x, y_0, z_0) = 13x^2 - 2$. $x_0 = 1$ es raíz de $f_3(x)$ módulo 11, pero no lo es de $f_3'(x)$. Como en las posibilidades anteriores vuelven a cumplirse las hipótesis del Lema de Hensel, que permite asegurar la existencia de una solución $(\overline{x_0}, y_0, z_0) \in (\mathbb{Q}_{11})^3$.

- $p = 13$. Si $x_0 = 0$ y $y_0 = 5$, $f_4(z) = f(x_0, y_0, z) = 11z^2 - 50$. Tomando $z_0 = 1$ tenemos una raíz de $f_4(z)$ módulo 13, pero no lo es de $f_4'(z)$, proporcionándonos, por el Lema de Hensel, una solución $(x_0, y_0, \overline{z_0}) \in (\mathbb{Q}_{13})^3$

Como $f = 0$ tiene solución no trivial sobre $(\mathbb{Q}_p)^3$ para todo $p \in V$, por el Teorema de Hasse-Minkowski posee igualmente una solución no trivial sobre $(\mathbb{Q})^3$. En efecto, una solución no trivial sobre $(\mathbb{Q})^3$ es $(3, 8, 1)$.

A continuación vamos a enunciar y demostrar algunos conocidos resultados referentes a sumas de cuadrados empleando el Teorema de Hasse-Minkowski.

Lema 5.11 ([2])**.** *Si un entero se puede escribir como suma de tres cuadrados de números racionales, entonces se puede escribir como suma de tres cuadrados de números enteros.*

Teorema 5.12 (Legendre)**.** *Sea $n \in \mathbb{Z}^+$, escribamos n como $n = 4^\alpha m$, donde $m \in \mathbb{Z}^+$ no es múltiplo de 4 y $\alpha \in \mathbb{Z}^+ \cup \{0\}$. Entonces n se puede escribir como suma de tres cuadrados de enteros si, y solo si, $m \not\equiv 7 \,(\text{mód } 8)$.*

Demostración. Por el Lema 5.11, si n es suma de tres cuadrados de enteros, m también lo es. En ese caso, puesto que los posibles valores de cuadrados de enteros módulo 8 son 0, 1 y 4, $m \not\equiv 7 \,(\text{mód } 8)$.

Veamos la condición suficiente. Si $m \not\equiv 7 \,(\text{mód } 8)$, entonces los posibles valores para m en módulo 8 son 1,2,3,5 y 6, ya que 4 y m son coprimos, por hipótesis. Veamos que m se puede escribir como suma de tres cuadrados de enteros. Si p es un cuadrado impar, entonces por el Teorema 4.16 (para el caso en el que los coeficientes valen todos 1) la ecuación $x^2 + y^2 + z^2 = 0$ tiene una solución no trivial en $\mathbb{Q}_p$. Por el Teorema 1.39, la forma cuadrática es universal para $\mathbb{Q}_p$. Es obvio que $x^2 + y^2 + z^2$ representa a m en $\mathbb{R}$, por lo que basta comprobar el caso $p = 2$ considerando la expresión de la forma cuadrática módulo 8 y distinguiendo diversas posibilidades en función de los valores de m módulo 8:

1. Si $m \equiv 1 \,(\text{mód } 8)$, entonces puede vale la terna $(0, 1, 0)$ y sus posibles permutaciones entre valores de las componentes (en este caso, $(1, 0, 0)$ y $(0, 0, 1)$).
2. Si $m \equiv 2 \,(\text{mód } 8)$, entonces puede vale la terna $(1, 1, 0)$ y sus posibles permutaciones.
3. Si $m \equiv 3 \,(\text{mód } 8)$, entonces vale la terna $(1, 1, 1)$.
4. Si $m \equiv 5 \,(\text{mód } 8)$, entonces puede vale la terna $(1, 2, 0)$ y sus posibles permutaciones.
5. Si $m \equiv 6 \,(\text{mód } 8)$, entonces puede vale la terna $(1, 2, 1)$ y sus posibles permutaciones.

Entonces $x^2 + y^2 + z^2 - mt^2$ tiene una solución primitiva módulo 8, y por la Proposición 4.18 posee una solución en $\mathbb{Q}_2$. Es decir, $x^2 + y^2 + z^2 = m$ tiene solución en $(\mathbb{Q}_p)^3$ para todo $p \in V$. Por el Teorema de Hasse-Minkowski, también existe una solución en $\mathbb{Q}$, y por el Lema 5.11, se puede escribir como suma de tres cuadrados de enteros. Como $n = 4^\alpha m$, n también es suma de tres cuadrados de enteros. □

Corolario 5.13 (Lagrange)**.** *Todo entero positivo se puede escribir como suma de cuatro cuadrados de enteros.*

Demostración. Sea $n \in \mathbb{Z}^+$. Factoricemos n como en el Teorema 5.12: $n = 4^\alpha m$, donde $m \in \mathbb{Z}^+$ no es múltiplo de 4 y $\alpha \in \mathbb{Z}^+ \cup \{0\}$. Si $m \not\equiv 7 \,(\text{mód } 8)$, m es suma de tres cuadrados de enteros, por lo que también lo es de cuatro trivialmente (basta tomar como cuarto cuadrado el 0). Si $m \equiv 7 \,(\text{mód } 8)$, $m - 1 \not\equiv 7 \,(\text{mód } 8)$, por lo que $m - 1$ es suma de tres cuadrados de enteros, y m será suma de estos tres cuadrados y el 1. □

Corolario 5.14 (Gauss)**.** *Todo entero positivo se puede escribir como suma de tres números triangulares.*

Demostración. Sea $n \in \mathbb{Z}^+$, y consideremos el entero $8n + 3$. Por el Teorema 5.12 aplicado a $8n + 3$, existen $x, y, z \in \mathbb{Z}$ tal que $x^2 + y^2 + z^2 = 8n + 3$. En este caso se tiene, además, que $x^2 + y^2 + z^2 = 8n + 3 \equiv 3 \,(\text{mód } 8)$, y tal y como hemos analizado en el Teorema 5.12, la única posibilidad es que $x^2 \equiv y^2 \equiv z^2 \equiv 1 \,(\text{ mód } 8)$, lo que quiere decir que x, y y z son enteros impares. Es decir, existen $m_1, m_2, m_3 \in \mathbb{Z}$ tales que $x = 2m_1 + 1$, $y = 2m_2 + 1$ y $z = 2m_3 + 1$.

Los números triangulares son números de la forma $\frac{m(m+1)}{2}$, donde $m \in \mathbb{Z}$, por lo que tendremos la siguiente igualdad:

$$n = \frac{1}{8}(8n + 3 - 3) = \frac{1}{8}(x^2 + y^2 + z^2 - 3) = \frac{1}{8}\left[\sum_{i=1}^{3}(2m_i + 1)^2 - 3\right] = \sum_{i=1}^{3}\frac{m_i(m_i + 1)}{2},$$

ya que $\sum_{i=1}^{3}(2m_i + 1)^2 - 3 = (\sum_{i=1}^{3} 4m_i^2 + 4m_i + 1) - 3 = \sum_{i=1}^{3} 4m_i^2 + 4m_i = \sum_{i=1}^{3} 4m_i(m_i + 1)$. Por tanto, $\frac{1}{8}\left[\sum_{i=1}^{3}(2m_i + 1)^2 - 3\right] = \sum_{i=1}^{3}\frac{m_i(m_i + 1)}{2}$. □

Bibliografía

[1] P. M. Cohn, Algebra, Vol. 1, John Wiley & Sons, London-New York-Sydney, 1974.

[2] A. Gamzon, The Hasse-Minkowski Theorem (2006).
URL `https://opencommons.uconn.edu/srhonors_theses/17/`

[3] F. Q. Gouvêa, p-adic Numbers. An introduction, Universitext, 3rd ed., Springer, Cham, 2020.

[4] J. Hatley, Hasse-Minkowski and the Local-to-Global Principle (2009).
URL `https://www.math.union.edu/~hatleyj/Capstone.pdf`

[5] N. Jacobson, Basic Algebra. II, 2nd ed., W. H. Freeman and Company, New York, 1989.

[6] Y. Kitaoka, Arithmetic of quadratic forms, Cambridge University Press, 1993.

[7] W. J. LeVeque, Fundamentals of Number Theory, Addison-Wesley Publishing Company, 1977.

[8] P. López Somoza, Números p-ádicos (2019).
URL `https://minerva.usc.es/xmlui/handle/10347/26355`

[9] K. Martin, Number Theory II. Spring 2010 notes (2019).
URL `http://www2.math.ou.edu/~kmartin/ntii/ntii.pdf`

[10] J. R. Munkres, Topology, 2nd ed., Prentice Hall, Inc., Upper Saddle River, NJ, 2000.

[11] J. Neukirch, Algebraic Number Theory, vol. 322 of Grundlehren der mathematischen Wissenschaften, Springer-Verlag, Berlin, 1999.

[12] A. Schinck, The Local-Global Principle in Number Theory (2001).
URL `https://www.collectionscanada.gc.ca/obj/s4/f2/dsk3/ftp04/MQ64047.pdf`

[13] E. S. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Arithmetica (85) (1951) 203–362.

[14] J.-P. Serre, A course in arithmetic, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973.

[15] J.-P. Serre, Local fields, Springer-Verlag, New York-Heidelberg, 1979.

[16] E. Soto, El Contraexemple de Selmer al Principi de Hasse (2013).
URL `http://hdl.handle.net/2445/54163`